

Contents

1	Introduction	1
1.1	Wireless Sensor Networks	1
1.1.1	Applications	2
1.1.2	Enabling Technologies	3
1.1.3	Constraints	5
1.2	Security Issues in Wireless Sensor Networks	7
1.2.1	Security Requirements and Related Issues	8
1.2.2	Attacks	11
1.2.3	Defensive Measures	14
1.3	Book Contributions	26
1.4	Book Overview	28
2	Pair-Wise Key Establishment	31
2.1	Introduction	31
2.2	Related Work	33
2.3	Preliminaries and Assumptions	34
2.3.1	Security Requirements and Threat Model	34
2.4	The ECCE Protocol	36
2.5	Security Analysis	39
2.5.1	Channel Existence	40
2.5.2	Channel Resilience	43
2.5.3	Probabilistic Authentication	43
2.6	Simulations and Discussion	44
2.7	Concluding Remarks	52
3	Capture Detection	53
3.1	Introduction	53
3.2	Related Work and Background	55
3.3	Node Capture Detection Through Mobility and Cooperation	58
3.3.1	Benchmark Solution	58
3.3.2	Our Approach	59
3.3.3	Assumptions and Notation	60

3.4	The Protocol	61
3.4.1	Protocol Description	61
3.5	Simulations and Discussion	64
3.5.1	Node Re-Meeting	64
3.5.2	Experimental Results	68
3.5.3	Massive Attacks	71
3.5.4	Other Mobility Patterns	71
3.6	Concluding Remarks	73
4	Clone Detection	75
4.1	Introduction	76
4.2	Related Work	77
4.3	The Threat Model	80
4.4	Requirements for the Distributed Detection Protocol	81
4.4.1	Witness Distribution	81
4.4.2	Overhead	82
4.5	The RED Protocol	83
4.6	Simulations	86
4.6.1	Witness Distribution	87
4.6.2	Storage Overhead	89
4.6.3	Energy Overhead	90
4.7	Detection Probability with Malicious Nodes	94
4.8	Concluding Remarks	100
5	Secure Data Aggregation	101
5.1	Introduction	101
5.2	Related Work	104
5.2.1	Greenwald et al.'s Approximate Median Algorithm	105
5.2.2	Chan et al.'s Verification Algorithm	106
5.3	Assumptions and Problem Description	107
5.4	Computing and Verifying an Approximate Median	109
5.4.1	GC Approach	109
5.4.2	A Histogram Verification Algorithm	110
5.4.3	Our Basic Protocol	112
5.5	Security and Performance Analysis of Our Basic Protocol	114
5.5.1	Security Analysis	114
5.5.2	Performance Analysis	115
5.6	Attack-Resilient Median Computation	117
5.6.1	Geographical Grouping	118
5.7	Simulation Results	121
5.7.1	Simulation Environment	121
5.7.2	Results and Discussion	122
5.8	Concluding Remarks	123

6 Privacy in Data Aggregation.	125
6.1 Introduction.	125
6.2 Related Work	127
6.3 Network Assumptions and Threat Model.	128
6.4 Protocol Overview	129
6.5 Twin-Key Agreement	131
6.5.1 Twin-Key Agreement: Protocol Description.	132
6.6 Data Aggregation.	136
6.6.1 Twin-Key Liveness Announcement: Protocol Description.	136
6.6.2 Data Aggregation with Shadow Values: Protocol Description.	139
6.6.3 A Complete Protocol Run.	141
6.7 Security and Complexity Analysis	141
6.7.1 Parameter Study	141
6.7.2 Security Analysis.	143
6.7.3 Complexity Analysis	150
6.7.4 Comparison.	153
6.8 Concluding Remarks	153
7 Conclusions and Future Works.	155
References.	157



<http://www.springer.com/978-1-4939-3458-4>

Secure Wireless Sensor Networks

Threats and Solutions

Conti, M.

2015, XIII, 169 p., Hardcover

ISBN: 978-1-4939-3458-4