

Contents

1	Introduction and Overview	1
1.1	WSN Security	2
1.1.1	Obstacles of WSN Security	2
1.1.2	Security Requirements	4
1.1.3	Attacks	7
1.1.4	Defensive Measures	10
1.2	Attackers Motivation	14
1.3	Research Challenges	15
1.4	Motivation of the Book	18
1.5	Contribution of the Book	20
1.6	Outline of the Book	20
	References	21
2	QoS as Means of Providing WSN Security	25
2.1	Introduction	25
2.2	QoS in Wireless Networks	27
2.2.1	QoS Concept	27
2.2.2	QoS Metrics	28
2.2.3	Security and QoS	28
2.2.4	QoS Challenges in Sensor Networks	29
2.3	Effect of Security on QoS	30
2.4	Reliability, Availability and Serviceability (RAS)	32
2.5	Calculating Availability and Probability Within WSN	34
2.6	Proposed Security Models	36
2.7	Experiment Evaluation	37
2.8	Summary	39
	References	39
3	Mathematical Model for Wireless Sensor Nodes Security	41
3.1	Introduction	41
3.2	Barrier Security	42

3.3	Problem Statement and Mathematical Model Design.	43
3.4	Formalization.	44
3.5	Ensuring Passive Resistance to Threat on Sensor Nodes	47
3.6	The Nodes Model Application	49
3.7	Summary	50
	References	51
4	Improved Feistel-Based Ciphers for Wireless Sensor	
	Network Security	53
4.1	Introduction.	53
4.2	Attacks Threats	54
4.3	The Efficiency of Existing WSN Algorithms	55
4.4	Techniques of Proposed Method	56
	4.4.1 Feistel Scheme	56
	4.4.2 Theoretical Approach of CPB	58
	4.4.3 An Improved Feistel Scheme for Block Data Transformation.	59
4.5	Comparison of CPB-Feistel Scheme Based Ciphers Versus Ciphers with No CPB	60
4.6	Summary	62
	References	62
5	The Distributed Signature Scheme (DSS) Based on RSA	65
5.1	Introduction.	65
5.2	RSA Based Secure Schemes	66
5.3	RSA Based Distributed Signature Scheme.	67
	5.3.1 Distributed Signature Features	68
	5.3.2 RSA Based Secret Key Distributions Main Approaches.	69
5.4	Our Approach on Scheme Establishment.	70
	5.4.1 Scheme Initialization	72
	5.4.2 Generation of Distributive Signature.	72
	5.4.3 Key Projection Distribution to New User	73
5.5	Summary	73
	References	74
6	Reliable Data Aggregation Protocol for Wireless	
	Sensor Networks	77
6.1	Introduction.	77
6.2	Problem Statement	79
6.3	Existing Data Aggregation Protocols.	80
6.4	Proposed Protocol	81
6.5	Security Assumptions	82

Contents	xi
6.6 Experiment Evaluation	82
6.7 Summary	83
References	84
Conclusions and Future Work	85
Bibliography	87

Security in Wireless Sensor Networks

Oreku, G.S.; Pazynyuk, T.

2016, XVII, 87 p. 20 illus., 7 illus. in color., Hardcover

ISBN: 978-3-319-21268-5