
Contents

About the editors	xvii
Preface	xix
PART I Fundamentals of physical layer security	1
1 Secrecy metrics for physical layer security over fading channels	3
<i>Biao He, Vincent K. N. Lau, Xiangyun Zhou, and A. Lee Swindlehurst</i>	
1.1 Introduction	3
1.2 Information-theoretic secrecy	4
1.2.1 Wiretap channel model	4
1.2.2 Classical information-theoretic secrecy	4
1.2.3 Partial secrecy	5
1.3 Classical secrecy metrics for fading channels	6
1.3.1 Wireless system setup	6
1.3.2 Ergodic secrecy capacity	7
1.3.3 Secrecy outage probability	8
1.4 New secrecy metrics for quasi-static fading channels	9
1.4.1 Limitations of secrecy outage probability	10
1.4.2 New secrecy metrics: a partial secrecy perspective	10
1.5 Illustrating the use of new secrecy metrics: an example with fixed-rate wiretap codes	12
1.5.1 System model	12
1.5.2 Secrecy performance evaluation	13
1.5.3 Impact on system design	15
1.6 Conclusion	18
References	18
2 Secure data networks with channel uncertainty	21
<i>Amal Hyadi, Zouheir Rezki, and Mohamed-Slim Alouini</i>	
2.1 Introduction	21
2.2 Secure single-user transmission with channel uncertainty	23
2.2.1 System model	24
2.2.2 Wiretap channel with noisy CSIT	24
2.2.3 Wiretap channel with limited CSI feedback	28
2.3 Secure multi-user transmission with channel uncertainty	31
2.3.1 System model	31
2.3.2 Secure broadcasting with noisy CSIT	31
2.3.3 Secure broadcasting with limited CSI feedback	34

2.4	Conclusion	39
	References	40
3	Confidential and energy-efficient communications by physical layer security	43
	<i>Alessio Zappone, Pin-Hsun Lin, and Eduard A. Jorswieck</i>	
3.1	Introduction	43
3.2	Preliminaries	45
3.2.1	Physical layer security and secrecy measures	45
3.2.2	Fractional programming theory	48
3.3	Radio resource allocation for SEE maximization	49
3.3.1	MIMOME system model	49
3.3.2	Radio resource allocation for MIMOME systems	52
3.3.3	SEE maximization with QoS constraints	54
3.3.4	Radio resource allocation for MISOSE systems	55
3.4	Numerical experiments	57
3.5	Conclusions	59
	References	60
PART II	Physical layer security for multiple-antenna technologies	65
4	Antenna selection strategies for wiretap channels	67
	<i>Shihao Yan, Nan Yang, Robert Malaney, and Jinhong Yuan</i>	
4.1	Introduction	67
4.2	Single transmit antenna selection	68
4.2.1	Index of the selected antenna	68
4.2.2	Secrecy performance metrics	69
4.2.3	Secrecy performance of single TAS	70
4.3	Transmit antenna selection with Alamouti coding	74
4.3.1	Indices of the two selected antennas	74
4.3.2	Transmission with Alamouti coding	75
4.3.3	Secrecy performance of TAS-Alamouti and TAS-Alamouti-OPA	76
4.4	Antenna selection in full-duplex wiretap channels	79
4.4.1	Transmit and receive antenna switching	79
4.4.2	Secrecy performance of the full-duplex wiretap channel with antenna switching	81
4.4.3	Other antenna selection problems in full-duplex wiretap channels	83
4.5	Single TAS with imperfect feedback and correlation	84
4.5.1	Single TAS with imperfect feedback	84
4.5.2	Single TAS with antenna correlation or channel correlation	87

4.6 Conclusion	89
References	89
5 Physical layer security for massive MIMO systems	95
<i>Jun Zhu, Robert Schober, and Vijay K. Bhargava</i>	
5.1 Fundamentals of massive MIMO	95
5.1.1 Time-division duplex and uplink pilot training	96
5.1.2 Downlink linear precoding	96
5.1.3 Multi-cell deployment and pilot contamination	97
5.2 Physical layer security basics	97
5.3 Motivations	98
5.3.1 Is massive MIMO secure?	98
5.3.2 How to improve security for massive MIMO?	99
5.3.3 State-of-the-art	100
5.4 System models for secure massive MIMO	100
5.4.1 Channel estimation and pilot contamination	101
5.4.2 Downlink data and AN transmission	103
5.5 Achievable ergodic secrecy rate and secrecy outage probability for secure massive MIMO systems	104
5.5.1 Achievable ergodic secrecy rate	104
5.5.2 Secrecy outage probability analysis	108
5.6 Linear data and AN precoding in massive MIMO systems	108
5.6.1 Linear data precoders for secure massive MIMO	108
5.6.2 Linear AN precoders for secure massive MIMO	110
5.6.3 Comparison of linear data and AN precoders	111
5.6.4 Optimal power splitting	112
5.6.5 Numerical examples	112
5.7 Conclusions and future prospects	114
A.1 Appendix	115
A.1.1 Proof of Lemma 5.1	115
A.1.2 Proof of Theorem 5.1	115
A.1.3 Proof of Theorem 5.2	116
A.1.4 Proof of Proposition 5.1	117
A.1.5 Derivation of κ_{opt}	118
References	119
6 Physical layer security for massive MIMO with anti-jamming	125
<i>Tan Tai Do, Hien Quoc Ngo, and Trung Q. Duong</i>	
6.1 Introduction	125
6.1.1 Massive MIMO	125
6.1.2 Physical layer security on massive MIMO	127
6.1.3 Jamming on massive MIMO systems	128
6.2 Uplink massive MIMO with jamming	129
6.2.1 Training phase	130
6.2.2 Data transmission phase	132

6.3	Jamming-pilot contamination	132
6.4	Achievable rate	134
6.5	Anti-jamming pilot re-transmission	137
6.5.1	Estimation of $ \mathbf{s}_j^T \mathbf{s}_u^* ^2$ and $\mathbf{s}_j^* \mathbf{s}_j^T$	137
6.5.2	Pilot re-transmission under random jamming	139
6.5.3	Pilot re-transmission under deterministic jamming	140
6.5.4	Numerical examples	141
6.6	Chapter conclusion	143
	References	143
7	Physical layer security for multiuser relay networks	145
	<i>Lisheng Fan and Trung Q. Duong</i>	
7.1	AF relaying	146
7.1.1	Relay and user selection	148
7.1.2	Lower bound	149
7.1.3	Asymptotic analysis	153
7.1.4	Numerical and simulation results	155
7.2	DF relaying	156
7.2.1	User and relay selection criteria	158
7.2.2	Closed-form analysis	159
7.2.3	Asymptotic analysis	162
7.2.4	Numerical and simulation results	164
	Appendix A	165
A.1	Proof of Theorem 1	165
	Appendix B	167
B.1	Proof of Theorem 2	167
	Appendix C	168
C.1	Proof of Theorem 3	168
	References	169
8	Trusted wireless communications with spatial multiplexing	171
	<i>Giovanni Geraci and Jinhong Yuan</i>	
8.1	Introduction to multiuser MIMO systems	171
8.2	Physical layer security in an isolated cell	172
8.2.1	The broadcast channel with confidential messages	172
8.2.2	Achievable secrecy rates in the BCC	174
8.2.3	The price of secrecy	178
8.3	Physical layer security in a random field of eavesdroppers	180
8.3.1	The broadcast channel with confidential messages and external eavesdroppers	180
8.3.2	Probability of secrecy outage	182
8.3.3	Mean secrecy rates	185
8.4	Physical layer security in a multi-cell system	187
8.4.1	Cellular networks with malicious users	187

8.4.2	Achievable secrecy rates	188
8.4.3	Probability of secrecy outage and mean secrecy rate	190
8.5	Conclusions	193
	References	194
PART III	Physical layer security with emerging 5G technologies	197
9	Physical layer security for wirelessly powered communication systems	199
	<i>Caijun Zhong and Xiaoming Chen</i>	
9.1	Introduction	199
9.1.1	Background	199
9.1.2	Literature review	200
9.1.3	Organization of the chapter	201
9.2	Secrecy performance of wirelessly powered wiretap channels	201
9.2.1	System model	201
9.2.2	Secrecy performance analysis	203
9.2.3	Resource allocation	207
9.2.4	Numerical results	211
9.3	Secrecy performance of wirelessly powered wiretap channels with a friendly jammer	213
9.3.1	System model	213
9.3.2	Transmit beamforming design	215
	Case 1: Perfect CSI of both $\mathbf{h}_{pb}$ and $\mathbf{h}_{pe}$	215
	Case 2: Perfect CSI of $\mathbf{h}_{pb}$, no CSI of $\mathbf{h}_{pe}$	216
9.3.3	Performance analysis	216
	Case 1: Perfect CSI of both $\mathbf{h}_{pb}$ and $\mathbf{h}_{pe}$	216
	Case 2: Perfect CSI of $\mathbf{h}_{pb}$ and no CSI of $\mathbf{h}_{pe}$	219
9.3.4	Numerical results	220
9.4	Conclusion and future directions	222
9.4.1	Future directions	222
	References	223
10	Physical layer security for D2D-enabled cellular networks	227
	<i>Chuan Ma, Jianting Yue, Hui Yu, and Xiaoying Gan</i>	
10.1	D2D communication in cellular networks	227
10.2	Physical layer security for D2D-enabled cellular networks	229
10.2.1	Securing cellular communication against third-party eavesdroppers	229
10.2.2	Securing cellular communication against D2D-type eavesdroppers	230
10.2.3	Securing D2D communication	230
10.2.4	Securing both cellular and D2D communications	231
10.2.5	Physical layer security in different communication modes	231

10.3	Secure transmission schemes for small-scale D2D-enabled cellular networks	231
10.3.1	System model	231
10.3.2	Optimal D2D link scheduling scheme	232
10.4	Secure transmission schemes for large-scale D2D-enabled cellular networks	234
10.4.1	Network model	234
10.4.2	Secrecy transmission in large-scale D2D-enabled cellular networks	236
10.4.3	Optimal D2D link scheduling schemes under the strong criterion	242
10.4.4	Optimal D2D link scheduling schemes under the weak criterion	245
10.5	Summary	249
	References	249
11	Physical layer security for cognitive radio networks	253
	<i>Van-Dinh Nguyen, Trung Q. Duong, and Oh-Soon Shin</i>	
11.1	Introduction	253
11.2	PHY-security of primary system	254
11.2.1	System model	255
11.2.2	Ergodic secrecy capacity of the primary system	257
11.2.3	Numerical results	261
11.3	PHY-security of secondary system	261
11.3.1	System model and problem formulation	262
11.3.2	Optimization problem design	265
11.3.3	Optimization over Γ_{tol}	269
11.3.4	Numerical results	271
11.4	PHY-security of cooperative cognitive radio networks	273
11.4.1	System model	273
11.4.2	Optimization approach for beamforming of ST	274
11.4.3	Optimization with transmit power of PT	278
11.4.4	Numerical results	278
11.5	Conclusions	280
	References	280
12	Physical layer security in mmWave cellular networks	285
	<i>Hui-Ming Wang</i>	
12.1	Introduction	285
12.2	System model and problem formulation	287
12.2.1	mmWave cellular system	287
12.2.2	Secrecy performance metrics	290

12.3	Secrecy performance of millimetre wave cellular networks	291
12.3.1	Non-colluding eavesdroppers	292
12.3.2	Colluding eavesdroppers	295
12.4	Simulation result	299
12.5	Conclusions	302
A.1	Appendix A	302
B.2	Appendix B	302
C.3	Appendix C	303
D.4	Appendix D	304
E.5	Appendix E	305
	References	307
PART IV Physical layer security with emerging modulation technologies		311
13	Directional-modulation-enabled physical-layer wireless security	313
	<i>Yuan Ding and Vincent Fusco</i>	
13.1	Directional modulation (DM) concept	313
13.2	DM transmitter architectures	315
13.2.1	Near-field direct antenna modulation	315
13.2.2	DM using re-configurable antennas in an array configuration	316
13.2.3	DM using phased antenna array	316
13.2.4	DM using Fourier beamforming networks	317
13.2.5	DM using switched antenna arrays	317
13.2.6	DM using digital baseband	317
13.3	Mathematical model for DM	318
13.4	Synthesis approaches for DM transmitters	321
13.4.1	Orthogonal vector approach for DM synthesis	322
13.4.2	Other DM synthesis approaches	325
13.4.3	A note on synthesis-free DM transmitters	326
13.5	Assessment metrics for DM systems	328
13.6	Extensions to the DM technique	328
13.6.1	Multi-beam DM	329
13.6.2	DM in a multi-path environment	330
13.7	DM demonstrators	331
13.8	Conclusions and recommendations for future studies on DM	331
	References	333
14	Secure waveforms for 5G systems	337
	<i>Stefano Tomasin</i>	
14.1	Secret transmission over parallel channels	338
14.1.1	Single user case	338

14.1.2	Multiple users case	342
14.1.3	Downlink with common message	345
14.2	Secret key agreement	347
14.2.1	Channel-model SKA over parallel channels	348
14.2.2	Source-model SKA over parallel channels	351
14.3	Waveforms peculiarities	353
14.3.1	OFDM	353
14.3.2	SC-FDMA	357
14.3.3	GFDM	357
14.3.4	UFMC	358
14.3.5	FBMC	358
14.3.6	Performance comparison	360
	References	361
15	Physical layer security in non-orthogonal multiple access	365
	<i>Hui-Ming Wang, Yi Zhang, and Zhiguo Ding</i>	
15.1	Introduction	365
15.2	Preliminary analysis of the secure performance of SISO NOMA systems	367
15.2.1	System model	367
15.2.2	Maximisation of the sum of secrecy rates	370
15.2.3	Simulation results	376
15.3	Secure transmissions realised by a multi-antenna jammer	378
15.3.1	System model	378
15.3.2	Secure transmissions based on secrecy rate guarantees	381
15.3.3	Simulation results	385
15.4	Conclusions and open issues	386
	References	387
16	Physical layer security for MIMOME-OFDM systems: spatial versus temporal artificial noise	391
	<i>Ahmed El Shafie, Zhiguo Ding, and Naofal Al-Dhahir</i>	
16.1	Introduction	391
16.2	Preliminary	393
16.2.1	Spatial AN	393
16.2.2	Temporal AN	394
16.3	System model and artificial noise design	395
16.3.1	System model and assumptions	395
16.3.2	Proposed hybrid spatio-temporal AN-aided scheme	395
16.3.3	Received signal vector at Bob	397
16.3.4	Design of Alice's data precoder matrix and Bob's receive filter matrix	399
16.3.5	Design of Alice's temporal and spatial AN precoders	399
16.3.6	Received signal vector at Eve	400

16.4	Average secrecy rate	400
16.4.1	Asymptotic average rates in MIMOME-OFDM channels	402
16.4.2	Temporal AN versus spatial AN	405
16.5	Simulation results	406
16.6	Conclusions	409
A.1	Appendices	409
A.1.1	Proof of Lemma 16.1	409
A.1.2	Distribution of $\mathbf{F}_{NE} \tilde{\mathbf{G}}_{\text{toep}}$	411
A.1.3	Distributions of $\mathbf{G}_k \mathbf{A}_k \mathbf{A}_k^* \mathbf{G}_k^*$ and $\mathbf{H}_k \mathbf{A}_k \mathbf{A}_k^* \mathbf{H}_k^*$	412
A.1.4	Proof of Lemma 16.2	413
A.1.5	Proof of Lemma 16.3	413
A.1.6	Proof of Lemma 16.4	414
A.1.7	Proof of Lemma 16.6	416
A.1.8	Proof of Lemma 16.7	417
	References	418
PART V	Applications of physical layer security	421
17	Physical layer security for real-world applications: use cases, results and open challenges	423
	<i>Stephan Ludwig, René Guillaume, and Andreas Müller</i>	
17.1	Introduction	423
17.1.1	Why physical layer security?	423
17.1.2	Flavours of physical layer security	425
17.1.3	Use cases and major requirements	425
17.1.4	Comparison to alternative key establishment schemes	427
17.2	Fundamentals	428
17.2.1	Information-theoretic foundation	428
17.2.2	General system architecture	429
17.2.3	Major metrics for performance evaluation	430
17.3	Channel-based key generation in practice	431
17.3.1	Channel characterization	431
17.3.2	Pre-processing	435
17.3.3	Quantization	436
17.3.4	Information reconciliation	436
17.3.5	Entropy estimation	437
17.3.6	Privacy amplification and key verification	437
17.3.7	Security considerations and energy consumption of CBKG	437
17.4	Experimental results	438
17.4.1	CSI-based experiments	439
17.4.2	RSSI-based experiments	443
17.5	Further aspects	446
17.5.1	Missing building blocks	446
17.5.2	Sensor-assisted authentication	448

17.5.3 Physical layer security for wireline systems	449
17.6 Summary and outlook	451
References	452
18 Key generation from wireless channels: a survey and practical implementation	457
<i>Junqing Zhang, Trung Q. Duong, Roger Woods, and Alan Marshall</i>	
18.1 Introduction	457
18.2 A survey of wireless key generation	458
18.2.1 Principles	458
18.2.2 Evaluation metrics	459
18.2.3 Key generation procedure	460
18.2.4 Channel parameters	463
18.3 Case study: practical implementation of an RSS-based key generation system	464
18.3.1 Preliminary	464
18.3.2 Measurement system and test scenario	466
18.3.3 Experiment results	467
18.4 Conclusion	470
References	470
19 Application cases of secret key generation in communication nodes and terminals	475
<i>Christiane Kameni Ngassa, Taghrid Mazloum, François Delaveau, Sandrine Boumard, Nir Shapira, Renaud Molière, Alain Sibille, Adrian Kotelba, and Jani Suomalainen</i>	
19.1 Introduction	475
19.2 Fundamental aspects of secret key generation	476
19.2.1 Channel-based random bit generators	477
19.2.2 Metrics for secret key generation assessment	478
19.2.3 Impact of channel characteristics	479
19.3 Integration of secret key generation into existing radio access technologies	482
19.3.1 Practical secret key generation scheme	482
19.3.2 Simulation results from single sense recorded signals	485
19.3.3 Simulation results from dual sense LTE signals	487
19.3.4 Experimental results from dual sense WiFi signals	492
19.4 Conclusion: security upgrades opportunities for radio access technologies	496
19.4.1 Existing vulnerabilities	496
19.4.2 Proposed solutions for securing radio access protocols with secret key generation	497

19.4.3 Practical usage of secret key generation into radio access technologies	498
References	499
20 Application cases of secrecy coding in communication nodes and terminals	501
<i>Christiane Kameni Ngassa, Cong Ling, François Delaveau, Sandrine Boumard, Nir Shapira, Ling Liu, Renaud Molière, Adrian Kotelba, and Jani Suomalainen</i>	
20.1 Introduction	501
20.2 Theoretical aspects of secrecy coding	502
20.2.1 Wiretap coding for discrete wiretap channels	502
20.2.2 Wiretap coding for Gaussian wiretap channels	506
20.2.3 Wiretap coding for MIMO and fading channels	509
20.3 Integration of secrecy-coding techniques into existing radio access technologies	512
20.3.1 Radio advantage establishment—case of MIMO transmission	512
20.3.2 Description of the practical secrecy-coding scheme	514
20.3.3 Performance analysis of designed secrecy codes	516
20.3.4 Simulation results on LTE signals	518
20.3.5 Experimental results on WiFi signals	520
20.3.6 Tuning of the radio advantage for OFDM/QPSK wave forms such as WiFi and LTE signals—considerations on radio engineering	525
20.4 Conclusion: security upgrades provided to future radio access technologies	526
References	528
Index	533