

# Table of Contents

<b>Preface</b>	<b>ix</b>
<b>I Part I</b>	<b>1</b>
<b>1 Jamming Attacks Detection and Classification in Cognitive UAV Radios</b>	<b>3</b>
<i>Ali Krayani, Lucio Marcenaro, Carlo Regazzoni</i>	
1.1 Introduction . . . . .	3
1.2 System Model . . . . .	5
1.3 Problem Formulation . . . . .	7
1.4 Proposed Automatic Jamming Modulation Classification (AJMC) . . . . .	8
1.4.1 Radio Environment Representation . . . . .	8
1.4.2 Learning Stage . . . . .	9
1.4.3 Testing Stage . . . . .	11
1.4.4 Multi-level Abnormality Measurements and Generalized Errors . . . . .	13
1.4.5 Extract Jammer and Learn the Corresponding Dynamic Model . . . . .	15
1.4.6 On-line Automatic Jamming Modulation Classification (AJC) . . . . .	16
1.5 Simulation Results and Discussion . . . . .	17
1.5.1 Simulation Setup . . . . .	17
1.5.2 Learning Reference Model and Jamming Models . . . . .	18
1.5.3 Online Classification Process . . . . .	21
1.6 Conclusion . . . . .	25
Bibliography . . . . .	26
<b>2 Physical and MAC Layer Techniques for Secure Positioning in Navigation Satellite Systems</b>	<b>29</b>
<i>Francesco Ardizzone, Laura Crosara, Nicola Laurenti, Stefano Tomasin</i>	
2.1 Introduction . . . . .	29
2.2 Attacks and Threats Against GNSS . . . . .	30
2.2.1 Jamming . . . . .	31
2.2.2 Spoofing . . . . .	31
2.3 Authentication Techniques . . . . .	32
2.3.1 System Side Authentication Techniques . . . . .	32
2.3.2 Receiver Side Anti-Spoofing Techniques . . . . .	38
2.4 Challenges and Perspectives for Cross-Authentication Techniques . . . . .	39
2.4.1 Timing Based Authentication Cross-Check . . . . .	39
2.4.2 Ranging Based Authentication Cross-Check . . . . .	40

2.4.3	Remarks on the Cross-Authentication Checks . . . . .	41
2.5	Timing Assurance Techniques . . . . .	42
2.5.1	Time Spoofing Attacks Against Timing Services . . . . .	42
2.5.2	Time Spoofing Detection Solutions . . . . .	43
2.6	Concluding Remarks . . . . .	43
	Bibliography . . . . .	44
<b>3</b>	<b>Physical Layer Security and Authentication with Practical Transmissions</b>	<b>49</b>
	<i>Linda Senigagliaesi, Marco Baldi, Ennio Gambi, Franco Chiaraluce</i>	
3.1	Introduction . . . . .	49
3.2	Confidentiality at the Physical Layer . . . . .	50
3.2.1	physical layer security (PLS) Notions and Metrics . . . . .	51
3.2.2	Application to Practical Transmissions . . . . .	53
3.2.3	Dealing with Partial Secrecy . . . . .	57
3.3	Authentication at the Physical Layer . . . . .	61
3.3.1	System Model . . . . .	62
3.3.2	Statistical Methods . . . . .	63
3.3.3	Machine Learning-based Methods . . . . .	64
3.3.4	Numerical Results . . . . .	64
3.4	Application to Cooperative Communications . . . . .	65
3.4.1	Cooperative PLS . . . . .	66
3.4.2	Authentication with Cooperative Communications . . . . .	69
3.5	Conclusion . . . . .	70
	Bibliography . . . . .	70
<b>4</b>	<b>Sensing and Privacy in Future Telecommunication Networks: a Joint Perspective</b>	<b>77</b>
	<i>Francesco Gringoli, Renato Lo Cigno, Marco Cominelli, Lorenzo Ghio</i>	
4.1	Introduction . . . . .	78
4.2	Scenarios, Applications, and Threats . . . . .	80
4.3	Principles of Sensing . . . . .	82
4.4	Principles of Obfuscation . . . . .	83
4.5	Transmitter-Side Pre-Distorsion . . . . .	84
4.6	SDR based Proof of Concept . . . . .	86
4.6.1	Resistance to AI-Localization . . . . .	89
4.6.2	BASE: Multi-Devices Experiments . . . . .	91
4.6.3	Communication Performance . . . . .	93
4.6.4	MIMO: Localizing with MIMO Devices . . . . .	95
4.6.5	OCTOPUS and FRANKENSTEIN: Impact of Devices and Antenna Position . . . . .	95
4.7	Implementation in 802.11n (openwifi) . . . . .	96
4.7.1	Resistance to AI-Localization (in openwifi) . . . . .	98
4.7.2	Communication Performance (in openwifi) . . . . .	100
4.8	RIS-based Protection . . . . .	102
4.9	Conclusions and Perspectives . . . . .	103
	Bibliography . . . . .	104

<b>5</b>	<b>Location Security in the Digital Era: Threats Detection, Analysis, and Mitigation Strategies</b>	<b>111</b>
	<i>Stefania Bartoletti, Ivan Palamà, Giuseppe Bianchi, Nicola Blefari Melazzi, Danilo Orlando</i>	
5.1	Introduction . . . . .	111
5.2	Malicious Attacks in 4G/5G Networks . . . . .	112
5.2.1	State-of-the-Art . . . . .	113
5.3	Location Spoofing: Threat Models and Bounds . . . . .	115
5.3.1	Formal Model . . . . .	116
5.3.2	Error Model for the Spoofing Attack . . . . .	117
5.3.3	Threat Model Example Case Study: Range-based Localization using RSSI	118
5.3.4	Error Bound under Spoofing Attack . . . . .	118
5.3.5	Case Study . . . . .	118
5.4	Spoofing and Jammer Detection Algorithms for Location Data . . . . .	121
5.4.1	Sensor model and problem formulations . . . . .	121
5.4.2	Noise-like Jammer Detectors . . . . .	121
5.4.3	Spoofing Detection Architectures . . . . .	123
5.4.4	Spoofing Detector: Uncorrelated Measurements . . . . .	124
5.4.5	Spoofing Detector: Correlated Measurements . . . . .	125
5.5	An Application: Location Security . . . . .	125
5.5.1	Simulation Setting and Operating Scenarios . . . . .	126
5.5.2	Performance of the BBNJ Detection Architectures . . . . .	127
5.5.3	Performance of the Spoofing Detection Architectures . . . . .	129
5.6	Conclusion . . . . .	131
	Bibliography . . . . .	132
<b>6</b>	<b>A Cybersecurity Framework for Securing Digital Service Chains</b>	<b>139</b>
	<i>G. Grieco, D. Striccoli, M. Repetto, A. Carrega, L. A. Grieco, R. Bolla, G. Piro, G. Boggia</i>	
6.1	Introduction . . . . .	139
6.2	Related Work . . . . .	141
6.3	The Reference Architecture . . . . .	141
6.4	Security Operations . . . . .	146
6.5	Module implementation . . . . .	148
6.6	Performance Analysis . . . . .	150
6.6.1	Elapsed Time for Service Authentication and Authorization . . . . .	151
6.6.2	Latency Overhead in Message Reception . . . . .	152
6.6.3	Resource Consumption . . . . .	154
6.7	Conclusions . . . . .	155
	Bibliography . . . . .	156
<b>7</b>	<b>Internet of Things Security Issues in LoRaWAN and Bluetooth Low Energy</b>	<b>159</b>
	<i>Andrea Lacava, Pierluigi Locatelli, Pietro Spadaccino, Francesca Cuomo</i>	
7.1	Introduction . . . . .	159
7.2	Low Power Technologies for Internet of things (IoT) . . . . .	160
7.2.1	LoRaWAN in a Nutshell . . . . .	160
7.2.2	Security in Bluetooth Low Energy (BLE) Mesh Networks . . . . .	162

7.3	Privacy Issues in LoRaWAN . . . . .	163
7.3.1	Privacy-Monitoring Methodologies for LoRaWAN . . . . .	164
7.3.2	Features Modelling . . . . .	166
7.3.3	Detection Procedure . . . . .	167
7.3.4	Metrics for Network Operators . . . . .	169
7.3.5	Countermeasures . . . . .	170
7.3.6	Performance Evaluation . . . . .	170
7.4	Hijacking Downlink Path Selection in LoRaWAN . . . . .	172
7.4.1	Attack Identification . . . . .	172
7.4.2	TWR Attack . . . . .	173
7.4.3	Effects . . . . .	174
7.4.4	Results . . . . .	177
7.5	Identification of DoS Attacks in BLE . . . . .	179
7.5.1	Intrusion Detection System (IDS) Architecture and Working . . . . .	180
7.5.2	Data Collection . . . . .	182
7.5.3	Results and Performance Evaluation . . . . .	185
7.6	Conclusions . . . . .	186
	Bibliography . . . . .	187
<b>8</b>	<b>Trustworthy Task Allocation in IoT: a Cognitive Game-Theoretical Use Case</b>	<b>191</b>
	<i>Virginia Pilloni, Marco Martalò, Luigi Atzori</i>	
8.1	Introduction . . . . .	191
8.2	Related Work . . . . .	192
8.3	System Model . . . . .	193
8.4	Malicious Attacks: a Use Case . . . . .	195
8.4.1	Spectrum Sensing in Malicious Cognitive IoT . . . . .	196
8.4.2	Cluster Node Bidding . . . . .	198
8.5	Simulation Results . . . . .	199
8.6	Concluding Remarks . . . . .	202
	Bibliography . . . . .	202
<b>III</b>	<b>Part III</b>	<b>207</b>
<b>9</b>	<b>Video Deepfake Detection by Identity Analysis</b>	<b>209</b>
	<i>Davide Cozzolino, Giovanni Poggi, Luisa Verdoliva</i>	
9.1	Introduction . . . . .	209
9.2	Video-based Identity Approach . . . . .	212
9.2.1	Feature Extraction . . . . .	212
9.2.2	Temporal ID Network . . . . .	213
9.2.3	3DMM Generative Network . . . . .	214
9.2.4	Identification . . . . .	215
9.3	Experimental Results . . . . .	215
9.3.1	Experimental Setup . . . . .	216
9.3.2	Ablation Study . . . . .	216
9.3.3	Comparisons to State of the Art . . . . .	217
9.3.4	Generalization and Robustness Analysis . . . . .	218

9.3.5	Visualization of the Embedded Vectors . . . . .	220
9.3.6	Robustness to Different Contexts . . . . .	220
9.3.7	A Real Case on the Web . . . . .	221
9.4	Conclusion . . . . .	221
9.5	Acknowledgment . . . . .	223
	Bibliography . . . . .	223
<b>10</b>	<b>Detecting Audio Deepfakes using Semantic Traces</b>	<b>227</b>
	<i>Davide Salvi, Clara Borrelli, Sara Mandelli, Paolo Bestagini, Stefano Tubaro</i>	
10.1	Introduction . . . . .	227
10.2	Synthetic Speech Detection Using Semantic Traces . . . . .	228
10.2.1	Problem Formulation . . . . .	229
10.2.2	Synthetic Speech Detection Through Emotion Recognition . . . . .	229
10.2.3	Synthetic Speech Detection Through Automatic Speaker Verification and Prosody Features . . . . .	231
10.3	Experimental Setup . . . . .	233
10.3.1	Dataset Description . . . . .	233
10.3.2	Considered Baseline . . . . .	235
10.3.3	Emotion-based Detector Setup . . . . .	235
10.3.4	Prosody-Speaker-based Detector Setup . . . . .	236
10.4	Results . . . . .	237
10.4.1	Emotion Detector Results . . . . .	237
10.4.2	ProsoSpeaker Detector Results . . . . .	238
10.4.3	Comparison between Emotion and ProsoSpeaker detectors . . . . .	242
10.5	Conclusions . . . . .	242
	Bibliography . . . . .	243
<b>11</b>	<b>A Hybrid Architecture for the Classification and Localization of GAN-generated Images with Improved Robustness and Generalization Capabilities</b>	<b>247</b>
	<i>Jun Wang, Benedetta Tondi, Mauro Barni</i>	
11.1	Introduction . . . . .	247
11.2	The Proposed Hybrid Architecture . . . . .	248
11.3	Detection of GAN-generated Flood Images . . . . .	250
11.3.1	Dataset Construction . . . . .	250
11.3.2	Experimental Setting . . . . .	252
11.4	Classification of GAN Face Editing . . . . .	258
11.4.1	Portrait Face Manipulation Dataset . . . . .	259
11.4.2	Experimental Setting . . . . .	259
11.4.3	Results . . . . .	263
11.5	Conclusion . . . . .	264
	Bibliography . . . . .	264
<b>12</b>	<b>Container and Content-based Media Signatures for Open-World Multimedia Foren- sics</b>	<b>271</b>
	<i>D. Baracchi, D. Shullani, A. Montibeller, M. Iuliani, C. Pasquini, G. Boato, A. Piva, F. De Natale</i>	
12.1	Introduction . . . . .	271
12.2	Proposed Open-World Forensic Framework . . . . .	273

12.2.1	Media Signature Encoder . . . . .	275
12.3	Experimental Setup . . . . .	276
12.3.1	Datasets . . . . .	277
12.3.2	Features . . . . .	280
12.3.3	Experiments . . . . .	281
12.4	System Usability . . . . .	284
12.4.1	System Scalability . . . . .	285
12.5	Conclusions . . . . .	288
	Bibliography . . . . .	289