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
   Biao He, Vincent K. N. Lau, Xiangyun Zhou, and A. Lee Swindlehurst
   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 12
      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
   Amal Hyadi, Zouheir Rezki, and Mohamed-Slim Alouini
   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
References 39
40

3 Confidential and energy-efficient communications by physical layer security 43
Alessio Zappone, Pin-Hsun Lin, and Eduard A. Jorswieck
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
Shihao Yan, Nan Yang, Robert Malaney, and Jinhong Yuan
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
5 **Physical layer security for massive MIMO systems**  
*Jun Zhu, Robert Schober, and Vijay K. Bhargava*

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Fundamentals of massive MIMO</td>
<td>95</td>
</tr>
<tr>
<td>5.1.1 Time-division duplex and uplink pilot training</td>
<td>96</td>
</tr>
<tr>
<td>5.1.2 Downlink linear precoding</td>
<td>96</td>
</tr>
<tr>
<td>5.1.3 Multi-cell deployment and pilot contamination</td>
<td>97</td>
</tr>
<tr>
<td>5.2 Physical layer security basics</td>
<td>97</td>
</tr>
<tr>
<td>5.3 Motivations</td>
<td>98</td>
</tr>
<tr>
<td>5.3.1 Is massive MIMO secure?</td>
<td>98</td>
</tr>
<tr>
<td>5.3.2 How to improve security for massive MIMO?</td>
<td>99</td>
</tr>
<tr>
<td>5.3.3 State-of-the-art</td>
<td>100</td>
</tr>
<tr>
<td>5.4 System models for secure massive MIMO</td>
<td>100</td>
</tr>
<tr>
<td>5.4.1 Channel estimation and pilot contamination</td>
<td>101</td>
</tr>
<tr>
<td>5.4.2 Downlink data and AN transmission</td>
<td>103</td>
</tr>
<tr>
<td>5.5 Achievable ergodic secrecy rate and secrecy outage probability for</td>
<td>104</td>
</tr>
<tr>
<td>secure massive MIMO systems</td>
<td>104</td>
</tr>
<tr>
<td>5.5.1 Achievable ergodic secrecy rate</td>
<td>104</td>
</tr>
<tr>
<td>5.5.2 Secrecy outage probability analysis</td>
<td>108</td>
</tr>
<tr>
<td>5.6 Linear data and AN precoding in massive MIMO systems</td>
<td>108</td>
</tr>
<tr>
<td>5.6.1 Linear data precoders for secure massive MIMO</td>
<td>108</td>
</tr>
<tr>
<td>5.6.2 Linear AN precoders for secure massive MIMO</td>
<td>110</td>
</tr>
<tr>
<td>5.6.3 Comparison of linear data and AN precoders</td>
<td>111</td>
</tr>
<tr>
<td>5.6.4 Optimal power splitting</td>
<td>112</td>
</tr>
<tr>
<td>5.6.5 Numerical examples</td>
<td>112</td>
</tr>
<tr>
<td>5.7 Conclusions and future prospects</td>
<td>114</td>
</tr>
<tr>
<td>A.1 Appendix</td>
<td>115</td>
</tr>
<tr>
<td>A.1.1 Proof of Lemma 5.1</td>
<td>115</td>
</tr>
<tr>
<td>A.1.2 Proof of Theorem 5.1</td>
<td>115</td>
</tr>
<tr>
<td>A.1.3 Proof of Theorem 5.2</td>
<td>116</td>
</tr>
<tr>
<td>A.1.4 Proof of Proposition 5.1</td>
<td>117</td>
</tr>
<tr>
<td>A.1.5 Derivation of $\kappa_{opt}$</td>
<td>118</td>
</tr>
</tbody>
</table>

References

6 **Physical layer security for massive MIMO with anti-jamming**  
*Tan Tai Do, Hien Quoc Ngo, and Trung Q. Duong*

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Introduction</td>
<td>125</td>
</tr>
<tr>
<td>6.1.1 Massive MIMO</td>
<td>125</td>
</tr>
<tr>
<td>6.1.2 Physical layer security on massive MIMO</td>
<td>127</td>
</tr>
<tr>
<td>6.1.3 Jamming on massive MIMO systems</td>
<td>128</td>
</tr>
<tr>
<td>6.2 Uplink massive MIMO with jamming</td>
<td>129</td>
</tr>
<tr>
<td>6.2.1 Training phase</td>
<td>130</td>
</tr>
<tr>
<td>6.2.2 Data transmission phase</td>
<td>132</td>
</tr>
</tbody>
</table>
PART III Physical layer security with emerging 5G technologies

9 Physical layer security for wirelessly powered communication systems

Caijun Zhong and Xiaoming Chen

9.1 Introduction

9.2 Secrecy performance of wirelessly powered wiretap channels

9.3 Secrecy performance of wirelessly powered wiretap channels with a friendly jammer

9.4 Conclusion and future directions

References

10 Physical layer security for D2D-enabled cellular networks

Chuan Ma, Jianting Yue, Hui Yu, and Xiaoying Gan

10.1 D2D communication in cellular networks

10.2 Physical layer security for D2D-enabled cellular networks

10.2.1 Securing cellular communication against third-party eavesdroppers

10.2.2 Securing cellular communication against D2D-type eavesdroppers

10.2.3 Securing D2D communication

10.2.4 Securing both cellular and D2D communications

10.2.5 Physical layer security in different communication modes

References
10.3 Secure transmission schemes for small-scale D2D-enabled cellular networks
   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
   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
   Van-Dinh Nguyen, Trung Q. Duong, and Oh-Soon Shin
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 $\Gamma_{\text{tol}}$ 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
   Hui-Ming Wang
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
PART IV Physical layer security with emerging modulation technologies 311

13 Directional-modulation-enabled physical-layer wireless security 313
Yuan Ding and Vincent Fusco

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
Stefano Tomasin

14.1 Secret transmission over parallel channels 338
   14.1.1 Single user case 338
14.1.2 Multiple users case \hspace{1cm} 342
14.1.3 Downlink with common message \hspace{1cm} 345
14.2 Secret key agreement \hspace{1cm} 347
  14.2.1 Channel-model SKA over parallel channels \hspace{1cm} 348
  14.2.2 Source-model SKA over parallel channels \hspace{1cm} 351
14.3 Waveforms peculiarities \hspace{1cm} 353
  14.3.1 OFDM \hspace{1cm} 353
  14.3.2 SC-FDMA \hspace{1cm} 357
  14.3.3 GFDM \hspace{1cm} 357
  14.3.4 UFMC \hspace{1cm} 358
  14.3.5 FBMC \hspace{1cm} 358
  14.3.6 Performance comparison \hspace{1cm} 360
References \hspace{1cm} 361

15 Physical layer security in non-orthogonal multiple access \hspace{1cm} 365
  Hui-Ming Wang, Yi Zhang, and Zhiguo Ding
15.1 Introduction \hspace{1cm} 365
15.2 Preliminary analysis of the secure performance of SISO NOMA systems \hspace{1cm} 367
  15.2.1 System model \hspace{1cm} 367
  15.2.2 Maximisation of the sum of secrecy rates \hspace{1cm} 370
  15.2.3 Simulation results \hspace{1cm} 376
15.3 Secure transmissions realised by a multi-antenna jammer \hspace{1cm} 378
  15.3.1 System model \hspace{1cm} 378
  15.3.2 Secure transmissions based on secrecy rate guarantees \hspace{1cm} 381
  15.3.3 Simulation results \hspace{1cm} 385
15.4 Conclusions and open issues \hspace{1cm} 386
References \hspace{1cm} 387

16 Physical layer security for MIMOME-OFDM systems: spatial versus temporal artificial noise \hspace{1cm} 391
  Ahmed El Shafie, Zhiguo Ding, and Naofal Al-Dhahir
16.1 Introduction \hspace{1cm} 391
16.2 Preliminary \hspace{1cm} 393
  16.2.1 Spatial AN \hspace{1cm} 393
  16.2.2 Temporal AN \hspace{1cm} 394
16.3 System model and artificial noise design \hspace{1cm} 395
  16.3.1 System model and assumptions \hspace{1cm} 395
  16.3.2 Proposed hybrid spatio-temporal AN-aided scheme \hspace{1cm} 395
  16.3.3 Received signal vector at Bob \hspace{1cm} 397
  16.3.4 Design of Alice’s data precoder matrix and Bob’s receive filter matrix \hspace{1cm} 399
  16.3.5 Design of Alice’s temporal and spatial AN precoders \hspace{1cm} 399
  16.3.6 Received signal vector at Eve \hspace{1cm} 400
PART V  Applications of physical layer security

17  Physical layer security for real-world applications: use cases, results and open challenges

Stephan Ludwig, René Guillaume, and Andreas Müller

17.1  Introduction

17.2  Fundamentals

17.3  Channel-based key generation in practice

17.4  Experimental results

17.5  Further aspects
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.5.3</td>
<td>Physical layer security for wireline systems</td>
<td>449</td>
</tr>
<tr>
<td>17.6</td>
<td>Summary and outlook</td>
<td>451</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>452</td>
</tr>
</tbody>
</table>

18 Key generation from wireless channels: a survey and practical implementation 457
Junqing Zhang, Trung Q. Duong, Roger Woods, and Alan Marshall

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
Christiane Kameni Ngassa, Taghrid Mazloum, François Delaveau, Sandrine Boumard, Nir Shapira, Renaud Molière, Alain Sibille, Adrian Kotelba, and Jani Suomalainen

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
20 Application cases of secrecy coding in communication nodes and terminals 501
Christiane Kameni Ngassa, Cong Ling, François Delaveau, Sandrine Boumard, Nir Shapira, Ling Liu, Renaud Molière, Adrian Kotelba, and Jani Suomalainen

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