

Contents

1	Introduction	1
1.1	Wireless Communication Technologies	1
1.2	Wireless Sensor Networks	2
1.3	Application Areas of WSNs	3
1.4	Challenges in the Design and Implementation of WSNs	4
1.5	Aims of the Book	6
	References	6
2	Principle of Wireless Sensor Networks	7
2.1	Introduction	7
2.2	IEEE 802.15.4 Standard and Wireless Sensor Network	9
2.2.1	OSI and WSN Stacks	9
2.2.2	Overview of IEEE 802.15.4 Standard	11
2.2.3	Full Function Device and Reduced Function Device	12
2.2.4	IEEE 802.15.4 Topologies	13
2.2.5	Multiple Access in IEEE 802.15.4 Wireless Systems	15
2.3	Constructing WSNs with IEEE 802.15.4	17
2.3.1	Radio Channel Assessment	18
2.3.2	Network Initialization	20
2.3.3	Network Establishment Announcement	24
2.3.4	Listen for/Initiate Joining Request	25
2.3.5	Listen for/Initiate Removal Request	25
2.3.6	Network Command Transmission/Reception	25
2.3.7	Data Transmission and Reception	26
2.3.8	Slotted and Unslotted CSMA-CA	28
2.3.9	Summary of Data Transmission in IEEE 802.15.4	31
2.4	ZigBee and Wireless Sensor Networks	32
2.4.1	ZigBee Stack Structure	32
2.4.2	ZigBee Topologies	34
2.4.3	ZigBee Address Allocation Scheme	37
2.4.4	ZigBee Management Mechanisms	39

2.5	6LoWPAN and Wireless Sensor Network	44
2.6	Summary	46
	References	47
3	Hardware Design for WSNs	49
3.1	General Wireless Sensor Node Architecture	49
3.2	System-on-Chip and Component-based Design	50
3.3	Design Guidelines	51
3.3.1	Microcontroller Selection	53
3.3.2	Communication Device Selection	54
3.3.3	Sensing Device Design	55
3.3.4	Power Supply Device Design	58
3.4	Design Case	59
3.4.1	Temperature Sensor Design	59
3.4.2	CO Sensor Design	61
3.4.3	Sensor Node Circuit Design	63
3.5	Power Management	64
3.6	Energy Scavenging	66
3.6.1	Solar Energy Harvesting Unit	67
3.6.2	Maximum Power Point Tracking Unit	68
3.6.3	Power Management Unit	68
3.6.4	Design Case	70
3.7	Conclusion	72
	References	72
4	Embedded Software Design for WSNs	73
4.1	Introduction	73
4.2	Embedded Software Design for WSNs	74
4.2.1	Jennic ZigBee Application Development	75
4.2.2	Contiki 6LoWPAN Application Development	77
4.3	Sensor Driver Development	80
4.3.1	General Procedure of Sensor Drivers	81
4.3.2	Sensor Driver for an Analog Flow Sensor	84
4.3.3	Sensor Driver for a Digital Temperature Sensor	86
4.4	Implementing a WSN with IEEE 802.15.4	91
4.5	Bridging WSNs with an External Public Network	98
4.6	Summary	100
	References	100
5	Routing Technologies in WSNs	101
5.1	Introduction	101
5.2	Classification of Routing Protocols in WSNs	102
5.2.1	Flat Routing Protocols	104
5.2.2	Hierarchical Routings Protocols	107

5.2.3	Location-Based Routings Protocols	110
5.3	AODV Routing Protocols	112
5.3.1	Principle of the AODV Routing Protocols	113
5.3.2	AODV Message Formats	114
5.3.3	Implementation of a Simplified Version of AODV	114
5.4	Cluster-Tree Routing Protocol	119
5.4.1	Single Cluster Network	120
5.4.2	Multi-Cluster Network	122
5.5	Energy-Aware Routing Protocols	124
5.6	Summary	127
	References	127
6	Optimization of Sink Node Positioning	129
6.1	Introduction	129
6.2	Challenges of Sink Node Positioning	130
6.3	Categories of Sink Node Positioning Approaches	131
6.3.1	Static Positioning of Sink Nodes	132
6.3.2	Dynamic Sink Node Positioning	133
6.3.3	Mobile Sink Node Positioning	133
6.4	Optimizing Locations of Static Multiple Sink Nodes	134
6.4.1	System Assumption	134
6.4.2	Simplified Routing Protocol	135
6.4.3	Energy Consumption Model	136
6.4.4	Optimal Locations of Multiple Sink Nodes	138
6.5	Solving Optimal Location Problems	139
6.6	Conclusions	140
	References	141
7	Interference of WSNs with IEEE 802.11b Systems	143
7.1	Introduction	143
7.2	Wireless Coexistence and Interference in WSNs	144
7.3	Performance Metrics	145
7.3.1	PHY Layer Performance Measures	145
7.3.2	MAC Layer Performance Measures	146
7.4	Coexistence Mechanism of IEEE 802.15.4	147
7.4.1	Direct Sequence Spread Spectrum	147
7.4.2	Frequency Division Multiple Access	150
7.4.3	Carrier Sense Multiple Access with Collision Avoidance	151
7.5	Mitigating Interference Between IEEE 802.11b and IEEE 802.15.4	151
7.5.1	Frequency Offset	151
7.5.2	Interfering Energy and Physical Separation	154
7.5.3	Recommendations Made in IEEE 802.15.4	157

7.6	Advanced Mitigation Strategies	158
7.6.1	Adaptive Interference-Aware Multi-Channel Clustering	158
7.6.2	Adaptive Radio Channel Allocation	159
7.6.3	Consecutive Data Transmission	161
7.6.4	Multi-hop Data Transmission Control	161
7.7	Empirical Study	166
7.7.1	Single Hop Transmission.	166
7.7.2	Multi-hop Transmission.	167
7.8	Summary	170
	References	171
8	Sensor Data Fusion and Event Detection	173
8.1	Introduction	173
8.1.1	Features of Sensor Data	173
8.2	Sensor Data Fusion Techniques	175
8.2.1	Sensor Data Pre-processing	175
8.2.2	Sensor Data Mining	178
8.2.3	Sensor Data Post-processing	178
8.3	Event Detection	179
8.3.1	Threshold-based Event Detection	179
8.3.2	Tempo-Spatial Pattern Based Event Detection	180
8.4	Generic Sensor State Model.	181
8.4.1	Generic Sensor State Model.	181
8.4.2	Neighbourhood Support.	182
8.5	Sensor State Model Based Event Detection	183
8.5.1	Threshold-based Event Detection	183
8.5.2	Tempo-Spatial Pattern Based Event Detection	183
8.6	Sensor Network as a Database	184
8.7	Summary.	185
	References	185
9	WSN Security.	187
9.1	Basic Concepts of OSI Security	187
9.2	Unique Challenges in WSN Security	189
9.3	Classifications of Security Attacks on WSNs.	190
9.4	ZigBee Security Services.	191
9.4.1	Cryptography Used in ZigBee Security	192
9.4.2	ZigBee Security Keys and Trust Centre	196
9.4.3	Key-Transport and Key-Establishment	197
9.5	Typical Existing Approaches for DoS Defences	198
9.6	Preventing Low-Level Denial of Service Attacks on WSN Based Home Automation Systems.	200
9.6.1	Virtual Home: DoS Attack Monitor and Trigger	201

9.6.2	Remote Home Server and DoS Defence Server	202
9.6.3	Virtual Home: DoS Attack Mitigation Mechanism . . .	203
9.6.4	Virtual Home Placement	204
9.7	Implementation of Virtual Home Based Approach for Defencing DoS Attacks on WSN Based HASs	206
9.7.1	RHS Client	206
9.7.2	Remote Home Server	206
9.7.3	DoS Defence Server	208
9.7.4	Home Gateway	209
9.8	Evaluation	210
9.8.1	Attack Tool	210
9.8.2	Analysis of Low Level DoS Attacks on WSN Based HASs.	211
9.8.3	Analysis of Low Level DoS Attacks on the Home Gateway.	213
9.9	Summary.	214
	References	215
10	Mobile Target Localization and Tracking	217
10.1	Introduction	217
10.2	Distance Determination	218
10.2.1	Received Signal Strength Indicator.	218
10.2.2	Link Quality Indicator.	220
10.2.3	Time of Arrival	220
10.2.4	Time Difference of Arrival	221
10.3	Localization Methods	221
10.3.1	Triangulation	222
10.3.2	Fingerprint.	224
10.3.3	Centroid Localization	225
10.4	Improving Tracking Accuracy	226
10.4.1	Environment Factor	226
10.4.2	Eliminating the Outliers of Radio Signals	228
10.4.3	Evolutionary Optimization.	228
10.5	Multiple Mobile Targets Tracking	230
10.6	Case Study—Underground Tunnel Mobile Target Tracking. . .	231
10.7	Summary.	233
	References	234
11	Hybrid RFID/WSNs for Logistics Management	235
11.1	Introduction	235
11.2	RFID	235
11.2.1	RFID Tag	236
11.2.2	Reader	238

11.3	Hybrid RFID/Sensor Network	238
11.3.1	Reader as a Sensor	238
11.3.2	Tag as a Sensor	240
11.4	Generic Hybrid RFID/Sensor Network Architecture	240
11.5	Possible Use in Humanitarian Logistics Management	242
11.6	Summary	245
	References	245
12	Internet of Things	247
12.1	Introduction	247
12.2	Challenges and Features of the IoT.	248
12.3	Connecting WSNs with the Internet	250
12.3.1	Front-end Proxy Solution.	250
12.3.2	Gateway Solution	251
12.3.3	TCP/IP Overlay Solution.	252
12.4	IoT Service-Oriented Architecture	253
12.4.1	Sensor Service Publisher	255
12.4.2	Local Historical Database	255
12.4.3	Domain Sensor Name Server	255
12.4.4	Implementation Issues.	257
12.5	Possible Implementations in Emergency Response	259
12.6	Conclusions	260
	References	260
13	ZigBee Smart Home Automation Systems	263
13.1	Introduction	263
13.2	Analysis of the Existing Home Automation Systems.	264
13.3	Home Automation System Architecture.	265
13.4	System Implementation	267
13.4.1	Implementation of ZigBee Home Automation Network.	267
13.4.2	Home Gateway Implementation	268
13.4.3	Virtual Home Implementation	269
13.4.4	Home Automation Devices Developed	271
13.5	Systems Evaluation.	271
13.6	Conclusion.	273
	References	273
14	Building Fire Safety Protection: SafetyNET.	275
14.1	Introduction	275
14.2	Information Infrastructure	276
14.3	SafetyNET Specific Devices	277
14.4	Mobile Fire Tender Networks	278
14.5	SafetyNET Wireless Sensor Networks.	280

- 14.5.1 SafetyNET Coordinator 281
 - 14.5.2 SafetyNET Routers 282
 - 14.5.3 SafetyNET End-Devices 283
 - 14.5.4 SafetyNET Adaptors 285
 - 14.6 Field Trial 285
 - 14.7 Summary 285
 - References 286
- 15 Conclusion 287**
 - 15.1 Summary 287
 - 15.2 Research Opportunities for Future Development. 288
 - References 288
- Index 291**

Wireless Sensor Networks

Principles, Design and Applications

Yang, S.-H.

2014, XVII, 293 p. 175 illus., 80 illus. in color.,

Hardcover

ISBN: 978-1-4471-5504-1