Advanced Sciences and Technologies for Security Applications

The series Advanced Sciences and Technologies for Security Applications comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

More information about this series at http://www.springer.com/series/5540

Laobing Zhang • Genserik Reniers

Game Theory for Managing Security in Chemical Industrial Areas

Springer

Laobing Zhang
Safety and Security Science Group
Delft University of Technology
Delft, The Netherlands

Genserik Reniers
Safety and Security Science Group
Delft University of Technology
Delft, The Netherlands

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-319-92617-9 ISBN 978-3-319-92618-6 (eBook)
https://doi.org/10.1007/978-3-319-92618-6

Library of Congress Control Number: 2018943895

Printed on acid-free paper

This Springer imprint is published by the registered company Springer International Publishing AG part of Springer Nature.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Introduction

We are convinced that physical security in chemical industrial areas can and should be improved, throughout the world. Chemical substances are stored and processed in large quantities in chemical plants and chemical clusters around the globe, and due to the materials' characteristics such as their flammability, explosiveness, and toxicity, they may cause huge disasters and even societal disruption if deliberately misused. Dealing with security implies dealing with intelligent adversaries and deliberate actions, as will also be further expounded in the next chapters. Such intelligent adversaries require smart solutions and flexible models and recommendations from the defender's side. Such is only possible via mathematical modelling and through the use of game theory as a technique for intelligent strategic decision-making support. In this book, we will elaborate and discuss on how this can be achieved. Figure 1 shows an overview of the book.

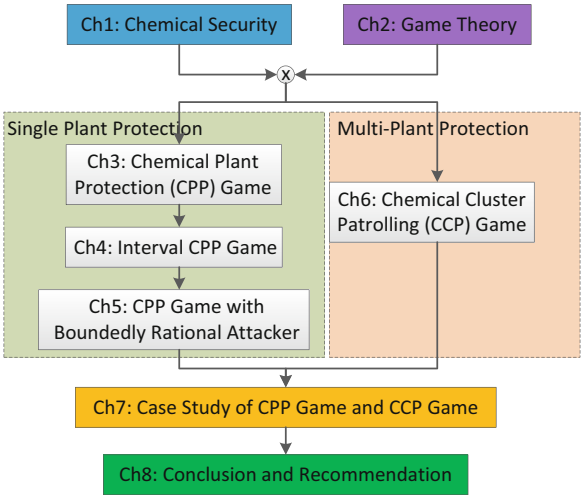

Fig. 1 Organization of the book

Chapter 1 points out that 'intentionality' is the key difference between a (deliberate) security event and a (coincidental) safety event. The importance of protecting a chemical plant as well as protecting a chemical cluster is illustrated in the chapter. State-of-the-art literature and governmental regulations are discussed. The lack of historical data and the existence of intelligent adversaries are identified as the main challenges for improving security in chemical industrial areas.

Chapter 2 introduces game theory, which is the main methodology used in this book. 'Players', 'strategies', and 'payoffs' are the main components of a game theoretic model. The 'common knowledge' assumption and the 'rationality' assumption are the most frequently used assumptions in game theoretic research and are thoroughly explained. Games with a discrete set of strategies are also discussed (and further used), since they are easier to solve as well as they better reflect reality than games with continuous strategies.

Chapters 3, 4, and 5 concern the physical protection of chemical plants belonging to a single operator. In Chap. 3, a Chemical Plant Protection (CPP) game is developed, based on the so-called multiple-layer protection approach for chemical plants. The CPP game is able to model intelligent interactions between the defender and the attackers. An analysis of the inputs and outputs of the CPP game is also provided.

However, the CPP game suffers a drawback, that is, a large amount of quantitative inputs is required. Chapter 4 therefore addresses this disadvantage, by proposing an Interval CPP game, which is an extension of the CPP game where the exact numbers of the attacker's parameters are no longer needed. Instead, in this game, only the intervals that the parameters will be situated in are required. Thus, the Interval CPP game considers the defender's distribution-free uncertainties on the attackers' parameters, and hence the inputs for the Interval CPP game are easier to obtain, for instance, by using the outputs from the API SRA method [1].

A second drawback of the CPP game concerns the rational attacker assumption. Chapter 5 therefore models bounded-rational attackers into the CPP game. In Chap. 5, three robust solutions are proposed for the CPP game, namely, the Robust solution with epsilon-optimal attackers, the MoSICP solution, and the MiniMax solution, for addressing attackers who may deviate from strategies having close payoffs to their 'best response' strategy, for addressing attackers who may play strategies with higher payoffs with higher probabilities, and for addressing attackers who only aim at minimizing the defender's maximal payoffs, respectively.

Chapter 6 employs game theory for optimizing the scheduling of patrolling in chemical clusters or chemical industrial parks. A Chemical Cluster Patrolling (CCP) game is formulated. Both the hazardousness level of each plant and the intelligence of adversaries are considered in the CCP game, for generating random but strategic and implementable patrolling routes for the cluster patrolling team.

In Chapter 7, two illustrative case studies are elaborated and investigated. In the first case study, the CPP game is applied to a refinery to show how the game works and what results can be obtained by implementing the game. The refinery case is also used in the API SRA document for illustrative purposes. Therefore, the outputs from

the API SRA method are used as one part of the inputs for the CPP game, while other inputs of the CPP game are illustrative numbers. In the second case study, the CCP game is applied to a chemical cluster composed of several plants, each belonging to different operators, for optimizing the patrolling of security guards in the multi-plant area. Results show that the patrolling route generated by the CCP game well outperforms the purely randomized patrolling strategy as well as all the fixed patrolling routes.

Eight conclusions are drawn and nine recommendations are given in Chap. 8.

Reference

1. API. Security risk assessment methodology for the petroleum and petrochemical industries. In: 780 ARP, editor. 2013.

Contents

1 Protecting Process Industries from Intentional Attacks: The State of the Art 1
1.1 Introduction 1
1.2 Safety and Security Definitions and Differences 2
1.3 Security in a Single Chemical Plant 5
1.3.1 The Need of Improving Security in Chemical Plants 5
1.3.2 Challenges with Respect to Improving Chemical Security . . 8
1.3.3 Security Risk Assessment in Chemical Plants: State-of-the-Art Research 9
1.3.4 Drawbacks of Current Methodologies 17
1.4 Protection of Chemical Industrial Parks (CIPs) or So-Called Chemical Clusters 18
1.4.1 Security Within Chemical Clusters 18
1.4.2 Chemical Cluster Security: State-of-the-Art Research 19
1.4.3 Future Promising Research Directions on Cluster Security 21
1.5 Conclusion 22
References 23

2 Intelligent Interaction Modelling: Game Theory 25
2.1 Preliminaries of Game Theory, Setting the Scene 25
2.1.1 Introduction 25
2.1.2 Players 26
2.1.3 Strategy (Set) 27
2.1.4 Payoff 28
2.1.5 The Assumption of ‘Common Knowledge’ 29

2.1.6 The Assumption of 'Rationality' . . . 31
2.1.7 Simultaneous and Sequential Game . . . 32
2.2 Game Theoretic Models with a Discrete Set of Strategies . . . 33
2.2.1 Discrete and Continuous Set of Strategies . . . 33
2.2.2 Nash Equilibrium . . . 34
2.2.3 Stackelberg Equilibrium . . . 37
2.3 Criticisms on Game Theoretic Models for Security Improvement . . . 38
2.4 Integrating Conventional Security Risk Assessment Methodologies and Game Theory for Improving Chemical Plant Protection . . . 39
2.5 Conclusion . . . 40
References . . . 41

3 Single Plant Protection: A Game-Theoretical Model for Improving Chemical Plant Protection . . . 43
3.1 General Intrusion Detection Approach in Chemical Plants . . . 43
3.2 Game-Theoretical Modelling: The Chemical Plant Protection Game (CPP Game) . . . 47
3.2.1 Players . . . 47
3.2.2 Strategies . . . 48
3.2.3 Payoffs . . . 50
3.3 Solutions for the CPP Game . . . 52
3.3.1 Nash Equilibrium . . . 53
3.3.2 Stackelberg Equilibrium . . . 54
3.3.3 Bayesian Nash Equilibrium . . . 55
3.3.4 Bayesian Stackelberg Equilibrium . . . 56
3.4 CPP Game from an Industrial Practice Point of View . . . 58
3.4.1 Input Analysis . . . 58
3.4.2 Output Analysis . . . 62
3.5 Conclusion . . . 63
References . . . 64

4 Single Plant Protection: Playing the Chemical Plant Protection Game with Distribution-Free Uncertainties . . . 65
4.1 Motivation . . . 65
4.2 Interval CPP Game Definition . . . 66
4.3 Interval Bi-Matrix Game Solver (IBGS) . . . 67
4.4 Parameter Coupling . . . 69
4.5 Interval CPP Game Solver (ICGS) . . . 74
4.6 Conclusion . . . 76
References . . . 77

5 Single Plant Protection: Playing the Chemical Plant Protection Game Involving Attackers with Bounded Rationality 79
5.1 Motivation 79
5.2 Epsilon-Optimal Attacker 81
5.2.1 Definition of an 'Epsilon-Optimal Attacker' 81
5.2.2 Game Modelling of the 'Epsilon-Optimal Attacker' 82
5.2.3 Solving the CPP Game with 'Epsilon-Optimal Attackers' 82
5.3 Monotonic Optimal Attacker 83
5.3.1 Definition of a 'Monotonic Optimal Attacker' 83
5.3.2 Game Modelling of the 'Monotonic Optimal Attacker' 84
5.3.3 Calculating the MoSICP 85
5.4 MiniMax Attacker 88
5.4.1 Definition of a 'MiniMax Attacker' 88
5.4.2 Game Modelling of the 'MiniMax Attacker' 88
5.4.3 Solving the CPP Game with 'MiniMax Attackers' 88
5.5 Conclusion 89
References 89

6 Multi-plant Protection: A Game-Theoretical Model for Improving Chemical Clusters Patrolling 91
6.1 Introduction 91
6.2 Patrolling in Chemical Clusters 92
6.2.1 A Brief Patrolling Scenario Within a Chemical Cluster 92
6.2.2 Formulating the Research Question 92
6.3 Game Theoretic Modelling 99
6.3.1 Players 99
6.3.2 Strategies 99
6.3.3 Payoffs 101
6.3.4 Computing the Probability of the Attack Being Detected (f) 102
6.4 Solutions for the Game 104
6.4.1 Stackelberg Equilibrium 104
6.4.2 Robust Solution Considering Distribution-Free Uncertainties 106
6.4.3 Robust Solutions Considering Implementation Errors and Observation Errors 108
6.5 Conclusion 109
References 109

7 Case Studies 111
7.1 Case Study #1: Applying the CPP Game to a Refinery 111
7.1.1 Case Study Setting 111
7.1.2 Chemical Plant Protection Game Modelling 114
7.1.3 CPP Game Results 118
7.2 Case Study #2: Applying the CCP Game for Scheduling Patrolling in the Setting of a Chemical Industrial Park 138
7.2.1 Case Study Setting 138
7.2.2 Game Modelling 139
7.2.3 CCP Game Results 140
7.3 Conclusion 147
References 148

8 Conclusions and Recommendations 151
References 157

List of Figures

Fig. 1 Organization of the book v

Fig. 1.1 The trend of global terrorist attacks from 2007 to 2015 5
Fig. 1.2 Security investment w.r.t. strategic vs. nonstrategic terrorist 8
Fig. 1.3 Safety trias and security trias 10
Fig. 1.4 SVA model 11
Fig. 1.5 SRFT example from Bajpai (CSRS: Current Security Risk Status) 13
Fig. 1.6 The API SRA procedure 15
Fig. 1.7 Hypothetical domino effect illustrating the complexity of domino events 20

Fig. 2.1 Game tree of a illustrative defend-attack game 27
Fig. 2.2 A simple bi-matrix game with multiple Nash Equilibria (NE) 36
Fig. 2.3 A framework of integrating the API SRA methodology and game theory 40

Fig. 3.1 General physical intrusion detection approach in chemical plants 44
Fig. 3.2 The intrusion and attack procedure 46

Fig. 5.1 Attacker's payoff by responding different pure strategies to y 85

Fig. 6.1 Layout of a chemical park in Antwerp port 93
Fig. 6.2 Graphic modelling of the chemical park 93
Fig. 6.3 Patrolling Graph of the illustrative example 97
Fig. 6.4 An illustrative figure of the overlap situation 103

Fig. 7.1 Layout of a refinery (PF = Production Facility) 112
Fig. 7.2 Formalized representation of the refinery. (**a**) Abstract description of the plant (**b**) Intrusion and attack procedure 113
Fig. 7.3 The coefficients in Tables 7.5 and 7.6 117
Fig. 7.4 Defender's payoff by responding with different strategies 123

Fig. 7.5 Attacker's payoff range 125
Fig. 7.6 Defender's expected payoff from different game solutions 128
Fig. 7.7 Robustness of different solutions 129
Fig. 7.8 Defender's payoffs by responding with pure strategies to the attackers' BNE strategies 131
Fig. 7.9 Attackers' payoff range 133
Fig. 7.10 Defender's expected payoffs from different solutions, considering multiple types of attackers 136
Fig. 7.11 Sensitivity analysis (of the epsilon value in the robust solution and of the interval radius in the interval game solution) 137
Fig. 7.12 The optimal patrolling strategy and the attacker's best response 141
Fig. 7.13 The patroller's optimal fixed patrolling route and the attacker's best response 144
Fig. 7.14 Robust solution of the interval CCP game 146
Fig. 7.15 Attacker payoff information of the robust solution of the Interval CCP game (PBR: possible best response) 148

Fig. 8.1 An extended framework of integrating conventional security risk assessment methods and security game 155
Fig. 8.2 Uncertainty space for the CPP game 156