Game Theoretic Risk Analysis of Security Threats

Edited by
Vicki M. Bier | M. Naceur Azaieez
Game Theoretic
Risk Analysis
of Security Threats
INT. SERIES IN OPERATIONS RESEARCH & MANAGEMENT SCIENCE

Series Editor: Frederick S. Hillier, Stanford University
Special Editorial Consultant: Camille C. Price, Stephen F. Austin State University

Titles with an asterisk (*) were recommended by Dr. Price

Axsaeter/ INVENTORY CONTROL, 2nd Ed.
Hall/ PATIENT FLOW: Reducing Delay in Healthcare Delivery
Józefowska & Węglarz/ PERSPECTIVES IN MODERN PROJECT SCHEDULING
Tian & Zhang/ VACATION QUEUEING MODELS: Theory and Applications
Yan, Y in & Zhang/ STOCHASTIC PROCESSES, OPTIMIZATION, AND CONTROL THEORY
APPLICATIONS IN FINANCIAL ENGINEERING, QUEUEING NETWORKS, AND MANUFACTURING SYSTEMS
Saaty & Vargas/ DECISION MAKING WITH THE ANALYTIC NETWORK PROCESS: Economic, Political, Social & Technological Applications w. Benefits, Opportunities, Costs & Risks
Yu/ TECHNOLOGY PORTFOLIO PLANNING AND MANAGEMENT: Practical Concepts and Tools
Kandiller/ PRINCIPLES OF MATHEMATICS IN OPERATIONS RESEARCH
Lee & L ee/ BUILDING SUPPLY CHAIN EXCELLENCE IN EMERGING ECONOMIES
Hooker/ INTEGRATED METHODS FOR OPTIMIZATION
Dawande et al/ THROUGHPUT OPTIMIZATION IN ROBOTIC CELLS
Friesz/ NETWORK SCIENCE, NONLINEAR SCIENCE and INFRASTRUCTURE SYSTEMS
Cai, Sha & Wong/ TIME-VARYING NETWORK OPTIMIZATION
Mamon & Elliott/ HIDDEN MARKOV MODELS IN FINANCE
del Castillo/ PROCESS OPTIMIZATION: A Statistical Approach
Józefowska/ JUST-IN-TIME SCHEDULING: Models & Algorithms for Computer & Manufacturing Systems
Yu, Wang & Lai/ FOREIGN-EXCHANGE-RATE FORECASTING WITH ARTIFICIAL NEURAL NETWORKS
Beyer et al/ MARKOVIAN DEMAND INVENTORY MODELS
Shi & Olafsson/ NESTED PARTITIONS OPTIMIZATION: Methodology and Applications
Samaniego/ SYSTEM SIGNATURES AND THEIR APPLICATIONS IN ENGINEERING RELIABILITY
Kleijnen/ DESIGN AND ANALYSIS OF SIMULATION EXPERIMENTS
Førsund/ HYDROPOWER ECONOMICS
Kogan & Taipierio/ SUPPLY CHAIN GAMES: Operations Management and Risk Valuation
Vanderbei/ LINEAR PROGRAMMING: Foundations & Extensions, 3rd Edition
Chhajed & Lowe/ BUILDING INTUITION: Insights from Basic Operations Mgmt. Models and Principles
Luenberger & Ye/ LINEAR AND NONLINEAR PROGRAMMING, 3rd Edition
Drew et al/ COMPUTATIONAL PROBABILITY: Algorithms and Applications in the Mathematical Sciences*
Chinneck/ FEASIBILITY AND INFEASIBILITY IN OPTIMIZATION: Algorithms and Computation Methods
Tang, Teo & Wei/ SUPPLY CHAIN ANALYSIS: A Handbook on the Interaction of Information, System and Optimization
Ozcan/ HEALTH CARE BENCHMARKING AND PERFORMANCE EVALUATION: An Assessment using Data Envelopment Analysis (DEA)
Wierenga/ HANDBOOK OF MARKETING DECISION MODELS
Agarwal & Smith/ RETAIL SUPPLY CHAIN MANAGEMENT: Quantitative Models and Empirical Studies
Brill/ LEVEL CROSSING METHODS IN STOCHASTIC MODELS
Zsidisin & Ritchie/ SUPPLY CHAIN RISK: A Handbook of Assessment, Management & Performance
Matsui/ MANUFACTURING AND SERVICE ENTERPRISE WITH RISKS: A Stochastic Management Approach
Zhu/ QUANTITATIVE MODELS FOR PERFORMANCE EVALUATION AND BENCHMARKING: Data Envelopment Analysis with Spreadsheets
Kubiak/ PROPORTIONAL OPTIMIZATION AND FAIRNESS*

~A list of the early publications in the series is found at the end of the book~
Game Theoretic
Risk Analysis
of Security Threats

edited by

Vicki M. Bier
University of Wisconsin-Madison
United States

M. Naceur Azaiez
King Saud University
Saudi Arabia
# TABLE OF CONTENTS

1 Why Both Game Theory and Reliability Theory Are Important in Defending Infrastructure against Intelligent Attacks ........................................................................................................... 1
   Vicki M. Bier, University of Wisconsin-Madison, USA
   Louis A. (Tony) Cox, Jr., Cox Associates, Inc., and University of Colorado Denver, USA
   M. Naceur Azaiez, King Saud University, Saudi Arabia

2 Game Theory Models of Intelligent Actors in Reliability Analysis: An Overview of the State of the Art ........................................................... 13
   Seth D. Guikema, Johns Hopkins University, USA

3 Optimizing Defense Strategies for Complex Multi-State Systems .............................................................. 33
   Gregory Levitin, The Israel Electric Corporation Ltd., Israel

4 Defending Against Terrorism, Natural Disaster, and All Hazards........................................................................... 65
   Kjell Hausken, University of Stavanger, Norway
   Vicki M. Bier, University of Wisconsin-Madison, USA
   Jun Zhuang, University at Buffalo (The State University of New York), USA

5 A Bayesian Model for a Game of Information in Optimal Attack/Defense Strategies ................................................................. 99
   M. Naceur Azaiez, King Saud University, Saudi Arabia

6 Search for a Malevolent Needle in a Benign Haystack ................................................................................ 125
   Donald P. Gaver, Naval Postgraduate School, USA
   Kevin D. Glazebrook, Lancaster University, United Kingdom
   Patricia A. Jacobs, Naval Postgraduate School, USA
<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Games and Risk Analysis: Three Examples of Single and Alternate Moves</td>
<td>M. Elisabeth Paté-Cornell, Stanford University, USA, with the collaboration of Russ Garber, Seth Guikema, and Paul Kucik</td>
</tr>
<tr>
<td>8</td>
<td>Making Telecommunications Networks Resilient against Terrorist Attacks</td>
<td>Louis A. (Tony) Cox, Jr., Cox Associates, Inc., and University of Colorado Denver, USA</td>
</tr>
<tr>
<td>9</td>
<td>Improving Reliability through Multi-Path Routing and Link Defence: An Application of Game Theory to Transport</td>
<td>Urszula Kanturska, Arup, United Kingdom&lt;br&gt;Jan-Dirk Schmöcker, Tokyo Institute of Technology, Japan&lt;br&gt;Achille Fonzone, Polytechnic of Bari, Italy&lt;br&gt;Michael G. H. Bell, Imperial College London, United Kingdom</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Index</td>
</tr>
</tbody>
</table>
Chapter 1

WHY BOTH GAME THEORY AND RELIABILITY THEORY ARE IMPORTANT IN DEFENDING INFRASTRUCTURE AGAINST INTELLIGENT ATTACKS

Vicki M. Bier, Louis A. Cox, Jr., and M. Naceur Azaiez

1. WHY GAME THEORY?

Many countries have multiple critical infrastructures that are potentially vulnerable to deliberate attacks by terrorists or other intelligent adversaries. These include networked infrastructures (oil and natural gas pipelines, electric power grids, transportation routes and facilities, telecommunications networks, water supply), built infrastructures (office buildings, hospitals, convention centers, sports stadiums, storage facilities), information infrastructures (flight control, civil defense, emergency broadcasting), and food-production, processing, and distribution supply chains or networks. Since September 11, 2001, determining how best to protect these and other critical infrastructures against intelligent attacks has become a topic of great concern. Researchers and practitioners have attempted a variety of approaches for dealing with this issue.

One motivation for this book is the belief that methods for guiding resource allocations to defend against intelligent antagonists should explicitly take into account the intelligent and adaptive nature of the threat. As discussed in this chapter, simple approaches to risk assessment that may work well in other contexts (such as protecting against accidents or acts of nature) can fail to correctly anticipate and quantify the risks from persistent, intelligent attackers (Golany et al., to appear). Therefore, a more effective approach is needed. It is natural to turn to game theory for ideas and
principles to help optimize defenses, taking into account that antagonists may adapt their subsequent actions to exploit remaining weaknesses.

Protecting critical infrastructures against intentional attacks is fundamentally different from protecting against random accidents or acts of nature. Intelligent and adaptable adversaries may try different offensive strategies or adapt their tactics in order to bypass or circumvent protective security measures and exploit any remaining weaknesses.

Although engineering risk and reliability analysis are clearly important for identifying the most significant security threats and vulnerabilities to terrorist attacks (particularly in complex engineered systems, whose vulnerabilities may depend on interdependencies that cannot be readily identified without detailed analysis), such analyses do not lead in any straightforward manner to sound recommendations for improvements. In particular, risk and reliability analysis generally assumes that the threat or hazard is static, whereas in the case of security, the threat is adaptive and can change in response to the defenses that have been implemented. Therefore, simply rerunning an analysis with the same postulated threat but assuming that some candidate security improvements have been implemented will in general significantly overestimate the effectiveness of the candidate improvements. (For example, installing anthrax sterilization equipment in every post office in the U.S., if publicly known, might have just caused future attackers to deliver anthrax by Federal Express or United Parcel Service.) The routine application of probabilistic reliability and risk analysis methods developed for system safety and reliability engineering is typically not adequate in the security domain.

Game theory provides one way to account for the actions of intelligent adversaries. However, the use of game theory in this context will generally require probabilities of different consequences (e.g., attack success or failure) for various possible combinations of attacker and defender actions. Quantitative risk assessment and reliability analysis models can provide these consequence probabilities. Thus, security and counter-terrorism analysis could benefit substantially from a combination of reliability analysis and game theory techniques.

Among the available approaches for defending against intelligent attacks, game-theoretic models stand out for their rigor and mathematical depth. They have the striking virtue of attributing intelligence (rather than, for example, random activity) to attackers; in other words, game-theoretic methods anticipate that attackers will attempt to exploit paths of least resistance, rather than acting blindly or randomly in response to defender preparations.

On the other hand, game-theoretic models can be difficult to develop, quantify, apply, and validate. Moreover, some game theory models ascribe
unrealistic levels of hyper-rationality and mathematical or computational sophistication to both attackers and defenders, so that both their predictions for real-world attacks and their prescriptions for real-world defenses may be questionable. In fact, many game-theoretic methods rely on idealized or unrealistic assumptions (such as “common knowledge” of prior beliefs about game structures and payoffs) that may not hold in practice. (These stringent assumptions can sometimes be relaxed when agents interact repeatedly and learn successful strategies by trial and error, but that may not be a realistic model for some types of attack strategies, such as attacks that require substantial advance planning and can be tried only once.)

Game-theoretic models are also sometimes criticized for ignoring important psychological and behavioral factors that may drive real-world behaviors. For example, experimental evidence shows that game-theoretic analyses of many standard problems—such as bargaining games, iterated Prisoner’s Dilemma, ultimatum games, escalation games, and others—have only limited predictive power in practice (Shermer, 2008).

Certainly, game-theoretic models of attack and defense can provide useful concepts and computational tools for thinking about risks and allocating resources to defend infrastructure targets against intelligent attackers. The crucial insight from game theory, that rational players base their actions in part on what they expect others to do, is too important to ignore. Yet, we believe that an approach that is more effective and practical than pure game-theoretic analysis is needed. To obtain realistic risk assessments and useful guidance for resource allocation, it is essential to take into account an adversary’s possible adaptive behaviors, but without necessarily descending into the mathematical quagmire of full game-theoretic modeling.

The purpose of this book is to delineate some elements of a more effective approach. In the past decade, attack-defense models have been formulated that avoid many of the computational complexities and recursive belief difficulties familiar in full game-theoretic models, while still allowing for the key feature that attackers are assumed to exploit weaknesses left by defenders. Such models typically allow the attacker to formulate an optimized attack, taking into account the defender’s preparations. Knowing this, the defender prepares accordingly. The additional sophistication allowed in full game-theoretic treatments (e.g., attackers taking actions based on imperfect information but rational conjectures about what the defender may have done, taking into account the attacker’s beliefs about the defender’s beliefs about the attacker’s priorities) is truncated in favor of a simpler approach (analogous to a Stackelberg game in economics), in which the defender acts first and the attacker responds. The power and utility of this approach are illustrated in several of the following chapters.
More generally, this book discusses how to apply a variety of game-theoretic approaches for defending complex systems against knowledgeable and adaptable adversaries. The results yield insights into the nature of optimal defensive investments to best balance the costs of protective investments against the security and reliability of the resulting systems.

2. WEAKNESSES OF RISK AND RELIABILITY ANALYSIS WITHOUT GAME THEORY

This section explores further some of the weaknesses of current non game-theoretic approaches to risk and reliability analysis in setting priorities for protecting infrastructure against terrorist attacks. For example, approaches that attempt to directly assess probabilities for the actions of intelligent antagonists, without modeling how they depend on the defender’s choices (which in turn may depend on assumptions about attack probabilities), are liable to produce ambiguous and/or mistaken risk estimates that are not suitable for guiding resource allocations in practice (National Academy of Sciences, 2008).

Many non game-theoretic applications of risk analysis to security and infrastructure protection rely, either explicitly or implicitly, on the following basic formula:

\[ Risk = \text{Threat} \times \text{Vulnerability} \times \text{Consequence} \]

For example, this is the basis of the Risk Analysis and Management for Critical Asset Protection (RAMCAP™) methodology used by the Department of Homeland Security (RAMCAP™ Framework, 2006) for chemical facilities. It has also been applied (at least implicitly) to agricultural terrorism (see for example Linacre et al., 2005), computer security (Computer Science and Telecommunications Board, 2002), and to protection of secure facilities (Indusi, 2003).

RAMCAP™ defines “risk” as “The potential for loss or harm due to the likelihood of an unwanted event and its adverse consequences.” Similarly, “threat is based on the analysis of the intention and capability of an adversary to undertake actions that would be detrimental to an asset or population”; “vulnerability” is defined as “Any weakness in an asset’s or infrastructure’s design, implementation or operation that can be exploited by an adversary”; and “consequence” accounts for “human casualties, monetary and economic damages and environmental impact, and may also include less tangible and therefore less quantifiable effects, including political ramifications, decreased morale, reductions in operational effectiveness or
other impacts.” Finally, “conditional risk” takes into account “consequences, vulnerability and adversary capabilities, but excludes intent” (for use in situations where intent would be extremely difficult to assess, such as long-range planning) by simply assuming that an attack takes place.

Systems like RAMCAP™ attempt to model the actions of rational adversaries holistically. Facility owners and operators are encouraged to use their knowledge (or perceptions and judgments) to assess the “attractiveness” of each facility to terrorists. They are asked to estimate potential adverse consequences of attacks using a “reasonable worst case” approach, considering (using what might be termed a “conversational game theory” approach) “that the adversary is intelligent and adaptive and will attempt to optimize or maximize the consequences of a particular attack scenario…” (RAMCAP™ Framework, p. 28).

However, in lieu of formal game-theoretic models, RAMCAP™ proposes two options for risk assessment, one qualitative and one quantitative. The “qualitative” (or semi-quantitative) approach uses tables to categorize and score consequences using ordinal scales. Vulnerability is assessed similarly, using an ordinal scale for “likelihood of attack success.” Finally, a “conditional risk matrix” assigns overall conditional-risk scores to pairs of consequence and vulnerability scores, via the formula:

\[
\text{Conditional Risk Score} = \text{Consequence Score} + \text{Vulnerability Score}
\]

The additive formula (rather than a multiplicative formula) for conditional risk reflects the fact that scales for consequence and vulnerability are logarithmic rather than linear (with each additional increment on the scale reflecting a multiplicative increase in consequence or vulnerability, respectively).

Unfortunately, this qualitative approach to risk rating does not necessarily provide adequate information for guiding resource allocation, since ultimately, quantitative numbers of dollars or other resources must be allocated to risk reduction. Also, Cox et al. (2005) note that qualitative risk rankings can in some cases lead to ranking reversals (with larger risks receiving smaller qualitative ratings).

Quantitative risk assessment in RAMCAP™ is also based on the formula:

\[
\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}
\]

but using approximate vulnerability and consequence estimates. The RAMCAP™ Framework states that, using this approach, “The risk associated with one asset can be added to others to obtain the aggregate risk
for an entire facility… [and] can be aggregated and/or compared across whole industries and economic sectors.”

However, even the basic multiplicative formula, \( \text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence} \), can be incorrect if the different components on the right-hand side are correlated with each other. In particular, positive correlations may arise, for example, if intelligent attackers are more likely to attack targets with high Vulnerability and Consequence values. In that case, if the \( \text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence} \) formula is applied to expected values of threat, vulnerability, and consequence, the result may substantially underestimate the true risk.

3. SOME LIMITATIONS OF \( \text{RISK} = \text{THREAT} \times \text{VULNERABILITY} \times \text{CONSEQUENCE} \)

Ordinarily, Threat is intended to reflect the probability of an attack (e.g., in a stated interval of time). However, when intelligent attackers use intelligence about the defender’s own beliefs, values, and defenses to plan their attacks, no such probability may exist. For example, assigning a high enough Threat value to a facility may justify sufficient defensive investment or vigilance to guarantee that the facility will not be attacked. Thus, threat estimates can be “self-defeating”: estimating a threat as high can make the true threat low, and vice versa. This may be viewed as a game in which the defender estimates threats and allocates resources, and the attacker attacks where the estimated threat is low and few defenses have been implemented. Such a game may have no pure-strategy equilibrium (although it may have mixed-strategy equilibrium solutions). This suggests that the concept of threat as a static probability to be estimated may be fundamentally inadequate for protecting against informed, intelligent attackers, since the threat estimate itself may affect the nature of the threat.

“Vulnerability” can also be ambiguous and difficult to calculate via risk-analysis methods such as event trees. Standard event-tree modeling that ignores adaptive, goal-oriented decision-making by the attacker, by treating attacker choices as random events, may underestimate risks. Treating attackers instead as optimizers who calculate their best responses to different possible defenses may lead to different resource allocations, and larger risk reductions (based on deterring attacker actions), than could be achieved using models that ignore the ability of intelligent attackers to adapt their plans as information becomes available before (and during) the course of an attack. Best-response models, in which the defender calculates the attacker’s best responses to various conditions and then chooses defensive investments to minimize the damage from the attacker’s best response (see for example
Brown et al., 2006), may be substantially easier to formulate and solve than full game-theoretic analyses, yet do a much better job than static vulnerability analyses (e.g., using event trees or other traditional tools of risk and reliability analysis) at capturing important features of likely attacker behavior.

This general approach, mathematically reminiscent of principal-agent games, has been developed by military operations-research experts into a powerful alternative to a full game-theoretic analysis that appears to be practical for many counter-terrorism and infrastructure-protection applications (e.g., Brown et al., 2006). Such hierarchical optimization approaches dispense with the concept of Threat as a single number to be estimated, and also go beyond simplistic estimates of vulnerability in the Risk = Threat × Vulnerability × Consequence framework. Instead, they focus on predicting and controlling attacker behaviors (via strategically chosen defensive investments). However, this is less sophisticated than a fully game-theoretic framework, since for example, in Brown et al. (2005), the attacker is assumed to be unaware even of the defender options when the defender chooses to keep the defenses secret, while a typical endogenous model usually assumes only that the attacker is unaware of the specific choice made by the defender, and has full knowledge of the defender’s options and preferences. This intermediate level of modeling and analysis has proven to be useful in practice, and avoids both the (potentially unrealistic) sophistication and idealizations of game theory, and the extreme simplicity (and concomitant limitations) of the Risk = Threat × Vulnerability × Consequence approach.

Thus, modeling an intelligent attacker’s intelligent (adaptive) behavior can lead to different recommendations and risk estimates from traditional risk analysis. The lesson is not that risk analysis cannot be used at all. In fact, once optimal defense and attack strategies have been determined, it may then be possible to represent them by event trees or other risk-analysis models. However, risk analysis by itself is not sufficient to represent and solve the key decision problems that defenders confront.

4. SUMMARY OF NON-GAME-THEORETIC MODELS FOR ALLOCATING DEFENSIVE RESOURCES

The preceding discussion suggests that the concepts of “Threat” and “Vulnerability” as static numbers that experts can estimate for use in calculating risk may be inadequate when risks result from the actions of intelligent actors. Defining “Threat” as “Probability of an attack in a stated
period of time” begs the key question of how an attacker makes and revises
attack decisions in response to intelligence about the defender’s actions and
beliefs. In fact, the use of static threat estimates can even be self-defeating, if
attackers use intelligence about the defender’s own threat estimates to help
them decide where and when to attack (for example, choosing to attack
targets that the defender believed were not at risk). Conversely, the mere fact
of defending a target can make it more attractive to attackers (for example,
by increasing the “prestige value” of a successful attack), and thereby make
it more likely to be attacked.

Similarly, the probability that an attack succeeds if it is attempted may
depend on the attacker’s knowledge, contingency plans, and ability to
dynamically adapt when obstacles are encountered. The information needed
to predict what an intelligent attacker will do and how likely it is to succeed
must include such contingency plans, and therefore is better represented by
game theory than by traditional risk and reliability analysis. Thus, attempting
to assess vulnerability by standard techniques of risk analysis (e.g., event
trees or fault trees), without explicit analysis of the attacker’s best responses
to candidate defenses, can produce misleading risk estimates and poor risk-
management recommendations.

An alternative approach (as illustrated, for example, in Brown et al.,
2006) is to avoid calculation of Threat, Vulnerability, and Consequence in
isolation, and to concentrate instead on optimizing allocation of defensive
resources, assuming that attackers will then adopt “best responses” to those
allocations. This leads to hierarchical optimization as a framework for
guiding risk-management decisions, with a game-theoretic flavor (even if
not fully endogenous). The examples given in Brown et al. (2006) suggest
that this approach is satisfactory in many applications.

The chapters in this book employ varying levels of game-theoretic
sophistication. Some of the chapters adopt the spirit of Brown et al. (2006),
and provide game-theoretic problem formulations, without necessarily
investigating equilibrium solutions. Others exploit the classical game-
theoretic approach more fully. Finally, some chapters could be characterized
as implementations of “conversational” game theory—thinking carefully
about attacker goals and motivations without actually computing best
responses to attacker actions.

5. OVERVIEW OF THE BOOK

The following chapters offer a variety of models and frameworks for
more realistic analysis and prevention of intentional attacks. Chapter 2 (by
Guikema) provides a state-of-the-art review of the use of game theory in
reliability. It focuses mainly on combining game theory with reliability to model attack-defense situations. The adequacy of game theory in this context is critically discussed, and several non-game theoretic approaches for modeling reliability problems in the presence of intelligent attackers are also reviewed.

Chapter 3 (by Levitin) considers an attack-defense model in which the attacker attempts to maximize the expected damage to a complex multi-state series-parallel system. The defender uses both separation and protection of system elements, as well as deployment of false targets, to reduce the risk of a successful attack. An optimization algorithm is suggested based on assessing the losses due to reduction in system performance, and applying a genetic algorithm for determining optimal defense strategies.

Chapter 4 (by Hausken et al.) considers a game where the defender of a particular asset plays against one active player (a terrorist) and one passive player (nature). The defender can deploy defenses that protect against: (a) terrorist attack only; (b) natural disaster only; or (c) both. A variety of simultaneous and sequential decision situations are considered, with the defender seeking to maximize expected utility.

Chapter 5 (by Azaiez) emphasizes the strategic role of information in a model of attack-defense strategies. The attacker has only partial information about the survivability of the targeted system. The defender, who moves first, attempts to deter the attack through modifications or improvements of the targeted system, by making the chance of a successful attack “sufficiently” low and/or the attacker’s estimate of that chance “sufficiently” unreliable. Intermediate levels of partial information are also discussed.

Chapter 6 (by Gaver et al.) deals with some specific games where the defender (a counter-terrorist) seeks to detect a hostile individual (terrorist) early on and neutralize it. The attacker invests time to identify an “attractive” target (e.g., a crowd of people). If not neutralized, the attacker attacks the first identified “attractive” target. The defender faces two types of errors: namely, false identification of the hostile individual within a population of non-hostile individuals; and failure to identify the hostile individual before an attack is launched. The probability of correct identification increases with the observation time of the defender, but of course this increases the probability that an attack is launched before the hostile individual is identified.

Chapter 7 (by Paté-Cornell et al.) applies a combination of game theory and probabilistic risk analysis to investigate links among the actions of different parties (e.g., the government on one side, and potential terrorists on the other) and the resulting state of a system. The results involve the probability of different outcomes (e.g., the chances of different attack scenarios) and the risks of various failure types.
Chapter 8 (by Cox) surveys recent developments in designing resilient networks to protect telecommunications infrastructure against deliberate attacks. Resilient networks are designed to provide enough flexibility, redundancy, and rapid recovery capability that any attempt to disrupt traffic results in automatic re-routing of traffic and uninterrupted service. The focus is on design of network topologies and methods of traffic routing and switching to make communications among nodes resilient to both link and node failures.

Chapter 9 (by Kanturska et al.) considers how to improve the reliability of transportation networks through multi-path routing and link defense in a game-theoretic setting. An illustration of an attacker-defender model shows the importance of mixed route strategies, and illustrates how critical links in the network can be identified. The approach is extended to a defender-attacker-defender game to investigate the optimal set of infrastructure to protect in advance. Varying degrees of visibility of the protection are considered; the results show that the visibility of the protective measures significantly affects their expected benefit.

In summary, the theoretical and applied work in the following chapters shows how defense against an intelligent, adaptive attacker can be designed rationally within the frameworks provided by attacker-defender models. Alternative approaches (both game-theoretic and non game-theoretic) are addressed briefly, but the main message is that attacker-defender models are now well enough developed to provide a new generation of infrastructure-defense planning and optimization algorithms that can substantially improve on earlier approaches.

REFERENCES


1. Why Both Game Theory and Reliability Theory Are Important


This page intentionally left blank
Chapter 2

GAME THEORY MODELS OF INTELLIGENT ACTORS IN RELIABILITY ANALYSIS
An Overview of the State of the Art

Seth D. Guikema

Abstract: Much research has been done to develop game theoretic methods for modeling intelligent actors in reliability analysis, especially in the context of modeling intentional attacks against systems. This work has provided strong, and at times unexpected, insights into how to best defend systems against intelligent attacks. General principles of how to best defend systems of specific types against intelligent attacks are emerging that can help system managers allocate resources to best defend their systems. However, there is still work to be done to improve these models. The current game theoretic models for intelligent threats are based on a number of assumptions, and the implications and appropriateness of these assumptions in different situations have not been fully explored. Further research to better characterize how well these assumptions match reality and what impacts changing these assumptions would have on both modeling difficulty and the suggested decisions would be fruitful.

Key words: game theory; risk analysis; reliability; terrorism; irrationality; utility functions; sensitivity analysis

1. INTRODUCTION

As discussed in the first chapter of this book, game theory provides a powerful framework for modeling strategic interactions between those defending a system and those attempting to harm that system. Game theory has also been used in modeling the reliability of complex systems and for suggesting the optimal allocation of defensive resources. In this case, the analysis builds from the usual definition of reliability as the probability of successful operation of a system under specified conditions for a defined
period of time to incorporate the effects of intelligent agents on system reliability. The usual definition of reliability still holds, but the nature of the initiating events that may lead to system failure and the types of risk management measures to be considered change substantially. However, the use of game theory as the basis for modeling system reliability in the face of intelligent threats is not uniformly accepted.

This chapter first provides a general overview of the use of game theory in modeling terrorist-defender interactions. This forms the historical and theoretical backdrop against which more recent advances in the use of game theory in reliability analysis have developed. The chapter then reviews the use of game theory in reliability engineering. A discussion of foundational issues and assumptions in game theory and an overview of alternate approaches follow the review of the use of game theory. Finally, the current state of the art in the use of game theory in reliability analysis is summarized.

2. GENERAL OVERVIEW OF GAME THEORY IN MODELING TERRORIST-DEFENDER INTERACTIONS

While there are a number of situations in which strategic interactions are of interest in reliability analysis such as modeling design teams, modeling vandalism, etc., much of the current interest in the use of game theory in risk and reliability analysis stems from increased concerns about terrorist attacks on western interests. Because the use of game theory in reliability analysis has built from game theoretic analyses of terrorist threats, it is important to summarize this past work as a basis for discussing the use of game theory in reliability analysis.

Game theoretic work on modeling terrorist actions has focused on modeling high-level strategic questions such as the effects of different national policies intended to reduce the likelihood or impact of terrorist attacks (Sandler, 2003; Sandler et al., 1983; Sandler and Scott, 1987; Enders and Sandler, 1993, 1995; Rosendorff and Sandler, 2004). Among other conclusions, this past work has suggested that vigorous, national anti-terrorism campaigns may induce terrorists to switch to more spectacular attacks rather than attacks that are less costly to the defender (Rosendorff and Sandler, 2004), particularly if anti-terrorism policy depends primarily on deterrence (Frey and Luechinger, 2002). Past game theoretic and related work also suggests that there is a substitution effect in which terrorists switch from one form of attack (e.g., hijackings) to another form of attack (e.g., assassinations) in response to national policies deterring a specific type
of action (e.g., Sandler and Scott, 1987; Sandler and Enders, 2004), and that
deterrence and pre-emption are both generally under-utilized for global
terrorism (Sandler and Siqueira, 2006). Other past work has focused on
modeling the cycles observed in terrorist activity on the basis of leader-
follower games (Faria, 2003) and system dynamics models (Udwadia et al.,
2006). Finally, one modeling effort has combined probabilistic risk analysis,
Bayesian influence diagrams, and basic game theory for analyzing high-
level, schematic terrorist risk (Paté-Cornell and Guikema, 2002). While this
model is more closely related to the use of game theory in reliability analysis
than the more global terrorist game theoretic models, it still focused on a
high-level analysis rather than the detailed analysis of system protection
options of interest in reliability analysis.

While the focus of these models is not on the detailed reliability analysis
central to this book, past game theoretic models for terrorism do provide the
backdrop against which game theoretic reliability analysis models are being
developed. They also share three key characteristics. First, past game
theoretic models for terrorist activity have assumed that both attackers and
defenders follow the rational actor paradigm. That is, they assume that
attackers and defenders act to maximize their own utility, given what they
know about their opponent’s objectives and knowledge. Second, past and
current game theoretic models explicitly model the strategic interactions
between attackers and defenders. That is, the response of one party to the
actions of the others is forecast based on a predictive model of behavior.
Other modeling approaches exist, and these will be summarized later in this
chapter. Finally, most past game theoretic analyses have treated attacker
behavior as deterministic with given targets being deterministically attacked
based on game theoretic equilibriums. This does not need to be the case, and
both mixed-strategy equilibriums and variations on standard game theory
can be used to model stochastic strategies. The past work using game theory
to model terrorism issues provides a basis on which the use of game theory
in reliability analysis has been built, and similar assumptions are often made
in game theory models in reliability analysis. The role and impacts of these
assumptions in using game theory for reliability analysis will be discussed
later in this chapter.

3. THE USE OF GAME THEORY IN RELIABILITY
ANALYSIS

Until relatively recently, game theory was not a major component of
reliability analysis. However, in the last few years, analysts have developed
game theoretic models for both examining the impacts of strategic
interaction on the reliability of systems as well as initial methods for optimizing system reliability in the face of intelligent threats. These models have progressed from relatively simple, one-shot game theoretic models to models for repeated strategic interactions. The insights provided by the models have correspondingly grown in sophistication. However, there is still work to be done in improving and testing game theoretic models in reliability analysis.

Early work in using game theory in reliability analysis focused on linking probabilistic risk analysis models with basic game theoretic models to incorporate the effects of strategic interactions into reliability analysis. For example, Hausken (2002) develops general models that treat system reliability as a public good and incorporate game theory into reliability analysis. These models focus on the case in which different players value system reliability differently and conflict arises in resource allocation decisions.

In Hausken’s model, each component of a system is matched with an individual player, and the reliability of component i, \( p(x_i,s_i) \), is assumed to depend on both that component’s player’s strategy \( s_i \) (e.g., effort level) and on the technical characteristics of the component \( x_i \) (Hausken, 2002). The reliability of the system components determines the overall system reliability \( p(x,s) \). Hausken uses a multi-attribute utility function to model a player’s utility as a function of their component’s reliability, the system’s reliability, their strategy, the technical state of their component, and any reimbursements and costs to the player. The utility function is assumed to be exogenously given.

Based on his basic model, Hausken (2002) then addresses a number of examples. The first example is of a series system. In particular, Hausken examines a stylized, perfectly circular island protected by dikes. Each citizen must individually decide whether or not to build and then maintain their dike, incurring a personal cost. The entire island floods (deterministically) if any individual does not build and maintain their section of the dike. If the marginal benefit of a perfectly effective dike system outweighs the cost of building the dikes, there are two Nash equilibriums. In the first, no dikes are built, and all players suffer loss due to a flood. In the second equilibrium, all players build and maintain their dikes, making all players better off. Note that the outcomes are assumed to occur deterministically given the actions of the individuals. The second of Hausken’s examples involves a purely parallel system. In the example, each citizen of a fictional country is responsible for operating an anti-ICBM interceptor site, but operating the site is costly. If any individual shoots down the incoming ICBM all players benefit. The equilibriums in this case involve either no-one shooting down the ICBM or a single player shooting down the ICBM at the cost of
obtaining the lowest utility. The other players effectively become free riders at the expense of the single shooter. Note that this model does not consider uncertainty in either the accuracy of the ICBM or the interceptor. The third example is one of mutual assistance among private companies. Each company benefits if other companies agree to provide mutual assistance, but the temptation to be the hold-out and benefit without agreeing to provide costly assistance is strong. There are multiple equilibriums to this game, depending on the relative costs and benefits of providing and receiving assistance.

Hausken’s work is significant because it gives the first organized linkage in the reliability and risk analysis literature between reliability analysis based on probabilistic risk analysis and game theory in which system reliability is treated as a public good. While the systems addressed (series, parallel, and summation) are simple from a reliability analysis point of view, the linkage with game theory highlights the importance of individual decision-making in many situations. Since the work of Hausken, a number of other researchers have expanded on this problem, especially in analyzing risk to technical systems due to possible terrorist attacks.

Major (2002) presents a relatively simple game theoretic analysis of target protection decisions. A fundamental assumption throughout much of the paper is that the attackers and defenders value the same thing (e.g., economic losses or lives lost), leading to a zero-sum game. This leads Major to concentrate on minimax defense strategies in which the defender minimizes their maximum possible loss. In a zero-sum game with symmetric and diametrically opposite utility functions, this leads to the optimal defensive strategy, but, as Major (2002) acknowledges, this strategy is generally not optimal when attackers and defenders value different things.

As discussed earlier in this chapter, Paté-Cornell and Guikema (2002) presents a model linking probabilistic risk analysis, influence diagrams, and game theory for analyzing terrorist risk. While the focus was not strictly on reliability analysis for an individual system, the results are applicable to reliability analysis problems. Paté-Cornell and Guikema (2002) developed an influence diagram to model U.S. anti-terrorism decisions and a separate influence diagram to model terrorists’ decisions of what target, if any, to attack with what weapon. These two detailed influence diagrams were linked with a relatively simple game theoretic model. However, Paté-Cornell and Guikema (2002) modified traditional game theoretic equilibrium concepts and assumed that terrorists would choose attacks stochastically, with attack probabilities proportional to the expected utility of each attack to them. While this was a fairly arbitrary assumption in the original work, it does correspond to a version of bounded rationality in which players choose
strategies with probabilities proportional to the utilities of the strategies (see Rubinstein, 1997).

In work that is similar in spirit to the approach used by Paté-Cornell and Guikema, Koller and Milch (2003) developed “multi-agent influence diagrams” or MAIDS to capture dependencies between decisions as well as dependencies between uncertainties in multi-player games. The focus of Koller and Milch (2003) was on more general modeling issues, not reliability analysis. However, the approach may prove particularly useful for reliability analysts dealing with large-scale systems because it offers the promise of increased computational efficiency relative to standard methods for solving game theoretic problems.

Bier and her collaborators published the first papers combining game theory and reliability analysis that dealt directly with allocating protective resources among the components of a technical system (Bier and Abhichandani, 2004; Bier et al., 2005). Their work builds from the approach of Hausken (2002) but focuses on a more detailed reliability model of the system. Bier et al. (2005) assume that an attacker acts rationally to maximize the expected amount of damage from an attack, that attacks on different system components succeed or fail independently of one another, and that the timing of failures is not important. Bier et al. (2005) examine the allocation of resources to protect the components of both series and parallel systems assuming both perfect attacker knowledge of defensive actions and no attacker knowledge of defensive actions. The results from Bier et al. (2005) show, for example, that for a single attack against a series system when the attacker has perfect knowledge of defensive actions, the optimal defensive strategy is to try to equalize the probability of failure of each of the components. However, if the same attacker with perfect information can attack more than once, the optimal allocation also depends on the relative marginal costs of decreasing the probability of failure for each of the components. For parallel systems, which are easier than series systems to defend in many cases, the optimal allocation of resources depends the cost-effectiveness of defensive investments, the available budget, and the probability of an attack against the system. In both the series and parallel cases, the results of Bier et al. (2005) suggest that decreasing the probability of system failure is more difficult if the attacker has knowledge of the system defenses than if they do not.

Zhuang and Bier (2007) build from the earlier work of Bier and Abhichandani (2004) and Bier et al. (2005) to model decisions of how best to protect against both natural disasters and terrorism simultaneously. Unlike most earlier work except for Major (2002), Zhuang and Bier (2007) modeled continuous attacker effort rather than discrete attack/no attack decisions. This yields a more realistic model for the many situations in which attackers
can exert differing amounts of effort and resources (money, weaponry, etc.) to attack a system. The results of Zhuang and Bier (2007) suggest that in some cases, increasing the stringency of defensive measures can lead to *increases* in attacker effort rather than decreases in attacker effort if the attractiveness of the target to the attacker is high enough. This, in turn, affects the attractiveness of investments in protecting against natural hazards.

Azaiez and Bier (2007) develop a game theoretic model for guiding the allocation of resources in protecting a series, parallel, or more general system. They assume that the defender’s goal is to make attacks as costly as possible to the attacker. They also assume that increases in component defense increase the cost of an attack but do not decrease the probability of an attack being successful. This is a reasonable proxy for the full problem of deterring attacks in many situations, especially in situations in which the attacker has tight resource constraints. In such a situation, increasing the cost of attacks could lead to the cost of attacks exceeding the attacker’s available resources.

In developing their model, Azaiez and Bier (2007) assume that each component can be attacked at most once, that the attacker stops attacking only if either (i) the system is disabled or (ii) they realize that they cannot disable the system within their resource constraints, and that the attacker has perfect knowledge of the system defense. For this type of attack, the model suggests that for a series system, the attacker should attack the weakest link first, but for a parallel system, the attacker should attack the component with the lowest ratio of attack cost to probability of surviving the attack. The result for the series system is intuitive. The attacker wishes to disable the system with the fewest possible attacks, so he or she attacks the weakest link first. On the other hand, the result for the parallel system at first may seem counterintuitive, but it serves to highlight the ability of game theoretic models to lead to non-intuitive but logical insights into system defense. For a parallel system, the attacker knows they will need to disable all of the components to disable the system. If they started with a low-cost attack with a relatively high probability of success, they may later be faced with failing in attacking a high-cost, low probability of success component. They would rather know as soon as possible if they will not be able to disable the system so that they do not waste resources on easier attacks early in the series of attacks only to fail later in a high-cost attack. This would lead them to attack the component with the lowest ratio of attack cost to probability of surviving the attack first, yielding an indication of whether or not they will be able to disable the system before they expend resources on attacks that are more likely to succeed.
In solving the defender’s resource allocation problem, Azaiez and Bier (2007) assume that the cost of attacks increases linearly with defensive allocations. This resource allocation problem leads, for general situations, to an optimization problem that can be solved as a series of nested linear programming problems. Azaiez and Bier (2007) simplify this problem by assuming that the cost-effectiveness of allocations is identical for all components. With this assumption, the solution for a series system is to first order the list of components in terms of increasing ratio of attack cost to probability of attack success. Then, starting at the top of the list, allocate resources to the first component. Once its ratio equals that of the second highest component, the defender should then allocate resources to both components such that their ratios remain equal. This process continues down the list until the entire budget is used. This is a fairly intuitive defensive strategy involving protecting those components most likely to lead to system failure first.

The solution for a parallel system suggests that the defender allocate resources to the component that is least likely be compromised first. Recall that in a parallel system only one component needs to work for the system to work. It then makes sense for the component with the highest ratio of attack cost to probability of surviving the attack to be reinforced first. Once this component becomes equally attractive to another component, meaning their ratios are the same, resources are allocated to both components. In this manner, the defender maximizes the probability of the system surviving the attack. Azaiez and Bier (2007) also discusses solutions for more general combined series-parallel systems, but the results for the series and parallel systems individually serve to illustrate the main results.

Azaiez and Bier (2007) also highlight fruitful areas for future research. They suggest that explicitly including an attacker budget in the model could make the model more realistic. While it would be difficult to know what this budget is in any given situation, one could treat the budget level parametrically, solving the problem for a range of budgets. This would give an indication of the appropriateness of the defender’s budget level and of the impacts of attacker budget limits. Azaiez and Bier (2007) also suggest that models incorporating imperfect attacker information would be useful. This too may represent a wider range of real scenarios, but the modeling effort becomes substantially more difficult. As suggested by Azaiez and Bier (2007), probing attacks in which the attacker iteratively attacks components in order to learn about system defenses could be modeled as a Bayesian learning process. Appropriate non-informative priors could be updated with observed attack results. Finally, Azaieiz and Bier (2007) suggest that their model could be made more general by allowing defensive allocations to decrease the probability of attack success in addition to increasing the cost of
the attack. This would be particularly valuable for problems in which the cost of an attack is so low as to not be a deterrent. Azaiez and Bier (2007) suggest that hacker attacks against a computer network may have this characteristic. Overall, models like that of Azaiez and Bier (2007) provide strong insights into general defensive strategies, and further refinements of the type they suggest may strengthen the applicability of these types of models in specific situations.

Kardes (2005) builds from the previous work in combining game theory with reliability analysis to develop a new approach for allocating defensive resources that is robust against uncertainty in both the attackers’ adaptive strategies and the attackers’ payoffs (utilities). This approach offers a promising direction for dealing with some of the challenges inherent in using game theoretic methods in reliability analysis, challenges that are discussed on the next section of this chapter.

4. CLASSICAL CRITIQUES OF GAME THEORY

As with all modeling approaches, game theory is based on a number of assumptions that may or may not be reasonable approximations of reality, depending on the circumstances in which the model is applied. When applied in a setting in which the assumptions are justifiable, game theory provides a powerful tool for analyzing the interactions between an intelligent attacker and an intelligent defender as the work discussed above has shown. However, in using models based on game theory to draw inferences about good defensive strategies, care should be taken to ensure that a reasoned consideration of the assumptions underlying the model suggests that they are an appropriate approximation to reality.

There are three fundamental assumptions of game theory that have drawn criticism from researchers in a number of fields, especially cognitive psychology and philosophy. These are the assumptions of instrumental rationality, common knowledge of rationality, and knowledge of the rules of the game. After these assumptions are discussed, issues of uncertainty in the parameters of a game theory model for system defense are briefly discussed.

4.1 Assumption of instrumental rationality

Game theory, in the form that it is most often used, is based on the assumption of instrumental rationality. This means that each player in the game is assumed to maximize their own utility in accordance with the axioms of subjective expected utility (SEU), and equilibrium(s) between the players of the appropriate sort for the given game are found and taken to be
the outcome of the game. With the exception of Paté-Cornell and Guikema (2002) and Kardes (2005), all of the game theoretic models for reliability analysis problems discussed in the previous section have relied on the assumption of instrumental rationality.

The assumption of instrumental rationality does offer advantages over other approaches. In particular, assuming instrumental rationality leads to strong, analytical insights that would not generally be possible with other approaches. For example, in the models of Bier et al. (2005), Zhuang and Bier (2007), and Azaiez and Bier (2007), the assumption that the defender chose attacks rationally allowed the optimal defensive actions to be determined analytically for specific but useful cases of system architectures. This, in turn, leads to insights into more general defensive strategies that would not be possible (or at least be substantially more difficult to obtain) with models requiring numeric solutions as some non-rationality models do.

Not only is rationality a convenient assumption, it is also a common assumption in a wide variety of fields and a reasonable assumption in some classes of problems. When individuals or groups choose actions in order to maximize an objective (utility) function, or at least act as if they do, they are acting rationally. The assumption of rationality is widely used in microeconomics, and it forms the basis of normative decision analysis. In many situations it describes how people want to behave, and it may often also be a reasonable approximation of how people actually do behave. However, the assumption of rationality is not universally accepted as a reasonable descriptive model of behavior, either for general members of society or for potential attackers such as terrorists.

Research in a number of areas has shown that individuals do violate the axioms of SEU in some situations. For example, spontaneity does not fit within the rational decision making framework (Elster, 1985). This restricts game theory to modeling situations with thought-out, as opposed to spontaneous, attacks, but this at least seems to not be a particularly large restriction. Serious, large-scale attacks would seldom be based on spontaneity. However, as reported in Heap and Varoufakis (1995), Hollis (1987, 1992) argues that honor, a concept likely of importance to some classes of adversaries, may not be amenable to inclusion in a utility function. Perhaps most famously, the Allais and Ellsberg paradoxes (Allais, 1953; Ellsberg, 1961) show empirically that test subjects do not always follow SEU. Work in prospect theory augments this by showing that individual’s utility functions are often frame-dependent (Kahneman and Tversky, 1979). While these frame-dependent utility functions could be included in SEU, this is not typically done. In a similar manner, lexicographic utility functions can be used to represent situations where a player has a vector of probability distributions on the actions of the other players (Blume et al., 1991a, 1991b).
This approach offers promise for incorporating subjective beliefs about opponents’ actions into game theory without relying directly on traditional equilibrium concepts, and it could be done in conjunction with game theory based on the subjective Bayesian view of probability as in Kadane and Larkey (1982). There are also a number of other extensions to game theory to account for deviations from rationality in general game theory problems (e.g., March and Olsen, 1976; March, 1978; Rosenthal, 1989; Rabin, 1993; Chen et al., 1997; Osborne and Rubinstein, 1998; Camerer and Ho, 1999), but these also have not found wide-spread use in analyzing the allocation of resources to defend systems against intelligent attacks.

Within the more specific context of modeling terrorist actions, the rationality of attackers is still subject to debate within the psychological literature. For example, Ruby (2002) reviews the literature pertaining to the rationality of terrorists. According to Ruby, the two main views on what leads people to become terrorists and initiate attacks are the personality defects model and the social learning theory model. The first of these, the personality defects model, posits that terrorists have pathologic personalities, meaning that terrorism is not a means to an end. Post (1984, 1986) and Kaplan (1981) give earlier work in this area. If this is an accurate model describing why individuals become terrorists, it would suggest that rational choice models may not be good representations of terrorist behavior. Inherent in the rational choice model is an understanding that actions are a means to an end, not a result of pathologic personalities. On the other hand, the social learning theory model leads one to much different conclusions.

Those supporting the social learning theory view of the root causes of terrorism argue that the conversion to terrorism and terrorist actions once an individual is converted result from societal influences that form the foundation of functional tendencies (e.g., Cooper, 1973). More recently, Crenshaw (1992, 2000) has argued in favor of this view of terrorism. If this is a correct descriptive model of terrorists and the drivers for their actions, terrorism is a means to an end. This would mean that rationality can be used as an appropriate model of terrorist behavior as long as the terrorists’ utility functions can be estimated.

In summarizing the state of the psychology literature on the causes of terrorism and the rationality or lack thereof of terrorists, Ruby (2002) concludes that there is very little empirical evidence available on the rationality of terrorists but that it does seem that terrorists are more likely than not rational in their behavior. However, Ruby (2002) cautions that the lack of empirical evidence would make it very difficult to reject a hypothesis that terrorists are not rational if the question were approached from the traditional (frequentist) statistical perspective.
Sageman (2004) provides a different perspective on the root causes of terrorism and the drivers of the behavior of potential attackers based on a combination of interactions with future members of salafi groups and original data gathered on approximately 170 terrorists. Sageman (2004) paints a picture in which group effects rather than individual rational decisions are the root causes of an individual joining a salafi terrorist organization such as Al-Qaeda. However, Sageman (2004) portrays attacks by salafi groups as being planned to achieve a specific goal, offering support for the assumption of instrumental rationality. However, these goals may change over time, and we may not fully understand what the goals of any particular group are.

While there is still debate in the psychological literature about the rationality of terrorists, the literature overall suggests that attackers do act to try to achieve specific objectives in many situations. This suggests that rationality may be a reasonable approximation as a descriptive model of attacker behavior in many situations. However, exploring the robustness of optimal defensive strategies to deviations from rationality in the attacker behavioral model would be interesting research that could help to shed light on the practical importance of this assumption.

4.2 Common knowledge of rationality (and consistency of beliefs)

If rationality is accepted as being an appropriate basis for a descriptive model of attacker actions, we must next examine assumptions about what each player knows about the other player’s utility function. Most applications of game theory assume common knowledge of rationality (CKR) (see, for example, Heap and Varoufakis, 1995). This means that each player knows that the other players are rational, they know that the others know they are rational, they know that the others know that they know they are rational, ad infinitum. It does not mean that any player knows the other players’ preferences, only that they are rational. Strictly speaking, the infinite progression poses a difficulty for belief formulation about other rational players’ preferences and information without further assumptions. A player cannot directly formulate beliefs about other players through observation and updating according to Bayes’ theorem because the other players’ actions directly depend on the beliefs being formulated.

One common way around this difficulty is to assume that the players’ beliefs are consistent in the sense that any two rational players with the same information will come to the same thought process. Perhaps the most well-known and succinct statement of this assumption is Harsanyi’s statement that two rational individuals holding the same information must draw the
same inferences and come to the same conclusion. This requires that the
prior beliefs formulated in accordance with Savage’s view of probability as a
subjective degree of belief (Savage, 1972) of the two players be consistent
with each other (e.g., they must assign non-zero probability to all events that
either player sees as plausible).

Aumann provides notable support for this subjective probability based
position within game theory by appealing to the idea of an exchange
between players over time (Aumann, 1976; Aumann and Hart, 1992). If two
players hold different beliefs about the probability of an event, they can
make a bet about the occurrence of the event that both players are willing to
accept. But the willingness of their opponent to make the bet is informative
to a player who will then (assuming he believes his opponent is rational)
revise his beliefs more towards his opponent’s beliefs in through Bayesian
updating. His opponent will also revise her beliefs. If this series of bets
continues long enough, the two players will reach a point at which they hold
the same beliefs and will be unable to conclude further bets. While this may
be reasonable for a repeated game with stationary information, there may be
difficulties that arise in assessing risk due to terrorist attacks.

Attacks against systems consist of a series of interactions (assuming
repeated attacks) between the attacker(s) and the defender(s). However,
strategies of the two groups change relatively rapidly, each player may
purposely attempt to hide information from their adversary, and major
interactions such as attacks and attempted attacks occur infrequently relative
to the frequency with which strategy and information changes may occur. It
seems problematic to apply Aumann’s recursive dialogue argument to this
situation as a basis for claiming consistency of beliefs. It seems perhaps
more plausible to assume that the beliefs of attackers and defenders about
the preferences and information of their adversary may be inconsistent. For
example, this would mean the defender may believe the attacker is operating
according to one objective function (e.g., maximize economic damage)
while the attacker is actually operating according to a different objective
function (e.g., maximize media coverage). It is difficult in many cases to
know what the objectives of attackers are.

Lack of consistently aligned beliefs in attacker-defender problems does
not invalidate the usefulness of the game theoretic framework for thinking
about these problems. Rather, one could argue that what is needed is a
combination of better knowledge about attacker objectives and attackers’
knowledge of the defender’s objectives together with more complete
sensitivity analyses for objective functions for both players. Gathering better
knowledge about attacker objectives and about what the attackers know
about the defender’s objectives would help to reduce the asymmetries in
knowledge. If this is coupled with sensitivity analysis to examine possible
alternate objective functions in cases where knowledge is incomplete, it could increase the confidence that decision-makers and policy-makers can place in the results of game theoretic models. This approach has not been widely adopted in game theoretic models for reliability analysis for intelligent threats, but it is a relatively straight-forward extension of existing models, at least in theory.

4.3 Knowledge of the “rules” of the game

In addition to assuming that players are instrumentally rational and have consistent beliefs, game theory is based on the assumption that the players know the “rules” of the game. That is, game theory assumes that the players know the set of actions available to each player and how each possible set of actions affects their and their opponents’ utilities. This assumption is potentially more problematic than the first two.

One difficulty is that game theory assumes that the payoffs to the different players, reflected in utility functions, are known at least probabilistically over a defined space of possible utility functions. As discussed above, in examining the available literature, Ruby (2002) concluded that there was little empirical evidence available about the causes of terrorism, the current motivations of terrorists, or even the rationality of terrorists. Furthermore, the information that is available suggests that different groups have much different motivations. Some religious groups such as Aum Shinrikyo seek to turn their apocalyptic visions into reality while others focus on bringing down a secular government (e.g., Juergensmeyer, 2003; Schbley, 2003). Other types of groups may focus on specific issues such as abortion or animal rights (e.g., Leader and Probst, 2003). These differences in goals highlight the need to at least treat different groups differently in terms of modeling their goals and objectives with a utility function in using game theory.

We must also be careful to ascertain whether or not we understand our adversaries well enough to compose a utility function that is good enough to form the basis for an analysis. Byman (2003) argues that at least for one important adversarial group, Al-Qaeda, the objectives of the group are complex and non-stationary and that we do not fully understand these objectives. This makes formulating general utility functions useful at different times for different problems difficult. Instead, an analyst may wish to use approximations to these utility functions, fully acknowledging that the utility functions are just that – an approximation to an unknown utility function – and that the recommended course of action may depend to some degree on the assumed utility function. Again, assessing the sensitivity of the
4.4 Uncertainty about model parameters

One of the criticisms of game theory that is more specific to attacker-defender situations deals with the ability of analysts (and by extension defenders) to know the needed model parameters. In particular, how can the analyst (or defender) know the attacker’s utility function and what the attacker thinks the defender’s utility function is? A standard game theoretic approach is to place a probability density function over all possible attacker utility functions and to use a probability density function to represent the attacker’s beliefs about the defender’s utility function. Similarly, the attacker’s and defender’s beliefs about the probability of an attack being successful as a function of defensive resource allocations could be represented by probability distributions. Taking a purely subjectivist Bayesian approach, this is not a problem. The attacker and defender each use probability density functions that best represents their beliefs. However, there is no guarantee that these beliefs would be consistent with each other or over time or that they would represent the actual utility functions or long-run rates of attack success. If the results from these models are to be used in important managerial or public policy decision-making, how should these Bayesian probabilities be treated? Modeling efforts that explore the robustness of suggested defensive strategies to changes in assumed model input values would be useful.

5. NON-GAME THEORETIC METHODS FOR RELIABILITY ANALYSIS FOR INTELLIGENT THREATS

The methods discussed above depend on using game theory as a behavioral model of attacker behavior. While these types of models can provide strong insights into general defensive strategies, not all reliability analysts adopt the game theoretic approach. While not the focus of this book or this chapter, an introduction to alternate methods is helpful. One approach that some have suggested is to base the estimates of attacker actions on expert opinion rather than behavioral models (e.g., Garrick et al., 2004). With this approach, the probability of an attack on each of the components of a system within a specified time period would be assessed with one or more experts. Possible advantages of this approach are that it avoids the assumptions that underlie any type of behavioral model, it can lead to a full
probability density function for the probability of an attack on each component\(^1\), and it permits issues not included in many behavioral models to be included. One disadvantage of this approach is that it is entirely dependent on the accuracy of the expert(s) used in the assessment, where accuracy here refers to how well their assessed probabilities match the future frequency of attacks on the different system components. It may be difficult to find appropriate experts, especially for problems in the classified realm.

A second disadvantage of the expert-based approach is that it does not lead to models that incorporate the strategic interactions between attackers and defenders. Instead, this approach leads to either a static snapshot of attack probabilities or a vector of conditional attack probabilities representing attacker behavior over time. However, assessing attacker behavior for every possible defender action would likely be a prohibitively difficult task in most real modeling situations.

Another approach that has been suggested is to avoid dealing with attacker behavior directly by choosing to protect the highest-valued system components first. Notable examples of this approach are Apostolakis and Lemon (2005) and Michaud and Apostolakis (2006). With the approach, the defender estimates the value of each system component, perhaps based on a multi-attribute utility function as suggested by Apostolakis and Lemon (2005). The defender then allocates money to the most highly valued system components. If defensive actions are carried out in a cost-effective manner and were effective in reducing the probability and/or severity of attacks, this screening approach would lead to a minimax solution in which the maximum possible loss of value to the defender was minimized. Moreover, if the situation were modeled as a zero-sum game, the minimax solution is also the solution to the zero-sum game as in Major (2002). The strength of this approach is that it does not depend on either behavioral models or expert assessments of attacker behavior, both of which are potentially problematic. However, this approach does not, in general, lead to an optimal defensive strategy, and it does not model the strategic interaction between the attacker and the defender.

---

\(^1\) Game theoretic and other behavioral models can in theory lead to a probabilistic description of attacker actions as well. As a simple example, mixed strategies could be considered in standard games. Uncertainty in the parameters of the behavioral models could then be incorporated, leading to estimates of the uncertainty in the mixed strategies. However, this is not commonly done in modeling attacker-defender interactions in reliability analysis.
6. CONCLUDING THOUGHTS

Much research has been done to develop game theoretic methods for modeling intelligent actors in reliability analysis, especially in the context of modeling intentional attacks against systems. This work has provided strong, and at times unexpected, insights into how to best defend systems against intelligent attacks. General principles of how to best defend systems of specific types (e.g., series, parallel, and series-parallel) against intelligent attacks are emerging that can help system managers allocate resources to best defend their systems. There is still work to be done to improve these models. The current game theoretic models for intelligent threats are based on a number of assumptions for which the implications and accuracy have not yet been fully explored. Further research to better characterize how well these assumptions match reality and what impacts changing these assumptions would have on both modeling difficulty and the suggested decisions would be fruitful. The chapters in the remainder of this book begin to explore these issues.

ACKNOWLEDGEMENTS

I would like to thank Russ Garber and two anonymous reviewers for helpful feedback on this chapter. Their efforts have substantially improved the text.

REFERENCES


Kardes, E., *Robust Stochastic Games and Applications to Counter-Terrorism Strategies*, 2005, Center for Risk and Economic Analysis of Terrorism Events, University of Southern California: Los Angeles, CA.


This page intentionally left blank
Chapter 3

OPTIMIZING DEFENSE STRATEGIES FOR COMPLEX MULTI-STATE SYSTEMS

Gregory Levitin

Abstract: This chapter presents a generalized model of damage caused to a complex multi-state series-parallel system by intentional attacks. The model takes into account a defense strategy that presumes both separation and protection of system elements, and also deployment of false targets. Protection importance indices are introduced that can be used for tracing bottlenecks in defense strategy, and for identifying the most important protections. Then a defense strategy optimization methodology is suggested, based on the assumption that the attacker tries to maximize the expected damage of an attack. An optimization algorithm is presented that uses a universal generating function for evaluating the losses caused by system performance reduction, and a genetic algorithm for determining the optimal defense strategy. The role of false targets in the optimal defense strategy is analyzed, and illustrative examples are presented.

Key words: survivability; importance; optimization; multi-state system; separation; protection; false target; attacker’s strategy; defense strategy; universal generating function; genetic algorithm

Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ED</td>
<td>expected damage</td>
</tr>
<tr>
<td>FT</td>
<td>false target</td>
</tr>
<tr>
<td>GA</td>
<td>genetic algorithm</td>
</tr>
<tr>
<td>PG</td>
<td>protection group</td>
</tr>
<tr>
<td>PI</td>
<td>protection importance</td>
</tr>
<tr>
<td>pmf</td>
<td>probability mass function</td>
</tr>
<tr>
<td>u-function</td>
<td>universal generating function</td>
</tr>
</tbody>
</table>
### Definitions

- **element**: lowest-level part of a system, which is characterized by its inherent value, availability, and nominal performance rate, and can have two states: normal operation, and total failure
- **component**: collection of elements with the same functionality connected in parallel
- **protection**: technical or organizational measure aimed at reducing the destruction probability of a group of system elements in case of an attack
- **separation**: action aimed at preventing simultaneous destruction of several elements in the case of a single attack (can be achieved by spatial dispersion, by encapsulating different elements in different protective casings, by use of different power sources etc.)
- **protection group**: group of system elements, that is separated from other elements (and possibly also protected), so that a single external impact destroying elements belonging to a given protection group cannot destroy elements from other groups
- **false target**: object that mimics a protection group, but does not contain any actual elements (so that the total damage caused by destruction of a false target is much lower than the damage caused by destruction of a protection group)
- **performance rate**: quantitative measure of the performance intensity of an element or system (capacity, productivity, processing speed, task completion time, etc.)

### Nomenclature

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \Pr(e) )</td>
<td>probability of event ( e )</td>
</tr>
<tr>
<td>( 1(\cdot) )</td>
<td>unity function: ( 1(\text{TRUE}) = 1, 1(\text{FALSE}) = 0 )</td>
</tr>
<tr>
<td>( \left\lfloor x \right\rfloor )</td>
<td>greatest integer less than or equal to ( x )</td>
</tr>
<tr>
<td>( N )</td>
<td>total number of system components</td>
</tr>
<tr>
<td>( J_n )</td>
<td>number of elements in component ( n )</td>
</tr>
<tr>
<td>( p_{nk} )</td>
<td>availability of element ( k ) in component ( n )</td>
</tr>
<tr>
<td>( x_{nk} )</td>
<td>performance rate of element ( k ) in component ( n ) when it is available</td>
</tr>
<tr>
<td>( M_n )</td>
<td>number of PG’s in component ( n )</td>
</tr>
<tr>
<td>( \Phi_n )</td>
<td>set of elements belonging to component ( n )</td>
</tr>
<tr>
<td>( \Phi_{nm} )</td>
<td>set of elements in component ( n ) belonging to PG ( m )</td>
</tr>
<tr>
<td>(</td>
<td>\Phi_{nm}</td>
</tr>
<tr>
<td>( \gamma )</td>
<td>set of vectors representing the distribution of system elements among PG’s:</td>
</tr>
<tr>
<td></td>
<td>( \gamma = { \gamma_{nj}, 1 \leq n \leq N, 1 \leq j \leq J_n } ), where ( \gamma_{nj} ) is the PG to which element ( j ) in component ( n ) belongs</td>
</tr>
<tr>
<td>( B_n+1 )</td>
<td>number of different types of protection available for component ( n ) (including the option of no protection)</td>
</tr>
<tr>
<td>( F )</td>
<td>number of false targets deployed</td>
</tr>
<tr>
<td>( d )</td>
<td>cost per false target</td>
</tr>
<tr>
<td>( v_n(k) )</td>
<td>expected vulnerability of protection type ( k ) in component ( n ), where ( v_n(0)=1 ) by definition, (depending on the problem formulation, ( v_n(k) ) can be interpreted as the probability of protection type ( k ) being destroyed either in a single attack, or in a series of attacks)</td>
</tr>
<tr>
<td>( o_n(k,y) )</td>
<td>cost of protection type ( k ) for a PG consisting of ( y ) elements in component ( n )</td>
</tr>
<tr>
<td>( \beta_n )</td>
<td>set of vectors of the protection types chosen for the various PG’s: ( \beta = { \beta_{nm},</td>
</tr>
</tbody>
</table>
Nomenclature (continued)

- $O(\beta, \gamma, F)$: cost of defense strategy $\beta, \gamma, F$
- $O^*$: maximum allowable cost of defense strategy
- $\mu(O(\beta, \gamma, F))$: penalized cost of defense strategy (actual cost, in an unconstrained problem, or penalty for exceeding $O^*$ in a constrained problem)
- $\rho$: penalty coefficient
- $\pi_{nm}$: probability of an attack on PG $m$ of component $n$
- $\pi_F$: probability of an attack on a false target
- $\pi$: set of vectors of attack probabilities (attacker’s strategy): $\pi = \{\pi_{nm}, |1 \leq n \leq N, 1 \leq m \leq M_n\}$
- $\pi(n,m)$: set of vectors representing a single predetermined attack on PG $m$ in component $n$: $\pi(n,m) = \{\pi_{nm} = 1, \pi_{kl} = 0 \text{ if } k \neq n \text{ or } l \neq m\}$
- $\Theta$: set of attacked targets
- $h_{nk}$: inherent value of element $k$ in component $n$ (the loss incurred by the defender if element $k$ is destroyed, not including any loss caused by reduced system performance)
- $H_{nm}$: inherent value of PG $m$ in component $n$ (the loss incurred by the defender if PG $m$ is destroyed, not including the values of the elements in PG $m$ or the loss caused by reduced system performance)
- $H_F$: inherent value of a false target (the loss incurred by the defender if a single FT is destroyed)
- $W$: system demand (desired level of system performance)
- $g_s$: system performance rate in state $s$
- $q_s$: probability that the system is in state $s$
- $G$: variable representing system random performance rate, where $G = g_s$ with probability $q_s$
- $S$: number of system states
- $c(g_s, W)$: cost of losses associated with system performance rate $g_s$ less than the demand $W$
- $C(\pi, \beta, \gamma, W)$: expected unsatisfied demand losses as function of the attack strategy $\pi$ and the defense strategy $\beta, \gamma$
- $D(\pi, \beta, \gamma, F)$: expected damage caused by the attack strategy $\pi$ given the defense strategy $\beta, \gamma, F$
- $r$: attractiveness of FT’s relative to PG’s
- $u_{nk}(z)$: u-function representing pmf for the performance rate of element $k$ in component $n$
- $U_{nm}(z)$: u-function representing the conditional pmf for the performance rate of PG $m$ in component $n$
- $\tilde{U}_{nm}(z)$: u-function representing the unconditional pmf for the performance rate of PG $m$ in component $n$
- $U_n(z)$: u-function representing the pmf for the performance rate of component $n$

1. INTRODUCTION

When considering the risk of intentional attacks, it is important to realize that the use of an adaptive strategy allows attacker to target the most sensitive parts of a system. Choosing the time, place, and means of attacks...
Chapter 3

gives the attacker an advantage over the defender. Therefore, the optimal policy for allocating resources among possible defensive investments should take into account the attacker’s strategy.

In [1] and [2], models of optimal defense investment were studied under the assumption that the attacker maximizes either the success probability of an attack, or the expected damage resulting from an attack on the system. While demonstrating a general approach and suggesting some useful recommendations, these models cannot be directly applied to minimizing expected damage in systems of realistic size and complexity. In particular, the models do not consider factors such as the limited availability of system elements, the possibility that several elements may be destroyed by a single attack, the damage caused by partial incapacitation of the system, and the discrete nature of protection alternatives. These factors should be included in a realistic model of optimal defense strategy for separation and protection of system elements to minimize the expected damage of an attack subject to defense budget constraints [3]. Moreover, defense strategies against intentional attacks can influence the adaptive strategy of the attacker—not only by separation and protection of system elements, but also by creating false targets.

A survivable system has been defined as one that can “complete its mission in a timely manner, even if significant portions are incapacitated by attack or accident” [4]. This definition presumes two important things: First, both external factors (attacks) and internal causes (failures) are presumed to affect system survivability, making it important to take into account the influence of finite availability of system elements due to random failures in determining system survivability.

Second, systems are presumed to have multiple different states, corresponding to different combinations of failed or damaged elements. Each state can be characterized by a system performance rate, which is the quantitative measure of a system’s ability to perform its task [5]. For example, the performance rates of power generating units, production lines, and communication channels can be represented by generating capacity, productivity, and bandwidth, respectively. In this context, the system success is defined as the ability of the system to meet a specified demand (desired performance rate). In multi-state systems, destruction of elements with different performance rates will have different effects. Therefore, the performance rates of system elements should also be taken into account when the damage caused by an attack is estimated.

In systems with non-identical elements and multiple protections, different protections may play different roles in providing for system survivability. Understanding the influence of the protection vulnerabilities on the survivability of the system provides useful information about the importance
of the various protections. In particular, importance evaluation is valuable in tracing bottlenecks in defense strategy, identifying the most important protections, finding weaknesses in protection design, and suggesting defense system upgrades. By analogy with the concept of reliability importance first introduced by Birnbaum [6], protection importance was defined in [7] as a measure of how system survivability changes as a function of the vulnerability of a given protection, so that reducing the vulnerability of the protection with the highest PI leads to the greatest rate of increase in system survivability. Protection importance can also be used to identify irrelevant protections; i.e., protections that have no impact on the system’s survivability. Elimination of irrelevant protections simplifies the system and reduces its cost, but in complex multi-state systems, finding irrelevant protections is not always a trivial task.

Numerous studies have attempted to estimate the impact of external factors on system survivability based on common-cause failures [8-17], but these studies are restricted to \( k \)-out-of-\( n \) systems with identical elements, and do not take into account elements with differing performance rates. Models of multi-state system survivability have been presented in [18-22], where optimal element separation and protection algorithms were proposed for complex series-parallel and bridge system configurations. However, in all of these studies, the adaptive nature of the attacker’s strategy was ignored.

This chapter presents an algorithm for evaluating the importance of different protections in complex series-parallel multi-state systems, and suggests a defense strategy optimization methodology that combines the ideas from [1, 2] and [18–22]. We also study the influence of false targets on the optimal defense strategy.

In the next section of this chapter, a basic model of system defense strategy is presented, and an index of protection importance is introduced. The defense strategy optimization problem is formulated in Section 3. A computational technique for evaluating the system performance rate for arbitrary attacker and defender strategies is described in Section 4. The optimization approach is briefly discussed in Section 5. Illustrative examples of protection importance analysis and defense strategy optimization for a power substation are presented in Section 6, and finally, directions for further research based on the proposed model are briefly outlined in Section 7.

2. **THE MODEL**

Consider a system consisting of \( N \) statistically independent components in a series-parallel configuration. In particular, let component \( n \) consist of \( J_n \) elements of the same functionality, connected in parallel, where element \( k \) in
component $n$ is characterized by its nominal performance rate $x_{nk}$ when available, and its availability $p_{nk}$. The states of the elements are assumed to be independent.

The elements within any given component can be separated (to avoid destruction of the entire component by a single attack), and can also be protected. Parallel elements not separated from one another are considered to belong to the same protection group, where all elements in a given protection group are assumed to be destroyed by a successful attack on that PG, but more than one PG cannot be destroyed by a single attack.

Since system elements with the same functionality can have different performance rates and different availability, the distribution of elements among the various PG’s affects the system survivability. The element separation problem for component $n$ involves partitioning a set $\Phi_n$ of $J_n$ items into a collection of $M_n$ mutually disjoint subsets $\Phi_{nm}$, such that

$$\bigcup_{m=1}^{M_n} \Phi_{nm} = \Phi_n,$$  \hspace{1cm} (1)

$$\Phi_{ni} \cap \Phi_{nj} = \emptyset, \ i \neq j.$$ \hspace{1cm} (2)

where each of the $\Phi_{nm}$ can contain from 0 to $J_n$ elements. If $|\Phi_{nm}| = J_n$ and $|\Phi_{nj}| = 0$ for all $j \neq m$, then all of the elements of component $n$ are included in a single PG. By contrast, if $|\Phi_{nm}| \leq 1$ for all $m$, then all of the elements are separated from each other.

Any partition of the set $\Phi_n$ can be represented by a vector $\{\gamma_{nj}, 1 \leq j \leq J_n\}$, where element $j$ belongs to set $\Phi_n\gamma_{nj}$ ($1 \leq \gamma_{nj} \leq M_n$). The set of vectors $\gamma = \{\gamma_{nj} | 1 \leq j \leq J_n, 1 \leq n \leq N\}$ determines the distribution of elements among protection groups for all components (i.e., the separation strategy of the defender).

For any given protection group belonging to component $n$, there exist $B_n + 1$ available protection options (including the option of no protection). For example, a group of elements can be located outdoors (no protection), within a shed, or in an underground bunker (most expensive, but most effective type of protection). Protection type $\beta_{nm}$ ($0 \leq \beta_{nm} \leq B_n$) is characterized by its cost and vulnerability $v_n(\beta_{nm})$, defined as the conditional probability that the PG is destroyed given that it is attacked, where protection type 0 is defined to reflect no protection. By definition, we take $v_n(0) = 1$; however, the cost of protection of type 0 can be positive, since it represents the cost of creating a (e.g., cost of land, construction, communications, etc.). In general, the cost of PG $m$ in component $n$, $o_n(\beta_{nms}, |\Phi_{nm}|)$, also depends on the number of
3. Optimizing Defense Strategies for Complex Multi-State Systems

elements contained in PG \( m \), \(|\Phi_{nm}|\). The set of vectors \( \beta = \{\beta_{nm} \mid 1 \leq n \leq N, 1 \leq m \leq M_n\} \) thus represents the entire protection strategy of the defender.

In addition to separation and protection, the defender also has the option of creating false targets in order to mislead the attacker. The more FT’s are deployed and the more attractive they are to the attacker, the lower the probability will be of attacks on the actual system components. The cost of deploying \( F \) (identical) false targets is given by \( dF \).

Thus, the total cost of the system defense strategy \( \beta, \gamma, F \) (separation, protection, and FT’s) is given by

\[
O(\beta, \gamma, F) = dF + \sum_{n=1}^{N} \sum_{m=1}^{M_n} o_n(\beta_{nm}, |\Phi_{nm}|). \tag{3}
\]

The behavior of the attacker can be represented by the probability of attack on any given FT, \( \pi_F \), and by the set of vectors \( \pi = \{\pi_{nm} \mid 1 \leq n \leq N, 1 \leq m \leq M_n\} \), where \( \pi_{nm} \) is the defender’s probability of an attack on PG \( m \) in component \( n \).

(Note that the attacker is not required to choose the targets probabilistically; \( \pi \) merely represents the defender’s uncertainty about the attacker’s choice). Given the attacker’s strategy \( \pi \), the unconditional probability of PG \( m \) in component \( n \) being destroyed is given by \( \pi_{nm} v_n(\beta_{nm}) \); it is assumed that attacked FT’s are destroyed with probability 1.

Note that the three components of defense strategy play different roles. Deployment of FT’s reduces the probability of attacks on the PG’s; protection reduces the conditional probability of destruction given an attack; and separation reduces the damage caused by a successful attack. For any given attacker strategy \( \pi \) and defender strategy \( \beta, \gamma, F \), one can determine the probabilistic distribution of the entire system performance (i.e. the pmf of random value \( G \)) in the form of a set of possible values \( g_s \), and their associated probabilities \( q_s(\pi, \beta, \gamma) = \Pr(G = g_s) \) \((1 \leq s \leq S)\), using the algorithm presented in Section 4).

Let \( c(g_s, W) \) be a function of losses associated with system performance \( g_s \) below the demand \( W \). The expected losses for given attacker and defender strategies can be determined as

\[
C(\pi, \beta, \gamma, W) = \sum_{s=1}^{S} q_s(\pi, \beta, \gamma) c(g_s, W). \tag{4}
\]

For example, when the losses are proportional to the unsupplied demand, then we have \( c(g_s, W) = \eta \max(W - g_s, 0) \) (where \( \eta \) is the cost per unit of unsupplied demand), and
Chapter 3

\[ C(\pi, \beta, \gamma, W) = \eta \sum_{s=1}^{S} q_s(\pi, \beta, \gamma) \max(W - g_s, 0). \quad (5) \]

Similarly, if the system fails completely whenever its performance is lower than the demand, then we have \( c(g_s, W) = \eta \cdot 1(g_s < W) \) (where \( \eta \) is the cost of system failure), and

\[ C(\pi, \beta, \gamma, W) = \eta \sum_{s=1}^{S} q_s(\pi, \beta, \gamma) \cdot 1(g_s < W). \quad (6) \]

Finally, for the case of variable demand \( W \) with pmf given by the possible \( w_k \) and their probabilities \( f_k = \Pr(W = w_k) \) (1≤ₖ≤₉), equation (4) takes the form

\[ C(\pi, \beta, \gamma, W) = \sum_{k=1}^{K} f_k \sum_{s=1}^{S} q_s(\pi, \beta, \gamma) c(g_s, w_k). \quad (7) \]

The total expected damage \( ED \) caused by the attack then includes both the cost of losses associated with system performance reduction and also the inherent values of any destroyed elements and the infrastructure; in other words,

\[ D(\pi, \beta, \gamma, F) = F \alpha_F H_F + \]
\[ \sum_{n=1}^{\pi} \sum_{m=1}^{\pi} \pi_{nm} v_n (\beta_{nm}) (H_{nm} + \sum_{k \in \Phi_{nm}} h_{nk}) + C(\pi, \beta, \gamma, W). \quad (8) \]

The importance of protection \( j \) is defined as the rate at which the ED changes with respect to changes in the vulnerability of protection \( j \), i.e.,

\[ I_j = \frac{\partial D}{\partial v_j}. \quad (9) \]

Observe that if the importance of protection \( j \) is equal to zero, the protection is irrelevant, and can be removed without increasing the ED.

The optimal defender strategy \( \beta^*, \gamma^*, F^* \) should minimize the expected damage \( D(\pi, \beta, \gamma, F) \) under the assumption that the attacker uses the most harmful strategy \( \pi \) possible (given the attacker’s resource constraint and level of information about the system and its defense).
3. DEFENSE STRATEGY OPTIMIZATION

In general, in order to define the optimal defense strategy, one has to consider a noncooperative game between the defender and the attacker. For systems and infrastructures whose defenses are readily observable by the attacker, it should be assumed that the defender moves first. The attacker then uses the available information to choose the optimal attack strategy. On the other hand, if the defender is able to keep the system structure and its defense secret, and the attacker’s strategy is also unknown, then the two agents optimize in a simultaneous game.

If the defender has a finite budget $O^*$, the optimal defense strategy is to minimize the ED subject to the budget constraint. If the budget is unlimited, the defender should instead minimize the expected damage plus the total defense investment cost. The defense optimization problem can be formulated as follows

$$\beta^*, \gamma^*, F^* = \arg\{\mu(O(\beta, \gamma, F)) + D(\pi, \beta, \gamma, F) \to \min\}. \quad (10)$$

For the constrained case, we have

$$\mu(O(\beta, \gamma, F)) = \rho \cdot 1(O(\beta, \gamma, F) > O^*), \quad (11)$$

where $\rho$ is a constant greater than the maximal possible damage. For the unconstrained case, we have

$$\mu(O(\beta, \gamma, F)) = O(\beta, \gamma, F). \quad (12)$$

If the attacker’s resource (the maximal possible number of attacks) is limited, then the optimal attack strategy ($\pi_{nm} \in \{0, 1\}$ for $1 \leq n \leq N, 1 \leq m \leq M_n$) is to maximize the ED by an appropriate choice of targets. If the attacker’s resource is unlimited, then the optimal attack strategy is to maximize the difference between the ED and the total attack cost. (If the attack cost is negligible compared to the ED, then the attacker would prefer to attack all possible targets.)

The general formulation of the game is thus

$$\begin{cases} \beta^*, \gamma^*, F^* = \arg\{\mu(O(\beta, \gamma, F)) + D(\pi, \beta, \gamma, F) \to \min\}, \\ \pi^* = \arg\{D(\pi, \beta, \gamma, F) \to \max\}. \end{cases} \quad (13)$$
Chapter 3

With a procedure for determining \( \mu(O(\beta, \gamma, F)) \) and \( D(\pi, \beta, \gamma, F) \) for any \( \pi, \beta, \gamma \) and \( F \), one can find the equilibrium solution by adapting one of algorithms presented in [23].

As in [2], we now consider several special cases depending on how many targets can be attacked, and on the attacker’s knowledge of the system and the defense strategy.

3.1 Single attack

The assumption that only a single attack is possible may be realistic in some cases, as discussed in [2]. In this case, the attacks on different PG’s and FT’s are mutually exclusive events, and the attack probability must satisfy

\[
\sum_{n=1}^{N} \sum_{m=1}^{M_n} \pi_{nm} + F \pi_F \leq 1. \tag{14}
\]

If the attacker has perfect knowledge about the system and its defenses, then the attacker’s optimal strategy is given by

\[
\pi_F = 0; \quad \pi = \pi(n,m), \tag{15}
\]

where \((n, m) = \arg \{D(\pi(n,m), \beta, \gamma) \rightarrow \max\}\), and \(\pi(n,m)\) is a matrix in which all elements are equal to zero except for element \(\pi_{nm}\), which is equal to one. Note that in this case, the FT’s are not meaningful, because the attacker can detect them perfectly.

If the attacker has no information about the system or cannot direct the attack precisely (as might be the case, for example, for a low-precision missile attack), we can assume that the attacker chooses targets at random, in which case we have

\[
\pi_F = \pi_{nm} = 1/(F + \sum_{n=1}^{N} M_n) \tag{16}
\]

for all components \(n\) and all PG’s \(m\). In this case, the FT’s are maximally effective.

In the case of imperfect attacker knowledge about the system, we can assume some positive correlation between the expected damage and the expected attack probability; i.e. \(\pi_{nm} \sim D(\pi(n,m), \beta, \gamma)\). In the simplest case, the probability of an attack on each target could be proportional to its
attractiveness to the attacker. For real targets (PG), we take the attractiveness to be proportional to the expected damage, and for FT’s the attractiveness depends on factors such as the quality of the FT, any intentional disinformation by the defender, etc. The relative attractiveness of FT’s to the attacker can be measured by an attractiveness ratio $r = \frac{D_F}{D_{\text{max}}}$, where $D_F$ is the damage that the attacker believes would be associated with destruction of a FT, and $D_{\text{max}}$ is the expected damage associated with the most harmful single attack; i.e., $D_{\text{max}} = \max_{n,m} \{D(\pi(n,m),\beta,\gamma)\}$. The attacker strategy in this case is of the form

$$\pi_{nm} = D(\pi(n,m),\beta,\gamma)/D_{\text{tot}}, \quad \pi_F = D_F/D_{\text{tot}} = rD_{\text{max}}/D_{\text{tot}},$$

where

$$D_{\text{tot}} = \sum_{n=1}^{N} \sum_{m=1}^{M} D(\pi(n,m),\beta,\gamma) + rF D_{\text{max}}.$$  

Finally, having the attacker strategy $\pi_F, \pi$, one can estimate the expected damage as

$$D(\pi,\beta,\gamma,F) = \sum_{n=1}^{N} \sum_{m=1}^{M} \pi_{nm} D(\pi(n,m),\beta,\gamma) + F \pi_F H_F$$

and find the optimal defense strategy as

$$\beta^*, \gamma^*, F^* = \text{arg} \{ \mu(O(\beta, \gamma, F)) + \sum_{n=1}^{N} \sum_{m=1}^{M} \pi_{nm} D(\pi(n,m),\beta,\gamma) + F \pi_F H_F \rightarrow \min \}$$

### 3.2 Multiple attacks

The attacks can take place sequentially or simultaneously. However, following [2], we assume that the attacks are independent (i.e., their probabilities do not change in accordance with achieved results so far).

Since several targets can be attacked, assumption (14) on the attacker’s strategy does not hold. In the worst case of unlimited attacker resources, all
targets will be attacked with probability 1; i.e., \( \pi_F = \pi_{nm} = 1 \) for \( 1 \leq n \leq N, 1 \leq m \leq M_n \). If the attacker’s resources are limited (i.e., the maximal possible number of attacks is \( E \)) and the attacker’s knowledge about the system is perfect, the most effective attack strategy is

\[
\pi_F = 0, \quad \pi(\Theta) = \{ \pi_{nm} = 1, (n,m) \in \Theta; \pi_{nm} = 0, (n,m) \notin \Theta \},
\]

where the set \( \Theta \) of targets to attack is determined as the solution of the program

\[
\Theta = \arg \{ D(\pi(\Theta), \beta, \gamma) \to \max \}
\]

subject to \( \sum_{n=1}^{N} \sum_{m=1}^{M_n} l((n,m) \in \Theta) = E \).

It can be easily seen that in both cases the FT’s are of no interest.

If the attacker’s resources are limited and the attacker’s knowledge about the system is imperfect, the attacker tries to maximize the total damage. According to the model of target attractiveness presented in the previous section, we have

\[
\Theta, \delta = \arg \{ D(\pi(\Theta), \beta, \gamma) + \delta rD_{max} \to \max \}
\]

subject to \( \delta + \sum_{n=1}^{N} \sum_{m=1}^{M_n} l((n,m) \in \Theta) = E, \quad \delta \leq F \), where \( \delta \) is the number of FT’s attacked. If the attacker has limited resources and no information about the system, the probability of an attack on any target can be estimated as

\[
\pi_F = \pi_{nm} = \frac{E}{(F + \sum_{n=1}^{N} M_n)}. \tag{24}
\]

Since different attacks are not mutually exclusive events, the expected damage cannot be obtained using Eq. (19), and the defense strategy optimization problem takes the form

\[
\beta^*, \gamma^*, F^* = \arg \{ \mu(\beta, \gamma, F) + D(\pi, \beta, \gamma, F) \to \min \}. \tag{25}
\]
In order to solve the optimization problems presented here, one has to develop an algorithm for evaluating the expected damage $D(\pi, \beta, \gamma, F)$ for arbitrary attacker and defender strategies. Having the system performance distribution in the form $g_{s}, q_{s}(\pi, \beta, \gamma, F)$ for $1 \leq s \leq S$, one can obtain the expected damage using equations (4) and (8). The system performance distribution can be obtained using the universal generating function (u-function) technique suggested in [24], which has proved to be an effective tool for reliability analysis and optimization [25].

### 4.1 Universal generating function technique

The u-function representing the pmf of a discrete random variable $Y$ is defined as a polynomial

$$u_Y(z) = \sum_{h=0}^{H} \sigma_h z^{y_h},$$

where the $Y$ is assumed to have $H+1$ possible values, $y_h$ is the $h$-th possible value of $Y$, and $\sigma_h = \Pr(Y = y_h)$.

To obtain the u-function representing the pmf of a function of two independent random variables $\varphi(X, T)$, the following composition operator is used:

$$U_{\varphi(1, 1)}(z) = u_Y(z) \otimes u_T(z) = \left( \sum_{h=0}^{H} \sigma_h z^{y_h} \right) \otimes \left( \sum_{d=0}^{D} \sigma_d z^{t_d} \right)$$

$$= \sum_{h=0}^{H} \sum_{d=0}^{D} \sigma_h \sigma_d z^{\varphi(y_h, t_d)}.$$  

This polynomial represents all possible combinations of realizations of the variables $Y$ and $T$, by relating the probability of each combination to the corresponding value of the function $\varphi(Y, T)$.

In our case, the u-functions can represent performance distributions of individual system elements or their groups. Any element $k$ of component $n$ has two possible states: functioning with nominal performance $x_{nk}$ (with probability $p_{nk}$); and failed (with probability $1-p_{nk}$). The performance of a failed element is taken to be zero. The u-function representing this performance distribution takes the form
\[ u_{nk}(z) = p_{nk}z^{x_{nk}} + (1 - p_{nk})z^0. \]  

If the combined performance of any pair of elements, connected in series or in parallel, is defined as a function of the individual performances of the two elements, the pmf of the entire system performance can be obtained using the following recursive procedure [25].

**Procedure 1.**

1. Find any pair of system elements connected in parallel or in series.
2. Obtain the u-function of this pair using the corresponding composition operator \( \otimes \) over the u-functions corresponding to the two elements, where the function \( \varphi \) is determined by the nature of the connection between the two elements.
3. Replace that pair with a single element having the u-function obtained in step 2.
4. If the system still contains more than one element, return to step 1.

The choice of the composition functions \( \varphi \) depends both on the type of connection between the elements, and on the type of the system. Different types of these functions are considered in [25]. For example, in systems with performance defined as productivity or capacity (e.g., continuous materials or energy transmission systems, manufacturing systems, power supply systems), the total performance of elements connected in parallel is equal to the sum of the performances of its elements. Therefore, the composition function for a pair of elements connected in parallel would take the form

\[ \varphi_{\text{par}}(Y, T) = Y + T. \]  

When the elements are connected in series, the element with the lowest performance becomes the bottleneck of the system. Therefore, the composition function for a pair of elements connected in series is

\[ \varphi_{\text{ser}}(Y, T) = \min(Y, T). \]  

### 4.2 Incorporating the destruction probability of a protection group

The u-function \( U_{nm}(z) \) for any PG \( m \) in component \( n \) can be obtained using **Procedure 1** above, with composition operator \( \otimes \) over all the
elements belonging to the set $\Phi_{nm}$, since the elements of a PG are effectively in parallel. This u-function represents the conditional pmf of the PG’s performance given that the PG is not destroyed by an attack. If the PG is protected by a protection of type $\beta_{nm}$, it can be destroyed with probability $\pi_{nm}v_n(\beta_{nm})$. In order to obtain the unconditional pmf of the PG’s performance, one should multiply the probabilities of all PG states in which the group has nonzero performance rates by $1–\pi_{nm}v_n(\beta_{nm})$. The u-function $\tilde{U}_{nm}(z)$ representing the unconditional pmf can then be obtained as

$$\tilde{U}_{nm}(z)=\frac{1}{1–\pi_{nm}v_n(\beta_{nm})}U_{nm}(z) + \pi_{nm}v_n(\beta_{nm})z^0.$$  \hspace{1cm} (31)

Having the operators (27) and (31), we can use the following procedure to obtain the pmf of the entire system performance for any expected attacker strategy $\pi$ and defender strategy $\beta, \gamma, F$.

**Procedure 2.**

1. For any component $n=1, \ldots, N$:
   1.1. Define $U_n(z)=z^0$
   1.2. For any nonempty PG $m$ (consisting of a set $\Phi_{nm}$ of elements):
      1.1.1. Determine $\pi_{nm}$ and $v_n(\beta_{nm})$ as functions of $\beta, \gamma, F$ in accordance with the expected attacker strategy $\pi$ (as described in Section 3).
      1.1.2. Define $U_{nm}(z)=z^0$.
      1.1.3. For any element $k$ belonging to $\Phi_{nm}$, modify $U_{nm}(z)$ as follows:
              $$U_{nm}(z)=U_{nm}(z) \otimes u_{nk}(z).$$
   1.3. Obtain the u-function $\tilde{U}_{nm}(z)$ representing the unconditional pmf of PG $m$ using Eq. (31).
   1.4. Modify the u-function $U_n(z)$ as follows: $U_n(z)=U_n(z) \otimes \tilde{U}_{nm}(z)$.

2. Apply Procedure 1 to the u-functions of the various system components in accordance with the series-parallel system structure.
5. **OPTIMIZATION TECHNIQUE**

In Section 3, complicated combinatorial optimization problems are formulated. An exhaustive examination of all possible solutions is not realistic, considering reasonable time limitations. As in most combinatorial optimization problems, the quality of a given solution is the only information available during the search for the optimal solution. Therefore, a heuristic search algorithm is needed that uses only estimates of solution quality, and does not require derivative information to determine the next direction of search.

Several powerful universal optimization meta-heuristics have been designed in recent times. Such meta-heuristics as the genetic algorithm [26], ant colony optimization [27], tabu search [28], variable neighbourhood descent [29], the great deluge algorithm [30], the immune algorithm [31], and their combinations (hybrid optimization techniques) have proven to be effective in solving reliability-optimization problems of realistic size and complexity.

All of these algorithms require representation of the solution in the form of a string. Any defense strategy \( \beta, \gamma \) can be represented by a concatenation of integer strings \( \{\gamma_{nj}, 1 \leq n \leq N, 1 \leq j \leq J_n\} \) and \( \{\beta_{nm}, 1 \leq n \leq N, 1 \leq m \leq M_n\} \), with the addition of a single integer number representing the number \( F \) of false targets. The total length of the resulting string is \( \sum_{n=1}^{N} J_n + 1 \). The substring corresponding to \( \gamma \) determines the distribution of the elements among protection groups, while the substring corresponding to \( \beta \) determines the types of protections chosen for the various PG’s. Since the maximal possible number of protections is equal to the total number of elements in the system (in the case of total element separation), the length of substring \( \beta \) should be equal to the total number of the elements. If the number of PG’s defined by substring \( \gamma \) is less than the total number of system elements, the redundant elements of substring \( \beta \) are ignored. For the case of limited defender resource, the solution can be represented by the concatenation of the integer strings \( \beta \) and \( \gamma \), whereas the value of \( F \) can be obtained as

\[
F = \begin{cases} 
0, & \text{if } O(\beta, \gamma, 0) \geq O^* \\
\frac{O^* - O(\beta, \gamma, 0)}{d}, & \text{if } O(\beta, \gamma, 0) < O^* 
\end{cases} 
\] (32)

In this work, the GA is used to obtain the solutions presented in the next section. The details of the GA implementation can be found in [5, 18-22]. The basic structure of the version of GA referred to as GENITOR [32] is as
follows: First, an initial population of $N_s$ randomly constructed solutions (strings) is generated. Within this population, new solutions are obtained during the genetic cycle by using crossover and mutation operators. The crossover produces a new solution (offspring) from a randomly selected pair of parent solutions, facilitating the inheritance of some basic properties of the parents by the offspring. Mutation results in slight changes to the offspring’s structure, and maintains a diversity of solutions. This procedure avoids premature convergence to a local optimum, and facilitates jumps in the solution space.

Each new solution string is decoded (to determine $\beta$, $\gamma$, and $F$), and its objective function (fitness) value is estimated. In our case, the fitness is determined as $D^* - D(\pi, \beta, \gamma, F)$ (where $D^*$ is a positive constant), so that solutions with the minimal expected damage $D(\pi, \beta, \gamma, F)$ have maximal fitness. The fitness values, which are a measure of quality, are used to compare different solutions. The comparison is accomplished by a selection procedure that determines which solution is better, the newly obtained solution or the worst solution in the population. The better of these two solutions joins (or remains in) the population, while the other is discarded. If the population contains multiple equivalent solutions, any redundancies are eliminated, and the population size decreases correspondingly.

After new solutions have been produced $N_{rep}$ times, new randomly constructed solutions are generated to replenish the shrunken population, and a new genetic cycle begins. The GA is terminated after $N_c$ genetic cycles. The final population contains the best solution achieved so far. It also contains multiple near-optimal solutions that may also be of interest in the decision-making process.

6. **ILLUSTRATIVE EXAMPLES**

6.1 **Evaluation of protection importance**

Consider the following series-parallel multi-state system corresponding to a power substation, which consists of five components connected in series:

1. Power transformers;
2. Capacitor banks;
3. Input high-voltage line sections;
4. Output medium-voltage line sections;
5. Blocks of commutation equipment.
Each component is built from several different elements of the same functionality. The structure (reliability block diagram) of the series-parallel system and its protections is presented in Figure 3-1. The availability, nominal performance rate, and inherent value of each element are presented in Table 3-1 (the performances are in MW, while the costs are in thousands of dollars). Within each component, the elements are separated and protected by different types of protections (e.g., outdoor, indoor, and underground locations for the transformers and capacitors; overhead, overhead insulated, and underground lines; etc.). The vulnerability and inherent value of each protection are presented in Table 3-2.

The system demand is constant at $W=120$. The cost of losses is proportional to the unsupplied demand (see Eq. (5)), with unit cost $\eta=85$.

The ED caused by any single attack on PG $j$, $D(\pi(j))$, calculated using the algorithm suggested above, are presented in Table 3-3. The protection importance for different PG’s of the system have been obtained for four different attacker strategies.

### 6.1.1 Single attack with no attacker knowledge about the system

In this case (the best case for the defender), the damage is a linearly increasing function of the protection vulnerabilities. These functions for different PG’s are presented in Figure 3-2. The obtained protection importance $I_j^n$ are given in Table 3-3. According to these indices, an improvement to the protection of PG 8 (i.e., a reduction of $v_8$) would cause the greatest reduction of ED. The second best option is to improve the protection of PG 5. The least important protection is that for PG 1. However, since any PG can be attacked, all of the protections are relevant.
3. Optimizing Defense Strategies for Complex Multi-State Systems

![Figure 3-2. Damage $D(v_j)$ for the case of a single attack and no attacker knowledge](image)

**Table 3-1. Characteristics of system elements**

<table>
<thead>
<tr>
<th>Component</th>
<th>Element</th>
<th>Availability</th>
<th>Nominal performance</th>
<th>Inherent value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>$k$</td>
<td>$p_{nk}$</td>
<td>$x_{nk}$</td>
<td>$h_{nk}$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0.75</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>0.70</td>
<td>25</td>
<td>32</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>0.80</td>
<td>25</td>
<td>35</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>0.80</td>
<td>30</td>
<td>40</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>0.85</td>
<td>35</td>
<td>50</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0.90</td>
<td>40</td>
<td>30</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0.85</td>
<td>50</td>
<td>30</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>0.80</td>
<td>60</td>
<td>42</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0.92</td>
<td>80</td>
<td>120</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>0.95</td>
<td>100</td>
<td>140</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0.70</td>
<td>35</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>0.65</td>
<td>40</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>0.62</td>
<td>50</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0.63</td>
<td>40</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>0.87</td>
<td>55</td>
<td>25</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>0.80</td>
<td>55</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>0.77</td>
<td>65</td>
<td>25</td>
</tr>
</tbody>
</table>

**Table 3-2. Characteristics of system protections**

<table>
<thead>
<tr>
<th>PG $j$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability $v_j$</td>
<td>1.0</td>
<td>0.6</td>
<td>0.5</td>
<td>1.0</td>
<td>0.3</td>
<td>0.9</td>
<td>0.4</td>
<td>0.2</td>
<td>1.0</td>
<td>0.3</td>
<td>1.0</td>
</tr>
<tr>
<td>Inherent value $b_j$</td>
<td>1.5</td>
<td>9</td>
<td>13.5</td>
<td>2.25</td>
<td>13.5</td>
<td>8.25</td>
<td>12</td>
<td>11.25</td>
<td>0.75</td>
<td>10.5</td>
<td>0.75</td>
</tr>
</tbody>
</table>
Table 3-3. Obtained protection importances

<table>
<thead>
<tr>
<th>No of PG</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage $D(\pi(j))$</td>
<td>4046.3</td>
<td>4509.6</td>
<td>4890.9</td>
<td>4331.0</td>
<td>4716.7</td>
<td>4150.9</td>
<td>4162.6</td>
<td>4505.8</td>
<td>4448.4</td>
<td>4433.3</td>
<td>4298.2</td>
</tr>
<tr>
<td>No attacker knowledge $I_j^*$</td>
<td>40.6</td>
<td>137.8</td>
<td>234.7</td>
<td>66.5</td>
<td>338.4</td>
<td>127.9</td>
<td>411.8</td>
<td>77.1</td>
<td>252.5</td>
<td>63.5</td>
<td></td>
</tr>
<tr>
<td>Multiple attacks $I_j^{**}$</td>
<td>199.9</td>
<td>531.5</td>
<td>799.0</td>
<td>249.8</td>
<td>964.0</td>
<td>523.9</td>
<td>1024.0</td>
<td>805.9</td>
<td>129.4</td>
<td>933.9</td>
<td>258.5</td>
</tr>
<tr>
<td>$I_j^*$</td>
<td>0</td>
<td>1516.1</td>
<td>2581.9</td>
<td>0</td>
<td>3722.5</td>
<td>1406.6</td>
<td>4529.3</td>
<td>0</td>
<td>2777.9</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>$v^*$</td>
<td>-</td>
<td>0.845</td>
<td>0.425</td>
<td>-</td>
<td>0.340</td>
<td>-</td>
<td>0.910</td>
<td>0.280</td>
<td>-</td>
<td>0.455</td>
<td></td>
</tr>
</tbody>
</table>

6.1.2 Single attack with perfect attacker knowledge about the system

In this case (the worst case for the defender), the damage is a linearly increasing function of protection vulnerability $v_j$ only when this value becomes greater than some threshold $v_j^*$ (Figure 3-3). Indeed, when the vulnerability $v_j$ of PG $j$ is small enough, then PG $j$ becomes less attractive to the attacker than some other PG (recalling that the attacker chooses the single PG resulting in the greatest ED). The protection importances in this case take the form

$$I_j^{p*} = \begin{cases} 0, & v_j \leq v_j^* \\ I_j^*, & v_j > v_j^* \end{cases}$$

The protection importance $I_j^*$ and thresholds $v_j^*$ are given in Table 3-3. In this case, PG’s 1, 4, 6, 9, and 11 are always unattractive for the attacker because, even unprotected, these PG’s do not play important enough roles in meeting the system demand. Therefore, the protections of these PG’s are irrelevant. For example, the protection of PG 6 can be removed without increasing the ED.

It can be seen from Figure 3-3 and Table 3-3 that the greatest increase of ED can be caused by deterioration of the protection of PG 8. However, the ED cannot be reduced by improvement of this protection, because its vulnerability $v_8=0.2$ is already smaller than $v_8^*=0.28$. Therefore, the only protection that can be improved in order to reduce the ED is that of PG 3 (since for the given protection vulnerabilities, the ED $D(\pi(3))$ is the greatest, and PG 3 is the most attractive target for the attacker). When the reduction of vulnerability $v_3$ causes $D(\pi(3))$ to fall below $D(\pi(5))=4716.7$, PG 5 becomes the most attractive to the attacker and further reduction of $v_3$ makes no sense. (Observe also that the ED in the case of perfect attacker knowledge is always greater than in the case of no knowledge.)
6.1.3 Single attack with imperfect attacker knowledge about the system when the attack probability is proportional to the ED

In this case, the ED is a quadratic function of the protection vulnerability (Figure 3-4), and protection importance is a linear function of the protection vulnerability. All protections are relevant. The order of protection importance for different PG’s is the same as in the case of no attacker knowledge. The ED is greater than in the case of no attacker knowledge, but less than in the case of perfect knowledge.

6.1.4 Multiple attacks with unlimited attacker resources (πj=1 for 1≤j≤M)

In this case, each PG is attacked. The damage is a linear increasing function of the protection vulnerabilities (Figure 3-5), and is always greater than in the worst case of a single attack. All protections are relevant; however, the order of protection importance differs from the order corresponding to a single attack (for example, the protection of PG 7 becomes the most important). This change in the order of the protection importances is caused by the fact that the probabilities of simultaneous destruction of different PG’s are taken into account in the case of multiple attacks. The obtained protection importances $I^m_j$ are again given in Table 3-3.
Figure 3-4. Damage $D(v_j)$ for the case of a single attack and attack probabilities proportional to ED

Figure 3-5. Damage $D(v_j)$ for the worst case of multiple attack

6.2 Optimal separation and protection strategy

Assume that in the series-parallel multi-state system considered here, the elements within each component can be separated and protected in an arbitrary way. Up to four different types of protection can be chosen for the various protection groups: outdoor location (type 0), shed (type 1), concrete building (type 2), and underground bunker (type 3) for the transformers, capacitors, and commutation equipment; and overhead lines (type 0), overhead insulated lines (type 1), lines with casing (type 2), and underground lines (type 3) for input and output lines. The vulnerabilities of
3. Optimizing Defense Strategies for Complex Multi-State Systems

Table 3-4. Characteristics of available protections

<table>
<thead>
<tr>
<th>No of component</th>
<th>Protection type</th>
<th>Vulnerability ( v )</th>
<th>1 element</th>
<th>2 elements</th>
<th>3 elements</th>
<th>4 elements</th>
<th>5 elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1.0</td>
<td>2</td>
<td>2.5</td>
<td>3</td>
<td>3.5</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0.8</td>
<td>8</td>
<td>12</td>
<td>15</td>
<td>17</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0.6</td>
<td>12</td>
<td>18</td>
<td>22</td>
<td>25</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1.0</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0.9</td>
<td>11</td>
<td>13</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0.4</td>
<td>9</td>
<td>14</td>
<td>17</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0.2</td>
<td>20</td>
<td>23</td>
<td>26</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0.2</td>
<td>24</td>
<td>30</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0.6</td>
<td>18</td>
<td>21</td>
<td>27</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0.2</td>
<td>20</td>
<td>30</td>
<td>38</td>
<td>—</td>
<td>—</td>
<td></td>
</tr>
</tbody>
</table>

The various types of protection and the protection costs (as functions of the number of elements in a PG) are presented in Table 3-4. The inherent value of PG infrastructure \( H_{nm} \) is assumed to equal to 75% of its protection cost.

The separation and protection optimization problem has been solved for a limited defender budget, and three different attacker strategies: single attack with perfect attacker knowledge; single attack with no attacker knowledge; and multiple attacks with unlimited attacker resources (\( \pi_{nm} = 1 \) for \( 1 \leq n \leq N, 1 \leq m \leq M_n \)). No false targets were allowed. The resulting solutions for different defender budgets are presented in Tables 3-5 to 3-7.

Table 3-5. Best obtained defense strategies against a single attack with perfect attacker knowledge

<table>
<thead>
<tr>
<th>Defense Strategy</th>
<th>Expected damage</th>
<th>Defense cost</th>
<th>Budget O*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component 1</td>
<td>0{1,2} 0{3} 0{4}</td>
<td>0{1} 0{2}</td>
<td>0{1} 0{2,4}</td>
</tr>
<tr>
<td>Component 2</td>
<td>0{5}</td>
<td>0{3} 1{2}</td>
<td>0{3}</td>
</tr>
<tr>
<td>Component 3</td>
<td>2{1,2} 0{3} 0{4}</td>
<td>0{1} 1{2}</td>
<td>0{1} 0{2}</td>
</tr>
<tr>
<td>Component 4</td>
<td>1{5}</td>
<td>1{3} 2{2}</td>
<td>1{3} 0{4}</td>
</tr>
<tr>
<td>Component 5</td>
<td>0{1} 0{2} 0{3} 1{4}</td>
<td>1{1} 1{2}</td>
<td>0{1} 1{4}</td>
</tr>
<tr>
<td>50.0</td>
<td>49.5</td>
<td>4862.48</td>
<td>50.0</td>
</tr>
<tr>
<td>100.0</td>
<td>98.0</td>
<td>4486.81</td>
<td>100.0</td>
</tr>
<tr>
<td>125.0</td>
<td>125.0</td>
<td>4266.90</td>
<td>125.0</td>
</tr>
</tbody>
</table>
### Table 3-6. Best obtained defense strategies against a single attack with no attacker knowledge

<table>
<thead>
<tr>
<th>Budget</th>
<th>Defense Strategy</th>
<th>Expected Defense cost</th>
<th>Expected Damage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Component 1</td>
<td>Component 2</td>
<td>Component 3</td>
</tr>
<tr>
<td>50.0</td>
<td>0{1} 0{2} 0{3}</td>
<td>0{4} 0{5} 0{6}</td>
<td>0{1} 0{2}</td>
</tr>
<tr>
<td>100.0</td>
<td>0{1} 0{2} 0{3}</td>
<td>0{4} 0{5} 1{6}</td>
<td>0{1} 1{2}</td>
</tr>
<tr>
<td>150.0</td>
<td>0{1} 0{2} 1{3}</td>
<td>0{4} 0{5} 2{6}</td>
<td>1{3} 2{6}</td>
</tr>
<tr>
<td>200.0</td>
<td>0{1} 1{2} 2{3}</td>
<td>2{4} 2{5} 3{6}</td>
<td>1{3} 3{6}</td>
</tr>
</tbody>
</table>

The defense strategies in these tables are presented for each system component in the form of lists of PG characteristics: \( \beta_{nm}\{\Phi_{nm}\} \). For example, 2{1,3} means that elements 1 and 3 form a separate PG with protection of type 2.

It can be seen that separation is highly effective against single attacks, because it reduces the damage caused by the attack. It is especially important in the case when the attacker has no knowledge about the system, and any PG can be attacked. In this case, total separation is used even for a minimal defense budget (see Table 3-6), even though this does not allow the defender to implement effective protections. When the attacker has perfect knowledge about the system, separation of some elements can be ineffective. For example, the optimal defense strategy for a budget of \( O=125 \) (last line of Table 3-5) does not presume any separation of elements 1 and 4, or elements 2 and 3 in component 4, because the corresponding PG’s are less attractive for the attacker than the PG consisting of element 5 in component 1.

In the case of multiple attacks with unlimited attacker resources, all the PG’s can be attacked simultaneously. Therefore, in this case, protection plays a more important role than separation, and the numbers of PG’s in the best defense strategies obtained for multiple attacks are smaller than the corresponding numbers for single attacks.

### Table 3-7. Best obtained defense strategies against multiple attacks with unlimited attacker resources

<table>
<thead>
<tr>
<th>Budget</th>
<th>Defense Strategy</th>
<th>Expected Defense cost</th>
<th>Expected Damage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Component 1</td>
<td>Component 2</td>
<td>Component 3</td>
</tr>
<tr>
<td>50.0</td>
<td>0{1,2,3,4,5}</td>
<td>0{1,2,3}</td>
<td>3{1,2}</td>
</tr>
<tr>
<td>100.0</td>
<td>0{1} 0{2}</td>
<td>0{1,2}</td>
<td>2{1,2}</td>
</tr>
<tr>
<td>150.0</td>
<td>2{1,2,3,4,5}</td>
<td>3{1,2,3}</td>
<td>3{1,2}</td>
</tr>
<tr>
<td>200.0</td>
<td>2{1,2,3}</td>
<td>3{1,2}</td>
<td>2{1}</td>
</tr>
</tbody>
</table>

The defense strategies in these tables are presented for each system component in the form of lists of PG characteristics: \( \beta_{nm}\{\Phi_{nm}\} \). For example, 2{1,3} means that elements 1 and 3 form a separate PG with protection of type 2.

It can be seen that separation is highly effective against single attacks, because it reduces the damage caused by the attack. It is especially important in the case when the attacker has no knowledge about the system, and any PG can be attacked. In this case, total separation is used even for a minimal defense budget (see Table 3-6), even though this does not allow the defender to implement effective protections. When the attacker has perfect knowledge about the system, separation of some elements can be ineffective. For example, the optimal defense strategy for a budget of \( O=125 \) (last line of Table 3-5) does not presume any separation of elements 1 and 4, or elements 2 and 3 in component 4, because the corresponding PG’s are less attractive for the attacker than the PG consisting of element 5 in component 1.

In the case of multiple attacks with unlimited attacker resources, all the PG’s can be attacked simultaneously. Therefore, in this case, protection plays a more important role than separation, and the numbers of PG’s in the best defense strategies obtained for multiple attacks are smaller than the corresponding numbers for single attacks.
3. Optimizing Defense Strategies for Complex Multi-State Systems

The separation efficiency also depends on the system demand. When the demand is relatively small, the system can tolerate the destruction of some elements, which makes separation efficient. By contrast, when the demand is close to the maximal possible system performance, the incapacitation of even a small part of the system can cause unsupplied demand. In this case, separation (which reduces the number of elements destroyed by a single attack) is less effective. Table 3-8 presents the best obtained defense strategies against multiple attacks with unlimited attacker resources for different values of system demand, holding the defense budget constant. It can be seen that the number of different PG’s decreases with increasing demand.

Table 3-8. Best obtained defense strategies against multiple attacks with unlimited attacker resources (defense budget \(O^* = 150\))

<table>
<thead>
<tr>
<th>Demand</th>
<th>Defense</th>
<th>Cost</th>
<th>Expected</th>
<th>Total</th>
<th>No. of PG</th>
<th>Component 1</th>
<th>Component 2</th>
<th>Component 3</th>
<th>Component 4</th>
<th>Component 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>W</td>
<td>O</td>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>30.0</td>
<td>150.0</td>
<td>2294.1</td>
<td>0{1,2}</td>
<td>2{3}</td>
<td>3{1,3}</td>
<td>3{1,2}</td>
<td>1{1,3}</td>
<td>3{1}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2{4}</td>
<td>2{5}</td>
<td>0{2}</td>
<td></td>
<td>1{2,4}</td>
<td>0{2,3}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60.0</td>
<td>149.0</td>
<td>4603.6</td>
<td>2{1,2,3,4}</td>
<td>0{1}</td>
<td>3{1,2}</td>
<td>1{1,2}</td>
<td>2{1,3}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2{5}</td>
<td>3{2,3}</td>
<td>1{3,4}</td>
<td></td>
<td></td>
<td>0{2}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>90.0</td>
<td>150.0</td>
<td>7037.1</td>
<td>2{1,2,3,4}</td>
<td>0{1}</td>
<td>3{1,2}</td>
<td>1{1,2,3,4}</td>
<td>2{1,2}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2{5}</td>
<td>3{2,3}</td>
<td>1{3,4}</td>
<td></td>
<td></td>
<td></td>
<td>1{3}</td>
<td></td>
</tr>
<tr>
<td>120.0</td>
<td>150.0</td>
<td>9502.9</td>
<td>2{1,2,3,4,5}</td>
<td>3{1,2,3}</td>
<td>3{1,2}</td>
<td>1{1,2,3,4}</td>
<td>3{1,2}</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The relationship between investment and effectiveness is important to decision makers. In particular, in the case of defense strategy optimization, it is important to know how much an increase in the defense budget can be expected to reduce the ED caused by attacks. The expected damage as a function of the defense budget is shown in Figure 3-6 for each attacker strategy.

From these curves, one can see, for example, that a budget greater than \(O^* = 125\) provides no benefit in the case of a single attack with perfect attacker knowledge about the system, for the given set of available protections. Indeed, when \(O^* \geq 125\), the greatest damage \(D = 4266.9\) is achieved by an attack on the PG consisting of element 5 in component 1, and having the highest protection type 2. Any further increase of the defensive investment can reduce the expected damage caused by the destruction of other groups, but will not change the expected damage caused by the destruction of this PG (since the maximal separation and protection of element 5 in component 1 has already been achieved). Because the attacker is assumed to choose the most harmful strategy, and is assumed to know that attacking element 5 in component 1 is the most damaging strategy, further investment cannot reduce the expected damage.
In order to analyze the influence of FT’s on the optimal defense strategy, the defense strategy optimization problem has been solved for different FT costs (for a limited defender budget and a single attack). The inherent value of the FT’s, $H_F$, is assumed to equal to 75% of their cost. Table 3-9 shows the best defense strategies obtained under the budget constraint $O^*=50$ for the cases of no attacker knowledge and imperfect attacker knowledge for different values of the FT attractiveness ratio $r$.

From Table 3-9 we can see that the number of FT’s in the optimal strategy, $F$, increases gradually in $r$ (where $r=0$ corresponds to the case when the attacker can identify FT’s and avoid striking them). The increase of $F$ is achieved at the expense of decreased separation. The relatively low FT cost $d=4$ makes them an effective element of defensive strategy.

To study the case when FT’s are relatively expensive, the optimal defense strategies have also been obtained for the case where $d=12$ and $O^*=150$ (see Table 3-10). In this case, FT’s are undesirable when their attractiveness is low ($F=0$ for both $r=0$ and $r=0.1$). However, since the budget is much greater than in the previous case, when the FT’s are attractive enough ($r \geq 0.5$), they are again deployed, at the expense of reduced separation and protection.

Figure 3-7 presents both the ED and the optimal number of FT’s for $O^*=50$ as functions of the FT cost. It can be seen that the number of FT’s is greatest for the case of no attacker knowledge. The greater the FT cost $d$ and
3. Optimizing Defense Strategies for Complex Multi-State Systems

Table 3-9. Best obtained defense strategies against single attack for $d=4, O^*=50$

<table>
<thead>
<tr>
<th>$r$</th>
<th>$D$</th>
<th>$F$</th>
<th>Component 1</th>
<th>Component 2</th>
<th>Component 3</th>
<th>Component 4</th>
<th>Component 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4351.57</td>
<td>0</td>
<td>0{1} 0{2} 0{3}</td>
<td>0{1} 0{2}</td>
<td>0{1}</td>
<td>0{1} 0{2}</td>
<td>0{1} 0{2}</td>
</tr>
<tr>
<td>0.1</td>
<td>4322.45</td>
<td>4</td>
<td>0{4} 0{5}</td>
<td>0{1} 0{2}</td>
<td>0{1}</td>
<td>0{1} 0{2}</td>
<td>0{1} 0{2}</td>
</tr>
<tr>
<td>0.5</td>
<td>3779.91</td>
<td>5</td>
<td>0{1,2,3,5}</td>
<td>0{1} 0{2}</td>
<td>0{1}</td>
<td>0{1} 0{2}</td>
<td>0{1} 0{2}</td>
</tr>
<tr>
<td>0.9</td>
<td>3054.85</td>
<td>6</td>
<td>0{4}</td>
<td>0{1} 0{2}</td>
<td>0{1}</td>
<td>0{1} 0{2}</td>
<td>0{1} 0{2}</td>
</tr>
<tr>
<td>No knowledge</td>
<td>3471.24</td>
<td>5</td>
<td>0{1,2,4}</td>
<td>0{1} 0{2}</td>
<td>0{1}</td>
<td>0{1} 0{2}</td>
<td>0{1} 0{2}</td>
</tr>
</tbody>
</table>

Table 3-10. Best obtained defense strategies against single attack for $d=12, O^*=150$

<table>
<thead>
<tr>
<th>$r$</th>
<th>$D$</th>
<th>$F$</th>
<th>Component 1</th>
<th>Component 2</th>
<th>Component 3</th>
<th>Component 4</th>
<th>Component 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3940.51</td>
<td>0</td>
<td>0{1} 1{2} 1{3}</td>
<td>1{1} 1{2}</td>
<td>0{1}</td>
<td>1{1} 1{2}</td>
<td>1{1} 1{2}</td>
</tr>
<tr>
<td>0.1</td>
<td>3940.51</td>
<td>0</td>
<td>1{4} 1{5}</td>
<td>1{1} 1{2}</td>
<td>0{1}</td>
<td>1{1} 1{2}</td>
<td>1{1} 1{2}</td>
</tr>
<tr>
<td>0.5</td>
<td>3074.57</td>
<td>10</td>
<td>0{1} 0{2} 0{3}</td>
<td>0{1,2,3}</td>
<td>0{1}</td>
<td>0{1} 0{2}</td>
<td>0{1} 0{2}</td>
</tr>
<tr>
<td>0.9</td>
<td>2223.62</td>
<td>10</td>
<td>0{4} 0{5}</td>
<td>0{1,2,3,4}</td>
<td>0{1}</td>
<td>0{1,2,3,4}</td>
<td>0{1} 0{2}</td>
</tr>
<tr>
<td>No knowledge</td>
<td>2659.10</td>
<td>9</td>
<td>0{1,2,4}</td>
<td>0{1} 0{2}</td>
<td>0{1}</td>
<td>1{1,2,3,4}</td>
<td>0{1,2}</td>
</tr>
</tbody>
</table>

Figure 3-7. Expected damage and optimal number of FT’s as functions of FT cost

the lower the FT attractiveness ratio $r$, the lower the optimal number of FT’s. Perhaps surprisingly, the expected damage for different values of the FT attractiveness ratio $r$ can be either greater or less than for the case of no
attacker knowledge. The ED corresponding to the case of no attacker knowledge falls between the values obtained for $r=0.5$ and $r=0.9$.

It is interesting to note that when the FT attractiveness ratio is proportional to the FT cost, the ED is relatively insensitive to the FT cost. As FT’s become both more costly and more attractive, the smaller number FT’s is compensated by their increased attractiveness. This is shown in Figure 3-8, which presents the expected damage and the optimal number of FT’s as functions of the FT cost under the assumption that $r=kd$ for some $k$. This suggests that if the function $r(d)$ increases faster than linearly, use of a smaller number of more expensive but more attractive FT’s would be beneficial. By contrast, if $r(d)$ increases more slowly than linearly, then use of a larger number of cheap FT’s is likely to be preferable.

Finally, Figure 3-9 presents the ED and the optimal number of FT’s as functions of the defense budget for a fixed FT cost and a fixed attractiveness ratio. It can be seen that the number of FT’s $F$ increases almost linearly in the budget, while the decrease in the ED slows diminishing marginal returns with increasing defensive budget.

![Figure 3-8. Expected damage and optimal number of FT's as functions of FT cost when $r=kd$](image)

7. CONCLUSIONS AND DIRECTIONS FOR FURTHER RESEARCH

The model proposed here is aimed at identifying bottlenecks in system defense and developing the optimal defense strategy under different system conditions and different attack scenarios. The combination of the universal generating function technique for evaluating expected damage, and meta-heuristics, such as the genetic algorithm, for solving complex optimization problems, allows analysts to analyze the defense of multi-state series-parallel systems of realistic size and complexity.
3. Optimizing Defense Strategies for Complex Multi-State Systems

Figure 3-9. Expected damage and optimal number of FT’s as functions of defense budget
\((d=4, r=0.5)\)

Within the suggested paradigm, the following directions of further research are suggested:

- The effect of misinforming the attacker on expected damage.
- The importance of intelligence to reduce the defender’s uncertainty about the attacker’s strategy.
- Incorporating the choice of optimal protection parameters into the defense optimization problem, in cases when the protection survivability is a continuous function of the parameters (e.g., the width of a protective casing, or the depth of an underground location).
- Optimization of system structure (type and number of system elements, and their separation and protection) for systems developed from scratch (a special case of this problem was considered in [20]).
- Optimization of system defense strategy against attacks causing multiple impacts (such as fire, debris, and pressure impulse), when different system elements have different sensitivities to these types of impacts (a special case of this problem was considered in [33]).
- Optimization of defense strategy for systems with multilevel protection (special cases of this problem were considered in [21], [22]).
- Optimization of the defense strategy for systems where functionally different elements might reside close together, and be equally susceptible to the same attack. In such systems, elements from different components could be in the same PG, so the assumption that elements belonging to the same PG form a series-parallel structure might not hold. For this case, the technique presented in [34] could be used.
• Joint optimization of system performance and defense, when improving the availability and/or performance of system elements is an alternative to reducing the expected damage.
• Optimization of dynamic defense strategy, when the attacker and the defender can change their strategies based on the results of previous attacks.
• Estimation of the possible qualitative damage caused by an attack (e.g., social, political, or environmental damage [35]).
• Optimization of the defense strategy in the case of uncertain knowledge about the system parameters and structure.
• Optimization of the defense strategy when several different types of attacks are available to the attacker.
• Optimization of the defense strategy for systems with differing structures (e.g., using the models presented in [25] to evaluate the expected damage).

REFERENCES

1. V. Bier, and V. Abhichandani, Optimal allocation of resources for defense of simple series and parallel systems from determined adversaries, Proceedings of the Engineering Foundation Conference on Risk-Based Decision making in Water Resources X. Santa Barbara, CA: American Society of Civil Engineers (2002).
Chapter 4

DEFENDING AGAINST TERRORISM, NATURAL DISASTER, AND ALL HAZARDS

Kjell Hausken, Vicki M. Bier, and Jun Zhuang

Abstract: This chapter considers both natural disasters and terrorism as threats. The defender chooses tradeoffs between investments in protection against natural disaster only, protection against terrorism only, and all-hazards protection. The terrorist chooses strategically how fiercely to attack. Three kinds of games are considered: when the agents move simultaneously; when the defender moves first; and when the terrorist moves first. Conditions are shown for when each type of agent prefers each kind of game. Sometimes their preferences for games coincide, but often their preferences are opposite. An agent advantaged with a sufficiently low normalized unit cost of investment relative to that of its opponent prefers to move first, which deters the opponent entirely, causing maximum utility for the first mover and zero utility to the deterred second mover, who prefers to avoid this game. When all-hazards protection is sufficiently cheap, it jointly protects against both the natural disaster and terrorism. As the cost increases, either pure natural disaster protection or pure terrorism protection joins in, dependent on which is more cost effective. As the unit cost of all-hazards protection increases above the sum of the individual unit costs, the extent of such protection drops to zero, and the pure forms of natural disaster protection and terrorism protection take over.

Key words: Terrorism, natural disaster, all hazards protection, unit cost of defense, unit cost of attack, contest success function.

1. INTRODUCTION

Some types of defenses are effective only against terrorism, or only against natural disaster. For example, bollards and other barriers around buildings protect only against terrorism, not against natural disaster. Similarly, improving the wetlands along a coastline protects only against
hurricanes (and some other types of natural hazards), not against terrorism. Other kinds of investment—say, emergency response (to minimize damage), or strengthening buildings (to protect against both terrorism and natural disaster)—would count as “all hazards” protection. This chapter intends to understand how a defender should allocate its investments between protecting against natural disaster, terrorism, and “all hazards.” At first glance, one might expect the unit cost of “all hazards” protection to be high, in which case protection against terrorism and natural disaster individually may be preferable. However, this will not always be the case; for example, one can imagine that improving wetlands might be so costly in some situations that it would be cheaper to harden buildings instead.

Terrorism is a subcategory of intentional attacks, and natural disasters are a subcategory of non-intentional attacks. Other examples of non-intentional attacks are technological hazards such as the Chernobyl nuclear accident, the Piper Alpha accident, etc. Other examples of intentional attacks might include acts of warfare by government actors, or criminal acts (for example, organized crime, which is generally motivated by the desire for economic rewards). Terrorism is often defined as those acts intended to create fear or “terror.” Typically, terrorism deliberately targets civilians or “non-combatants,” may be practiced either by informal groups or nation states, and is usually perpetrated to reach certain goals (as opposed to a “madman” attack), which may be ideological, political, religious, economic, or of some other nature (such as obtaining glory, prestige, fame, liberty, domination, revenge, or attention for one’s cause). For ease of exposition, this chapter refers to the tradeoff between terrorism and natural disasters, but the results could equally apply to tradeoffs between other intentional and non-intentional attacks.

As in Bier et al. (2007), games are considered in which the defender moves either before the terrorist (by implementing observable defenses), or simultaneously with the terrorist (by keeping its defenses secret). Games where the defender moves first are often realistic, since defenders often build up infrastructures over time, which terrorists take as given when they choose their attack strategies. However, games are also considered in which the terrorist acts first, leaving the defender to move second. In general, which agent moves first is likely to depend on the types of threats and defenses being considered.

Examples of cases in which the terrorist moves first are when the terrorist announces (in a manner perceived to be credible) that a new attack will occur at some point in the future, or the terrorist commits resources to such an attack and the defender gains intelligence about those investments. In such cases, the defender can take the terrorist’s decision as given when choosing its defensive strategy.
Some past work (e.g., Zhuang and Bier, 2007) concludes that the defender always has a first-mover advantage, but in practice, this cannot always be true. Therefore, this work relaxes that restriction, and makes clear how and when either side can have a first-mover advantage.

The unit costs of attack and defense are essential in determining whether the terrorist or the defender has an advantage in any given instance. The terrorist is at a disadvantage if its unit cost of attack is too high. The defender has three unit costs: one for defense against a natural disaster; one for defense against terrorism; and one for all-hazards protection. These three unit costs taken together determine how weak or strong the defender is relative to the terrorist. (A particular focus of this chapter is on how the defender chooses strategically between these three kinds of investments.)

Clausewitz (1832:6.1.2) argued for the “superiority of defense over attack,” which applies for classical warfare: “The defender enjoys optimum lines of communication and retreat, and can choose the place for battle.” Surprise is an attacker advantage, but leaving fortresses and depots behind through extended operations also leaves attackers exposed. Examples of features improving defense are the use of trenches (combined with the machine gun) in World War I, castles and fortresses with cannon fire from higher elevations, and the use of checks and guards (in the broad sense of those terms).\footnote{The superiority of the defense over the attack appears to be even larger for production facilities and produced goods than for Clausewitz’s mobile army (Hausken 2004).} In World War II, tanks and aviation technology gave some increased advantage to attackers. In the cyber context, the attacker generally has an advantage. In particular, Anderson (2001) argues that “defending a modern information system could … be likened to defending a large, thinly-populated territory like the nineteenth century Wild West: the men in black hats can strike anywhere, while the men in white hats have to defend everywhere.”

The need to trade off between protection from terrorism and natural disasters is made clear by the fact that the defender must make decisions about both, in a world of competition for scarce resources. Moreover, these decisions are sometimes made by a single organization (e.g., the Department of Homeland Security in the U.S.). In some cases, defense against both terrorism and natural disasters is possible and cost efficient. In other cases, the focus of defense may appropriately be tilted toward one type of defense, possibly even to the exclusion of the other. In analyzing both terrorism and natural disasters in the same model, we do not intend in any way to neglect the critical differences between these two types of threats. In particular, terrorism is an intentional act, by an intelligent and adaptable adversary, and the purpose of our model is precisely to determine how this fact should be taken into account in making decisions about defensive investments.
(However, since our model focuses specifically on investment in defenses, we do not consider other strategies for dealing with terrorism, such as negotiation or the threat of retaliation.)

This chapter uses contest success functions to represent the interaction between the defender on the one hand, and terrorism and the natural disaster on the other hand. Contest success functions are commonly used to represent the interactions between intelligent agents. The use of contest success functions in the case of a passive threat (the natural disaster) is perhaps somewhat unorthodox, and basically serves only as a way to specify the intensity of this threat parametrically. Unlike in the case of terrorism, our use of a contest success function for natural disaster does not assume that the disaster has a choice variable over which it can optimize.

Section 2 presents a simple model of the game we formulate to model attacker and defender investments and utilities. Section 3 analyzes the model when the defender and the terrorist move simultaneously; Section 4 lets the defender move first and the terrorist move second, in a two-period game; and Section 5 lets the terrorist move first and the defender move second. Section 6 compares the three games. Section 7 provides sensitivity-analysis results for various numerical examples, and Section 8 concludes.

2. **THE MODEL**

Consider an asset that the defender values at $r$. The asset is threatened by a natural disaster, which occurs with probability $p$, $0 \leq p \leq 1$. If not damaged by natural disaster, the asset can also be targeted by a terrorist. For simplicity, the terrorist is assumed not to attack if a natural disaster occurs. This simplification can be justified by the rare-event approximation (if damage from either terrorism or natural disaster individually is already quite unlikely), or by the assumption that a second incident of damage has at best second-order effects (Kunreuther and Heal, 2003). This latter argument seems plausible in practice—for example, New Orleans may no longer be an interesting target for a terrorist attack after Hurricane Katrina. Of course, a city already devastated by a terrorist attack could still fall victim to a natural disaster afterward, but our model neglects this possibility as a second-order consideration.

In our model, the defender incurs an effort $t_1 \geq 0$ at unit cost $b_1$ to protect against natural disaster, an effort $t_2 \geq 0$ at unit cost $b_2$ to prevent a successful terrorist attack, and an effort $t_3 \geq 0$ at unit cost $b_3$ as “all-hazards” protection. We require $b_3 > \max (b_1, b_2)$, so that all-hazards protection is never optimal for protecting against only one type of hazard.
(natural disasters or terrorism alone). The unit costs $b_i$ ($i=1, 2, 3$) are inefficiencies of investment; i.e., $1/b_i$ is the efficiency.

The terrorist values the defender’s asset at $R$, and seeks to destroy the asset (or at least part of it) by incurring an effort $T \geq 0$ at unit cost $B$. The expenditures $b_t i$ and $BT$ can reflect capital costs and/or expenses such as labor costs, while the magnitude of the natural disaster is given by a constant $D$.

We assume that the contests between the defender and the natural disaster, and between the defender and the terrorist, take a form that is common in the literature on conflict and rent seeking (Hirshleifer, 1995; Skaperdas, 1996). For the natural-disaster contest, the defender gets to retain an expected fraction $h$ of its asset where $h$ is a contest success function satisfying $\partial h/\partial t_1 > 0$, $\partial h/\partial t_3 > 0$, and $\partial h/\partial D < 0$. For the terrorist contest, the defender gets to retain an expected fraction $g$ of its asset, and the terrorist gets the remaining fraction $G = 1 - g$, where $g$ is a contest success function satisfying $\partial g/\partial t_2 > 0$, $\partial g/\partial t_3 > 0$, and $\partial g/\partial T < 0$. The fractions $h$, $g$ and $G$ can be thought of as either fractions of the asset value (if a natural disaster or terrorist attack results in partial damage), or probabilities of total destruction (if a natural disaster or terrorist attack destroys the entire asset with some probability). We use the common ratio formula (Hausken, 2005; Skaperdas, 1996; Tullock, 1980):

$$h = \frac{t_1 + t_3}{t_1 + t_3 + D}, \quad g = \frac{t_2 + t_3}{t_2 + t_3 + T}, \quad G = \frac{T}{t_2 + t_3 + T}$$

(1)

In principle, $h$, $g$ and $G$ are undefined when nobody spends any effort, but in practice this will never occur. When the terrorist exerts no effort, the status quo is assumed to be preserved, and the defender keeps the asset. Consequently, the defender’s and terrorist’s utilities are given by $u$ and $U$, respectively, where:

$^2$ Strictly speaking, the first term in the square brackets in the expression for the defender’s utility should perhaps be written as $p \min\left(\frac{t_1 + t_3}{t_1 + t_3 + D}, \frac{t_2 + t_3}{t_2 + t_3 + T}\right)$, which means that the defender’s weakest defense, whether against natural disaster or against terrorism, should determine the defender’s chance of success. In other words, the “weakest link” is what counts for the defender, and the “best shot” is what counts for the terrorist. In this model, if the defender defends equally well against natural disasters and terrorism (i.e., $t_1 + t_3 = t_2 + t_3$), and $T=D$, then one of the attacks can be ignored, since this alternative model implicitly assumes that the natural disaster and the terrorist target the same fraction of the asset value $r$. See Hausken (2002) and Hirshleifer (1983) for “weakest link” versus “best shot” analyses. The min function can be considered as representing a series system, in which both components have to be operative for the system to be operative. Use of the min
This chapter distinguishes between simultaneous and sequential games. Simultaneous games can be used even if all agents do not move simultaneously, as long as the agents moving later are unaware of any earlier actions. In other words, the crucial feature of a simultaneous game is that no agent knows any other agent’s decision at the time of its own decision. By contrast, in sequential games (sometimes also called dynamic games), those agents moving later have some (possibly quite imperfect) knowledge of earlier actions. For convenience, simultaneous games are often represented in normal form (as payoff matrices), while sequential games are usually represented in extensive form (as decision trees with nodes and branches). See e.g. Fudenberg and Tirole (1991) or Rasmusen (2001) for further discussions about games.

3. ANALYZING THE MODEL WHEN DEFENDER AND TERRORIST MOVE SIMULTANEOUSLY

The three first-order conditions for the defender, and the unique first-order condition for the terrorist, are given by

\[
\begin{align*}
\frac{\partial u}{\partial t_1} &= \frac{pDr}{(t_1 + t_3 + D)^2} - b_1 = 0, \\
\frac{\partial u}{\partial t_2} &= \frac{(1-p)Tr}{(t_2 + t_3 + T)^2} - b_2 = 0, \\
\frac{\partial u}{\partial t_3} &= \frac{pDr}{(t_1 + t_3 + D)^2} + \frac{(1-p)Tr}{(t_2 + t_3 + T)^2} - b_3 = 0, \\
\frac{\partial U}{\partial T} &= \frac{(1-p)(t_2 + t_3)R}{(t_2 + t_3 + T)^2} - B = 0
\end{align*}
\]

See Appendix 1 for the second-order conditions, which are always satisfied, and the Hessian matrix. The four equations in (3) actually have

function assumes that the terrorist undertakes attack effort $T$ regardless of the occurrence of a natural disaster with probability $p$. This alternative model formulation will be especially realistic when the terrorist moves first (before any possible natural disaster).
only three unknowns, $t_1 + t_3$, $t_2 + t_3$, and $T$. An interior solution is possible only when $b_1 + b_2 = b_3$, which causes multiple optima, and which means that investment in all-hazards protection is as effective as protection from both natural disaster and terrorism individually. Although unit costs of such sizes are realistic, the equality is unlikely to hold in practice. Hence an interior solution is unlikely, and we do not consider this case further.

The use of ratio contest success functions implies that in equilibrium, no contestant withdraws from a simultaneous game. (We define equilibrium as a solution from which no agent prefers to deviate unilaterally.) Hence, we never have $t_2 = t_3 = 0$, and we never have $T = 0$; for one of these to occur, the relevant agent would have to choose off-equilibrium behavior, which we do not consider. When $B$ is large, the terrorist chooses low $T$ and earns low utility, but prefers this over choosing $T = U = 0$. Hence, the five relevant corner solutions are $t_1 = 0$, $t_2 = 0$, $t_3 = 0$, $t_1 = t_2 = 0$, and $t_1 = t_3 = 0$, which are illustrated below.

First, consider the case when $b_1 + b_2 < b_3$. In this case, the more general all-hazards protection has a higher unit cost than the sum of the defender’s other two unit costs, yielding $t_3 = 0$. Solving the first, second, and fourth equations in (3) when $b_1 + b_2 < b_3$ gives

$$t_1 = \begin{cases} \frac{pD}{b_1/r} - D & \text{when } \frac{p}{b_1/r} \geq D, \\ 0 & \text{otherwise} \end{cases}$$

$$t_2 = \frac{(1 - p)B/R}{(B/R + b_2/r)^2},$$

$$t_3 = 0, \ T = \frac{(1 - p)b_2/r}{(B/R + b_2/r)^2},$$

$$u = \begin{cases} \left(\frac{(1 - p)(B/R)^2}{(B/R + b_2/r)^2} + \left(\sqrt{p} - \sqrt{D}b_1/r\right)^2\right) r & \text{when } \frac{p}{b_1/r} \geq D, \\ \frac{(1 - p)(B/R)^2}{(B/R + b_2/r)^2} r & \text{otherwise} \end{cases},$$

$$U = \frac{(1 - p)(b_2/r)^2}{(B/R + b_2/r)^2} R.$$

In this case, the defender invests in protection against the natural disaster, except when the natural disaster is not sufficiently damaging to justify investment in protection. If the natural disaster had been an intentional agent,
Chapter 4

$D$ would have been chosen at a level where $t_1$ would always be positive in equilibrium. However, since $D$ is exogenously given, $t_1=0$ is possible. Hence, $t_1=t_3=0$ is also possible, in contrast to the contest with the terrorist, in which $t_2=t_3=0$ is not possible.

Observe that $t_1$ is inverse $U$ shaped in $D$, and that $t_2/T = (B/R)/(b_2/r)$. Thus, the defender may choose to invest nothing in protection from natural disaster when the threat is too small, but also when the threat is so overwhelming that it cannot be countered cost-effectively. By contrast, the defender always invests in protection from terrorism, since withdrawal means losing the asset even when the terrorist invests an arbitrarily small effort. Not defending against the terrorist threat thus actually increases the threat.

Now, consider the case when $b_1+b_2>b_3$. In this case, the more general all-hazards protection has a lower unit cost than the sum of the defender’s other two unit costs. This means that either $t_1=0$ or $t_2=0$ at equilibrium. When $t_1=0$, then $t_3$ is applied against the disaster. For convenience, let $s_1 = t_1 + t_3$, and $s_2 = t_2 + t_3$. Then, solving the second, third, and fourth equations in (3) when $b_1+b_2>b_3$ gives

$$t_1 + t_3 = s_1 = \begin{cases} \sqrt{\frac{pD}{b_3-b_2}/r} - D & \text{when } \frac{p}{(b_3-b_2)/r} \geq D, \\ 0 & \text{otherwise} \end{cases}$$

$$t_2 + t_3 = s_2 = \frac{(1-p)B/R}{(B/R+b_2/r)^2}, T = \frac{(1-p)b_2/r}{(B/R+b_2/r)^2},$$

$$u = \begin{cases} \left( \frac{(1-p)(B/R)}{(B/R+b_2/r)^2} + \left( \sqrt{p} - \sqrt{D(b_3-b_2)/r} \right)^2 \right)r & \text{when } \frac{p}{(b_3-b_2)/r} \geq D, \\ \frac{(1-p)(B/R)^2}{(B/R+b_2/r)^2}r & \text{otherwise} \end{cases}$$

$$U = \frac{(1-p)(b_2/r)^2}{(B/R+b_2/r)^2}R$$

When $s_1 \leq s_2$, then equation (5) implies that the defender invests in all-hazards protection at level $s_1$, and $t_2$ provides the remaining needed defense against the terrorist. If $b_2$ is sufficiently large, then $t_2=0$. This can occur when $b_2 < b_3$, and means that all-hazards protection takes care of both the disaster and the terrorist. We do not analyze this case explicitly here, but
solving it amounts to setting $t_1=t_2=0$ and solving the third and fourth equations in (3) with respect to $t_3$ and $T$ (which gives a third-order equation).

By contrast, when $b_1+b_2>b_3$ but $t_2=0$, then $t_3$ is applied against terrorism. Solving the first, third, and fourth equations in (3) gives

$$t_1 + t_3 = s_1 = \begin{cases} \sqrt{\frac{pD}{b_1/r}} - D & \text{when } \frac{p}{b_1/r} \geq D, \\ t_3 & \text{otherwise} \end{cases}$$

$$t_2 + t_3 = s_2 = \frac{(1-p)B/R}{(B/R + (b_3-b_1)/r)^2} \text{ when } \frac{p}{b_1/r} \geq D,$$

third order expression otherwise

$$T = \begin{cases} \frac{(1-p)(b_3-b_1)/r}{(B/R + (b_3-b_1)/r)^2} & \text{when } \frac{p}{b_1/r} \geq D, \\ \text{third order expression otherwise} \end{cases}$$

$$u = \begin{cases} \frac{(1-p)(B/R)^2}{(B/R + (b_3-b_1)/r)^2} + \left(\sqrt{p} - \sqrt{Db_1/r}\right)^2 & \text{when } \frac{p}{b_1/r} \geq D, \\ \text{third order expression otherwise} \end{cases}$$

$$U = \begin{cases} \frac{(1-p)((b_3-b_1)/r)^2}{(B/R + (b_3-b_1)/r)^2} \cdot R & \text{when } \frac{p}{b_1/r} \geq D, \\ \text{third order expression otherwise} \end{cases}$$

When $s_2 \leq s_1$, equation (6) implies that the defender invests in all-hazards protection at level $s_2$, and $t_1$ provides the remaining needed defense against the natural disaster. If $b_1$ is sufficiently large, then we will have $t_1=0$. This can occur when $b_1<b_3$, and means that all-hazards protection takes care of both the disaster and the terrorist. As before, solving this case amounts to setting $t_1=t_2=0$ and solving the third and fourth equations in (3) with respect to $t_3$ and $T$ (which gives a third-order equation).
For the two-period game where the defender moves first and the terrorist moves second, the second period is solved first. The first-order condition for the terrorist is

\[
\frac{\partial U}{\partial T} = \frac{(1-p)(t_2 + t_3)R}{(t_2 + t_3 + T)^2} - B = 0 \implies T = \sqrt{(1-p)(t_2 + t_3)R/B} - (t_2 + t_3) \tag{7}
\]

The second-order conditions in Appendix 1 remain unchanged. Inserting (7) into (2) gives

\[
u = \left[ p \frac{t_1 + t_3}{t_1 + t_3 + D} + \sqrt{(1-p)(t_2 + t_3)B/R} \right] r - b_1 t_1 - b_2 t_2 - b_3 t_3 \tag{8}
\]

The first-order conditions for the defender in the first period are given by

\[
\frac{\partial u}{\partial t_1} = \frac{pDr}{(t_1 + t_3 + D)^2} - b_1 = 0 \implies t_1 + t_3 = \frac{pD}{b_1 / r} - D,
\]

\[
\frac{\partial u}{\partial t_2} = \frac{\sqrt{(1-p)B/R} - b_2}{2\sqrt{t_2 + t_3}} = 0 \implies t_2 + t_3 = \frac{(1-p)B/R}{4(b_2 / r)^2}, \tag{9}
\]

\[
\frac{\partial u}{\partial t_3} = \frac{pDr}{(t_1 + t_3 + D)^2} + \frac{\sqrt{(1-p)B/R}}{2\sqrt{t_2 + t_3}} r - b_3 = 0
\]

See Appendix 2 for the second-order conditions, which are always satisfied, and the Hessian matrix. As in the previous section, we distinguish between three cases. First, \(b_1 + b_2 < b_3\) causes \(t_3 = 0\). Solving the first two equations in (10), and inserting into (8) and (2), gives
4. Defending against Terrorism, Natural Disaster, and All Hazards

When $2b_2/r - B/R < 0$, the terrorist withdraws from the contest which causes a contest between the defender and the natural disaster, which we do not consider.

Second, consider the case where $b_1 + b_2 > b_3$ and $t_1 = 0$. Solving the second and third equations in (9), and inserting into (7) and (2), gives

$$
t_1 + t_3 = s_1 = \begin{cases} 
\sqrt{\frac{pD}{b_1/r}} - D \text{ when } \frac{p}{b_1/r} \geq D, \\
0 \text{ otherwise}
\end{cases}
$$

$$
t_2 + t_3 = s_2 = \frac{(1-p)B/R}{4(b_2/r)^2},
$$

$$
T = \frac{(1-p)[2b_2/r - B/R]}{4(b_2/r)^2},
$$

$$
U = \frac{(1-p)(2b_2/r - B/R)^2}{4(b_2/r)^2} R,
$$

$$
u = \begin{cases} 
\left(\frac{(1-p)B/R}{4b_2/r} + \left(\sqrt{p - \sqrt{Db_1/r}}\right)^2\right) r \text{ when } \frac{p}{b_1/r} \geq D, \\
\frac{(1-p)B/R}{4b_2/r} r \text{ otherwise}
\end{cases}
$$
When \(2b_2 / r - B/R < 0\), the terrorist withdraws from the contest, which causes a contest between the defender and the natural disaster, which we do not consider.

Third, consider the case where \(b_1 + b_2 > b_3\) and \(t_2 = 0\). Solving the first and third equations in (8), and inserting into (7) and (2), gives

\[
t_1 + t_3 = \begin{cases} \frac{pD}{b_1 / r} - D & \text{when } \frac{p}{b_1 / r} \geq D, \\ t_3 & \text{otherwise} \end{cases}
\]

\[
t_2 = 0, t_3 = \begin{cases} \frac{(1-p)B / R}{4((b_3 - b_1) / r)^2} & \text{when } \frac{p}{b_1 / r} \geq D, \\ \text{fifth order expression otherwise} \end{cases}
\]

\[
T = \begin{cases} \frac{(1-p)[2(b_3 - b_1) / r - B / R]}{4((b_3 - b_1) / r)^2} & \text{when } \frac{p}{b_1 / r} \geq D, \\ \text{fifth order expression otherwise} \end{cases}
\]

\[
u = \begin{cases} \frac{(1-p)B / R + \left(\sqrt{p - \sqrt{D b_1 / r}}\right)^2}{4(b_3 - b_1) / r} & \text{when } \frac{p}{b_1 / r} \geq D, \\ \text{fifth order expression otherwise} \end{cases}
\]

\[
U = \begin{cases} \frac{(1-p)(2(b_3 - b_1) / r - B / R)^2}{4((b_3 - b_1) / r)^2} R & \text{when } \frac{p}{b_1 / r} \geq D, \\ \text{fifth order expression otherwise} \end{cases}
\]

The fifth-order equations that result when the natural disaster is highly damaging can be solved numerically, but are too complicated to present here. When \(2(b_3 - b_1) / r - B/R < 0\), the terrorist withdraws from the contest, which causes a contest between the defender and the natural disaster, which we again do not consider.

5. **ANALYZING THE MODEL WHEN TERRORIST MOVES FIRST AND DEFENDER MOVES SECOND**

For the two-period game where the terrorist moves first (say, by committing to a specific plan of attack) and the defender moves second, the second period is again solved first. (We assume that the attacker cannot change its strategy after having chosen it, and that the contest takes place
4. Defending against Terrorism, Natural Disaster, and All Hazards

after the defender has chosen its strategy.) The first-order conditions for the defender in this case are

\[
\frac{\partial u}{\partial t_1} = \frac{pD}{(t_1 + t_3 + D)^2} - b_1 = 0 \quad \Rightarrow \quad t_1 + t_3 = \sqrt{\frac{pD}{b_1}} - D,
\]

\[
\frac{\partial u}{\partial t_2} = \frac{(1 - p)T}{(t_2 + t_3 + T)^2} - b_2 = 0 \quad \Rightarrow \quad t_2 + t_3 = \sqrt{(1 - p)T} / b_2 - T,
\]

\[
\frac{\partial u}{\partial t_3} = \frac{pD}{(t_1 + t_3 + D)^2} + \frac{(1 - p)T}{(t_2 + t_3 + T)^2} - b_3 = 0
\]

Since the defender’s optimization problem remains the same as in Section 3, the second-order condition verification remains the same.

We distinguish between three cases. First, \(b_1 + b_2 < b_3\) causes \(t_3 = 0\).

Inserting the second equation in (13) into (2) gives

\[
U = R\sqrt{(1 - p)T} / r - BT
\]

The first-order condition for the terrorist in the first period is

\[
\frac{\partial U}{\partial T} = \frac{\sqrt{(1 - p)T}}{2\sqrt{T}} R - B = 0 \quad \Rightarrow \quad T = \frac{(1 - p)b_2}{4(B / R)^2}
\]

The second-order condition is satisfied; i.e.

\[
\frac{\partial^2 U}{\partial T^2} = -\frac{\sqrt{(1 - p)b_2}}{4T^{3/2}} R < 0
\]

Inserting (15) into (13) and (2) when \(b_1 + b_2 < b_3\) gives
When \( 2B/R - b_2/r < 0 \), the defender withdraws from the contest with the terrorist, setting \( t_2 = t_3 = 0 \). The terrorist earns \( U = (1 - p) R - B T \), with investment \( T \) defined in (17). The contest with the natural disaster remains, and the defender invests \( t_1 \) in this contest.

Second, we consider \( b_1 + b_2 > b_3 \) and \( t_1 = 0 \). Equations (14)–(16) remain as before. Inserting (15) into (13) and (2) gives

\[
t_1 + t_3 = s_1 = \begin{cases} \sqrt{\frac{pD}{b_3 - b_2}} - D \text{ when } \frac{p}{b_3 - b_2} \geq D, \\ 0 \text{ otherwise} \end{cases}
\]

\[
t_2 + t_3 = s_2 = \frac{(1 - p)[2B / R - b_2 / r]}{4(B / R)^2},
\]

\[
T = \frac{(1 - p)b_2 / r}{4(B / R)^2}, \quad U = \frac{(1 - p)b_2 / r}{4B / R} R,
\]

\[
u = \begin{cases} \left( \frac{(1 - p)(2B / R - b_2 / r)^2}{4(B / R)^2} \right)^{s_2} + \left( \frac{p}{(b_3 - b_2) / r} \right)^{s_3} - D \frac{b_3 - b_2}{r} \right)^2} \right) \text{ when } \frac{p}{b_3 - b_2} \geq D, \\ \frac{(1 - p)(2B / R - b_2 / r)^2}{4(B / R)^2} \text{ otherwise} \end{cases}
\]
When $2B/R - b_2/r < 0$, the defender withdraws from investing directly in the contest with the terrorist, setting $t_2 = 0$, while $t_3$ provides protection against both the natural disaster and the terrorist.

Third, we consider $b_1 + b_2 > b_3$ and $t_2 = 0$. Solving the first and third equations in (13) gives

$$t_3 = \sqrt{\frac{(1-p)T}{r}(b_3 - b_1)} - T$$  \hspace{1cm} (19)

Observe that (19) is similar to the second equation in (15), but with $b_2$ replaced by $b_3 - b_1$. Inserting (19) into (2) gives

$$U = R\sqrt{\frac{(1-p)T}{r}(b_3 - b_1)} - BT$$ \hspace{1cm} (20)

The first-order condition for the terrorist in the first period is

$$\frac{\partial U}{\partial T} = \frac{\sqrt{(1-p)(b_3 - b_1)/r}}{2\sqrt{T}} R - B = 0 \Rightarrow T = \frac{(1-p)(b_3 - b_1)/r}{4(B/R)^2}$$ \hspace{1cm} (21)

The second-order condition is always negative; i.e.

$$\frac{\partial^2 U}{\partial T^2} = -\frac{\sqrt{(1-p)(b_3 - b_1)/r}}{4T^{3/2}} R < 0$$ \hspace{1cm} (22)

Observe that (20)–(22) are equivalent to (14)–(16), but with $b_2$ again replaced by $b_3 - b_1$. Inserting (21) into (13) and (2) gives
\( t_1 + t_3 = s_1 = \begin{cases} \frac{pD}{b_1 / r} - D \text{ when } \frac{p}{b_1 / r} \geq D, \\ t_3 \text{ otherwise} \end{cases} \)

\( t_2 + t_3 = s_2 = \begin{cases} \frac{(1 - p)(2B / R - (b_3 - b_1) / r)}{4(B / R)^2} \text{ when } \frac{p}{b_1 / r} \geq D, \\ \text{higher order expression otherwise} \end{cases} \)

\( T = \begin{cases} \frac{(1 - p)(b_3 - b_1) / r}{4(B / R)^2} \text{ when } \frac{p}{b_1 / r} \geq D, \\ \text{higher order expression otherwise} \end{cases} \)

\( U = \begin{cases} \frac{(1 - p)(b_3 - b_1) / r}{4B / R} R \text{ when } \frac{p}{b_1 / r} \geq D, \\ \text{higher order expression otherwise} \end{cases} \)

\( u = \begin{cases} \frac{(1 - p)(2B / R - (b_3 - b_1) / r)^2}{4(B / R)^2} + \left(\sqrt{p} - \sqrt{Db_1 / r}\right)^2 \text{ when } \frac{p}{b_1 / r} \geq D, \\ \text{higher order expression otherwise} \end{cases} \)

(As before, the higher-order expressions can be evaluated numerically.)

When \(2B/R - (b_3 - b_1)/r < 0\), the defender withdraws from the contest with the terrorist, setting \(t_2 = t_3 = 0\). The terrorist earns \(U = (1 - p) R - B T\), where \(T\) is determined by (23). The contest with the natural disaster remains, and the defender invests \(t_1\). In the special case where \(t_1 = t_2 = 0\), inserting \(t_1 = t_2 = 0\) into the third equation in (13) and solving with respect to \(t_3\) gives a fourth-order equation for \(t_3\) as a function of \(T\). Inserting this value of \(t_3\) into (2) gives the terrorist’s first-period utility.

6. **COMPARING THE THREE GAMES**

Tables 4-1 to 4-3 below compare the equilibrium levels of effort and utilities, respectively, for the three games outlined above. For simplicity, these tables do not show the expressions that apply when one agent is completely deterred. Table 4-3 assumes \(p/(b_1 / r) \geq D\) since the higher order expressions in (6), (12), (23) are either voluminous or intractable; hence, the max operator is not needed in the expressions for \(s_1\) and \(u\).
4. Defending against Terrorism, Natural Disaster, and All Hazards

Table 4-1. Equilibrium efforts and utilities for the three games when \( b_1 + b_2 < b_3, t_3 = 0, 0 \leq p \leq 1 \)

<table>
<thead>
<tr>
<th></th>
<th>( t_1 )</th>
<th>( t_2 )</th>
<th>( T )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simultaneous game</td>
<td>( \max \left{ 0, \sqrt{pD / b_3} - D \right} )</td>
<td>( (1 - p)B / R ) ( \frac{B / R + b_3 / r}{(B / R + b_3 / r)^2} )</td>
<td>( (1 - p)b_3 / r ) ( \frac{B / R + b_3 / r}{(B / R + b_3 / r)^2} )</td>
</tr>
<tr>
<td>Defender moves first</td>
<td>( (1 - p)B / R ) ( \frac{4(b_3 / r)^2}{4(b_3 / r)^2} )</td>
<td>( (1 - p)[2b_3 / r - B / R] ) ( \frac{4(b_3 / r)^2}{4(b_3 / r)^2} )</td>
<td>( (1 - p)b_3 / r ) ( \frac{B / R}{4B / R} )</td>
</tr>
<tr>
<td>Terrorist moves first</td>
<td>( (1 - p)[2B / R - b_3 / r] ) ( \frac{4(B / R)^2}{4(B / R)^2} )</td>
<td>( (1 - p)b_3 / r ) ( \frac{4(B / R)^2}{4(B / R)^2} )</td>
<td>( u ) ( U )</td>
</tr>
</tbody>
</table>

Simultaneous game for both Defender and Terrorist moves first:

- Defender moves first:
  \( \left( 1 - p \right) \left( \frac{B / R + b_3 / r}{4b_3 / r} \right) + \left( \max \left\{ 0, \sqrt{p - \sqrt{D(b_3 - b_2) / r}} \right\} \right) r \)
  \( \frac{(1 - p)b_3 / r}{(B / R + b_3 / r)^2} \)

- Terrorist moves first:
  \( \left( 1 - p \right) \left( \frac{2B / R - b_3 / r}{4B / R} \right) + \left( \max \left\{ 0, \sqrt{p - \sqrt{D(b_3 - b_2) / r}} \right\} \right) r \)
  \( \frac{(1 - p)b_3 / r}{(B / R + b_3 / r)^2} \)

Table 4-2. Equilibrium efforts and utilities for the three games when \( b_1 + b_2 < b_3, t_1 = 0, 0 \leq p \leq 1 \)

<table>
<thead>
<tr>
<th></th>
<th>( t_3 )</th>
<th>( s_2 = t_2 + t_3 )</th>
<th>( T )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simultaneous game</td>
<td>( \max \left{ 0, \sqrt{pD / (b_3 - b_2)} - D \right} )</td>
<td>( (1 - p)B / R ) ( \frac{B / R + b_3 / r}{(B / R + b_3 / r)^2} )</td>
<td>( (1 - p)b_3 / r ) ( \frac{B / R + b_3 / r}{(B / R + b_3 / r)^2} )</td>
</tr>
<tr>
<td>Defender moves first</td>
<td>( (1 - p)B / R ) ( \frac{4(b_3 / r)^2}{4(b_3 / r)^2} )</td>
<td>( (1 - p)[2b_3 / r - B / R] ) ( \frac{4(b_3 / r)^2}{4(b_3 / r)^2} )</td>
<td>( (1 - p)b_3 / r ) ( \frac{4(B / R)^2}{4(B / R)^2} )</td>
</tr>
<tr>
<td>Terrorist moves first</td>
<td>( (1 - p)[2B / R - b_3 / r] ) ( \frac{4(B / R)^2}{4(B / R)^2} )</td>
<td>( (1 - p)b_3 / r ) ( \frac{4(B / R)^2}{4(B / R)^2} )</td>
<td>( u ) ( U )</td>
</tr>
</tbody>
</table>

Since \( b_1 + b_2 < b_3 \), which causes \( t_3 = 0 \) in Table 4-1, no variables depend on \( b_3 \).

Since \( b_1 + b_2 > b_3 \) and \( t_1 = 0 \) in Table 4-2, no variables depend on \( b_1 \). The defender substitutes optimally between \( t_2 \) and \( t_3 \) so that \( s_2 = t_2 + t_3 \), and the terrorist’s investment \( T \) and utility \( U \) do not depend on \( b_3 \). In this substitution, only \( t_3 \) affects the risk from the natural disaster. Hence, \( s_2, T, U \) do not depend on \( b_3 \).
Table 4-3. Equilibrium efforts and utilities for the three games when \( b_1 + b_2 < b_3, t_2 = 0, \) and \( p / (b_1/r) \geq D \)

<table>
<thead>
<tr>
<th>Simultaneous game</th>
<th>( s_1 = t_1 + t_3 )</th>
<th>( t_3 )</th>
<th>( T )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defender moves first</td>
<td>( \sqrt{\frac{pD}{b_1/r} - D} )</td>
<td>( \frac{(1-p)(B/R)^2}{(B/R + (b_3 - b_1)/r)^2} + \left( \sqrt{p - \sqrt{Dh_1/r^2}} \right)^2 )</td>
<td>( \frac{(1-p)(b_3 - b_1)/r}{(B/R + (b_3 - b_1)/r)^2} )</td>
</tr>
<tr>
<td>Terrorist moves first</td>
<td>( \frac{(1-p)(2B/R - (b_3 - b_1)/r)}{4(B/R)^2} )</td>
<td>( \frac{(1-p)(b_3 - b_1)/r}{4(B/R)^2} )</td>
<td></td>
</tr>
</tbody>
</table>

and \( U \) depend only on \( b_2, B, r, R, \) and \( p. \) However, the defender’s investment \( t_3 \) in all-hazards protection decreases as \( b_2 \) increases above \( b_2, \) which causes the defender’s utility also to decrease as \( b_3 \) increases above \( b_2, \) since \( T \) is independent of \( b_3. \)

Since \( b_1 + b_2 > b_3 \) and \( t_2 = 0 \) in Table 4-3, no variables depend on \( b_2. \)

Roles are changed compared with Table 4-2. The defender substitutes optimally between \( t_1 \) and \( t_3 \) so that \( t_1 + t_3 \) does not depend on \( b_3 \) (although \( t_3, T, \) and \( U \) depend on the extent to which \( b_3 > b_2 \)). In this substitution, only \( t_3 \) affects the terrorist. Both the defender’s investment \( t_3 \) in all-hazards protection and the defender’s utility \( u \) decrease as \( b_3 \) increases above \( b_1. \)

When the terrorist moves first, its investment and utility increase in \( b_3. \) In other words, the terrorist benefits from a high unit cost of all-hazards defense. The first-order derivatives \( \partial T / \partial b_3 \) and \( \partial U / \partial b_3 \) in Table 4-3 are straightforward to set up, but are not discussed here, since they can be either positive or negative (depending on the parameter values), and their interpretation is complicated to explain.

Table 4-4 compresses Tables 4-1 to 4-3 into one table. In particular, Table 4-4 is equivalent to Table 4-1 \( (b_1 + b_2 < b_3, t_3 = 0) \) when \( b_v = b_1, b_w = b_2, x = t_1, \) and \( y = t_2. \) Table 4-4 gives Table 4-2 \( (b_1 + b_2 > b_3, t_1 = 0) \) when \( b_v = b_3 - b_2, b_w = b_2, x = t_3, \) and \( y = t_2 + t_3. \) Finally, Table 4-4 gives Table 4-3 \( (b_1 + b_2 > b_3, t_2 = 0) \) when \( b_v = b_1, b_w = b_2 - b_1, x = t_1 + t_3, \) and \( y = t_3, \) assuming \( p / (b_1/r) \geq D \). In this notation, \( x \) is the defense against the natural
disaster \((t_1, t_3, \text{ or } t_1 + t_3)\), and \(y\) is the defense against terrorism \((t_2, t_3, \text{ or } t_2 + t_3)\).

We first consider the efforts. For the simultaneous game, the defender’s effort \(y\) in defense against terrorism increases in the terrorist’s unit cost \(B\) divided by the terrorist’s valuation \(R\) when the normalized marginal cost of terrorism defense, \(b_w/r\), is greater than \(B/R\), and otherwise decreases in \(B/R\). Analogously, the terrorist’s effort \(T\) increases in the defender’s normalized marginal cost of terrorism defense \(b_w/r\) is greater than \(B/R\), and otherwise decreases in \(b_w/r\).

Evidently, when all-hazards protection is sufficiently cheap, it replaces both pure natural disaster protection and pure terrorism protection.

\[
\text{Table 4-4. Equilibrium efforts and utilities for the three games}
\]

<table>
<thead>
<tr>
<th>Effort</th>
<th>(x)</th>
<th>(y)</th>
<th>(T)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simultaneous game</td>
<td>(\max \left{ 0, \frac{pD}{b_w/r} - D \right} )</td>
<td>(\frac{(1-p)B/R}{(B/R + b_w/r)^2} ) (\frac{(1-p)b_w/r}{(B/R + b_w/r)^2} )</td>
<td>(\frac{(1-p)B/R}{4(b_w/r)^2} ) (\frac{(1-p)(2b_w/r - B/R)}{4(b_w/r)^2} )</td>
</tr>
<tr>
<td>Defender moves first</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terrorist moves first</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(u)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simultaneous Game</td>
<td>(\frac{(1-p)B/R}{(B/R + b_w/r)^2} + \left( \max \left{ 0, \sqrt{p - \sqrt{Db_w/r}} \right} \right)^2 ) (\frac{(1-p)(b_w/r)^2}{B/R + b_w/r)^2} )</td>
<td>(\frac{(1-p)B/R}{4(b_w/r)^2} ) (\frac{(1-p)(b_w/r)^2}{4(b_w/r)^2} )</td>
<td>(\frac{(1-p)B/R}{4(B/R)^2} ) (\frac{(1-p)(2b_w/r - B/R)^2}{4(b_w/r)^2} )</td>
</tr>
<tr>
<td>Defender moves first</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terrorist moves first</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Proposition 1:**
When the defender moves first, its effort \(y\) is higher than in the simultaneous game when

\[
b_w/r < B/R \tag{24}
\]

When the defender moves first, the terrorist is deterred from incurring effort when \(2b_w/r < B/R\), in which case the terrorist chooses \(T = 0\) and earns zero utility.

**Proof:**
Follows from Table 4-4.
In other words, with a sufficiently low unit cost of defense, or a sufficiently high asset value, the defender can deter the terrorist altogether.

**PROPOSITION 2:**
When the terrorist moves first, its effort is higher than in the simultaneous game when the inequality in (24) is reversed; that is, when

\[ \frac{B}{R} < \frac{b_w}{r} \]  \hspace{1cm} (25)

Here again, when the terrorist moves first, the defender is deterred from incurring effort when \( \frac{B}{R} < \frac{b_w}{2r} \), in which case the defender chooses \( t_z = 0 \), loses its asset, and earns zero utility.

**PROOF:**
Follows from Table 4-4.

As with the defender, if the terrorist has a sufficiently low unit cost of attack or a sufficiently high asset value, it can deter the defender from investing in protection from terrorism altogether.

Let us now consider the utilities of the two agents.

**PROPOSITION 3:**
(a) Over the three games, both the defender and the terrorist always prefer the game in which they move first rather than a simultaneous game. (b) The defender prefers the terrorist to move first rather than herself to move first if and only if \( 1 < \frac{B}{R} \frac{b_w}{r} < 2.62 \). (c) The terrorist prefers the defender to move first rather than moving first itself if and only if \( 0.38 < \frac{B}{R} \frac{b_w}{r} < 1 \). (d) The defender prefers a simultaneous game rather than allowing the terrorist to move first if and only if \( 0 < \frac{B}{R} \frac{b_w}{r} < 1 \). (e) The terrorist prefers a simultaneous game rather than allowing the defender to move first if and only if \( \frac{B}{R} \frac{b_w}{r} > 1 \).

**PROOF:**
See Appendix 3.

Proposition 3 is illustrated in Figure 4-1. When the terrorist is advantaged with a low unit cost, it prefers to move first due to its relative strength, which
the defender seeks to avoid. Conversely, when the terrorist is disadvantaged with a high unit cost, it prefers to move first to prevent being deterred from attacking at all, while the defender prefers to deter an attack through its first-mover advantage. When $0.38 < (B/R)/(b_w/r) < 1$, both agents prefer that the defender moves first, and when $1 < (B/R)/(b_w/r) < 2.62$, both agents prefer that the terrorist moves first. At the transition points 0.38, 1, 2.62, the agents are indifferent between the two neighboring strategies.

![Figure 4-1](image)

**Figure 4-1.** Defender and terrorist preferences when accounting for all preference orders

7. **SENSITIVITY ANALYSIS AS PARAMETERS VARY**

The base-case parameter values for the sensitivity analyses given in this section are $b_1 = b_2 = B = 0.5$, $b_3 = r = R = 1$, $p = 0.2$, $D = 0.05$. This means that the unit costs of defense against the natural disaster and terrorism are equal, and equal to the terrorist’s unit cost, while all-hazards protection is twice as expensive. While the case with equal unit costs may be unlikely to occur in practice (just as any other choice may be unlikely), it makes it easy to show the effects of changing any one parameter. The probability of a natural disaster is 20%, the defense against it is fixed at 0.05, and the defender and terrorist value the asset equally at one.

Figure 4-2 shows $t_1$, $t_2$, $t_3$, $T$, $u$, and $U$ for all three games, as functions of $b_1$. The defender’s investment $t_1$ against the natural disaster and its utility $u$ decrease convexly in $b_1$ when $b_1 < 0.5$. These variables are determined by (4). At $b_1 = b_2 = 0.5$, $t_1$ becomes too expensive and drops from 0.09 to zero, $t_2$ drops from 0.4 to 0.31, and all-hazards protection $t_3$ takes over.
Figure 4-2. $t_1, t_2, t_3, T, u, U$ as functions of $b_1$ for all three games.

Figure 4-3 shows the same six variables as functions of $b_2$ for the simultaneous game. The defender’s investment $t_2$ against terrorism and utility $u$ decrease convexly in $b_2$ when $b_2 < 0.5$. At $b_2 = b_1 = 0.5$, $t_2$ and $t_1$ make downward shifts such that $t_1 = 0$ when $b_2 > 0.5$, while $t_3$ makes an upwards shift. As $b_2$ increases above 0.5, defense against terrorism becomes increasingly expensive, and $t_2$ decreases, reaching zero at $b_2 = 0.86$. For $0.86 < b_2 < 1$, all-hazard protection single-handedly takes care of both the natural disaster and terrorism. The inverse $U$ shape for the terrorist’s investment $T$ is commonly observed in contests of this kind (Hausken 2006). When $b_2$ is low, the terrorist is overwhelmed by the solid defense and withdraws due to weakness. When $b_2$ is high, there is no need for the terrorist to invest heavily, since the defense is weak. As we might expect, the defender’s utility $u$ decreases while the terrorist’s utility $U$ increases as $b_2$ increases.

Figure 4-3. $t_1, t_2, t_3, T, u, U$ as functions of $b_2$ for the simultaneous move game
Figure 4-4, for the game in which the defender moves first, is roughly similar, except that when $b_2 < 0.25$, the terrorist is completely deterred (in accord with Proposition 1), since $2b_2/r < B/R$. Figure 4-5 shows the six variables as functions of $b_2$ for the game when the terrorist moves first. For the particular parameter values used in Figure 4-5, the defender is not deterred from investing in protection from terrorism, in contrast to Figure 4-4, in which the terrorist is deterred. Like Figure 4-4, Figure 4-5 is roughly similar to Figure 4-3, except that $T$ is not inverse $U$ shaped, and instead is always increasing in $b_2$. The terrorist’s utility also increases in $b_2$. This means that when the terrorist moves first and $b_2$ is large, it must invest heavily to prevent being countered by heavy defensive investment after the fact. The terrorist has a first mover disadvantage when $0.5 < b_2 < 0.79$ in Figure 4-5. The range $0.5 < b_2 = b_w < 0.79$ in Table 4-2, which with the given parameters can be written as $0.63 < b_w / r < 1$, is thus also such, according to Figure 4-1, that both agents prefer the defender to move first.

Figure 4-6 shows the six variables as functions of $b_3$ for the simultaneous game when $b_1 = B = 0.5$, $b_2 = 0.72$, $r = R = 1$, $p = 0.2$, $D = 0.05$. When $b_3 < 0.82$, all-hazard protection takes care of all needed protection. As $b_3$ increases above 0.82, all-hazard protection starts getting expensive, and it becomes preferable to use some pure terrorism protection. Hence, $t_2$ increases, while $t_3$ decreases. As $b_3$ increases above $b_1 + b_2 = 1.22$, all-hazard protection vanishes as being too expensive, causing $t_3 = 0$, pure natural disaster protection $t_1$ jumps from 0 to 0.09, and pure terrorism protection $t_2$ jumps from 0.18 to 0.27. The terrorist’s investment and utility

![Figure 4-4. $t_1, t_2, t_3, T, u, U$ as functions of $b_2$ when defender moves first](image)
Figure 4-5. $t_1, t_2, t_3, T, u, U$ as functions of $b_2$ when terrorist moves first.

Figure 4-6. $t_1, t_2, t_3, T, u, U$ as functions of $b_3$ for the simultaneous move game. No natural disaster protection when $b_3 < 1.22$.

are constant, and the defender’s utility decreases in $b_3$ over the range $0.82 < b_3 < 1.22$.

Figure 4-7 shows the six variables as functions of $b_3$ for the simultaneous game when $b_1 = 0.5$, $b_2 = 0.6$, $B = 1.5$, $r = R = 1$, $p = 0.5$, $D = 0.2$. (Note that the defender’s utility has been divided by 3 in this figure, for scaling purposes.) When $b_3 < 0.74$, all-hazard protection takes care of all protection. As $b_3$ increases above 0.74, all-hazard protection starts getting expensive, and it is preferable for an alternative means of protection to take over. Whereas pure terrorism protection starts taking over in Figure 4-6, in Figure 4-7 it is preferable for pure natural disaster protection to take over. Hence, $t_1$ increases, while $t_2$ remains at $t_2 = 0$. As $b_3$ increases above $b_1 + b_2 = 1.1$, the same logic as in Figure 4-6 applies. All-hazard protection vanishes
4. Defending against Terrorism, Natural Disaster, and All Hazards

Figure 4-7. $t_1, t_2, t_3, T, u, U$ as functions of $b_3$ for the simultaneous move game. No pure terrorism protection when $b_3 < 1.1$

as being too expensive, causing $t_3 = 0$; natural disaster protection $t_1$ jumps from 0.08 to 0.25; and pure terrorism protection $t_2$ jumps from 0 to 0.17. The terrorist’s investment and utility now do depend on $b_3$, and increase as $b_3$ increases, while the defender’s utility decreases in $b_3$, as we might expect.

8. CONCLUSIONS

This chapter considers two threats, natural disaster and terrorism, from which a defender can protect through three kinds of investments. These defenses are against the disaster only, against terrorism only, or against all hazards. The defender makes tradeoffs between these three kinds of investments, under the assumption that the terrorist chooses optimally how fiercely to attack, there is a fixed probability of a natural disaster of an exogenously determined magnitude, and the defender and terrorist can have different evaluations of the asset that the defender seeks to protect.

Three kinds of games are considered: when the agents move simultaneously; when the defender moves first; and when the terrorist moves first. Conditions are shown for when each agent prefers each kind of game. Sometimes their preferences coincide, but often their preferences are opposite.

A crucial insight is that an agent advantaged with a low unit cost of investment prefers to move first, which deters its opponent from investing at all, causing maximum utility for the first mover and zero utility to the deterred second mover, who prefers to avoid this game. However, perhaps
surprisingly, there are also cases in which an agent prefers to force its opponent to pre-commit to a given level of investment. When all-hazards protection is sufficiently cheap, it jointly protects against both the natural disaster and terrorism, with no need for either pure natural disaster protection or pure terrorism protection. As the cost of all-hazards protection increases above a certain level, either pure natural disaster protection or pure terrorism protection (but not both) joins in as supportive of all-hazards protection. As the unit cost of all-hazards protection increases further, it eventually reaches a level where pure natural disaster protection and pure terrorism protection become more cost effective, at which point all-hazards protection drops to zero.

To understand the implications of these results, when protecting targets that have relatively low value to potential terrorists (if only because the terrorists can easily substitute some other target of comparable value), defenders will more often wish to invest in protection from natural disasters and/or all-hazards protection, and less often wish to invest in protection against terrorism alone. For the same reason, protections that are effective against only a relatively narrow range of terrorist threats (such as defending a specific target) may be less desirable than investments that protect against a broader range of threats (such as protecting an entire country through improved border security). However, one caveat to this conclusion is that the history of large-scale natural disasters is much longer than the history of large-scale terrorism. This suggests that any one terrorist attack contains much more “signal value” than any one natural disaster, and argues for protecting against potentially catastrophic forms of terrorism (but not necessarily against terrorist threats with lesser consequences).

A key caveat in this work is that throughout this chapter, the expenditures increase linearly in the investments. Future research may allow the expenditures to depend non-linearly on the investments, or let the unit costs depend on the levels of investment; e.g., showing diminishing marginal returns to investment in both attack and defense.

REFERENCES


Clausewitz, C. V., 1984, 1832, On War, Princeton University Press.


ACKNOWLEDGEMENT

We thank a referee for useful comments.

This research was partially supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number 2007-ST-061-000001. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security.
APPENDIX 1: VERIFICATION OF SECOND-ORDER CONDITIONS FOR SECTION 3

For the terrorist’s optimization problem, the second-order condition is trivial; there is only one decision variable, $T$, so the fact that \[
\frac{\partial^2 U}{\partial T^2} = -\frac{2(1-p)(t_2 + t_3)R}{(t_2 + t_3 + T)^2} < 0
\]
is sufficient. For the defender’s optimization problem, since there are three decision variables ($t_1$, $t_2$, and $t_3$), we want to see that the corresponding Hessian matrix is negative semi-definite:

\[
H = \begin{bmatrix}
\frac{\partial^2 u}{\partial t_1^2} & \frac{\partial^2 u}{\partial t_1 \partial t_2} & \frac{\partial^2 u}{\partial t_1 \partial t_3} \\
\frac{\partial^2 u}{\partial t_2 \partial t_1} & \frac{\partial^2 u}{\partial t_2^2} & \frac{\partial^2 u}{\partial t_2 \partial t_3} \\
\frac{\partial^2 u}{\partial t_3 \partial t_1} & \frac{\partial^2 u}{\partial t_3 \partial t_2} & \frac{\partial^2 u}{\partial t_3^2}
\end{bmatrix}
\]

\[
= \begin{bmatrix}
\frac{-2pDr}{(t_1 + t_3 + D)^3} & 0 & \frac{-2pDr}{(t_1 + t_3 + D)^3} \\
0 & \frac{-2(1-p)Tr}{(t_2 + t_3 + T)^3} & \frac{-2(1-p)Tr}{(t_2 + t_3 + T)^3} \\
\frac{-2pDr}{(t_1 + t_3 + D)^3} & \frac{-2(1-p)Tr}{(t_2 + t_3 + T)^3} & \frac{-2(1-p)Tr}{(t_2 + t_3 + T)^3}
\end{bmatrix}
\] (A1)

In order to show that $H$ is negative semi-definite, it is sufficient to show the following three conditions: (1) $|H_{11}| \leq 0$; (2) $\begin{bmatrix} H_{11} & H_{12} \\ H_{21} & H_{22} \end{bmatrix} \begin{bmatrix} H_{13} \\ H_{31} \end{bmatrix} = H$; and (3) $|H| \leq 0$. The first condition obviously holds, because $|H_{11}| = H_{11} = \frac{-2pDr}{(t_1 + t_3 + D)^3} < 0$. The second condition also holds, since

\[
\begin{bmatrix} H_{11} & H_{12} \\ H_{21} & H_{22} \end{bmatrix} = H_{11}H_{22} - H_{12}H_{21} = \begin{bmatrix} \frac{2pDr}{(t_1 + t_3 + D)^3} & \frac{2(1-p)Tr}{(t_2 + t_3 + T)^3} \end{bmatrix}
\]

Finally, the third condition holds, since we have
This completes the verification.

**APPENDIX 2: VERIFICATION OF SECOND-ORDER CONDITIONS FOR SECTION 4**

Since the terrorist’s optimization problem remains the same as in Section 3, the second-order condition is still satisfied. For the defender’s optimization problem in Equation (8), again we want to see that the corresponding Hessian matrix is negative semi-definite:

\[
H = \begin{bmatrix}
\frac{\partial^2 u}{\partial t_1^2} & \frac{\partial^2 u}{\partial t_1 \partial t_2} & \frac{\partial^2 u}{\partial t_1 \partial t_3} \\
\frac{\partial^2 u}{\partial t_2 \partial t_1} & \frac{\partial^2 u}{\partial t_2^2} & \frac{\partial^2 u}{\partial t_2 \partial t_3} \\
\frac{\partial^2 u}{\partial t_3 \partial t_1} & \frac{\partial^2 u}{\partial t_3 \partial t_2} & \frac{\partial^2 u}{\partial t_3^2}
\end{bmatrix}
\]

\[
= \begin{bmatrix}
\frac{2pDr}{(t_1 + t_3 + D)^3} & 0 & -\frac{2pDr}{(t_1 + t_3 + D)^3} \\
0 & -\frac{\sqrt{(1-p)B/R}}{4(t_2 + t_3)^{3/2}} & r\frac{\sqrt{(1-p)B/R}}{4(t_2 + t_3)^{3/2}} \\
-\frac{2pDr}{(t_1 + t_3 + D)^3} & r\frac{\sqrt{(1-p)B/R}}{4(t_2 + t_3)^{3/2}} & -\frac{2pDr}{(t_1 + t_3 + D)^3} - \frac{\sqrt{(1-p)B/R}}{4(t_2 + t_3)^{3/2}} r
\end{bmatrix}
\]

(A3)
In order to show that \( H \) is negative semi-definite, it is sufficient to show the following three conditions: (1) \( |H_{11}| \leq 0 \); (2) \[
\begin{vmatrix}
H_{11} & H_{12} \\
H_{21} & H_{22}
\end{vmatrix} \geq 0
\]; and (3) \( |H| \leq 0 \). The first condition obviously holds, because
\[
|H_{11}| = H_{11} = -\frac{2pDr}{(t_1 + t_3 + D)^3} < 0 .
\] The second condition also holds, since
\[
\begin{vmatrix}
H_{11} & H_{12} \\
H_{21} & H_{22}
\end{vmatrix} = H_{11}H_{22} - H_{12}H_{21} = \left( \frac{2pDr}{(t_1 + t_3 + D)^3} \right)^2 \left( \frac{(1-p)B}{R} \right) > 0 .
\] Finally, the third condition also holds, since we have
\[
|H| = H_{11}
\begin{vmatrix}
H_{22} & H_{23} \\
H_{32} & H_{33}
\end{vmatrix} - H_{12}
\begin{vmatrix}
H_{21} & H_{23} \\
H_{31} & H_{33}
\end{vmatrix} + H_{13}
\begin{vmatrix}
H_{21} & H_{22} \\
H_{31} & H_{32}
\end{vmatrix} < 0 .
\]

\[
(A4)
\]

APPENDIX 3: PROOF OF PROPOSITION 3

(a) The defender (weakly) prefers to move first rather than playing the simultaneous game when
\[
\frac{(1-p)B}{4b_w/r} > \frac{(1-p)(B/R)^2}{(B/R + b_w/r)^2} \iff \frac{1}{4b_w/r} > \frac{B/R}{(B/R + b_w/r)^2} \iff (B/R - b_w/r)^2 > 0
\]
which is always satisfied. Similarly, the terrorist prefers to move first rather than playing the simultaneous game when
\[
\frac{(1-p)b_w/r}{4B/R} > \frac{(1-p)(b_w/r)^2}{(B/R + b_w/r)^2} \iff \frac{1}{4B/R} > \frac{b_w/r}{(B/R + b_w/r)^2} \iff (B/R - b_w/r)^2 > 0
\]

\[
(A5)
\]
This is always (weakly) satisfied. Therefore, we have shown that over the three games, both the defender and the terrorist always prefer the game in which they move first rather than a simultaneous game.

(b) When $0 \leq \frac{B/R}{b_w/r} < 0.5$, by Proposition 2 the defender is deterred from exerting effort, and earns zero utility against an overwhelming terrorist that moves first. Therefore the defender prefers herself moving first rather than allowing the terrorist to move first. When $\frac{B/R}{b_w/r} \geq 0.5$, the defender is not deterred in a game in which the terrorist moves first and therefore we can use Table 4-4. By Table 4-4, the defender prefers the terrorist to move first rather than herself moving first if and only if

$$\frac{(1-p)B/R}{4b_w/r} \leq \frac{(1-p)(2B/R-b_w/r)^2}{4(B/R)^2}$$

$$\Leftrightarrow \left(\frac{B}{R} - \frac{b_w}{r}\right)\left(\frac{B}{R} - \frac{(3-\sqrt{5})b_w}{2r}\right)\left(\frac{B}{R} - \frac{(3+\sqrt{5})b_w}{2r}\right) < 0$$

$$\Leftrightarrow 1 < \frac{B/R}{b_w/r} < 2.62$$

(c) Analogously, when $\frac{B/R}{b_w/r} > 2$, by Proposition 1 the terrorist is deterred from exerting effort, and earns zero utility against an overwhelming defender that moves first. Therefore the terrorist prefers moving first rather than allowing the defender to move first. When $\frac{B/R}{b_w/r} \leq 2$, the terrorist is not deterred in a game in which the defender moves first and therefore we can use Table 4-4. By Table 4-4, the terrorist prefers the defender to move first rather than moving first if and only if
(d) When \(0 < \frac{B}{R} \leq \frac{b_w}{r} < 0.5\), by Proposition 2 the defender is deterred from exerting effort, and earns zero utility against an overwhelming terrorist that moves first. Therefore the defender prefers the simultaneous game rather than allowing the terrorist to move first. When \(\frac{B}{R} \geq \frac{0.5}{b_w/r}\), the defender is not deterred in a game in which the terrorist moves first and therefore we can use Table 4-4. By Table 4-4, the defender prefers the simultaneous game rather than allowing the terrorist to move first if and only if

\[
\frac{(1-p)(B/R)^2}{(B/R + b_w/r)^2} > \frac{(1-p)(2B/R - b_w/r)^2}{4(B/R)^2}
\]

\[
\Leftrightarrow \frac{(B/R)^2}{(B/R + b_w/r)^2} > \frac{(2B/R - b_w/r)^2}{4(B/R)^2}
\]

\[
\Leftrightarrow \frac{(B/R)}{(B/R + b_w/r)} > \frac{(2B/R - b_w/r)}{2(B/R)} \quad \text{(note we have } \frac{B}{R} \geq \frac{0.5}{b_w/r} \text{ here)}
\]

\[
\Leftrightarrow (B/R) < (b_w/r)
\]

Equation (A9) is satisfied if and only if \(0.5 \leq \frac{B}{R} \leq \frac{b_w}{r} < 1\). In summation we have shown that the defender prefers a simultaneous game rather than allowing the terrorist to move first if and only if \(0 < \frac{B}{R} \leq \frac{b_w}{r} < 1\).

(e) When \(\frac{B}{R} > 2\), Proposition 1 gives that the terrorist is deterred if the defender moves first, which the terrorist seeks to avoid and therefore the terrorist prefers a simultaneous game rather than allowing the defender to
move first. When \( \frac{B}{R} \frac{b_w}{r} \leq 2 \), the terrorist is not deterred if the defender moves first, and then we can use Table 4-4. By Table 4-4, the terrorist prefers the simultaneous game rather than allowing the defender to move first if and only if

\[
\frac{(1 - p)(b_w / r)^2}{(B / R + b_w / r)^2} > \frac{(1 - p)(2b_w / r - B / R)^2}{4(b_w / r)^2}
\]

\[\iff\]

\[
\frac{(b_w / r)^2}{(B / R + b_w / r)^2} > \frac{(2b_w / r - B / R)^2}{4(b_w / r)^2}
\]

\[\iff\]

\[
\frac{(b_w / r)}{(B / R + b_w / r)} > \frac{(2b_w / r - B / R)}{2(b_w / r)} \quad \text{(note we have} \quad \frac{B}{R} \frac{b_w}{r} \leq 2 \text{ here)}
\]

\[\iff\]

\[
(B / R) > (b_w / r)
\]

In summation, we have shown that the terrorist prefers a simultaneous game rather than allowing the defender to move first if and only if \( \frac{B}{R} \frac{b_w}{r} > 1 \).
Chapter 5

A BAYESIAN MODEL FOR A GAME OF INFORMATION IN OPTIMAL ATTACK/DEFENSE STRATEGIES

M. Naceur Azaiez

Abstract: In defense/attack strategies, the attacker estimates the chance of a successful attack prior to launching his/her attack. If such a chance is not sufficiently high, then the attacker can be deterred. Ideally, the estimation is made under perfect knowledge of the targeted system so that it is error-free. For the defender, the ideal case in which the attacker could be deterred is one of nearly complete absence of knowledge, in which case the estimation error would be large enough to lead to an unreliable estimate of the probability of successful attack. In practice, the available information constitutes an intermediate situation between the two extreme cases above. We consider the case where the attacker can have information at the system level but has no access to information at the component level. The proposed game is so that the defender could make improvement on the targeted system to make the information to be collected by the attacker as ambiguous as possible in a way to deter the attack. At the same time, we assume that the improvement will increase the survivability of the system components, as a second alternative to the defender to deter the attack. The attacker strategy is to attack only if the chance of a successful attack is perceived to be sufficiently high, and the estimation made using only information at the system level is sufficiently accurate. This may be the case if the attacker for instance faces strong opposition to launching an attack. We assume that the attacker is also aware of the system configuration, the survivability of the system components prior to any improvement and of the defender optimal defense strategy. A Bayesian approach is suggested to analyze the problem. A variety of systems are investigated and optimization/decision models are suggested to solve the problem of each player. The problem is also extended to the situation where the attacker can access more information without reaching the perfect case, in which precise information at every component is available to the attacker.

Key words: attack/defense strategies, reliability, optimization, game theory, Bayesian updating
1. INTRODUCTION

Information plays a critical role in defense/attack strategies. While defenders opt for maximum levels of secrecy in building their defensive systems including deceptions, attackers employ important resources to gain information about such defensive systems (including spying and seeking the services of intelligence agencies). The more correct information the attacker gathers, the higher the accuracy in estimating the chance of a successful attack and the less the tragic impacts of such attack. In fact, attackers usually prefer less severe casualties and less perpetual damage outside the targeted system to avoid worsening much their image in front of the public opinion.

Most of the studies that have investigated optimal defense/attack strategies either have totally ignored the factor of information in determining the different strategies, or have limited focus on the two extreme cases of complete knowledge versus absence of knowledge of the defensive systems. For instance, Azaiez and Bier (2007) consider optimal defense attack strategies under the assumption that the attacker has full knowledge about the targeted system. Levitin (2008) considers the two extreme cases of perfect knowledge and total absence of knowledge of the defensive system. An exception is found in Dighe et al. (2008), where the level of secrecy in defensive investment is used as a strategy to deter attacks. In particular, the authors show that releasing partial information about the defensive allocation of resources helps deter attacks at lower investment costs than would be possible if the defensive allocation were disclosed.

The current chapter considers a game where the defender attempts to make the available information to the attacker as ambiguous as possible as a strategy to deter attacks. It is assumed that the attack is deterred if one of two conditions occurs; either the chance of a successful attack is sufficiently low or if the information available would not allow for accurately estimating such a chance. This will be the case if the attacker lacks of support to opt for an attack and therefore does not want to launch a failed attack. It is also assumed that the defender has too few resources to improve the defensive system sufficiently so that the chance of a successful attack would be considerably low. Consequently, the defender could opt for a unified strategy for deterring the attack by seeking to make one (or both) of the two conditions for deterring an attack occur. The defender could judge which condition would be more likely, and then allocate the resources accordingly (based on importance weights that reflect his/her judgment about the likelihood of each condition).

Before tackling the problem, we will describe in section 2 some results in a different context; namely the concept of perfect aggregation in Bayesian reliability models. In fact, the results of the current chapter will apply by
simple analogy with those developed in the context of such aggregation. Next, the problem will be defined and analyzed in Section 3. A variety of models will be discussed. Section 4 will extend the focus to the case where more information is available to the attacker. The methodology (which will be a natural extension of the one suggested in section 3) will be briefly outlined and illustrated. Finally, Section 5 will provide a summary, and directions for future work.

2. BACKGROUND (PERFECT AGGREGATION/AGGREGATION ERROR)

Consider estimating the reliability of a system which consists of a number of components, using Bayesian updating. Also, suppose that failure data is available both at the aggregate (i.e., system) and disaggregate (i.e., component) levels. Then a multitude of approaches could be adopted. At one extreme, a prior distribution of the system reliability could be combined with observations concerning system performance (e.g., failures or successes during some observation period) as a whole through Bayes theorem. This yields a posterior distribution of system reliability. Such an approach is referred to as an aggregate analysis. Aggregate analysis ignores the performance (observations) at the individual levels. For instance, if the system is series, then the aggregate analysis will only consider the cumulative number of failures of all components and neglects the information about the particular components that have failed. At the other extreme, a prior distribution of the reliability of each component will be combined with the observations on the performance of that component to yield a posterior distribution of the component reliability. Next the system configuration will be used to combine the posterior distributions at the component levels to yield a posterior distribution of the system reliability. Such an approach is called a disaggregate analysis. Note that when all components are independent in the sense that the failure of one component does not affect the performance of others, then the disaggregate analysis makes use of all available information. For the remainder of the chapter, only independent components/items will be considered. Other approaches would be to use a disaggregate analysis at several subsystems and then combine the obtained posterior distributions at the sub-system levels to obtain a posterior distribution at the system level. Clearly, the more information is used (i.e., the more the data is disaggregated) the more accurate is the estimation, assuming that the observations are error-free. However, in practice, the type of analysis to be adopted could be dictated by
considerations such as the cost of data collection, the scarcity of data at disaggregate levels or unreliability of disaggregate data.

In general, the aggregate and disaggregate analyses yield different results. In this case, we say that an aggregation error occurs. The absence of aggregation error is referred to as perfect aggregation. Azaiez and Bier (1994, 1995) determined necessary and sufficient conditions for perfect aggregation for general combined series/parallel systems under the assumptions of independence, non-degeneracy and no replications (excluding for instance \(k\)-out-of \(n\) systems). In particular, they showed that perfect aggregation is nearly inevitable. In addition, Azaiez and Bier (1996) provided quantitative tools to estimate the size of aggregation error. We will expose below some of the results of interest from Azaiez and Bier (1994, 1995, and 1996) for the current chapter. Interested readers may refer to the above papers for proofs.

**2.1 Results on perfect aggregation**

Consider a system of independent components that can be configured as combined series/parallel (with no replications) where each component fails in a Bernoulli manner. We neglect the case of deterministic failures (corresponding to a degenerate failure distribution). For series (respectively parallel) systems of \(n\) components (for some positive integer \(n\)), the data collection process is made so that component \(i+1\) is tested only if component \(i\) is found operating (respectively failing) for all \(i=1, ..., n-1\). The approach is extended to combined series/parallel systems using the same logic.

**Theorem 2.1**

Consider a parallel system of \(n\) components satisfying the assumptions above. Let \(P_i\) be the failure probability of component \(i\) \((i=1, ..., n)\). Then, perfect aggregation occurs if and only if the prior distribution of \(P_i\) is Beta \((c_i, d_i)\) with \(c_i = c_{i+1} + d_{i+1}, i=1, ..., n-1\).

**Theorem 2.2**

Consider a series system of \(n\) components satisfying the assumptions above. Let \(P_i\) be the failure probability of component \(i\) \((i=1, ..., n)\). Then, perfect aggregation occurs if and only if the prior distribution of \(P_i\) is Beta \((c_i, d_i)\) with \(d_i = c_{i+1} + d_{i+1}, i=1, ..., n-1\).

We will also expose a special case of a general result in Azaiez and Bier (1995) adapted to a series-parallel system. Consider a series system of \(n\) components where each component \(k\) is made of \(j_k\) items. Let \(P_k\) be the failure probability of component \(k\) and \(P_{i,k}\) be the failure probability of item \(i\).
in component \( k \) (\( k=1, \ldots, n \), and \( i=1, \ldots, j_k \)). Then, under the specified assumptions above, the following result holds.

**Theorem 2.3**

Perfect aggregation occurs if and only if \( P_{i,k} \sim \text{Beta}(c_{ik}, d_{ik}) \), with \( c_{ik} = c_{i+1,k} + d_{i+1,k} \), for \( i=1, \ldots, j_k - 1 \), \( P_k \sim \text{Beta}(c_k, d_k) \) with \( d_k = c_{k+1} + d_{k+1} \), \( d_k = \sum_{i=1}^{j_k} d_{ik} \), and \( c_k = c_{jk,k} \).

### 2.2 Aggregation error

The error represents the gap between the estimations based on the disaggregate analysis (which contains all the needed information) and the aggregate analysis (which only uses the information at the system level). Alternative measures of aggregation error could be considered (Azaiez and Bier, 1996). When using an aggregate analysis, only the aggregate data will be observed. For the same set of aggregate data there corresponds a number of candidate sets of disaggregate data. One possible (conservative) measure of aggregation error would be to estimate the worst possible discrepancy between the aggregate mean on one hand and all the candidate corresponding disaggregate means, on the other hand. More specifically, let \( P \) be the failure probability of the considered system, \( AD \) be the observed aggregate data (corresponding to the total number of trials and the total number of failures at the system level). Also, let \( \Omega(AD) \) be the set of all candidate disaggregate data \( DD \) (indicating the number of trials and failures for each component of the system) consistent with \( AD \). That is, both \( AD \) and \( DD \) have the same number of trials and the same number of failures at the system level. Finally, let \( E(.) \) be the expected value operator. Then, the aggregation error, \( AGE \) is given by:

\[
AGE = \sup_{DD \in \Omega(AD)} \left| E(P|DD) - E(P|AD) \right|
\]

Such a measure is conservative. However, it is consistent with the context of the current study where the attacker wants to avoid any risk of wrong estimation of the probability of a successful attack, as will be explained later. We expose now some of the results given in Azaiez and Bier (1996) that pertain to the current study.

Let \( U \) (respectively \( L \)) be the upper bound (respectively lower bound) of the disaggregate mean of the failure probability over all possible candidates \( DD \) of \( \Omega(AD) \). That is,
\[ U = \sup_{DD \in \Omega(AD)} E(P|DD) \text{ and } L = \inf_{DD \in \Omega(AD)} E(P|DD) \]

Consequently, the following results apply:

**Proposition 2.1**
\[ AGE = \max \left\{ U - E(P|AD); E(P|AD) - L \right\} \]

**Proposition 2.2**
\[ (U-L)/2 \leq AGE \leq (U-L). \]

Proposition 2.2 offers a useful tool to approximate the size of the error without using the aggregate mean, which is usually costly to calculate. The bounds on the error are valid independently of the system configuration (as a combined series-parallel) and the number of its components. The only real challenge remaining in estimating the size of the error is the calculation of \( U \) and \( L \), which suggests in general solving discrete nonlinear optimization models. However, for series and parallel systems \( U \) and \( L \) are knapsack problems solved by dynamic programs.

We will illustrate below the case of a parallel system of \( n \) components.

Let the aggregate data be \( AD = \{k_0, k_n\} \), where \( k_0 \) and \( k_n \) denote respectively the number of trials and the number of system failures (which also coincides with the number of failures of component \( n \)). Then, the set of candidate disaggregate data will be \( \Omega(AD) = \{k_0, k_1, \ldots, k_n\} \), where all \( k_i \)'s are integer with \( k_0 \geq k_1 \geq \ldots \geq k_n \). We let the stages of the DP be \( 1, 2, \ldots, n \), the decision variables be \( k_1, k_2, \ldots, k_{n-1} \) and the states be \( s_1, s_2, \ldots, s_n \), where for all \( i \), \( s_i \) is the number of trials on component \( i \). That is, \( s_i = k_{i-1} \). Consequently, we have \( k_0 \geq s_i \geq k_n \). Then, define \( f^*_n(s_n) = E(P|s_n, k_n) \). Also, for all \( i = n-1, \ldots, 1 \), define recursively
\[
 f^*_i(s_i) = \max_{s_{i+1}} \left\{ E(P|s_i, k_i) f^*_{i+1}(k_i) \right\} \]

Then, \( f^*_i(s_i) = U \). Similarly, by changing maximization to minimization, we obtain \( L \).

The DP to obtain \( U \) and \( L \) for series system will be somewhat similar.

### 3. THE PROBLEM

Consider the case in which the attacker is willing to launch an attack only under a sufficient level of confidence (as illustrated below) that the attack
will be successful (say, will totally destroy or disable the targeted system). Such a situation could be encountered if the attacker faces strong opposition to attacking. For instance, the attacker may lack support both internally (i.e., with respect to his/her people) and externally (i.e., with respect to the international community) to resolve a conflict through the use of power. If the attacker ignores all the opposition he/she is confronted with and will insist on launching his/her attack, then the consequences of a failed attack could be highly severe. Therefore, we assume that the attacker is motivated to estimate carefully the success probability of an attack on a targeted system before making the decision to attack. We also assume that, while the attacker is aware of the system configuration, he/she is unable to access information at the individual components of the system and can collect observations (for instance through satellite images) only at the system level. In addition, we assume that the defender who is aware of the pressure on the attacker to avoid a failed attack, has some alternatives to improve the survivability of his/her components and to mislead the attacker regarding the estimation of the success probability (e.g., by hardening the components, changing their design, locations, etc.). Thus, we have a game of information, in which the attacker seeks perfect information about the targeted system in order to accurately estimate the success probability, while the defender uses all feasible means to make the available information at the system level as ambiguous as possible while improving the system survivability.

Estimation of the success probability can be approached through Bayesian updating. The attacker will try a number of attacks on a local “similar system” and then will use the observed results through Bayes’ Theorem to update the prior knowledge (which is obtained previously based on collected information on the targeted system). We assume that information used in constructing a local system with “comparable” survivability to the targeted system is accessible only at the system level. Consequently, the tentative defensive system used by the attacker on the local system need not be amply consistent with the real one and therefore, the observations to be collected by the attacker at the component level may be weakly reliable. In particular, we assume that the problem to be solved by the attacker will be based on one representative scenario which would match with the real scenario on the overall survivability only at the system level but not at the component level. Thus, the attacker will only rely on observations at the aggregate level in the Bayesian updating of the probability of a successful attack.

Because an estimation error could result from assessing the success probability using exclusively data at the system level, the attacker strategy will be to launch an attack only if such an error is sufficiently small and if the assessed probability of successful attack is sufficiently large. In such a
situation, the exact success probability (which would be obtained using disaggregate data) will also likely to be sufficiently large.

3.1 Notation and problem formulation

Let \( \pi \) be the mean of the estimated success probability using information only at the system level, \( \pi_0 \) be a threshold level (sufficiently close to one), \( \varepsilon \) be the estimation error (due to the lack of information at the component level), and \( \varepsilon_0 \) be a threshold value (sufficiently close to zero). Then, the defender moves first and will attempt through the possible improvements on the targeted system to make \( \pi \) as small as possible or \( \varepsilon \) as large as possible. This suggests solving an optimization model in which the optimal prior parameters will be selected so as to maximize a weighed expression related to \( \pi \) and \( \varepsilon \) under the constraints of improvements feasibility. The relevant details will be provided later. The attacker moves next. The attacker strategy consists in:

- estimating \( \pi \) and \( \varepsilon \) (based on the optimal values of the prior distributions to be set by the defender),
- Assigning the free choice variables \( \pi_0 \) and \( \varepsilon_0 \) and
- attacking only if:

\[
\pi \geq \pi_0 \tag{1}
\]

and

\[
\varepsilon \leq \varepsilon_0 \tag{2}
\]

This says that the game is sequential and the defender will have the first move. Also, the choice of \( \pi_0 \) and \( \varepsilon_0 \) is made subjectively by the attacker and is assumed not to be known to the defender.

Using a simple analogy with the concept of aggregation in reliability analysis and the terminology of Section 2, \( \pi \) will be the equivalent of the aggregate mean of the system failure probability and \( \varepsilon \) will the equivalent of the aggregation error. When \( \varepsilon \) is a small fraction (e.g., 5%), then the error will be a smaller fraction of the disaggregate mean (which lies in [0, 1]). We may continue to use the same measure of aggregation error as in Section 2 given the conservatism of the attacker in accurately estimating the success probability of an attack. It follows immediately that:
PROPOSITION 3.1

The error vanishes (leading to $\varepsilon \leq \varepsilon_0$) if and only if perfect aggregation occurs.

The defender will invest to harden the components so that the success probability of an attack on a given component will decrease in an attempt to prevent (1). This will also affect the initial parameters of the prior distributions of successful attacks on components. The defender will also attempt to make such changes favorable not only for an aggregation error to occur, but also for the size of the error to be as large as possible (trying to prevent (2)).

Given that the defender does not know the threshold values of (1) and (2), he/she will invest to deter the attacker by making $\varepsilon$ as large as possible and $\pi$ as small as possible. We let $w_s$ (respectively $w_e$) be the importance weight allocated by the defender for improving the survivability of a component (respectively, increasing the error of the attacker) in a goal-programming spirit; or the scaling constants of an additive utility function in a multi-attribute utility spirit. Then, the defender strategy will be to maximize a measure of survivability improvement and maximize a measure of error, weighed by the relevant importance weights. This suggests using goal programming/multi-attribute utility to determine the optimal defender strategies. Assuming that the attacker is aware of the alternatives available to the defender and thus his/her optimal defense strategy, the attacker will estimate $\pi$ and $\varepsilon$ based on the optimal values of the prior distributions to be set by the defender. For instance, the information available to the attacker including the know-how and resources of the defender would allow for an improvement of the system survivability of up to 15%. However, the attacker would not know which alternative leading to such an improvement level has been adopted by the defender. That is, the lack of information at the disaggregate level of the defender choices is the core of the game. Also, because the estimation of the aggregate mean and the size of aggregation error are computationally inefficient, the attacker will use approximations in evaluating $\pi$ and $\varepsilon$. We will distinguish three cases in which the attacker is optimistic, pessimistic and neutral. Reconsider the upper and lower bounds $U$ and $L$ on the disaggregate means given the aggregate data (discussed in Section 2); then, from the results in Section 2, the aggregate mean will lie between $L$ and $U$, while the aggregation error will lie between $(U-L)/2$ and $U-L$.

3.1.1 Case of an optimistic attacker

In this case, (1) and (2) will be approximated by:
\( U \geq \pi_0 \) \hspace{1cm} (3)

and

\( \frac{(U-L)}{2} \leq \varepsilon_0 \) \hspace{1cm} (4)

### 3.1.2 Case of a pessimistic attacker

In this case, (1) and (2) will be approximated by:

\( L \geq \pi_0 \) \hspace{1cm} (5)

and

\( (U-L) \leq \varepsilon_0 \) \hspace{1cm} (6)

### 3.1.3 Case of a neutral attacker

In this case, using Hurwicz optimism index (see for instance Arnold et al. (2002)) set to 0.5, (1) and (2) will be approximated by:

\( \frac{(L+U)}{2} \geq \pi_0 \) \hspace{1cm} (7)

and

\( \frac{3(U-L)}{4} \leq \varepsilon_0 \) \hspace{1cm} (8)

That is, the midpoints of the intervals where the aggregate mean and the aggregation error range are taken as estimates (in the appropriate order). Note that the case of optimistic (pessimistic) attacker coincides with the case where Hurwitz optimism index is set to one (zero). In the remainder of the chapter, the case of the neutral attacker will be the base case for analysis. In addition, the following assumptions will apply to all the models that will be considered.

1. All components/items are independent in the sense that the failure of one component/item upon an attack will not affect the performance of the others.
2. No more than one attack is possible per component/item (justifications are offered in Bier and Azaiez (2007); for instance, a second attack on the same component may lead to the capture of the attacker).

3. All components must be attacked in sequence. The reasons for that is that the attacker’s policy is neither to overuse resources through simultaneous attacks, nor to cause more damage than needed to disable the system (for instance attacking simultaneously two components where the failure of each one will lead to system failure will both overuse resources and cause excessive damage).

3.2 Case of a parallel system of an arbitrary size $n$

Assume that the targeted system is a parallel system of $n$ components where $n$ is some positive integer. Recall that a single attack is feasible per component, attacks are to be made sequentially, and components are independent. Moreover, assume that the attack should stop if an attacked component is not disabled, as the system will survive the sequence of attacks anyway. Using the terminology of Azaiez and Bier (2007), the component to be attacked first is the most attractive to the attacker. A result in Azaiez and Bier (2007) essentially states (when the cost of attacks are the same) that, under an optimal attack strategy, the most attractive one in a parallel system is the one with highest chance to survive the attack. The attack will continue (if at all) from the most to the least attractive components in that order. In the context of the current work, the justification is obvious, since a failed attack on only a few components will have less consequence to the attacker (given the pressure he/she faces for using power) than a more costly attack that ends up failing. As a consequence, when considering a Bayesian approach for evaluating the chance of a successful attack, the number of attacks $k_0$ to be tried (on the simulated improved system; i.e., accounting for the optimal improvement of the defender which match the real improvement only at an aggregate level) will be the number of attacks on the most attractive component. Also, the number of successes $k_1$ will be also the number of attacks on the second component (again on the simulated system), and so on. At the end, the number of successes on the least attractive component $k_n$ will be the number of successful attacks on the entire (simulated) system, given the parallel configuration of the system. That is, the Bayesian updating will be made by the attacker using simulation, to assess the new “aggregate” success probability of an attack upon the first move of the defender (i.e., the system improvement). This assessment will take place before a real attack is launched (when (1) and (2) are found to occur). This setting will be a perfect analogy with that of aggregation in Bayesian reliability models for a parallel system. Consequently, before any
Chapter 5

Defensive actions are undertaken, the following result follows immediately from Proposition 3.1 and from section 2 results.

**Proposition 3.2**

For the estimation of the success probability of an attack using only observations at system level to be error free (i.e., for $\varepsilon$ to vanish) it is necessary and sufficient that the probability of successful attacks on components $1, 2, ..., n$ will have independent conjugate prior distributions $P_i \sim \text{Beta}(c_i, d_i)$, for $i=1, ..., n$ with $c_i = c_{i+1} + d_{i+1}$, for $i=1, ..., n-1$.

The parameters of the prior distributions can be interpreted as:

$c_i$ = the number of successful attacks and $c_i + d_i$ = the number of trials on component $i$.

Therefore, the restrictive conditions on parameters of Proposition 3.2 essentially state that the number of trials on component $i+1$ will be the number of successes on component $i$ (consistent with the assumption on an attack strategy). In addition, the prior probability of a successful attack on component $i$ has a mean of $c_i/(c_i + d_i)$ (i.e., number of successes over total number of trials). Moreover, if the estimation is to be error free, then both the aggregate and disaggregate means will coincide at the value $(c_n + k_n)/(c_1 + d_1 + k_0)$.

We now consider the game where the defender will have the first move of attempting to increase the value of $\varepsilon$ (seeking to exceed the unknown threshold value $\varepsilon_0$) and to increase the survivability of the different components to potential attacks. Note that $\varepsilon_0$ is assumed to be known only to the attacker (as it represents the attacker judgment on how low the error must be). Consequently, the defender will attempt to increase $\varepsilon$ as much as possible. We will assume that the priors are independent conjugate prior distributions (i.e., Beta distributed in this case) and that the improvements will affect the parameters of the distribution to yield for a given component $i$ new values $c_i^\text{new}$ and $d_i^\text{new}$. In addition, the defender seeks to make the discrepancy between $c_i^\text{new}$ and $c_{i+1}^\text{new} + d_{i+1}^\text{new}$ as large as possible in hope of making $\varepsilon$ exceed $\varepsilon_0$. Knowing that there are limits on possible improvements on each component $i$, the new values of the parameters must lie between a lower bound, $c_i^\text{min}$ (respectively $d_i^\text{min}$) and an upper bound $c_i^\text{max}$ (respectively $d_i^\text{max}$). Finally, using the importance weights $w_s$ and $w_e$ allocated by the defender for deterring the attacker by increasing the components’ survivability and by increasing the error due to the lack of information, respectively, it follows that the defender problem will be to use
the available alternatives to solve the following non-smooth optimization model:

\[
\max Z = w_s \left[ -\prod_{i=1}^{n} \frac{c_i}{c_i + d_i} \right] + w_e \left[ \sum_{i=1}^{n} c_i - c_{i+1} - d_{i+1} \right]
\]

\[\text{s.t.} \quad c_{i}^{\text{min}} \leq c_i \leq c_{i}^{\text{max}}, \quad i = 1, \ldots, n\]
\[d_{i}^{\text{min}} \leq d_i \leq d_{i}^{\text{max}}, \quad i = 1, \ldots, n\]

(9)

In order to get rid of the absolute value expression in the objective function of (9), we suggest introducing a sufficiently large M, binary variables \(y_i\), and continuous variables \(\eta_i\) \((i=1, \ldots, n-1)\) to obtain the equivalent mixed integer-nonlinear program given by (10). Note that the factor multiplying \(w_s\), \(0 < w_s < 1\) is a probability, while the factor multiplying \(w_e\) is a sum of ranges that could be significantly larger than 1. Consequently, for the objective function to be meaningful for the defender, the assessments of the importance weights must be carefully estimated. In particular, when the defender is indifferent about which objective to favor, then \(w_s\) must be significantly larger than \(w_e\) to compensate the considerable differences in the size of the measure of each objective. When the defender favors deterring an attack through increasing the size of the error, then the weights could be of comparable values.

\[
\max Z = w_s \left[ -\prod_{i=1}^{n} \frac{c_i}{c_i + d_i} \right] + w_e \sum_{i=1}^{n-1} \eta_i
\]

\[\text{s.t.} \quad \eta_i - c_i + c_{i+1} + d_{i+1} - My_i \leq 0, \ i = 1, \ldots, n-1\]
\[\eta_i + c_i - c_{i+1} - d_{i+1} + My_i \leq M, \ i = 1, \ldots, n-1\]
\[c_i^{\text{min}} \leq c_i \leq c_i^{\text{max}}, \quad i = 1, \ldots, n\]
\[d_i^{\text{min}} \leq d_i \leq d_i^{\text{max}}, \quad i = 1, \ldots, n\]
\[\eta_i \geq 0, \quad y_i = 0,1, \quad i = 1, \ldots, n-1\]

(10)

The attacker will have the next move by solving the defender problem (10), then using the optimal values \(c_i^{\text{new}}\) and \(d_i^{\text{new}}\) in the dynamic program described at the end of section 2 to evaluate \(U\) and \(L\), and subsequently inserting the obtained values in (7) and (8) in order to decide whether to launch the attack.
EXAMPLE 3.1

Consider a parallel system of four components where the probabilities of successful attacks are given respectively by:

\[ P_1 \sim \text{Beta}(11,1), \ P_2 \sim \text{Beta}(10,1), \ P_3 \sim \text{Beta}(9,1), \ P_4 \sim \text{Beta}(8,1). \]

Note that the components are ordered from the most attractive to the least attractive to the attacker. That is, the expected probabilities of a successful attack are given in a decreasing order. Next, assume that the attacker strategy is to attack only if: \( \pi \geq \pi_0 \) and \( \epsilon \leq \epsilon_0 \), or, using the approximations given in (7) and (8), the attack will occur if:

\[ \frac{L+U}{2} \geq \pi_0 \text{ and } \frac{3(U-L)}{4} \leq \epsilon_0, \]

where \( \pi_0 \) is assumed to be 60% and \( \epsilon_0 \) to be 5%. In other words, we assume that the attacker will attack only if there is at least 60% chance of success and at most 5% discrepancy in the estimation due to the use of observations at the (simulated) system level only.

Before any defensive actions are taken, it should be clear that perfect aggregation occurs, leading to zero error in the estimation. Moreover, the expected (prior) probability of a successful attack is 0.667, which satisfies the first condition. Therefore, this situation is favorable for an attack. The defender will have to make improvements in order to deter the attacker by decreasing the chance of a successful probability and by increasing the discrepancy as much as possible. We assume that no matter what improvements are made, the first parameter of the prior distributions must always lie respectively in the following intervals: [10.5;11.5], [9.5;10.5], [8.5;9.5], and [7.5;8.5]. Also, we assume that the second parameter will lie in [0.9; 1.2] for all distributions.

Assume that the defender tends to favor deterring the attack by making the error sufficiently large. Consequently, the defender may opt for equal values of the scaling constants \( w_s = w_e = 1 \). Note that, as more information is available to the defender about the attacker strategy, he/she can change the weights and thus priorities to favor increasing further the discrepancy or decreasing the chance of successful attacks, as appropriate.

The solution to the optimization model given in (10) is given by:

\[ c_1^{\text{new}} = 10.5, \ c_2^{\text{new}} = 10.5, \ c_3^{\text{new}} = 8.5, \ c_4^{\text{new}} = 8.5, \ d_3^{\text{new}} = 0.9 \text{ and } d_i^{\text{new}} = 1.2 (i \neq 3). \]

In addition, the discrepancies used to increase the size of the error (represented in the optimization model by \( \eta_i \), \( i=1, 2, 3 \)) are respectively 1.2, 1.1, and 1.2.
The solution suggests taking the largest possible values of the second parameter in 3 out of 4 cases of the Beta distribution, as this helps decrease the mean probability of a successful attack. The first parameter also takes the lowest values for 3 out of 4 cases, which also serves the same objective. In addition, perfect aggregation no longer holds. However, because the limited space where the parameters can vary, the mean of the new prior success probability is 62.5%, which is still sufficiently high for an attack to be launched. If the defender considers giving more importance to improving system survivability, then when taking $w_s$ to be 10 instead of 1, then there is no change in the optimal solution. When $w_s$ takes the value 50, then the mean of the prior success probability will decrease from 62.5% to 61.5%. If $w_s$ increases further to reach the values of 100 and 1000 (in a pre-emptive spirit), then the value of the mean will decrease to 60.8% and 60.19% respectively, while the deviations (given by $\sum_{i=1}^{3} \eta_i$) will become very small). It is clear that the improvements made are very limited and let us assume that the defender will attempt to deter the attack by increasing the error. Reconsidering the case of equal weights or scaling constants which provides the same solution as for the case when $w_e$ is 10). Note that the defender can only estimate the improved prior mean but has no access to the information on the posterior mean. Moreover, the defender can only have indications about the size of the error through the deviation values $\eta_i$, i=1, 2, 3.

Next, it is the turn of the attacker to move. The attacker will take a number of observations based on simulated attacks on the local system (after the similar improvements/ modifications as those to be made by the defender on the targeted system at the aggregate level) in order to assess whether the situation is still favorable for an attack. We assume that the number of simulated observations taken is $k_0=6$ and the number of observed successes is found to be $k_4=4$. We next solve for $U$ and $L$ in order to estimate the new success probability and the new size of the error based on a Bayesian updating of an aggregate analysis. Using the dynamic programs discussed above, $U$ is found to be 0.652 and $L$ is found to be 0.644. It follows that the estimate of the aggregate mean $(U+L)/2$ is 0.648, which is still above 0.6. Moreover, the estimate of the aggregation error (i.e., $3(U–L)/4$) is found to be 0.006. Even in the case of a pessimistic attacker where the error is approximated by its upper bound $(U–L)$ and the success probability by its lower bound $L$, the results favor an attack. This says that the defender (even under an optimal strategy) has too limited improvement margin to deter an attack in this example.

Note however that the attacker would be deterred (even under the optimistic case) if the attacker strategy were to take $\pi_0$ to be 2/3 (instead of 60%). Consequently, the defender may feel confident about deterring the
attack in the absence of knowledge about the attacker strategy. On the other hand, under perfect knowledge of the attacker strategy (in which \( \pi_0 \) is 60%), the defender would opt for reducing the success probability while ignoring the second objective of increasing the discrepancy (which is very small anyhow) in a preemptive goal programming spirit. Unfortunately for the defender, he/she will not succeed to deter the attack in this case, either! However, the defender could at least attempt to decrease the damage caused by the attack by decreasing as much as possible the likelihood of the success probability.

3.3 Case of a series system of an arbitrary size \( n \)

Again, the attacker would start by the most attractive one, which is in this case the one with least chance to survive upon an attack. Similarly, as for the case of parallel systems, we assume that the components are ranked from most to least attractive. Moreover, the attacker would move to the next component only if the current one survives rather than fails. By considering \( Q_i \) as the chance of a failed attack on component \( i \) (\( i=1, \ldots, n \)), then the chance that the attack will fail is given by:

\[
Q = \prod_{i=1}^{n} Q_i
\]

This suggests using the same methodology as in the case of a parallel system while using the \( Q_i \) instead of the \( P_i \) and changing the attacker strategy so that the attack will be launched if

\[
\bar{\pi} \leq \bar{\pi}_0 \text{ and } \varepsilon \leq \varepsilon_0,
\]

where \( \bar{\pi} \) is the probability of a failed attack and \( \bar{\pi}_0 \) is a threshold value (which could be viewed as the complementary of \( \pi \) and \( \pi_0 \), respectively). In particular, the optimization model (10) will be slightly modified so that the probabilities of failed attacks will increase for the defender strategy, and the same DP models will be used for the attacker strategy. Note, however, that when the estimation of the chance of a failed attack is error-free, this corresponds equivalently to the case where the success probabilities will follow Beta distributions with parameters \( d_i = c_{i+1} + d_{i+1} \) (\( i=1, n \)). In addition, the aggregate and disaggregate data will use the number of failed (rather than succeeded) attacks. Finally, \( U \) and \( L \) will switch roles when considering optimistic vs. pessimistic attacker.
Example 3.2
Consider the case of a series system of four components. Assume that the attacker will launch an attack if the chance of a failed attack is less than 10% (i.e. chance of a successful attack more than 90%) and the error is less than 5%. The components initially have conjugate prior distributions for the probability of failed attacks with the following values (ordered from most to least attractive; or equivalently from lowest to highest average prior probability of failed attacks):

\[ c_1 = 4, \quad d_1 = 6, \quad c_2 = 2, \quad d_2 = 2, \quad c_3 = 1, \quad d_3 = 1, \quad c_4 = 0.7, \quad d_4 = 0.3. \]

Consequently, perfect aggregation holds and the assessment of a failed attack at the system level is error free. Also, the prior expected probability of a failed attack is 7%. Consequently, before any defensive improvements, the attacker strategy is to attack the system. We assume that the improvements that could be made by the defender are so that the parameters \( c_1, c_2, c_3, \) and \( c_4 \) can lie respectively in the following ranges:

\[ [3, 5], \quad [1, 3], \quad [0.5, 1.5], \quad \text{and} \quad [0.3, 1]. \]

Similarly, the parameters \( d_1, d_2, d_3, \) and \( d_4 \) can lie respectively in the following ranges: \([4, 8], \quad [1, 3], \quad [0.5, 1.5], \quad \text{and} \quad [0.1, 0.5].\)

The corresponding optimization model will be as follows:

\[
\begin{align*}
\text{max} \quad Z &= w_s \left[ \prod_{i=1}^{n} \frac{c_i}{c_i + d_i} \right] + w_e \sum_{i=1}^{3} \eta_i \\
\text{s.t.} \quad \eta_i - c_i + c_{i+1} + d_{i+1} - M \eta_i &\leq 0, \quad i = 1, 2, 3 \\
\eta_i + c_i - c_{i+1} - d_{i+1} + M \eta_i &\leq M, \quad i = 1, 2, 3 \\
3 \leq c_1 &\leq 5, \quad 1 \leq c_2 \leq 3, \quad 0.5 \leq c_3 \leq 1.5, \quad 0.3 \leq c_4 \leq 1, \\
4 \leq d_1 &\leq 8, \quad 1 \leq d_2 \leq 3, \quad 0.5 \leq d_3 \leq 1.5, \quad 0.1 \leq d_4 \leq 0.5, \\
\eta_i &\geq 0, \quad y_i = 0, 1, \quad i = 1, 2, 3
\end{align*}
\]

When the defender favors deterring the attack by increasing the error, say leading to equal values of the scaling constants or weights \( w_s \) and \( w_e \), the optimal solution is given by:

\[ c_{1}^{\text{new}} = 5, \quad c_{2}^{\text{new}} = 1, \quad c_{3}^{\text{new}} = 1, \quad \text{and} \quad c_{4}^{\text{new}} = 0.3, \quad d_{1}^{\text{new}} = 4, \quad d_{2}^{\text{new}} = 1, \quad d_{3}^{\text{new}} = 1.5, \quad \text{and} \quad d_{4}^{\text{new}} = 0.1. \]

Also, the gaps in the conditions of perfect aggregation are given by:
Note that the prior expected probability of a failed attack after defensive improvements is given by $Q^{\text{new}}=8.33\%$, which constitutes some minor improvement compared to the initial value of 7\%. This is due to the fact that the defender’s concern was to increase the size of the error. If the importance weights have changed so that the defender will give more importance to reducing the chance of a successful attack then, $Q^{\text{new}}$ will remain unchanged for $w_{s}=10$, while it will jump to 28.4\% in a preemptive manner (say with $w_{s}=100$). However, the sum of the gaps will be reduced from 6 to 2.4.

Consider the case of equal weights. The attacker will use the estimation of the aggregate posterior mean of a failed attack. We assume that the attacker experimentally observes 6 attacks, 1 of which will fail. Solving the corresponding DP’s (discussed in Section 2) yields $U=0.228$ and $L=0.134$. Consequently, the estimate of the aggregate mean of the probability of a failed attack will be 18.1\% and the estimate of the error is 7.05\%. This says that both the error and the expected probability of a failed attack are too large, compared respectively to the threshold values set by the attacker, which results in deterring the attack.

### 3.4 Case of a combined series-parallel Systems

We may extend the discussion to include complex systems that are arbitrarily obtained from combining series and parallel configurations. Both the results and the approaches will be natural extensions of the previous ones. As an illustration, we consider a series/parallel system, which is a series system of an arbitrary number of components, each in turn made by a parallel configuration of an arbitrary number of items. We may also reverse the roles of successes and failures to discuss the case of a parallel/series system where each of the parallel components is made of a series configuration of items. This latter case could be treated through a simple analogy with the series/parallel system, and therefore will not be explicitly discussed.

**SERIES/PARALLEL SYSTEMS**

Consider now the case of a series/parallel system, where $n$ components are placed in series ($n$ being an arbitrary positive integer) and where each component $k$ ($k=1,\ldots,n$) consists of $j_k$ items in parallel ($j_k$ being also an arbitrary positive integer). In this case, the attacker would start by attacking the first (most attractive) component. A successful attack is one where all items within that component (again considered from the most to the least attractive in the sequenced attacks) are disabled. The attacker will move to
the next component and the first attack will be considered as failed (on component 1) if one item will survive after being attacked. Thus, the number of attacks on component 1 will be the number of attacks on system. The number of failed attacks on component 1 will be the number of attacks on component 2 (the next most attractive component), and so on. Consequently, the number of failed attacks on system will be the number of failed attacks on last component.

We continue to use the same notations as for a series system, as well as the same attacker strategy (12). In particular, the probability of a failed attack on the system is given by

\[ Q = \prod_{k=1}^{n} Q_k \]

In addition, assuming that the success probability of an attack on item \( i \) of component \( k \) is \( P_{i,k} \), then the success probability of an attack on each component \( k \) will be given by

\[ P_k = \prod_{i=1}^{j_k} P_{i,k} \]  

(13)

By analogy to the series/parallel system in the reliability context in section 2, the following result (which is an immediate consequence of theorem 2.3) applies:

**PROPOSITION 3.3**

\( \varepsilon \) will vanish if and only if:

\[ P_{i,k} \sim \text{Beta}(c_{ik}, d_{ik}), \quad c_{ik}=c_{i+1,k}+d_{i+1,k}, \quad i=1, \ldots, j_k-1, \quad Q_k \sim \text{Beta}(d_k, c_k), \quad d_k=d_{k+1}+c_{k+1}, \quad k=1, \ldots, n-1 \quad \text{(or equivalently,} \quad P_k \sim \text{Beta}(c_k, d_k), \quad d_k=c_{k+1}+d_{k+1}), \quad d_k=\sum_{i=1}^{j_k} d_{ik}, \quad c_k=c_{jk,k} \]

Again, the defender will be interested in strengthening the different items/components of the system within the allowable ranges while enlarging the discrepancy between the estimated and the exact probabilities of a successful attack. The defender objective function will be to maximize the weighted sum of the probability of a failed attack and the sum of the absolute values of the discrepancies. Moreover, for the discrepancy in the estimation to increase, it is sufficient that none of the conditions imposed by Proposition 3.3 is satisfied and all the corresponding gaps are enlarged as much as possible. This leads to the following objective function:
The corresponding non-smooth optimization model will be given by:

\[
\max Z_i \quad \text{s.t.} \quad c_{ik}^{\min} \leq c_{ik} \leq c_{ik}^{\max}, \quad k = 1, \ldots, n; i = 1, \ldots, j_k
\]

\[
d_{ik}^{\min} \leq d_{ik} \leq d_{ik}^{\max}, \quad k = 1, \ldots, n; i = 1, \ldots, j_k
\]

An equivalent version of the above model would be obtained by introducing a big \( M \), the binary variables \( y_{ik} \) and \( y_k \), and continuous variables \( \eta_{ik} \) and \( \eta_k \) leading to the following model:

\[
\max Z = w_r \left[ \prod_{k=1}^n \left( 1 - \prod_{i=1}^{j_i} \frac{c_{ik}}{c_{ik} + d_{ik}} \right) \right] + w_c \left[ \sum_{k=1}^n \sum_{i=1}^{j_i-1} \eta_{ik} + \sum_{k=1}^{n-1} \eta_k \right]
\]

\[
\text{s.t.} \quad \eta_{ik} - c_{ik} + c_{i+1,k} + d_{i+1,k} - M y_{ik} \leq 0, \quad k = 1, \ldots, n; i = 1, \ldots, j_k - 1
\]

\[
\eta_{ik} + c_{ik} - c_{i+1,k} - d_{i+1,k} + M y_{ik} \leq M, \quad k = 1, \ldots, n; i = 1, \ldots, j_k - 1
\]

\[
\eta_k - \sum_{i=1}^{j_i} d_{ik} + \sum_{i=1}^{j_i+1} d_{i,k+1} + c_{j_i+1,k} - M y_k \leq 0, \quad k = 1, \ldots, n-1
\]

\[
\eta_k + \sum_{i=1}^{j_i} d_{ik} - \sum_{i=1}^{j_i+1} d_{i,k+1} - c_{j_i+1,k} + M y_k \leq M, \quad k = 1, \ldots, n-1
\]

\[
c_{ik}^{\min} \leq c_{ik} \leq c_{ik}^{\max}, \quad k = 1, \ldots, n; i = 1, \ldots, j_k
\]

\[
d_{ik}^{\min} \leq d_{ik} \leq d_{ik}^{\max}, \quad k = 1, \ldots, n; i = 1, \ldots, j_k
\]

\[
\eta_{ik} \geq 0, \quad \eta_k \geq 0, \quad y_{ik}, y_k = 0, 1, \quad k = 1, \ldots, n; i = 1, \ldots, j_k - 1.
\]

Next, the attacker will estimate the values of \( U \) and \( L \) to determine whether or not to attack based on the considered strategy. Note that DP is no longer applicable here, as the number of trials for a given component/item will not depend solely on the number of successes/failures of the immediate predecessor of that component/item, but would depend in general on the results for a number of previous items/components, as illustrated in the example below. Therefore, one should consider nonlinear discrete optimization problems to solve for \( U \) and \( L \). The example below will illustrate the process.

**Example 3.3**

Consider the case of a system of two components in series where each component is a parallel subsystem of two items. Assume that the attacker
strategy is to attack the system if the chance of a successful attack is at least 70% and the error in estimating such a chance is less than 5%. Let the probability of a successful attack on component 1 be \( P_1 \), on component 2 be \( P_2 \), on item 1 of component 1 be \( P_{11} \), on item 2 of component 1 be \( P_{21} \), on item 1 of component 2 be \( P_{12} \), and on item 2 of component 2 be \( P_{22} \). Moreover, assume that:

\[
P_{11} \sim \text{Beta}(c_{11}, d_{11}), \quad P_{21} \sim \text{Beta}(c_{21}, d_{21}), \quad P_{12} \sim \text{Beta}(c_{12}, d_{12}), \quad P_{22} \sim \text{Beta}(c_{22}, d_{22}),
\]

where \( c_{11} = 10, \quad d_{11} = 5, \quad c_{21} = 8, \quad d_{21} = 2, \quad c_{12} = 4, \quad d_{12} = 3, \quad c_{22} = 3 \), and \( d_{22} = 1 \).

Note that perfect aggregation holds. In fact, we have:

\[
c_{11} = 10 = c_{21} + d_{21}, \quad c_{12} = 4 = c_{22} + d_{22}, \quad d_{11} + d_{21} = 7 = c_{12} + d_{12}.
\]

Moreover, the items and components are ordered according to attractiveness. In fact, we have

\[
E(P_{11}) = 2/3 < E(P_{21}) = 4/5, \quad E(P_{12}) = 4/7 < E(P_{22}) = 3/4,
\]

and

\[
E(P_1) = 8/15 > E(P_2) = 3/7.
\]

Note that attractiveness for parallel (respectively series) systems increases with the increase (respectively decrease) of survivability upon an attack. Also, note that \( P_1 \sim \text{Beta}(c_{21} + d_{21}, d_{12} + d_{22}) \).

Finally, assume that the ranges in which the parameters of the prior distributions can lie (if defensive improvements will be undertaken) are as follows: \([7, 13]\) for \( c_{11} \), \([3, 7]\) for \( d_{11} \), \([5, 11]\) for \( c_{21} \), \([1, 3]\) for \( d_{21} \), \([2, 6]\) for \( c_{12} \), \([1.5, 5]\) for \( d_{12} \), \([2, 5]\) for \( c_{22} \), and \([0.5, 2]\) for \( d_{22} \).

Prior to any defensive improvement, the probability of a successful attack is 83.3% and the estimation is error free. Therefore, this situation is favorable for an attack to be launched. Note that the conditions above on the parameters of the conjugate prior distributions are too restrictive to apply in a realistic situation. However, the defensive strategy will not change if the error is nonzero but still sufficiently small. The defender will attempt to decrease the probability of a successful attack and to make the available information as useless as possible through implementing the optimal policy to be obtained by solving (15). Now, using the data above, when both weights are equal, the solution to (15) is given by:

\[
c_{11}^{\text{new}} = 13, \quad d_{11}^{\text{new}} = 3, \quad c_{21}^{\text{new}} = 5, \quad d_{21}^{\text{new}} = 1, \quad c_{12}^{\text{new}} = 2, \quad d_{12}^{\text{new}} = 5, \quad c_{22}^{\text{new}} = 5, \quad d_{22}^{\text{new}} = 2
\]
The gaps reflecting the estimation error are given by \( \eta_{11} = 7 \), \( \eta_{12} = 5 \), and \( \eta_1 = 8 \). The new prior mean probability of a successful attack is 74.3\%. When more weight is placed on increasing the probability of a failed attack (say, \( w_s = 10 \)), then no change occurs in the optimal solution. However, when \( w_s \) increases to 100, then the new mean probability of a successful attack decreases to 41.1\%. On the other hand, the sum of the deviations will decrease from 20 to 4. Note that the defender in this case has enough range for improvement of the defensive system. It seems therefore that the defender should focus more on reducing the size of the probability of a successful attack. Assume therefore that the defender will adopt the last strategy (with \( w_s = 100 \)).

Assuming that the attacker aggregate data is four successful attacks out of six trials, then the disaggregate mean of a successful attack probability will be given by:

\[
E(P|k_0 = 6, k_{11}, k_{21}, k_{12}, k_{22} + k_{21} = 4) =
\left[ 1 - \left( 1 - \frac{c_{11} + k_{11}}{c_{11} + d_{11} + k_0} \right) \left( 1 - \frac{c_{21} + k_{21}}{c_{21} + d_{21} + k_0} \right) \right]
\left[ 1 - \left( 1 - \frac{c_{12} + k_{12}}{c_{12} + d_{12} + k_0 - k_{21}} \right) \left( 1 - \frac{c_{22} + k_{22}}{c_{22} + d_{22} + k_{12}} \right) \right]
\]  

(16)

In (3.16), \( k_{21} + k_{22} = 4 \), \( k_{21} \leq k_{11} \leq k_0 \), and \( k_{22} \leq k_{12} \leq k_0 - k_{21} \). Solving for \( U \) (respectively for \( L \)) consists of maximizing (respectively minimizing) the objective function given by (16) under the above constraints and the integrality of all \( k_{ij} \).

For the example above, using the last values of the Beta parameters obtained by the defender (where the emphasis was to reduce the size of the average probability of a successful attack), the procedure yields: \( U = 0.667 \) and \( L = 0.525 \). Consequently, the estimate of the mean probability of a successful attack will be 0.596, while the estimate of the size of the error is 0.107. That is, the defender succeeds in making the success probability far below the threshold level of 70\% set by the attacker, and in making the error sufficiently large (about twice the threshold level of 5\%). Note, however, that the attacker would have been deterred only by the size of error even if the threshold value had been smaller.

The case of a parallel-series system as well as extensions to more complex configurations of combined series/parallel systems can be treated similarly.
4. **CASE OF INTERMEDIATE LEVELS OF INFORMATION**

We will briefly discuss the case where the information available to the attacker is more than that at the aggregate level (i.e., at the system level only) but without reaching fully the disaggregate level (complete information). If the information about some items/components is accessible to the attacker, then the attacker would use the results on the relevant observations as constant values rather than decision variables in the estimation of $U$ and $L$ which makes the discrepancy $U-L$ smaller than that of the case where the information is available at the aggregate level only. Of course such additional information can not benefit the success probability but could improve the accuracy of its estimation.

**Example 4.1**

Suppose that the attacker in the previous example has access to reliable information on the second item of component 2. Assume therefore that the observed number of successful attacks on that item is $k_{22}=2$. From the aggregate data of 4 successful attacks, it follows that $k_{21}=2$. The optimal solutions to maximize (respectively minimize) the disaggregate mean probability of a successful attack yield $U=0.824$ and $L=0.778$. Consequently, the size of the error will be reduced to 3.45% instead of 10.7%. If, however, the value of $k_{22}$ was zero, then $U=0.760$, $L=0.724$, and the aggregation error will be only 2.7%. This says that the attacker can benefit a great deal by accessing information at some disaggregate levels.

5. **CONCLUSIONS**

In this chapter, a Bayesian model for the game of information in defense/attack strategies is suggested. The attacker would be deterred if the success probability of an attack is not large enough. Because the available information to the attacker is not perfect, then the attacker would also be deterred if the estimation of such a probability could be highly unreliable. The defender seeks to deter the attack either by making the available information as ambiguous as possible to prevent the attacker from a careful estimation of the probability of a successful attack; or by making such a probability sufficiently low. It is assumed that the defender has limited resources and can only make little improvement on system survivability upon an attack. Moreover, the defender has little or no information about the level of success (ambiguity) below (above) which the attack is deterred. Thus, the defender opts for a combined strategy of improving system
survivability and for making the error due to the lack of perfect information as large as possible given the limited range of changes that the defender could perform.

A variety of mixed integer-nonlinear goal programming models are proposed for various system configurations (series, parallel, and combined series/parallel), in which the importance weights are left to the defender to subjectively allocate based on how he/she estimates the opportunity for deterring an attack. The models rely on previous results (by analogy) in the context of perfect aggregation in reliability models as well as on results on optimal attack strategies for combined series/parallel models to determine the sequence of attacks to be carried out to the different components/items of the targeted system. The validity of the results relies on some assumptions specified in section 3.

A natural extension of this work would be to consider in the defensive strategy alternatives to reduce the damage due to an attack in case the defender finds out that no improvement could deter the attacker. Extensions to other system configurations (such as $k$-out-of-$n$ systems) could be another direction for future research. A third future research avenue would be to consider the case where the defender also seeks to gain information about the attacker strategies and/or capabilities. One more direction for future work would be to consider other games of information but with cost considerations. For instance, one could investigate the case where the attacker, having limited budget, may access more pieces of information at some cost. In this case, the attacker would be interested in selecting which pieces of information are the most helpful to make the estimation sufficiently accurate while the defender may invest (also with limited budget) to make the accessible information as costly as possible to the attacker in order to make the most important pieces of information out of the reach of the attacker.

REFERENCES


Dighe, N. S., Zhuang, J., and Bier, V. M., 2008, Secrecy in defensive allocations as a strategy for achieving more cost-effective attacker deterrence, accepted for publication in the International Journal of Performability.


ACKNOWLEDGMENT

The author would like to thank Professor Vicki Bier for her invaluable assistance that enhanced significantly both the quality of the content and the clarity of the presentation of this work.
Chapter 6

SEARCH FOR A MALEVOLENT NEEDLE IN A BENIGN HAYSTACK

D. P. Gaver, K. D. Glazebrook, and P. A. Jacobs

Abstract: A domain contains a number \( w \) of non-hostile White (W) individuals: humans, vehicles, ships. A hostile Red (R) individual enters the domain and travels through the domain towards targets. If R reaches an attractive valuable target, perhaps a crowd of people on land or a ship at sea containing liquid natural gas (LNG), it attacks the target. A Blue counter-terrorist, C, patrols the domain and classifies (perhaps incorrectly) individuals of interest as R or W. The probability of correct classification is an increasing function of the time spent classifying an individual. The misclassification of a W as an R is a false positive; misclassification of the R as a W is a false negative. C follows (or tracks) any individual it classifies as R until it is relieved by another platform or individual that may neutralize the possible R. C is unable to detect and classify additional individuals while it is following a suspicious individual. A small classification time may yield many false positives that C must service. A large classification time may result in R achieving its goal before being neutralized, so an appropriate compromise is sought.

A game-theoretic model is formulated and studied to evaluate the probability that R is successfully neutralized before achieving its goal. C’s policy is to choose a classification time. Targets have independent identically distributed (iid) values, and R’s policy is to specify a target value threshold; R will attack the first target it finds whose value exceeds the threshold unless neutralized first.

Key words: maritime domain awareness and protection; port security; suicide bomber; Nash equilibrium
1. INTRODUCTION AND FORMULATIONS

Consider an arena (Kress, 2005) or domain, D (Gaver et al., 2006; Gaver et al., to appear), i.e., a spatial region, in which a collection of benign/harmless entities, called Whites (Ws) gather. These can be passengers and accompanying individuals in a boarding lounge awaiting an airline flight, bus, or other conveyance. Alternatively, the collection is a crowd of potential workers assembled to obtain jobs. Another example could be a group of military platforms parked closely outside a repair facility, or the collection of neutral vessels used for recreation, commerce or defense occupying a maritime domain neighboring a harbor; see Gaver et al., 2006; and Gaver et al., to appear). Still another could be a large queue outside a medical emergency care clinic or hospital; the queue is the result of a surge of injuries, possibly from natural causes, such as Katrina, (for instance the refugees being packed into the New Orleans Coliseum). There are many equally important examples.

Such a collection-crowd-"haystack" is the natural target for a single suicide bomber, denoted R, or for a malevolently-inclined “Red” maritime domain invader, (e.g., a small boat), likely disguised to resemble benign Ws in size, appearance, and behavior. Presumably it will attempt to surreptitiously mingle with the White crowd and pick a moment for detonation that creates a maximum number of casualties. This suggests that R should seek to be in the part of D where most, or most-apparently-valuable Ws congregate. On the other hand, the effect of a suicide bomb in a densely packed region could be counterproductive: Ws near the explosion will likely be hit/killed, but their bodies shield those slightly further away; see Kress (2005).

Now introduce (at $t = 0$, initiation of the process) a single friendly searcher-neutralizer into the domain D; denote such a “Blue” counter-terrorist by C. In fact, there could be several such, and they need not be identical, but complementary; for example, on land, one or more areas could be equipped with active and sensitive trained dogs, which would be visible and tend to herd the R—along with some Ws—into a subdomain $D' \subset D$ that can be quickly searched by C; on the other hand if such herding occurred it might trigger early detonation by R. We omit such plausible modeling options for the present.

The scenario is that C searches/detects/travels to an individual. The search/detect/travel times to successive individuals are independent and identically distributed (iid). The individual is then classified as either a W or an R; classification takes a time $\tau$, a decision variable. The probability of a correct classification is an increasing function of $\tau$. If the individual is classified as an R (perhaps incorrectly), the C follows/tracks the individual until it is relieved by another platform or individual. C then resumes
searching. The successive follow/tracking times are iid, and C cannot detect/classify other individuals while it is following a suspicious individual. There is a constant number of Ws in the domain; these could be individuals that are unclassified by other means. If the classification time $\tau$ is too small, then C may be prone to misclassify Ws as Rs and may spend substantial time following benign individuals, increasing the possibility that R reaches its objective. If the classification time is too large, then R may reach its objective before C detects and correctly classifies it.

We make the following assumptions:

1. There is only one R.
2. There is a constant number of Ws in the domain and detected individuals are obtained by sampling with replacement from the population of Ws and R. C does not retain or use information about individuals who were closely examined, classified, and then released. Once a W is classified as a W, it is not tagged, and may be classified again; correct tagging can be a great advantage, but incorrect tagging can be enormously counter productive. We postpone the discussion of tradeoffs. Alternatively, a classified W is replaced by another W entering the domain.
3. The W’s are a subset of the entire population. The remainder of the population is classified as harmless as a result of a first cursory surveillance; we assume that this first cursory surveillance is perfect. The Ws are members of the population that are subject to further surveillance.

Section 2 presents an optimization model where the goal is the maximization of the probability that C successfully neutralizes R. Examples are presented illustrating the tradeoff between a large classification time $\tau$ resulting in a larger probability of correct classification but also a smaller effective search rate. Section 3 presents a game that elaborates the model for R. Possible targets for R have iid values. R encounters targets according to a Poisson process. R kills the first target it encounters whose value exceeds a predetermined threshold, unless C neutralizes R first. C chooses a classification time $\tau$ to minimize the maximum value of the expected killed target value, while R chooses a threshold value to maximize the minimum expected killed target value. Section 4 concludes the paper.

2. **STOCHASTIC MODEL 1**

In this model, R detonates after an exponential time, presumably when near a valuable target. The model of Section 3 makes this more explicit. Model parameters and random variables appear below.
\( \delta_s dt \) = the probability that R detonates in \((t, t + dt)\), given that it has not
done so before \( t \), and has not been neutralized by C. Choice of detonation to
achieve a specified value/effect is considered later in Section 3. Note: We
could let \( \delta_s = \delta_s(x) \), where \( x \) stands for various conditions, such as elapsed
time or environmental conditions; omitted for present.

\( D = \) time to detonate if not neutralized. We let \( D \) be random having an
exponential distribution:

\[
P\{D > t | \text{Not neutralized}\} = \exp[-\delta_s t].
\] (2.1)

\( T_c \) is a random time from when C has finished processing (classifying
and perhaps tracking) a detected individual until C detects and travels to
another member of the Ws or the single R in D; \( T_c \) will depend on the size
of the domain, the environment, the number of Ws in the domain, C’s speed,
the search pattern, etc. Successive detection/travel times are iid.

\[
k_r(\bullet) = \frac{1}{w+1} \quad \text{(respectively, } k_w(\bullet) = \frac{w}{w+1}\text{)}
\]
is the probability that the
detected individual is the R (respectively, a benign W).

Let \( p_{rr}(\tau) \) be the conditional probability that the detected R is classified
as R when \( \tau \) time units are spent classifying it; \( p_{rr}(\tau) \) is an increasing
function of \( \tau \) where \( \tau \) is a decision parameter. The probability that the
detected R is misclassified is \( p_{rw}(\tau) = 1 - p_{rr}(\tau) \). Similarly, let \( p_{ww}(\tau) \) be
the conditional probability that a detected W is classified as W when \( \tau \) time
units are spent classifying it; \( p_{wr}(\tau) = 1 - p_{ww}(\tau) \) is the probability that a
detected W is misclassified as R (a false positive). The response to a false
positive is that the counter-terrorist, C, takes intensive (but futile) action to
thwart a potential suicide attack (e.g., by neutralizing or disabling the
misidentified attacker, thus unnecessarily losing valuable search time).

Let \( X_c \) be a random service or response time to thoroughly examine and
neutralize a captured true R (provided that it is disabled before detonation),
or to examine and release a false positive W. Successive response times are
iid. The response time is in addition to the classification time. Of course, the
response time is a penalty time to C if the examination/neutralization is of a
W that was incorrectly classified as R. During this time, C is occupied by
following and neutralizing the potential R and cannot search for other
possible Rs. Neutralization involves tracking the suspicious individual until
escort personnel arrive, after which the suspicious individual is escorted to
another position for further examination. If R detects unusual attention by
something it interprets as C, it may well detonate shortly before
apprehension by C; however, R might also choose to leave D in that case, or attempt to sidle close to C and then detonate, thus achieving an extra bonus. We do not treat such concept of operations on the part of R here, but intend to do so in later work.

$I_{cr}(\tau) =$ the total elapsed clock/calendar time to detect, identify, and neutralize the (true) R when the classification time is $\tau$. For simplicity, this includes the (random) time “used up” in discovering that potential Rs are actually benign, (i.e., that they are instead harmless Ws). We presume that neutralization of a suspect is not terminal; the suspect is fully disabled and searched, possibly off-site. In some cases, this will be wasted time, of course. A serious issue to avoid would be serious harm to an individual that turns out to be an innocent bystander.

Conditional on $I_{cr}(\tau)$, the time to neutralize R, the probability that R is neutralized in time (before detonation) is $\exp[-\delta_I I_{cr}(\tau)]$. This event (preemptive neutralization) can take place under two conditions:

(i) the first time C detects a suspicious individual, that individual is R, and is correctly identified, and thoroughly neutralized; or

(ii) the first time C detects a suspicious individual, that individual is R and that individual is misclassified and released, or that individual is a W and is correctly classified and released. At this point the search begins over from scratch, as in renewal theory.

Note (again) that the present model is (conservatively) memoryless: there is no tagging or labeling of those suspicious individuals that are released. Correct tagging would increase the rate at which R could be neutralized, and is a strong candidate for future study. However, high rates of incorrect tagging could lead to severe degradation of C’s operational success.

Let the unconditional probability that R is detected and neutralized before it detonates be given by

$$P_B(\tau) = E\left[ e^{-\delta_I I_{cr}(\tau)} \right].$$

This is the success probability for C when $\tau$ time units are spent classifying a suspicious individual. Conditionally, using (i) and (ii), we have
\[ P_B(\tau) = E \left[ \exp\left\{ -\delta_s T_c - \delta_s \tau \right\} k_r(\cdot) p_{rr}(\tau) \exp\left\{ -\delta_s X_c \right\} \right] \]
\( \text{(a*)} \)

\[ + E \left[ \exp\left\{ -\delta_s T_c - \delta_s \tau \right\} k_w(\cdot) p_{ww}(\tau) \right] \frac{P_B(\tau)}{P_B(\tau)} \]
\( \text{(b*)} \quad (2.3) \)

\[ + E \left[ \exp\left\{ -\delta_s T_c - \delta_s \tau \right\} k_w(\cdot) p_{wr}(\tau) \exp\left\{ -\delta_s X_c \right\} \right] \frac{P_B(\tau)}{P_B(\tau)} . \]
\( \text{(c*)} \)

\[ + E \left[ \exp\left\{ -\delta_s T_c - \delta_s \tau \right\} k_r(\cdot) p_{rw}(\tau) \right] \frac{P_B(\tau)}{P_B(\tau)} . \]
\( \text{(d*)} \)

Solving gives C’s success probability:

\[ P_B(\tau) = \frac{E \left[ \exp\left\{ -\delta_s T_c - \delta_s \tau \right\} k_r(\cdot) p_{rr}(\tau) \exp\left\{ -\delta_s X_c \right\} \right]}{D(T_c, X_c)} \]
\( \text{(2.4,a)} \)

where

\[ D(T_c, X_c) \]
\[ = 1 - E \left[ \exp\left\{ -\delta_s T_c - \delta_s \tau \right\} k_w(\cdot) p_{ww}(\tau) \right] \]
\[ - E \left[ \exp\left\{ -\delta_s T_c - \delta_s \tau \right\} k_w(\cdot) p_{wr}(\tau) \exp\left\{ -\delta_s X_c \right\} \right] \]
\[ - E \left[ \exp\left\{ -\delta_s T_c - \delta_s \tau \right\} k_r(\cdot) p_{rw}(\tau) \right] . \]
\( \text{(2.4,b)} \)

Note that the term (c*) in equation (2.3) could be modeled in several alternative ways. First, W can be incorrectly classified as R in which case C tracks the W for a relatively short time \( X_c \) until relieved by an auxiliary platform with a sensor, (e.g. an unmanned aerial vehicle (UAV)). In this case, C may simply cease searching, or move to another area, so the search may never re-start; in this case, R will never be detected. Alternatively, W can be incorrectly classified as R, and \( X_c \) represents the relatively long time for an escort team to arrive and assume responsibility for the target. Then the C may begin searching again if at the termination the target is identified as...
6. Search for a Malevolent Needle in a Benign Haystack

an innocuous W. Variations in equation (2.3) can therefore be justified (e.g., if Blue search incorrectly terminates), but are not included here.

EXAMPLE

All numerical examples will use the following maritime domain protection scenario. An aircraft, C, is patrolling a rectangular domain; $M_x$ is the $x$-distance of the rectangular domain; $M_y$ is the $y$-distance of the domain. R is a small boat carrying explosives. C uses a sensor to search the domain. The footprint of the sensor is a square with length of a side equal to $f$. The total time for C to cover a one-footprint square is $f/v_s$; $v_s$ is the velocity of the aircraft. The mean time for C to cover the domain is $\left[ M_x \times M_y / f^2 \right] f/v_s$; the mean time between detection of individuals is $\left[ M_x \times M_y / f^2 \right] f/v_s / (w+1)$, where $w$ is the (constant) number of benign Ws in the domain. When C classifies a vessel as R, it tracks the vessel until it is relieved by another platform.

For illustration, let

$$p_{ww}(\tau) = p_{rr}(\tau) = \exp\left\{ -\alpha / \tau^\beta \right\}$$

(2.5)

for $\tau > \tau_{0.5}$ where $\tau_{0.5}$ is the time at which the probability of correct classification is 0.5. Note that $p_{ww}(\tau)$ is a cumulative Fréchet distribution function (which optimistically approaches unity for $\tau$ increasing). The parameters $\alpha$ and $\beta$ (both positive) are determined here by specifying two quantiles (in this case the median, $\tau_{0.5}$, and the 90th percentile, $\tau_{0.9}$). If data were available, $\alpha$ and $\beta$ could be statistically estimated using maximum likelihood or Bayes inference. Since $p_{ww}(\tau) = p_{rr}(\tau)$, we are assuming that R is attempting to blend in with Ws in the domain (although there are of course other possibilities). Table 6-1 displays some parameter values.

Figure 6-1 displays the probability that R is neutralized before it detonates as a function of the time spent classifying a detected individual, when the search/detect travel times $T_c$ and the additional time the sensor is engaged for response to an individual classified as R (service/response time) $X_c$ are both gamma distributed with shape parameter 0.1. The mean response time is 0.2 hours. For comparison, if there are no benign vessels, and classification takes no time and is perfect, then the probability of neutralizing R is 0.82.
Table 6-1. Parameter values for Model 1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E[T_c]$</td>
<td>Mean time to search/detect a suspicious individual (hrs.)</td>
<td>Variable</td>
</tr>
<tr>
<td>$p_{rr}(\tau) = p_{ww}(\tau)$</td>
<td>Probability of correct classification</td>
<td>$\tau_{0.5} = 3/60$ hrs. $\tau_{0.9} = 6/60$ hrs.</td>
</tr>
<tr>
<td>$\beta$</td>
<td>Parameter (“shape”) for the probability of correct classification</td>
<td>2.72</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>Parameter (“scale”) for the probability of correct classification</td>
<td>0.0002</td>
</tr>
<tr>
<td>$w$</td>
<td>Number of benign Ws in the domain</td>
<td>Variable</td>
</tr>
<tr>
<td>$k_w = 1 - k_{ww}$</td>
<td>Probability detected individual is the R</td>
<td>$1/(1 + w)$</td>
</tr>
<tr>
<td>$E[X_c]$</td>
<td>Mean time for second more intensive inspection (response time) (hrs.)</td>
<td>Variable</td>
</tr>
<tr>
<td>$1/\delta_x$</td>
<td>Mean time until the R detonates if it is not neutralized (hrs.)</td>
<td>6</td>
</tr>
<tr>
<td>$f$</td>
<td>Side of square sensor footprint in nautical miles (nm)</td>
<td>10</td>
</tr>
<tr>
<td>$v_y$</td>
<td>Velocity of sensor platform in knots (kts)</td>
<td>250</td>
</tr>
<tr>
<td>$M_x$</td>
<td>Length of $x$-direction of rectangular domain (nm)</td>
<td>75</td>
</tr>
<tr>
<td>$M_y$</td>
<td>Length of $y$-direction of rectangular domain (nm)</td>
<td>100</td>
</tr>
</tbody>
</table>

Figure 6-1. Probability R is neutralized in Model 1.

**DISCUSSION**

The optimal classification time decreases a little as the number of benign Ws in the domain increases. However, even if the estimate of the number of Ws is wrong, the optimal classification time still seems to perform reasonably well. The probability of neutralizing R is sensitive to the number of benign Ws. Fewer benign Ws in the domain result in larger times between
detections of suspicious individuals, and a larger probability of neutralizing R. Results of Gaver et al. (2006, to appear) suggest that the probability of neutralizing R is sensitive to the distribution of the travel and response times. Note also that a large classification time is less harmful than a short time.

The sensitivity of the best classification times to the model assumptions and the parametric form for the probability of correct classification is next explored. The model parameters are those of Table 6-1 unless otherwise displayed in Table 6-2.

Table 6-2. Parameter values for sensitivity analysis

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E[T_c]$</td>
<td>Mean time between detections of suspicious individuals (hrs.)</td>
</tr>
<tr>
<td>$p_{rr}(\tau) = p_{ww}(\tau)$</td>
<td>Probability of correct classification</td>
</tr>
<tr>
<td>$\beta$</td>
<td>Parameter (&quot;shape&quot;) for the probability of correct classification</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>Parameter (&quot;scale&quot;) for the probability of correct classification</td>
</tr>
<tr>
<td>$w$</td>
<td>Number of benign Ws in the domain</td>
</tr>
<tr>
<td>$E[X_c]$</td>
<td>Mean response time (hrs.)</td>
</tr>
</tbody>
</table>

Three distributional forms are considered for the search/travel times to individuals and the additional time the searcher is engaged when an individual is classified as R (response time). In each case, the distributional family is the same for both times. The distributions considered are constant times, exponential distributions, and gamma distributions with shape parameter 0.1. The means of the travel (respectively, response) times are equal in all cases.

Two functional forms are considered for the probability of correct classification when the classification time is $\tau$. These forms are the Fréchet distribution in (2.5) and the Weibull distribution,

$$p_{ww}(\tau) = p_{rr}(\tau) = 1 - \exp \left\{ -\alpha \tau^\beta \right\} ; \quad (2.6)$$

In both cases, the parameters $\alpha$ and $\beta$ are found by specifying the median and 90th percentile of the distribution. The median is $\tau_{0.5} = 0.05$ hours in all cases. The classification times considered are only those greater than or equal to the median of the time for correct classification (i.e. the probability of correct classification is at least 0.50).

Figures 6-2a and 6-2b display the classification times $\tau$ that maximize the probability of neutralizing R for various values of $\tau_{0.9}$;
Figure 6-2a. Best classification time for Model 1 with Fréchet probability of correct classification.

Figure 6-2b. Best classification time for Model 1 with Weibull probability of correct classification.

\[ p_{ww}(\tau_{0.9}) = p_{rr}(\tau_{0.9}) = 0.9 \]. Figure 6-3 displays the resulting probabilities of correct classification for the best classification time using the Fréchet probability of correct classification from equation (2.5). Figure 6-4 displays
results comparing the use of different C classification times when C’s travel and response times have a gamma distribution with shape parameter 0.1 and the classification probabilities are given by equation (2.5). Figure 6-4 displays: the resulting maximum probability of neutralizing R; the probability of neutralizing R if the classification time is given by \( \tau = \tau_{0.9} \); the probability of neutralizing R if \( \tau = \tau_{0.5} \); the probability of neutralizing R for the policy that uses the (incorrect) exponential distribution for the travel and response times; and the probability of neutralizing R for the policy that uses the (incorrect) Weibull distribution for the classification probabilities. For comparison, if the classification time is 0 and classification is perfect, then the probability of neutralizing R is 0.72 for the parameter values of Figure 6-4.

![Figure 6-3. Probability of correct classification for the best classification time in Model 1 with Fréchet probability of correct classification.](image)

As can be seen, the best classification times are smaller for travel and response times having gamma distributions with shape parameter 0.1 than for the other cases. Since the travel times and response times are more likely to be less than their means in the gamma case, one can afford to have a slightly smaller probability of correct classification. The maximizing classification times are apparently concave as a function of \( \tau_{0.9} \). If \( \tau_{0.9} \) is close to \( \tau_{0.5} \), then the maximizing classification time is close to (but larger than) \( \tau_{0.9} \); it increases as \( \tau_{0.9} \) increases and results in a maximum probability of correct classification greater than 0.9. Eventually, \( \tau_{0.9} \)
becomes too large (with respect to $\tau_{0.5} = 0.05$), and the maximizing classification time begins to decrease slightly, with the resulting probability of correct classification decreasing to about 0.7. In Figure 6-4, the probability of neutralizing R is about the same regardless of whether the classification time is based on the correct model, the incorrect exponential distribution, or the incorrect Weibull distribution. In fact in Figure 6-4, the probabilities of neutralizing R are indistinguishable for these cases. Thus, Figure 6-4 suggests that the best classification times are somewhat insensitive to these model assumptions.

3. STOCHASTIC MODEL 2

A lethal Red, R, stalks groups or clusters of neutral Whites at random in an arena or domain. Assume that R eventually identifies a group of sufficiently high threshold value; the value is the size of the group or the importance of its constituency. The R mingles with this group and self-destructs, reducing the value of the group from $V$ to $0 \leq V' \leq V$. Given that one (or more) counter-terrorists are in search of R, and require time to thoroughly identify a suspect—which may be ill-advised if the suspect is only a harmless White (W)—what is an optimal strategy for R to pick a target group, and for the counter-terrorist C to detain a potential R, when there is a chance that C is actually neutralizing a neutral (White)?
Suppose $R$ encounters or contacts groups of possible targets at random in
a Poisson manner at rate $\lambda$, and suppose the $i$th group to appear has a
random value, $V_i$; the values of the various groups are assumed iid. It may
be that $V_i$ is merely the number of individuals in the group, but it could also
be the value associated with a single exceptional individual (person, or
platform). If $F$ is the distribution from which the collection of $\{V_i\}$ is
drawn, then the maximum group value seen by $R$ in $(0, t]$ has distribution

$$P\{V(t; M) \leq v\} = \sum_{n=0}^{\infty} e^{-\lambda t} \frac{[\lambda t]^n}{n!} [F(v)]^n$$

$$= e^{-\lambda t [1-F(v)]} \equiv e^{-\lambda t F(v)}.$$

While $R$ hunts for valuable White targets, Blue $C$ searches for $R$ as
effectively and surreptitiously as possible.

$R$ chooses a minimum threshold value $\omega$ for a target to pursue. $R$
detonates the first time it encounters a target with value at least $\omega$. The time
until $R$ detonates, $D$, has an exponential distribution with mean

$$1/ \delta_s(\omega) = 1/ \lambda [1 - F(\omega)] \equiv 1/ \lambda F(\omega).$$

### 3.1 Blue Searcher Strategy

The Blue searcher, $C$, covers or searches the domain. $C$ chooses a time $\tau$
to spend classifying detected individuals. The probability that $R$ does not
detonate before it is neutralized is $P_{B}(\tau)$ given in equations (2.4a–2.4b)
with $\delta_s = \delta_s(\omega)$ given by equation (3.2). Hence, the expected lethal value
achieved by the $R$ is

$$E[V; \omega, \tau]$$

$$= \int_{0}^{\infty} v F(dv)$$

$$= [1 - P_{B}(\tau)]^\omega \frac{\omega}{F(\omega)}.$$
C’s problem: \[ \min_{\tau > \tau_{0.5}} \max_{\omega} \mathbb{E}[V; \omega, \tau] \]
for \( \tau > \tau_{0.5} \) given \( r \). 

R’s problem: \[ \max_{\omega} \min_{\tau > \tau_{0.5}} \mathbb{E}[V; \omega, \tau] \]
for \( \tau > \tau_{0.5} \) given \( \omega \).

Empirical evidence suggests that this game has a Nash equilibrium; see Figure 6-5.

**Example**

Assume that the target values have an exponential distribution. The travel times of C between individuals, \( T_c \), and the time until C is relieved after classifying an individual as R, \( X_c \), are independent and exponentially distributed. Moreover, we assume that \( P_{ww}(\tau) = P_{rr}(\tau) = \exp\left\{-\alpha / \tau^\beta\right\} \) for \( \tau > \tau_{0.5} \). Figure 6-5 displays the expected value of the return to R as a function of R’s threshold and C’s classification time for the model parameters displayed in Table 6-1. In Figure 6-5 \( \mathbb{E}[T_c] = 0.5 \) hours, \( \mathbb{E}[X_c] = 1 \) hours, the rate at which R encounters groups is 2 per hour, and the mean group size is 10. Note that the function apparently has a saddle point.

Parameter values are displayed in Table 6-3. Table 6-4 displays the best policies for both C and R for various values of the mean time until C is relieved after classifying an individual as R, the number of Ws in the domain, and the mean target value. Table 6-4 displays results for two different distributions for C’s travel times and response times. The family of distributions is assumed to be the same for both travel times and response times; the two distributions are the exponential distribution and the gamma distribution with shape parameter 0.1 having the same mean as the exponential. Such a positively skewed gamma represents substantial spatial clumpiness of surface entities, hence permitting C to investigate several suspicious individuals in more rapid succession than would be true for the exponential case; see the right-most column of Table 6-4.

**Discussion**

The expected lethal value achieved by R increases: as the mean time until the searcher is relieved, \( \mathbb{E}[X_c] \), increases; as the mean target value
6. Search for a Malevolent Needle in a Benign Haystack

**Figure 6-5.** Expected value of the return to R.

**Table 6-3.** Parameter values for Model 2

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_{rr}(\tau) = P_{ww}(\tau)$</td>
<td>Probability of correct classification</td>
</tr>
<tr>
<td>$P_{rr}(\tau) = P_{ww}(\tau)$</td>
<td>$\tau_{0.5} = 3/60 \text{hrs.}$</td>
</tr>
<tr>
<td>$P_{rr}(\tau) = P_{ww}(\tau)$</td>
<td>$\tau_{0.9} = 5/60 \text{hrs.}$</td>
</tr>
<tr>
<td>$\beta$</td>
<td>Parameter (“shape”) for the probability of correct classification</td>
</tr>
<tr>
<td>$\beta$</td>
<td>3.69</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>Parameter (“scale”) for the probability of correct classification</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>0.00001</td>
</tr>
<tr>
<td>$k_r = 1 - k_w$</td>
<td>Probability detected individual is the R</td>
</tr>
<tr>
<td>$k_r = 1 - k_w$</td>
<td>$1/(1 + w)$</td>
</tr>
<tr>
<td>$f$</td>
<td>Side of square sensor footprint (nm)</td>
</tr>
<tr>
<td>$f$</td>
<td>10</td>
</tr>
<tr>
<td>$v_s$</td>
<td>Velocity of sensor platform (kts)</td>
</tr>
<tr>
<td>$v_s$</td>
<td>250</td>
</tr>
<tr>
<td>$M_x$</td>
<td>Length of $x$-direction of rectangular domain (nm)</td>
</tr>
<tr>
<td>$M_x$</td>
<td>20</td>
</tr>
<tr>
<td>$M_y$</td>
<td>Length of $y$-direction of rectangular domain (nm)</td>
</tr>
<tr>
<td>$M_y$</td>
<td>20</td>
</tr>
</tbody>
</table>

increases; and as the rate at which R encounters possible targets increases. The best threshold value $\omega$ for R increases in the mean of $X_c$, the mean target value, the number of Ws, and the rate at which R encounters possible targets. The best classification time $\tau$ for the searcher increases as the mean of $X_c$ increases. The best classification time $\tau$ for the searcher appears not
Table 6-4. Representative results for Model 2

<table>
<thead>
<tr>
<th>Rate R</th>
<th>Expected Value Achieved by R</th>
<th>τ</th>
<th>ω</th>
<th>Probability R is Neutralized</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exponential (Gamma)</td>
<td></td>
<td></td>
<td>Exponential (Gamma)</td>
</tr>
<tr>
<td></td>
<td>Encounters Targets</td>
<td>Mean Target Value</td>
<td>λ</td>
<td>Exponential (Gamma)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.1</td>
<td>0.1</td>
<td>0</td>
<td>5</td>
<td>0.18</td>
</tr>
<tr>
<td></td>
<td>[0.17]</td>
<td></td>
<td></td>
<td>[0.084]</td>
</tr>
<tr>
<td>0.5</td>
<td>0.1</td>
<td>0</td>
<td>5</td>
<td>0.36</td>
</tr>
<tr>
<td></td>
<td>[0.32]</td>
<td></td>
<td></td>
<td>[0.084]</td>
</tr>
<tr>
<td>0.1</td>
<td>0.1</td>
<td>5</td>
<td>5</td>
<td>0.41</td>
</tr>
<tr>
<td></td>
<td>[0.41]</td>
<td></td>
<td></td>
<td>[0.080]</td>
</tr>
<tr>
<td>0.5</td>
<td>0.1</td>
<td>5</td>
<td>5</td>
<td>0.65</td>
</tr>
<tr>
<td></td>
<td>[0.61]</td>
<td></td>
<td></td>
<td>[0.098]</td>
</tr>
<tr>
<td>0.1</td>
<td>0.1</td>
<td>10</td>
<td>5</td>
<td>0.63</td>
</tr>
<tr>
<td></td>
<td>[0.62]</td>
<td></td>
<td></td>
<td>[0.080]</td>
</tr>
<tr>
<td>0.5</td>
<td>0.1</td>
<td>10</td>
<td>5</td>
<td>0.90</td>
</tr>
<tr>
<td></td>
<td>[0.86]</td>
<td></td>
<td></td>
<td>[0.100]</td>
</tr>
<tr>
<td>0.1</td>
<td>0.1</td>
<td>0</td>
<td>10</td>
<td>0.36</td>
</tr>
<tr>
<td></td>
<td>[0.35]</td>
<td></td>
<td></td>
<td>[0.084]</td>
</tr>
<tr>
<td>0.5</td>
<td>0.1</td>
<td>0</td>
<td>10</td>
<td>0.73</td>
</tr>
<tr>
<td></td>
<td>[0.65]</td>
<td></td>
<td></td>
<td>[0.084]</td>
</tr>
<tr>
<td>0.1</td>
<td>0.1</td>
<td>5</td>
<td>10</td>
<td>0.83</td>
</tr>
<tr>
<td></td>
<td>[0.82]</td>
<td></td>
<td></td>
<td>[0.080]</td>
</tr>
<tr>
<td>0.5</td>
<td>0.1</td>
<td>5</td>
<td>10</td>
<td>1.30</td>
</tr>
<tr>
<td></td>
<td>[1.22]</td>
<td></td>
<td></td>
<td>[0.098]</td>
</tr>
<tr>
<td>0.1</td>
<td>0.1</td>
<td>10</td>
<td>10</td>
<td>1.25</td>
</tr>
<tr>
<td></td>
<td>[1.25]</td>
<td></td>
<td></td>
<td>[0.080]</td>
</tr>
<tr>
<td>0.5</td>
<td>0.1</td>
<td>10</td>
<td>10</td>
<td>1.81</td>
</tr>
<tr>
<td></td>
<td>[1.71]</td>
<td></td>
<td></td>
<td>[0.100]</td>
</tr>
<tr>
<td>0.1</td>
<td>1.5</td>
<td>5</td>
<td>10</td>
<td>9.12</td>
</tr>
<tr>
<td></td>
<td>[6.84]</td>
<td></td>
<td></td>
<td>[0.078]</td>
</tr>
<tr>
<td>0.5</td>
<td>1.5</td>
<td>5</td>
<td>10</td>
<td>11.64</td>
</tr>
<tr>
<td></td>
<td>[8.16]</td>
<td></td>
<td></td>
<td>[0.088]</td>
</tr>
<tr>
<td>0.1</td>
<td>1.5</td>
<td>10</td>
<td>10</td>
<td>11.84</td>
</tr>
<tr>
<td></td>
<td>[8.89]</td>
<td></td>
<td></td>
<td>[0.078]</td>
</tr>
<tr>
<td>0.5</td>
<td>1.5</td>
<td>10</td>
<td>10</td>
<td>14.26</td>
</tr>
<tr>
<td></td>
<td>[10.31]</td>
<td></td>
<td></td>
<td>[0.090]</td>
</tr>
</tbody>
</table>

to depend strongly on the mean target value. The gamma distribution for the $T_c$ and $X_c$, results in shorter optimal classification times for the searcher than for the exponential distribution. Apparently, this is due to the fact that C’s travel times and response times are more likely to be less than their means in the gamma case than in the exponential case. The probability of neutralizing R decreases in $\lambda$, since small values of $\lambda$ reflect R’s difficulty finding targets; thus, it is apparently worthwhile to “harden” facilities in order to deny R access to potential targets.
The sensitivity of the searcher’s best classification times and best threshold values, \( \omega \), to model assumptions and parametric forms is now explored. The model parameters are those of Table 6-1, as modified by Table 6-2. The rate at which R encounters individuals is given by \( \lambda = 2 \), and the mean of the exponential target values is 5. As before, two distributional forms are considered for the searcher’s travel time and the response time with the same distributional family used for both times. The distributions considered are the exponential distribution and the gamma distribution with shape parameter 0.1. The means of the travel (respectively, response) times are equal in all cases. Two functional forms are considered for the probability of correct classification when the classification time is \( \tau \). These forms are the Fréchet distribution of equation (2.5) and the Weibull distribution of equation (2.6). As before, the parameters \( \alpha \) and \( \beta \) are determined by specifying the median and 90\(^{th}\) percentile of the distribution and only classification times greater than or equal to the median are considered.

Figures 6-6a and 6-6b display the optimal classification times \( \tau \) for various values of \( \tau_{0.9} \) when \( \tau_{0.5} = 0.05 \). Figure 6-7 displays the resulting probabilities of correct classification for the best classification times for the Fréchet classification probability function. Figure 6-8 (respectively Figure 6-9) displays the best threshold value, \( \omega \), (respectively, the expected target value achieved by R) for the two distributions for the searcher’s travel and response times. Figure 6-10 (respectively Figure 6-11) displays the resulting best game probability of neutralizing the R (respectively the expected target value achieved by R) for various choices of classification times when C’s travel and response times have a gamma distribution with shape parameter 0.1 and the probability of correct classification is of form (2.5); the classification times considered are the best classification time; \( \tau_{0.9} \); \( \tau_{0.5} \); the best classification time for the incorrect model of exponential times; and the best classification time for incorrect Weibull classification probabilities. In all cases R is assumed to use its optimal threshold value \( \omega \) for the correct model.

The best classification times are smaller for travel and response times having gamma distributions with shape parameter 0.1 than for those with an exponential distribution. Since the travel and response times are more likely to be less than their means in the gamma case, one can afford to have a slightly smaller probability of correct classification. The maximizing classification times are apparently concave as a function of \( \tau_{0.9} \). Figure 6-8 suggests that the maximizing threshold value for R is about the same regardless of whether the searcher’s travel and response times are exponential or gamma distributed. However, R achieves a lower expected target value for gamma distributed searcher travel and response times than in
Figure 6-6a. Best classification time for Model 2 with Fréchet probability of correct classification.

Figure 6-6b. Best classification time for Model 2 with Weibull probability of correct classification.

the exponential case. Figures 6-10 and 6-11 suggest setting the classification time equal to $\tau_{0.9}$ results in almost the same probability of neutralizing R as using the optimal classification time for values of $\tau_{0.9}$ between 0.06 hours and 0.4 hours; however, the probability of neutralizing R decreases for larger
6. Search for a Malevolent Needle in a Benign Haystack

Figure 6-7. Probability of correct classification for the best classification time in Model 2 with Fréchet probability of correct classification.

Figure 6-8. Best R threshold value for Model 2 with Fréchet probability of correct classification.

values of $\tau_{0.9}$. Thus, it is apparently worthwhile for the searcher to determine and use the optimal classification time at least when large classification times might be needed to achieve a 90% probability of correct classification. Figures 6-10 and 6-11 suggest that the probability of
Figure 6-9. Expected target value achieved by R for Model 2 with Fréchet probability of correct classification.

neutralizing R is somewhat insensitive to both the distributional form of the searcher’s travel and response times and the model for the probability of correct classification.
4. CONCLUSIONS

In the scenario described in this chapter, there are neutral individuals, Whites (W), and one hostile individual, Red (R), traveling within a domain. The R’s purpose is to attack a target. A patrolling counter-terrorist, C, detects individuals in the domain, and classifies them as W or R. The probability of correct classification is an increasing function of the classification time. C follows each individual that is classified as R (perhaps incorrectly) until relieved by others; during this time, C is unavailable to detect and classify additional individuals. The ability to detect and correctly classify R before R reaches its objective is influenced by the size of the domain, the number of Ws in the domain, and the probability of correctly classifying detected individuals.

In both models, C wishes to choose the best classification time. If the classification time is too small, C will “waste time” following misclassified Ws, and thereby increase R’s chance of reaching its objective; if the classification time is too long, R will reach its objective before C can detect and neutralize it. In the initial model of Section 2, R reaches its objective after an exponential time if not neutralized before then; this exponential time is independent of C’s actions. In the model of Section 3, the targets have values, and R chooses a policy to maximize its expected reward (equal to 0 if R is neutralized, and equal to the value of the target if R reaches its objective). The numerical results suggest that the probability of neutralizing R resulting from the best policy is robust to incorrect specification of the
distribution of the travel and response times, provided the correct mean times
are used. The numerical results also suggest that the neutralization probability
responding to the best policy is robust to incorrect specification of the
probability of correct classification as a function of time. The probability of
neutralizing R can be increased by decreasing the number of unidentified
neutral individuals and by decreasing the rate at which R encounters possible
targets (possibly by hardening infrastructure, for example).

The time until R achieves its objective has an exponential distribution for
both of the models discussed here. However, the results of Gaver et al.
(2006, to appear) suggest that the probability of neutralizing R is sensitive to
the distribution of the time until R achieves its objective, so other functional
forms should perhaps be considered. It would also be of interest to study the
effect of C tagging those Ws it has already investigated.

In the model of Section 3, R knows the distribution of target values.
Another area of future study is the development of models in which R learns
about its target population. In this case, we would expect R’s policy to
depend on the variability of the target values. As the target values become
more variable, we expect it would be worthwhile for R to spend more time
observing target values before determining a threshold target value. Further,
if the mean prior arrival rate is large, then we would expect that only a small
amount of time would be needed by R to get good information about target
values, reducing the risk of being neutralized.

ACKNOWLEDGEMENTS

D. P. Gaver and P. A. Jacobs acknowledge with thanks support from the
Center for Defense Technology and Education for the Military Services
Initiative at the Naval Postgraduate School.

REFERENCES

maritime domain awareness and protection,” Naval Postgraduate School Technical Report,
NPS-OR-06-010.
domain awareness and protection,” to appear in International Journal of Performability
Engineering.
Approaches to Reading the Opponent’s Mind), Chapman & Hall/CRC, New York.
Kress, M., 2005, “The effect of crowd density on the expected number of casualties in a
Chapter 7

GAMES AND RISK ANALYSIS
Three Examples of Single and Alternate Moves

Elisabeth Paté-Cornell, with the collaboration of
Russ Garber, Seth Guikema and Paul Kucik

Abstract: The modeling and/or simulation analysis of a game between a manager or a government can be used to assess the risk of some management strategies and public policies given the anticipated response of the other side. Three examples are presented in this chapter: first, a principal-agent model designed to support the management of a project's development under tight resource (e.g., time) constraints, which can lead the agent to cut corners and increase the probability of technical failure risk in operations; second, a case in which the US government is facing one or more terrorist groups and needs to collect intelligence information in time to take action; and third, the case of a government that faced with an insurgency, is trying to balance the immediate need for security and the long-term goal of solving the fundamental problems that fuel the insurgency. In the first case, the result is an optimal incentive strategy, balancing costs and benefits to the managers. In the second case, the result is a ranking of threats on the US considering a single episode of potential attack and counter-measures. In the third case, the result is the probability of different states of country stability after n time periods, derived from the simulation of an alternate game between government and insurgents.

Key words: risk analysis, game theory, project schedule, principal-agent, counterinsurgency

1. GAMES AND RISK: INTERACTIONS

When a risk of system failure or attack from insurgents is the result of one or several actions from another person or group, anticipating these moves and assessing their long-term effects permit proactive risk management. This is the case, for example, of the supervisor of a construction site who wants to make sure that his employees do not
compromise the integrity of a structure, or of a policy maker trying to control an insurgency who wants to balance the short-term and long-term consequences of his decisions. Game theory (Nash, 1951; Harsanyi, 1959; Gibbons, 1992) and game analysis (e.g., through simulation) provide useful models when the decision maker has an understanding of the basis for the other side’s actions and of the consequences of his or her decisions.

Of particular interest here is the case where some moves affect the state of a system, and when this system’s performance can be assessed through a probabilistic risk analysis (PRA) (Kumamoto and Henley, 1996; Bier et al., 2005). This approach is especially helpful if the decisions affect either the capacity of that technical system or the load to which it is subjected.

When the success of operations depends on the decisions and actions of operators (technicians, physicians, pilots etc.) directly in charge, the managers can set the rules to influence their behaviors. The principal-agent theory (e.g., Milgrom and Roberts, 1992) provides a classic framework for this analysis. At the collective level, the managers set the structure, the procedures, and to some degree, the culture of the organization. At the personal level, they set the incentives, provide the information, and define the options that shape the “agent’s” performance. In previous work, the author described a model called SAM (System, Actions, Management) designed to link the probability of failure of a system of interest to the decisions and actions of the technicians directly involved, and in turn to management decisions (Murphy and Paté-Cornell, 1996). This model was illustrated by the risk of failure of a space shuttle mission due to failures of the tiles (Paté-Cornell and Fischbeck, 1993), of patient risk in anesthesia using a dynamic model of accident sequences (Paté-Cornell et al.), and of the risk of tanker grounding that can cause an oil spill (Paté-Cornell, 2007).

In this chapter, the objective is to develop further the link between the actions of the parties involved and the resulting state of a system, physical or political. The approach is a combination of game analysis and PRA. The results involve the probability of different outcomes and the risks of various failure types. This work is in the line of previous studies of games and risks cited above. Three models and applications are presented.

The first one is a principal-agent model coupled with a system-level PRA that allows assessing the effects on a system’s performance of the decisions of a manager (principal; “she”) who sets constraints for an agent (“he”) in charge of its development or maintenance or operations. The focus is first on the decision of the agent in the case where he discovers that his part of the project is late. At that point, he has the choice of either paying the price of lateness or taking shortcuts that increase the probability of system failure (Garber and Paté-Cornell, 2006; Garber, 2007). The objective of that model is to support the decisions of the manager who sets incentives and penalties
for lateness and induced failures and decides on a level of monitoring of the agent’s actions or inspection of his work. The problem was motivated by an observation of NASA technicians in charge of maintaining the shuttle between flights. The question is to assess the risk of system failure given the incentives and monitoring procedures in place, and to minimize this risk given the resource constraints.

The second model is designed to support the decisions of a government trying to allocate its resources at a specific time to decrease the threat of terrorist attacks (Paté-Cornell and Guikema, 2002). Given the preferences of different terrorist groups and the means of action at their disposal, the first objective of this model is to rank the threats by type of weapons, targets and means of delivery. The results can then be used to support resource allocation decisions, including prioritization of targets reinforcement, detection and prevention of the use of different types of weapons, and monitoring of various means of delivery (cars, aircraft, ships, etc.). This general model was developed after the attacks of 9/11 2001 on the US. It is illustrated by the ranking of four types of weapons based on the probability that they are used and on the damage that they can inflict on the United States (a nuclear warhead, a dirty bomb, smallpox virus and conventional explosives). It is a single-move model designed to support US response at a given time. It is based on a one-time decision on the part of a terrorist group (choice of single attack scenario) and response from US intelligence and counter-terrorism.

The third model is based on the simulation of an alternate game involving several moves between a government and an insurgent group (Kucik, 2007). It is designed to assess the risks of various outcomes in a specified time frame from the government perspective. One objective is to weigh the respective benefits of short-term measures designed to reduce the immediate risk of insurgent attacks, and of long-term policies designed to address the fundamental problems that cause the insurgency. This model can then be used to compute the chances that after a certain number of time units, the country is in different states of political and economic stability (or turmoil). Historically, some insurgent groups have essentially disappeared (e.g., the Red Brigades in Germany in the 1970’s-1980’s); others have become legitimate governments including that of the United States, or the state of Israel. One objective is to identify policies that lead more quickly to the stabilization of a country and that serve best the global interests. This model is illustrated by the case of an Islamist insurgency in a specified part of the Philippines, based on data provided by local authorities and by the US Army (ibid.)

These three models rely on several common assumptions and mathematical tools. The first one is an assumption of rationality on the part
of the US. In Models 1 and 3, both sides are assumed to choose the option that maximizes their expected utility at decision time. In Model 2, terrorist behavior is modeled assuming bounded rationality as described by Luce (1959). Therefore, it is assumed that the main decision maker (manager, country, government) generally knows the preferences of the other side, their assessment of the probabilities of different events, their means of action and the options that they are considering. In reality, the knowledge of the principal may be imperfect for many reasons including the agent’s successful acts of deception. Again, rationality does not imply common values between the principal and the agents, or preferences that seem reasonable or even acceptable based on particular standards. It simply means consistency of the preferences of each side as described by utility functions defined according to the von Neumann axioms of rational choices (von Neumann and Morgenstern, 1947). Another similarity across these models is the use of influence diagrams, in which the decisions of both sides are represented and linked.

The models presented here are based on some principles of game theory, but involve mostly game analysis. The focus is either on one move or on alternate moves on both sides, and on an assessment of the chances of various outcomes at the end of a number of times or game periods. One assumption is that the probabilities of various events are updated when new information becomes available.

In reality, both preferences and probabilities can change over time. Preference can change, for instance with new leadership on either side. It is assumed here that decisions are made in a situation where both leaderships are stable enough that their preferences are known, and do not vary in the case of repeated moves. This assumption can be relaxed if necessary, but that involves anticipating at the time of the risk assessment the possibility and the probabilities of these changes.

Finally, a common feature of these models is that the decisions of the two sides are linked to represent the dependences of the state and decision variables between the different players (e.g., Hong and Apostolakis, 1992). For example, in these graphs, the decision of one side is represented as an uncertainty (state variable) for the other, and the principal’s decision regarding incentives and penalties is shown to affect the utility of the agent.
2. **MODEL 1: A PRINCIPAL-AGENT MODEL OF POSSIBLE SHORTCUTS AND INDUCED FAILURE RISKS (WITH THE COLLABORATION OF RUSS GARBER)**

Consider the case of a physical system composed of subsystems in series, some of which involve elements in parallel. Consider also the situation of the “agent” (mission director, technician, operator) in charge of the development or the maintenance of that system\(^1\) and that of the general manager of the project. The agent finds out that his project is late and that he faces a known penalty if that situation persists. At the same time, he also feels that he has the option to take shortcuts\(^2\) in one or more of the tasks of the system components’ development to catch up, with or without authorization. The problem, of course, is that these shortcuts increase the probability of a system failure in the future, for example, at the time of the launch of a space mission or in further stages of system’s operations. Furthermore, failures of subsystems and components may be dependent. In both cases, a failure clearly induced by shortcuts carries a penalty, whereas a “regular” failure would not, at least for the agent.

The “principal” (manager) has several options. First, she can choose the level of penalty imposed on the agent for being late in delivering his system, and for causing a failure by cutting corners. At the same time, she can also inspect the agent’s work and impose a penalty if he is caught taking shortcuts. But monitoring has its costs and she may sometimes prefer not to know what the agent is doing as long as the project is on time and she trusts his judgment that the failure risk remains acceptable. The focus of the model is on the management of the time constraints in project development from the perspective of the principal\(^3\).

A key factor is the failure probability of the technical system (e.g., a satellite). Assume for simplicity that the failures considered here are those that occur in the first time unit of operations. Therefore, the cost of those failures (regular or induced by shortcuts) will be incurred at a known future time. Both the principal and the agent discount future failure costs and

---

\(^{1}\) The agent is assumed here to be a male and the principal a female.

\(^{2}\) A shortcut is defined both as “a more direct route than the customary one” and a “means of saving time or effort” (as defined by the American Heritage Dictionary), which implies here skipping some steps or abbreviating the classic or agreed-upon procedures of system development.

\(^{3}\) This section is a simplified version of the Ph.D. thesis of Russ Garber at Stanford University (August 2007).
Chapter 7

Notations

k: index of subsystems in series
i: index of components in parallel in each subsystem
{(k₁,i₁), (k₂,i₂), etc}: set of components for which the agent decides to cut corners
{(0,0)}: special case of {(k,i)}: no short cut
E(.): expected value of (.)
UA(.): disutility to the agent of some costs (penalties)
P(.): disutility to the principal of some costs (penalties)

Penalties to the agent:

CL: cost of being late (independent of the length of the delay)
CF': cost of induced failure. A regular failure does not imply a penalty to the agent.
CC: cost of being caught cutting corner. In that case, it is assumed that the system will be late and that there will be no further opportunity for shortcuts.
L: number of time units to be re-gained (through shortcuts) to be back on time.
g(k,i): time gained (number of time units) by cutting corners in component k,i (one option per component); g(k,i) is assumed to be deterministically known.
pk,i: probability of failure of component k,i without shortcut.
p'k,i: probability of failure of component k,i given shortcut.
M: Boolean decision variable for the principal, to set a monitoring system M or not.
CM: cost of monitoring to the principal.
CF: cost of failure to the principal.
p(C): probability that the agent is caught cutting corners given monitoring.
p(F): probability of system failure in the first period of operation, induced or not.
p(F'): probability of system failure in the first period of operation caused by shortcuts.
PRA ({pk,i}, {p'k,i}): probabilistic risk analysis function linking the probability of failure of the system and of failure of its components, with or without shortcuts.
{(k,i)}**: agent’s optimal set of short cuts if he decides to cut some corners.
{(k,i)}*: agent’s global optimal set of short cuts (including the possibility of none).

failure penalties at their own discount rate. However, the agent’s penalty for being late or being caught cutting corners is assumed to be concurrent with his decision to take shortcuts or not, and no discounting is involved.

The approach in this model is to identify first, the best option for the agent given the incentives set by the principal, then the best options for the principal given what the agent will do in each case. Again, it is assumed that both parties are rational and know the other side’s utilities and probability assessment. The principal, however, does not know whether the project is late or not.

The main equations of the model are the minimization of the expected disutility attached to costs and penalties on both sides. For the agent who responds to the incentive structure, the problem is to minimize his expected
disutility for the consequences of the different scenarios that may follow
taking shortcuts in one or more component(s):

\[\text{Min}_{\{(k,i)\}} \ E_{\text{U}}[\text{consequences of scenarios given shortcut set } \{(k,i)\}, \text{including } \{(0,0)\}]\]

Subject to: \(\sum_{\{(k,i)\neq(0,0)\}} g(k,i) \geq L, \text{ if some shortcuts are taken} \quad (1)\)

This implies that if the agent decides to take shortcuts, he chooses the set of components \(\{(k,i)\}\) so as to make up at least for the current delay \(L\) and to minimize the expected disutility to himself of the consequences of his actions. Alternatively, he may choose not to cut corners at all (option \(\{(0,0)\}\)). Equation 1 (the agent’s optimum) can be written as an explicit function of the probability of being caught and the probability of induced system failure, as well as the penalties for being late, being caught cutting corners and causing induced failure. Assuming that the principal monitors the development process, the agent’s problem is to minimize his expected disutility given that he may or may not get caught taking shortcuts, and that if he is not, the systems may or may not experience induced failures.

\[
\text{Min}_{\{(k,i),(0,0)\}} p(C|\{(k,i)\}) \times U_{\text{A}}(CC+CL) + (1-p(C|\{(k,i)\})) \times U_{\text{A}}(CF') \\
\text{subject to: } \sum_{\{(k,i)\neq(0,0)\}} g(k,i) \geq L \\
\Rightarrow \text{local optimum given some shortcuts } = \{(k,i)\}_{\text{SC}}^{**} \\
\text{If } U_{\text{A}}(\{(k,i)\}_{\text{SC}}) < U_{\text{A}}(CL), \text{ global optimum } \{(k,i)\}^{*} = \{(k,i)\}_{\text{SC}}^{**} \text{ (selective shortcuts)} \\
\text{If } U_{\text{A}}(\{(k,i)\}_{\text{SC}}) > U_{\text{A}}(CL), \text{ global optimum } \{(k,i)\}^{*} = \{0\} \text{ (no short cut)}. \quad (2)
\]

Equation 2 implies that depending on the penalty for admitting that he is late, the agent decides either not to cut corners (option \(\{(0,0)\}\)) and to incur the penalty of being late, or that he chooses a corner cutting option (a set of components) that allows him to get back on time, accounting for the probability and penalty of being caught (then being late), and if he is not caught, the probability (and penalty) of induced failure.

Note that the probability of being caught is a function of the number and the nature of the components where shortcuts are taken. The probability of system failure induced by the agent (and as it appears in Equation 3) is a function of the probabilities of failure of the different components with or without shortcuts, depending on his decision. For his optimal decision, it is the value \(p(F') = \text{PRA } \{\{p_{ki}\}, \{p'_{ki}\}\}\), which is the probability of failure of his system that corresponds to his optimum set of short cuts, \(\{(k,i)\}^{*}\) and...
involves the probability of failure of each component given shortcut or no shortcut in each of them.

Given his anticipation of the agent’s decision, the principal decides to monitor the process or not, and chooses the level of penalty to the agent for being late, being caught cutting corners and causing an induced failure as shown in Eq. 3. The disutilities (i.e., the preferences and risk attitudes) of the principal and of the agent are thus critical to the result. For the principal who sets -or not- a monitoring or inspection system and the penalties for being late, for being caught corner cutting, and for inducing a failure, the problem is to minimize her expected disutility for the consequences of the different scenarios that may follow these decisions, given the agent’s response to these various penalties.

$$\text{Min}_{M, CL, CC, CF} \, \text{EU}_P[\text{conseq. of scenarios} \mid \text{set of options} \{M, CL, CC, \text{and CF}\}]$$ (3)

It is assumed here that the principal’s problem is unconstrained, and that monitoring occurs or not (other options would be to describe the monitoring effort by a continuous variable, and/or to consider explicitly which components are inspected). All costs and penalties are described in this model as inverse functions of the principal’s or the agent’s disutilities.

ILLUSTRATION

Consider as an illustration, the system shown in Figure 7-1.

For the system represented in Figure 7-1, one option to the agent is to cut corners in elements (1,1), (2,1) and (3,1) (option {(1,1), (2,1), (3,1)}). The disutility functions of the principal and the agent are shown below. The numbers fit a convex disutility characteristic of risk aversion in both cases.

![Figure 7-1. A simple system that is developed or maintained under time constraints.](image-url)
For illustrative purposes, assume the following data:

Probabilities of failure without and with shortcuts (marginal and conditional)

Without shortcuts:  
\[
p_{11} = 0.01 \quad p_{21} = 0.001 \quad p_{22|21} = 0.9 \quad p_{31} = 0.01
\]

With shortcuts:  
\[
p'_{11} = 0.1 \quad p'_{21} = 0.01 \quad p'_{22|21} = 0.95 \quad p'_{31} = 0.1
\]

The project is late by 10 days. The times gained by shortcuts in each component are:

\[g_{11} = 5 \quad g_{21} = 3, \quad g_{22} = 3 \quad g_{31} = 4\]

Assume that the time gained by taking several shortcuts is additive.

Based on these data, the probability of system failure without shortcut is \(p(F) \approx 0.0209\). In practice, the shortcut options are limited to four possibilities with the corresponding approximate probabilities of system failure:

\[
\begin{align*}
\{(1,1), (2,1), (3,1)\} & \quad p(F') \approx 0.20 \\
\{(1,1), (2,1), (2,2)\} & \quad p(F') \approx 0.11 \quad p(F) \approx 0.12 \quad (F \text{ can also be caused by failure of 3.1}) \\
\{(2,1), (2,2), (3,1)\} & \quad p(F') \approx 0.11 \quad p(F) \approx 0.12 \quad (F \text{ can also be caused by failure of 1.1}) \\
\{(1,1), (2,2), (3,1)\} & \quad p(F') \approx 0.19
\end{align*}
\]

Other shortcut options would not be sufficient to cover the ten days of delay, or would be more than needed and dominated by a smaller probability to the agent of being caught cutting corners. For each of these options, the probability of being caught (if the principal decides to monitor the work) is assumed to be 0.3. The costs to the agent are defined as the inverse of his disutility function. Assume that initially, the principal, if she decides to monitor operations, has set the penalties so that:

\[U_A(\text{CL}) = 0.5, \quad U_A(\text{CC + CL}) = 0.8, \quad U_A(\text{CF'}) = 0.9.\]

The disutility to the agent of not taking shortcuts and being late is 0.5, of being caught cutting corners and being late is 0.8, and of being identified as the culprit for system failure because of the shortcuts he took is 0.9.
If the agent assumes that the principal is monitoring his operations and he decides to cut corners, his best option is to take shortcuts either in components \{(1,1), (2,1), (2,2)\} or \{(2.1), (2.2), (3.1)\} with an expected disutility of 0.31 in both cases. If he assumes that the principal is not monitoring his operations, his best options are the same with an expected disutility of 0.1 in both cases. Therefore, the rational agent adopts either of these two options (he is indifferent). In both cases, a portion of the failure risk cannot be attributed to shortcuts (the portion that is due to the failure of (1,1) or (3,1)).

It is important to note that because the agent uses a PRA and accounts for the dependencies of component failures, he reduces the probability of system failure with respect to what would happen if he chose shortcuts at random. For example, if he decided to cut corners in (1,1), (2,1) and (3,1) instead of one of the optimal sets, the probability of system failure would increase from 0.12 to 0.20 (about 64% increase) and the agent’s disutility would increase from 0.31 to 0.37.

Knowing the options and preferences of the agent, the principal’s problem is to decide whether or not to monitor, and how to set the penalties. For simplicity, the decision is limited here to the choice to monitor the agent’s work or not for all components. Assume that her probability that any project is late is 0.2 and that her disutility function is characterized by:

\[
\begin{align*}
U\_P(CM) &= 0.2, \\
U\_P(CL) &= 0.8, \\
U\_P(CM+CL) &= 0.85, \\
U\_P(CF) &= 0.9, \\
U\_P(CF+CM) &= 0.95, \\
U\_P(CM+CL+CF) &= 1 \\
\end{align*}
\]

For this set of data, the expected disutility of the principal if she decides to monitor the process, is her expected disutility associated with the optimal decision of the agent (cut corners in (1,1), (2,1) and (2,2), or in (2,1), (2,2) and 3,1)). It is equal to 0.26. If the principal decides not to monitor but leaves the penalty for induced failure at the current level, the best option of the agent is unchanged (in part, because the cost of lateness is high) and the disutility of the principal has gone down to 0.04 (since there is no cost of monitoring). This is a case where the optimal decision for the principal is simply to let the agent manage lateness based upon his knowledge of the system. If however, the principal’s disutility for lateness was lower and the probability of failure associated with shortcuts was higher, the principal’s policy would shift to monitoring and discouraging shortcuts (e.g., by increasing the penalty for induced error and/or decreasing the penalty for lateness).

The use of the PRA, in this case, allows the agent to reduce significantly the probability of failure. The principal can adjust the incentives to the agent and the agent can choose his best option as a function of the probabilities of
component failures and of their “disutility” for each scenario. The optimal set of options for the principal (whether or not to monitor and where to set the penalties to the agent) can then be formulated as an optimization problem: for each joint option, one identifies the agent’s best decision (no shortcut or the cutting corners in each subsystem as determined above) and in turn, the principal’s optimal setting. (For a general formulation and illustration of this continuous optimization problem –constrained or not- see Garber, 2007). The link between the principal’s and the agent’s decisions is critical because it determines the effect of penalties and monitoring on the agent’s behavior and in turn, the optimal decision for the principal. It is assumed here that the principal minimizes her expected disutility. In other cases, she may use a threshold of acceptable failure probability to make these decisions. Non-rational, descriptive behavioral models can also be applied to both parties, but especially to the agent if for instance, his utility/disutility function changes with the reference point. This general framework, using both a PRA and a principal-agent model, can be applied, for example, to the management of construction projects or to the development of space systems.

3. A GAME ANALYSIS APPROACH TO THE RELATIVE PROBABILITIES OF DIFFERENT THREATS OF TERRORIST ATTACKS (WITH THE COLLABORATION OF SETH GUIKEMA)

Another application of the game analysis/risk analysis combination was used to rank terrorist threats in the wake of the 9/11 attacks on the US. In that study (Paté-Cornell and Guikema, 2002), the objective was to set priorities among different types of attacks in order to rank countermeasures. The approach is to use systems analysis, decision analysis and probability to compute the chances of different attack scenarios.

The different attack scenarios (limited here to a choice of weapon) represent options potentially available to the terrorists. The probabilities of the different attack scenarios by each terrorist group are assumed to be proportional to the expected utility of each option for the considered group. This approach is not based on the classic model of rationality, but on stochastic behaviors as described by Luce (1959), and subsequently by Rubinstein (1998) in his extensive description of models of bounded rationality. In Luce’s model, the decision maker (here, the terrorist side) selects each possible alternative with a probability that is the ratio of the expected utility of that alternative to the sum of the expected utilities of all considered alternatives.
This model is intuitively attractive in this case, because the most likely scenarios are those that are the easiest to implement and that have the most satisfactory effects from the perspective of the perpetrators. Given their probabilities of occurrence, the threats are then ranked from the US point of view according to the expected disutility of each scenario. This probabilistic ranking can then be used to allocate counter-terrorism resources, in the reinforcement of targets, development of infrastructures, or implementation of protective procedures.

This analysis accounts first for the preferences and the “supply chain” of each of the considered terrorist groups and second, for the information that can be obtained by the US regarding current threats, and the possibility of counter measures. One can thus consider this model as a one-step game in which terrorists plan an attack for which they choose a target, a weapon and the means of delivery (attack scenario). The US intelligence community may get information about the plot and appropriate measure may be taken.

The overarching model is described in Figure 7-2, which represents an influence diagram of events and state variables (oval nodes), decision variables (rectangles) and outcome to the US (diamond) as assessed by the US at any given time. The probability of each attack scenario is computed as proportional to its expected utility to the group as assessed by the US, based on intent, probability of success given intent and attractiveness from the terrorists’ point of view based on their statements and past actions.

Critical steps in this analysis thus involve first, the formulation of the problem, including identification of the main terrorist groups and assessment of their preferences, and second, identification of the different types of attack scenarios (targets, weapons and means of delivery). The kinds of targets considered here include computer networks, electric grids, harbors and airports, as well as crowded urban areas. The next step is to assess the probabilities and consequences of a successful attack on these targets at a given time, from the perspective of terrorist groups based on the information available to the US. The following step is to evaluate the effects of US intelligence collection and analysis, and of immediate as well as long-term counter-terrorism measures.

This model was originally designed as part of a larger study that assumed availability of some intelligence information and provided a way to structure that information. One of the objectives was to organize that information and sharpen the collection focus. It is assumed here that intelligence is updated every day. The focus of this model is thus on the formulation of the problem to provide a framework in which all the information that becomes available at any given time through different channels, can be integrated to set priorities among US options. Again, the variables of the model are assessed by the US based on current information. The realizations of the state variables and the values of the probabilities vary at any given time. This
model is thus a pilot model to be used and updated in real time to set priorities among threats and support protection decisions.

Figure 7-2. Influence diagram representing the risk of a terrorist attack on the US.
(Source: Paté-Cornell and Guikema, 2002)

3.1 Model structure

The variables of the model (nodes in the influence diagram of Figure 7-2) are represented as usual as state variables (oval nodes), decision variables (rectangle) and outcome variables (diamond-shaped nodes). Each state variable and outcome variable is represented by its realizations, and their probabilities conditional on the variables that influence it. The decision variables are represented by the corresponding options.

The realizations of the different variables are the following:

- **Terrorist groups**: At any given time, one of several terrorist group may be planning an attack on the US in a given time window (e.g., Islamic fundamentalists, and disgruntled Americans).
- **Preferences of the terrorists**: Each of these groups’ preferences translated by the analysts into utility functions, have often been revealed by their leaders, for example, maximizing American losses of lives and dollars and disrupting the US economy, but also the visibility of the target (e.g., a major financial district) and the financial damage to US interests.
• Each group’s “supply chain” is characterized by the people working for them and their skills, the weapons at their disposal, their financial strength (cash), their means of communications, and their transportation system.

• Help from US insiders ("insiders’ role") can make available to terrorists means and attack possibilities that they would not have otherwise. It is of particular concern in critical functions of the US military and police forces, but also in many key positions of operations and management of critical infrastructures.

• Attack scenario: An attack scenario is considered here as a choice of a target (e.g., a major US urban center), weapon (e.g., conventional explosives) and means of delivery (e.g., a truck).

• Intelligence information: At any given time, the US intelligence community gathers (or may fail to obtain) signals that depend on the nature of the attack scenario, the supply chain of the group, and the possibility of inside help. That information, if properly collected and communicated, is then used to update the existing information.

• Counter-measures: The credibility, the specificity, the accuracy and the lead time of that information allow taking counter-measures. Obviously, the possibility and the effectiveness of the response depend in part on the planning and the availability of the resources needed. Some of these measures can be taken after the attack itself to mitigate the damage. Therefore, they reflect decisions of the US leadership faced with the prospect of an attack or the news that it has taken place.

• The nature and the success of the attack scenario as well as the effectiveness of these counter-measures determine the outcome to the US.

The results derived from this diagram are thus based on the following data and computations:

1. Assessment by US analysts of the utility to each terrorist group of the successful use of different types of weapon on various targets. Computation of the expected utility (to the terrorists) of each option based on the probabilities of state variables as estimated by US experts, including the probability of success of the weapon’s delivery.

2. The probability of each attack scenario is computed as proportional to the expected utility of that scenario to the terrorists (based on US knowledge) as a fraction of the sum of the expected utilities of all possible attack scenarios.

3. The total probability of successful attacks for each type of threat (e.g., weapons) is then computed as the sum of the probabilities of successful attacks of that type for all groups (of targets and means of delivery).
4. Finally, the disutility to the US of different types of attack is computed as a function of their probabilities and the potential losses to this country.

Again, the probability of an attack is assessed using a bounded rationality model of terrorist behavior. It is the ratio of the expected utility to terrorists of a specific operation to the sum of the expected utilities of the possible options, based on intelligence information and on the probability of success of counter-terrorism measures as assessed by the US intelligence community. The benefits of different countermeasures can then be assessed based on their effects on the probability of outcomes of different types of attacks and the losses to the US (disutility) if the attack succeeds.

This model is dynamic in the sense that all information used here varies with new pieces of intelligence information and signals. The data are assumed to vary daily. The probabilities are seldom based on statistics, which may not be available or relevant, but often reflect the opinions of experts (political scientists, engineers, analysts etc.). The realizations of the different variables may also vary over time, for instance because a particular group has acquired a new weapon. The preferences of the actors may vary as well over time and have to be anticipated in the use of this model.

The model is thus structured here as a one-step decision problem to be reformulated as the basic data evolve. The decisions of both sides can be represented as the two-sided influence diagram shown in Figure 7-3, in which each side bases its decisions on the available information and on its preferences. The set of equations used in these computations directly reflect the structure and the input of these influence diagrams. Note again that the terrorist decisions are analyzed here based on Luce’s bounded-rationality model.

3.2 Illustration

This model was run on the basis of hypothetical data (ibid.) and restricted to two terrorist groups (fundamentalist Islamic and American extremists) and three types of weapons (nuclear warhead, smallpox, and conventional explosives). The computations involved the probability of success of an attack given the intent, the attractiveness to the perpetrators of a successful attack with the considered weapon, and the expected utility of such an attack to the terrorist group. The severity of the damage to the US was then assessed and the weapons ranked by order of expected disutility (to the US), including both the likelihood that they be used and the losses that they are likely to cause.

The results can be summarized as follows:
In terms of probabilities of occurrences, the illustrative ranking of attacks was: 1. repeated conventional explosions, 2. attack by small pox virus, and 3. a nuclear warhead explosion.

In terms of expected negative impact, however, the illustrative ranking involving both probability and effects, were 1. a nuclear warhead explosion, 2. a small pox virus attack, and 3. repeated conventional attacks.

The chances of use of nuclear warheads in an attack on the US are probably increasing, but still relatively small given the complexity of the operations. Nonetheless, they can cause such enormous damage that they still top the list of priorities. Conventional explosives are easy to procure and use. The release of small pox virus is a less likely choice for any decision maker who puts a negative value on the possibility that it could immediately backfire on the rest of the world. In addition, one could consider the possibility of a dirty bomb involving a combination of nuclear wastes and conventional weapons. It may not cause a large amount of immediate damage, but could create serious panic, great disruption and financial losses and the temporary unavailability of a large area.

In this example, the “game” depends on the intent and capabilities of terrorists as well as the state of information of the US intelligence and the
US response (e.g., to prevent the introduction of conventional explosives on board civilian aircraft). The threat prioritization however, is intended to guide US decisions that have a longer horizon based on expected utilities at the time of the decision. The model can be used to assess the benefits of various counter-measures in terms of avoided losses (distribution, expected disutility or expected value). In our illustrative example, the considered measures included protection of specific urban populations such as vaccinations and first response capabilities, transportation networks (e.g., trains and airlines), government buildings and symbolic buildings.

The model presented here is designed to structure the thought process in an allocation of resources. Clearly, it is only as good as the data available. If it is implemented systematically, it allows accounting for different types of information, including preferences as revealed. It can be particularly helpful in thinking beyond the nature of the last attack, which tends to blur long-term priorities.

4. COUNTER-INSURGENCY: A REPEATED GAME (WITH THE COLLABORATION OF PAUL KUCIK)

While the terrorism model described in the previous section, considered multiple opponents during a single time period, this section involves the simulation of an alternate game of moves from a government and an insurgent group within a specified time horizon (Kucik, 2007). This simulation can be extended over several years. It allows computation of the probability that after a certain number of time units, the village, the province, or the country is in one of several possible states of security and economic performance. This model is used to assess a number of counter-insurgency strategies, some designed to maintain security and order in the short-term, and some designed to address in the long-term the fundamental problems that are at the roots of the insurgency.

Each side is assumed to be a rational decision maker, although a change of preferences (e.g., because of change of leadership on either side) can be included in the simulation. The possible outcomes of each move are discounted to reflect the time preferences of both sides. The use of appropriate disutility functions and discount rates permits including the preferences of both sides in the choice of their strategies.

This modeling exercise is motivated by the urgency of insurgency problems across the world and the need to face the short-term versus long-term tradeoff when allocating resources.
An insurgency is defined as “an organized movement aimed at the overthrow of a constituted government through use of subversion and armed conflict.”

Insurgency is a struggle for the hearts and minds, but also compliance, of a population. The side that can adapt more quickly and is more responsive to the needs of the people has a decided advantage. As a result, insurgency (and counter-insurgency) is best fought at the local level, even though higher-level decisions may need to be made in the choice of a global strategy.

Insurgencies usually arise from nationalist, ethnic, religious, or economic struggles. The result is a long-term, complex interaction between military, diplomatic, political, social, and economic aspects of political life. Depending on the complexity of insurgency, even at the local level, it can be very difficult for a local government leader to understand the impact of policy decisions that affect security, the local economic situation, and various political issues. At the same time, government leaders must make a real tradeoff between spending resources to meet immediate security needs and investing in long-term projects designed to improve living standards. In order to support effective policy decisions, we show below how to conduct a dynamic simulation of insurgency. On that basis, one can develop risk-based estimates of the results of counterinsurgency strategies, while including the effects of focusing on short-term exigencies versus long-term investments.

The fundamental model hinges on two linked influence diagrams that represent the decision problem of both the government and the insurgency leaderships. The two can be merged for analytical purposes. Figure 7-4 shows an influence diagram that represents both sides’ decision analytic problems in the first time period. As in the previous sections, it is assumed that they act as rational actors, i.e., that their preferences can be described at any given time as a unique utility function, even though that utility may change in the long run (for instance, with a change of leadership). It is also assumed that this “game” is played by alternate moves, one per time unit. Note that one can also adjust the time unit if needed to represent a faster pace of events. The general strategy of balance guides the decisions of the government. One can trace on a graph the situation (based on utility functions of both sides) of the village after a specified number of time units and for a particular strategy. That situation is represented by two clearly dependent main attributes (social stability and economic performance), aggregated as shown below in a utility function that represents the preferences of the local leadership. One can thus use this model to assess, for example, the risk that within a given time horizon, the local area is still in a state of disarray.

---

4 Joint Publication 1-2 (Department of Defense Dictionary of Military and Associated Terms).
4.1 The Insurgent Leader’s Decision Problem

In order to broadly describe the decision situation facing the insurgent decision maker at any point in time, one must first outline here his alternatives, information, and preferences. The insurgent leader’s decision problem is represented in the upper part of Figure 7-4.

4.1.1 Alternatives

The insurgent leader’s options, at any point in time, include launching an attack, organizing civil disobedience, conducting support activity, or seeking a lasting peace.

4.1.2 Information

The insurgent leader gathers information about the capabilities of his or her organization, the capabilities of the local government, and the current socioeconomic and political circumstances. This information is gathered through the insurgent group’s management process and ongoing intelligence efforts. In the dynamic formulation, described further, the probability estimates (and other data) are those of the insurgents as assessed by the government intelligence community. They need to be revised through Bayesian updating as new information becomes available to the insurgent leader.

4.1.3 Preferences (and Objectives)

In general, several factors motivate insurgent leaders. These factors vary across different groups and the various levels of mobilization within a group. Objectives include increasing the power of the insurgent organization, securing personal financial gain, and ensuring security of one’s family. Although there are many possible preference orderings for an insurgent leader, this model assumes that he or she is primarily motivated by a desire to better the insurgent organization. The model represents the government’s perception of these preferences, based on statements made by the insurgents and information gathered through other intelligence sources.

4.2 The Government Leader’s Decision Problem

The objective of the model is to support effective policies for local government leaders. Therefore, one needs to understand the issue of insurgency from the government leader’s perspective. This section outlines his alternatives, information, and preferences.
4.2.1 Alternatives

The government leader’s options include short-term and long-term possibilities. With a long-term perspective, he can consider various possible resource allocations among economic, political, and security policy areas,

Figure 7-4. Interactive Influence Diagrams of both insurgency and government leaders
(Source: Kucik, 2007)
including spending on programs of various durations. In the short term, when faced with the possibility of insurgent attacks, the government leader needs to choose between an emphasis on targeted responses or initiatives in counterinsurgency combat operations.

4.2.2 Information

The government gathers information about its own capabilities, insurgent organization capabilities, popular support for insurgency, and the current socioeconomic and political circumstances. To represent the decision-analytic problem at a different time, the probabilities as assessed by the government decision maker are revised through Bayesian updating.

4.2.3 Preferences (and Objectives)

Many factors may motivate a local government leader such as improving the life of the constituency, personal gain (of money or authority), or ensuring the security of his or her family. The model presented here assumes a government leader whose primary objective is to improve the security and general conditions of the population. The secondary objective is to remain in office beyond the current term.

Based on these objectives, we use the linear utility function shown in Equation 4 to map the state of the environment to the level of benefit for the government leader as a weighted sum of the utilities of short-term and long-term benefits.

\[
EU_{n}^{gov} = \sum_{m} \beta_{m} \left[ AT_{m,(n+1)} + AT_{m,(n+1)}^{#} \right] (4)
\]

With:

- \( EU_{n}^{gov} \) = expected utility of the government at time \( n \)
- \( AT_{m,(n+1)} \) = expected value of attribute \( m \) at time \( n+1 \)
- \( AT_{m,(n+1)}^{#} \) = expected net present value at time \( n+1 \) of previously funded programs whose benefits in terms of attribute \( m \) will be realized in the future

- \( m \): index of attributes
  - 1: Economic
  - 2: Political
  - 3: Security
4: Initiative in Counterinsurgency Operations
5: Precision in Counterinsurgency Operations

n: index of time

$\beta_m$: weight of attribute m in a linear multi-attribute utility function

The government leader’s alternatives, information and preferences are shown in the lower part of the influence diagram of Figure 7-4.

The attributes of the preference function can be further described (in a simplified way) as follows:

1. Population’s Economic Situation: described here by the fraction of the population below the poverty line; a continuous parameter on the \([0, 1]\) interval.
2. Population’s Political Situation: described here by the fraction of population who would protest or use violence to change the current political, social, or religious situation; a continuous parameter on the \([0, 1]\) interval.
3. Population’s Security Level (Vulnerability): described here by the number of actionable tips received by government forces in a month divided by number of attacks (+1); a continuous parameter on the \([0, \infty]\) open interval.
4. Initiative in Counterinsurgency Combat Operations: described here by the fraction of combat engagements initiated by the government force; a continuous parameter on the \([0, 1]\) interval.
5. Precision in Counterinsurgency Operations: described here by the fraction of insurgents killed to total killed by government; a continuous parameter defined on the \([0, 1]\) interval.

4.3 Integration of the Insurgent and Government Models

Insurgency is a dynamic strategic competition where learning plays a critical role. It is represented here by a dynamic model over several time periods shown in Figure 7-4 as an interactive model. Beginning in the first time period \((n=1)\), the model simulates the insurgents’ selection of the alternative associated with the highest expected utility. Once this alternative is selected the result of that choice is simulated based on the probability distribution of the variable “Outcome of Insurgent’s Course of Action”. Figure 7-4 shows the insurgent leader’s decision analytic problem in the first time period.
In second time period (n=2), the “Outcome of Insurgent Course Of Action” (from the first time period) affects the four variables describing the current situation in the government influence diagram: Population’s Economic Situation, Population’s Political, Social, and Religious Situation, Population’s Security Level, and Initiative in Counterinsurgency Combat Operations. Based on this new situation, the model then simulates the government leader’s selection of the alternative that maximizes his or her expected utility. The outcome of the government leader’s simulated decision is probabilistically described by the probability distribution of the variable Outcome of Government Course of Action.

This process continues for the duration of the simulation. In the illustration, an insurrection in the Philippines, n is equal to 36 periods involving alternating insurgent and government decisions. Because the support of the population is the center of gravity of the insurgency (members of the population provide the insurgent group with intelligence, logistic support, money, and armed fighters), both leaders seek to influence the local situation facing the population (dashed arrows in Figure 7-4).

In the simulation, each opponent thus chooses the alternative with the highest expected utility, discounting at the appropriate rate the future effects of each strategy. Each time a leader makes a decision, he/she affects the situation faced by his/her opponent. Figure 7-5 shows the output of this illustration from a sample of 36 runs. The satisfaction levels of the government and of the insurgency leaders are both represented because they are relevant to the stability of the end state.

The model parameters in this illustration were set based on a particular village (Nalapaan in the Philippines) for a particular time period (2000-2003). The simulation was run on the basis of an initial state resulting in one final state, even though the actual final state was known when the illustration was run. Each path represented in Figure 7-4 thus represents one run in the simulation exercise.

This study simulated the situation in one village over a three-year period (36 months). In that time period, a number of events represented in our model as probabilistic actually occurred. They constituted one realization of the model variables among an infinite number of possible scenarios. The actual final state fell within range of outcomes of the simulation runs and was similar to the mean final state of the set of runs shown in Figure 7-5.

4.4 Applications to risk analysis

One useful application of this model is to determine the probability of meeting a given threshold of satisfaction (utility) for the state of the community. For example, the analyst may be interested in the probability
that the insurgent group will grow to more than 100 armed fighters within the next three years. This can be accomplished by running the simulation, and tracking the relative frequency with which the number of insurgent combatants exceeds the threshold (100).

![Insurgent Leader Utility](image1)

![Government Leader Utility](image2)

*Figure 7-5. Sample output of the alternate game simulation model for the illustrative case of an insurgency in the Philippines over 36 time periods (Source: Kucik, 2007)*

A second application is to develop a policy analysis. While every insurgency is different and the local circumstances vary, the analyst can observe the patterns of policy decisions that result in the best outcome at the end of the simulated period. Based on an analysis of trends, one can identify policy rules applicable to particular circumstances (village, group, etc). For
example, in the village of Nalapaan, an approach that balanced some immediate military and socioeconomic measures and a significant investment in long-term programs tended to result in the highest utility for the government leader (Kucik, 2007).

A third application (closely related to the second) is a support of long-term approaches as part of a peace process. Some insurgencies have been long and bloody before a new order settled in (this is the case of the Irish Republican Army), others have been short-lived (e.g., the Red Brigades), others are perennial and rooted in long-terms problems of development, oppression, and economic imbalance. One might thus ask whether there is a way to resolve such conflicts better and perhaps faster, and how in a world where resources are limited, one might address the unavoidable balance between immediate security problems and long-term solutions. For a lasting peace, both the government and insurgent leaders must be able to envision circumstances where each is at least as well off at the end as during the conflict. The analyst advising a policy maker can facilitate the process of reconciliation by monitoring both government and insurgent utilities in order to determine the set of policies, for both sides, that result in the highest total utility (or alternatively maximize one utility, subject to a minimum level for the second).

There are many advantages to a simulation of insurgency at the local level for leaders facing such a threat. Insurgency is a long-term problem with short-term realities. Local leaders often focus on the most recent or most damaging attacks and are less inclined to allocate resources to programs that yield benefits far in the future. The type of simulation shown above that includes a spectrum of military, economic, political, and social options can help leaders understand the underlying dynamics and make effective policy decisions. It can also help them balance the use of military and law enforcement elements to meet near-term security needs, and all other political, judicial, and economic means to address the root causes of the insurgency.

5. CONCLUSIONS AND OBSERVATIONS

Game analysis and simulation can be a powerful basis of risk assessment and decision support as illustrated here through three applications, ranging from the management of technical system developments to counter-insurgency policy decisions. These models however, are only as good as the underlying assumptions and the variable input. The main assumption of the approach described here is rationality on both sides. If it does not hold, a better descriptive behavioral model has to be introduced. Other assumptions
include the common knowledge of both sides’ states of information, preferences and options. The results of risk analysis models based on game analysis are thus limited not by the availability of information, but also by imagination of what could possibly happen. As is often the case in risk analysis, the main challenge is in the problem formulation and the choice of variables. Probability, simulation and linked influence diagrams are then useful tools to derive a probabilistic description of the possible outcomes of various options.

REFERENCES


This page intentionally left blank
Abstract: How well can telecommunications networks be designed to withstand deliberate attacks by intelligent agents? This chapter reviews methods for designing communications networks that are resilient to attacks—that is, that quickly and automatically reroute traffic around affected areas to maintain communications with little or no interruption. Current network architectures, routing and restoration protocols, and design techniques can already protect networks against the loss of any single link or node, so defending against deliberate attacks focuses on designing networks that can withstand even multiple simultaneous failures.

We first survey deterministic optimization approaches for designing networks that can reroute all traffic after loss of any $k$ links or nodes, where $k$ is an integer reflecting the attacker’s ability to do simultaneous damage. Next, we consider probability models for failures in packet-switched data networks caused by attacks on most-loaded nodes. Such networks are inherently resilient to attacks if and only if they have enough spare capacity at each node (typically about 10$k$% more than would be required in the absence of attacks, if the attacks are focused on the $k$ most heavily loaded nodes). Networks with less than this critical amount of extra node capacity are vulnerable to cascading failures following a successful attack. Finally, we present several game-theoretic examples showing that network owners and users may all benefit from institutions that enable them to mutually commit to larger investments in network resiliency than they would otherwise make.

Key Words: Telecommunications, survivable networks, resilient networks, scale-free networks, game theory, prisoner’s dilemma, free riding, tipping point
1. INTRODUCTION: DESIGNING TELECOMMUNICATIONS NETWORKS TO SURVIVE ATTACKS

How can one design telecommunications networks to provide reliable communications when terrorists or other intelligent adversaries might deliberately attack the network infrastructure? Three possible approaches are as follows.

- **Approaches based on physical defenses** seek to “harden” selected network nodes and links enough to make attacks undesirable, perhaps by burying cables more deeply or reinforcing buildings against attacks.
- **Information defenses** use secrecy, deception, and randomization (Brown et al., 2006; Parachuri, 2007) about facility locations and interconnection plans to increase the costs of planning successful attacks.
- **Resilient networks**, the main focus of this chapter, provide enough flexibility, redundancy, and rapid recovery (or “self healing”) capability so that any affordable attempts to disrupt traffic instead result in automatic re-routing of traffic and uninterrupted service. This chapter surveys recent ideas, methods and models for designing such resilient networks to protect telecommunications infrastructure against deliberate attacks.

Throughout this chapter, networks are understood to consist of nodes and links. Nodes represent locations where network elements, consisting of equipment such as add-drop multiplexers (ADMs) and remotely configurable optical cross-connect switches (OXC), carry out switching, grooming (i.e., aggregation from lower- to higher-bandwidth signals), regeneration and amplification of optical signals, and routing of traffic. Links, such as fiber-optic cables and microwave links, carry signals between nodes. More specifically, terminating equipment for creating and receiving traffic coded as modulated laser light is situated at the nodes. Any other equipment that is located on the links themselves (e.g., regenerator huts, where optical signals are strengthened for transmission over long distances) will be treated as part of the links. The key question addressed in this chapter is: How should network topologies be designed and how should traffic be routed and switched to make communication among nodes resilient to link and node failures, whether accidental or resulting from deliberate attacks?
2. BACKGROUND: DIVERSE ROUTES AND PROTECTION SWITCHING

Modern fiber-optic telecommunications networks are vulnerable to failures of links (i.e., individual fibers or entire fiber cables carrying bundles of fibers) and failures of nodes (e.g., due to failures of terminating equipment or to fires in central offices.) Historically, major fiber breaks have occurred several times per year in the United States, usually because of backhoes accidentally digging through buried fiber conduits. Node failures are uncommon, but do occur. For example, a 1988 fire at the Hinsdale central office in Illinois, which was a hub for multiple long distance companies, led to multiple simultaneous outages. This event taught the telecommunications industry the importance of avoiding the possibility of such single-point failures. However, deliberate attacks might increase the frequency of failures, especially, coordinated simultaneous failures intended to disrupt the flow of telecommunications network traffic. Resilience of networks to such coordinated failures requires additional analysis.

2.1 Automated protection switching (APS)

Telecommunications networks rely on automated protection switching to automatically re-route traffic when failures of nodes or links occur. Two quite different types of traffic can be rerouted automatically: data packets and light paths. Packets are used to carry information in data networks and in many mobile and wireless networks. Light paths are dedicated sequences of links and equipment, together with optical channel assignments for each link, that carry very high-bandwidth optical signals (typically consisting of many lower-level channels multiplexed together and encoded as modulated laser light) through optical networks. For purposes of resilient network design, the main difference is that packets can follow different routes through a network, although constraints on latency times for video and other applications may limit the diversity of routes used by consecutive packets from the same session. By contrast, a light path must provide dedicated end-to-end connectivity; thus, if a link fails, each light path that has been using it must promptly switch to another path with the same origin and destination nodes for all traffic in order to avoid any interruption of service.

2.2 Demands consist of origins, destinations, and bandwidth requirements

It is often convenient to describe optical network traffic in terms of demands, with each demand being specified by its origin node, destination
node, and size (meaning the amount of bandwidth that it requires, typically measured in units of optical channels.) The digital hierarchy of optical channels used in these networks provides discrete standard sizes of bandwidth, ranging from a single optical channel (an “OC-1”) up to 192 channels (OC-192) or more, in standard multiples (OC-1, OC-3, OC-12, OC-48, and OC-192). Smaller channel sizes (measured in bandwidth units such as STS-1, DS-3, and DS-1s) are also available and are used in the access networks that feed into optical backbone networks, but will not be considered further here. The design issues and solution approaches considered in this chapter apply to all levels of granularity.

At any moment, an optical network is provisioned to carry a given set of demands. This is done by assigning each demand to a specific light path that includes the desired origin and destination nodes and that has sufficient capacity (i.e., bandwidth) to carry this demand in addition to other demands assigned to it.

2.3 Multiple levels of protection for demands

In addition to its origin, destination, and size, each demand has a required level of protection that determines what should happen in the event of a network failure event. Unprotected demands are routed on a best-effort basis, and they may be dropped if a node or link fails. Each protected demand has an associated contingency plan that allows the possibility of re-routing if such a failure condition occurs.

Different degrees of protection are available. For example, a very strong form of protection reserves dedicated protection capacity for each demand on a “protection” (or “backup”) light path with all links disjoint from those on the primary light path that normally carries the demand. (For maximum protection, all nodes other than the origin and destination may also be required to be disjoint from those on the primary path.) If the primary path is interrupted at any point, the entire demand is immediately switched onto the reserved protection path. Such protection typically provides a physically diverse route (unless primary and backup links happen to pass through the same conduit, which can be avoided with additional design effort), with adequate capacity already reserved, for each protected demand. Recovery following a failure is therefore extremely fast, since protection paths are pre-computed and no further computation is needed to figure out what to do when a failure occurs.
2.3.1  Example: Self-healing in SONET rings

Many existing legacy synchronous optical network (SONET) ring networks in metropolitan areas embody this principle of fully redundant protection capacity. Traffic is routed around an optical fiber ring in one primary direction (for unidirectional SONET rings), with a duplicate signal being sent around in the other direction for protection. Add-drop multiplexers (ADMs) positioned at nodes on the fiber ring (e.g., local wire centers) insert (“add”) or receive (“drop”) traffic in timeslot channels within each optical channel. (An optical channel typically uses a specific wavelength, or color, of laser light. This wavelength, called a “lambda”, is modulated at a high frequency to transmit information. Wavelengths in the vicinity of 1530-1560 nanometers can travel great distances through modern fiber-optic glass before having to be amplified or regenerated. These wavelengths are partitioned into optical channels separated by guard bands of unused wavelengths. Different timeslot channels within wavelengths are assigned the laser pulses coding the information for different demands.) If a link between two adjacent nodes on the ring fails, traffic still flows between all origin-destination pairs of nodes using the reverse direction of routing. Thus, restoration is almost instantaneous (less than 50 milliseconds), and SONET ring owners can offer “self-healing” services.

However, this arrangement is costly, in that half the capacity of the ring is used only by an unneeded duplicate signal unless a failure occurs. (In a bidirectional SONET ring, protected signals are normally sent in only one direction and preemptable lower-priority traffic may use the other direction. If a failure occurs, the preemptable traffic is dropped and the direction of flow for all protected traffic is reversed, occupying the bandwidth that had been used for the preemptable traffic.) In addition, of course, a ring architecture is vulnerable to a coordinated attack that results in two simultaneous link failures that create two ring segments that are no longer connected. No node in one segment can then send a signal to any node in the other.

Weaker forms of protection do not require the entire protection path for a demand to be disjoint from the primary path. Instead, when a link fails, other non-failed links in the primary path may continue to be used, with traffic being switched locally around the failed link. Such local rerouting to restore traffic flows, called *restoration*, uses capacity more efficiently (and is less disruptive) than protection path switching, since a relatively small set of flows can be rerouted based on the specific location of a failure. Moreover, if it is assumed that only one or at most a few links will ever fail simultaneously, then the same protection paths and capacity can be reserved to handle the traffic from multiple primary paths. This leads to *shared-
capacity protection plans, where multiple primary paths are assigned the same protection capacity under the assumption that not all of them will require it simultaneously. Intelligent attackers may try to exploit such less-than-full redundancy to crash part of the network by causing more traffic to be switched onto protection paths than their capacity can hold. However, several contemporary network designs are resilient to any small set of failures.

2.3.2 Example: Resilient Packet Ring (RPR) protection scheme

Resilient Packet Rings (RPRs) use Ethernet packets, rather than dedicated light paths, to carry demands. They achieve fast recovery from fiber cuts, comparable to SONET ring self-healing services, while providing more efficient and flexible utilization of available capacity (bandwidth on links) since packets from the same session can follow different routes. RPRs are organized as sets of intersecting small fiber rings (called “ringlets”) which provide for highly flexible routing of traffic. As in a SONET ring, protected traffic can be “steered” or “wrapped” around a ringlet to avoid a failed link. (“Steering” redirects traffic in the event of a node or link failure by informing all nodes of the change in connectivity and letting the routing algorithms update packet routing decision tables based on the new topology. “Wrapping” simply treats the last node prior to the failure point as a new origin and forwards packets on to their destinations from there.) In addition, since each packet contains its destination node address (coded into the packet header data), this information can be used to route packets through the network while avoiding congested (or failed) links, using concurrent information about the currently least-congested routes as well as information about the priority classes for demands (e.g., to avoid slow delivery of consecutive packets in applications such as video that are sensitive to transmission delays). The intersecting-rings design allows many possible routes between origin and destination nodes, making the network “resilient” to failures in one or a few nodes or links.

3. TWO-STAGE ATTACKER-DEFENDER MODEL

Most traditional network designs have considered a network to be “survivable” if all protected traffic can be re-routed and carried without service interruption following loss of any single link (and/or node). Multiple simultaneous failures are usually treated as negligibly rare events. Of course, this can change dramatically when the failures are intelligently planned and coordinated instead of occurring at random. Multiple-failure events may then
become realistic possibilities, and network designs must be revised accordingly to defend against such events.

The vulnerability of a telecommunications network to intelligent attacks can be assessed with the help of the following two-stage attacker-defender model, in which an intelligent defender designs a network to withstand attack by an intelligent attacker with limited resources, anticipating that the attacker will optimally exploit any weaknesses.

STAGE 1 (DEFENDER’S MOVE):

The network operator (“Defender”) decides on all of the following:

- **Network topology**: What nodes are joined by what fiber links?
- **Fiber capacity**: How much bandwidth is installed on each link? (This typically involves deciding what terminating equipment to put at the nodes at the two ends of the link.)
- **Equipment locations and quantities**: What equipment (referred to generically as “network elements”) should be placed where in the network? This step specifies the locations of add-drop multiplexers (ADMs), regenerators and amplifiers to boost optical signals attenuated by passage through fiber, and wavelength conversion equipment (typically based on remotely configurable tunable lasers) to change the wavelengths used to carry specific optical signals, thus allowing more efficient use of wavelengths that would otherwise be underutilized. (Regenerators may be placed on links, but other network elements are placed at nodes; thus, this decision is mainly about what equipment to place at each site.)
- **Network interconnection**: Which fibers connect which network elements?
- **Admission control policy**: When new demands arrive dynamically, as requests for given amounts of connection bandwidth between two points (or among multiple points, for broadcast demands) for stated time intervals, the admission control policy determines which requests to accept and reserves primary paths and restoration capacity (for protected demands) to accommodate them. This chapter does not address dynamic admission control, but takes demands as given and known.
- **Traffic routing**: How is each demand routed through the network? Which channels on which wavelengths on which fibers carry each demand (for dedicated routes)? If the signal is converted from one channel or wavelength to another along the way, then which cards (electronics boards that plug into slots in the shelves of equipment racks) in which slots of which shelves in which equipment bays receive, convert, and send the signal? (Such detailed route planning is required to assure that sufficient ports and capacity are available to handle the assigned traffic.) In other words, what is the primary path for each demand? Assignments
of traffic to primary paths must be feasible, as determined by capacity constraints (including availability of cards and ports), interconnect plans, and signal power budgets and distance constraints (required to keep attenuation of optical signals and the optical signal to noise ratio, OSNR, within the tolerance of the signal processing equipment). For packetized traffic, what decision rules, algorithms, or routing tables are used to route packets through the network?

- **Restoration plans:** For protected demands, how will each demand be rerouted if nodes, network elements, or links on its primary path fail? For packet networks, how will packets be rerouted if congestion or failure is encountered, while still meeting constraints on delivery times, i.e., “latency”?

**Stage 2 (Attacker’s move):**

Once Defender’s move has been completed, Attacker may cut any \( k \) links simultaneously. Here, \( k \) is an integer reflecting Attacker’s ability to launch simultaneous attacks on multiple links simultaneously. A variation is to allow attacks on nodes instead of, or in addition to, links. (“Simultaneous” cuts are cuts completed within a short enough time so that the last is completed before the first is repaired.)

To model intelligent attacks in this framework, one might assume that the attacker has some particular goal in mind (e.g., to disconnect one or more specific target nodes or subsets of nodes, perhaps representing strategic command and control centers, from the rest of the network). The defender seeks to reserve sufficient protection capacity and diversity of paths in Stage 1 so that these targets can withstand any \( k \)-cut attack in stage 2. This means that, after any \( k \) links are cut, all protected demands can be re-routed on the reserved capacity. In particular, the network will withstand an attack in which Attacker optimizes some objective function (which may be unknown to the defender) to select which \( k \) links to cut. Formulating the problem as protecting against any \( k \) cuts makes it unnecessary to speculate more deeply about exactly how the attacker decides which links to target.

### 4. RESULTS FOR NETWORKS WITH DEDICATED ROUTES (“CIRCUIT-SWITCHED” NETWORKS)

This section considers the problem of designing attack-resistant circuit-switched optical networks. In a circuit-switched network, each demand is normally carried by a dedicated light path. The following special cases of this framework have been investigated.
4.1 Designing networks to withstand one link cut

The case $k = 1$ is the classic “survivable network” design problem of greatest interest when failures are random and are rare enough so that the probability of multiple simultaneous failures can be ignored. Designs that protect against any single link failure (such as “self-healing” SONET ring designs) also trivially protect against any single deliberate link cut.

Solving the multiple interdependent decision problems in Stage 1 even for $k = 1$ can lead to very large-scale, computationally intractable optimization problems (Tornatore et al., 2002) that include as sub-problems well-known difficult (NP-complete) combinatorial optimization problems such as the bandwidth-packing problem (Laguna and Glover, 1993; Parker and Ryan, 1994; Villa and Hoffman, 2006) and multicommodity network flow problems (one for each failure scenario) (Rajan and Atamturk, 2004). However, several solution heuristics and meta-heuristics have proved to be highly effective in solving real-world survivable network design problems with $k = 1$ (Soriano et al., 1998). For example, Rajan and Atamturk (2004) compare: (a) A relatively naïve two-stage hierarchical design approach, in which demands are first routed ignoring survivability requirements and then additional capacity is added to links to allow traffic to be re-routed in the event of any single link failure; to (b) A more sophisticated joint design approach that simultaneously routes demands along primary paths and reserves sufficient additional capacity to allow all traffic to be rerouted following any link failure. The joint design approach can be made practical by appropriate heuristics (discussed next) and achieves significant cost savings (on the order of 20%) compared to the hierarchical approach when capacity is expensive.

Although the literature on capacitated survivable network design problems is now vast (e.g., Soriano et al., 1998), many practical approaches use a combination of a few key heuristic ideas, such as:

1. Consider only a subset of all possible primary and protection paths.
   These are typically generated using a greedy or fast (low-order polynomial-time) heuristic (e.g., Dacomo et al., 2002), such as paths or rings constructed using modified shortest-path or minimal spanning tree algorithms. For networks with general topologies (i.e., mesh networks), it is common practice to search for rings or directed cycles that “cover” the nodes and links of the network, meaning that each node and each link belongs to at least one ring. These rings are then used to form protection paths. Finding minimal-cost ring covers in which each protection link is used exactly once can be accomplished easily for planar networks (since then each ring corresponds to a face of the graph), but is NP-hard in general. However, effective (polynomial-time) heuristics are available for
various ring-covering problems (including “double cycle covers” in which each ring appears in exactly two rings, being covered by a cycle in each direction exactly once) (Maier and Pattavina, 2002).

2. **Iteratively improve feasible solutions** by using local (myopic) search and optimization procedures to add or delete capacities to maintain feasibility while seeking to reduce costs.

3. **Ignore or relax difficult (e.g., integer-capacity) constraints** at first, so that useful initial approximate solutions can be obtained using linear programming. The solutions to the relaxed problem serve as starting points for myopic improvement heuristics.

4. **Use multiple random starting solutions and evolve the population of candidate solutions** (using meta-heuristics such as simulated annealing, greedy randomized search procedure (GRASP), Tabu Search (Laguna and Glover, 1993) and genetic algorithms) to discover lower-cost feasible ones.

The survivable network design approach of Rajan and Atamturk (2004) illustrates several of these ideas. To obtain a tractably small number of possibilities to evaluate, their solution heuristic only evaluates a subset of directed cycles as candidate paths for restoring traffic flows following a link failure. The cycles are generated and evaluated within an iterative “column-and-cut generation” heuristic optimization algorithm that uses a variant of a shortest-path calculation to quickly generate candidate directed cycles to consider as restoration paths. This restriction allows formulation of mixed integer programs (MIPs) that describe the capacitated survivable network design problem. The decision variables are the amounts of capacity added to each link. The constraints require that enough capacity be added to carry all traffic (i.e., demands) in the absence of failure and also following any single link failure. The objective function to be minimized is the total cost of all the capacity installed in the network. The resulting MIPs can be solved approximately in a matter of hours using a linear programming relaxation, strengthened with valid inequalities representing the survivability requirements.

Many other researchers have also proposed integer linear programming (ILP) formulations of the capacitated survivable network design problem with $k = 1$, differing according to the details of the technologies modeled, such as whether it is assumed that light paths must use the same wavelengths on all links or instead allow for wavelength conversion at nodes. Current solution heuristics typically give solutions with costs that are close (often within about 3%) of the theoretical optimum on benchmark cases where the exact solution is known or for which useful bounds are available (usually based on branch-and-bound solvers with relatively long run times).

A theoretical result of Brightwell et al. (2001) nicely captures both the computational intractability of exact solutions and the availability of good
approximate solution heuristics for the design of survivable networks with $k = 1$. The result is expressed for a particularly simple model in which the attacker seeks to cut a link to cause at least some traffic between a specified source node $s$ and destination node $t$ to become unroutable using the remaining capacitated links in the network. To prevent this, the defender is allowed to add additional discrete increments of capacity to the links (e.g., corresponding to additional terminating equipment). The defender knows the costs of adding different amounts of capacity to the links, and seeks a minimum-cost set of capacity additions that will allow all protected traffic to be rerouted between $s$ and $t$ following any single link cut. In this framework, Brightwell et al. establish that: (a) The problem can be solved easily (in polynomial time) using an algorithm based on shortest paths if the discreteness of capacity additions is ignored. (b) The problem is computationally intractable (NP-hard) when constraints are enforced reflecting the discrete nature of capacity expansion decisions (due to the fact that only a whole number of discrete capacity additions can be made on any link). (c) Despite this theoretical intractability, a simple polynomial-time heuristic based on modified least-cost path assignments provides solutions that are not more than 15/14 times more expensive than the exact (but perhaps too hard to compute) cost-minimizing solution.

4.2 Designing networks to withstand $k = 2$ link cuts

In light of the maturity and widespread practical deployment of survivable network designs for $k = 1$ cuts, an intelligent attacker attempting to disconnect one or more target nodes from a modern network by severing links will typically have to make at least two simultaneous cuts (e.g., one for each direction in a SONET ring). Choi et al. (2002) address the design of networks that remain connected when any two edges fail. Such networks, which must be 3-connected, must therefore also have 3 link-disjoint paths between any two nodes (by Menger’s Theorem in graph theory). These link-disjoint paths can be identified quickly (using a Ford-Fulkerson max flow algorithm). They are used to create a primary backup path and a secondary backup path. Any single link failure automatically triggers switching of affected traffic to the primary backup path, while a subsequent link failure then triggers switching to the secondary backup path.

Choi et al. consider several variations of this basic idea, involving different amounts of signaling after a failure event (to alert nodes to the change in network topology) and using different information about path failure vs. specific link failures. Based on an evaluation of restoration possibilities in three real-world networks (ARPANET, NJ LATA Network, and a national network), they conclude that “It is possible to achieve almost
100% recovery from double-link failures with a modest increase in backup capacity”. Thus, although much more can be done (e.g., to allow for dynamic restoration based on specific information about failed links, rather than pre-computed protection paths; or to minimize restoration capacity costs), it appears that designing networks to protect against $k = 2$ simultaneous cuts is practical.

### 4.3 Results for the general case of $k$ cuts

Brightwell et al. have extended some of their results for $k = 1$ to larger values of $k$, as follows. The problem of finding a minimum-cost set of protective capacity reservations (using link-disjoint paths) so that a specific demand can be restored following any simultaneous deletion of at most $k$ links, can be solved in polynomial time using a linear programming or ellipsoid algorithm, provided that the requirement that the capacities be integer amounts is ignored. (Recall that the demand is identified by a specific origin node $s$, a specific destination node $t$, and a bandwidth requirement $T$.) However, the problem is strongly NP-hard (even for $k = 1$) when the integer constraint is enforced. Despite this theoretical complexity, good approximate solutions can be found with relatively little computational effort using a successive shortest path method (involving solving several shortest path problems) for minimum-cost flow problems. For some specific formulations of the minimum-cost capacity-reservation problem, it can be shown that the solution found by ignoring integer constraints is no more than 6/5 times more expensive than the true optimal solution with integer constraints enforced, but is much easier to find.

In summary, it is practical to design networks that are resilient enough to protect any single specified demand against the failure of any $k$ arcs or nodes. The next step is to investigate extensions of this encouraging result from a single demand to all protected demands. This will require quantifying the costs of protecting different amounts of demand against simultaneous attacks of different sizes, $k \geq 1$. The work reviewed in this section provides the beginnings of a theory of resilient network design for arbitrary $k$, but much remains to be done to develop practical resilient designs for arbitrary $k \geq 1$.

### 5. Statistical Risk Models and Results for Scale-Free Packet Networks

This section considers statistical properties of failures in packet-switched networks when intelligent attacks are modeled by assuming that the attacker always targets the most heavily loaded node(s). In packet networks (e.g., the
internet), failures can be caused by overloading nodes; that is, by forcing more traffic to be routed through a node (e.g., a router) than it has capacity to handle. In this case, packets dropped at the overloaded node must be rerouted, shifting additional load onto nearby nodes. This may trigger a spreading cascade of congestion and node failures.

Although such a cascading failure process might be difficult to model mathematically in detail, it turns out that fairly simple methods adopted from statistical physics—especially, the statistical mechanics of phase transitions—provide useful insights into both the probability that a deliberate attack on the most-linked node(s) will succeed in inducing a cascade of node failures, and also the probable size of resulting network service outages.

Precise results have been developed for scale-free networks, i.e., networks in which the statistical distribution of connectivity is such that the probability that a randomly selected node is connected to $x$ other nodes is proportional to $x^{-\gamma}$ (a Yule-Simon power law distribution). Such networks arise naturally through preferential attachment growth processes in which “the rich probably grow richer”, i.e., each new node added to the growing network forms links to previously existing nodes with probabilities proportional to how many links they already have. These (and some other) random growth processes lead to networks in which a small fraction of nodes are major hubs with many links, while most nodes have relatively few links.

Empirically, scale-free networks with $\gamma$ values between 2 and 3 have been found to describe well both the statistical pattern of World Wide Web page links and also the statistical distribution of connections among routers (i.e., nodes) in the internet (as well as other networks, such as air traffic networks and metabolic and proteomic networks in systems biology). A study of 284,805 internet routers revealed a value of $\gamma = 2.3$, with the probability that a randomly selected node has $x = 1$ neighbor being $\Pr(x = 1) = 0.53$ and the probability that it has 100 neighbors being $\Pr(x = 100) = 2.5 \times 10^{-5}$ (Deccio et al., 2003).

Qualitatively, scale-free networks tend to be highly resistant to random failures, yet very vulnerable to targeted attacks. This is a direct consequence of the fact that they typically have a tiny proportion of very heavily connected nodes, so that crashing (in effect, deleting from the network) a few of the most heavily-loaded nodes can cause most of the network to collapse through cascading failures (Albert et al., 2000). For example, Deccio et al. (op. cit.) found that randomly deleting 1% of the nodes in a scale-free network (based on real internet router data) would leave over 97% of the original nodes operating normally; but targeting the top 1% of most heavily connected nodes for removal would reduce the size of the functioning network to less than 60% of its original size. Similarly, Crucitti
et al. (2004) found that the average time required to send packets through a network in many simulated examples with 2000 nodes and 10,000 edges was much more sensitive to intelligently targeted attacks than to random failures. Complete network failure (inability to deliver packets) occurred when about 0.4 of the nodes were removed in a targeted way, but not when 90% or more of nodes were removed randomly.

In practice, of course, even carefully planned and targeted attacks are more likely to bring down only a few nodes simultaneously than a high proportion of all nodes in a network. It is therefore desirable to understand the risk of network failure from an attack that succeeds in knocking out only one or a few most-heavily loaded nodes. To this end, it is convenient to adopt the following explicit (though admittedly simplified) model of how network traffic loads are initially allocated among nodes and how they are redistributed following a successful attack (Zhao et al., 2004).

1. In each time period, each node sends one unit of traffic to each other node via the shortest path between them. (Ties are resolved arbitrarily.)
2. The total load on any node is the total amount of traffic per unit time passing through it. By assumption (1), this is just the number of shortest paths passing through it. For scale-free networks, it can be deduced that node loads follow a power law distribution of the form $L(x) \sim x^\eta$, where $\eta > 0$ is a scaling exponent and $L(x)$ is the load on a node that is connected to $x$ neighbors (Zhao et al., 2004.)
3. The total capacity of a node is the maximum load that it can process.
4. A node fails if and only if the traffic load sent to it exceeds its capacity.
5. If a node fails, then all traffic is rerouted using the new set of shortest paths available after the failed node is deleted from the network.
6. The attacker chooses to attack the node with the largest number of links (i.e., neighbors).
7. The defender purchases sufficient capacity at each node to carry all of its original load plus some additional fraction $\alpha$ of that load: 
   
   $\text{Capacity allocated to node } i = (1 + \alpha) \times (\text{Load at node } i)$, 
   
   where $\alpha \geq 0$ is called the tolerance parameter.

This simple model leads to the following striking qualitative result. There is a critical value of the tolerance parameter, denoted $\alpha_c$ (a function of the scaling exponents in the power laws for the load distribution and the degree distribution, $\eta$ and $\gamma$, respectively, and of the number of nodes in the network) such that:

- If sufficient node capacities are allocated so that $\alpha > \alpha_c$, then attack on a single node in a large network has probability close to zero of crashing the network. More quantitatively, the ratio of the numbers of nodes in the
largest connected component of the network before the attack and after
the attack (and after any cascade of node failures that it triggers) will be
approximately 1.

- On the other hand, if $\alpha < \alpha_c$, then a successful attack that deletes
the single most-loaded node in a network has high probability (close to 1) of
crashing the network. In other words, the ratio of the numbers of nodes in
the largest connected component of the network before and after the
attack (and after any cascade of node failures that it triggers) will be
approximately 0 with high probability.

- Theoretical calculations and numerical simulations show that the
numerical value of the critical value of the tolerance parameter is
approximately $\alpha_c \approx 0.10$.

The critical value of the tolerance parameter may be interpreted as a
statistical margin of safety at which a statistical phase transition occurs
between the network being resilient to deletion of any single node (meaning
that other nodes remain connected, with high probability) and the network
being vulnerable to deletion of a single node (meaning that it triggers a
cascade of failures that end up disconnecting most nodes).

Many variations of this basic phase transition model have been explored,
and investigations of more realistic models and of the detailed statistics of
how networks break apart into disconnected fragments (including the
distributions of their numbers and sizes) in the vicinity of the phase
transition point $\alpha_c$ are ongoing (e.g., Duenas-Osorio et al., 2004). For
example, numerical simulations suggest that an attacker who attacks the
$k > 1$ most-linked nodes simultaneously can induce collapse of the network at
higher values of the tolerance parameter. The critical value of the tolerance
parameter increases approximately in proportion to the number of
simultaneous attacks, $k$ (Zhao et al., op. cit., Figure 4.) Attacks on edges as
well as on nodes have been studied and scale-free networks have been
modified to include different types of clustering (e.g., Holme et al., 2002).
Dynamic models, in node deletions by an attacker and node additions or
reparis by a defender take place over the same time interval, have also been
examined. These lead to the conclusion that the evolving network remains
highly connected (it has a giant component) with high probability
(approaching 1 in large networks) if the rate at which the attacker can delete
nodes is sufficiently small compared to the rate at which the defender can
repair or replace damaged nodes (Flaxman et al., 2007). Recently, effects of
attacker information on the vulnerability of scale-free networks have been
investigated. One conclusion is that concealing information about a small
fraction of nodes from the attacker can greatly improve the ability of
networks to withstand intelligent (but incompletely informed) attacks
(Gallos et al., 2005; Wu et al., 2007).
These more sophisticated models share with simpler ones the key qualitative property of phase transitions, in which sufficient capacities (and/or repair rates) protect against large-scale failures with high probability (approaching 1 in large networks), while insufficient capacities (or repair rates) allow the possibility that a small set of attacks (possibly on only one node) can trigger a cascade of failures that leave most of the network disconnected. Although a great deal of additional quantitative detail has been uncovered through theoretical analysis and numerical simulation of attack-defense processes near the phase transition boundary, and although this remains a very active area of research, the crucial qualitative insight that there is often a well-defined transition from low-vulnerability to high-vulnerability as load increases relative to capacity is one of the most valuable and robust lessons to emerge from the study of attack and defense in scale-free networks.

The existence of such a phase transition suggests that many network risk management decision problems can be simplified to the task of keeping networks in the low-vulnerability regime. This is done by maintaining sufficient margins of safety (e.g., greater than $\alpha_c$) so that the network will be able to withstand attacks. Simulation and detailed mathematical analysis of phase transitions provide practical methods for quantitative assessment of the required safety measures. For the specific attack model of Zhou et al. (2004) discussed above, a useful design rule of thumb is that $\alpha > k*10\%$ provides an adequate safety margin for withstanding $k$-link attacks.

6. DISINCENTIVES TO INVEST IN PROTECTION

The preceding sections have described several recent constructive approaches to designing telecommunications networks (circuit-switched or packet-switched) that can withstand targeted attacks at several locations simultaneously. These approaches indicate how investing in protection capacity can make it possible to restore protected demands or sessions almost immediately following such an attack. This section assumes that investment in extra capacity can indeed protect against potential attacks, and asks whether network owners and operators have the incentives to actually make such investments. How do interdependencies among the risks and benefits of jointly owned network infrastructure affect incentives to invest in protection?

Telecommunications networks typically have many owners and many users; they exemplify systems in which interactions among players drive the costs and the benefits received by each. Many of the best-studied models in game theory may be interpreted as special cases of network games. The
8. Making Telecommunications Networks Resilient

Following examples are intended to illustrate how some of the most familiar paradigms of cooperative and non-cooperative game theory apply to decisions about whether to invest in improved reliability (or resilience, if failures come from deliberate attacks) in telecommunications networks. Throughout this section, the focus is on whether network owners will invest in improved network reliability, without regard for whether potential failures result from deliberate attacks or random failure events; thus, we will use the general term “reliability” to refer to the probability that a system does not fail, without further inquiry into possible reasons for failure.

6.1 Example: An N-Person Prisoner’s Dilemma for Network Maintenance

**Setting:**
Suppose that three different owners own the three different links in the following linear series network.

\[
A \rightarrow B \rightarrow C \rightarrow Z
\]

It costs $1 to maintain each link. Doing so guarantees that the link can reliably transport 2 units of traffic. Without maintenance, the link deteriorates with probability 0.5 (possibly due to deliberate attacks, but this example can also be applied to random failures); a deteriorated link can reliably transport only 1 unit of traffic. In this simplified model, each owner decides at the start of the game about whether to invest in maintenance, and any deterioration of non-maintained links takes place immediately after the decision has been made.

Demand for network services is such that customers will use this linear chain network to carry as much traffic as it can carry reliably (1 unit or 2 units), generating either $6 or $12 units of revenue, respectively, which is then shared equally among the link owners, giving each either $2 or $4, respectively.

**Problem:**
What is each owner’s optimal strategy for investing in maintenance?

**Solution:**
If all players maintain their links, each receives a profit of \((\$4 \text{ revenue} - \$1 \text{ maintenance cost}) = \$3\). A player who does not maintain his own link when both the other two players maintain theirs also receives \(0.5 \times \$4 + 0.5 \times \$2 = \$3\) expected profit. A player who maintains his own link when only one of the other two players does so receives an expected profit of \(0.5 \times \$4 +\)
0.5 \times $2 - $1 = $2; but if he chooses not to maintain his own link, then his expected profit increases to $0.25 \times $4 + 0.75 \times $2 = $2.5. A player who maintains his own link when neither other player does likewise receives an expected profit of $0.25 \times $4 + 0.75 \times $2 - $1 = $1.5; but if he chooses not to maintain his own link, then his expected profit increases to $0.125 \times $4 + 0.875 \times $2 = $2.25. Thus, no matter what the other players do, each player maximizes his own expected profit by not maintaining his own link. Doing otherwise might decrease, but cannot increase, his expected profit.

DISCUSSION:

When all players follow the unique dominant strategy of not investing in maintenance, each receives an expected profit of only $2.25 (or $2 per day in the long run, if the play is repeated on consecutive days until all links fail). But if all players would maintain their links, each would receive a profit of $3. Thus, the dominant strategy is Pareto-inefficient: all players could do better by choosing a different (dominated) strategy. This is like a three-player version of Prisoner’s Dilemma, in that the unique dominant strategy for all players gives each a lower payoff than would one of the dominated strategies. A similar result holds in analogous games with \( N > 3 \) players, i.e., the unique Nash equilibrium is to under-invest in maintenance.

This example suggests how the presence of multiple owners in a network can lead to free-riding incentives, under-investment in network maintenance or quality, and Pareto-inefficient provision of network resources to users who would be willing to pay for better service.

6.2 Example: Nash equilibrium can be inadequate for predicting investments

SETTING:

Suppose that player 1 owns the link from A to B and that player 2 owns the link from B to C in the simple network: \( A \rightarrow B \rightarrow C \). A customer is willing to pay up to $100 per month to use this network to send messages from A to C, provided that the product of the reliabilities of the two links is sufficiently great, say \( p_1p_2 \geq 0.5 \). Assume that Player 1 must select a non-negative reliability \( p_1 \) between 0 and 1 (inclusive) for link AB, and that Player 2 must select a non-negative reliability \( p_2 \) between 0 and 1 for link BC. The customer will pay each player $50 per month if and only \( p_1p_2 \geq 0.5 \), and otherwise will pay 0 and will forego using the network. It costs a player $50p per month to maintain a reliability level \( p \) on his link.

PROBLEM:

What reliability level should each player choose for his link?
SOLUTION:
This is an instance of the classical two-person bargaining game (isomorphic to the “divide a dollar” game), to which an entire large literature is devoted. Every pair of nonnegative reliabilities \((p_1, p_2)\) such that \(p_1 p_2 = 0.5\) is a Nash equilibrium, since if one player can credibly insist on maintaining a level \(p\), then the other player’s unique best response is to settle for maintaining level \(0.5/p\). Thus, the Nash equilibrium concept is inadequate to predict a unique outcome for this game. Axiomatic bargaining theory (including the Nash bargaining solution) proposes various normative justifications for specific solutions, especially the symmetric (in dollars, although not necessarily in utilities) solution \((p_1, p_2) = (0.707, 0.707)\), but confident prediction of a specific outcome is impossible. In some cases players may commit themselves to inadequate investments in unsuccessful attempts to induce each other to spend more, thus arriving at a Pareto-inefficient outcome in which neither sells capacity to the customer (Roth, 1985).

6.3 Example: Unstable network collusion

PROBLEM:
A customer is willing to pay $6 to send crucial data from the origin \(O\) to the destination \(D\) along any highly reliable path. There are three owners, 1, 2, and 3, of network links. Links \(AB\) and \(BE\) belong to player 1, links \(BD\) and \(CE\) belong to player 2, and link \(ED\) belongs to player 3. Suppose that all links are currently low-reliability, but that any link can be converted to high-reliability by adding expensive terminating equipment at either end. If it costs $1 to upgrade the links, how should the three players cooperate to make an offer to the customer?

![Figure 8-1. Network showing which player (1, 2, or 3) owns each link.](image)

SOLUTION:
This is an example of a cooperative game with an empty core: there is no coalition and agreement among its members that is proof against different
coalitions being formed that can improve the profits offered to each of its members. Therefore, *no possible coalition is stable*. The customer may wait forever for the owners to stop realigning and make an offer.

For example, suppose that player 1 approaches player 2 and proposes that they each invest a dollar (player 1 to upgrade link AB and 2 to upgrade link BD) and then offer the customer the use of path OABD and split the $6 from the customer evenly. Under this agreement, players 1 and 2 each make a profit of $3.00 – $1.00 = $2.00 and player 3 makes nothing. Dissatisfied with this outcome, player 3 might approach player 2 with the suggestion that player 3 invest in upgrades for both 3’s own link (ED) and also one of player 2’s (CE). Then the two can team up to offer path OCED to the customers, split the $6 evenly, and player 2 will make a profit of $3.00 (beating the profit made in the proposal from player 1) while player 3 will make a $1.00 profit (beating its zero profit under player 1’s proposal.) Player 1 will now be excluded and make no profit. (Player 3 might propose many other deals, but this illustrates that player 3 has both the incentive and the ability to make a deal with 2 that both of them would prefer to the one that player 1 initially proposed.)

Rather than making no profit, player 1 can do better by offering to team with player 3. For example, player 1 might now offer to invest $2.00 (one each in links AB and BE), have player 3 invest in only one (ED), and split the $6 evenly, so that player 1 makes a $1.00 profit and player 3 makes a $2.00 profit. Player 2 is excluded. But now, player 1 can re-propose player 1’s original offer back to player 1 (giving each of them a profit of $2.00). And so the cycle continues: Whoever is currently left worst off (e.g., excluded from making a profit) by any proposed agreement can make an offer to one of the other players that will increase both their profits (and make someone else worst off, and hence ready to propose a different deal.) There is no possible agreement that cannot be improved (in the sense of increasing profits for all who participate) by some subset of two players who have both the incentive and the power to do so. Thus, companies trying to find the best deal for themselves by exploring different partnerships will find that there is no solution to this problem.

### 6.4 Example: A tipping point

Suppose that Player 1 will invest in security if at least 2 other players do; that player 2 will invest in security if at least one other player does, and that player 3 would like to invest in security, but only if everyone else does. If these preferences are common knowledge, then player 3 can tip the system from no investment by any player to investment by all players by being the first to invest (thus inducing player 2, and then player 3, to follow.) If the
players do not know each others’ preferences, however, then each will wait for someone else to move first, no tipping point is reached, and the players fail to make the mutual investment in security that all three of them would prefer to make. Thus, knowing the player’s preferences and willingness-to-pay for investments in security (or network reliability) is not sufficient to predict what will happen: knowledge of what the players know about each others’ preferences is also needed.

The examples in this section have led to the same major policy-relevant conclusion by different routes: even if it is possible to solve the purely technical problems of devising cost-effective networks that are resilient against accidental and/or malicious failure (e.g., using the heuristic design methods and statistical phase transition/safety margin approaches discussed in earlier sections), *interdependencies among network owners can undermine willingness to invest in network resilience, leading to socially sub-optimal (Pareto-inefficient) decisions that invest too little.* In some cases, there may be simple solutions (e.g., to create an artificial “tipping point” by stimulating initial investments in increased security or by providing players with credible information about each others’ preferences.) However, the incentive, information, and distributed decision-making challenges illustrated in these examples have proved to be enduring and difficult in many applications of game theory. Socially optimal investment in more resilient telecommunications networks may be inhibited by these challenges, even when algorithms for minimizing the costs of protecting against intelligent attacks are well developed.

7. **SUMMARY AND CONCLUSIONS**

Mathematical optimization approaches can be used to design networks that can withstand the simultaneous loss of any \( k \) links or nodes, where \( k \) is a small integer reflecting the attacker’s ability to do simultaneous damage. Approaches for \( k = 1 \) and \( k = 2 \) are well developed. However, optimal (least-cost) design of networks that are resilient to \( k \) link cuts or node deletions, for arbitrary \( k \), remains an open problem.

Simple probability and statistical models have been developed that predict the effects of attacks and repairs in large scale-free networks (typical of large data networks, including the internet), assuming that the attacker always targets the most heavily loaded links or nodes. These models typically exhibit a *phase transition*, in which the networks are inherently resilient to attacks if and only if they have enough spare capacity at each node (about \( 10k\% \) more than would be required in the absence of attacks, if the attacks are focused on the \( k \) most heavily loaded nodes). Networks with
enough extra capacity at each node can absorb the impacts of successful attacks by redistributing the traffic originally routed through failed nodes to surviving neighbors, leaving almost 100% of the network (other than the failed nodes) still connected. On the other hand, networks with less than this critical amount of extra node capacity are vulnerable to cascading failures (similar to spreading blackouts in an electric grid), so that a successful initial attack can lead to the progressive collapse of the network, with the largest connected component remaining after the attack and its aftermath probably consisting of a negligibly small fraction (close to 0%) of all nodes. This threshold-like division between resilient and vulnerable networks makes it relatively simple to design resilient networks: simply include enough extra capacity at each node so that attacks will be absorbed rather than causing cascading failures.

Although optimization and probability models may reveal how to design networks that can withstand intelligent attacks, network operators who own only some portions of a network may lack incentives to actually make the required investments. Strategic incentives can encourage network owners to invest too little in network reliability and resilience. The traditional game-theoretic problems of free-riding, Pareto-inefficient Nash equilibria, non-unique Nash equilibria, empty cores, and poor coordination due to private information, can be powerful in network investment settings. Each problem can result in under-investment in network protection, as judged by the criterion that all players would benefit if all could commit to make greater investments in network reliability and resilience. Regulatory intervention, centralized command and control, or improved institutional designs facilitating binding mutual commitments and multi-way contracting may be required to overcome such adverse incentive effects, enabling network owners and users to reap the potential benefits from greater network reliability and resilience.

REFERENCES


8. Making Telecommunications Networks Resilient


Chapter 9

IMPROVING RELIABILITY THROUGH MULTI-PATH ROUTING AND LINK DEFENCE
An Application of Game Theory to Transport

Urszula Kanturska, Jan-Dirk Schmöcker, Achille Fonzone, and Michael G H Bell

Abstract: This paper looks at the vulnerability of transportation networks against minor (e.g. demonstrations) and major (e.g. terrorists attacks) incidents by using an attacker-defender model which applies the game theoretic approach proposed by Bell (2000). An example based in London illustrates the use of the model. The example analysis shows how the critical links can be identified in the network and illustrates the benefits of using mixed route strategies. The chapter further looks at the impact of infrastructure protection on the optimal solution through defender-attacker-defender models. Different scenarios are defined to reflect the degree of visibility of the protection and the solutions show that this will influence the expected benefit significantly.

1. INTRODUCTION

The origins of reliability analysis in the field of transportation arise from the fact that transport networks are subject to two types of phenomena: (1) fluctuations of the transport demand, and (2) variations in the supply of transport services. Some variability of demand is normal and occurs on day-to-day basis, but one can distinct also abnormal variations, associated with exceptional conditions, such as major sporting or cultural events. Bell and Iida (1997) note that although networks can be designed to cope more efficiently with normal fluctuations of flows, planning for abnormal events is more difficult. Supply variations might be expected by the traveller (for example pre-announced building sites) or unexpected (for example accidents) and in return lead to further demand variations. Nicholson et al (2003) distinguish between benevolent, neutral and malevolent network
interventions, the latter being most likely to cause the greatest disruption. Benevolent incidents are those that aim for impact minimisation (e.g., placing building sites at night when flow is low), natural disasters can be classified as neutral or random interventions, while examples of malevolent actions are terrorist attacks or demonstrations, both which intend to cause maximum commotion. In assessing the reliability of networks it is therefore necessary to take into account the level of malevolence of the potential intervention. For example assessment of networks in terms of their resilience against random failures requires a different methodology than assessment of their ability to cope with targeted attacks. The mitigation measures as well as the expected cost of disruption will be different for each of these cases and situations where malevolent attacks are more likely might justify higher spending on protective measures.

The reliance of modern societies on various networks and concentrating vital assets in urban areas make them an attractive target for destructive attacks. There have been numerous studies devoted to the impact of link failures in transportation networks (see for example papers in Bell and Cassir (2000) or Bell and Iida (2003)), but aside from Angeloudis and Fisk (2006) very few studies were devoted specifically to the topic of terrorist attacks on transport networks. This chapter looks at the vulnerability of transportation networks against minor (e.g., demonstrations) and major (e.g., terrorists attacks) malevolent incidents. Due to the fact that in most cases it is impossible to predict probabilities for such events or to influence the hazards in order to reduce the risk, consequence minimisation has become an important aspect of vulnerability studies.

The remainder of this chapter is organised as follows: The next section (Section 2) reviews various methods proposed in the literature to analyse scenarios of “attack and defence”, where the “defence” represents both rerouting opportunities and protective measures. This includes a general description of the game theoretic approach adopted in this research. Section 3 presents an application of the game-theoretic methods to VIP transport problem in London. The method developed by Bell (2000) is applied in Section 3.2, while in Section 3.3 a second level of defence, namely active link protection is discussed. The theory and previous applications of such Defender-Attacker-Defender models are described in the literature review. In this chapter the defence of a link is understood as a measure which completely excludes the possibility of an attack to be successful on this link. In practice such a defence might be supplied by police whose presence would make it impossible for any spoiler to succeed. Section 3.3 presents three different scenarios which differ in terms of the visibility of the defensive measures. Firstly, the link defence is visible in which case the spoiler will aim to attack a different, non-protected link. In the second
scenario the link defence is invisible which means that the attack fails in case it hits a defended link. In the final scenario the three-person game is played, in which the traveller and the attacker both anticipate the presence of protective measures and adjust their strategies respectively. The chapter finishes with a comparison and discussion of the results obtained in each case and points out limitations of the current work to be addressed in further research.

2. LITERATURE REVIEW

2.1 Reliability of transportation networks under attack

The quality of service offered by transport systems has been subject to extensive research in recent years. Immers et al. (2004) highlight that a transport system is reliable when experienced travel time is not very different from the expected one; in general the divergences are brought about by changes in demand and supply patterns which can be expected or unexpected, frequent or exceptional as discussed in the introduction. For example, a terrorist attack against transported VIPs (Very Important Persons) would be unexpected with respect to type and location, exceptional and highly malevolent; in such a case Berdica (2002) suggests focusing on vulnerability and on consequence minimisation.

In coping with vulnerability and, more generally, with reliability in the field of transportation, it may be tempting to use the achievements of other engineering disciplines dealing with networks (e.g., Grubesic and Murray, 2006). Their applicability is however limited for several reasons: firstly, organization and topological features of networks differ (for an exhaustive analysis of the characteristics of the structure of road networks, see Xie and Levinson, 2006); secondly the settings of the problems e.g. the time scale of changes in the system (Wong, 1984) is not the same; thirdly the nature of its users of transport networks is unique, as they are characterised by self-awareness and freedom (Clement et al., 2005).

In order to consider these attributes of travellers Bell (2000) and Bell (2003) look at the impact of routing strategies on network reliability given a malevolent attack. Jenelius et al. (2006) put forward the concepts of link importance and site exposure to deal with very rare events, proposing measures based on the increase in generalised travel cost caused by rerouting when some links are removed. A similar approach can be found in Scott et al. (2006), who present case studies implementing an equilibrium assignment and show that their measure of link importance, called the Network Robustness Index, can improve the effectiveness of highway planning. Their
index ranks the link importance according to the increase in travel cost if the link would be blocked.

The need for including cost-benefit analysis of reliability and vulnerability into investment project evaluation is highlighted in Husdal (2004), while Zhang and Levinson (2004) show that investment policies determine the hierarchy of transport networks and so their performance in case of link failure.

### 2.1.1 Attacker-Defender models

The literature concerning transport networks under attack can be classified according to the degree of complexity in representing flows: the simplest models, referred to as 0-degree models, consider empty networks and examine just their topological features. An example of such an approach is Angeloudis and Fisk (2006), who inspect the topology and robustness of the largest subway systems in the world in the case of targeted attacks following Albert et al. (2000).

The most studied problem is that of a flow between a single origin-destination pair (in the following abbreviated as ‘O-D pair’), sometimes referred to as 1-degree models and in the operations research literature also known as network interdiction problems (see Pan (2005) for a comprehensive bibliography). The interdiction model is an Attacker-Defender (AD) model, in which an attacker maximizes the defender’s minimum operating cost. Situations are studied in which an attacker tries to thwart the mobility in a network, interdicting a given number of links with the intent of maximizing the shortest path (e.g., Israeli and Wood 2002) or minimizing the maximum flow between two nodes. The latter case of interdiction problem has been studied in two ways; deterministic, in which there is no uncertainty related to network features and attack effectiveness (Wood, 1993; Washburn and Wood, 1995; Royset and Wood, 2006) and stochastic, in which arc capacities and/or attack outcomes are random, (Cormican et al., 1998; Pan, 2005). Recently interest is growing in analysing networks with many O-D pairs (n-degree models), as in the above-mentioned Scott et al. (2006) paper. AD models lead to bi-level optimization problems, which enable to find the most critical links in case of no defence. Brown et al. (2006) highlight that if resources for such a defence are available, the elements classified as critical through an AD model do not necessarily coincide with the ones to be protected.
2.1.2 Defender-Attacker-Defender models

Brown et al. (2006) therefore propose to embed an AD model in a tri-level optimization problem called a defender-attacker-defender (DAD) model, in which the defender has limited resources to protect the system and must decide where to employ them to minimize the damage the attacker is able to cause. An example of a DAD approach is Church and Scaparra (2005), dealing with the “interdiction median problem” and considering protective measures referred to as “fortification”. The objective of this problem is to find the so called interdiction set, i.e. to find those locations of supply which, when removed, yield the highest increase in travel distance. The authors show that each subset of facilities “which when fortified, provide the best protection to a subsequent optimal $r$-interdiction strike” must contain at least one element of the interdiction set, but does not necessarily coincide with it. Also Smith et al. (2007) implement a DAD model for the design of survivable networks. Their paper considers two-player games under three different attack strategies: in the first game the spoiler destroys the links with the largest capacities, in the second the ones with the highest initial flows, in the last the ones with the highest initial flows, in the last those whose failure minimizes the revenues generated by the flows.

2.2 Games in Transportation problem

2.2.1 Introduction

The theory of games, initially developed in the 1950’s in the field of economics (see Osborne (2003) for an exhaustive introduction to the topic), is a study of the interaction between rational decision makers. Game theory approach is useful for studying multi-agent environments, in which the utilities of agents, depend on the interaction of all agents. Transport systems are such complex environments in which local and global, benevolent and malevolent, cooperative and non-cooperative actors play the same game. Similarities and differences between Wardrop’s principle that “at the equilibrium, the cost of the used paths are equal and no single user can change path without decreasing her utility” (Wardrop, 1952) and Nash equilibrium, in which “given the strategies of other players, no player has interest in changing its own” (Nash, 1950; Nash, 1951), are dealt with by Altman and Wynter (2004). The authors explain that Wardrop equilibrium belongs to a class of games known as “potential” games (Monderer and Shapley, 1996), which are special cases of the “population” games (Sandholm, 2001).
2.2.2 Non cooperative games

Non-cooperative games are those in which “players are unable to make enforceable contracts outside of those specifically modelled in the game. Hence, it is not defined as games in which players do not cooperate, but as games in which any cooperation must be self-enforcing” (Shor, 2005) and so are particularly suitable to describe behaviours in a transport system. Hollander and Prashker (2006) provide a review of non-cooperative game theory applications in the field of transportation, stressing that game theory can contribute significantly to the insight of a given situation. Games are classified in four groups: against a “demon”, between travellers, between authorities and between travellers and authorities.

Games against a demon are zero-sum games, in which one or more spoiler try to maximise user costs. Given the great generality of game theory, players and their strategies can be of completely diverse nature: In Colony (1970), the user can choose between an arterial road and a motorway; in Bell (2000), and in Bell and Cassir (2002) one or multiple users look for the best routing strategy given one or multiple demons, being part of the game; in Bell (2004) the case of a freight dispatcher is dealt with. The solutions obtained in Bell’s games, represent a pessimistic perspective of network users and give useful indications on network reliability. A non-cooperative game interpretation can be given also for the solution to the risk-averse routing of hazardous materials as in Bell (2006), where the use of a mix of routes is proposed as a measure to minimize risks.

Games between travellers and authorities can be seen as a generalization of the games against a demon, in which players have different but not necessarily opposite goals. These models provide a source of fruitful ideas regarding network vulnerability. In particular, Fisk (1984) and Lim et al. (2005) who solve bi-level optimisation (AD-like) problems, respectively for signal control regulation and for continuous network design, referring to the framework of Stackelberg games. Lim et al. (2005), Chen and Ben-Akiva (1998) and Van Zuylen and Taale (2004) discuss how the game structure, i.e. the degree of certainty with which each player knows others’ strategy, can influence the outcomes of the game.

2.2.3 Bell’s approach

Hollander and Prashker also distinguish between conceptual and applicable games, classifying the zero-sum games against the demon into the first group. This chapter demonstrates that the method proposed by Bell (2003) not only fits into a wider DAD framework, but is also a ready-to-
apply tool for the assessment of network vulnerability against an attack, as demonstrated.

This method is a game between (1) a traveller, referred to as the ‘router’, who seeks a least-cost path between his origin and destination, and (2) a demon, who strives to maximize the trip cost by failing one link. The equilibrium solution to the game gives the optimal strategy for the traveller to avoid excessive costs, as well as the optimal strategy for the demon to be sure that at least a certain loss will be caused irrespective of the path selected by the traveller. The expected trip-cost at equilibrium can be treated as a measure of overall network vulnerability, while the link failure probabilities indicate links that are critical for network performance. The optimal strategy for the traveller in general involves using more than one path. Similarly, the optimal spoiler strategy is to split disruption probabilities over more than one link. The solution delivers the worst case link attack probabilities, on the assumption that that these are what the traveller is reacting to. At the equilibrium, the expected cost is the same irrespective of which link is attacked. The sequence of actions performed by both players is depicted in Figure 9-1.

![Figure 9-1. The sequence of the game by Bell (2003).](image-url)
3. APPLICATION OF GAME THEORY TO THE VIP TRANSPORT VULNERABILITY

3.1 Problem description

What strikes many visitors more than anything else about London is the size of the city. Stretching for more than thirty miles on either side of the River Thames this ethnically diverse place hosts world-class museums, galleries and institutions. London’s traditional sights continue to attract millions of tourists every year, while the financial City draws in the prosperous enterprises. Businessmen, diplomats, politicians, artists, sportsmen, let alone Royal Family members are all intrinsic to the city’s public scene. Everyday some famous, influential or prominent people are moved across London, protected by the bullet-proof windshields of their cars and a team of devoted bodyguards.

Providing safe, secure and reliable transport for the VIPs is a challenge which motivated the research presented in this chapter. Policing, security checks, remote surveillance and security service patrols are usually deployed when a VIP is present at an event or transported from one place to another. However, some network connections, links or routes may be more liable to attack or disruption than others, and if so, strategies should be deployed which protect assets and people most effectively.

In the face of raising security concerns this chapter considers transport between important public venues as an example to understand the benefits of risk-averse planning. The data available for this analysis comprised of the entire Greater London road network including link characteristics, such as permitted speeds, capacities and number of lanes. The analysis described here was focused on the transport link between Greenwich Park in South London and Victoria Park north of the river in the London Borough of Hackney.

Greenwich Park is part of the Greenwich World Heritage Site and as site of historical interest and great visual appeal, attracts numerous visitors everyday. It is also used for cultural and sporting events. On the other hand, Victoria Park is the oldest public park in Britain located in the heart of London’s East End. In recent times, the park became noted for its open-air music festivals, often linked with a political cause. The considered part of the network comprises three river crossings: (1) Blackwall Tunnel, (2) Rotherhithe Tunnel and (3) Tower Bridge.

It is shown that, given no information about a potential attack, the risk of an incident can be minimised if multiple routing is applied. In order to assess the vulnerability of the connection between the parks i.e. to identify those links whose failure would disrupt the transportation the most, an AD model
based on the method proposed by Bell (2000) is applied referred to as the “base scenario”.

The solution of the AD model identifies a set of critical assets (components) for system performance. This prompts questions such as: What can be done to decrease systems exposure to threat? Which link should be protected assuming that there are only limited resources sufficient to assure reliability of just one link? Is it better to keep the planned defence plan secret, and if yes, should it be unknown even to the traveller? These and similar questions triggered development of some heuristics for approximating the solution to the “optimal defence problem” presented in this chapter as scenarios “visible defence” and “invisible defence”. It further leads to embedding the AD model (“base scenario”) into a DAD framework and extending it to what is further described as “anticipated defence” scenario.

In all of the models described below the traveller’s path choice behaviour was modelled by VISUM, a macroscopic traffic assignment software, widely used for small- and large-scale traffic assignment problems as well as for multimodal assignment problems. VISUM has been interfaced via the COM-interface with purpose-written Python scripts. In the iterative solution procedure Python updates link costs upon which the least cost path search is performed by VISUM.

3.2 The AD approach to the VIP transport vulnerability

In Bell and Cassir (2002) and Cassir et al. (2003) it is considered that the travel cost is indirectly influenced by the link status because a failed link is defined as a link with reduced capacity and hence leading to higher congestion. In contrast, the VIPs that could be an appealing terrorist target are often transported with a priority, assisted by emergency vehicles. Therefore background traffic flows are not taken into account and it is assumed that the travel cost is directly influenced by the disruption. Let us consider a network composed of $N$ nodes and $L$ links. There are $R$ origin-destination relations of interest and it is assumed that there exist $|F|$ failure scenarios.

Following Bell (2003) the game described above can be expressed as a bi-level optimisation problem, but in contrast to standard bi-level problems both problems are solved simultaneously.
Chapter 9

Notation

- **p**: vector of link choice probabilities
- **q**: vector of link failure probabilities
- **h**: vector of route choice probabilities
- **d**: vector of link defence (protection) probabilities
- **F**: set of links that can be attacked (set of failure scenarios)
- **TC**: total cost of travel between one O-D pair expressed here in terms of travel time
- **C**: matrix of travel costs on link \(i\) under failure scenario \(j\)
- **tt\(_i\)**: travel time on link \(i\)
- **DC**: disruption factor indicating the increased cost in travelling an attacked link (input parameter reflecting severity of an attack)
- **sc\(_i\)**: expected travel cost on link \(i\)
- **a\(_{ijk}\)**: link-route incidence matrix (1 if link \(i\) is on route \(k\), 0 otherwise)
- **g\(_{jk}\)**: travel cost on route \(k\) under failure scenario \(j\)
- **u\(_j\)**: the expected trip cost under failure scenario \(j\)
- **v\(_k\)**: the expected cost of a path \(k\) under all failure scenarios

3.3 Mathematical Formulation

As indicated in the notation, each link can assume two states: normal or failed. An attack on a link leads to its failure, which is expressed as an increase in travel time by factor \(DC\). Similarly to Bell (2003) we assume that each scenario \(j \in F\) corresponds to the attack on one single link, hence the link costs can be expressed as in Equation 1:

\[
c_{ij} = \begin{cases} 
  tt_i & i \neq j \quad \text{- cost of link } i \text{ in a normal state} \\
  DC \cdot tt_i & i = j \quad \text{- cost of link } i \text{ in a failed state}
\end{cases}
\]  

The game can now be formulated as the optimization of the total cost \(TC\) with respect to the link-use probabilities \(p\) and the attack probabilities \(q\). If only transport between a single O-D pair is considered the bi-level problem is then to solve the maximin problem in Eq. (2) simultaneously:

\[
\max_{q} \min_{p} TC(p, q) = \sum_{i} \sum_{j} p_i c_{ij} q_j 
\]

subject to \(\sum_{j} q_j = 1\) and \(\sum_{k} h_k = 1\) with \(q_j \geq 0 \forall j; h_k \geq 0 \forall k\),

where link-use probabilities are formulated in terms of path-use probabilities \(h_k\) via the path-link incidence matrix.

\[
p_j = \sum_{k} a_{jk} h_k
\]
At equilibrium the link failure probability $q_j$ can only be nonzero if the expected trip cost $u_j = \sum_k g_{jk} h_k$ under failure scenario $j$ reaches a maximum:

$$\sum_k g_{jk} h_k = \max_s \sum_k g_{sk} h_k \Leftrightarrow q_j \geq 0$$

$$\sum_k g_{jk} h_k < \max_s \sum_k g_{sk} h_k \Leftrightarrow q_j = 0$$

(4)

where $g_{jk} = \sum_i a_{ik} c_{ij}$ for all paths $k$ and scenarios $j$.

Similarly, at equilibrium the path-use probabilities $h_k$ will only have a non-zero value if the expected cost of a path $k$ under all failure scenarios $v_k = \sum_j q_j g_{jk}$ is minimal:

$$\sum_j q_j g_{jk} = \min_s \sum_j q_j g_{jk} \Leftrightarrow h_k \geq 0$$

$$\sum_j q_j g_{jk} > \min_s \sum_j q_j g_{jk} \Leftrightarrow h_k = 0$$

(5)

Noted should be the lack of a time dimension: The router does not proceed through the network links dynamically. However, taking into account a fact that the VIP routes are generally pre-planned and not adjusted in the course of the journey (as opposed to usual car drivers), such a static approach seems suitable, especially for strategic planning.

The above notation, as well as objective function, are expressed in terms of link use probabilities as it allows for easy implementation with Python scripts. However, it is also possible to consider this and following problems in terms of path choice probabilities, as e.g. in Bell (2003). The latter formulation proves more useful when one needs to generalise the problem and consider an attack on several links.

The algorithm used to solve this bi-level problem is based on the Method of Successive Averages (Sheffi, 1985), commonly abbreviated as MSA. In an initial step the failure probabilities for all links that can be attacked is set equal as the spoiler has no knowledge which failure scenario would cause the most damage. After the initialisation in Step 0 in each iteration $n$ the lower problem (find optimal route flows) and upper problem (find optimal link failure probabilities) are solved until satisfactory convergence is achieved and neither $p$ nor $q$ changes significantly anymore. The MSA used in steps 4 and 8 updates $P$ and $q$ according to “knowledge” from previous
iterations and the new “experience” gained in the current iteration. The more iterations the more the previous knowledge will outweigh the new experience. Though a formal proof for the convergence of the MSA is missing, it has been used very widely and experience shows that the solutions are not far from the user equilibrium. In the transportation literature often gap measures between path costs found in different iterations are used to show that the MSA leads to a solution that fulfils Wardrop’s principle and hence user equilibrium conditions.

3.4 Solution algorithm—(base scenario)

**Step 0:** Initialise $q_j$ for all scenarios and $p_i$ for all links $q_j = (1/|F|)$; $p_i = 0$, set $n \leftarrow 1$

**Step 1:** Calculate expected link costs $sc_i$ for all links:

$$sc_i = \sum_j c_{ij} \cdot q_j$$

**Step 2:** Search for the least expected cost path $k$ in VISUM with expected link costs

**Step 3:** Obtain auxiliary link flow vector $x$ by setting $x_i = 1$ if link is on path $k$ and 0 otherwise

**Step 4:** Update the link-use probabilities $p$ using the MSA:

$$p_i \leftarrow \left(\frac{1}{n}\right) \cdot x_i + \left(1 - \frac{1}{n}\right) \cdot p_i$$

**Step 5:** Calculate expected losses for all failure scenarios $j$:

$$sc_j = \sum_i p_i \cdot c_{ij}$$

**Step 6:** Choose the scenario with the highest expected loss $sc_j$

**Step 7:** Obtain auxiliary vector $y$ by setting $y_j = 1$ if scenario $j$ gives the highest expected trip cost, 0 otherwise

**Step 8:** Update the failure scenario probabilities $q$ using the MSA:
Step 9: If convergence is satisfactory stop, otherwise set $n \leftarrow n+1$ and return to Step 1.

The extension of this approach to multiple O-D allowing for consideration of their various relative importance is discussed and applied in Kanturska (2006).

3.5 Results

The following paragraphs present an application of the game to finding the critical routes between Greenwich Park and Victoria Park. Figure 9-2 shows the location of three river crossings and the shortest path for this O-D pair obtained in free-flow conditions (green) together with the critical link (pink) in case of single path routing. A low disruption cost factor ($DC = 2$) was chosen in this example meaning that an incident would cause the link costs to double. Given such a disruption, the total cost of travelling this route would be 847 units, as indicated in Figure 9-2.
In contrast, Figure 9-3 show the results obtained after 1000 iterations which is more than sufficient to reach the equilibrium (note: one might also set an appropriate stopping criteria in particular in large-scale applications to reduce the computational effort). In this case the security considers not only the direct route but also allows for the option of re-routing the VIPs via a nearby Rotherhithe Tunnel. This route would be taken with a probability of 46%, whereas the route including the tunnel would be used in 54% of cases as indicated in Figure 9-3. The opportunity for re-routing leads to a decrease in the solution cost to 825 units.

The scenario shown in Figure 9-3 might correspond to the case where one takes into account only the possibility of minor disruption (e.g., a demonstration that might hold up the VIPs) whereas the scenario with a very high disruption cost might be used to plan for the scenario where the risk of a life-threatening attack is anticipated.

Figure 9-4 shows the equilibrium solution in the case of $DC=1,000,000$. Such a high value was chosen in order to demonstrate that the solution obtained depends on the severity of the attack. In the scenario with a high disruption cost in addition to the two routes shown in Figure 9-3 a third route

---

![Figure 9-3. Equilibrium solution (low disruption cost).](image)
is added via Tower Bridge, resulting in an even longer detour. This route is preferred ($h_k = 62\%$) for two reasons. Firstly, the cost of disruption, being proportional to link travel time, is lower for shorter links, hence the shorter river crossing will be favoured. Secondly, the longer travel time with the detour via Tower Bridge is still relatively low compared to the disruption cost.

The above analysis shows that anticipating heavily disruptive incidents the VIP security units should consider a wider spread of routes. Additional analysis with different $DC$ values showed that for $DC < 2$ multiple paths do not need to be considered, as the potential benefit from rerouting does not cover the inconvenience of using other paths than the shortest one.

Table 9-1 below summarises the results obtained in each case and illustrates that the optimal routing strategy is a cost-effective measure to distribute the risk.

The following Figures 9-5 and 9-6 show the convergence of the MSA for the solution cost and for the link-use probabilities of the three river crossings (colours of the lines correspond to the colours of the numbers placed next to each river-crossing in Figure 9-4). Although the solution cost converges rapidly and is unique at the solution, this may result from multiple equilibria of link use and link failure probabilities. Given the size and the non-symmetric structure of the network the existence of several equilibria is however unlikely.
Table 9-1. Solution cost in the considered scenarios

<table>
<thead>
<tr>
<th>Total Cost</th>
<th>Minor Disruption DC=2</th>
<th>Major Disruption DC=1,000,000</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Does not happen</td>
<td>Does happen</td>
</tr>
<tr>
<td>Single route</td>
<td>727</td>
<td>847</td>
</tr>
<tr>
<td>Optimal routes</td>
<td>753</td>
<td>825</td>
</tr>
<tr>
<td>INVESTMENT 26 BENEFIT 22</td>
<td>INVESTMENT 375 BENEFIT 96 x 10^6</td>
<td></td>
</tr>
</tbody>
</table>

Figure 9-5. Convergence of link use probabilities.

3.6 The DAD approach applied to the VIP transport problem

3.6.1 Introduction

The solutions presented in the previous section identified links critical to network performance. As discussed in the introduction this triggers a search for an optimal or near-optimal defence plan. Below the extension of the base model into DAD models is presented, where a third party—a defender—is introduced. Three versions are discussed distinguishing the visibility of the defence. In each case a defence strategy against a major attack is examined, corresponding to the high disruption factor $DC$ in the base scenario. Let $B$ be defined as the benefit achieved from the protective measure, i.e.
9. Improving Reliability through Multi-Path Routing and Link Defence

Figure 9-6. Convergence of the solution cost TC.

\[ B = TC_d - TC_0 \]  \hspace{1cm} (6)

where \( TC_d \) denotes the travel cost with and \( TC_0 \) the travel cost without defensive measure.

### 3.6.2 Scenario 1: “Visible Defence”

**FORMULATION**

In this scenario it is assumed that it is publicly known which links are protected (e.g., police on the route is obvious) is discussed. The task of the defender is to choose a link for protection so that the lowest possible solution cost of the game played between a router and a spoiler is achieved.

Let ‘link protection’ be defined as the unfeasibility of an attack on such a link being successful. This is expressed by extending cost matrix \( C[c_{ij}] \) into a three-dimensional matrix \( C[c_{ijs}] \) where \( s \) identifies the protected link. Under the assumption that all links \( j \) that can be attacked can also be protected this leads to:

\[
c_{ijs} = \begin{cases} 
  tt_i & \text{if } i \neq j \text{ and } i = j = s \\
  DC \cdot tt_i & \text{if } i = j \neq s 
\end{cases} \hspace{1cm} (7)
\]
where $s$ identifies a single protected link. The assumption of Equation (6) is that the cost of a link under attack is not increased by disruption cost $DC$ as long as this link is protected ($j = s$). The game now consists of finding the minimal solution cost $TC$ among all games where one link $s$ is protected.

$$\min_s [TC(q, p, s)] = \min_s [\max_p \min_q \sum_i \sum_{j \neq s} p_i c_{ij} q_j]$$

subject to $\sum_j q_j = 1$ and $\sum_k h_k = 1$ with $q_j \geq 0 \forall j$; $h_k \geq 0 \forall k$

The solution approach consists of a simple enumerative technique: One by one different protection scenarios $s$ are checked and the one with the lowest solution cost is chosen. Therefore the defender appears to be an external observer of this game, choosing one link for protection at a time, and consecutively, one after another examines the outcome of the game.

For the problem of simultaneous attack on multiple links and the protection of an optimal set of links, the above approach would have to be reformulated. In such case link defence should be expressed using a vector $s$ containing binary elements, which would indicate whether a given link is protected or not.

**SOLUTION ALGORITHM—SCENARIO “VISIBLE PROTECTION”**

**Step 0:** Form a set $F$ of candidate links for attack and protection. Select a link $s \in F$ for protection.

**Step 1:** Solve ”Base Scenario” algorithm using link cost (7) instead of (1)

**Step 2:** Save solution cost $TC(s)$

**Step 3:** Change $s$ and return to Step 1 until all protection scenarios are checked

**Step 4:** Set $TC^{opt} = \min_s TC(s)$

**APPLICATION**

The choice of the link for protection takes place before the game starts, so the defence is visible to the spoiler. As a result the spoiler chooses different attack target. It means that the attack can not be avoided, but only shifted to another link. The interaction between traveller and defender is indirect: they both learn about each other only by observing the choices
made by the spoiler. The defender chooses a link for protection based purely on link failure probabilities, not on link-use probabilities, while the traveller is completely unaware of the existence of any protective measures at the start of the game, because the defence as such does not influence the route choice.

Although this method can be applied to find an optimal set of links for protection, the analysis was limited to a predefined set of candidate links and the protection of one link only. The enumerative character of the method increases the computational effort significantly in case of large networks, as the number of possible links increases linearly with network size. Further the combinations of protected links increase exponentially with the number of links to be protected. The results presented below refer to an analysis limited to the choice of one link from a subset of 23 links. Only these 23 links were considered as they were attacked by the spoiler in the base case without protection. It is reasonable to assume that protection of any other link than contained in this set would not lead to a lower solution cost. Therefore 23 games were played one by one and for each case the solution cost was obtained. Figure 9-7 below shows the location of these links in the network together with indication of the Solution Cost obtained when a given link was protected.

*Figure 9-7. Location of candidate links for protection (corresponding to links attacked in Base Scenario).*
If the re-routing is the only risk-averse behaviour allowed, as in the base scenario, the solution cost \( TC = 24,130,840 \) units. The results in Table 9-2 below show that the benefit from active protection can lower the solution cost to 16,962,456 units, a result obtained when Tower Bridge is protected. This corresponds to 37% decrease of the solution cost compared to the game without protection. Figure 9-6 and Table 9-2 show that as long as only one link is attacked and one link can be protected, it proves most beneficial to protect one of the river-crossings.

Table 9-2. Solution cost in ascending order obtained for various protection scenarios.

<table>
<thead>
<tr>
<th>Link chosen for protection</th>
<th>Solution Cost ( TC )</th>
<th>Link use prob. ( p_i )</th>
<th>Link failure prob. ( q_i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tower Bridge</td>
<td>17.0 ( \times 10^6 )</td>
<td>0.62</td>
<td>0.55</td>
</tr>
<tr>
<td>Rotherhithee Tunnel</td>
<td>17.1 ( \times 10^6 )</td>
<td>0.18</td>
<td>0.17</td>
</tr>
<tr>
<td>Blackwall Tunnel</td>
<td>17.8 ( \times 10^6 )</td>
<td>0.21</td>
<td>0.20</td>
</tr>
<tr>
<td></td>
<td>21.5 ( \times 10^6 )</td>
<td>0.41</td>
<td>0.01</td>
</tr>
<tr>
<td></td>
<td>21.5 ( \times 10^6 )</td>
<td>0.41</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>22.3 ( \times 10^6 )</td>
<td>0.67</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>22.3 ( \times 10^6 )</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td><strong>Links close to origin and destination</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

3.6.3 **Scenario 2 “Invisible Defence”**

**Formulation**

This scenario presents a situation in which neither traveller nor spoiler expects the existence of protective measures. Therefore both of them behave as if no protection was present, i.e. identically to the base scenario. Only when the solution is known, the defender makes a choice which link to protect. The candidate links are, obviously, those which became the spoiler targets \( (q_j > 0) \) at game solution.

As in the all scenarios the criterion used by the defender for the choice of which link to protect is the potential benefit \( B_s \) from protection. In this scenario the benefit through protection of link \( s \) can be directly estimated from the base scenario with \(9\)

\[
B_s = p_s \cdot DC \cdot tt_s \cdot q_s + p_s \cdot tt_s (1-q_s) - p_s \cdot tt_s = p_s \cdot q_s \cdot tt_s (DC-1)
\]

(9)

Hence, the optimisation can be specified as follows:

\[
\min_s [TC_0[p,q] - p_s q_s (c^+_s - c_s)]
\]

(10)
subject to $\sum_j q_j = 1$ and $\sum_k h_k = 1$ with $q_j \geq 0 \forall j; h_k \geq 0 \forall k$.

**SOLUTION ALGORITHM—SCENARIO: “INVISIBLE PROTECTION”**

**Step 0:** Solve base scenario algorithm

**Step 1:** Form a set of candidate links for protection of those which were attacked at the solution obtained in Step 0. Select a link $s$ for protection.

**Step 2:** Calculate potential benefit $B_s$ from protecting link $s$ with (9)

**Step 3:** Change $s$ and return to Step 1 until all protection scenarios are checked

**Step 4:** Set $TC^{opt} = \min TC^{new}(s)$

**APPLICATION**

The application to the VIP transport problem shows that maximum benefit from link protection ($B = 14,014,578$ units, which amounts to 58% of the solution cost in the base scenario) is achieved when the bridge most distant from the shortest path (Tower Bridge) is defended (see Figure 9-8).

The new total cost is significantly lower than the cost achieved in the scenario “visible defence”, although the protected link is exactly the same as before. It can be concluded that invisibility of the protective measures creates an additional payback. This is because the spoiler is not only unaware of the location of the protection, but also takes not into account that the attack might fail. Such a situation can be considered an “unexpected defence” and therefore is plausible in relatively rare instances, e.g. when protective measures are concealed from the spoiler and the traveller, and are installed ad hoc. In most cases however, one would expect some security measures. This leads to a scenario discussed in the subsequent section.

### 3.6.4 Scenario 3—“Anticipated Defence”

**FORMULATION**

In this scenario it is assumed that the traveller as well as the spoiler are aware of the existence of some protective measures and anticipate that one link will be protected. However, they do not posses any knowledge regarding the defence strategy, so they do not know which link will be
protected. This uncertainty leads to a different representation of defence than it was in the two previous scenarios. In this case we introduce link defence probabilities:

\[ \mathbf{d}: \text{ is a vector of link defence (protection) probabilities} \]

Throughout the game the traveller and the spoiler accumulate knowledge about each others choices and about the choices of the defender and adjust their own strategy accordingly. Furthermore, the defender is well aware that the traveller and the spoiler will react to his strategy. Hence this problem is a three-person game.

As in previous scenarios it is assumed that the defender protects only one link and similarly to (7) it is assumed that the increase in link costs will only occur if a link is attacked and not defended. In this case however we do not apply enumerative solution procedure, so the third dimension of the cost matrix, which arises from the existence of defence, has been represented by expressing the increase in link cost as a function of \( d_i \):

\[
c_{ij}(d_i) = \begin{cases} 
  tt_i & i \neq j \\
  tt_i + (DC \cdot tt_i - tt_i)(1 - d_i) = tt \cdot d_i + DC \cdot tt_i(1 - d_i) & i = j 
\end{cases} \tag{11}
\]
9. Improving Reliability through Multi-Path Routing and Link Defence

It should be noted that \( d \) is a vector of probabilities, as distinct from \( s \) in Scenario 1 where the elements are binary. With this notation the three-person game representing the full DAD optimization problem can be described as:

\[
\min_d \max_q \min_p \; TC(p, q, d) = \sum_{i,j} p_i \cdot c_{ij} (d_i) \cdot q_j
\]

subject to \( \sum_j q_j = 1; \sum_k h_k = 1 \) and \( \sum_s d_s = 1 \) with \( q_j \geq 0 \forall j; h_k \geq 0 \forall k \) and \( d_s \geq 0 \forall s \).

Relaxing the constraint on \( d \) to allow for multiple link failures (all with defence probabilities between 0 and 1) is possible and would not change the problem described in Eq. 12. It would however require some more complex criteria in Step 10 of the solution algorithm presented below to choose the links to be defended. Simply choosing the two or \( n \) links with the highest expected link benefits would ignore that other combinations might be more effective in ensuring a safe path for the traveller. Similarly, relaxing the constraint on \( q \) is possible, but leads to complex searches of the optimum link cut sets that would divide the network and make it impossible for the traveller to reach his destination without using an attacked link.

**Solution Algorithm—Scenario “Anticipated Protection”**

**Step 0:** Initialise \( q_j \) for all failure scenarios, \( d_s \) for all protection scenarios and \( p_i \) for all links: \( q_j = (1/|F|); \; d_s = (1/L) \); \( p_i = 0 \), set \( n \leftarrow 1 \)

**Step 1:** Calculate expected link costs for all links: \( sc_i = \sum_j c_{ij} \cdot q_j \)

**Step 2:** Search for the least expected cost path in VISUM

**Step 3:** Obtain auxiliary link flows vector \( x \) by setting the \( x_i = 1 \) if link lies on the path, 0 otherwise

**Step 4:** Update the link-use probabilities \( p_i \) using the MSA:

\[
p_i \leftarrow \left( \frac{1}{n} \right) \cdot x_i + \left( 1 - \frac{1}{n} \right) \cdot p_i
\]

**Step 5:** Calculate expected losses for all failure scenarios:
\[ sc_j = \sum_i p_i \cdot c_{ij} \]

**Step 6:** Choose the scenario with the highest expected loss \( sc_j \)

**Step 7:** Obtain auxiliary link failure vector \( y \) by setting the \( y_j = 1 \) if scenario \( j \) gives the highest expected trip cost, 0 otherwise

**Step 8:** Update the failure scenario probabilities \( q_j \) using the MSA:

\[ q_j \leftarrow \left( \frac{1}{n} \right) \cdot y_j + \left( 1 - \frac{1}{n} \right) \cdot q_j \]

**Step 9:** Calculate expected costs for each link: \( TC_s = \sum_j p_s \cdot c_{sj}(d_s) \cdot q_j \)

**Step 10:** Choose the defence scenario: Protect link with the highest expected trip cost \( TC_s \)

**Step 11:** Obtain auxiliary link protection vector \( z \) by setting \( z_s = 1 \) if link \( s \) has the highest expected trip cost, 0 otherwise

**Step 12** Update the defence probabilities \( d_s \) using the MSA:

\[ d_s \leftarrow \left( \frac{1}{n} \right) \cdot z_s + \left( 1 - \frac{1}{n} \right) \cdot d_s \]

**Step 13:** Update the cost matrix \( C \) with new \( d \)

**Step 14:** If convergence is satisfactory stop, otherwise set \( n \leftarrow n+1 \) and return to **Step 1**.

**APPLICATION**

The solution cost in this case is 15,131,901 units. This is a benefit of 8,998,939 units compared to the version without protection, which equates to 30% of the initial solution cost. As illustrated on Figure 9-9, the highest probability of defence is observed on Tower Bridge (\( d=0.48 \)). Other links with high defence probabilities are those in the proximity of origin and destination.

Figures below show the convergence of link use probability (green line), link defence probability (red line) and link failure probability (blue line) for Tower Bridge (Figure 9-10) and Rotherhithe Tunnel (Figure 9-11).
9. Improving Reliability through Multi-Path Routing and Link Defence

Figure 9-9. Optimal protection probabilities for DAD model.

Figure 9-10. Convergence of $p$, $q$ and $d$ for Tower Bridge.
3.7 Comparison

The solution costs and benefits from introducing active protective measures in each model are compiled in Table 9-3 below. Clearly, the invisible defence yields the highest benefits, which highlights the importance of concealing information about any planned security measures. Interestingly, in the considered example of highly malevolent attack the visible measures seem to be nearly as efficient as those not obvious, but anticipated.

Table 9-3. Solution cost obtained in particular models.

<table>
<thead>
<tr>
<th></th>
<th>Base Scenario</th>
<th>Visible Defence</th>
<th>Invisible Defence</th>
<th>Anticipated Defence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution Cost</td>
<td>24,130,840</td>
<td>16,962,456</td>
<td>10,116,262</td>
<td>15,131,901</td>
</tr>
<tr>
<td>Benefit n/a</td>
<td>n/a</td>
<td>7,168,384</td>
<td>14,014,578</td>
<td>8,998,939</td>
</tr>
<tr>
<td>% of the Solution Cost</td>
<td>n/a</td>
<td>30%</td>
<td>58%</td>
<td>37%</td>
</tr>
</tbody>
</table>

4. CONCLUSIONS

Since the probabilities of attacks on transport links are in most cases unknown, game theory has proved to be a useful tool to analyse network reliability. In this study the game has been played between a single traveller
and a spoiler who has the possibility to attack exactly one link. The method can be applied to examine multiple O-D pairs at the same time, as well as to model the impact of protecting a chosen asset from an attack. The results showed that as long as travel costs are small in relation to the losses arising from a disruption a mix of routes resulting from the minimax approach should be used as a rational measure to distribute the risk.

As an example the problem of transporting VIPs across London is used. A terrorist attack could cause considerable chaos and fear, not to mention costs of destroyed assets, costs of delays, let alone lost lives. Although many security measures are commonly applied to protect VIPs while transported, the chapter suggests that such measures could be easily supported by a multi-path routing strategy.

The approach was then extended to find the optimal set of infrastructure to be protected and hence to extend the game-theoretic approach into a Defender-Attacker-Defender model. Following the work of Brown (2005) three protection scenarios are considered, different in terms of the visibility of protection measures from the viewpoint of a traveller and an attacker: firstly evident protection, secondly invisible protection and thirdly protection that is unspecified, but anticipated. The latter case represents a three-player game, whereas in the former two cases simple enumeration techniques can be used.

The comparison of the results obtained using different approaches applied to the VIP transport problem show that the expected travel cost can be significantly reduced, even if the resources allow for the protection of one link only. Furthermore, the expected cost is lowest if the protection is not visible. The scenario where the defence is only anticipated but the exact location is unknown leads to lower expected costs compared to the scenario with visible defence, as one would also expect.

All the methods explored in this chapter looked at scenarios in which only one link is attacked and one link can be defended at a time. Further work should investigate the case with multiple links being attacked and/or defended. Another aspect worth examining is the application of deceptive strategies that could reflect situations in which players have different levels of knowledge.

ACKNOWLEDGEMENTS

We would like to thank PTV Karlsruhe for providing us with high quality data and Mr Pieter De Beule from Imperial College London for his comments and advice on an earlier version of this chapter.
REFERENCES


Berdica, K., 2002, An introduction to road vulnerability: what has been done, is done and should be done, *Transport Policy* **9**:117–127.


9. Improving Reliability through Multi-Path Routing and Link Defence


Osborne, M. J., 2003, *An Introduction to Game Theory*. Oxford University Press, USA.

Pan, F., 2005, Stochastic Network Interdiction: Models and Methods, PhD dissertation, University of Texas at Austin, USA.


This page intentionally left blank
INDEX

Abhichandani, V., 18, 22, 29, 62, 91, 172
AD model. See Attacker–defender model
Add-drop multiplexers, 176, 179, 181
ADM. See Add-drop multiplexers
Agarwal, S., 63
Aggregation error, Bayesian model, 99–102
Al-Qaeda, 24–27
	objectives of, 26
Albert, R., 187, 196, 202, 226
Allais, M., 22, 29
Altman, E., 203, 226
Anderson, P., 63
Anderson, R., 67, 90
Angeloudis, P., 200, 202, 226
Anticipated defense scenario, VIP transport
vulnerability, 219–224
Anude, O., 63
Apostolakis, G., 28–29, 31, 62, 64, 172
APS. See Automated protection switching
Argyrakis, P., 189, 197
Arnold, B.F., 120
ARPANET, 185–186
Atamturk, A., 183–184, 197
Attacker-defender model, 10, 180–182,
199–200, 202–203, 206–208, 214,
223, 225
Aultmann-Hall, L., 201–202, 227
Aumann, R.J., 25, 29
Automated protection switching, 177
Azaiez, M.N., 1–12, 19–22, 29, 90, 97–122
Babayev, D., 5, 10
Bai, D., 62
Bandwidth requirements, 177–178
Barabási, A.-L., 187, 196, 202, 226
Barbacci, M., 62
Bargaining games, 3
Bayesian influence diagrams, 15
Bayesian learning process, 20
Bayesian model, 97–122
aggregation error, 99–102
combined series-parallel systems, 114–118
examples, 110–114, 117–119
intermediate levels of information, 119
neutral attacker, 106–107
notations, 104–107
optimistic attacker, 106
parallel system, arbitrary size, 107–112
parallel systems, 114–118
perfect aggregation, 99–102
results on, 100–101
pessimistic attacker, 106
problem formulation, 104–107
problems, 103–118
propositions, 102, 105–109
series/parallel systems, 114–118
series system, arbitrary size, 112–114
theorems, 100–101
Bayesian updating, 25, 97–122, 165
Bell, M.G.H., 199–227
Bell approach, 204–205
Ben-Akiva, M.E., 204, 226
Berdica, K., 201, 226
Bertsimas, D., 10
Bier, V.M., 1–12, 18–22, 29, 31, 62, 65–98,
100–101, 107, 120–121, 172
Birghtwell, G., 196
Birnbaum, L.. 1989, 37, 62
Birner, R., 4, 11
Bleukx, A., 201, 226
Blue searcher strategy, 137–145
Blume, L., 22, 29–30
Borwn, G., 10
Brandenburger, A., 22, 29–30
Brightwell, G., 184, 186
Brown, G., 6–8, 176, 202–203, 225–226
Bunde, A., 189, 197
Byman, D.L., 26, 30

Camerer, C., 23, 30
Carlye, M., 6–8, 176, 202–203, 226
Carlyle, M., 10
Case of Irish Republican Army, 171
Cassir, C., 200, 204, 226
Cauley, J., 14, 31
Chae, K., 62
Chekuri, C., 196
Chen, H.C., 23, 30
Chen, O.J., 204, 226
Chen, T., 63
Choi, H., 185, 196
Chung, S., 62
Church, R.L., 203, 226
Circuit-switched networks, networks with, 182–186

CKR. See Common knowledge of rationality
Clark, G., 62

Classical critiques, game theory, 21–27
Clausewitz, C.V., 67, 91
Clement, M., 187, 197, 201
Cohen, M.J., 4, 11
Cohen, R., 189, 197
Coit, D., 63
Colony, D.C., 204, 226

Combined series-parallel systems, Bayesian model, 114–118

Common knowledge of rationality, 21, 24–26
Complex multi-state systems, 33–64
defense strategy optimization, 41–44
multiple attacks, 43–44
single attack, 42–43
destruction probability of protection group, incorporation of, 46–47
equations, 49–60
future research, 60–62
imperfect attacker knowledge about system, attack probability proportional to ED, single attack with, 53
model, 37–40

no attacker knowledge about system, single attack with, 50–52
optimal defense strategy, influence of FT's on, 58–60
optimal separation, protection strategy, 54–58
optimization technique, 48–49
perfect attacker knowledge about system, single attack with, 52–53
protection importance evaluation, 49–54
system performance, evaluating PMF, 45–47
universal generating function technique, 45–46
unlimited attacker resources, multiple attacks with, 53–54

Component, defined, 34

Computer Science and Telecommunications Board, 4, 10

Conditional risk, 5

Conditional risk matrix, 5

Contest success functions, 65–98

Cooper, H.A., 30
Cormican, K.J., 202, 226

Counter-insurgency

government leader's decision problem, 165–168
alternatives, 166–167
information, 167
objectives, 167–168
insurgent leader's decision problem, 164–165
alternatives, 165
information, 165
objectives, 165
integration, insurgent, government models, 168–169
repeated game, 163–171
risk analysis applications, 169–171
government leader utility, 170
insurgent leader utility, 170


Cox, L.A., 1–12, 175–198
Cox, S., 187, 197
Craig, J.I., 197

Crenshaw, M., 23, 30
Crucitti, P., 187–188, 197

Dacomo, A., 197

DAD model. See Defender-attacker-defender model
Dai, Y., 63
De Patre, S., 197
Deccio, C.T., 187, 197
Dedicated routes, networks with, 182–186
Defender-attacker-defender model, 199–200, 203, 214–225
Definitions:, 34
Dekel, E., 22, 30
Denardo, E.V., 10
Deng, H.Z., 189, 197
Destinations, 177–178
Destruction probability of protection group incorporation, complex multi-state systems, 46–47
Dhillon, B., 63
Dighe, N.S., 98, 121
Disincentives to invest in protection, 190
Duenas, O.L., 197
Element, defined, 34
Ellsberg, D., 22, 30
Elster, J., 22, 30
Enders, W., 14–15, 30–31
Escalation games, 3
Falck-Zepeda, J., 4, 11
False target, defined, 34
False targets, 33–64
Faria, J.R., 30
Fisk, C., 204, 226
Fisk, D., 200, 202, 226
Flaxman, A.D., 189, 197
Fonzone, A., 199–227
Fortz, B., 183
Free riding, 175–198
Frey, B.S., 14, 30
Friedman, J.W., 23, 30
Frieze, A.M., 189, 197
Fudenberg, D.M., 70, 91
Future research, complex multi-state systems, 60–62
Gallos, L.K., 189, 197
Garber, R., 148, 151–157, 172
Garrick, J.B., 30
Gaskell, J., 4, 11
Gaver, D.P., 126–146
Gendreau, M., 183
Genetic algorithms, 33–64
Gibbons, R., 148, 172
Glazebrook, K.D., 126–146
Glover, F., 183–184, 197
Golany, B., 1–2, 11
Goodno, B.J., 197
Government leader's decision problem, 165–168
alternatives, 166–167
information, 167
objectives, 167–168
Grossi, I., 120
Guikema, S., 157–163
Guo, F., 201–202, 227
Gupta, A., 196
Haim, H.B., 63
Han, S.K., 197
Harasanyi, J.C., 24, 148, 172
Hart, S., 25, 29
Hausken, K., 16–18, 30, 65–98, 172
Hausken model, 16
Havlin, S., 189, 197
Heal, G., 68, 91
Heap, S.P.H., 22, 24, 30
Henley, E.J., 148, 172
Heydecker, B.G., 204, 227
Hirshleifer, J., 69, 91
Ho, T.H., 23, 30
Holland, Y., 204, 226
Hollis, M., 22, 30
Holme, P., 197
Hong, Y., 172
Huber, W., 5, 10
Husdal, J., 202, 226
Iida, Y., 199–200, 227
ILP. See Integer linear programming
Immers, B., 201, 226
Imperfect attacker knowledge about system, attack probability proportional to ED, single attack with, 53
Indusi, J.P., 4, 11
Infanger, G., 11
Infrastructure defense, 1–12
bargaining games, 3
conditional risk, 5
conditional risk matrix, 5
escalation games, 3
game-theoretic applications, basic formula, 4
iterated prisoner's dilemma, 3
limitations of risk, 6–7
limited predictive power, 3
non-game-theoretic models, defensive resource allocation, 1–8
problems with game-theoretic models, 3
reliability theory, 1–12
bargaining games, 3
conditional risk, 5
conditional risk matrix, 5
escalation games, 3
game-theoretic applications, basic formula, 4
iterated prisoner's dilemma, 3
limitations of risk, 6–7
limited predictive power, 3
non-game-theoretic models, defensive resource allocation, 1–8
problems with game-theoretic models, 3
Risk Analysis and Management for Critical Asset Protection, 4–5, 11
definition of risk, 4
risk and reliability analysis, weaknesses without game theory, 4–6
Stackelberg game, in economics, 3
threat, concept of, 6–7
ultimatum games, 3
vulnerability, concept of, 6–7
risk, reliability analysis, weaknesses without game theory, 4–6
Risk Analysis and Management for Critical Asset Protection, 4–5, 11
definition of risk, 4
Stackelberg game, in economics, 3
threat, concept of, 6–7
ultimatum games, 3
vulnerability, concept of, 6–7
Instrumental rationality, assumption of, 21–24
Insurgent leader's decision problem, 164–165
alternatives, 165
information, 165
objectives, 165
Integer linear programming, 184
Integration, insurgent, government models, 168–169
Intelligent actor models, reliability analysis, 13–32
classical critiques of game theory, 21–27
common knowledge of rationality, 21, 24–26
Hausken model, 16
instrumental rationality, assumption of, 21–24
knowledge of rules of game, 26–27
model parameters, uncertainty about, 27
multi-agent influence diagrams, 18
Nash equilibriums, 16, 125, 138, 192–193, 203
non-game theoretic methods, 27–28
reliability analysis, 15–21
subjective expected utility, 21–22
terrorist-defender interactions, modeling, 14–15
Interactions between games, risk, 147–150
Intermediate levels of information, Bayesian model, 119
Invisible defense scenario, VIP transport vulnerability, 218–219
Israeli, E., 226
Iterated prisoner's dilemma, 3
Jacobs, P.A., 126–146
Jenelius, E., 201, 226
Jeong, H., 187, 196, 202, 226
Juergensmeyer, M., 26, 30
Kadane, J.B., 23, 30
Kahneman, D., 22, 30
Kanturska, U., 199–227
Kaplan, A., 23, 30
Kaplan, E., 1–2, 11
Kardes, E., 21–22, 30
Kim, B., 197
Knowledge of rules of game, 26–27
Koller, D., 18, 30
Komen, J., 4, 11
Koo, B., 4, 11
Korczak, E., 63
Kott, A., 146
Kress, M., 126, 146
Kucik, P.D., 149, 163–172
Kulturel-Konak, S., 63
Kumamoto, H., 148, 172
Kumar, A., 196
Kunreuther, H., 68, 91
Labbe, M., 183
Laguna, M., 183–184, 197
Lai, Y.-C., 188–190, 197
Lambertini, L., 15, 31
Larkey, P.D., 23, 30
Latora, V., 187–188, 197
Leader, S.H., 30
Lee, S., 204, 227
Leitmann, G., 15, 31
Lemon, D.M., 28–29
Levinson, D., 202, 227
Levitin, G., 33–64, 98, 121
Liang, Y., 63
Lim, C., 203, 227
Lim, Y., 204, 227
Linacre, N.A., 4, 11
Link defense, transport, 199–227
Bell approach, 204–205
defender-attacker-defender model, 199–200, 203, 214, 223, 225
literature review, 201–205
non cooperative games, 204
reliability under attack, 201–203
VIP transport vulnerability, 206–224
  (See also VIP transport vulnerability)
Wardrop's principle, 203, 210
zero-degree models, 202
zero-sum games, 17, 28, 204

Lisnianski, A., 62–63
Louis A., 1–12
Luce, R.D., 150, 157, 172
Luechinger, S., 14, 30

MAIDS. See Multi-agent influence diagrams
Maier, G., 183–184, 197
Major, J.A., 17–18, 28, 31
Mamur, A., 1–2, 11
March, J.G., 31
Marchiori, M., 187–188, 197
Maritime domains, 126–146
Marseguerra, M., 63
Martinelli, M., 197
Mattsson, L.-G., 201, 226
McDonald, J.C., 30
McEneaney, W.M., eds., 146
Menger's theorem, graph theory, 185
Michaud, D., 28, 31
Milch, B., 18, 30
Milgrom, P.R., 148, 172
MIPs. See Mixed integer programs
Mixed integer programs, 184
Model parameters, uncertainty about, 27
Monderer, D., 203, 227
Morgenstern, O., 173
Morton, D.P., 202, 226
Msangi, S., 4, 11
Multi-agent influence diagrams, 18
Multi-path routing, transport, 199–227
Bell approach, 204–205
defender-attacker-defender model, 199–200, 203, 214, 223, 225
literature review, 201–205
non cooperative games, 204
reliability under attack, 201–203
VIP transport vulnerability, 206–224
  (See also VIP transport vulnerability)
Wardrop's principle, 203, 210
zero-degree models, 202
zero-sum games, 17, 28, 204

MSAN LATA Network, 185–186
Non cooperative games, 204
Non-game theoretic methods, 27–28
Non-game-theoretic models, defensive resource allocation, 1–8
Novak, D.C., 201–202, 227

Oliveros, S., 66, 91
Optical cross-connect switches, 176
Optimal separation, complex multi-state system protection strategy, 54–58
Orlodo, G., 184, 186, 196
Osborne, M.J., 23, 31, 203, 227
O'Toole, T., 30
OXCs. See Optical cross-connect switches
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Padovani, E., 63</td>
</tr>
<tr>
<td>Page, L., 62</td>
</tr>
<tr>
<td>Pan, F., 202, 227</td>
</tr>
<tr>
<td>Parallel systems</td>
</tr>
<tr>
<td>arbitrary size, Bayesian model, 107–112</td>
</tr>
<tr>
<td>Bayesian model, 114–118</td>
</tr>
<tr>
<td>Parameter variation, sensitivity analysis with, natural disasters, 85–89</td>
</tr>
<tr>
<td>Park, K., 188–190, 197</td>
</tr>
<tr>
<td>Parker, M., 183, 197</td>
</tr>
<tr>
<td>Pattavina, A., 183–184, 197</td>
</tr>
<tr>
<td>Patterson, S., 64</td>
</tr>
<tr>
<td>Perfect aggregation, Bayesian model, 99–102</td>
</tr>
<tr>
<td>Perfect attacker knowledge about system, single attack with, 52–53</td>
</tr>
<tr>
<td>Performance rate, defined, 34</td>
</tr>
<tr>
<td>Perry, J., 62</td>
</tr>
<tr>
<td>Petersen, T., 201, 226</td>
</tr>
<tr>
<td>Poh, K.L., 63</td>
</tr>
<tr>
<td>Port security, 126–146</td>
</tr>
<tr>
<td>Post, J.M., 23, 31</td>
</tr>
<tr>
<td>PRA. See Probabilistic risk analysis</td>
</tr>
<tr>
<td>Prasheker, J.N., 204, 226</td>
</tr>
<tr>
<td>Principal-agent model, possible shortcuts, induced failure risks, 151–157</td>
</tr>
<tr>
<td>illustration, 154–157</td>
</tr>
<tr>
<td>Prisoner’s dilemma, 3, 175–198</td>
</tr>
<tr>
<td>Probabilistic risk analysis, 9, 15–17, 148, 152–153, 156–157</td>
</tr>
<tr>
<td>Problems with game-theoretic models, 3</td>
</tr>
<tr>
<td>Probst, P., 30</td>
</tr>
<tr>
<td>Protection, defined, 34</td>
</tr>
<tr>
<td>Protection group, defined, 34</td>
</tr>
<tr>
<td>Protection importance evaluation, 49–54</td>
</tr>
<tr>
<td>Protection switching, 177–180</td>
</tr>
<tr>
<td>Rabin, M., 23, 31</td>
</tr>
<tr>
<td>Rajan, D., 183–184, 197</td>
</tr>
<tr>
<td>RAMCAP. See Risk Analysis and Management for Critical Asset Protection</td>
</tr>
<tr>
<td>Rapisarda, A., 187–188, 197</td>
</tr>
<tr>
<td>Rasmussen, E., 70, 91</td>
</tr>
<tr>
<td>Rationality, 13–32</td>
</tr>
<tr>
<td>Ravi, V., 63</td>
</tr>
<tr>
<td>Raz, D., 196</td>
</tr>
<tr>
<td>Relative probabilities, different threats of terrorist attacks, game analysis approach to, 157–163</td>
</tr>
<tr>
<td>illustration, 161–163</td>
</tr>
<tr>
<td>model structure, 159–161</td>
</tr>
<tr>
<td>Religious terrorism. See Al-Qaeda</td>
</tr>
<tr>
<td>Resilient networks, 175–198</td>
</tr>
<tr>
<td>Resilient packet ring protection scheme, 180</td>
</tr>
<tr>
<td>Rindskopf, E., 30</td>
</tr>
<tr>
<td>Risk Analysis and Management for Critical Asset Protection, 4–5, 11</td>
</tr>
<tr>
<td>definition of risk, 4</td>
</tr>
<tr>
<td>Roberts, J., 148, 172</td>
</tr>
<tr>
<td>Rosegrant, M.W., 4, 11</td>
</tr>
<tr>
<td>Rosendorff, B.P., 14, 31</td>
</tr>
<tr>
<td>Rosenthal, R., 23, 30–31</td>
</tr>
<tr>
<td>Roth, A.E., ed., 197</td>
</tr>
<tr>
<td>Rothblum, U.G., 1–2, 10–11</td>
</tr>
<tr>
<td>Roysset, J.O., 202, 227</td>
</tr>
<tr>
<td>RPR protection scheme. See Resilient Packet Ring protection scheme</td>
</tr>
<tr>
<td>Rubinstein, A., 18, 23, 31, 157, 173</td>
</tr>
<tr>
<td>Ruby, C.L., 23, 26, 31</td>
</tr>
<tr>
<td>Ryan, J., 183, 197</td>
</tr>
<tr>
<td>Sageman, M., 24, 31</td>
</tr>
<tr>
<td>Salmeron, J., 10</td>
</tr>
<tr>
<td>Salmeron, J., 6–8, 176, 202–203, 226</td>
</tr>
<tr>
<td>SAM. See System, Actions, Management</td>
</tr>
<tr>
<td>Samuelson, L., 66, 91</td>
</tr>
<tr>
<td>Sandholm, W.H., 203, 227</td>
</tr>
<tr>
<td>Sandler, T., 14–15, 30–31</td>
</tr>
<tr>
<td>Sato, H., 126, 133, 146</td>
</tr>
<tr>
<td>Savage, L.J., 25, 31</td>
</tr>
<tr>
<td>Scale-free networks, 175–198</td>
</tr>
<tr>
<td>Scale-free packet networks, statistical risk models, results, 186–190</td>
</tr>
<tr>
<td>Scaparra, M.P., 203, 226</td>
</tr>
<tr>
<td>Schbley, A., 26, 31</td>
</tr>
<tr>
<td>Schmöcker, J.-D., 199–227</td>
</tr>
<tr>
<td>Scott, D.M., 201–202, 227</td>
</tr>
<tr>
<td>Scott, J.L., 14–15, 31</td>
</tr>
<tr>
<td>Seguin, R., 183</td>
</tr>
<tr>
<td>Self-healing synchronous optical network ring networks, 179–180</td>
</tr>
<tr>
<td>Separation, 33–64</td>
</tr>
<tr>
<td>defined, 34</td>
</tr>
<tr>
<td>Series system, arbitrary size, Bayesian model, 112–114</td>
</tr>
<tr>
<td>SEU. See Subjective expected utility</td>
</tr>
<tr>
<td>Shapley, L., 203, 227</td>
</tr>
<tr>
<td>Sheffi, Y., 209, 227</td>
</tr>
<tr>
<td>Shephard, F.B., 184, 186, 196</td>
</tr>
<tr>
<td>Shermer, M., 3, 11</td>
</tr>
<tr>
<td>Shor, M., 204, 227</td>
</tr>
<tr>
<td>Shortcuts, induced failure risks, principal-agent model, 151–157</td>
</tr>
</tbody>
</table>

Other abbreviations used: PRA, SEU, RPR.
Index

illustration, 154–157
Single attack, complex multi-state systems, 42–43
Single attack with no attacker knowledge about system, 50–52
Single link cut, designing networks to withstand, 183–185
Siqueira, K., 15, 31
Skaperdas, S., 69, 91
Smith, A., 63
Smith, J.C., 203, 227
Smith, M., 187, 197
Snell, Q., 187, 197
SONET ring networks. See Synchronous optical network ring networks
Soriano, P., 183
Stackelberg game, economics, 3
Stada, J., 201, 226
Stahlecker, P., 120
Stochastic models, 127–145
Subjective expected utility, 21–22
Subramaniam, S., 185, 196
Sudargho, F., 203, 227
Surivable networks, 175–198
Synchronous optical network ring networks, 179–180, 183, 185
System, Actions, Management, 148
Taale, H., 204, 227
Tan, Y.J., 189, 197
Telecommunications networks, 175–198
add-drop multiplexers, 176, 179, 181
ARPANET, 185–186
automated protection switching, 177
bandwidth requirements, 177–178
circuit-switched networks, networks with, 182–186
dedicated routes, networks with, 182–186
design of telecommunications networks, 176
destinations, 177–178
disincentives to invest in protection, 190
diverse routes, 177–180
integer linear programming, 184
Menger's theorem, graph theory, 185
mixed integer programs, 184
multiple levels of protection, 178–180
multiple link cuts, designing networks to withstand, 185–186
Nash equilibrium, 192–193
national network, 185–186
NJ LATA Network, 185–186
optical cross-connect switches, 176
origins, 177–178
protection switching, 177–180
resilient packet ring protection scheme, 180
restoration possibilities, evaluation of, 185–186
scale-free packet networks, statistical risk models, results, 186–190
self-healing synchronous optical network ring networks, 179–180
single link cut, designing networks to withstand, 183–185
synchronous optical network ring networks, 179–180, 183, 185
tipping point, 194–195
two-stage attacker-defender model, 180–182
unstable network collusion, 193–194
Yule-Simon power law distribution, 187
Terrorist-defender interactions, modeling, 14–15
Thisse, J.F., 23, 30
Thomas, L.C., 146
Threat, concept of, 6–7
Tipping points, 175–198
Tirole, J., 70, 91
Tornatore, M., 183, 197
Transport, multi-path routing, link defense, 199–227
Bell approach, 204–205
defender-attacker-defender model, 199–200, 203, 214, 223, 225
literature review, 201–205
non cooperative games, 204
reliability under attack, 201–203
VIP transport vulnerability, 206–224
(See also VIP transport vulnerability)
Wardrop's principle, 203, 210
zero-degree models, 202
zero-sum games, 17, 28, 204
Trivelpiece, A.W., 30
Tschrhart, J.T., 14, 31
Tullock, G., 69, 91
Tversky, A., 22, 30
Two-stage attacker-defender model, 180–182
Udwadia, F., 15, 31
Ultimatum games, 3
Index

Unit costs of attacks, 65–98
Unit costs of defenses, 65–98
Unlimited attacker resources, multiple attacks with, 53–54
Unstable network collusion, 193–194
Ushakov, I., 63
Van Arsdale, L.A., 30
Van der Heyden, L., 10
Van Zuyle, H.J., 204, 227
Varoufakis, Y., 22, 24, 30
Vaurio, J., 63
Vera, J., 189, 197
Vesely, W., 62
Villa, C., Hoffman, K., 183, 197
Von Stengel, B., 63
Vulnerability, concept of, 6–7

Wan, J., 187, 197
Wardrop, J.G., 203, 227
Wardrop's principle, 203, 210
Washburn, A., 202, 227
Weaknesses without game theory, risk, reliability analysis, 4–6
Whitley, D., 63
Wood, K., 10
Wu, C., 63
Wu, J., 189, 197
Wynants, C., 183
Wynter, L., 203, 226

Xie, M., 63, 201
Yoon, C.N., 197
You, P., 63
Yperman, I., 201, 226
Yule-Simon power law distribution, 187
Yun, W., 62
Zebroski, E.L., 30
Zero-degree models, 202
Zero-sum games, 17, 28, 204
Zhang, L., 202, 227
Zhao, L., 188–190, 197
Zhu, D.Z., 189, 197
Zhuang, J., 18–19, 22, 31, 65–98, 121
Zio, E., 63
Early Titles in the
INTERNATIONAL SERIES IN
OPERATIONS RESEARCH & MANAGEMENT SCIENCE
Frederick S. Hillier, Series Editor, Stanford University

Saigal/ A MODERN APPROACH TO LINEAR PROGRAMMING
Nagurney/ PROJECTED DYNAMICAL SYSTEMS & VARIATIONAL INEQUALITIES WITH APPLICATIONS
Padberg & Rijal/ LOCATION, SCHEDULING, DESIGN AND INTEGER PROGRAMMING
Vanderbei/ LINEAR PROGRAMMING
Jaiswal/ MILITARY OPERATIONS RESEARCH
Gal & Greenberg/ ADVANCES IN SENSITIVITY ANALYSIS & PARAMETRIC PROGRAMMING
Prabhu/ FOUNDATIONS OF QUEUEING THEORY
Fang, Rajasekera & Tsao/ ENTROPY OPTIMIZATION & MATHEMATICAL PROGRAMMING
Yu/ OR IN THE AIRLINE INDUSTRY
Ho & Tang/ PRODUCT VARIETY MANAGEMENT
El-Taha & Stidham/ SAMPLE-PATH ANALYSIS OF QUEUEING SYSTEMS
Miettinen/ NONLINEAR MULTIOBJECTIVE OPTIMIZATION
Chao & Huntington/ DESIGNING COMPETITIVE ELECTRICITY MARKETS
Weglarz/ PROJECT SCHEDULING: RECENT TRENDS & RESULTS
Sahin & Polatoglu/ QUALITY, WARRANTY AND PREVENTIVE MAINTENANCE
Tavares/ ADVANCED MODELS FOR PROJECT MANAGEMENT
Taylor, Ganeshan & Magazine/ QUANTITATIVE MODELS FOR SUPPLY CHAIN MANAGEMENT
Weyant, J./ ENERGY AND ENVIRONMENTAL POLICY MODELING
Shanthikumar, J.G. & Sumita, U./ APPLIED PROBABILITY AND STOCHASTIC PROCESSES
Liu, B. & Esogbue, A.O./ DECISION CRITERIA AND OPTIMAL INVENTORY PROCESSES
Gal, T., Stewart, T.J., Hanne, T./ MULTICRITERIA DECISION MAKING: Advances in MCDM Models, Algorithms, Theory, and Applications
Fox, B.L./ STRATEGIES FOR QUASI-MONTE CARLO
Hall, R.W./ HANDBOOK OF TRANSPORTATION SCIENCE
Grassman, W.K./ COMPUTATIONAL PROBABILITY
Pomerol, J-C. & Barba-Romero, S./ MULTICRITERION DECISION IN MANAGEMENT
Axsäter, S./ INVENTORY CONTROL
Wolkowicz, H., Saigal, R., & Vandenberghe, L./ HANDBOOK OF SEMI-DEFINITE PROGRAMMING: Theory, Algorithms, and Applications
Dar-EI, E./ HUMAN LEARNING: From Learning Curves to Learning Organizations
Armstrong, J.S./ PRINCIPLES OF FORECASTING: A Handbook for Researchers and Practitioners
Balsamo, S., Personé, V., & Onvural, R./ ANALYSIS OF QUEUEING NETWORKS WITH BLOCKING
Bouyssou, D. et al./ EVALUATION AND DECISION MODELS: A Critical Perspective
Hanne, T./ INTELLIGENT STRATEGIES FOR META MULTICRITERIA DECISION MAKING
Saaty, T. & Vargas, L./ MODELS, METHODS, CONCEPTS and APPLICATIONS OF THE ANALYTIC HIERARCHY PROCESS
Chatterjee, K. & Samuelson, W./ GAME THEORY AND BUSINESS APPLICATIONS
Hobbs, B. et al./ THE NEXT GENERATION OF ELECTRIC POWER UNIT COMMITMENT MODELS
Vanderbei, R.J./ LINEAR PROGRAMMING: Foundations and Extensions, 2nd Ed.
Kimms, A./ MATHEMATICAL PROGRAMMING AND FINANCIAL OBJECTIVES FOR SCHEDULING PROJECTS
Baptiste, P., Le Pape, C. & Nuijten, W./ CONSTRAINT-BASED SCHEDULING
Feinberg, E. & Shwartz, A./ HANDBOOK OF MARKOV DECISION PROCESSES: Methods and Applications
Ramík, J. & Vlach, M./ GENERALIZED CONCAVITY IN FUZZY OPTIMIZATION AND DECISION ANALYSIS
Song, J. & Yao, D./ SUPPLY CHAIN STRUCTURES: Coordination, Information and Optimization
Kozan, E. & Ohuchi, A./ OPERATIONS RESEARCH/ MANAGEMENT SCIENCE AT WORK
Early Titles in the
INTERNATIONAL SERIES IN
OPERATIONS RESEARCH & MANAGEMENT SCIENCE
(Continued)

Bouyssou et al. / AIDING DECISIONS WITH MULTIPLE CRITERIA: Essays in Honor of Bernard Roy
Cox, Louis Anthony, Jr. / RISK ANALYSIS: Foundations, Models and Methods
Dror, M., L’Ecuyer, P. & Szidarovszky, F. / MODELING UNCERTAINTY: An Examination of Stochastic Theory, Methods, and Applications
Dokuchaev, N. / DYNAMIC PORTFOLIO STRATEGIES: Quantitative Methods and Empirical Rules for Incomplete Information
Sarker, R., Mohammadian, M. & Yao, X. / EVOLUTIONARY OPTIMIZATION
Zhu / QUANTITATIVE MODELS FOR PERFORMANCE EVALUATION AND BENCHMARKING
Ehrgott & Gandibleux / MULTIPLE CRITERIA OPTIMIZATION: State of the Art Annotated Bibliographical Surveys
Bienstock / Potential Function Methods for Approx. Solving Linear Programming Problems
Alpern & Gal / THE THEORY OF SEARCH GAMES AND RENDEZVOUS
Hall / HANDBOOK OF TRANSPORTATION SCIENCE - 2nd Ed.
Glover & Kochenberger / HANDBOOK OF METAHEURISTICS
Graves & Ringuest / MODELS AND METHODS FOR PROJECT SELECTION: Concepts from Management Science, Finance and Information Technology
Hassin & Haviv / TO QUEUE OR NOT TO QUEUE: Equilibrium Behavior in Queueing Systems
Gershwin et al. / ANALYSIS & MODELING OF MANUFACTURING SYSTEMS
Makros / COMPUTATIONAL TECHNIQUES OF THE SIMPLEX METHOD
Harrison, Lee & Neale / THE PRACTICE OF SUPPLY CHAIN MANAGEMENT: Where Theory and Application Converge
Shanthikumar, Yao & Zijm / STOCHASTIC MODELING AND OPTIMIZATION OF MANUFACTURING SYSTEMS AND SUPPLY CHAINS
Nabrzyski, Schopf & Węglarz / GRID RESOURCE MANAGEMENT: State of the Art and Future Trends
Thissen & Herder / CRITICAL INFRASTRUCTURES: State of the Art in Research and Application
Carlsson, Fedrizzi, & Fullér / FUZZY LOGIC IN MANAGEMENT
Soyer, Mazzuchi & Singpurwalla / MATHEMATICAL RELIABILITY: An Expository Perspective
Chakravarty & Eliashberg / MANAGING BUSINESS INTERFACES: Marketing, Engineering, and Manufacturing Perspectives
Talluri & van Ryzin / THE THEORY AND PRACTICE OF REVENUE MANAGEMENT
Kavadias & Loch / PROJECT SELECTION UNDER UNCERTAINTY: Dynamically Allocating Resources to Maximize Value
Brandeau, Sainfort & Pierskalla / OPERATIONS RESEARCH AND HEALTH CARE: A Handbook of Methods and Applications
Cooper, Seiford & Zhu / HANDBOOK OF DATA ENVELOPMENT ANALYSIS: Models and Methods
Luenberger / LINEAR AND NONLINEAR PROGRAMMING, 2nd Ed.
Sherbrooke / OPTIMAL INVENTORY MODELING OF SYSTEMS: Multi-Echelon Techniques, Second Edition
Chu, Leung, Hui & Cheung / 4th PARTY CYBER LOGISTICS FOR AIR CARGO
Gass & Assad / AN ANNOTATED TIMELINE OF OPERATIONS RESEARCH: An Informal History
Greenberg / TUTORIALS ON EMERGING METHODOLOGIES AND APPLICATIONS IN OPERATIONS RESEARCH
Early Titles in the
INTERNATIONAL SERIES IN
OPERATIONS RESEARCH & MANAGEMENT SCIENCE
(Continued)

Weber/UNCERTAINTY IN THE ELECTRIC POWER INDUSTRY: Methods and Models for Decision Support
Figueira, Greco & Ehrigott/MULTIPLE CRITERIA DECISION ANALYSIS: State of the Art Surveys
Reveliotis/REAL-TIME MANAGEMENT OF RESOURCE ALLOCATIONS SYSTEMS: A Discrete Event Systems Approach
Kall & Mayer/STOCHASTIC LINEAR PROGRAMMING: Models, Theory, and Computation
Sethi, Yan & Zhang/INVENTORY AND SUPPLY CHAIN MANAGEMENT WITH FORECAST UPDATES
Cox/QUANTITATIVE HEALTH RISK ANALYSIS METHODS: Modeling the Human Health Impacts of Antibiotics Used in Food Animals
Ching & Ng/MARKOV CHAINS: Models, Algorithms and Applications
Li & Sun/NONLINEAR INTEGER PROGRAMMING
Kaliszewski/SOFT COMPUTING FOR COMPLEX MULTIPLE CRITERIA DECISION MAKING
Bouyssou et al/EVALUATION AND DECISION MODELS WITH MULTIPLE CRITERIA: Stepping stones for the analyst
Blecker & Friedrich/MASS CUSTOMIZATION: Challenges and Solutions
Appa, Pitsoulis & Williams/HANDBOOK ON MODELLING FOR DISCRETE OPTIMIZATION
Herrmann/HANDBOOK OF PRODUCTION SCHEDULING

* A list of the more recent publications in the series is at the front of the book *