

Contents

	<i>Preface</i>	<i>page</i> xii
	<i>Acknowledgments</i>	xv
	<i>Artwork</i>	xvi
	<i>Notation</i>	xvii
Part I	Introduction	1
1	Introduction	3
	1.1 Network security	4
	1.2 The approach	8
	1.3 Motivating examples	13
	1.3.1 Security games	13
	1.3.2 Security risk-management	15
	1.3.3 Optimal malware epidemic response	16
	1.4 Discussion and further reading	18
2	Network security concepts	20
	2.1 Networks and security threats	21
	2.1.1 Networks and the World Wide Web	21
	2.1.2 Security threats	23
	2.2 Attackers, defenders, and their motives	27
	2.2.1 Attackers	27
	2.2.2 Defenders	28
	2.3 Defense mechanisms	29
	2.4 Security tradeoffs and risk-management	32
	2.4.1 Security tradeoffs	32
	2.4.2 Security risk-management	34
	2.5 Discussion and further reading	34

Part II Security games	37
3 Deterministic security games	39
3.1 Security game model	40
3.2 Intrusion detection games	43
3.2.1 Matrix games	43
3.2.2 Games with dynamic information	45
3.3 Sensitivity analysis	47
3.4 Modeling malicious behavior in social networks	48
3.5 Security games for vehicular networks	51
3.5.1 Vehicular network model	51
3.5.2 Attack and defense model	52
3.5.3 Game formulation and numerical analysis	53
3.6 Security games in wireless networks	56
3.6.1 Random access security games	57
3.6.2 Interference limited multiple access security games	63
3.7 Revocation games	66
3.7.1 Revocation game model	67
3.7.2 Sequential revocation games	68
3.7.3 Static revocation games	71
3.8 Discussion and further reading	72
4 Stochastic security games	74
4.1 Markov security games	75
4.1.1 Markov game model	76
4.1.2 Solving Markov games	77
4.2 Stochastic intrusion detection game	80
4.3 Security of interconnected systems	83
4.3.1 Analysis of an illustrative example	84
4.3.2 Linear influence models	86
4.4 Malware filter placement game	90
4.4.1 Stochastic game formulation	92
4.4.2 Simulations	93
4.5 Discussion and further reading	95
5 Security games with information limitations	98
5.1 Bayesian security games	99
5.1.1 Bayesian intrusion detection game	99
5.1.2 Bayesian games for wireless security	106
5.2 Security games with observation and decision errors	109
5.2.1 Game model and fictitious play	110
5.2.2 Fictitious play with observation errors	112
5.2.3 Fictitious play with decision errors	120

	5.2.4 Time-invariant and adaptive fictitious play	123
	5.3 Discussion and further reading	129
Part III Decision making for network security		131
6	Security risk-management	133
	6.1 Quantitative risk-management	134
	6.1.1 Risk in networked systems and organizations	134
	6.1.2 A probabilistic risk framework	137
	6.1.3 Dynamic risk mitigation and control	143
	6.2 Security investment games	150
	6.2.1 Influence network and game model	151
	6.2.2 Equilibrium and convergence analysis	153
	6.2.3 Incentives and game design	156
	6.3 Cooperative games for security risk-management	158
	6.3.1 Coalitional game model	158
	6.3.2 Coalition formation under ideal cooperation	161
	6.4 Discussion and further reading	165
7	Resource allocation for security	166
	7.1 An optimization approach to malware filtering	167
	7.1.1 Traffic centrality measures	168
	7.1.2 Filtering problem formulations	169
	7.2 A robust control framework for security response	173
	7.2.1 Network traffic filtering model	174
	7.2.2 Derivation of optimal controller and state estimator	176
	7.3 Optimal and robust epidemic response	179
	7.3.1 Epidemic models	180
	7.3.2 Feedback response for malware removal	182
	7.3.3 Multiple networks	183
	7.4 Discussion and further reading	187
8	Usability, trust, and privacy	189
	8.1 Security and usability	190
	8.1.1 A system for security alert dissemination	191
	8.1.2 Effective administrator response	195
	8.2 Digital trust in online communities	198
	8.2.1 Community trust game	199
	8.2.2 Dynamics and convergence	203
	8.2.3 Numerical analysis	206
	8.3 Location privacy in mobile networks	210
	8.3.1 A location privacy model	211

x	Contents	
	8.3.2 Location privacy games	213
	8.4 Discussion and further reading	215
	Part IV Security attack and intrusion detection	217
9	Machine learning for intrusion and anomaly detection	219
	9.1 Intrusion and anomaly detection	220
	9.1.1 Intrusion detection and prevention systems	221
	9.1.2 Open problems and challenges	224
	9.2 Machine learning for security: an overview	225
	9.2.1 Overview of machine-learning methods	226
	9.2.2 Open problems and challenges	228
	9.3 Distributed machine learning	230
	9.3.1 SVM classification and decomposition	231
	9.3.2 Parallel update algorithms	232
	9.3.3 Active set method and a numerical example	238
	9.3.4 Behavioral malware detection for mobile devices	241
	9.4 Discussion and further reading	243
10	Hypothesis testing for attack detection	244
	10.1 Hypothesis testing and network security	245
	10.2 An overview of hypothesis testing	246
	10.2.1 Bayesian hypothesis testing	247
	10.2.2 Minimax hypothesis testing	247
	10.2.3 Neyman–Pearson hypothesis testing	249
	10.2.4 Other hypothesis testing schemes	250
	10.3 Decentralized hypothesis testing with correlated observations	255
	10.3.1 Decentralized hypothesis testing	255
	10.3.2 Decision rules at the sensors and at the fusion center	257
	10.3.3 Decentralized Bayesian hypothesis testing	259
	10.3.4 Decentralized Neyman–Pearson hypothesis testing	264
	10.4 The majority vote versus the likelihood ratio test	268
	10.5 An algorithm to compute the optimal thresholds	270
	10.6 Discussion and further reading	273
A	Optimization, game theory, and optimal and robust control	274
	A.1 Introduction to optimization	274
	A.1.1 Sets, spaces, and norms	274
	A.1.2 Functionals, continuity, and convexity	275
	A.1.3 Optimization of functionals	276
	A.2 Introduction to noncooperative game theory	281
	A.2.1 General formulation for noncooperative games and equilibrium solutions	282

A.2.2	Existence of Nash and saddle-point equilibria in finite games	284
A.2.3	Existence and uniqueness of Nash and saddle-point equilibria in continuous-kernel (infinite) games	285
A.2.4	Online computation of Nash equilibrium policies	287
A.3	Introduction to optimal and robust control theory	288
A.3.1	Dynamic programming for discrete-time systems	289
A.3.2	Dynamic programming for continuous-time systems	291
A.3.3	The minimum principle	294
A.3.4	H^∞ -optimal control	296
	<i>References</i>	302
	<i>Index</i>	312