Emerging Methodologies and Applications in Modelling, Identification and Control

Cloud Control Systems

Analysis, Design and Estimation

Magdi S. Mahmoud
King Fahd University of Petroleum and Minerals
Systems Engineering Department
Dhahran, Saudi Arabia

Yuanqing Xia
Beijing Institute of Technology
School of Automation
Beijing, China

Series Editors
Stephen Ison
Lucy Budd

ELSEVIER

ACADEMIC PRESS
An imprint of Elsevier

Contents

About the authors xv
Preface xvii
Acknowledgments xxi

1. An overview

1.1 Preliminaries 1
1.1.1 Real-time distributed control systems 2
1.1.2 Synopsis of the security problem 3
1.2 Basics of cloud control systems 4
1.2.1 Cloud control security 5
1.2.2 Different types of cyber attacks 6
1.2.3 Passive versus active attacks 7
1.2.4 Fundamental requirements 8
1.2.5 Design consideration 11
1.3 A view on modeling cloud control systems 12
1.3.1 Development and activities 14
1.3.2 Architecture of cloud control systems 15
1.4 Notes 17

2. Cloud control systems venture

2.1 Introduction 19
2.1.1 Characteristics 20
2.1.2 Cloud control system venture 20
2.1.3 Security 21
2.2 Cloud control system security objectives 21
2.2.1 Confidentiality 22
2.2.2 Integrity 22
2.2.3 Availability 23
2.2.4 Reliability 23
2.2.5 Robustness 23
2.2.6 Trustworthiness 23
2.3 Types of attacks in cloud control system 23
2.3.1 Detection of cyber attacks 25
2.3.2 Bayesian detection with binary hypothesis 25
2.3.3 Weighted least-squares approaches 26

2.3.4 χ^2 Detector based on Kalman filters 27
2.3.5 Fault detection and isolation techniques 28
2.4 Denial-of-service attacks 29
2.4.1 Approaches of modeling a denial-of-service attack 29
2.4.2 Secure estimation approaches 31
2.4.3 Secure control approaches of denial-of-signal attack 32
2.4.4 Jamming attack 38
2.5 Deception attack 40
2.5.1 Modeling the deception attack 40
2.5.2 Secure estimation approaches of the deception attack 42
2.5.3 Secure control approaches of the deception attack 44
2.5.4 Replay attack 46
2.6 Notes 47

3. Distributed denial-of-service attacks

3.1 Introduction 51
3.2 Methods and tools 52
3.2.1 DDoS strategy 54
3.2.2 Types of DDoS attacks 55
3.3 Detection techniques against DDoS attacks 57
3.3.1 Literature review 57
3.3.2 Signature-based detection technique 57
3.3.3 Anomaly-based detection technique 58
3.3.4 Artificial neural network intrusion detection techniques 58
3.3.5 Genetic algorithm intrusion detection systems 59
3.4 Epilogue 59
3.5 Stabilization of distributed discrete systems 60
3.5.1 Introduction 60
3.5.2 Distributed cloud control system (DCCS) 62
3.5.3 Characteristics of the denial-of-service attacks 62
3.5.4 Nominal design results 63
3.5.5 A small-gain approach for distributed CPS 66
3.5.6 Stability analysis under denial-of-service attacks 69
3.5.7 Illustrative example 72
3.6 Notes 75

4. Distributed cloud control systems

4.1 Introduction and wireless control design challenge 77
4.2 Embedded virtual machines 82
4.2.1 Network CCS related work 84
4.2.2 Design flow of embedded virtual machines 85
4.2.3 Platform-independent domain-specific language 86
4.2.4 Control problem synthesis 87
4.3 EVM architecture 89
4.3.1 Embedded virtual machine extensions to the nano-RK RTOS 90

4.3.2 Virtual component interpreter 91
4.3.3 Virtual tasks 91
4.3.4 Virtual component manager 92
4.4 Virtual task assignment 93
4.4.1 General formulation 93
4.4.2 Problem relaxation 99
4.5 EVM runtime operation 101
4.5.1 Adaptation to planned and unplanned network changes 101
4.5.2 Communication schedulability analysis 102
4.5.3 Computation schedulability analysis 103
4.6 EVM implementation 104
4.6.1 EVM case study 105
4.6.2 Limitations of the EVM approach 107
4.7 Wireless control networks 108
4.7.1 An intuitive overview 108
4.7.2 Model development 109
4.8 Synthesis of an optimal wireless control network 114
4.8.1 Robustness to link failures 116
4.8.2 Wireless control networks with observer style updates 117
4.9 Robustness to node failure 121
4.10 Control of continuous-time plants 122
4.11 Process control application 125
4.11.1 Case description 125
4.11.2 Wireless control network experimental platform 125
4.11.3 Wireless control networks results 126
4.12 Notes 128

5. Secure stabilization of distributed systems

5.1 Introduction 131
5.2 Networked distributed system 133
5.2.1 Denial-of-service attacks–frequency and duration 133
5.3 Analytical results 135
5.3.1 A small-gain approach 135
5.3.2 Stabilization under denial of service 138
5.4 Approximation of resilience with reduced communication 141
5.4.1 Zeno-free event-triggered control 142
5.4.2 Hybrid transmission strategy under DoS 143
5.5 Simulation results 145
5.5.1 Simulation example 1 145
5.5.2 Simulation example 2 145
5.6 Notes 148

6. False data injection attacks

6.1 Related work 149
6.2 Kalman filter-based systems 151

6.2.1 Physical plant 151
6.2.2 Data buffer 152
6.2.3 Communication network 152
6.2.4 Control prediction generator 153
6.2.5 Network delay compensator 154
6.3 FDI attacks 154
6.3.1 Design results 156
6.4 Simulation results 159
6.4.1 Case 1: A and F are stable 160
6.4.2 Case 2: A is stable and F is unstable 161
6.4.3 Case 3: A is unstable and F is stable 162
6.5 Experimental results 164
6.5.1 Case 1: F is stable 165
6.5.2 Case 2: F is unstable 165
6.6 Notes 166

7. Stabilization schemes for secure control

7.1 Introduction and objectives 169
7.1.1 Process dynamics and ideal control action 171
7.1.2 DoS and actual control action 172
7.1.3 Control objectives 173
7.1.4 Stabilizing control update policies 174
7.2 Input-to-state stability under denial of service 177
7.2.1 Assumptions of time-constrained denial of service 178
7.2.2 Input-to-state stability under denial of service 179
7.2.3 Disturbance-free case 189
7.2.4 Resilient control logic 190
7.2.5 Periodic sampling logic 190
7.3 Event-based periodic sampling logic 191
7.3.1 Self-triggering sampling logic 192
7.3.2 Simulation examples and discussions 193
7.3.3 Numerical example 196
7.3.4 Slow-on-the-average DoS: disturbance-free case 197
7.4 Observer-based secure control 199
7.4.1 Problem formulation 200
7.4.2 Design results 203
7.4.3 Illustrative example I 206
7.5 Stabilization of discrete-time systems under DoS attack 208
7.5.1 Preliminaries 211
7.5.2 Discrete-time distributed system 213
7.5.3 Characteristics of the DoS attacks 214
7.5.4 Design results 215
7.5.5 The small-gain approach 218
7.5.6 Stability analysis under DoS attacks 221
7.5.7 Illustrative example II 223
7.6 Notes 226

8. Secure group consensus

8.1 Couple-group consensus conditions under denial-of-service attacks 229
8.1.1 Introduction 230
8.1.2 Algebraic graph theory 231
8.1.3 Consensus problem 231
8.1.4 Group consensus 232
8.1.5 Attack model 234
8.1.6 First-order group consensus under DoS attack 234
8.1.7 Simulation studies 241
8.2 Adaptive cluster consensus with unknown control coefficients 246
8.2.1 Introduction 247
8.2.2 Algebraic graph theory 250
8.2.3 Consensus 251
8.2.4 Group consensus 251
8.2.5 Single-integrator linear dynamics 251
8.2.6 Single integrator with nonlinear dynamics 253
8.2.7 Linear double-integrator dynamics 256
8.2.8 Nonlinear dynamics 257
8.2.9 Simulation studies 260
8.2.10 Single integrator with linear dynamics 261
8.2.11 Single integrator with nonlinear dynamics 261
8.2.12 Double integrator with linear dynamics 263
8.2.13 Double integrator with nonlinear dynamics 264
8.3 Notes 266

9. Cybersecurity for the electric power system

9.1 Problem description 271
9.2 Risk assessment methodology 273
9.2.1 Risk analysis 273
9.2.2 Risk mitigation 274
9.3 Power system control security 274
9.3.1 Model of microgrid system 277
9.3.2 Observation model and cyber attack 278
9.3.3 Cyber attack minimization in smart grids 280
9.3.4 Stabilizing feedback controller 281
9.4 Security of a smart grid infrastructure 282
9.4.1 Introduction 283
9.4.2 A cyber-physical approach to smart grid security 285
9.4.3 Cybersecurity approaches 286
9.4.4 System model 287
9.4.5 Cybersecurity requirements 287
9.4.6 Attack model 289
9.4.7 Countermeasures 293
9.4.8 Secure communication architecture 293
9.4.9 System and device security 294

9.4.10 System-theoretic approaches 295
9.4.11 Security requirements 297
9.4.12 Attack model 297
9.4.13 Countermeasures 297
9.4.14 Bad data detection 297
9.4.15 The need for cyber-physical security 298
9.4.16 Defense against replay attacks 300
9.4.17 Cybersecurity investment 303
9.5 Notes 306

10. Resilient design under cyber attacks

10.1 Introduction 307
10.2 Problem statement 309
10.2.1 System model 310
10.2.2 Attack monitor 310
10.2.3 Switching the controller 313
10.2.4 Simulation results I 316
10.3 Secure control subject to stochastic attacks 319
10.3.1 Problem formulation and preliminaries 320
10.3.2 Design results 324
10.3.3 Simulation results II 334
10.4 Notes 334

11. Safety assurance under stealthy cyber attacks

11.1 Introduction 339
11.2 Cloud system model subject to cyber attacks 340
11.3 Stealthy deception attack design 343
11.3.1 Actuators are compromised 343
11.3.2 Sensors are compromised 344
11.3.3 Both actuators and sensors are compromised 346
11.3.4 Application to UAV navigation systems 349
11.4 Notes 352

12. A unified game approach under DoS attacks

12.1 Introduction 353
12.2 Problem description 355
12.2.1 Model of NCS subject to DoS attack 355
12.2.2 MTOC and CTOC design 356
12.2.3 Defense and attack atrategy design 357
12.3 MTOC and CTOC control strategies 358
12.4 Defense and attack strategies 361
12.4.1 Development of defense strategies 361
12.4.2 Development of attack strategies 362
12.5 Validation results 364
12.5.1 Building model description 364

12.5.2 Strategy design 365
12.5.3 Robust study 366
12.5.4 Comparative study 367
12.6 Experiment verification 367
12.7 Notes 369

13. Secure estimation subject to cyber stochastic attacks

13.1 Estimation against stochastic cyber attacks 373
13.1.1 Introduction 374
13.1.2 Problem formulation 375
13.1.3 Secure estimation design results 377
13.1.4 Illustrative example I 388
13.2 Resilience state estimation against integrity attacks 389
13.2.1 Introduction 391
13.2.2 System model 392
13.2.3 Attack model 393
13.2.4 Generic resilient estimator 394
13.2.5 Resilient estimator with L1-penalty 395
13.2.6 Resilience analysis 396
13.2.7 Necessary and sufficient conditions 397
13.2.8 Performance evaluation without attacks 400
13.2.9 Performance evaluation under attacks 401
13.2.10Illustrative example II 403
13.3 Notes 403

14. Cloud-based approach in data centers

14.1 Preliminaries 405
14.1.1 A modeling approach 406
14.1.2 Architecture 406
14.1.3 Tier levels 407
14.2 Modeling and control for energy efficiency 407
14.2.1 Server level control 410
14.2.2 Group level control 411
14.2.3 Data center level control 412
14.3 A cloud control system model of data centers 413
14.3.1 Computational network 414
14.3.2 Thermal network 416
14.3.3 Control strategies 417
14.3.4 Baseline controller 419
14.3.5 Uncoordinated controller 419
14.3.6 Coordinated controller 420
14.3.7 Simulation results I 421
14.3.8 A cyber-physical index for data centers 425
14.4 Dynamic server provisioning 428
14.4.1 Zone level model 429
14.4.2 System dynamics 430

14.4.3 Performance model 430
14.4.4 Data center level model 431
14.4.5 Zone-level controller 434
14.4.6 Data center level controller 436
14.4.7 Simulation results II 438
14.5 Notes 444
References 445
Index 471