CALIFORNIA STATE SCIENCE FAIR
2014 PROJECT SUMMARY

Name(s) **Arjun M. Tambe**	**Project Number** 34682

Project Title

Improving Algorithms for the Optimal Allocation of Security Resources, Year 2

Abstract

Objectives/Goals

Security is a ubiquitous concern, vital for counterterrorism, wildlife reserve protection, crime prevention, and many other critical applications. Strategic resource allocation is crucial since limits on security resources prevent full protection of all targets at all times. Since adversaries can exploit predictable security strategies, protection schedules must be efficient and random. Algorithms based on game theory offer a mathematically sound approach for creating weighted random strategies that account for predicted adversary reactions and different values of different targets, and they are currently being used to allocate security resources at several global locations. While many of these algorithms assume perfect rationality among adversaries, a recent algorithm, MATCH, accounts for humans' imperfect decision-making and has offered better protection than other algorithms. Last year's research developed a new algorithm, NewMATCH, that outperforms MATCH in certain cases. Both MATCH and NewMATCH contain a certain parameter whose value affects the operation of the algorithm, but changing this value has not yet been explored in detail. This project aims to create new procedures for adjusting the value of this parameter to make MATCH and NewMATCH more effective.

Methods/Materials

This study offers 2 innovations: a new model for predicting adversary behavior that is also used in a procedure that determines the optimal value of the parameters in MATCH or NewMATCH, and the application of this procedure to tune these parameters. To test the procedures as applied to both algorithms in a setting that models a real-world security situation, this study solicited online participation with human subjects. Subjects took the role of an attacker in an online game, playing against a security force whose strategy was determined either with or without the new procedures.

Results

The new model for predicting adversary behavior better predicted adversary behavior than any of the other existing models tested. Algorithms whose parameters are tuned via the new procedures are shown to be more effective than algorithms that are not tuned.

Conclusions/Discussion

The new procedures offer significantly increased security and improved predictions of adversary behavior. The innovations in this project may have great potential to reduce the risk of dangerous security breaches if applied in the real world.

Summary Statement

A program for tuning algorithms that allocate limited security resources and a new model of human behavior are developed, which are more effective than procedures currently being used to protect many vulnerable locations.

Help Received

Dad (computer science professor) advised the research and writing of the abstract.

Preliminary