USC CREATE
HOMELAND SECURITY CENTER

Stochastic Game Models for Homeland Security

Erim Kardes, University of Southern California
kardes@usc.edu

1. Overview

Objective of this research is to model and analyze homeland security related adversarial decision problems thorough game theory. Using game theoretical approaches offers an alternative approach to the conventional decision analysis techniques as it captures the antagonism inherent in terrorism related decision making problems, where two (or more) decision makers interact adversely. Our primary objective is to capture this antagonism and to explicitly model an attacker. In this sense, our aim is to analyze the best response behavior of a defender against an attacker.

In many decision problems concerning adversaries, the decision process for a defender involves multiple stages. That is, once a decision is made by the defender, consequences of this decision may require subsequent decisions. Our secondary objective is to capture the multi-stage nature present in real-life decision making problems that include adversaries. To this end, we use concepts from stochastic game theory, which provide powerful tools to model such problems.

2. Research Accomplishments

2.1. Innovations in Modeling Decision Problems Including Adversaries

Stochastic game theory concepts offer a rich set of tools that helps us model multi-stage adversarial decision making problems. In this research, we first provide how these concepts can be used to construct models that are easy to communicate to the associated decision makers. Our modeling approach includes a graphical representation of the decision problem.

"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."

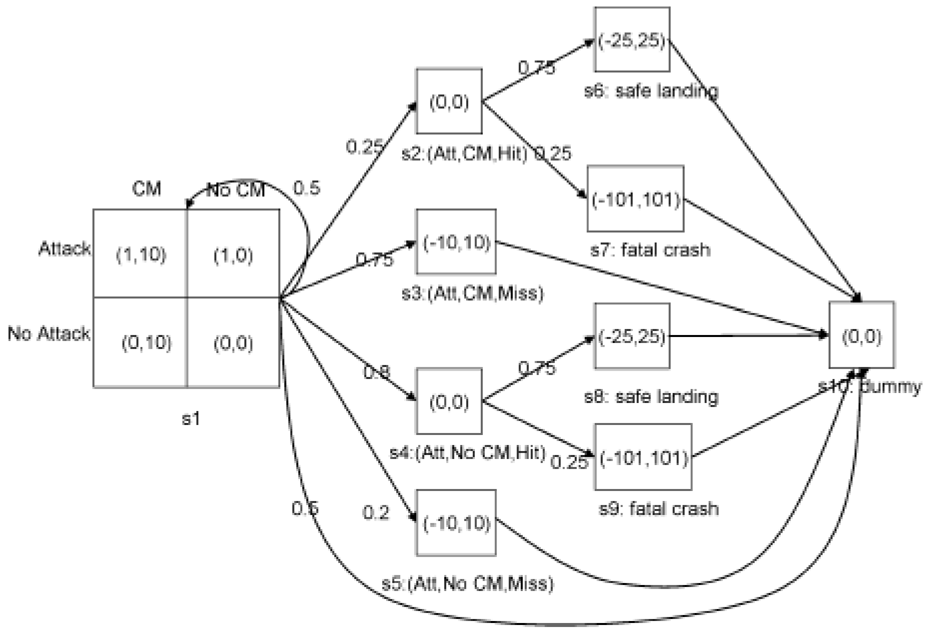

Figure 1. Graphical Representation of an Example Stochastic Game Model

Figure 1 depicts an example of a stochastic game model for the MANPADS problem. The first state in the model includes two alternative options for each player: The alternatives of “Attack” and “No Attack” for the attacker and the alternatives of “CM” and “No CM” that stand for the decisions to install countermeasures or not. The pairs of numbers in the cells of this 2x2 matrix indicate the baseline payoffs associated with each alternative combination. For example, if the defender chooses to install countermeasures and the attacker chooses to attack, the attacker is incurred a cost of attacking, which is $1 billion, whereas the defender is incurred the installation and maintenance cost of countermeasures of $10 billion over a horizon of ten years. Based on the possibly chosen alternatives in the first state, the process then moves into subsequent states where additional payoffs are incurred to the two players. For instance, if the defender chooses to install countermeasures and the attacker chooses to attack, with the possibility of a hit, the process moves onto state 2 with 0.25 probability, or to state 3 if there is no hit with a probability of 0.75. If there is a hit, the two subsequent states represent the possibilities of safe landing and fatal crash. If there is a miss, the game ends, but there is a possibility that the game will be repeated, represented by the arc from state 1 to itself.

2.2. Equilibrium Analysis

A set of analyses and results in stochastic game models for homeland security pertains to equilibrium behavior of the players. In other words, we first solve the above model for an equilibrium, where both the defender and the attacker strive to minimize their own payoffs (a negative payoff for the attacker implies a beneficial payoff). To this end, any given model is converted to an optimization problem, the optimum solution of which prescribes players the equilibrium policies. These policies may suggest a player to choose a given alternative with certainty, or to use randomized policies.

The important step in equilibrium analysis is to convert the graphical model to its associated optimization model. This is accomplished using a mathematical programming language, AMPL. The resulting optimization problems can be solved by using a nonlinear nonconvex optimization solver, named LOQO.

2.3. Sensitivity Analysis

Another line of analysis in stochastic game applications to homeland security investigates the behavior of the equilibrium solution as a function of critical parameter values. To this end, a tornado diagram can be constructed. A tornado diagram illustrates the sensitivity of the defender's overall cost in the game to the most significant parameters in the model, along the equilibrium path. To this end, we use command scripts in AMPL to alter parameters in the model and re-calculate equilibrium policies in an iterative manner. Sensitivity is measured by fluctuating one parameter value in the range assigned to it, while keeping all other parameters at their base values. Figure 2 illustrates a tornado diagram example associated with a container security model. In summary, a larger bar in Figure 2 implies a more sensitive parameter of the model.

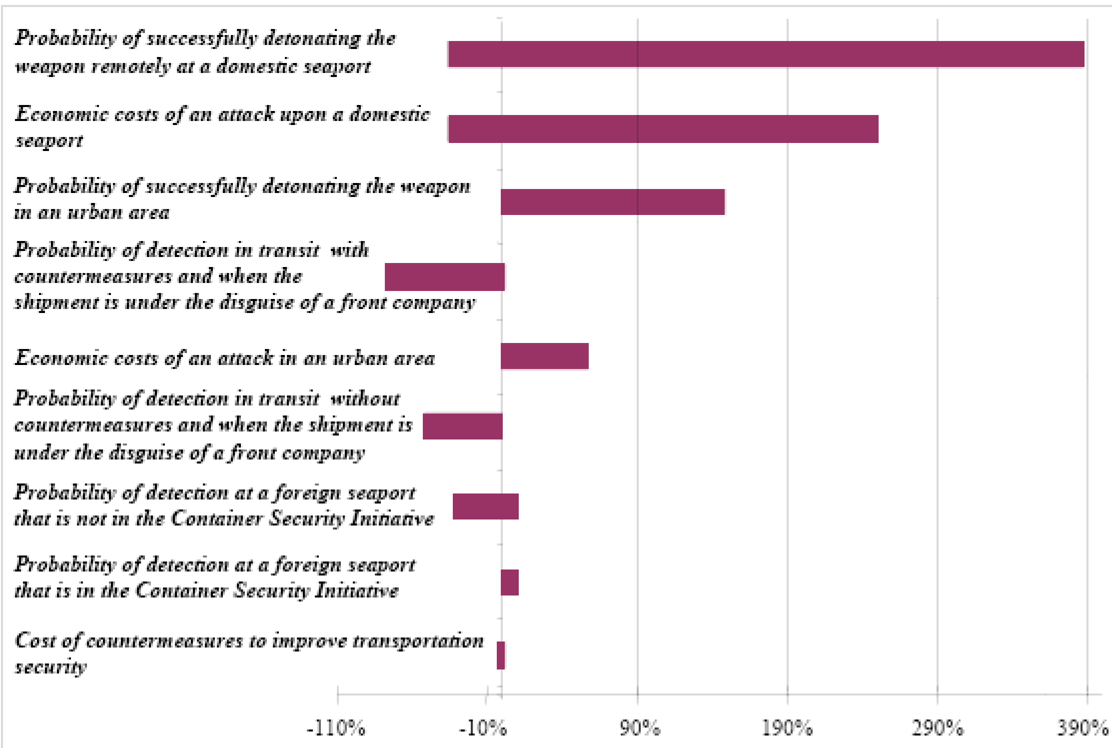

Figure 2. Tornado diagram illustrating the sensitivity of the overall costs to the defender

To understand the behavior at equilibrium better, we also analyze two-way sensitivity plots for significant parameters. These plots depict the data ranges that favor a specific alternative for each player.

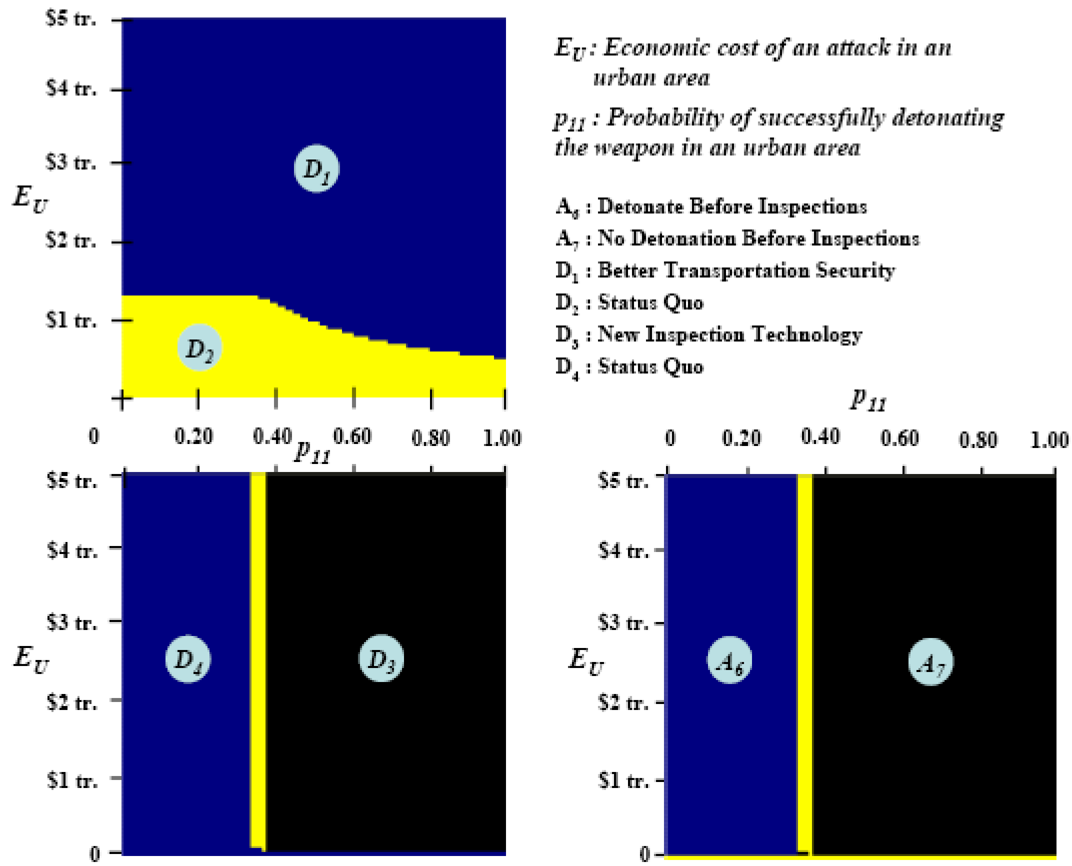

Figure 3. Illustrative Example for 2-way sensitivity analyses

Figure 3 depicts an illustrative example of two-way sensitivity analyses. Shaded regions indicate the parameter combinations that favor a specific defender decision (D_i) or an attacker decision (A_j).

2.4. Best Response Analysis

A third set of analyses that can be performed in stochastic game applications to homeland security is the best response analysis. The motivation for best response analysis is that an attacker may not behave rationally . Rather than determining policies by minimizing overall costs, the attacker may consider arbitrary polices that can be unpredictable to the defender. In such a case, we simulate the attacker's policies and determine the best response of the defender against such simulated policies. To this end, we use techniques from Markov decision processes, since the defender faces a Markov decision process when a decision for the attacker is simulated. Therefore, in this type of analyses, we solve corresponding Markov decision problems from the viewpoint of the defender.

3. Applied Relevance

3.1. MANPADS

In this work, we use concepts from stochastic game theory to investigate the strategies of two opponents in the MANPADS problem. Our analyses suggest that the countermeasures are cost-effective if the countermeasures cost over a ten year period is around $10 billion, the attack probability is high,

and if the fatal crash cost is more than $ 75 billion. This conclusion mirrors the conclusion given in [von Winterfeldt and Sullivan(2006)]. Furthermore, we conclude that if the attack probability is less than 0.4 and the re-play probability is low (around 0.1), then the countermeasures are not cost-effective unless economic costs associated with a fatal crash are very high (above $250 billion).
Finally, our results suggest that assuming the attack probability is around 0.2, countermeasures could be cost-effective if economic costs of a fatal crash is above $50 billion, and if the MANPADS threat continues to exist with high probability, given that no attacks occur and no countermeasures are installed.

The novel modeling approach presented in this study gave rise to another study within CREATE, which is briefly described next.

3.2. Overseas Cargo Container Security

In this work, we propose a stochastic game model that comparatively evaluates alternatives for improving container security. The players are an attacker who plans to send a nuclear weapon, and a defender who considers two alternatives at two nodes of interdiction along the path of containers. The attacker can choose the path of the container, the method of intrusion and the target, whereas the defender chooses whether to improve transportation security and whether to improve inspections at domestic seaports. The base case results suggest that the attacker chooses to attack by sending the nuclear weapon under the disguise of a front company and through a foreign seaport that does not participate in the Container Security Initiative. The target of choice is likely to be a domestic seaport despite the higher economic toll of an urban area attack. The defender, on the other hand, chooses to improve transportation security, but not inspections at domestic seaports given that the attacker plans to detonate the weapon before the authorities get a chance to act on it. We run sensitivity analyses to determine the most significant parameters of the model, and see how the baseline decisions change as a function of these significant parameters. The results in general recommend strong security measures along the entire path of containers movement rather than simply at the United States ports of entry. Results also suggest that terrorists will probably execute the attack as soon as the weapon reaches United States shores to reduce the probability of interdiction

3.3. Other Applicable Areas and Possible Collaborations

In stochastic game applications to homeland security, we develop AMPL scripts to solve our models for equilibrium as well as to perform sensitivity analyses and simulation. Using these scripts and a suitable solver, sensitivity could be performed both on the equilibrium strategies, as well as the on best response problems for the defender and the attacker. This program could be useful if it could be incorporated into RAW. It is very natural to represent stochastic game models via a user friendly graphical interface that could easily be understood by managers. It could be used by DHS analysts interested in best response analyses for various problem types studied within CREATE, such as biological threats, border security, and etc.

4. Research Products

Research Products (Please detail below)		**#**
5a	# of peer-reviewed journal reports published	
5a	# of peer-reviewed journal reports accepted for publication	
5a	# of non-peer reviewed publications and reports	1
5a	# of scholarly journal citations of published reports	
5b	# of scholarly presentations (conferences, workshops, seminars)	2
5b	# of outreach presentations (non-technical groups, general public)	

5c	# of products delivered to DHS, other Federal agencies, or State/Local	
5c	# of patents filed	
5c	# of patents issued	
5c	# of products in commercialization pipeline (products not yet to market)	
5c	# of products introduced to market	

4.1. Publications and Reports

Kardes, Erim - University of Southern California	Ref	Not Ref
1. Kardes, E., Hall, R.,"A Repeated Game for the MANPADS Problem," in preparation, 2008		x
2. Kardes, E, "The Use of Stochastic Games on a Homeland Security Problem," *CREATE Report*, 2008		x

4.2. Presentations

Kardes, E., "A Queuing Control Application using Discounted Robust Stochastic Games," INFORMS, Annual, Washington D.C, Meeting, Oct 15, 2008