Contents

Part I Architecture and Applications

1 **Envisioned Network Architectures for IoT Applications** 3
P. Sarwesh, N. Shekar V. Shet, and K. Chandrasekaran
1.1 Introduction 3
1.2 Network Level Challenges in IoT 5
1.2.1 Energy Efficiency 5
1.2.2 Reliability and QoS 6
1.3 Factors that Affect the Network Performance 6
1.3.1 Energy Hole (Node Overload) 7
1.3.2 Multi-Retransmissions 7
1.3.3 Collision 7
1.3.4 Control Packet Overhead 8
1.3.5 Delay 8
1.3.6 Motivation 8
1.4 Envisioned Network Architecture for Low Power IoT Networks 9
1.4.1 E-Health 9
1.4.2 Environmental Monitoring 10
1.4.3 Industrial Automation 11
1.4.4 Smart Grid 13
1.5 Suitability of Proposed Network Architectures for IoT Scenario and Network Assumptions 16
1.6 Conclusion 16
References 16

2 **A Measurement Study of Campus WiFi Networks Using WiFiTracer**. 19
Chengwei Zhang, Xiaojun Hei, and Brahim Bensaou
2.1 Introduction 20
2.2 WiFi Measurement Platform 21
2.2.1 Measurement Framework Overview 22
2.2.2 WiFiTracer Architecture 22
2.2.3 Measurement Sampling Procedure 24

2.3 Sensing Result Analysis 25
2.3.1 Basic WiFi Dataset 26
2.3.2 General Analysis of WiFi Networks 26
2.3.3 Characterizing Public Campus WiFi Networks 30
2.4 Characterization of WiFi Connection Time 35
2.4.1 WiFi Connection Dataset 35
2.4.2 Characterizing Successful WiFi Connections 36
2.5 Related Work 39
2.6 Conclusion 40
References 40

3 People as Sensors: Towards a Human–Machine Cooperation Approach in Monitoring Landslides in the Three Gorges Reservoir Region, China 43
Zhenhua Li, Guoxuan Cheng, Wenming Cheng, and Hongbo Mei
3.1 Introduction 43
3.2 Project Description 44
3.3 The Sensor-Based Monitor System 44
3.3.1 The Remote Sensing Monitoring System 45
3.3.2 The GPS System 45
3.3.3 The Comprehensive Monitoring System 47
3.4 The Human-Based Monitoring System: People as Sensors 47
3.5 The Monitoring and Early Warning Platform 49
3.6 Conclusions 50
References 52

4 Two Major Applications in Vehicular Ad Hoc Networks 55
Binbin Zhou, Zhan Zhou, Gang Pan, Shijian Li, Hexin Lv, and Tiaojuan Ren
4.1 Introduction 56
4.2 Rear-End Collision Warning 57
4.2.1 Problem Description 58
4.2.2 Our Collaborative Real-Time Rear-End Collision Warning Algorithm 59
4.2.3 Evaluation 62
4.3 Automatic Incidents Detection 64
4.3.1 Problem Formulation 65
4.3.2 Our Automatic Incidents Detection Approach 65
4.3.3 Experiments and Analysis 67
4.4 Conclusion 69
References 70

5 Concurrency and Synchronization in Structured Cyber Physical Systems 73
Jitender Grover and Ram Murthy Garimella
5.1 Introduction 74

5.2 Concurrent Cyber Physical Systems: Modeling 78
5.2.1 Concurrency in Cyber Physical Systems 78
5.2.2 Coordination and Maintenance of Concurrent Cyber Physical Systems 79
5.2.3 Design Issues: Concurrent CPSs 80
5.2.4 Modeling Linear Concurrent CPS 80
5.3 Synchronization of Concurrent Cyber Physical Systems 83
5.3.1 Networked Cyber Physical Systems: Synchronization 83
5.3.2 Clock's Synchronization: Multidimensional CPSs 84
5.4 Temporal Semantics: Design of Cyber Physical Systems 84
5.4.1 Classification of Cyber Physical Systems (CPSs) 85
5.4.2 Real-Time CPSs: Temporal Semantics 86
5.4.3 Software System: Temporal Semantics 88
5.5 Reliability and Fault Tolerance: Concurrent Cyber Physical Systems 89
5.5.1 Fault Tolerance 89
5.5.2 Fault/Failure Localization: 89
5.5.3 Architectural Considerations: Cyber Physical Systems 90
5.5.4 Reliability and Fault Management Using Edge Servers 91
5.6 Agent Working in Different Conditions 92
5.7 Conclusion 94
References 94

Part II Security and Privacy

6 Survey on Access Control Models Feasible in Cyber-Physical Systems 103
Mikel Uriarte, Jasone Astorga, Eduardo Jacob, Maider Huarte, and Oscar López
6.1 Introduction 103
6.2 Context-Related Features and Requirements 106
6.2.1 Constrained Device Classification 106
6.2.2 Constrained Networks 107
6.2.3 Life Cycle and Access Control Requirements 108
6.2.4 Use-Case-Driven Access Control Model 109
6.2.5 Security Policy 109
6.2.6 Security Architecture Overview 111
6.2.7 Cryptographic Schema and Key Establishment 113
6.3 Access Control Foundations 114
6.3.1 Policy-Driven Security Management 114
6.3.2 Access Control Models 115
6.4 Access Control Policy Languages 117
6.4.1 XACML 117
6.4.2 Ponder Policy Language 119
6.4.3 Rei Policy Language 120

6.4.4 Authorization Specification Language (ASL) 121
6.4.5 Obligation Specification Language (OSL) 121
6.4.6 Privacy-Focused Policy Languages 121
6.4.7 Capability-Based Access Control CapBAC 122
6.4.8 Discussion on Foundational Approaches 123
6.5 IoT Tailored Access Control Approaches............................. 124
6.5.1 Authorization Framework for the IoT Based on XACML 125
6.5.2 Usage-Based Access Control Adapted to IoT (UCON)....... 128
6.5.3 CapBAC in IoT 130
6.5.4 Distributed CapBAC in IoT 131
6.5.5 Delegated CoAP Authentication and Authorization Framework (DCAF) 134
6.5.6 OSCAR... 136
6.5.7 Ladon.. 138
6.5.8 Hidra.. 140
6.5.9 Discussion About IoT Taylored Access Control Solutions ... 143
6.6 Conclusions and Future Work 146
References 149

7 Security Challenges and Concerns of Internet of Things (IoT) 153
Aniruddha Bhattacharjya, Xiaofeng Zhong, Jing Wang, and Xing Li
7.1 Introduction 154
7.2 Internet of Things Architectures, Properties, and Security Requirements.. 156
7.2.1 Architectures and Basic Properties 156
7.2.2 Main Security Requirements and Their Sub-Components.... 163
7.3 Constrained Application Protocol: Application Layer Connection-Less Lightweight Protocol for the Internet of Things ... 170
7.3.1 Constrained Application Protocol............................. 170
7.3.2 Constrained Application Protocol–IP Security 171
7.4 Datagram Transport Layer Security Overview and Supporting Constrained Application Protocol 174
7.4.1 Datagram Transport Layer Security Protocol 174
7.4.2 Supporting Constrained Application Protocol................ 177
7.5 Case Studies and Open Research Issues 179
References 182

8 Cyber-Physical System Security Controls: A Review 187
Subhrajit Majumder, Akshay Mathur, and Ahmad Y. Javaid
8.1 Introduction 187
8.2 Background.. 188
8.2.1 Cyber-Physical Systems 188
8.2.2 CPS Communications 190
8.2.3 CPS Models and Aspects...................................... 192
8.2.4 Security in CPS 196

8.3 CPS Security Threats 197
8.3.1 General CPS Threat Model 197
8.3.2 CPS Security Threats 198
8.4 CPS Security Vulnerabilities 200
8.4.1 Causes of Vulnerabilities 200
8.4.2 Vulnerabilities in ICS 201
8.4.3 Vulnerabilities in Smart Grid 203
8.4.4 Vulnerabilities in Medical Devices 205
8.4.5 Vulnerabilities in Smart Cars 207
8.5 Real-World CPS Attacks 209
8.5.1 Attacks on Industrial Control System (ICS) 209
8.5.2 Attacks on Smart grids 216
8.5.3 Attacks on Medical Devices 218
8.5.4 Attacks on Smart Cars 219
8.6 Security Control and Solutions 221
8.6.1 General CPS Controls 221
8.6.2 Application-Specific Controls 222
8.7 Security Challenges 228
8.7.1 Challenges in General CPS 228
8.7.2 Challenge in ICS 228
8.7.3 Challenges in Smart Grids 229
8.7.4 Challenges in Medical Devices 230
8.7.5 Challenges in Smart Cars 230
8.8 Conclusion 231
References 232

Index 241