6-18-2015

Generation of Strategies for Environmental Deception in Two-Player Normal-Form Games

Howard E. Poston

GENERATION OF STRATEGIES FOR ENVIRONMENTAL DECEPTION IN TWO-PLAYER NORMAL-FORM GAMES

THESIS

Howard E. Poston III, Civilian, USAF

AFIT-ENG-MS-15-J-004

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-15-J-004

GENERATION OF STRATEGIES FOR ENVIRONMENTAL DECEPTION IN TWO-PLAYER NORMAL-FORM GAMES

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Operations

Howard E. Poston III, BS

Civilian, USAF

June 2015

AFIT-ENG-MS-15-J-004

GENERATION OF STRATEGIES FOR ENVIRONMENTAL DECEPTION IN TWO-PLAYER NORMAL-FORM GAMES

Howard E. Poston III, BS

Civilian, USAF

Committee Membership:

Dr. Brett J. Borghetti
Chair

Dr. Gilbert L. Peterson
Member

Dr. Meir N. Pachter
Member

AFIT-ENG-MS-15-J-004

Abstract

Methods of performing and defending against deceptive actions are a popular field of study in game theory. However, the focus is mostly on *action* deception in turn-based games. This work focuses on developing strategies for performing *environmental* deception in two-player, strategic-form games. Environmental deception is defined as deception where one player has the ability to change the other's perception of the state of the game through modification of their perception of the game's payoff matrix, similar to the use of camouflage. The main contributions of this research are an expansion of the definition of the stability of a Nash equilibrium to include cells outside the equilibrium, and the creation of four algorithms for developing strategies for environmental deception, including closed-form solutions for the creation of a 3x3 deceptive game with a 2x2 mixed-strategy Nash equilibrium (MSNE) that benefits the deceiver from a 3x3 game containing a 2x2 MSNE. It is found that the value gain produced by a deceptive algorithm is dependent upon the type of game to which it is applied and the maximum amount of allowable change to the payoff matrix, emphasizing the importance of carefully selecting an algorithm to match the situation to which it is applied.

Acknowledgments

I would like to thank my advisor Dr. Brett Borghetti and my committee members Dr. Gilbert Peterson and Dr. Meir Pachter for their guidance during this thesis process. I would also like to thank my girlfriend and my family for their support throughout this Master's program.

Howard E. Poston III

Table of Contents

Page

List of Figures

Page

List of Tables

Page

GENERATION OF STRATEGIES FOR ENVIRONMENTAL DECEPTION IN TWO-PLAYER NORMAL-FORM GAMES

1. Introduction

Deception in game theory is an area that has been widely studied in the fields of economics, military decision making, and security. The ability of one player in a competitive game to deceive his opponent(s) provides him with the ability to achieve an outcome more favorable to him than if the potential for deception does not exist. This opportunity for increased advantage has motivated the study of deception in game theory in many different forms.

Game theory provides a means to generate models of situations and determine the best available action to take. In game theory, games are dichotomized in multiple different ways based upon the purpose, structure, and solution of the game. This provides a means to succinctly describe the key features of a situation based upon which class it falls into for each of the dichotomies.

One of the characteristics of games in game theory is if it is *cooperative* or *competitive*. In a *cooperative* game, the players are able to form coalitions where agreements are enforceable by some means and the result of the game is based upon the coalitions that are formed [1]. Such games are structured so that the incentives for cooperation are built into the payoff matrix of the game. In a *competitive* or *non-cooperative* game, the players are not able to form such coalitions or the coalitions are not enforceable [2]. The games studied in this research are competitive games where a gain on the part of one player represents a loss by their opponent.

Another dichotomy of games in game theory is the game structure. Two possible structures exist: *strategic-form* games and *extensive-form* games. In *strategic-form*, also known as *normal-form*, games, all players simultaneously select an action and the result of the game is the result of the combination of actions. A strategic-form game can be represented as an *n*-dimensional matrix where each dimension corresponds to the actions of one of the *n* players and a cell of the matrix contains the payoff matrix for all players if the combination of actions that intersects in that cell is played. An example of a strategic-form game is rock-paper-scissors, where players select one of three possible moves simultaneously and the result of the game is determined by the combination of moves played. *Extensive-form* games are turn-based games where the players alternate moves until an end state is reached. An extensive-form game can be represented by a tree where each node is a state of the game and each child node is the result of the current player taking one of the actions available to her. An example of an extensive-form game is chess, where players alternate moves until a checkmate or draw occurs. The games studied in this work are strategic-form games.

Finally, games are distinguished based upon the type of solution that they contain. In 1951, John Nash published the concept of the Nash equilibrium which states that every game contains an equilibrium strategy profile for each player where each player's strategy profile is a best response to the others' and no-one has incentive to deviate from their equilibrium strategy profile [2]. The term *strategy profile* is used here to describe a set of actions to take with a given probability of play for each action. A strategy that is a *best response* to another strategy provides the highest possible payoff given that the opponent is playing the other strategy [2].

Nash defined two types of equilibria: *pure-strategy* Nash equilibria and *mixed-strategy* Nash equilibria. In a *pure-strategy* Nash equilibrium (PSNE), all players have a single strategy that they will play 100% of the time. Deviation from this strategy will provide a lower payoff to a player if their opponents do not change their strategy as well. In a *mixed-strategy* Nash equilibrium (MSNE), all players have a set of strategies that they randomize over so that their opponents do not know which strategy that they will select. Each strategy has a set probability of selection intended to make the opponents indifferent between the strategies in their equilibrium strategy set, i.e. each strategy has the same expected value. Games containing both pure-strategy and mixed-strategy Nash equilibria are considered in this research; however, the equilibrium type can affect the strategy used so it is useful to note.

1.1 Problem Statement

The particular class of game studied in this research is a two-player strategic-form competitive game in which each cell of the payoff matrix a payoff value for each player than are constrained to the range [0,1] and sum to one. These values represent the remaining percent of full functionality of the deceiver's systems after the actions chosen by the deceiver and mark are executed and the percent by which the attacker has degraded the deceiver's functionality. The games studied will contain three actions for each player and are represented such that the row player or *evader* attempts to maximize remaining functionality while the column player or *pursuer* attempts to maximize the degradation of the deceiver's functionality.

For the purpose of this research, the evader or *deceiver* is given the ability to take deceptive action against the pursuer or *mark*. The evader has full knowledge of the complete state of the payoff matrix and the ability to change the values of the payoff matrix as perceived by the pursuer before play begins and each player selects his strategy. This ability is constrained by the resources available to the evader, represented by a maximum amount by which the payoff values can be changed. The goal of this research is to determine strategies where, given a game, the evader can maximize the amount of benefit received from using deception with the limited resources provided to him. This form of deception is referred to as *environmental deception* as the deceiver changes the mark's perception regarding the state of the world rather than his perception of the deceiver's choice of actions, as is studied in *action deception*. It is important to note that environmental deception changes only the attacker's *perception* of the world, not the actual state of the world. All benefit gained by the evader through deception is gained by causing the pursuer to play using a strategy different than the strategy he would play if presented the true payoff matrix. This change in the pursuer's strategy occurs because the pursuer's perception of the game being played differs, causing him to select a different strategy of play in order to achieve a high payoff for himself. The evader can design the deceptive game to increase the probability that the pursuer will select a strategy that increases the payoff to the evader in the true game.

An example of the type of situation modeled by the games and use of deception in this research is the use of flares and chaff by planes in dogfighting. The goal of the use of flares and chaff is to deceive the enemy missiles into believing the state of the world, i.e. the location of the target plane, is different than the truth. Chaff can deceive radar by

appearing as another metallic object near to the target aircraft, while flares have a heat signature that can cause infrared sensors to target them rather than the plane being targeted. The intelligent use of flares or chaff increases the remaining functionality of the evader's plane after the missile has exploded while the wrong choice provides little or no benefit. Further, an evader's deceptive strategies are constrained by the resources available to him as a plane can only carry a finite amount of flares and chaff which, once exhausted, provides no benefit to the evader. An optimal deceptive strategy makes the best use of the available resources to increase the evader's functionality after an attack.

The determination of strategies for environmental deception is simplified by the existence of *isomorphic transformations* of games. Isomorphic transformations refer to reordering of the rows and/or columns of the payoff matrix. A game that is an isomorphic transformation of another game is equivalent to the other game given relabeling of the rows and columns. This means that a deceptive strategy developed for one game can also be applied to all games that are isomorphic transformations of the game if the appropriate transformation is applied to the deceptive strategy. This greatly decreases the search space for effective strategies and makes possible the development of deceptive strategies that depend upon a certain ordering of the rows and columns of the payoff matrix.

1.2 Challenges

The greatest challenge for determining optimal deception strategies is the existence of discontinuities in the mapping from the *n*-space representation of the payoff matrix of a game to the equilibrium value and probabilities of play of the players' strategies.

These *knife edges*, where the value and strategy profiles of a game change dramatically with a small change in the payoff matrix of the game, can be located using stability analysis as described by Arsham [3] and expanded in this thesis. When changes to the values of cells in the payoff matrix cause the equilibrium strategies of the two players to change, the value of the game can change dramatically.

The existence of these knife edges complicates the development of deceptive strategies as games with extremely similar payoff matrices may react very differently to a deceptive strategy. Therefore, measures of similarity based upon distances between the payoff matrices of games are incorrect and other methods for determining similarity between games must be developed in order to make development of deceptive strategies for groups of games rather than individual games possible. The locations of knife edges within game space can be determined based upon calculation of the stability of cells within the payoff matrix. The calculation of cell stability is touched on in Chapter 3 and discussed at length in Appendix B.

1.3 Contributions

The main contributions of this research are an expansion of the definition of the stability of cells within a payoff matrix as described by Arsham in [3] to include cells outside of the equilibrium of a game, the definition of a set of criteria to evaluate strategies for environmental deception, the creation of an algorithm that performs effective environmental deception on any game with minimal information (for use as a baseline for evaluation of other environmental deception algorithms), and the development of closed-form solutions for calculating deceptive strategies that transform a 3x3 game containing a

2x2 MSNE into a deceptive game containing a 2x2 MSNE where equilibrium play by the mark in the deceptive game provides an increase in value of the game to the deceiver. It is found that the value gain produced by a deceptive algorithm is dependent upon the type of game to which it is applied and the maximum amount of allowable change to the payoff matrix, emphasizing the importance of carefully selecting an algorithm to match the situation to which it is applied.

The remainder of this thesis is organized as follows. Chapter 2 provides information regarding related work in game theory on topics such as deception, equilibrium stability, and equivalence classes of games. Chapter 3 provides an expanded definition of stability for cells in a payoff matrix, describes four methods for generating deceptive strategies and provides metrics for comparison between them based upon the necessary attributes of a strategy for effective environmental deception. Chapter 4 presents the results of applying these algorithms to a set of games and compares the effectiveness of each algorithm. Chapter 5 concludes and makes recommendations for future work. Appendix A describes the properties of the games being studied and Appendix B is devoted to a discussion of stability analysis.

2. Literature Review

A rich body of work exists in the field of game theory. Since game theory can be applied to any decision-making process which can be represented as a finite number of players and actions and their corresponding payoffs, it can be applied to a variety of problems. Fields that commonly use game theory to model decision-making problems include computer science, economics, and military/political decision making.

The field of game theory contains a large variety of sub-fields focused on the analysis of different types of games, analysis using different techniques, or the study of different attributes of games. For this research, three of the subfields are of interest: deception in game theory, stability analysis of games, and equivalence classes of games. The study of deception in game theory is of interest as it relates to the goal of this research: determining effective strategies for environmental deception. The fields of stability analysis of games and equivalence classes of games provide information useful to determining which strategies will be effective for different types of games. This section provides an exploration of the literature that exists on each of these three subjects.

2.1 Deception in Game Theory

The use of deception in game theory has been widely studied in the literature; however, the type of deception used varies widely from study to study. The most prominent form of deception in the literature is applied to extensive-form or turn-based games. In this deceptive paradigm, the deceiver attempts to make the deceived player believe that the deceiver took a different action in their turn than they truly did. As the game is turn-based, this affects the decisions of the deceived player, likely leading to an improved

payoff to the deceiver in the game. Since our research uses only normal form games, the turn-based form of deception does not apply.

In [4] and [5], Carroll and Grosu [4] and Garg and Grosu [5] examine deception in network security in the context of a signaling game. A computer is selected to be attacked and the defender sends a signal (truthful or not) that the computer is a honeypot. The attacker chooses to attack or not based upon the signal received. Pibil et al. [6] extend Carroll, Grosu, and Garg's research, developing game theoretic models for the optimal use of honeypots. Zhuang et al. [7] also examine an attacker/defender signaling game where the defender sends a signal to the attacker and the attacker updates his belief state based on the signal received. A fourth signaling game is studied by Hespanha et al. [8], where the attacker and defender allocate three defensive units over two locations and the defender can reveal the location of any number of units to influence the attacker's choice of target. Ma et al. [9] explore attacker/defender signaling games and the use of deception for protecting electric grids. Lee and Teo [10] also study deception in the context of a signaling game. Their study considers a scenario where one player observes the payoff in two boxes and labels them as he wishes. The other player selects a box and receives the payoff contained within, which the first player attempts to minimize. Lee and Teo assume that the first player distorts the information to penalize the second player and solve the game using linear equations.

Yavin [11] studies deception in the context of a pursuer-evader game where the evader has the ability to induce errors in the pursuer's sensors and control the type of errors induced. Levitin and Hausken [12] study the utility of protecting genuine and false targets against a two-phased attack. They find that the defense of some false targets

against the first wave helps to increase the security of the system against the second wave of the attack. Fuchs and Khargonekar [13] study a game in which one player has an information advantage derived from a sensor net whose information can be corrupted by the other player, decreasing their informational advantage. They develop closed-form solutions for a set of situations based upon the solution of dual linear programming problems and provide a demonstration of the truth of Jones' lemma.

An example of deception relevant to our research is described in the work of Lisý et al. [14]. In Lisý's work, the objective is to defeat environmental deception in a surveillance coverage environment. The goal of the attacker is to perform surveillance to observe a given geographical region of interest while paying additional attention to certain important sites. The defender in this scenario has a limited ability to change the perceived importance of certain sites, increasing the difficulty of the attacker's efforts to cover the region with the appropriate levels of surveillance. A method is developed which provides the ability to determine, based on the information corrupted by the defender, the sites of interest that require increased surveillance with accuracy better than an approach that ignores information regarding sites of interest entirely.

The relation between our research and that described in Lisý et al.'s work is that Lisý studies the same problem with a different purpose. The ability to modify the apparent importance of sites in the region undergoing surveillance granted to the defender is equivalent to a deceptive party's ability to modify the payoff values of the matrix as perceived by the deceived player. The difference is that our research determines the optimal strategy for the defender while Lisý attempts to optimize the strategy pursued by the attacker performing surveillance.

The theory of deception has been studied from multiple different perspectives in the literature. Gharesifard et al. [15, 16, 17] use hypergames to model the changing belief states of players playing games with incomplete information. This is relevant to the study of deception in game theory as the mark in a game where deception is occurring has incomplete information. However, since the games studied here are single-phase games, the mark does not have the ability to update their belief state over time, so this research does not apply.

Wagner and Arkin [18, 19] study whether deception should or should not be performed by robots and the type of deception to perform based on the mark. This relates to research on deception in game theory in general, but does not relate to our research as opponent modeling is not explored in our work. Instead, the mark is assumed to be fully deceived and play the Nash equilibrium of the deceptive game.

Greenberg [21, 20] explores the effects of deceiving the mark about the probability that a certain state of the world is the truth upon the mark's choice of strategy. This is relevant to our research as the goal of deception is to affect the mark's choice of strategy by changing their perception of the game being played. However, Greenberg does not provide a mechanism for creating deception, instead studying the effects of the uncertainty caused by deception upon the mark's choice of strategy. This differs from our research, where a mechanism for generating a deception that causes the mark to react in a desired way is developed.

Li and Cruz studied the effect of increased information upon the decision making of a player and the effects of a deceiver corrupting the additional information upon the decision making of the mark in [22]. The work done by Li and Cruz is relevant to our

research due to their study of the effects of corrupted information upon the decision making of the mark. However, in their paradigm, the mark has the same base source of information as the deceiver as well as an additional information source that the deceiver can corrupt. In our research, the mark possesses the same information sources as the deceiver (a means to gather the information necessary to determine the payoff matrix of the game being played), but the deceiver has the ability to corrupt all information received by the mark. In this way, the deceiver completely controls the mark's perception of the state of the world.

2.2 Stability Analysis in Game Theory

The second area of interest to our work is that of equilibrium stability analysis for games. The stability of a game, as used in this work, measures by how much the payoff values of a game's payoff matrix can be changed without the value and/or equilibrium strategy sets of the game being changed. Previous research and definitions of stability analysis in game theory can be expressed in two categories.

The definition of equilibrium stability most widely found in the literature is presented by Kohlberg and Mertens [23]. A stable equilibrium by their definition is an equilibrium in an extensive-form game that is self-enforcing, i.e. no player will ever deviate from it. They provide an example game where the second player deviates from the equilibrium because they are presented with a choice that provides them with additional information regarding the state of the game and deviation from the equilibrium in this state provides them with an increased payoff. While interesting, Kohlberg and Mertens' defi-

nition of equilibrium stability has no relation to our work because we use a different definition for stability.

Only one other line of research presents an alternative definition of stability. Arsham [3] provides a definition of stability analysis in game theory that has no relation to the definition of equilibrium stability used by Kohlberg and Mertens. Arsham's work focuses on determining the amount by which a mixed-strategy Nash equilibrium's payoff values can be perturbed while still maintaining the original MSNE strategy profile. Arsham's research represents a subset of our work and differs in two major ways. First, Arsham only allows modifying the payoff values of cells within the MSNE (our work doesn't make this restriction). Second, our work determines how much any value of the payoff matrix can be changed while producing an equilibrium that is strategy-equivalent to the original game. By determining the minimum amount of change necessary to change the strategy profile of a game, we define the lower bound on cost necessary to perform effective environmental deception as defined above.

2.3 Equivalence Classes of Games

The final area of interest in this research is that of equivalence classes of games. One obvious measure of equivalence could be determined based on the relationship between the payoff values in a game. By transforming a payoff matrix to a standard form and generating a vector of payoff values for the game, each game can be represented as a vector in 9-space. Unfortunately, due to the knife edges that exist in payoff between strategy profiles, the Euclidean or Manhattan distance proximity of two 3x3 games in 9-space does not necessarily imply that they have similar equilibrium strategy and value.

Since normal distance measures are not applicable, it is necessary to determine new measures of similarity between games that provide information that helps in determining effective deceptive strategies for a game. For this reason, literature in the area of equivalence classes is reviewed here.

Several forms of equivalence classes are introduced in the literature. Commonly used equivalence classes are zero-sum versus non-zero-sum games, cooperative versus common interest versus competitive games, and strategic versus extensive form games [24]. Other equivalence classes defined in the literature are Nash equivalence classes, rationalizable strategy-equivalence classes, iterated strict dominance equivalence classes, correlated equilibrium equivalence classes, best response equivalence classes, better response equivalence classes, and von Neumann-Morgenstern equivalence classes.

Germano defines equivalence relationships as relations on a space of games that map games from this space into sets [25]. Equivalence classes are the various sets that the games are mapped to, separated by those games for which the relation is discontinuous. The number of equivalence classes is further decreased through the use of transformation of games by relabeling the players and/or their actions to determine games isomorphic to the original game.

Nash equivalence is defined by Germano [24, 25]. This definition states that two games are Nash equivalent if there exists a transformation of the second game such that a continuous path through the space of games exists between the first game and the transformed second game. In this context, a continuous path refers to a series of isomorphic transformations to the game and/or changes to the payoff values of the game such that no modification crosses a knife edge in the mapping from payoff values to strategy profiles

where a small change in payoffs yields a large change in strategy. Germano finds that the set of 2x2 games can be divided into three classes of Nash equivalent games, while thirty-two Nash equivalence classes exist for 3x3 games.

Germano also introduces equivalence classes based upon the concepts of rationalizable strategies, iterated strict dominance, and correlated equilibria. Rationalizable strategies [26] are those that best respond to an opponent's strategy (whether or not the opponent's selection is in the Nash equilibrium). Iterated strict dominance involves the sequential elimination of strictly dominated strategies until no such strategies remain [27]. A strictly dominated strategy for a player is one for which another strategy provides a better payoff to the player for all of the possible strategies their opponent can play. Correlated equilibria are defined by Aumann [28] as the strategies that would be selected by each player to maximize their expected payoffs given a probability distribution of all of the states in the world. Equilibrium classes based upon rationalizable strategies and iterated strict dominance can be created by counting the number of rationalizable strategies or strategies surviving iterated strict dominance elimination for both players. Two games are defined to be equivalent based upon correlated equilibrium relations if a continuous path exists between one game and the transformed second game such that the dimension of the set of correlated equilibria remains constant [24].

Morris and Ui [29] introduce best response, better response, and von Neumann-Morgenstern equivalence classes. Two games are defined to be best response equivalent if for every pair of strategies the ratio of payoff differences of switching between the strategies is always the same, positive number w_i. For two games to be better response

equivalent, they must have the same dominance relations between strategies and for every pair of strategies that do not strictly dominate each other, the ratio of payoff differences for switching between the strategies is always the same, positive value, w_i. Von Neumann-Morgenstern equivalent games have the relationship that for any two strategies for a player, the ratio of payoff differences is always the same, positive value w_i where w_i is the same for all pairs of strategies.

The equivalence classes introduced in this thesis, *value equivalence* and *strategy-equivalence*, are a special case of the Nash equivalence class [24]. Germano found that after allowing transformations to identify isomorphically equivalent games that the three resulting equivalence classes of 3x3 games corresponded to the types of equilibria contained within the games: 1) a single pure-strategy Nash equilibrium, 2) a single mixed-strategy Nash equilibrium, and 3) a single mixed-strategy Nash equilibrium co-existing with two pure-strategy Nash equilibria.

The notion of strategic equivalence as defined in our work is identical to Germano's Nash equivalence; simplification of equivalence classes based upon isomorphic equivalence classes is also used in our research. Three key points differentiate our work and Germano's: 1) the retention of the value of the game as an important feature in equivalence classes, 2) the restriction to constant-sum games and the resulting effects upon the derived equivalence classes, and 3) the consideration of multiple pure-strategy Nash equilibria with the same value within a game.

The purpose of this chapter is to provide an introduction to the terminology and research relating to this work. The next chapter describes the proposed algorithms for generation of deceptive strategies.

3. Environmental Deception Strategy Generation

The goal of this thesis is the development of strategies for effective environmental deception. This chapter begins by describing the stability of cells within the payoff matrix of a game. This information is useful for environmental deception as it shows where deception can be applied most profitably to the deceiver. Next, some metrics for evaluating environmental deceptive strategies are defined for use in Chapter 4 to evaluate the deceptive strategy generation algorithms described in this thesis. The final third of this chapter describes the four deceptive strategy generation algorithms in detail, leading into the analysis of their effectiveness and comparative performance in Chapter 4.

3.1 Equilibrium Stability of Two-Player Constant-Sum Games

The *stability* of a cell in the payoff matrix of a game reflects its ability to change the value and/or equilibrium strategy set of a game. The stability of a cell is used here to refer to the minimum value by which a cell can be modified and cause the equilibrium of the game to change in value or strategy profile. This information is useful as it provides targeting information for modifications to the payoff matrix presented to the mark when environmental deception is being performed.

Two forms of stability are explored in this section. The *value stability* of a cell is the amount by which the value of the cell can be changed without the equilibrium value of the game being changed. The *strategy stability* of a cell is the amount by which the cell may be modified without changing the equilibrium strategy set of the row or column player.

The stability of a cell is dependent upon the type of Nash equilibrium contained within the game, pure-strategy or mixed-strategy, and the location of the cell in relation to the game's equilibrium. In this section, a brief summary of the stability of cells for each location and each equilibrium type is presented. A more complete explanation is presented in Appendix B.

The stability of a cell depends on its location relative to the equilibrium of the game. The four stability regions are the equilibrium itself, cells within the row of equilibrium cell(s), cells that share a column with equilibrium cell(s), and cells that share neither a row nor a column with equilibrium cells. This section provides stability equations for cells in each of the four regions for games containing pure-strategy Nash equilibria and mixed-strategy Nash equilibria.

3.1.1 Stability of Games Containing Pure-Strategy Nash Equilibria

The first case considered for stability analysis is for games containing a pure-strategy Nash equilibrium (PSNE). In games containing PSNEs, the equilibrium cell(s) must be the minimum in their row and the maximum in their column based on payoffs from the perspective of the row player (see Appendix A for more details). This is important to stability analysis as the stability of a cell in a game containing a PSNE game is equal to the amount by which that cell may be modified without violating these conditions for the equilibrium.

Another important property of pure-strategy Nash equilibria in constant-sum games is that only a single unique-valued equilibrium can exist in such a game. If multiple PSNEs cells exist in a game, they must have the same value and every cell at the intersection of a row containing a PSNE cell and a column containing a PSNE cell must

also be a PSNE cell with the same value (see Appendix A for a proof of this statement). If such a *multi-cell* PSNE exists within a game, it affects the stability calculation for the game as well.

Table **1** displays the stability bounds of cells based upon their location within the game and the type of PSNE contained within the game (single cell or multi-cell). Stability bounds refer to the maximum amount of modification m that can be applied to a cell while retaining the original equilibrium value or strategy profile. Equations 1 and 2 provide the definitions for r' and c' used within Table 1, where r is the value of a cell within the row of equilibrium cell(s) and c is the value of a cell sharing a column with equilibrium cell(s).

$$r' = \min(r) \tag{1}$$

$$c' = \max(c) \tag{2}$$

Table 1. Stability Bounds for Games Containing PSNEs

Modification Location	**Value Stability**	**Strategy Stability**
Equilibrium Location (single-cell PSNE)	$m \neq \min\begin{pmatrix}\min(r-v),\\ \min(v-c)\end{pmatrix}$	$m < \min\begin{pmatrix}\min(r-v),\\ \min(v-c)\end{pmatrix}$
Equilibrium Location (multi-cell PSNE)	m unbounded	$m = 0$
Row of Equilibrium (single row of PSNEs)	$m < r' - v$	$m < r' - v$
Row of Equilibrium (multiple rows of PSNEs)	m unbounded	$m < r' - v$
Column of Equilibrium (single column of PSNEs)	$m > c' - v$	$m > c' - v$
Column of Equilibrium (multiple rows of PSNEs)	m unbounded	$m > c' - v$

3.1.2 Stability of Cells Containing Mixed-Strategy Nash Equilibria

The second case considered here is the stability of cells within games that contain mixed-strategy Nash equilibria (MSNEs). In Appendix A, a proof is provided that only a single PSNE can exist in a two-player, constant-sum game, so this case is distinct from that of the previous section. Like the section on PSNEs, the stability bounds of cells are defined here based upon location within the payoff matrix with a more in-depth explanation provided in Appendix B.

Table **2** presents the stability bounds for cells in a game containing a MSNE based upon the relative location of the cells to the MSNE. In Table **2**, the values of r' and c' are defined in Equations 3 and 4, where *v* is the value of the game, *r* is the value of a cell in the row of the equilibrium, r'' is the value of the other cell in the row of the equilibrium (assuming a 2x2 MSNE), *c* is the value of a cell in the column of the equilibrium, c'' is the other cell in the column of the equilibrium, and *p* and *q* are the probabilities that the strategies resulting in r' or c' are played.

$$r' = \min\left(\frac{v - (1-p)\cdot r''}{p}\right) \tag{3}$$

$$c' = \min\left(\frac{v - (1-q)\cdot c''}{q}\right) \tag{4}$$

Table 2. Stability Bounds for Games Containing MSNEs.

Modification Location	**Value Stability**	**Strategy Stability**
Equilibrium Location	$m = 0$	$m = 0$
Row of Equilibrium	$m < r'$	$m < r'$
Column of Equilibrium	$m > -c'$	$m > -c'$

3.2 Success Criteria for Deceptive Strategies

The development of an effective strategy for environmental deception is a multi-objective optimization problem. A strong deceptive strategy must provide a large benefit to the deceiver, be attainable, and work effectively under many opponent models. All of these requirements translate directly to constraints that can be used to evaluate possible deceptive strategies during the generation process. This section describes *value gain*, *deceptive cost*, *benefit delay*, believability, *opponent risk*, and *efficiency* and their impact on the effectiveness of a strategy for environmental deception.

Value gain is the most significant of the criteria when selecting a strategy for environmental deception because an increase in the value of the game from the perspective of the deceptive player is the reason for performing environmental deception. A deceptive strategy that provides no benefit to the deceiver is a waste of resources and should not be pursued.

The value gain of a deceptive strategy is measured as the difference in the payoff value of the game to the deceptive player when the mark plays a strategy based upon the Nash equilibrium of the deceptive game and the payoff value when deception does not

occur. The goal of the deceiver is to select a strategy that maximizes this value given the other constraints on his possible deceptive strategy choices.

Deceptive cost is a constraint on the possible deceptive strategies the deceiver can employ that is based upon the resources available to the deceiver and their effects upon his ability to perform deception. The deceptive cost is measured as the Manhattan distance from the deceptive game from the original game or the sum of the absolute values of the changes of the payoff values of each cell of the payoff matrix. This cost function is shown in Equation 5, where d represents the deceptive game, o represents the original game, and l is the number of cells in both payoff matrices.

$$cost = \sum_{i=1}^{l} abs(d[i] - o[i]) \tag{5}$$

Another constraint related to the deceptive cost is the maximum allowable cost of deception. The maximum allowable cost of deception states the amount of resources available to the deceiver and limits the possible deceptive strategies that can be employed. If the cost of the cheapest effective deceptive strategy, i.e. the strategy with minimum deceptive cost and a positive value gain, exceeds the maximum cost of deception, environmental deception is impractical. Selection of a deceptive strategy is a multi-objective optimization problem which attempts to maximize value gain while minimizing deceptive cost.

Maximum allowable cost can be defined in different ways depending on the situation being modeled by the game. The maximum cost can relate to the payoff matrix as a whole, bounding the sum of the costs applied to each cell, or be defined on a cell-by-cell basis, bounding the maximum allowable change to each cell of the matrix. Maximum

cost values can also be set values or percentages based upon the values of the cells of the payoff matrix. Finally, the deceptive cost can be completely unconstrained with the deception focused solely on maximization of the value gain achieved.

The **benefit delay** of an algorithm for environmental deception measures whether the deceiver must apply units of deceptive cost with no benefit before reaching a condition where the deception causes an increase in value to the deceiver. The algorithms described in this work are labeled as having no benefit delay if the application of deceptive cost immediately produces increases in value gain to the deceiver or having a benefit delay if some deceptive cost must be applied with no value gain to the deceiver to achieve a condition where the value of the game increases for the deceiver due to deception.

Believability of deception is an important factor in the selection of a strategy for environmental deception. Environmental deception cannot modify the actual state of the world, only the mark's perception of it. If the result of the mark's and deceiver's choice of strategy results in a cell where the deceiver has performed deception, the mark will be aware of the deception when he receives a payoff different from the payoff which he anticipates. This may affect the strategy of the mark in future games as he now anticipates the possibility of deception and adjusts his play accordingly. Therefore, if it is desirable that deception is sustainable over multiple games or if it is necessary that the mark does not realize the deception even after payoffs are received, a deceptive strategy that is believable to the mark is desirable.

Believable environmental deception requires only that the payoff received by the mark be the payoff expected given knowledge of the actions taken by both players. As the mark's choice of actions is not under the control of the deceiver, any payoffs reacha-

ble given the deceiver's chosen strategy profile must remain unmodified. With the deceiver as the row player, this means that all cells in the rows of a strategy that the deceiver might play must remain unchanged in the deception since there is no guarantee that the opponent is rational or believes the deceptive game.

Each algorithm described in this chapter will be labeled as having high, medium, or low believability. A highly believable algorithm never produces a deceptive strategy in which the mark can receive a payoff value that has been changed in the deceptive game. An algorithm with medium believability does not produce deceptive strategies where a rational, deceived mark (i.e. one playing a strategy derived from the Nash equilibrium of the deceptive game) will receive a payoff that has been modified in the deceptive game. An algorithm with low believability produces deceptive strategies where a mark can receive payoffs that have been modified in the deceptive game even if he plays at the Nash equilibrium of the deceptive game.

Opponent risk refers to the potential for loss of value to the deceiver due to an irrational or suspicious opponent. When presenting a deceptive game to an opponent, the deceiver hopes that the opponent will play in a predictable way, preferably using the strategy profile defined by the Nash equilibrium of the deceptive game. An irrational opponent may deviate from this equilibrium strategy by accident and provide a greater or lesser payoff to the deceiver as a result. A suspicious player may suspect that deception is being performed and deliberately play with a strategy differing from that suggested by the deceptive game in hopes of achieving a better payoff than if he played into the deception. Regardless of cause, there exists the possibility that an opponent may not act in the way intended by the deceiver while crafting the deceptive game.

Opponent risk describes how much an irrational or suspicious opponent can reduce the value of the game for a deceiver using a given deceptive strategy. The algorithms presented in this thesis are labeled as having high or low opponent risk. Each algorithm for generating deceptive strategies classified as having high or low opponent risk. A high value of opponent risk indicates that a deceptive strategy is highly dependent upon the mark playing the equilibrium strategy of the deceptive game. If the mark deviates from the deceptive game's equilibrium, the value of the game to the deceptive player is decreased significantly. A deceptive strategy has low opponent risk if the deceptive player plays in a way that is rational for the true game, therefore receiving a payoff at or near the value of the true game if the mark does not play the equilibrium of the deceptive game.

An ideal deceptive strategy minimizes opponent risk; however, this is a tradeoff with the value gain of the deception. If the deceiver plays at the equilibrium of the true game, he has low opponent risk; however, he may not gain as much value from deception as if he played a strategy that accounts for the deception performed and the mark's expected response to it. Conversely, playing based upon the deceptive game may increase the value of the game to the deceiver but risks the deceiver receiving a lower payoff from the game if the mark is not deceived and plays a strategy based upon knowledge of the deception.

The **efficiency** of an algorithm for generating strategies for environmental deception measures the length of time it takes on average for the algorithm to generate a deceptive strategy for a game. This criterion is important as the development of a deceptive

strategy may be time-sensitive and an algorithm that cannot provide an effective deception strategy within the allotted time is no better than having no algorithm at all.

The games described in the following section will be labeled as having high, medium, or low efficiency in Chapter 4. A highly efficient algorithm has complexity on the order of $O(1)$ or constant time. An algorithm with medium efficiency has efficiency on the order of $O(m)$ where m is the size of the game's payoff matrix. An algorithm with low efficiency has complexity worse than $O(m)$.

3.3 Environmental Deception Strategy Generation for 3x3 Games

While the number of deceptive games that can be derived from a given game increases exponentially with the maximum allowable cost, many of these games provide little or no deceptive benefit to the deceptive player or are outperformed by other games with regard to value gain for cost spent. This section describes methods by which games that provide a benefit to the deceptive player can be determined from an initial game.

The algorithms presented in this section are based on the assumption that deception must have high or medium believability. As defined previously, high believability means that an opponent will never receive a payoff modified as part of the deception. Medium believability means that a rational opponent playing the Nash equilibrium of the deceptive game will not receive a payoff modified as a result of deception. This first algorithm presented here has medium believability, while the rest have high believability.

The first algorithm presented, the naïve algorithm, is a simple algorithm that uses the minimum possible amount of information necessary to perform effective deception in a game containing any type of equilibrium. The remainder of the section is devoted to

descriptions of methods by which games containing mixed-strategy Nash equilibria can be transformed to the benefit of the deceptive player. These methods are equilibrium-preserving deception and equilibrium-destroying deception applied to rows or columns.

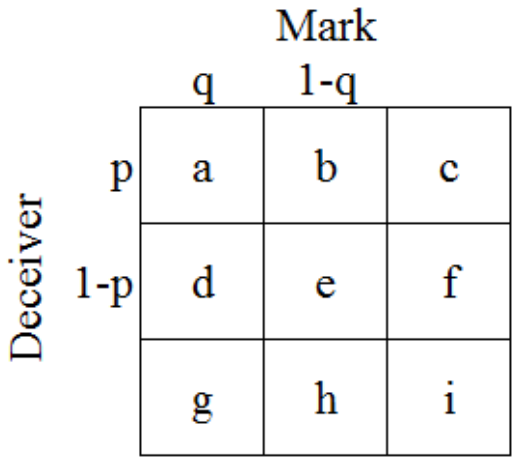

Figure 1. Labeling of 3x3 Game Payoffs and Probabilities.

The methods for deception described in this section are based upon the relationships between payoffs in 3x3 two-player, sum-to-one games. In a sum-to-one game, the payoffs for both players within a cell add to one, so a gain to one player represents an equal loss to the other. The methods use the labeling of cells and strategies in the payoff matrix shown in Figure 1, where payoffs are from the perspective of the deceptive row player. The values of p and q in Figure 1 represent the probabilities that the row and column players play the strategies in the top row and leftmost column respectively. The games are structured so that all equilibrium cells are in the top, left corner, and the highest value cell in the equilibrium is at location a and cells along the diagonal of the equilibrium starting at a are the greatest in their row and column of the equilibrium.

3.3.1 Naïve Algorithm

The first algorithm proposed for the generation of deceptive strategies is the naïve algorithm. Currently, there exists no baseline for the evaluation of deceptive strategy generation. A baseline environmental deception algorithm would accomplish the goal of performing effective deception, i.e. deception that produces a positive value gain for the deceiver, while using the minimum possible amount of knowledge of game theory, i.e. ability to compute the equilibrium value and strategy profile of a random game. The naïve algorithm attempts to fill this gap.

This algorithm makes uses of the knowledge of the payoff value of the starting game for the deceptive player and the properties of Nash equilibria in constant-sum games (see Appendix A). This section begins with the description and rationale for the use of this information, followed by a description of the resulting algorithm.

The value of the initial game to the deceptive player is defined as the expected functionality of the deceiver's systems after an attack if both players play rationally with strategies derived from the Nash equilibrium. It is necessary to provide this information to the naïve algorithm as it allows the algorithm to determine if the goal of improving the deceiver's payoff has been accomplished. The calculation of this value is shown in Equation 6, where R and C are the rows and columns of the payoff matrix, p_x is the probability that the row/column player plays row/column x, and $f_{r,c}$ is the deceiver's payoff found at row r and column c of the payoff matrix.

$$value = \sum_{r \in R} \sum_{c \in C} p_r \cdot p_c \cdot f_{r,c} \tag{6}$$

The other piece of information provided to the naïve algorithm is the properties of pure-strategy Nash equilibria (PSNEs) in two-player, constant-sum games. These properties, described in Appendix A, are derived from the fact that, in a PSNE, neither player has incentive to change from the equilibrium strategy.

The knowledge of the properties of pure strategy Nash equilibria in two-player, constant-sum games is necessary for the baseline algorithm because it allows the algorithm to complete its goal with no other knowledge of the state of the modified game. If one or more cells exist that fulfill the constraints described by the first two properties, then PSNEs exist in that game with the value of those cells. Otherwise, a mixed-strategy Nash equilibrium (MSNE) exists in the game and more information regarding the relationships between the cells of the payoff matrix is necessary to determine the value of the game. As the purpose of the naïve algorithm is to provide a baseline where decisions are based upon the minimum possible amount of information, it is desirable that the naïve algorithm only creates games containing PSNEs and does not need to calculate the value of games containing MSNEs (assuming that the value of the initial game is provided to it so it can determine if the deceptive game provides a higher value to the deceiver).

With this information in mind, it is now possible to define an algorithm to act as a baseline for comparison to other methods of developing deceptive strategies. The proposed algorithm accomplishes the goal by selecting all cells with values greater than or equal to the value of the initial game as potential equilibria and creates potential deceptive games with pure strategy Nash equilibria at these locations. This is accomplished by modifying the values of the cells in the row and column of each potential equilibrium so

that their relationships to the equilibrium cell fulfill the constraints defined by the first two properties of PSNEs as described in Appendix A.

These potential final games are then evaluated for their ability to fulfill the cost constraints of the scenario. The cost of the deception is calculated as the Manhattan distance between the payoff vectors, and all potential final games with a cost higher than the defined threshold are eliminated from the pool of potential options. If multiple potential final games still exist, then the final game with the highest ratio of value gain to deceptive cost is returned as the result of the algorithm.

Algorithm 1. Naïve Algorithm

```
function NaiveAlgorithm(payoff matrix, maxCost, stepSize)
returns modified payoff matrix maximizing value gain with cost as tie-
breaker
o,r ← payoff matrix
GL ← [] // List of cells with value greater than original game value
// Determines potential equilibrium cells for deceptive game
for i=1:length(o)
    if o[i] > getEqValue(o)
        GL ← [GL; i]
ε ← minimum step size of cost (stepSize)
for each cell g in GL do
    v ← payoff value at g
    s ← o  // Initialize potential modified game with PSNE at g
    // Create desired PSNE
    for each cell c in column of g
        s[c] ← min(s[c], v – ε)
    for each cell r in row of g
        s[r] ← max(s[r], v + ε)
    if getCost(s, o) > maxCost
        continue
    // Replace current game if new game is better
    if getEqValue(s) > getEqValue (r) || (getEqValue(s) == getEqValue(r) && getCost(s, o) <
getCost(r, o))
        r ← s
return r
```

```
function getCost(revised payoff matrix, original payoff matrix)
returns  cost to change from original matrix to revised matrix
r ← revised payoff matrix
o ← original payoff matrix
c ←0
for each cell i in r
    c ← c + abs(r[i] − o[i])
return c
```

This naïve algorithm is defined in pseudocode in Algorithm 1 and presents a baseline for evaluation of other algorithms for the generation of deceptive strategies. Some representative results of the performance of this algorithm are presented in Chapter 4.

3.3.2 Equilibrium-Preserving Deception

The equilibrium-preserving method of environmental deception is intended to increase the value of the game to the evader while retaining the equilibrium strategy set of the original game for both players. The benefit for the deceiver in environmental deception is derived from influencing the mark to change the probability that he plays the strategies available to him.

For the equilibrium-preserving method of deception, three possible scenarios are explored. In all scenarios, the mark plays at the Nash equilibrium of the deceptive game and it is assumed that the true game contains a MSNE in cells *a*, *b*, *d*, and *e*. In the first scenario, the deceiver plays his equilibrium strategies with the probabilities suggested by the true game. In the second scenario, the deceiver selects a strategy from the equilibrium to play before developing the deceptive game. In the third scenario, the deceiver plays the Nash equilibrium of the deceptive game.

Equations 7, 8 and 9 provide information about the value of the game derived from knowledge of the Nash equilibrium, using the labeling of cells presented in

Figure **1** 1. As stated previously, the true game is assumed to have a 2x2 MSNE containing cells *a*, *b*, *d*, and *e*. As the equilibria of the true and deceptive games contain the same cells, these equations apply to both if a cell is replaced by its modified value for the deceptive game. Equation 7 presents the canonical definition for the value of the game. Equations 8 and 9 are based upon knowledge of the Nash equilibrium and the fact that the row or column player must receive equal value from each of his strategies within the equilibrium (so he is indifferent between then) and less value from strategies outside the equilibrium (so he has no incentive to deviate from the equilibrium). From Equation 8, the probabilities of play p and q of the deceiver and mark can be calculated as shown in Equations 10 and 11.

$$v = a \cdot p \cdot q + b \cdot p \cdot (1 - q) + d \cdot (1 - p) \cdot q + e \cdot (1 - p) \cdot (1 - q) \tag{7}$$

$$v = a \cdot q + b \cdot (1 - q) = d \cdot q + e \cdot (1 - q) = a \cdot p + d \cdot (1 - p) = b \cdot p + e \cdot (1 - p) \tag{8}$$

$$g \cdot q + h \cdot (1 - q) < v < c \cdot p + f \cdot (1 - p) \tag{9}$$

$$p = \frac{-d + e}{a - b - d + e} \tag{10}$$

$$q = \frac{-b + e}{a - b - d + e} \tag{11}$$

Using the information in Equations 7-11, the three cases for equilibrium-preserving deception can be considered.

3.3.2.1 True Equilibrium

The first scenario considered for equilibrium-preserving deception is one where the deceiver creates a deceptive game but plays at the Nash equilibrium of the true game. The goal of this deception is to increase the value of the game for the deceiver while maintaining believability, i.e. no payoffs that the evader may receive as a result of gameplay may be modified as part of the deception. With the deceiver playing the true equilibrium of the original game, this means that all cells in a row that the deceiver may play, *a*-*f* in Figure 1, cannot be modified by the deception. As shown in Equation 7, the value of the true and deceptive games are based completely upon the values of cells *a*, *b*, *d*, and *e*. Therefore, equilibrium-preserving environmental deception cannot be both effective and believable if the deceiver plays the Nash equilibrium of the true game.

3.3.2.2 Chosen Action

In chosen action deception, the deceiver selects a strategy to play from the equilibrium of the true game and creates a deceptive game that increases the value of the game for the deceiver if he plays his selected strategy and the mark plays the equilibrium of the deceptive game. As described earlier, the games are structured so that the maximum value in the equilibrium of the game is located at *a*. Therefore, in chosen action deception, the deceiver plays the top row strategy and attempts to increase the probability that he receives the payoff at location *a*.

To increase the probability that he will receive payoff *a*, the deceiver must increase the probability of *q* for the mark in the deceptive game. Unlike the previous case,

the deceiver selects a strategy to play before developing the deceptive game, allowing modification of cells within the equilibrium at *d* and *e*.

Equation 12 shows the minimum amount, *s*, by which *d* can be increased in order to achieve the desired increase to *q* in the deceptive game.

$$\begin{gathered} q' > q \\ \frac{-b+e}{a-b-d-s+e} > \frac{-b+e}{a-b-d+e} \\ (-b+e)\cdot(a-b-d+e) > (-b+e)\cdot(a-b-d-s+e) \\ (-b+e)\cdot(a-b-d+e) > (-b+e)(a-b-d+e) - s\cdot(-b+e) \\ 0 > -s\cdot(-b+e) \\ s > 0 \end{gathered} \tag{12}$$

As shown in Equation 12, the only condition necessary to achieve the desired increase to *q*' is that *s* must be greater than zero, therefore any increase to the value of *d* increases the value of *q* in the deceptive game. Equation 13 provides a similar analysis of the minimum increase, *t*, to the value of *e* necessary to increase the value of *q* in the deceptive game over that of the true game.

$$\begin{gathered} q' > q \\ \frac{-b+e+t}{a-b-d+e+t} > \frac{-b+e}{a-b-d+e} \\ (-b+e+t)\cdot(a-b-d+e) > (-b+e)\cdot(a-b-d+e+t) \\ (-b+e)\cdot(a-b-d+e) + t\cdot(a-b-d+e) > (-b+e)\cdot(a-b-d+e) + t\cdot(-b+e) \\ t\cdot(a-d) + t\cdot(-b+e) > t\cdot(-b+e) \\ t\cdot(a-d) > 0 \\ t > 0 \end{gathered} \tag{13}$$

As shown in Equation 13, any increase to the value of *e* also increases the value of *q* in the deceptive game (since the amount by which it is increased, *t*, must only be greater than zero). However, while increases to *d* and *e* help to create the desired value

of q in the deceptive game, increasing them by too large an amount may destroy the desired equilibrium in the deceptive game. Equation 14 shows the calculation of a bound on the amount, s, by which d can be increased while preserving the desired equilibrium.

$$
\begin{gathered}
a \cdot p' + (d+s) \cdot (1-p') < c \cdot p' + f \cdot (1-p') \\
a \cdot p' + (d+s) - (d+s) \cdot p' < c \cdot p' + f - f \cdot p' \\
p' \cdot (a-c-d-s+f) < -d-s+f \\
\frac{-d-s+e}{a-b-d-s+e} \cdot (a-c-d-s+f) < -d-s+f \\
(-d-s+e) \cdot (a-c-d-s+f) < (-d-s+f) \cdot (a-b-d-s+e) \\
(-d-s+e) \cdot (-d-s+f) + (-d-s+e) \cdot (a-c) < (-d-s+f) \cdot (-d-s+e) + (-d-s+f) \cdot (a-b) \\
(-d-s+e) \cdot (a-c) < (-d-s+f) \cdot (a-b) \\
(-d+e) \cdot (a-c) - s \cdot (a-c) < (-d+f) \cdot (a-b) - s \cdot (a-b) \\
s \cdot (b-c) < (-d+f) \cdot (a-d) - (-d+e) \cdot (a-c)
\end{gathered}
\tag{14}
$$

Whether the calculations in Equation 14 provide an upper or lower bound on the acceptable value for the amount of change, s, to d is dependent upon the values of b and c. Regardless, Equation 14 provides useful information regarding possible changes for effective equilibrium-preserving deception in 2x2 MSNEs. Equation 15 provides a similar calculation for the maximum change, t, to the value of e that does not destroy the desired equilibrium in the deceptive game.

$$
\begin{gathered}
b \cdot p' + (e+t) \cdot (1-p') < c \cdot p' + f \cdot (1-p') \\
b \cdot p' + (e+t) - (e+t) \cdot p' < c \cdot p' + f - f \cdot p' \\
p' \cdot (b-c-e-t+f) < -e-t+f \\
\frac{-d+e+t}{a-b-d+e+t} \cdot (b-c-e-t+f) < -e-t+f \\
(-d+e+t) \cdot (b-c-e-t+f) < (-e-t+f) \cdot (a-b-d+e+t) \\
(-d+e+t) \cdot (-e-t+f) + (-d+e+t) \cdot (b-c) < (-e-t+f) \cdot (-d+e+t) + (-e-t+f) \cdot (a-b) \\
(-d+e+t) \cdot (b-c) < (-e-t+f) \cdot (a-b) \\
(-d+e) \cdot (b-c) + t \cdot (b-c) < (-e+f) \cdot (a-b) - t \cdot (a-b) \\
t \cdot (a-c) < (-e+f) \cdot (a-b) - (-d+e) \cdot (b-c)
\end{gathered}
\tag{15}
$$

Whether Equation 15 represents an upper or lower bound upon the possible changes, *t*, to *e* is dependent upon the values of *a* and *c*. The final consideration of interest is whether increasing *d* or *e* has a greater effect on the value of *q* in the deceptive game. Equation 16 determines the conditions necessary for changing *d* to be more beneficial to the deceiver than changing *e*.

$$\frac{-b+e}{a-b-d-s+e} > \frac{-b+e+t}{a-b-d+e+t}$$

$$(-b+e)\cdot(a-b-d+e+t) > (-b+e+t)\cdot(a-b-d-s+e)$$

$$\begin{aligned}(-b+e)\cdot(a-b-d+e)+(-b+e)\cdot t \\ > (-b+e)\cdot(a-b-d+e)-(-b+e+t)\cdot s+t\cdot(a-d)+t\cdot(-b+e)\end{aligned} \tag{16}$$

$$s\cdot(-b+e+t) > t\cdot(a-d)$$

$$s > \frac{t\cdot(a-d)}{(-b+e+t)}$$

$$\frac{a-d}{-b+e+t} < 1$$

$$a-d < -b+e+t$$

$$t > a+b-d-e$$

Equation 16 shows the conditions necessary for changing *d* to be more effective than changing *e* for the deceiver. As shown, if the value of *e* is increased by a value, *t*, that is more than $a+b-d-e$, then modifying *d* is more effective than modifying *e*. The decision of how to perform equilibrium-preserving deception should be based upon this information and the boundary conditions described in Equations 14 and 15.

3.3.2.3 Deceptive Equilibrium

Equilibrium-preserving deception where the deceiver plays the equilibrium of the deceptive game has the same issues as equilibrium-preserving deception where the deceiver plays the equilibrium of the true game. In order for deception to be effective, the value of the game must increase as a result of the deception. However, the value of the game is based solely on the value of cells within the game's equilibrium. If the deceiver is playing at the equilibrium of the deceptive game, which contains the same strategies as

the true game's equilibrium, then effective deception cannot be believable since it would require changing the values of payoffs which may be received by the mark.

3.3.3 Equilibrium-Destroying Deception (Rows)

The third method of deception considered is row-changing equilibrium-destroying deception. In this case, the deceptive game's equilibrium contains one of the row player's original equilibrium strategies and the other original equilibrium strategy for the row player is replaced by the strategy outside the equilibrium in the true game.

For all cases, Equations 17, 18, and 19 provide information about the value of the true game derived from knowledge of the Nash equilibrium. The equations also use the labeling of the cells and probabilities of play shown in Figure 1. From Equation 18, the probabilities of play p and q of the deceiver and mark can be calculated as shown in Equations 20 and 21.

$$v = a \cdot p \cdot q + b \cdot p \cdot (1 - q) + d \cdot (1 - p) \cdot q + e \cdot (1 - p) \cdot (1 - q) \tag{17}$$

$$v = a \cdot q + b \cdot (1 - q) = d \cdot q + e \cdot (1 - q) = a \cdot p + d \cdot (1 - p) = b \cdot p + e \cdot (1 - p) \tag{18}$$

$$g \cdot q + h \cdot (1 - q) < v < c \cdot p + f \cdot (1 - p) \tag{19}$$

$$p = \frac{-d + e}{a - b - d + e} \tag{20}$$

$$q = \frac{-b + e}{a - b - d + e} \tag{21}$$

As the deceptive game contains an equilibrium different from that of the true game, Equations 17-21 do not apply. Equations 22, 23, and 24 show calculations of the value of the deceptive game based upon knowledge of the Nash equilibrium, using the

labeling provided in Figure 1. Equations 25 and 26 are based on Equation 23 and provide the Nash equilibrium probabilities p' and q' that the row player and column player play the top row and leftmost column strategies of the deceptive game.

$$v' = a \cdot p' \cdot q' + b \cdot p' \cdot (1 - q') + g \cdot (1 - p') \cdot q' + h \cdot (1 - p') \cdot (1 - q') \tag{22}$$

$$v' = a' \cdot q' + b' \cdot (1 - q') = g' \cdot q' + h' \cdot (1 - q') = a' \cdot p' + g' \cdot (1 - p') = b' \cdot p' + h' \cdot (1 - p') \tag{23}$$

$$d' \cdot q' + e \cdot (1 - q') < v' < c \cdot p' + f \cdot (1 - p') \tag{24}$$

$$p' = \frac{-g' + h'}{a' - b' - g' + h'} \tag{25}$$

$$q' = \frac{-b' + h'}{a' - b' - g' + h'} \tag{26}$$

Using Equations 17-26, the three cases for row-changing, equilibrium-destroying deception can be considered.

3.3.3.1 True Equilibrium

The first case considered for equilibrium-destroying deception where the actions of the row player (deceiver) are changed is when the deceiver plays the equilibrium of the true game. Under these circumstances the deceiver may appear irrational to the mark since there exists the possibility that the deceiver will play an action outside the equilibrium of the deceptive game.

If the apparent rationality of the deceiver is unimportant, then believable deception using the row-changing, equilibrium-destroying method of deception is possible while playing the equilibrium of the true game. For deception to be effective, the value

of the game must increase as a result of deception, as shown in the first line of Equation 27. The values of the game used in the first line of Equation 27 are based upon the definition shown in Equation 17. The mixing of p and q' in the first half of the first line of Equation 27 is intentional as the row player plays at the equilibrium of the true game (with probabilities p and $1-p$) and the column player plays at the equilibrium of the deceptive game (with probabilities q' and $1-q'$).

$$\begin{aligned}
&a\cdot p\cdot q' + b\cdot p\cdot(1-q') + d\cdot(1-p)\cdot q' + e\cdot(1-p)\cdot(1-q') \\
&\qquad > a\cdot p\cdot q + b\cdot p\cdot(1-q) + d\cdot(1-p)\cdot q + e\cdot(1-p)\cdot(1-q) \\
&a\cdot p\cdot q' + b\cdot p - b\cdot p\cdot q' + d\cdot(1-p)\cdot q' + e - e\cdot p - e\cdot(1-p)\cdot q' \\
&\qquad > a\cdot p\cdot q + b\cdot p - b\cdot p\cdot q + d\cdot(1-p)\cdot q + e - e\cdot p - e\cdot(1-p)\cdot q \\
&a\cdot p\cdot q' - b\cdot p\cdot q' + d\cdot(1-p)\cdot q' - e\cdot(1-p)\cdot q' \\
&\qquad > a\cdot p\cdot q - b\cdot p\cdot q + d\cdot(1-p)\cdot q - e\cdot(1-p)\cdot q \\
&q'\cdot\big(a\cdot p - b\cdot p + d\cdot(1-p) - e\cdot(1-p)\big) > q\cdot\big(a\cdot p - b\cdot p + d\cdot(1-p) - e\cdot(1-p)\big) \\
&\qquad q' > q
\end{aligned} \tag{27}$$

As shown in Equation 27, in order for this deception to be effective (i.e. the deception provides an increase in the value of the game to the deceptive player), the value of q' in the deceptive game must exceed that of q in the true game. In order to maintain believability, only the values in the bottom row of the payoff matrix can be changed. These conditions are identical to that of the chosen action case for row-changing, equilibrium-destroying deception and will be described in detail in the following section. However, even if deception is believable, there exists the possibility that the deceiver will play

a strategy outside the equilibrium of the deceptive game, appearing irrational to the mark and possibly causing them to question the believability of the game.

3.3.3.2 Chosen Action

In the chosen action case of the row-changing equilibrium-destroying method of environmental deception, the deceiver selects an action from the equilibrium of the true game to play before creating the deceptive game. The goal of the deceptive game is to increase the probability that the mark plays a strategy resulting in a high value cell in the deceiver's chosen row. Due to the structure of the game as described previously, the deceiver should select the top row and attempt to increase the value of q for the mark, increasing the probability of the deceiver receiving the payoff at location a. The calculation of q for the original and revised game is shown in Equation 28.

$$q' > q$$
$$\frac{-b + h'}{a - b - g' + h'} > \frac{-b + e}{a - b - d + e} \tag{28}$$

As shown in Equation 28, the value of q in the revised game (shown as q') can be affected by the payoffs at locations a, b, g, and h. In order to achieve believable deception, the values at a and b cannot be changed, but g and h can be modified to increase the value of q in the deceptive game. Ideally modifications to g and h will increase the value of q in the deceptive game and help create the desired equilibrium. First, the increase, s, to g necessary to increase the value of q in the deceptive game are considered, as shown in Equation 29.

$$\frac{-b+h}{a-b-g-s+h} > \frac{-b+e}{a-b-d+e}$$

$$(-b+h)\cdot(a-b-d+e) > (-b+e)\cdot(a-b-g-s+h)$$

$$(-b+h)\cdot(a-b-d+e) > (-b+e)\cdot(a-b-g+h) - s\cdot(-b+e)$$

$$(-b+h)\cdot(a-b-d+e) - (-b+e)\cdot(a-b-g+h) > -s\cdot(-b+e)$$

$$s > -\frac{(-b+h)\cdot(a-b-d+e) - (-b+e)\cdot(a-b-g+h)}{-b+e} \tag{29}$$

$$s > -\frac{(-b+h)\cdot(a-d) + (-b+h)\cdot(-b+e) - (-b+e)\cdot(a-g) - (-b+e)\cdot(-b+h)}{-b+e}$$

$$s > -\frac{(-b+h)\cdot(a-d) - (-b+e)\cdot(a-g)}{-b+e}$$

$$s > \frac{(b-h)\cdot(a-d)}{b-e} + (a-g)$$

As shown in Equation 29, increases to the value of g increase the value of q in the deceptive game (since a lower bound for s is shown). The other requirement for effective row-changing, equilibrium-destroying environmental deception is that the bottom row of the payoff matrix replaces the middle row as part of the equilibrium in the deceptive game. In order to accomplish this, the value of the bottom row must exceed that of the middle row given the mark's probabilities of play for each strategy in the true game. The calculation of the change, s, to the value of g necessary to accomplish this is shown in Equation 30.

$$(g+s)\cdot q + h\cdot(1-q) > d\cdot q + e\cdot(1-q)$$

$$g\cdot q + s\cdot q > d\cdot q + e\cdot(1-q) - h\cdot(1-q)$$

$$s\cdot q > (d-g)\cdot q + (e-h)\cdot(1-q) \tag{30}$$

$$s > \frac{(e-h)\cdot(1-q)}{q} + (d-g)$$

Equation 30 shows that increases to the value of g help to create the desired equilibrium in the deceptive game in addition to increasing the value of q in the deceptive game (since once again a lower bound is provided for the value of s). A constraint on the

maximum amount, *s*, by which *g* can be changed is defined by the fact that changing the mark's equilibrium strategies is not desirable. This provides another bound on the maximum change to *g* as shown in Equation 31.

$$
\begin{gathered}
a \cdot p' + (g+s) \cdot (1-p') < c \cdot p' + i \cdot (1-p') \\
a \cdot p' + g + s - (g+s) \cdot p' < c \cdot p' + i - i \cdot p' \\
p' \cdot (a - c - g - s + i) < -g - s + i \\
\frac{-g-s+h}{a-b-g-s+h} \cdot (a - c - g - s + i) < -g - s + i \\
(-g-s+h) \cdot (a - c - g - s + i) < (-g - s + i) \cdot (a - b - g - s + h) \\
(-g-s+h) \cdot (-g-s+i) + (-g-s+h) \cdot (a-c) < (-g-s+i) \cdot (-g-s+h) + (-g-s+i) \cdot (a-b) \\
(-g+h) \cdot (a-c) - s \cdot (a-c) < (-g+i) \cdot (a-b) - s \cdot (a-b) \\
s \cdot (-b+c) < (-g+i) \cdot (a-b) - (-g+h) \cdot (a-c)
\end{gathered}
\tag{31}
$$

Whether Equation 31 provides an upper or another lower bound upon the change, *s*, to *g* depends on the values of *b* and *c*. Regardless, it provides more information about the range of values by which *g* can be modified in a way useful to the deceiver.

The value of *q* in the deceptive game can also be affected by changes in the value of the payoff at location *h*. The minimum change, *t*, to the value of *h* necessary to create a value of *q* in the deceptive that exceeds the value of *q* in the original game is shown in Equation 32.

$$
\begin{aligned}
q' &> q \\
\frac{-b+h+t}{a-b-g+h+t} &> \frac{-b+e}{a-b-d+e} \\
(-b+h+t)\cdot(a-b-d+e) &> (-b+e)\cdot(a-b-g+h+t) \\
(-b+h)\cdot(a-b-d+e)+t\cdot(a-d)+t\cdot(-b+e) &> (-b+e)\cdot(a-b-g+h)+t\cdot(-b+e) \\
(-b+h)\cdot(-b+e)+(-b+h)\cdot(a-d)+t\cdot(a-d) &> (-b+e)\cdot(-b+h)+(-b+e)\cdot(a-g) \\
(-b+h)\cdot(a-d)+t\cdot(a-d) &> (-b+e)\cdot(a-g) \\
t\cdot(a-d) &> (-b+e)\cdot(a-g)-(-b+h)\cdot(a-d) \\
t &> \frac{(-b+e)\cdot(a-g)}{a-d}-(-b+h)
\end{aligned}
\tag{32}
$$

Equation 32 demonstrates that increases to the value of *h* in the deceptive payoff matrix increases the value of *q* in the deceptive game (since a lower bound for the modification, *t*, to the value to *h* is calculated). Equation 33 shows the modification, *t*, to the value of *h* necessary for the desired equilibrium to exist in the deceptive game, the other necessary condition for effective row-changing equilibrium-destroying environmental deception to occur.

$$
\begin{aligned}
g\cdot q+(h+t)\cdot(1-q) &> d\cdot q+e\cdot(1-q) \\
h\cdot(1-q)+t\cdot(1-q) &> d\cdot q+e\cdot(1-q)-g\cdot q \\
t\cdot(1-q) &> (d-g)\cdot q+(e-h)\cdot(1-q) \\
t &> \frac{(d-g)\cdot q}{(1-q)}+(e-h)
\end{aligned}
\tag{33}
$$

As shown in Equation 33, increases to *h* do help to create the desired equilibrium as a minimum value for the increase, *t*, to the value of *h* is calculated. As for the possible modifications to the value of *g*, the possible changes to *h* are bounded by the fact that changes to *h* may destroy the desired equilibrium of the deceptive game by changing the mark's equilibrium strategy profile. Equation 34 calculates the bounds on the modification, *t*, to the value of *h* based upon this property.

$$
\begin{gathered}
b \cdot p' + (h+t) \cdot (1-p') < c \cdot p' + i \cdot (1-p') \\
b \cdot p' + h + t - (h+t) \cdot p' < c \cdot p' + i - i \cdot p' \\
p' \cdot (b - c - h - t + i) < -h - t + i \\
\frac{-g+h+t}{a-b-g+h+t} \cdot (b - c - h - t + i) < -h - t + i \\
(-g+h+t) \cdot (b - c - h - t + i) < (-h - t + i) \cdot (a - b - g + h + t) \\
(-g+h+t) \cdot (-h - t + i) + (-g+h+t) \cdot (b-c) < (-h - t + i) \cdot (-g+h+t) + (-h - t + i) \cdot (a-b) \\
(-g+h) \cdot (b-c) + t \cdot (b-c) < (-h+i) \cdot (a-b) - t \cdot (a-b) \\
t \cdot (a-c) < (-h+i) \cdot (a-b) - (-g+h) \cdot (b-c)
\end{gathered}
\tag{34}
$$

Whether Equation 34 provides an upper or another lower bound upon the change, *t*, to the value of *h* depends on the values of *a* and *c*. Regardless, it provides more information about the range of values by which *h* can be modified in a way useful to the deceiver.

Since both *g* and *h* can both simultaneously work to increase the value of *q* in the deceptive game and create the desired equilibrium in the deceptive game, it would be helpful to know how much of an effect an increase in the value of *g* or *h* has upon the value of the game for the deceiver. Equation 35 shows the calculation of the value gain due to an increase of *s* to the value of *g* if the desired equilibrium exists in the deceptive game.

$$
\begin{aligned}
\Delta v_g = v' - v &= a \cdot q' + b \cdot (1-q') - a \cdot q - b \cdot (1-q) = (q'-q) \cdot (a-b) \\
&= (a-b) \cdot \left(\frac{-b+h}{a-b-g-s+h} - \frac{-b+e}{a-b-d+e} \right) \\
&= (a-b) \cdot \frac{(-b+h) \cdot (a-b-d+e) - (-b+e) \cdot (a-b-g-s+h)}{(a-b-g-s+h) \cdot (a-b-d+e)} \\
&= (a-b) \cdot \frac{(-b+h) \cdot (-b+e) + (-b+h) \cdot (a-d) - (-b+e) \cdot (-b+h) - (-b+e) \cdot (a-g-s)}{(a-b-g-s+h) \cdot (a-b-d+e)} \\
&= (a-b) \cdot \frac{(-b+h) \cdot (a-d) - (-b+e) \cdot (a-g-s)}{(a-b-g-s+h) \cdot (a-b-d+e)}
\end{aligned}
\tag{35}
$$

Equation 36 calculates the amount by which the value of the game to the deceiver is increased when the payoff at location h is increased by an amount t, assuming that the desired equilibrium exists in the deceptive game.

$$\begin{aligned}
\Delta v_h &= v' - v = a \cdot q' + b \cdot (1 - q') - a \cdot q - b \cdot (1 - q) = (q' - q) \cdot (a - b) \\
&= (a - b) \cdot \left(\frac{-b+h+t}{a-b-g+h+t} - \frac{-b+e}{a-b-d+e} \right) \\
&= (a - b) \cdot \frac{(-b+h+t)\cdot(a-b-d+e) - (-b+e)\cdot(a-b-g+h+t)}{(a-b-g+h+t)\cdot(a-b-d+e)} \\
&= (a - b) \cdot \frac{(-b+h+t)\cdot(-b+e) + (-b+h+t)\cdot(a-d) - (-b+e)\cdot(-b+h+t) - (-b+e)\cdot(a-g)}{(a-b-g+h+t)\cdot(a-b-d+e)} \\
&= (a - b) \cdot \frac{(-b+h+t)\cdot(a-d) - (-b+e)\cdot(a-g)}{(a-b-g+h+t)\cdot(a-b-d+e)}
\end{aligned} \tag{36}$$

Using the results of Equations 35 and 36, it is now possible to determine whether an increase to the value of g or h has a greater effect upon the value of the game. Equation 37 shows under which circumstances an increase to g is more effective than an increase to h.

$$\Delta v_g > \Delta v_h$$

$$(a-b)\cdot\frac{(-b+h)\cdot(a-d)-(-b+e)\cdot(a-g-s)}{(a-b-g-s+h)\cdot(a-b-d+e)} > (a-b)\cdot\frac{(-b+h+t)\cdot(a-d)-(-b+e)\cdot(a-g)}{(a-b-g+h+t)\cdot(a-b-d+e)}$$

$$\frac{(-b+h)\cdot(a-d)-(-b+e)\cdot(a-g-s)}{(a-b-g-s+h)\cdot(a-b-d+e)} > \frac{(-b+h+t)\cdot(a-d)-(-b+e)\cdot(a-g)}{(a-b-g+h+t)\cdot(a-b-d+e)}$$

$$\big((-b+h)\cdot(a-d)-(-b+e)\cdot(a-g-s)\big)\cdot(a-b-g+h+t)$$

$$>$$

$$\big((-b+h+t)\cdot(a-d)-(-b+e)\cdot(a-g)\big)\cdot(a-b-g-s+h)$$

$$\big((-b+h)\cdot(a-d)-(-b+e)\cdot(a-g)+s\cdot(-b+e)\big)\cdot(a-b-g+h+t)$$

$$>$$

$$\big((-b+h)\cdot(a-d)+t\cdot(a-d)-(b+e)\cdot(a-g)\big)\cdot(a-b-g-s+h)$$

$$\begin{gathered}(-b+h)\cdot(a-d)\cdot(a-b-g+h)+(-b+h)\cdot(a-d)\cdot t-(-b+e)\cdot(a-g)\cdot(a-b-g+h)\\ -(-b+e)\cdot(a-g)\cdot t+s\cdot(-b+e)\cdot(a-b-g+h+t)\\ >\\ (-b+h)\cdot(a-d)\cdot(a-b-g+h)-(-b+h)\cdot(a-d)\cdot s+t\cdot(a-d)\cdot(a-b-g-s+h)-(-b+e)\\ \cdot(a-g)\cdot(a-b-g+h)\cdot(-b+e)\cdot(a-g)\cdot s\end{gathered} \tag{37}$$

$$(-b+h)\cdot(a-d)\cdot t-(-b+e)\cdot(a-g)\cdot t+s\cdot(-b+e)\cdot(a-b-g+h+t)$$

$$>$$

$$(-b+h)\cdot(a-d)\cdot s+(-b+e)\cdot(a-g)\cdot s+t\cdot(a-d)\cdot(a-b-g-s+h)$$

$$(-b+h)\cdot(a-d)\cdot t-(-b+e)\cdot(a-g)\cdot t+s\cdot(-b+e)\cdot(a-g)+s\cdot(-b+e)\cdot(-b+h+t)$$

$$>$$

$$(-b+h)\cdot(a-d)\cdot s+(-b+e)\cdot(a-g)\cdot s+t\cdot(a-d)\cdot(-b+h)+t\cdot(a-d)\cdot(a-g-s)$$

$$(-b+e)\cdot\big((a-g)\cdot t+(-b+h+t)\cdot s\big)>(a-d)\cdot\big((-b+h)\cdot s+t\cdot(a-g-s)\big)$$

$$(-b+e)\cdot\big((a-g)\cdot t+(-b+h)\cdot s+s\cdot t\big)>(a-d)\cdot\big((a-g)\cdot t+(-b+h)\cdot s+s\cdot t\big)$$

$$(-b+e)>(a-d)$$

As shown in Equation 37, the relative values of the cells *b*, *e*, *a*, and *d* determine whether modifying *g* or *h* is more effective to increasing the value of the game to the deceiver. If $(-b+e) > (a-d)$, then increases to the value of *g* are more beneficial to the deceiver, otherwise increases to the value of *h* are more effective. The other goal of modifying the values of *g* and *h* is to increase the value of the strategy containing them for the row player so that it replaces the middle row as part of the equilibrium for the deceptive game. For this purpose, the modification that increases the row's value more quickly is preferable. Equation 38 shows the ratio of the effectiveness of modifications to *g* (shown as *s*) and *h* (shown as *t*) towards accomplishing this task.

$$\begin{gathered}(g+s)\cdot q + h\cdot(1-q) = g\cdot q + (h+t)\cdot(1-q) \\ g\cdot q + s\cdot q + h\cdot(1-q) = g\cdot q + h\cdot(1-q) + t\cdot(1-q) \\ s\cdot q = t\cdot(1-q) \\ \frac{s}{t} = \frac{1-q}{q}\end{gathered} \tag{38}$$

As shown in Equation 38, if *q* is greater than 1-*q*, then modifications to *h* are more effective and vice versa. The circumstances under which *q* is greater than 1-*q* are shown in Equation 39.

$$\begin{gathered}q > 1-q \\ \frac{-b+e}{a-b-d+e} > 1 - \frac{-b+e}{a-b-d+e} \\ \frac{-b+e}{a-b-d+e} > \frac{a-d}{a-b-d+e} \\ -b+e > a-d\end{gathered} \tag{39}$$

As shown in Equation 39, increasing *h* is more effective in creating the desired equilibrium under the same circumstances that increasing *g* is more effective in increasing the value of the game to the deceiver. If sufficient cost is available to create the de-

sired equilibrium using the method that provides the better value gain, then the deceiver should do so if the other bounds on the amount of modification to the cell allow. Otherwise, a strategy which involves modifying both g and h to maximize value gain while achieving the desired equilibrium may be necessary.

3.3.3.3 Deceptive Equilibrium

The third case considered for the row-changing equilibrium-destroying method of deception is when the deceiver plays the Nash equilibrium of the deceptive game. In order for deception to be effective, the value of the game to the deceiver must increase due to deception. In order for deception to be believable, the cells within the equilibrium of the deceptive game must remain unchanged, i.e. the cells at locations a, b, g, and h. A necessary condition for the value to increase is shown in Equation 40.

$$\begin{aligned} v' &> v \\ a \cdot q' + b \cdot (1 - q') &> a \cdot q + b \cdot (1 - q) \\ a \cdot q' + b - b \cdot q &> a \cdot q + b - b \cdot q \\ q' \cdot (a - b) &> q \cdot (a - b) \\ q' &> q \end{aligned} \tag{40}$$

The final step of Equation 40 is true since the value at location a is greater than that at location b due to the structure of the payoff matrix described earlier. As shown, for the value of the game to increase, the value of q must increase in the deceptive game. Another necessary condition for the value of the game to increase is shown in Equation 41.

$$
\begin{gathered}
v' > v \\
g \cdot q' + h \cdot (1 - q') > d \cdot q + e \cdot (1 - q) > g \cdot q + h \cdot (1 - q) \\
g \cdot q' + h \cdot (1 - q') > g \cdot q + h \cdot (1 - q) \\
g \cdot q' + h - h \cdot q' > g \cdot q + h - h \cdot q \\
q' \cdot (g - h) > q \cdot (g - h) \\
q' < q
\end{gathered}
\tag{41}
$$

In Equation 41, the final step is true because g must be less than h given the structure of the game described previously and the existence of a MSNE in the deceptive game. As shown in Equations 40 and 41, in order to increase the value of the deceptive game, the value of q must be both strictly greater than and strictly less than the value of the original game. Since these conditions are mutually incompatible, playing the equilibrium of the deceptive game while performing believable row-changing equilibrium-destroying deception provides no benefit to the deceiver.

3.3.4 Equilibrium-Destroying Deception (Columns)

For the scenarios where the game contains a 2x2 MSNE, Equations 42, 43, and 44 provide information about the value of the game derived from knowledge of the Nash equilibrium, using the labeling of cells and probabilities shown in Figure 1. From Equation 43, the probabilities of play p and q of the deceiver and mark can be calculated as shown in Equations 45 and 46.

$$v = a \cdot p \cdot q + b \cdot p \cdot (1 - q) + d \cdot (1 - p) \cdot q + e \cdot (1 - p) \cdot (1 - q) \tag{42}$$

$$v = a \cdot q + b \cdot (1 - q) = d \cdot q + e \cdot (1 - q) = a \cdot p + d \cdot (1 - p) = b \cdot p + e \cdot (1 - p) \tag{43}$$

$$g \cdot q + h \cdot (1 - q) < v < c \cdot p + f \cdot (1 - p) \tag{44}$$

$$p = \frac{-d + e}{a - b - d + e} \tag{45}$$

$$q = \frac{-b + e}{a - b - d + e} \tag{46}$$

As the deceptive game contains an equilibrium different from that of the true game, Equations 42-46 do not apply. Equations 47, 48, and 49 show calculations of the value of the deceptive game based upon knowledge of the Nash equilibrium. Equations 50 and 51 are based on Equation 48 and provide the Nash equilibrium probabilities that the row and column players play the top row strategy and the leftmost column strategy in the deceptive game.

$$v' = a \cdot p' \cdot q' + c \cdot p' \cdot (1 - q') + d \cdot (1 - p') \cdot q' + f \cdot (1 - p') \cdot (1 - q') \tag{47}$$

$$v' = a' \cdot q' + c' \cdot (1 - q') = d' \cdot q' + f' \cdot (1 - q') = a' \cdot p' + d' \cdot (1 - p') = c' \cdot p' + f' \cdot (1 - p') \tag{48}$$

$$g' \cdot q' + i' \cdot (1 - q') < v' < b' \cdot p' + e' \cdot (1 - p') \tag{49}$$

$$p' = \frac{-d' + f'}{a' - c' - d' + f'} \tag{50}$$

$$q' = \frac{-c' + f'}{a' - c' - d' + f'} \tag{51}$$

Using the information provided in Equations 42-51, the effectiveness of column-changing, equilibrium-destroying deception for 2x2 MSNEs can be considered.

3.3.4.1 True Equilibrium

The first case considered for the column-changing, equilibrium-destroying method of environmental deception is when the deceiver plays the Nash equilibrium of the

true game. In order for deception to be beneficial to the deceiver, the value of the game to him must increase as a result of deception. As shown in Equation 47, the value of the deceptive game is dependent solely on the values at locations *a*, *c*, *d*, and *f*. As these values are all within the strategies playable by the deceiver at the equilibrium of the true game, it is impossible for the deceiver to perform effective, believable deception using the column-changing, equilibrium-destroying method if he plays the equilibrium of the true game.

3.3.4.2 Chosen Action

The second option for the deceiver performing column-changing, equilibrium-destroying deception is to select a strategy to play before developing a deceptive game to present to the mark. Under these circumstances, as in previous cases, the deceiver is assumed to select the top row strategy and attempts to increase the probability that he receives the payoff at location *a* by increasing the value of *q* in the deceptive game. In order to maintain believability, the deceiver is limited to modifying values outside of his chosen action, i.e. the values of *d*, *e*, and *f*. As the values of *d* and *f* affect the value of *q* in the deceptive game, the effects of changing them are considered. Equation 52 shows the effect of changing the value of *d* by an amount *s* upon the value of *q* in the deceptive game.

$$
\begin{gathered}
q' > q \\
\frac{-c+f}{a-c-d-s+f} > \frac{-b+e}{a-b-d+e} \\
(-c+f)\cdot(a-b-d+e) > (-b+e)\cdot(a-c-d-s+f) \\
(-c+f)\cdot(-b+e)+(-c+f)\cdot(a-d) > (-b+e)\cdot(-c+f)+(-b+e)\cdot(a-d-s) \\
(-c+f)\cdot(a-d) > (-b+e)\cdot(a-d)-s\cdot(-b+e) \\
(-c+f)\cdot(a-d)-(-b+e)\cdot(a-d) > -s\cdot(-b+e) \\
s > (a-d)-\frac{(-c+f)\cdot(a-d)}{-b+e}
\end{gathered}
\tag{52}
$$

As shown in Equation 52, increasing the value of *d* increases the value of *q* in the deceptive game (since a lower bound on *s* is calculated). In addition to having an increased value of *q*, the deceptive game must contain the desired equilibrium, where the mark plays a different strategy profile than the true game. The existence of the equilibrium in the deceptive game depends on the rightmost column replacing the center column as part of the equilibrium. The change, *s*, to *d* necessary to accomplish this is shown in Equation 53.

$$
\begin{gathered}
b\cdot p'+e\cdot(1-p') > c\cdot p'+f\cdot(1-p') \\
b\cdot p'+e-e\cdot p' > c\cdot p'+f-f\cdot p' \\
p'\cdot(b-c-e+f) > -e+f \\
\frac{-d-s+f}{a-c-d-s+f}\cdot(b-c-e+f) > -e+f \\
(-d-s+f)\cdot(b-c-e+f) > (-e+f)\cdot(a-c-d-s+f) \\
(-d-s+f)\cdot(b-c)+(-d-s+f)\cdot(-e+f) > (-e+f)\cdot(a-c)+(-e+f)\cdot(-d-s+f) \\
(-d+f)\cdot(b-c)-s\cdot(b-c) > (-e+f)\cdot(a-c) \\
-s\cdot(b-c) > (-e+f)\cdot(a-c)-(-d+f)\cdot(b-c) \\
s\cdot(b-c) < -(-e+f)\cdot(a-c)+(-d+f)\cdot(b-c)
\end{gathered}
\tag{53}
$$

As shown in Equation 53, increasing the value of *d* does help to create the desired equilibrium while achieving a higher value of the game to the deceiver under certain cir-

cumstances. However, other constraints do apply. The value of d cannot exceed the value of e or the row of the equilibrium will change instead of the column, therefore $d + s < e$. Another constraint on the increase, s, to the value of d is that the leftmost column strategy must have a lower value than the other two row strategies in the new equilibrium. The computation of this constraint is shown in Equation 54.

$$a \cdot p' + (d+s) \cdot (1-p') < b \cdot p' + e \cdot (1-p')$$

$$a \cdot p' + (d+s) - (d+s) \cdot p' < b \cdot p + e - e \cdot p'$$

$$p' \cdot (a-b-d-s+e) < -d-s+e$$

$$\frac{-d-s+f}{a-c-d-s+f} \cdot (a-b-d-s+e) < -d-s+e$$

$$(-d-s+f) \cdot (a-b-d-s+e) < (-d-s+e) \cdot (a-c-d-s+f)$$

$$\begin{aligned}(-d-s+f) \cdot (a-b) + (-d-s+f) \cdot (-d-s+e) \\ < (-d-s+e) \cdot (a-c) + (-d-s+e) \cdot (-d-s+f)\end{aligned} \tag{54}$$

$$(-d-s) \cdot (a-b) + f \cdot (a-b) < (-d-s+e) \cdot (a-c)$$

$$-(d+s) \cdot (a-b) < (-d-s+e) \cdot (a-c) - f \cdot (a-b)$$

$$(d+s) \cdot (a-b) > -(-d-s+e) \cdot (a-c) + f \cdot (a-b)$$

$$(d+s) > -\frac{(-d-s+e) \cdot (a-c)}{a-b} + f$$

$$e > -\frac{(-d-s+e) \cdot (a-c)}{a-b} + f$$

$$(e-f) \cdot (a-b) > -(-d-s+e) \cdot (a-c)$$

$$(e-f) \cdot (a-b) > -(-d+e) \cdot (a-c) + s \cdot (a-c)$$

$$(e-f) \cdot (a-b) + (-d+e) \cdot (a-c) > s \cdot (a-c)$$

As shown in Equation 54, additional constrains upon the increase, s, to the value of d exist; however, under some circumstances increases to the value of d also help to create the desired equilibrium. The other value that can be changed to affect the value of q in the deceptive game is the value at location f of the payoff matrix. The effect of

changing the value of f by an amount t upon the value of q in the deceptive game is shown in Equation 55.

$$\begin{gathered} q' > q \\ \frac{-c+f+t}{a-c-d+f+t} > \frac{-b+e}{a-b-d+e} \\ (-c+f+t)\cdot(a-b-d+e) > (-b+e)\cdot(a-c-d+f+t) \\ (-c+f+t)\cdot(a-d)+(-c+f+t)\cdot(-b+e) > (-b+e)\cdot(a-d)+(-b+e)\cdot(-c+f+t) \\ (-c+f+t)\cdot(a-d) > (-b+e)\cdot(a-d) \\ -c+f+t > -b+e \\ t > -b+c+e-f \end{gathered} \tag{55}$$

As shown in Equation 55, increasing the value of f also increases the value of q in the deceptive game (as a lower bound on the value of t is calculated). The other necessary condition for the deceptive game is for the desired equilibrium in the deceptive game to exist. The value of f has an effect upon the location of the equilibrium, as described in Equation 56, where t is the amount by which the value of f is increased.

$$\begin{gathered} b\cdot p+e\cdot(1-p) > c\cdot p+(f+t)\cdot(1-p) \\ b\cdot p+e\cdot(1-p)-c\cdot p > f\cdot(1-p)+t\cdot(1-p) \\ (b-c)\cdot p+(e-f)\cdot(1-p) > t\cdot(1-p) \\ t < \frac{(b-c)\cdot p}{1-p}+(e-f) \end{gathered} \tag{56}$$

As shown in Equation 56, increasing the value of f has an adverse effect upon the creation of the desired equilibrium in the deceptive game. Therefore, increasing d is better as it works toward both of the deceiver's goals under some circumstances.

3.3.4.3 Deceptive Equilibrium

The third case considered for column-changing, equilibrium-destroying deception is if the deceiver chooses to play the Nash equilibrium of the deceptive game. In order for the deception to be both believable and worthwhile to the deceiver, the value of the

game must increase due to deception without changing the values of any of the cells contained within the strategies that the deceiver may play. Equation 48 shows that the value of the deceptive game is based upon the cells within the equilibrium of the deceptive game. If the deceiver plays the equilibrium of the deceptive game, it is impossible to increase the value of the game while performing believable deception using the method of column-changing, equilibrium-destroying environmental deception.

4. Results

In Chapter 3, four methods of performing deception were described. The first, the naïve algorithm, applies to any size game with any size or type of equilibrium and works by creating a pure-strategy Nash equilibrium in the deceptive game at a location with value greater than the true game's value. The remaining three algorithms work on 3x3 games containing a 2x2 mixed-strategy Nash equilibrium (MSNE). The goal of these algorithms is to perform deception within the equilibrium of the deceptive game while retaining the original equilibrium strategy set, changing the row player's equilibrium strategy set, or changing the column player's equilibrium strategy set.

Chapter 3 demonstrated that believable, effective deception is only possible for the equilibrium-preserving and equilibrium-destroying algorithms if the deceiver selects an action to play before creating the deceptive game. This allows for deception in the equilibrium and focuses deceptive efforts toward a specific goal: increasing the probability that a high-value cell (from the perspective of the deceiver) is the result of gameplay.

The goal of this chapter is to empirically demonstrate the correctness of the closed-form solutions for equilibrium deception described in the previous chapter and compare the four methods of deception based upon the criteria for deception described in Chapter 3. In the first half of this chapter, deception will be applied to three 3x3 games containing a 2x2 MSNE. Multiple games were generated to test the algorithms described in Chapter 3, and the three selected games were chosen as they are representative of the set of possible games and demonstrate differing relative values of cells while retaining the desired features of a 2x2 MSNE within a 3x3 game.

For each game, each form of equilibrium deception will be considered separately to demonstrate that the closed-form solutions for deception described in Chapter 3 accurately reflect the behavior of the game when deception is applied. Then, the performance of all four algorithms for the game will be compared. The remainder of the chapter compares the four algorithms based upon the criteria for deception described in Chapter 3.

4.1 Performance of Algorithms for 3x3 Games with 2x2 MSNE

The first game considered is the one shown in Figure 2. This game has a 2x2 MSNE containing the top and middle rows for the row player and the left and center columns for the column player. The probabilities of play at equilibrium for each strategy (rounded to the nearest percent) are shown above and to the left of the payoff matrix.

	0.15	0.85	0
0.62	0.75	0.5	0.8
0.38	0.2	0.6	0.65
0	0.1	0.2	0.5

Figure 2. Test Game 1.

The results of applying equilibrium-preserving deception to the game shown in Figure 2 are shown in Figure 3. The figure shows the anticipated value of the game using a chosen-action deception and the true value of the game using a chosen-action deception. The plateauing of the value indicates that the equilibrium would be broken by fur-

ther increases to the selected value and/or the selected value has reached its maximum value of one.

In the figure, the anticipated value of the game when the value of *d* is increased (shown as blue dots) assumes that *d* is increased by the given deceptive cost and is calculated by Equation 57, where q' is the probability that the mark plays the leftmost column based upon the Nash equilibrium of the deceptive game as calculated using the equations presented in Chapter 3.

$$v = a \cdot q' + b \cdot (1 - q') \qquad v = .75 \cdot q' + .5 \cdot (1 - q') \tag{57}$$

The true value of the game when *d* is increased (shown as green circles) is calculated using Equation 57 as well, but computing the true value of q for the deceptive game rather than the anticipated value based upon the equations presented in Chapter 3. The anticipated and true values of the game when *e* is increased (red x's and black +'s respectively) are computed identically to those for the games with increases to *d*. If the equations presented in Chapter 3 are correct, the values of the game computed by both methods will be identical.

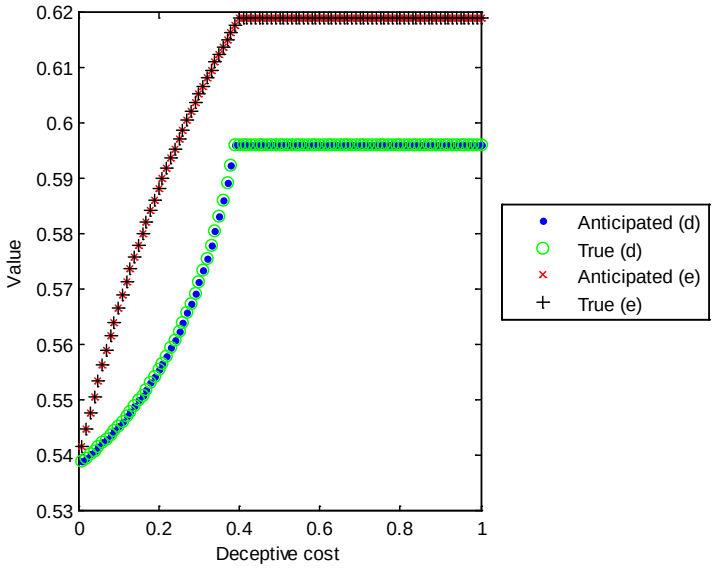

Figure 3. Equilibrium-Preserving Deception Results for Test Game 1.

As shown in Figure 3, equilibrium-preserving deception provides immediate increases in value to the deceiver. The anticipated and true values of the game using the chosen-action deception are identical, indicating that the closed-form solutions for deception presented in Chapter 3 are correct for this case. For the game shown in Figure 2, increases to the value of *e* provide better results to the deceiver than increases to the value of *d*. In practice, modifications to both *d* and *e* simultaneously should be used to maximize the value gain to the deceiver, but separating the possible changes in this context demonstrates the correctness of the equations in Chapter 3 for this case and the relative effectiveness of increasing *d* or *e*.

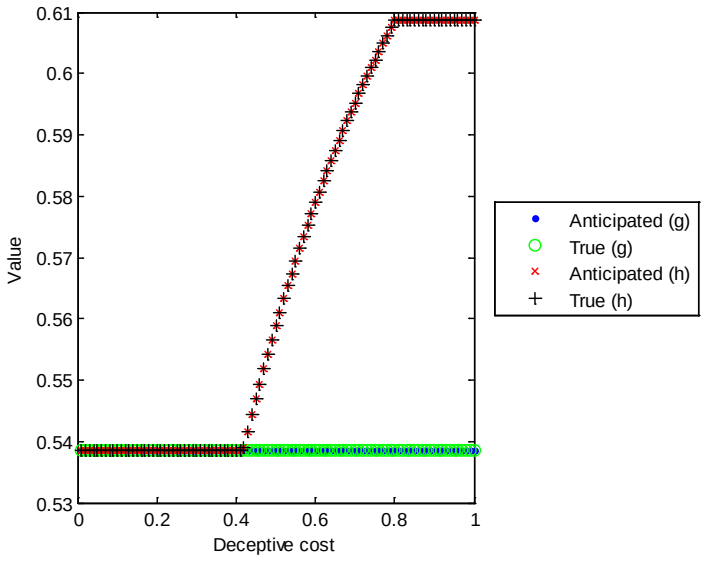

Figure 4. Row-Changing Deception Results for Test Game 1.

Figure 4 shows the results of applying row-changing, equilibrium-destroying deception to the game shown in Figure 2. The anticipated values of the game given increases to the values of g and h (blue dots and red x's respectively) are also computed using Equation 57 and the value of q' calculated from the equations in Chapter 3. The true values of the game given increases to g and h (green circles and black +'s) are also computed using Equation 57 using the true value of q' for the deceptive game and should be identical to the anticipated value of the game.

As expected, the row-changing deception does not provide immediate benefit to the deceiver since some cost must be applied in order to change the equilibrium of the deceptive game before the applied cost affects the value of the game. As shown, for the game in Figure 2, increases to the value of h provide more benefit to the deceiver than increases to the value of g.

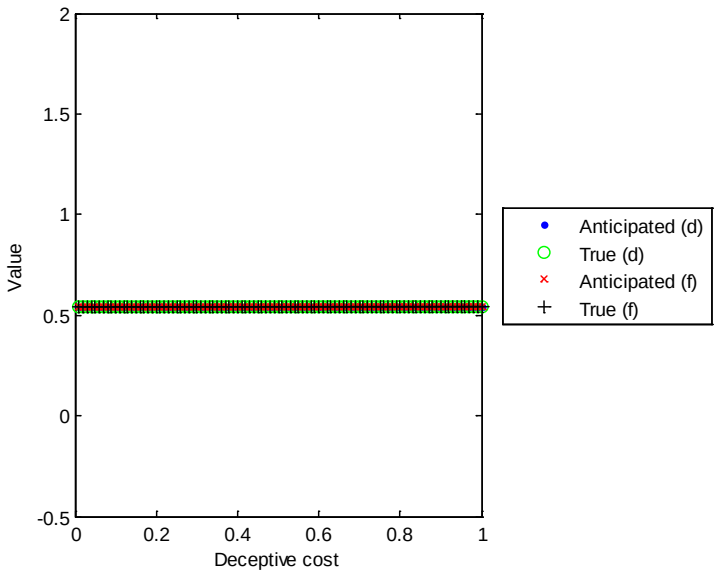

Figure 5. Column-Changing Deception Results for Test Game 1.

Figure 5 shows the results of performing column-changing, equilibrium-destroying deception on the game shown in Figure 2. The anticipated values of the game given changes to *d* and *f* (blue dots and red x's respectively) are calculated using Equation 57 and the value of q' determined based upon the equations in Chapter 3. The true values of the game given changes to *d* and *f* (green circles and black +'s) are calculated using Equation 57 and the true equilibrium probabilities of play for the mark in the deceptive game. As shown, this game does not fulfill the necessary constraints for an increase to *d* to change the equilibrium of the deceptive game, so no benefit is derived from deception under these circumstances. Column-changing deception could occur if the value of *e* was increased to create the desired deceptive equilibrium; however, the value of *e* has no effect upon the value of the game once the desired equilibrium is produced and the

result would be equivalent to performing equilibrium-preserving deception with a different initial game, equilibrium location, and maximum deceptive cost.

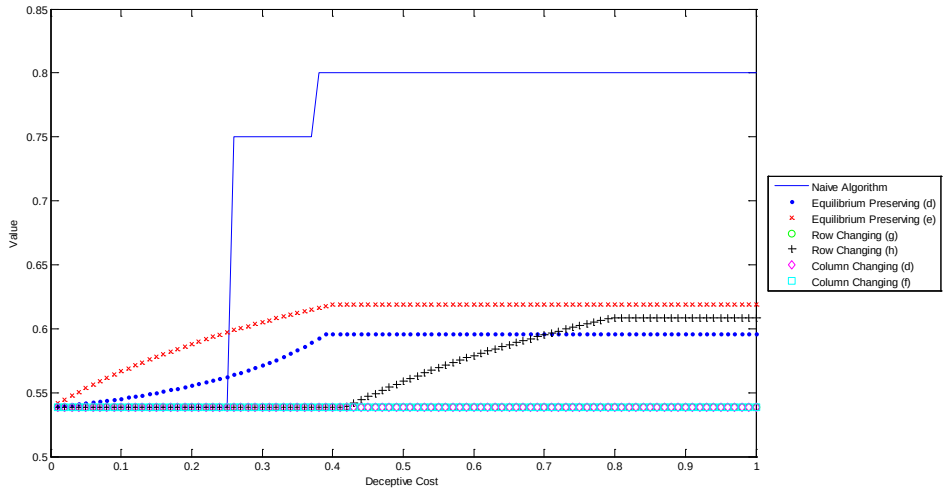

Figure 6. Comparison of Deception Results for Test Game 1.

Figure 6 displays the comparative performance of the algorithms applied to the game shown in Figure 2. As expected, the equilibrium-preserving algorithms modifying *d* and *e* provided benefits to the deceiver immediately, while the remaining algorithms have some delay. The naïve algorithm performed the best as cost increased. In this case, the naïve algorithm had sufficient deceptive cost available to it to increase the value of the deceptive game to the evader to the maximum value of the payoff matrix in the true game.

	0.46	0.54	0
0.48	0.91	0.13	0.63
0.52	0.1	0.81	0.96
0	0.28	0.16	0.55

Figure 7. Test Game 2.

The second game considered is shown in Figure 7. The probabilities of play at equilibrium for each strategy (rounded to the nearest percent) are shown above and to the left of the payoff matrix. The game contains a 2x2 MSNE at the same location as the game shown in Figure 2. However, the relative values of *c* and *f* and *g* and *h* are reversed for this game.

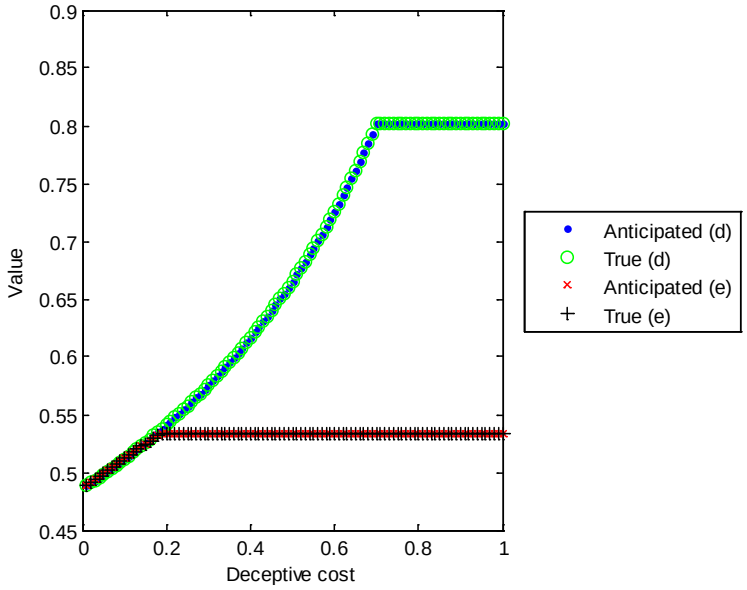

Figure 8. Equilibrium-Preserving Deception Results for Test Game 2.

Figure 8 shows the results of applying equilibrium-preserving deception to the game shown in Figure 7. The value of the game for each case is calculated using Equation 58, with a value of q' derived from the equations in Chapter 3 or the true value in the deceptive game.

$$v = a \cdot q' + b \cdot (1 - q')$$
$$v = .91 \cdot q' + .13 \cdot (1 - q') \tag{58}$$

Like the equilibrium-preserving case for the first game, the anticipated value is correct for the changes to the values of *d* and *e* in the payoff matrix. Unlike the first case, the modifications to the value of *d* outperform the modifications to the value of *e* for this game.

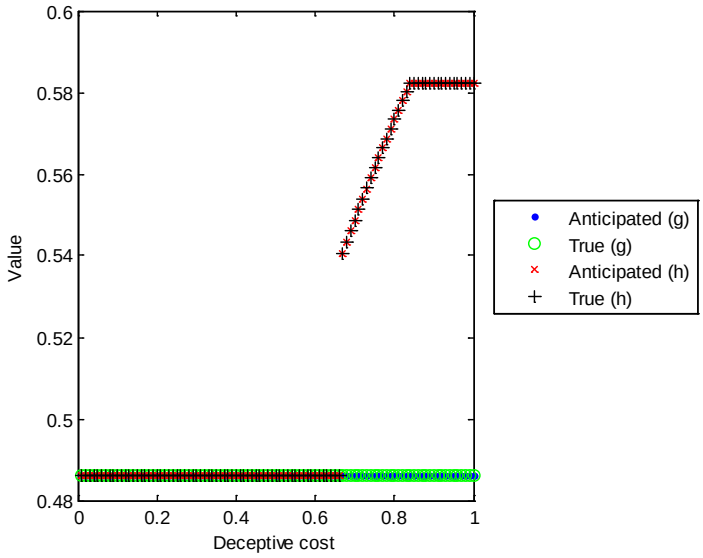

Figure 9. Row-Changing Deception Results for Test Game 2.

Figure 9 shows the results of performing row-changing environmental deception upon the value of the game shown in Figure 7. The value of the game for each case is calculated using Equation 58 and the values of q' computed as described previously.

Like the first game, changing the value of *h* was more effective than changing the value of *g*. As shown, the value of the game remains constant until *h* is changed sufficiently to create the desired equilibrium, causing a rapid increase in the value of the game to the deceiver.

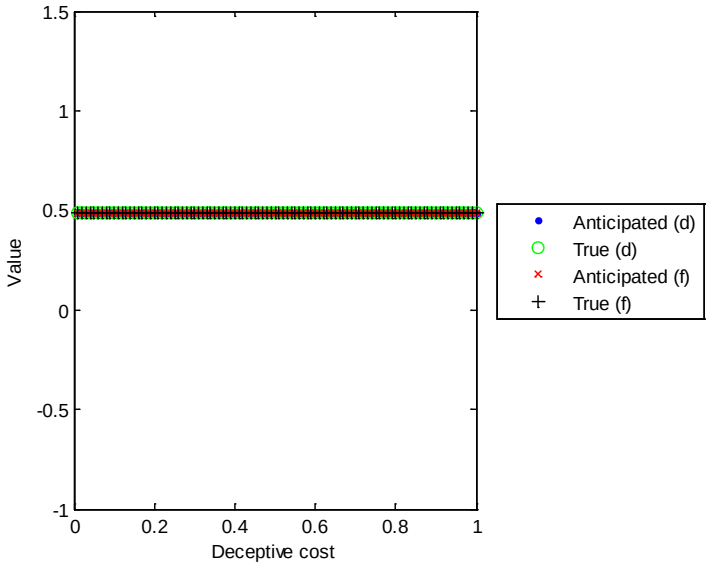

Figure 10. Column-Changing Deception Results for Test Game 2.

Figure 10 shows the results of performing column-changing, equilibrium-destroying deception on the game in Figure 7. The anticipated and true values of the game for increases to the value of *d* and *f* are computed using Equation 58 as described previously. As for the results for the first game, the necessary conditions for the increase to *d* to create the desired equilibrium are not fulfilled for this game.

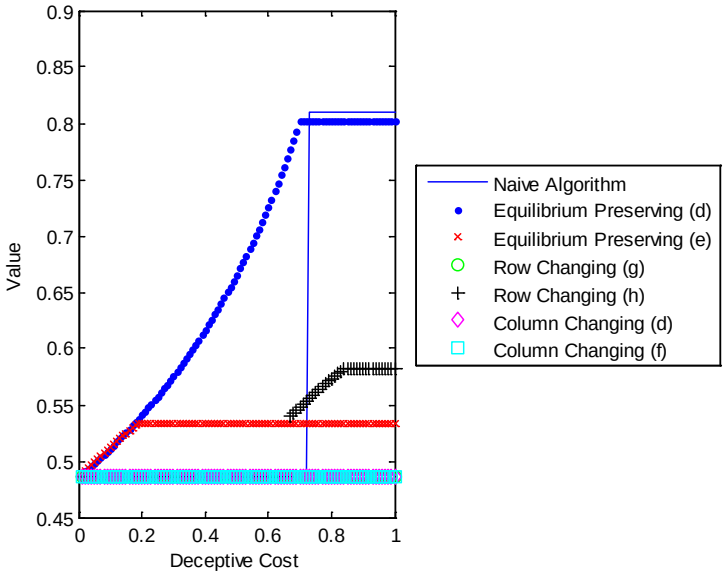

Figure 11. Comparison of Deception Results for Test Game 2.

Figure 11 shows the results of the four algorithms when used to generate deceptive strategies for the game shown in Figure 7. This graph is similar to that of the previous game overall, but is interesting in how the performance of the naïve algorithm does not have as clear of a lead over the other algorithms as in the previous case. In this graph, the naïve algorithm only outperforms the equilibrium preserving algorithm after applying over 0.7 units of cost. This is caused by the great difference in value between the high and low values within the MSNE of the payoff matrix.

Also interesting is the fact that the naïve algorithm never reached the value of the maximum value in the payoff matrix in this case. This indicates that the algorithm has insufficient deceptive cost available to do so and deception is costly to the deceiver using this algorithm. However, modifications to the value of *d* provide instant benefit to the deceiver and continue to do so until the boundary condition is reached.

	0.27	0.73	
0.63	0.61	0.4	0.5
0.37	0.2	0.55	0.53
	0.1	0.56	0.5

Figure 12. Test Game 3.

Figure 12 shows the third game to which the strategies for deception are applied. The probabilities of play at equilibrium for each strategy (rounded to the nearest percent) are shown above and to the left of the payoff matrix. In this game, the relative values of the cells at locations *e* and *h* are reversed. The game contains a 2x2 MSNE at the same location as the previous two games.

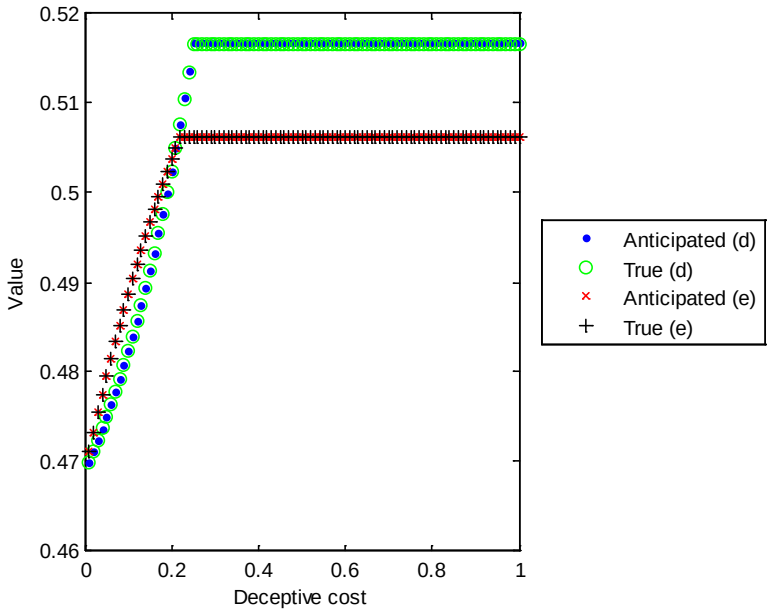

Figure 13. Equilibrium-Preserving Deception Results for Test Game 3

Figure 13 shows the results of applying the equilibrium-preserving deception algorithm to the game shown in Figure 12. The anticipated and true values of the game are calculated using the computation of q' as described previously and Equation 59.

$$v = a \cdot q' + b \cdot (1 - q')$$
$$v = .97 \cdot q' + .49 \cdot (1 - q') \tag{59}$$

As shown, both sets of anticipated game values match the truth, demonstrating the correctness of the equations described in Chapter 3 for this case.

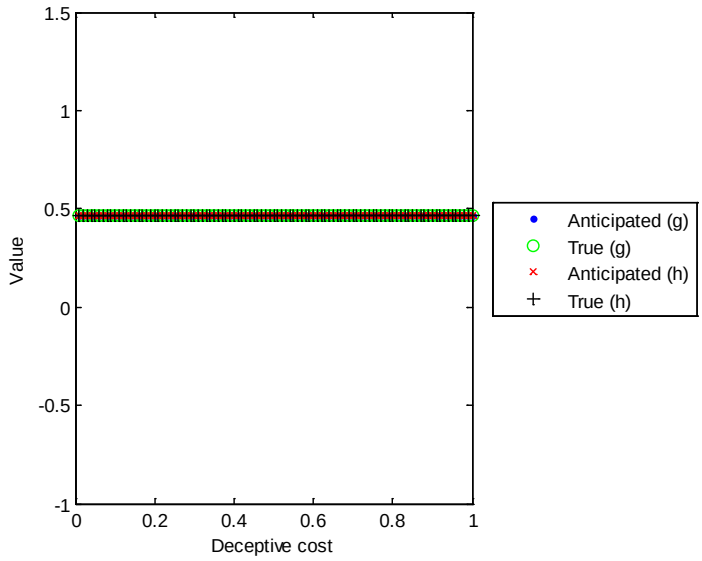

Figure 14. Row-Changing Deception Results for Test Game 3.

Figure 14 shows the results of applying row-changing, equilibrium-destroying deception to the game shown in Figure 12. The anticipated and true values of the game for all cases were computed using Equation 59 and the computation of q' as described for the previous two games. In this game, row-changing, equilibrium-destroying deception could not be performed as g is greater than h in the initial game (which makes the desired MSNE impossible if g is further increased) and no value for h exists that does not violate at least one of the boundary conditions for h.

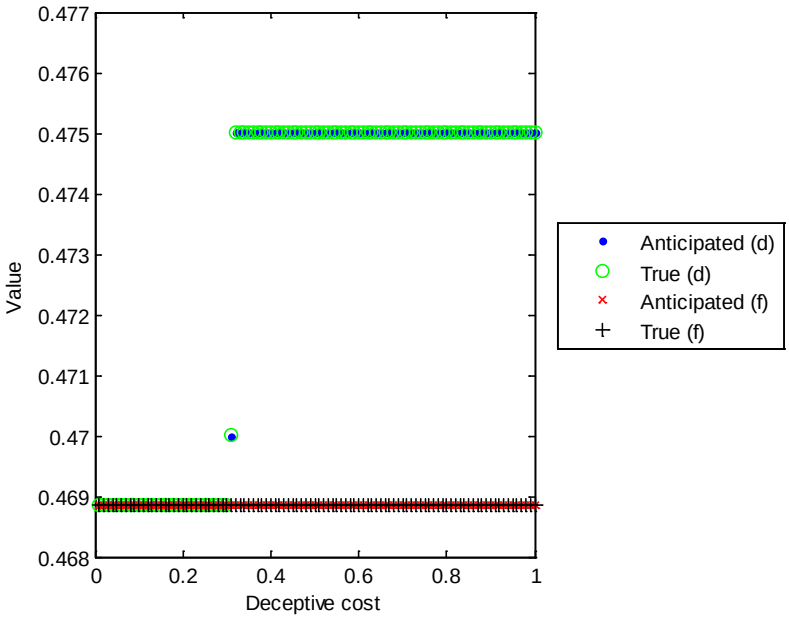

Figure 15. Column-Changing Deception Results for Test Game 3.

Figure 15 shows the results of performing column-changing, equilibrium-destroying deception on the game shown in Figure 12. The value of the game for each case is calculated as described previously using Equation 59. As shown, unlike the previous two games the necessary conditions for creating the equilibrium by increasing the value of *d* are fulfilled in this case, allowing the column-changing equilibrium-destroying algorithm to perform effective deception if the value of *d* is increased.

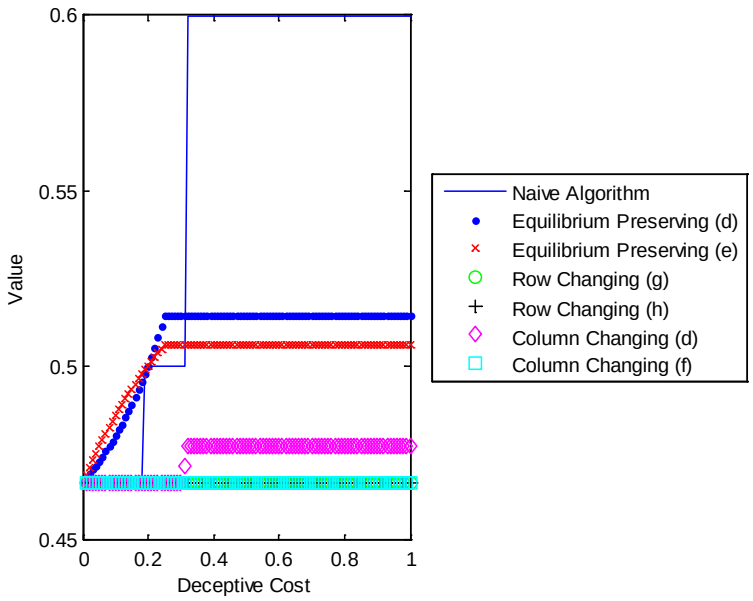

Figure 16. Comparison of Deception Results for Test Game 3.

Finally, Figure 16 demonstrates the performance of the four deceptive algorithms described in Chapter 3 when applied to the game shown in Figure 12. This graph is similar to that of the first game, with the naïve algorithm only narrowly outperforming the equilibrium-preserving algorithm and at significant cost. Unlike the first and second games, the column-changing equilibrium-destroying deception algorithm does provide positive results, but is outperformed by both the naïve and equilibrium-preserving algorithms. Once again, the naïve algorithm does not reach the highest value of the payoff matrix due to cost constraints.

This section demonstrates the effectiveness of the four algorithms described in Chapter 3 for developing strategies for environmental deception. Three 3x3 games containing a 2x2 MSNE with differing relative cell values were considered and the correctness of the closed-form solutions for deception were empirically validated for each. Each

method of deception and means for creating the desired deceptive equilibrium is considered separately in this section to highlight their relative strengths and weaknesses, but combinations of multiple types are possible if cost is available. The effectiveness of each algorithm with regard to value gain and deceptive cost varies based upon the structure of the game. The next section compares the four algorithms based upon the remaining four criteria for effective deception: benefit delay, believability, opponent risk, and efficiency.

4.2 Comparative Performance of Algorithms With Regard to Criteria

In Chapter 3, six criteria for evaluating the performance of the environmental deception algorithms were presented. These criteria are the value gain achieved by deception, the deceptive cost incurred, the delay in benefits to the deceiver due to deception, the believability of the deception, the opponent risk of deception, and the efficiency of the algorithm.

The relative effectiveness of the algorithms with regard to value gain and deceptive cost are shown in the previous section for various games. As discussed previously, the effectiveness of an algorithm is dependent upon the type of games to which it is applied.

The benefit delay of an algorithm does not depend upon the type of game to which the algorithm is applied. The only algorithm presented here with no benefit delay is the equilibrium-preserving algorithm, as the application of deceptive cost produces an instant value gain to the deceiver. The naïve, row-changing, and column-changing algorithms all have a benefit delay as some cost is necessary to help create the desired equi-

librium within the deceptive game before the deceptive player receives an increase in the value of the game due to deception.

The believability of a deceptive algorithm is independent of the type of game to which an algorithm for developing deceptive strategies is applied. Each algorithm is labeled here as having high, medium, or low believability.

A highly believable algorithm never produces a deceptive strategy in which the mark can receive a payoff value that has been changed in the deceptive game. The equilibrium deception algorithms have high believability as the deceiver selects a strategy to play in advance and does not modify the values of any of the payoff cells contained within that strategy.

An algorithm with medium believability does not produce deceptive strategies where a rational, deceived mark (i.e. one playing a strategy derived from the Nash equilibrium of the deceptive game) will not receive a payoff that has been modified in the deceptive game. However, a mark that does not play rationally may receive a payoff that has been modified. The naïve algorithm falls into this category as it creates a PSNE within the game and does not modify that value of the PSNE cell. However, cells in the row of the PSNE may be modified, so an irrational or suspicious mark may receive a payoff that has been modified in the deceptive game.

An algorithm with low believability produces deceptive strategies where a mark can receive payoffs that have been modified in the deceptive game even if he plays at the Nash equilibrium of the deceptive game. None of the algorithms presented here fall into this category.

Opponent risk measures the amount of risk to the deceiver caused by a mark that is irrational or suspicious. The deceptive strategies generated by the algorithms described previously assume that the mark is deceived and plays at a strategy derived from the Nash equilibrium of the deceptive game. However, the loss of value gain and believability caused by violation of this assumption varies from algorithm to algorithm and is measured by opponent risk. Each algorithm for generating deceptive strategies classified as having high or low opponent risk.

A high value of opponent risk indicates that a deceptive strategy is highly dependent upon the mark playing the equilibrium strategy of the deceptive game, as is the case for the naïve algorithm. In this algorithm, the deceiver forces a PSNE in the deceptive game regardless of the type or location of the equilibrium of the true game. This blind approach to deception is highly dependent upon the mark's cooperation and thus has high opponent risk.

A deceptive strategy has low opponent risk if the deceptive player plays in a way that is rational for the true game. This is true of the equilibrium deception algorithms. For all of these algorithms, the deceiver selects a strategy within the equilibrium of the true game to play. If the mark is not deceived and plays the equilibrium of the true game, these deceptive strategies do not cause a loss for the deceiver.

Finally, the efficiency of the algorithm is important to the determination of deceptive strategies. If an algorithm cannot determine a deceptive strategy within the time allotted to it, the effectiveness of the resulting strategy is immaterial. The efficiencies of the deceptive strategy generation algorithms are measured as high, medium, and low.

An algorithm with high efficiency has efficiency on the order of $O(1)$. This is true for the equilibrium deception algorithms as the number of calculations necessary to determine the best deception is based simply off maximizing the increase to a value while not violating the boundary conditions or cost threshold.

The naïve algorithm has medium efficiency as the majority of the means for developing a deceptive strategy is determined in advance. Once a cell is selected to be the PSNE cell of the modified game, the desired modified game can be created in time on the order of $O(m)$ where m is the number of cells within the payoff matrix of the game.

No algorithms presented here have efficiency worse than linear in the size of the game or the cost of deception.

In selecting a method of deception to perform, tradeoffs must be made. Based upon believability, opponent risk, and efficiency, the three equilibrium deception algorithms appear equal and outperform the naïve algorithm. However, the equilibrium deception algorithms are currently limited to 2x2 MSNEs within a 3x3 game, while the naive algorithm can operate on any game.

As shown in this and the previous section, the three equilibrium deception algorithms are not equal with regard to effectiveness per unit expended cost. The equilibrium-destroying algorithms require an input of deceptive cost to create the desired equilibrium before any benefit comes to the deceiver. If the deceiver has a maximum allowable deceptive cost less than the amount necessary to create the equilibrium, then equilibrium-destroying deception is useless to him.

The effectiveness of a method for environmental deception is very much dependent upon the game to which it is applied and the selection should take into account the tradeoffs described in this section and the results presented earlier in the chapter for games with different relative values of cells with the same equilibrium structure.

5. Conclusions and Recommendations

The study of performing and defending against deception is a field of great interest in game theory; however, the focus of research is primarily on *action* deception and extensive-form games. The goal of this research is to develop methods to generate strategies for performing environmental deception in strategic-form games, where the deception centers upon the mark's perception of the game being played rather than the actions taken by the deceiver.

To this end, four algorithms were developed using different methods for generating strategies for modifying the mark's perception of the payoff matrix in order to induce him to play using a suboptimal strategy and increase the value of the game for the deceiver. These algorithms are the naïve, equilibrium preserving, row-changing equilibrium-destroying and column-changing equilibrium-destroying algorithms. The naïve algorithm is applicable to all sizes of games containing all types of Nash equilibria, while the current versions of the remaining algorithms are only capable of generating deceptive strategies for 3x3 games containing 2x2 MSNEs.

The algorithms were applied a set of 3x3 games containing a 2x2 MSNE where the payoff values for the deceiver and mark in a cell of the payoff matrix sum to one. The algorithms are evaluated based upon the

1. Increase in value of the game for the deceiver due to the deception,
2. The cost of deception,
3. The believability of the deception,
4. The risk related to deception if the attacker does not play at the Nash equilibrium of the deceptive game due to irrationality or suspicion

5. The efficiency of the algorithm.

Based upon these results, it is found that the value gain produced by a deceptive algorithm is dependent upon the type of game to which it is applied and the maximum amount of allowable change to the payoff matrix emphasizing the importance of carefully selecting an algorithm to match the situation to which it is applied. The naïve algorithm is applicable to all games but risks discovery of deception and has efficiency linear in the size of the payoff matrix. The remaining three algorithms are only applicable to games containing 2x2 MSNEs in 3x3 games and have high believability and high efficiency, but cannot achieve the same maximum value gain to the deceiver as the naïve algorithm if sufficient cost is available to the deceiver.

The major contributions of this research are an expansion of the notion of equilibrium stability as described in [3] to include cells outside of the equilibrium of a game, the definition of a set of criteria to evaluate strategies for environmental deception, the creation of an algorithm that performs effective environmental deception on any game with minimal information (for use as a baseline for evaluation of other environmental deception algorithms), and the development of closed-form solutions for calculating deceptive strategies that transform a 3x3 game containing a 2x2 MSNE into a deceptive game containing a 2x2 MSNE where equilibrium play by the mark in the deceptive game provides an increase in value of the game to the deceiver.

Several areas of further research exist based upon the work described in this thesis. This work demonstrates that closed-form solutions for effective, believable environmental deception can be determined for a 2x2 MSNE within a 3x3 game. The first two

areas of future work are the expansion of these closed-form solutions to include different types of equilibria within a 3x3 game.

Based upon the stability analysis described earlier, the minimum amount of change to a game containing a PSNE can be easily calculated, resulting in a MSNE to which the current closed-form solutions can be applied. However, there is no guarantee that the lowest cost transformation produces the MSNE for which the deceiver can apply the methods described here to achieve the greatest value gain for minimum cost. Exploration of the transformation of PSNEs in the true game to MSNEs in the deceptive game is a promising area of future research.

Secondly, while the research described here describes methods for deception in 3x3 games containing 2x2 MSNE, the case of a 3x3 MSNE within a 3x3 game has not been solved. Equilibrium-preserving deception can be performed simply by generalizing the current equations, but the optimal selection of cells to modify has not yet been determined. The determination of a closed-form solution for effective equilibrium-destroying deception that transforms a 3x3 MSNE to a desired 2x2 MSNE while benefitting the deceiver is also an area open for future study.

Finally, the expansion of the research to games larger than 3x3 is an area for future work. Deception for larger games containing 2x2 MSNEs is definitely possible and increasing the sizes and types of the equilibria as described previously will allow environmental for deception in a much larger variety of games.

Appendix A. Properties of Non-Cooperative Sum-To-One Games

The type of games studied in this research- non-cooperative, strategic-form games whose payoffs sum to one- have properties that are of interest when developing strategies for effective environmental deception. These properties include the properties of pure-strategy Nash equilibria in such games and the existence of only a single PSNE or MSNE in a game. This Appendix explains these properties and provides proofs of their accuracy.

A.1 Properties of Pure-Strategy Nash Equilibria in Sum-To-One Games

Pure-strategy Nash equilibria (PSNEs) are the rarer of the two equilibrium types in competitive games due to the conditions necessary for their existence. For a PSNE to exist in a game, there must exist a strategy that provides a payoff better for both players given their opponent's choice of strategy. For these conditions to exist, the following properties of pure-strategy Nash equilibria must be true.

1. All equilibrium cells have the minimum payoff value in their row from the perspective of the row player (from the perspective of the column player, this is the maximum in the row and therefore the player has no incentive to deviate from this strategy)
2. All equilibrium cells must have the maximum payoff value in their column from the perspective of the row player (the row player must have no incentive to deviate from the equilibrium strategy)

3. If multiple PSNEs exist in a game, they all have the same payoff value from the perspective of both players (based on von Neumann's Minimax Theorem [30])
4. Any cell at the intersection of the row of one PSNE and the column of another PSNE is also a PSNE with the same value (based on von Neumann's Minimax Theorem [30])

The first and second properties are based upon the definition of a Nash equilibrium which states that neither player has incentive to unilaterally deviate from the equilibrium strategy. The third and fourth properties are based upon the proof that only a single equilibrium can exist in a game, though it may contain multiple cells, and the definition of incentive to deviate. When another cell provides an equal value to a player, there is no incentive to change to that cell as it provides no additional value; however, there is no cost to the player if they do so. This definition of incentive to deviate is important to the proof in the following section.

A.2 Existence of a Single Equilibrium in Sum-To-One Games

In games where the payoffs in a cell of the payoff matrix do not have a constant sum, multiple equilibria can exist within a game. However, in non-cooperative, constant-sum games, only a single equilibrium can exist in a game. This section provides proofs that two pure-strategy Nash equilibria cannot coexist and that a pure-strategy Nash equilibrium cannot coexist with a mixed-strategy Nash equilibrium.

a	*b*	*c*
d	*e*	*f*
g	*h*	*i*

Figure 17. Example 3x3 Game.

For the proof against the co-existence of two PSNEs, the properties of PSNEs and the definition of incentive discussed in the previous section are important. For this proof, inequalities regarding the relative values of equilibrium cells to other cells are assumed to be strict. Once the proof is completed, the effects of allowing equality between values of the equilibrium cells and non-equilibrium cells are discussed. The goal is to provide a proof by contradiction of the existence of two equilibrium cells with unequal value in cells *a* and *i* of the payoff matrix as shown in Figure 17. Payoffs used are from the perspective of the row player.

1. $a > d$ From existence of a PSNE at *a*
2. $a > g$ From existence of a PSNE at *a*
3. $a < b$ From existence of a PSNE at *a*
4. $a < c$ From existence of a PSNE at *a*
5. $i > c$ From existence of a PSNE at *i*
6. $i > f$ From existence of a PSNE at *i*
7. $i < h$ From existence of a PSNE at *i*
8. $i < g$ From existence of a PSNE at *i*
9. $a > i$ From 2 and 8
10. $a < i$ From 4 and 5

As 9 and 10 are mutually contradictory, PSNEs with unique values cannot exist at *a* and *i*. This proof is based upon von Neumann's Minimax Theorem [30]. Allowing non-strict inequalities results in the following relationships based upon 2, 8, 4, and 5: $a \geq g \geq i$ and $a \leq c \leq i$. If *a* and *i* are both PSNEs with the same value, *c* and *g* must also be PSNEs with the same value. This case is accounted for in the stability analysis in Appendix B.

The proof that a PSNE and an MSNE cannot coexist is also a proof by contradiction. By definition, an MSNE contains all strategies that provide equivalent value with the given equilibrium strategy profiles for both players. Therefore, any strategy not within the equilibrium must have a value strictly less than the value of the game with the given probabilities of play of the equilibrium strategies. Once again, the payoff values in Figure 17 are used from the perspective of the row player. The row player is assumed to play the top row with probability p and the middle row with probability $(1 - p)$. The

column player plays the leftmost column with probability q and the middle column with probability $(1-q)$. A PSNE is assumed to exist at location i.

1. $v = aq + b(1-q) = dq + e(1-q)$
2. $v > gq + h(1-q)$
3. $1 - v = (1-a)p + (1-d)(1-p) = (1-b)p + (1-e)(1-p)$
4. $1 - v > (1-c)p + (1-f)(1-p) = 1 - (cp + (1-f)p)$
5. $v < cp + (1-f)(1-p)$
6. $i > c$
7. $i > f$
8. $i < g$
9. $i < h$
10. $v > iq + i(1-q) = i$
11. $v < ip + (1-i)(1-p) = i$

As 10 and 11 are mutually contradictory, a PSNE and a MSNE cannot coexist in a game where the payoffs for both players within a cell of the payoff matrix sum to one. This proof is also based upon von Neumann's Minimax Theorem [30]. Between this proof and the previous, it is shown that only a single equilibrium exists within a constant-sum game.

Appendix B. Stability of Two-Player Zero-Sum Games

The *stability* of a cell in the payoff matrix of a game reflects its ability to change the value and/or equilibrium strategy set of a game. The stability of a cell is used here to refer to the minimum value by which a cell can be modified and cause the equilibrium of the game to change in value or strategy profile. This information is useful as it provides targeting information for modifications to the payoff matrix presented to the mark when environmental deception is being performed. The stability of a cell is dependent upon the type of Nash equilibrium contained within the game, pure-strategy or mixed-strategy, so the two cases are discussed separately in this Appendix.

B.1 Stability of Games Containing Pure-Strategy Nash Equilibria

The first case for stability analysis of a game is games containing pure-strategy Nash equilibria. In this section, the game is broken into four regions and each is analyzed separately. The four regions considered are the equilibrium cell(s) of the game, cells in the row(s) of the game's equilibrium cell(s), cells in the column(s) of the game's equilibrium cell(s), and cells that share neither a row nor a column with an equilibrium cell.

B.1.1 Stability of Equilibrium Cells

If only one PSNE cell exists, changing the value of the payoff at the equilibrium location will change the value of the game since the value of the game for a player is that player's payoff at this location (unless it is changed enough to cause a new equilibrium to be formed). If the equilibrium remains at the original location, then the modified game is strategy-equivalent to the original game but not value-equivalent. In the event that the modification to the payoff value of the equilibrium cell causes it to be no longer an equi-

librium, the game is no longer strategy-equivalent to the original game, (but may be value-equivalent if the new equilibrium happens to have the same value as the original equilibrium). In either case, the value at the equilibrium location (when only one equilibrium cell exists) cannot be modified without altering the strategy-equivalence, value-equivalence, or both.

If multiple PSNE cells with the same value exist, then the effect of modifying a single one of these cells depends upon the number and locations of the equilibrium cells. The effects of modifications based upon the direction of modification (increase/decrease) and the number and location of equilibrium cells is summarized in Table **3**.

Table 3. Value and Strategy Stability of Games Containing Multi-Cell PSNE**s**

Equilibrium Size and Location	**Modification Direction**	**Result**	
		Value Equivalent	**Strategy Equivalent**
Multiple rows and columns of equilibrium	Either	Yes	No
Single Row of Equilibrium	Increase	Yes	No
	Decrease	No	No
Single Column of Equilibrium	Increase	No	No
	Decrease	Yes	No

B.1.2 Stability of Cells in Row of Equilibrium Cells

By the first property of PSNEs within a constant sum game as presented in Appendix A where the row player is the maximizer, the row player's payoff value for a cell that shares a row with an equilibrium cell must be strictly greater than the value of the equilibrium cell(s) of the game. If the cell has a value equal to the equilibrium cell, it would be part of the equilibrium. As the value(s) of these cells in the row of the equilibrium cell(s) have no effect on the value of the game, the only constraint on the payoff value of these cells is that they fulfill this strict inequality requirement. In order for a cell

with value *r* in the row of an equilibrium cell to change the strategy profile and value *v* of the game, it must violate the constraint shown in Equation 60.

$$r > v \tag{60}$$

Therefore, any game whose payoff for the row player for these cells fulfills this constraint without any other changes to other cells is value-equivalent and strategy-equivalent to the original game. Violation of this constraint causes the modified game to be neither value-equivalent nor strategy-equivalent to the original game (unless the resulting new Nash equilibrium happens to be value-equivalent with the original game).

B.1.3 Stability of Cells in Column of Equilibrium Cells

The second property of PSNEs within a constant sum game (presented in Appendix A) bounds the values of cells within the column of an equilibrium cell. These cells must be strictly less than the value of the equilibrium cell or the strategy profile of the game is changed (either by changing the equilibrium location or adding another PSNE cell). This constraint is shown in Equation 61, where *c* is the value of a cell in the column of an equilibrium cell and *v* is the value of the game.

$$c < v \tag{61}$$

Changing the value of same-column cells has no effect on the value of the game as long as the original equilibrium is maintained. Therefore, any game with these cells fulfilling the constraint shown in Equation 61 and no other changes to the payoff matrix that violate payoff value constraints is both value-equivalent and strategy-equivalent to the original game. Violation of this constraint leads to a change in equilibrium and therefore the altered game cannot be strategy-equivalent to the original game (and it will not

be value-equivalent unless the resulting new equilibrium has the same value as the original game).

B.1.4 Stability of Cells in neither Row nor Column of Equilibrium Cells

Changing payoffs can only modify the value or strategy profile of the game by eliminating the existing PSNE or by creating a new one. As the existing PSNE has no dependency upon the values of the cells outside the row and column of the PSNE, modifications of these values will have no effect upon the existence of the current PSNE of the game. The properties of PSNEs described in Appendix A state that it is impossible for two unique PSNEs to exist in the game, so modifying these cells cannot create a second unique-value PSNE in the game. Also, any cell at the intersection of the row of one equilibrium cell and the column of the other must also be a non-unique PSNE. Using this information, we can conclude that it is impossible to create a non-unique PSNE at this location without modification to create the other necessary equilibrium cells. Therefore, modification of the payoff values of these cells without changing other cells to violate the constraints described in Equations 60 and 61 create a game which is value-equivalent and strategy-equivalent to the original game. The only exception to this is if the cells in the intersection of the row/column of the cell being modified and the column/row of the equilibrium cell have the same value as the equilibrium cell. This case results in the equilibrium cell shifting to the modified cell but only applies if these equalities are true.

Two two-player, constant-sum games are value and strategy-equivalent as long as they both contain PSNEs with the same value in the same locations (after necessary isomorphic transformations), all values in the row of a PSNE cell are strictly greater than the value of the game, and all the rows in the column of an equilibrium cell are strictly less

than the value of the game. The scenarios in which the original game and the modified game are value-equivalent or strategy-equivalent have also been described. Next, the stability of the equilibrium is determined by finding the maximum value by which any cell of the payoff matrix can be changed without causing a change in the value or strategy profile of the game. This is accomplished by calculating the *sensitivity* of the equilibrium: the minimum modification to one or more payoff values that causes either the game's value or strategy profile to change.

The sensitivity of a pure strategy Nash equilibrium in a two-player, constant-sum game can be determined by the minimum amount of change to the payoff value of a cell necessary to create a mixed strategy Nash equilibrium (MSNE) within the game or relocate the PSNE.

A MSNE can be created by modification of the payoff values in the matrix such that no payoff location fulfills the requirements for a PSNE, (minimum in its row and maximum in its column from the row player's perspective). Once a MSNE is created in the game, the strategy profile of the game is different from that of the original game.

Modifying a non-equilibrium payoff value to be equal to the Nash equilibrium value can create an equilibrium where one player is indifferent between two strategies because they both yield the same payoff. Changing a value in the row (or column) of the Nash equilibrium cell to be strictly less than (or greater than) the equilibrium cell can eliminate the original PSNE. The sensitivity of the game's equilibrium (reported as a payoff difference) can be quantified as the minimum amount of payoff change necessary to add a PSNE or eliminate an existing one, as shown in Equation 62, where r is the value

of a cell in the row of the PSNE cell, and c is the value of a cell in the column of the PSNE cell.

$$s = \min((\forall r, \min(r - v)), (\forall c, \min(v - c))) \tag{62}$$

As the equilibrium's sensitivity provides a minimum change necessary to cause a game to change equilibrium classes, a game's stability is bounded above by this value. The stability bounds for games with PSNEs are shown in Table **4**, where *m* is the change in value to the payoff value of the indicated cell. The bounds constrain the value of *m* to ranges that do not break the value or strategy stability of the game. In Table **4**, the values for r' and c' are defined in Equations 63 and 64, where *r* is a cell in the row of the equilibrium and *c* is the value of a cell in the column of the equilibrium.

$$r' = \min(r) \tag{63}$$

$$c' = \max(c) \tag{64}$$

Table 4. Stability Bounds for Games Containing PSNEs.

Modification Location	**Value Stability**	**Strategy Stability**
Equilibrium Location	$m \neq \min\begin{pmatrix} r' - v, \\ v - c' \end{pmatrix}$	$m < \min\begin{pmatrix} r' - v, \\ v - c' \end{pmatrix}$
Row of Equilibrium (single row of PSNEs)	$m < r' - v$	$m < r' - v$
Row of Equilibrium (multiple rows of PSNEs)	m unbounded	$m < r' - v$
Column of Equilibrium (single column of PSNEs)	$m > c' - v$	$m > c' - v$
Column of Equilibrium (multiple rows of PSNEs)	m unbounded	$m > c' - v$

Using the stability bounds described in Table **4**, it is now possible to calculate the stability of a game containing a PSNE. As stated earlier, the stability of a game is defined as the minimum amount by which a cell in the game can be modified to produce a game that is not strategy-equivalent to the original game.

Strategy-equivalence is the important aspect of equilibrium stability for our research because in the environmental deception paradigm, both players receive the payoff values produced by their choices of strategy based upon the payoff matrix of the original game. As the deception does not affect reality, modifying the payoff matrix in a way that preserves the original strategy profile of the game has no benefit to the deceiver. Environmental deception can only affect the value of the game by causing the mark to use a different strategy profile than he would choose if he knew the true payoff matrix of the game. Therefore, strategy stability is the important aspect of equilibrium stability for this research.

Table **4** provides the stability values for each of the three regions of the payoff matrix where modifications to the payoff matrix have an effect upon the equilibrium stability of the game. The stability of a game with a PSNE is described in Equation 65, where s_e, s_r, and s_c are the upper bounds on the cell stability as described in Table 4 of the equilibrium location, row of equilibrium, and column of equilibrium respectively.

$$stability = \min(s_e, s_r, s_c) \tag{65}$$

This value of stability is useful as it defines the lower bound on the amount of cost necessary to perform environmental deception in a game containing a PSNE. If the maximum allowable cost of deception does not exceed this value, then it is impossible to

modify the strategy profile of the mark in the game and all cost incurred in deception is wasted. The next section expands the definition of stability presented here to cover games containing MSNEs.

B.2 Stability of Games Containing Mixed-Strategy Nash Equilibria

Now that we have presented a means for determining the equilibrium stability and payoff generalizations of a game containing pure strategy Nash equilibria, we shift our focus to games with mixed strategy Nash equilibria (MSNE). We begin by defining mixed-strategy Nash equilibria and use this definition to compute the relative payoff values of the various strategy profiles within the game. Using this information, we can derive the payout generalizations and equilibrium stability for various forms of mixed strategy Nash equilibria.

A mixed strategy Nash equilibrium exists when for all players in a game, a player's mixed strategy maximizes his payoff given that the opponent's strategies are fixed [2]. In a mixed-strategy Nash equilibrium, each player selects the probability of playing each of their strategies to make their opponent indifferent between each of the strategies in their strategy set, i.e. the expected payoff value of all of their strategies in their strategy set are equal. Also, this expected value is strictly greater than the expected value gained by selecting a strategy outside of this strategy set.

The existence of a MSNE implies that those strategies outside of the MSNE have a strictly lower expected value than those within the MSNE and have no effect on the value of the game. Therefore, two games with the same payoff values of the cells within the mixed strategy Nash equilibrium and for which all strategies outside the strategy set

of the MSNE for a given player are less desirable to that player than those within the MSNE strategy set for that player are both value-equivalent and strategy-equivalent.

a	*b*	*c*
d	*e*	*f*
g	*h*	*i*

Figure 18. Example 3x3 Game.

As an example, we use the 3x3 zero sum game shown in Figure 18, where values with a subscript of one are the payoff to the row player and values with a subscript of two are payoffs for the column player. Assume that a mixed strategy Nash equilibrium exists in this game in which the row player will play the top row with probability p and the middle row with probability 1-p. Similarly, the column player will play the leftmost and middle columns with probabilities q and 1-q respectively. By the definition of mixed strategy Nash equilibria, the value v of the game for the row player is presented in Equation 66, where each variable other than q is the payoff value of the given cell from the perspective of the row player.

$$v = q \cdot a_1 + (1 - q) \cdot b_1 = q \cdot d_1 + (1 - q) \cdot e_1 \tag{66}$$

The same value of the game can be calculated by equating the strategies of the column player while using the row player's payoffs for each cell as shown in Equation 67. This is possible because the payoffs and value of the game of the column player are one minus that of the row player. For the remainder of this Appendix, the subscript will be removed and the value used is the payoff from the perspective of the row player.

$$\begin{gathered} v_2 = p \cdot a_2 + (1-p) \cdot d_2 = p \cdot b_2 + (1-p) \cdot e_2 \\ v_2 = p \cdot (1-a_1) + (1-p) \cdot (1-d_1) = p \cdot (1-b_1) + (1-p) \cdot (1-e_1) \\ v_2 = p - a_1 p + 1 - d_1 - p + d_1 p = p - b_1 p + 1 - e_1 - p + e_1 p \\ v_2 = 1 - (a_1 p + d_1 - d_1 p) = 1 - (b_1 p + e_1 - e_1 p) \\ 1 - v_1 = 1 - (a_1 p + d_1 - d_1 p) = 1 - (b_1 p + e_1 - e_1 p) \\ v_1 = p \cdot a_1 + (1-p) \cdot d_1 = p \cdot b_1 + (1-p) \cdot e_1 \end{gathered} \tag{67}$$

From the knowledge of the mixed strategy equilibrium in the game, we can also conclude that strategies outside of the equilibrium have values that are less desirable than the value of the game given the current probabilities of the opponent. For the row player, this means the value should be less than the current value of the game from the row player's perspective. For the column player, this means a value greater than the value *v* while using the row player's payoff values. These conditions are represented in Equations 68 and 69.

$$v > q \cdot g + (1-q) \cdot h \tag{68}$$

$$v < p \cdot c + (1-p) \cdot f \tag{69}$$

As long as these conditions hold, the existing MSNE of the game will remain the same. Therefore, the values of *g*, *h*, *c*, and *f* are bounded as shown in Equations 70-73.

$$g < \frac{v - (1-q) \cdot h}{q} \tag{70}$$

$$h < \frac{v - q \cdot g}{1-q} \tag{71}$$

$$c > \frac{v - (1-p) \cdot f}{p} \tag{72}$$

$$f > \frac{v - p \cdot c}{1-p} \tag{73}$$

These inequalities bound the payoff values of those cells that are contained within the strategy set of one player but not the other in a MSNE. The final type of cell is that

which is contained in the strategy set of neither player. For this cell to affect the equilibrium of the game, it is necessary for its value to be preferred to the current strategy set for both players, i.e. it must become a PSNE. This cannot occur unless the values of other cells are modified in a way that already would eliminate the original Nash equilibrium.

It can be proven based upon von Neumann's Minimax Theorem that a MSNE and a PSNE cannot exist simultaneously within a game where the payoffs in each cell of the matrix sum to one (see Appendix A). Modification of only the value of *i* has no effect upon the value or strategy profile of the game because it cannot become a PSNE without eliminating the existing MSNE. As the existing MSNE constrains the values of same-row and same-column members (such as *c*, *f*, *g*, and *h*), but not non-row or non-column payoffs such as *i*, modifications to the value of *i* cannot eliminate the MSNE. Therefore, the value of a cell that is not contained in any of the strategy sets of a MSNE has no effect on the equilibrium and games with identical MSNEs and no other constraint violations are equivalent with regard to value and strategy regardless of their value of cells that are not contained within any strategy of the Nash equilibrium.

Now that we have determined the bounds for the various classes of variables in a game containing a mixed strategy Nash equilibrium, we can determine the stability of the game: the maximum modification to a payoff from the game possible without changing the value or strategy profile of the game. This value is found by calculating the equilibrium's *sensitivity*, the minimum change necessary to change the value or strategy profile of the game. The change in value or strategy profile of the game can be accomplished either by modifying the payoff values within the mixed strategy equilibrium of the game or by modifying those cells contained by one player's strategy set but not the other's.

MSNEs are sensitive to perturbations to the payoff values of the cells within the equilibrium. Modification of the payoff values within the mixed strategy equilibrium by any amount has an effect on the value and/or probabilities of the equilibrium. As the probabilities are selected to make the opponent indifferent between two or more strategies that possibly have different total payoffs, a modification of these payoffs necessitates a different set of probabilities to achieve this goal. If the payoff values of the cells within the MSNE are changed enough, it is possible that new strategies may be added or removed from the equilibrium as their value to a player relative to the value of the equilibrium increases or decreases. These changes equate to modifying the value of the equilibrium cell of a PSNE. The stability bounds for this case are shown in the first row of Table **5**, where *m* is the amount of change made to the payoff value of the indicated cell. The stability bounds describe the values of *m* that do not break the game's value stability or strategy stability.

A MSNE can also be changed by modifying the payoff values contained in only one set without changing both sets of strategies. These modifications are similar to the modifications of cells within the row and column of a PSNE discussed above and like those are quantifiable by the minimal modification to have an effect. Like the cells in the row and column of a PSNE, the cells in one player's strategy set are bounded by the maximum or minimum values they can contain without disrupting the equilibrium. Therefore the stability of the equilibrium is bounded by the minimum perturbation to one of these cells that causes the cell to violate the constraints bounding it. The stability bounds for cells in the rows and columns of the equilibrium are shown in the second and third rows of Table **5** respectively. In Table **5**, the values of r' and c' are defined in Equations 74

and 75, where *v* is the value of the game, *r* is the value of a cell in the row of the equilibrium, r'' is the value of the other cell in the row of the equilibrium (assuming a 2x2 MSNE), *c* is the value of a cell in the column of the equilibrium, c'' is the other cell in the column of the equilibrium, and *p* and *q* are the probabilities that the strategies resulting in *p* or *c* are played.

$$r' = min\left(\frac{v - (1-p)\cdot r''}{p}\right) \tag{74}$$

$$c' = \min\left(\frac{v - (1-q)\cdot c''}{q}\right) \tag{75}$$

Table 5. Stability Bounds for Games Containing MSNEs

Modification Location	**Value Stability**	**Strategy Stability**
Equilibrium Location	$m = 0$	$m = 0$
Row of Equilibrium	$m < r'$	$m < r'$
Column of Equilibrium	$m > -c'$	$m > -c'$

The above analysis derives the stability bounds and sensitivity of cells in a 3x3 game with a 2x2 MSNE. This analysis can be expanded to different sizes of games with MSNEs of different sizes based upon the same principles and relationships between cells used for the 2x2 MSNE in the example game.

Bibliography

[1] A. Brandenburger, "Cooperative Game Theory: Characteristic Functions, Allocations, Marginal Contribution," Stern School of Business New York University, New York, 2007.

[2] J. Nash, "Noncooperative Games," *The Annals of Mathematics Second Series*, vol. 54, no. 2, pp. 286-295, September 1951.

[3] H. Arsham, "Stability of Essential Strategy in Two-Person Zero-Sum Games," *Congress Numerantium*, vol. 110, pp. 167-180, 1995.

[4] T. E. Carroll and D. Grosu, "A Game Theoretic Investigation of Deception in Network Security," in *Proceedings of 18th International Conference on Computer Communications and Networks*, San Francisco, 2009.

[5] N. Garg and D. Grosu, "Deception in Honeynets: A Game-Theoretic Analysis," in *Proceedings of the 2007 IEEE Workshop on Information Assurance*, West Point, 2007.

[6] R. Pibil, V. Lisy, C. Kiekintveld, B. Bosansky and M. Pechoucek, "Game Theoretic Model of Strategic Honeypot Allocation in Computer Networks," *Decision and Game Theory for Security*, vol. 1, pp. 201-220, 2012.

[7] J. Zhuang, V. M. Bier and O. Alagoz, "Modeling Secrecy and Deception in a Multiple-Period Attacker-Defender Signaling Game," *European Journal of Operational Research*, vol. 203, pp. 409-418, 2010.

[8] J. P. Hespanha, Y. S. Ateskan and H. H. Kizilocak, "Deception in Non-Cooperative Games with Partial Information," in *Proceedings of the 2nd DARPA-JFACC Symposium on Advances in Enterprise Control*, 2000.

[9] C. Y. Ma, D. K. Yau, X. Lou and N. S. Rao, "Markov Game Analysis for Attack-Defense of Power Networks Under Possible Misinformation," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1676-1686, 2013.

[10] K. T. Lee and K. L. Teo, "A Game with Distorted Information," *Naval Research*

Logistics, vol. 40, pp. 993-1001, 1993.

[11] Y. Yavin, "Pursuit-Evasion Games with Deception or Interrupted Observation," *Computers & Mathematics with Applications,* vol. 13, no. 1-3, pp. 191-203, 1987.

[12] G. Levitin and K. Hausken, "Is it wise to leave some false targets unprotected?," *Reliability Engineering and System Safety,* vol. 112, pp. 176-186, 2013.

[13] Z. E. Fuchs and P. P. Khargonekar, "Games, Deception, and Jones' Lemma," in *2011 American Control Conference,* San Francisco, 2011.

[14] V. Lisy, R. Zivan and K. Sycara, "Deception in Networks of Mobile Sensing Agents," in *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems,* Toronto, 2010.

[15] B. Gharesifard and J. Cortes, "Evolution of Players' Misperceptions Under Perfect Observations," *IEEE Transactions on Automatic Control,* vol. 57, no. 7, pp. 1627-1640, 2011.

[16] B. Gharesifard and J. Cortes, "Stealthy Deception in Hypergames Under Informational Asymmetry," in *IEEE Transactions on Systems, Man, and Cybernetics*, 2013.

[17] B. Gharesifard and J. Cortes, "Stealthy Strategies for Deception in Hypergames with Asymmetric Information," in *50th IEEE Conference on Decision and Control and European Control Conference,* Orlando, 2011.

[18] A. R. Wagner and R. C. Arkin, "Robot Deception: Recognizing when a robot should deceive," in *2009 IEEE International Symposium on Computational Intelligence in Robotics and Automation (CIRA),* Daejeon, 2009.

[19] A. R. Wagner and R. C. Arkin, "Acting Deceptively: Providing Robots with the Capacity for Deception," *International Journal of Social Robotics,* vol. 3, no. 1, pp. 5-26, 2011.

[20] I. Greenberg, "The Role of Deception in Decision Theory," *The Journal of Conflict Resolution,* vol. 26, no. 1, pp. 139-156, 1982.

[21] I. Greenberg, "The Effect of Deception on Optimal Decisions," *Operations Research Letters*, vol. 1, no. 4, pp. 144-147, 1982.

[22] D. Li and J. B. Cruz Jr., "Information, decision-making, and deception in games," *Decision Support Systems*, vol. 47, pp. 518-527, 2009.

[23] E. Kohlberg and J.-F. Mertens, "On the Strategic Stability of Equilibria," *Econometrica*, vol. 54, no. 5, pp. 1003-1037, September 1986.

[24] F. Germano, "On Nash Equivalence Classes of Generic Normal Form Games," *Université catholique de Louvain, Center for Operations Research and Econometrics (CORE) Discussion Papers*, vol. 1998033, pp. 1-31, May 1998.

[25] F. Germano, "On Some Geometry and Equivalence Classes of Normal Form Games," *International Journal of Game Theory*, vol. 34, no. 4, pp. 561-581, November 2006.

[26] B. D. Bernheim, "Rationalizable Strategic Behavior," *Econometrica*, vol. 52, no. 4, pp. 1007-1028, July 1984.

[27] M. Dufwenberg and M. Stegeman, "Existence and Uniqueness of Maximal Reductions Under Iterated Strict Dominance," *Econometrica*, vol. 70, no. 5, pp. 2007-2023, September 2002.

[28] R. J. Aumann, "Correlated Equilibrium as an Expression of Bayesian Rationality," *Econometrica*, vol. 55, no. 1, pp. 1-18, January 1987.

[29] S. Morris and T. Ui, "Best Response Equivalence," *Games and Economic Behavior*, vol. 49, pp. 260-287, April 2004.

[30] J. von Neumann, "Zur Therorie der Gesellschaftsspiele," *Mathemaitsche Annalen*, vol. 100, no. 1, pp. 295-320, 1928.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
18-06-2015	Master's Thesis	August 2013 – June 2015

TITLE AND SUBTITLE

Generation of Strategies for Environmental Deception in Two-Player Normal-Form Games

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Poston III, Howard E., Civilian, USAF

5d. PROJECT NUMBER
15G225

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-8865

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-15-J-004

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Intentionally Left Blank

10. SPONSOR/MONITOR'S ACRONYM(S)

N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRUBTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

Methods of performing and defending against deceptive actions are a popular field of study in game theory; however, the focus is mostly on action deception in turn-based games. This work focuses on developing strategies for performing environmental deception in two-player, strategic-form games. Environmental deception is defined as deception where one player has the ability to change the other's perception of the state of the game through modification of their perception of the game's payoff matrix, similar to the use of camouflage. The main contributions of this research are an expansion of the definition of the stability of a Nash equilibrium to include cells outside the equilibrium, and the creation of four algorithms for developing strategies for environmental deception, including closed-form solutions for the creation of a 3x3 deceptive game with a 2x2 mixed-strategy Nash equilibrium (MSNE) that benefits the deceiver from a 3x3 game containing a 2x2 MSNE. It is found that the value gain produced by a deceptive algorithm is dependent upon the type of game to which it is applied and the maximum amount of allowable change to the payoff matrix emphasizing the importance of carefully selecting an algorithm to match the situation to which it is applied.

15. SUBJECT TERMS

Game theory, environmental deception, equilibrium stability

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Brett Borghetti AFIT/ENG
U	U	U	UU	112	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-6565, ext 4612 brett.borghetti@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18