

# Table of Contents

<b>Chapter 1. Network Coding: From Theory to Practice</b> . . . . .	1
Youghourta BENFATTOUM, Steven MARTIN and Khaldoun AL AGHA	
1.1. Introduction . . . . .	1
1.2. Theoretical approach . . . . .	2
1.2.1. Max-flow min-cut . . . . .	4
1.2.2. Admissible code . . . . .	5
1.2.3. Linear code . . . . .	6
1.2.4. Algebraic resolution . . . . .	6
1.2.5. Random code . . . . .	8
1.3. Practical approach . . . . .	10
1.3.1. Topologies . . . . .	11
1.3.1.1. Multihop wireless networks . . . . .	11
1.3.1.2. Cellular networks . . . . .	18
1.3.2. Applications . . . . .	19
1.3.2.1. Network coding and TCP . . . . .	19
1.3.2.2. Network coding and P2P . . . . .	21
1.3.2.3. Network coding with priority . . . . .	22
1.4. Conclusion . . . . .	23
1.5. Bibliography . . . . .	24

<b>Chapter 2. Fountain Codes and Network Coding for WSNs</b> . . . . .	27
Anya APAVATJRUT, Claire GOURSAUD, Katia JAFFRÈS-RUNSER and Jean-Marie GORCE	
2.1. Introduction . . . . .	27
2.2. Fountain codes . . . . .	29
2.2.1. Generalities . . . . .	30
2.2.2. Families of fountain codes . . . . .	33
2.2.2.1. Random fountain codes . . . . .	33
2.2.2.2. Luby Transform (LT) . . . . .	34
2.2.2.3. Raptor code . . . . .	40
2.2.2.4. Code complexity . . . . .	41
2.3. Fountain codes in WSNs . . . . .	41
2.3.1. Implementation . . . . .	42
2.3.2. Protocol of reliability enhancement: ARQs versus fountain codes . . . . .	43
2.3.3. Discharge and overflow . . . . .	45
2.4. Fountain codes and network code for sensor networks . . . . .	49
2.4.1. Impact of network coding on the degree distribution of an LT flow . . . . .	50
2.4.1.1. XOR network coding and LT code . . . . .	50
2.4.2. Design a network code for LT code . . . . .	54
2.4.2.1. Solutions of network coding . . . . .	55
2.4.3. Application to multihop sensor networks . . . . .	58
2.4.3.1. Multihop linear networks . . . . .	58
2.4.3.2. Sensor networks . . . . .	61
2.5. Conclusion . . . . .	66
2.6. Bibliography . . . . .	67

<b>Chapter 3. Switched Code for <i>Ad Hoc</i> Networks: Optimizing the Diffusion by Using Network Coding</b> . . . . .	73
Nour KADI and Khaldoun AL AGHA	
3.1. Abstract . . . . .	73
3.2. Introduction . . . . .	74
3.3. Diffusion in <i>ad hoc</i> networks . . . . .	77
3.4. Diffusion and network coding . . . . .	78
3.5. Switched code: incorporate erasure codes with network coding . . . . .	83
3.5.1. Definitions . . . . .	84
3.5.2. Coding function of switched code . . . . .	84
3.6. Decoding function of switched code . . . . .	85
3.7. Design and analysis of a new distribution . . . . .	87
3.7.1. Analysis of switched distribution . . . . .	90
3.8. Conclusion . . . . .	96
3.9. Bibliography . . . . .	97
<b>Chapter 4. Security by Network Coding</b> . . . . .	99
Katia JAFFRÈS-RUNSER and Cédric LAURADOUX	
4.1. Introduction . . . . .	99
4.2. Attack models . . . . .	100
4.2.1. A type-II wiretap network . . . . .	102
4.2.2. A nice but curious attacker . . . . .	104
4.3. Security for a <i>wiretap network</i> . . . . .	105
4.4. Algebraic security criteria . . . . .	106
4.4.1. Note on random linear network coding . . . . .	107
4.4.2. Algebraic security . . . . .	109
4.4.3. The algebraic security criterion . . . . .	109
4.4.4. Algorithmic application of the criterion . . . . .	111
4.5. Conclusion . . . . .	112
4.6. Bibliography . . . . .	112

<b>Chapter 5. Security for Network Coding</b> . . . . .	115
Marine MINIER, Yuanyuan ZHANG and Wassim ZNAÏDI	
5.1. Introduction . . . . .	115
5.2. Attack models . . . . .	116
5.2.1. Eavesdroppers . . . . .	117
5.2.1.1. Internal eavesdroppers . . . . .	117
5.2.1.2. External eavesdroppers . . . . .	117
5.2.2. Active attackers . . . . .	118
5.2.2.1. Pollution attacks . . . . .	118
5.2.2.2. Flooding attack . . . . .	119
5.2.3. Definition of homomorphic ciphering schemes . . . . .	120
5.2.3.1. Two specific schemes . . . . .	122
5.2.3.2. Completely homomorphic encryption schemes . . . . .	123
5.2.4. Homomorphic encryption and confidentiality in network coding . . . . .	124
5.2.4.1. The case of network coding using XOR . . . . .	125
5.2.4.2. The case of network coding in general . . . . .	127
5.3. Confidentiality . . . . .	128
5.3.1. Alternatives for confidentiality . . . . .	128
5.4. Integrity and authenticity solutions . . . . .	130
5.4.1. Definitions of homomorphic MAC and homomorphic hash functions . . . . .	132
5.4.1.1. Definition . . . . .	132
5.4.1.2. Examples of such schemes . . . . .	133
5.4.2. Definition of homomorphic signature schemes . . . . .	134
5.4.2.1. Definition . . . . .	134
5.4.2.2. Examples of such schemes . . . . .	135
5.4.3. Alternatives for integrity and authenticity . . . . .	136
5.4.3.1. Polynomial method . . . . .	137

5.4.3.2. Method using checksums . . . . .	139
5.4.3.3. Overlapping MAC . . . . .	140
5.5. Conclusion . . . . .	142
5.6. Bibliography . . . . .	143

## **Chapter 6. Random Network Coding and**

<b>Matroids . . . . .</b>	<b>147</b>
Maximilien GADOULEAU	

6.1. Protocols for non-coherent communication . . .	148
6.1.1. Routing . . . . .	148
6.1.2. Random linear network coding . . . . .	149
6.1.3. Random affine network coding . . . . .	151
6.1.4. Example and comparison . . . . .	152
6.2. Transmission model based on flats of matroid . . . . .	153
6.2.1. Matroids . . . . .	153
6.2.2. Model and comments . . . . .	156
6.2.3. Matroids for SAF, RLNC, and RANC . . . . .	158
6.3. Parameters for errorless communication . . . . .	160
6.3.1. Rate, delay and throughput . . . . .	161
6.3.2. Number of independent elements received . . . . .	164
6.4. Error-correcting codes for matroids . . . . .	167
6.4.1. Operator channel and lattice distance . . . . .	168
6.4.2. Matroid codes . . . . .	170
6.4.3. Matroid codes for SAF . . . . .	171
6.5. Matroid codes for network coding . . . . .	173
6.5.1. Rank metric codes . . . . .	173
6.5.2. Matroid codes for RLNC . . . . .	175
6.5.3. Matroid codes for RANC . . . . .	177
6.6. Conclusion . . . . .	180
6.7. Bibliography . . . . .	181

<b>Chapter 7. Joint Network-Channel Coding for the Semi-Orthogonal MARC: Theoretical Bounds and Practical Design</b> . . . . .	185
Atoosa HATEFI, Antoine O. BERTHET and Raphael VISOZ	
7.1. Introduction . . . . .	185
7.1.1. Related work . . . . .	186
7.1.2. Contribution . . . . .	188
7.1.3. Chapter outline . . . . .	190
7.1.4. Notation . . . . .	191
7.2. System model . . . . .	191
7.3. Information-theoretic analysis . . . . .	195
7.3.1. Outage analysis of SOMARC/JNCC . . . . .	196
7.3.2. Outage analysis of SOMARC/SNCC . . . . .	200
7.3.3. Types of input distributions . . . . .	202
7.3.3.1. Gaussian i.i.d. inputs . . . . .	202
7.3.3.2. Discrete i.i.d. inputs . . . . .	202
7.3.4. Information outage probability achieving codebooks . . . . .	203
7.4. Joint network channel coding and decoding . . . . .	203
7.4.1. Coding at the sources . . . . .	203
7.4.2. Relaying function . . . . .	204
7.4.2.1. Relay detection and decoding . . . . .	205
7.4.2.2. JNCC . . . . .	206
7.4.3. JNCD at the destination . . . . .	208
7.4.3.1. SISO MAP detector and demapper . . . . .	208
7.4.3.2. Message-passing schedule . . . . .	209
7.5. Separate network channel coding and decoding . . . . .	212
7.6. Numerical results . . . . .	214
7.6.1. Information-theoretic comparison of the protocols . . . . .	215
7.6.1.1. Individual $\epsilon$ -outage capacity with Gaussian inputs . . . . .	215

7.6.1.2. Individual information outage probability with discrete inputs . . . . .	216
7.6.2. Performance of practical code design . . . . .	219
7.6.2.1. Comparison of JNCC functions: XOR versus general scheme . . . . .	220
7.6.2.2. Gap to outage limits . . . . .	222
7.6.2.3. Comparison of the different protocols . . . . .	224
7.7. Conclusion . . . . .	226
7.8. Appendix. MAC outage performance of high SNR . . . . .	228
7.9. Bibliography . . . . .	230
<b>Chapter 8. Robust Network Coding . . . . .</b>	<b>235</b>
Lana IWAZA, Marco Di RENZO and Michel KIEFFER	
8.1. Coherent network error-correction codes . . . . .	237
8.2. Codes for noncoherent networks, random codes . . . . .	240
8.3. Codes for noncoherent networks, subspace codes . . . . .	242
8.3.1. Principle of subspace codes . . . . .	242
8.3.2. Recent developments . . . . .	244
8.4. Joint network–channel coding/decoding . . . . .	245
8.4.1. Principle . . . . .	247
8.4.2. Recent developments . . . . .	248
8.5. Joint source–network coding/decoding . . . . .	249
8.5.1. Exploiting redundancy to combat loss . . . . .	250
8.5.1.1. Artificially introduced correlation . . . . .	250
8.5.1.2. Existing correlation . . . . .	253
8.5.2. Joint source–network coding . . . . .	254
8.6. Conclusion . . . . .	256
8.7. Acknowledgments . . . . .	257
8.8. Bibliography . . . . .	257

<b>Chapter 9. Flow Models and Optimization for Network Coding</b> . . . . .	265
Eric GOURDIN and Jeremiah EDWARDS	
9.1. Introduction . . . . .	265
9.2. Some reminders on flow problems in graphs . . . . .	267
9.3. Flow models for multicast traffic . . . . .	272
9.4. Flow models for network coding . . . . .	277
9.5. Conclusion . . . . .	284
9.6. Bibliography . . . . .	285
<b>List of Authors</b> . . . . .	289
<b>Index</b> . . . . .	291