

Contents

1	Introduction	1
1.1	Background and Motivation	1
1.2	Contributions	2
1.3	Outline of the Book	3
	References	4
2	Feasibility of Launching User Spoofing	5
	References	6
3	Attack Detection Model	7
3.1	Formulation of Attack Detection	8
3.2	Theoretical Analysis of the Spatial Correlation of RSS	8
3.3	Detection Philosophy	11
3.4	Experimental Methodology	13
3.4.1	Experimental Setup	13
3.4.2	Metrics	14
3.5	Performance Evaluation	16
3.5.1	Impact of Threshold and Sampling Number	16
3.5.2	Handling Different Transmission Power Levels	16
3.5.3	Performance of Detection	19
3.5.4	Impact of Distance Between the Spoofing Node and the Original Node	19
3.6	Summary	21
	References	21
4	Detection and Localizing Multiple Spoofing Attackers	23
4.1	Problem Formulation	24
4.2	Attacker Number Determination	25
4.2.1	Silhouette Plot	25
4.2.2	System Evolution	27
4.2.3	The SILENCE Mechanism	29
4.2.4	Support Vector Machines Based Mechanism	33

- 4.3 Localizing Adversaries 35
 - 4.3.1 Framework 35
 - 4.3.2 Algorithms 36
 - 4.3.3 Experimental Evaluation 40
- 4.4 Summary 40
- References 41
- 5 Detecting Mobile Agents Using Identity Fraud 43**
 - 5.1 Motivation 43
 - 5.2 Detection System Approach 44
 - 5.2.1 Attack Model 44
 - 5.2.2 DEMOTE System Overview 44
 - 5.2.3 RSS Partitioning 45
 - 5.2.4 Trace Reconstruction 49
 - 5.2.5 Correlation Coefficient Calculation 50
 - 5.3 Experimental Evaluation 53
 - 5.3.1 Experimental Methodology 53
 - 5.3.2 Detection in Signal Space 55
 - 5.3.3 Detection in Physical Space 61
 - 5.4 Summary 64
 - References 65
- 6 Related Work 67**
 - References 68
- 7 Conclusions and Future Work 71**



<http://www.springer.com/978-3-319-07355-2>

Pervasive Wireless Environments: Detecting and
Localizing User Spoofing

Yang, J.; Chen, Y.; Trappe, W.; Cheng, J.

2014, VIII, 72 p. 27 illus., Softcover

ISBN: 978-3-319-07355-2