

# SpringerBriefs in Computer Science

## Series Editors

Stan Zdonik

Computer Science Department, Brown University, Providence, Rhode Island, USA

Shashi Shekhar

University of Minnesota Dept. Computer Science & Engineering, Minneapolis, Minnesota, USA

Jonathan Katz

Dept. Computer Science, University of Maryland, College Park, Maryland, USA

Xindong Wu

University of Vermont Dept. Computer Science, Burlington, Vermont, USA

Lakhmi C. Jain

School of Electrical and Information Engineering, University of South Australia, Adelaide, South Australia, Australia

David Padua

University of Illinois Urbana-Champaign Siebel Center for Computer Science, Urbana, Illinois, USA

Xuemin (Sherman) Shen

Department of Electronic and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada

Borko Furht

Florida Atlantic University Dept. of Computer Science & Engineering, Boca Raton, Florida, USA

V. S. Subrahmanian

Computer Science Department, University of Maryland, College Park, Maryland, USA

Martial Hebert

Carnegie Mellon University, Pittsburgh, Pennsylvania, USA

Katsushi Ikeuchi

University of Tokyo Inst. Industrial Science, Tokyo, Japan

Bruno Siciliano

Dipartimento di Ingegneria Elettrica e T, Università di Napoli Federico II, Napoli, Napoli, Italy

Sushil Jajodia

George Mason University, Fairfax, Virginia, USA

More information about this series at <http://www.springer.com/series/10028>

Jie Yang • Yingying Chen • Wade Trappe  
Jerry Cheng

# Pervasive Wireless Environments: Detecting and Localizing User Spoofing

 Springer

Jie Yang  
Department of Computer Science and Engineering  
Oakland University  
Rochester  
Michigan  
USA

Wade Trappe  
Wireless Information Network Lab  
Rutgers, The State University  
of New Jersey  
North Brunswick  
New Jersey, USA

Yingying Chen  
Department Electrical & Computer Engineering  
Stevens Institute of Technology  
Hoboken  
New Jersey  
USA

Jerry Cheng  
Rutgers, The State University  
of New Jersey  
New Brunswick  
New Jersey  
USA

ISSN 2191-5768

ISSN 2191-5776 (electronic)

ISBN 978-3-319-07355-2

ISBN 978-3-319-07356-9 (eBook)

DOI 10.1007/978-3-319-07356-9

Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014940861

© The Author(s) 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science + Business Media ([www.springer.com](http://www.springer.com))

# Preface

As more wireless and sensor networks are deployed, information provided and shared by wireless systems has become an inseparable part of our social fabric. However, wireless security is often cited as a major technical barrier that must be overcome before widespread adoption of wireless information systems. Due to the shared nature of the wireless medium, adversaries can gather useful identity information during passive monitoring and further utilize the identity information to perform user spoofing. During an user spoofing attack, an adversary can forge its identity to masquerade as another device, or even creates multiple illegitimate identities in the networks. For instance, in Wi-Fi network, it is easy for an attacker to modify its MAC address of network interface card (NIC) to another device through vendor-supplied NIC drivers or open-source NIC drivers. In addition, by masquerading as an authorized wireless access point or as an authorized client, an attacker can launch denial of service attacks, bypass access control mechanisms, or falsely advertise services to wireless clients.

Attacks originated from user spoofing will have a serious impact on the successful deployment of pervasive wireless environments. It is thus desirable to detect the presence of user spoofing and eliminate it from the network. The traditional approach to prevent user spoofing is to apply cryptographic authentication. However, authentication requires additional key management infrastructural overhead and extra computational power associated with distributing, and maintaining cryptographic keys. Due to the limited power and resources available on the wireless devices and the dynamics introduced by the node mobility, it is not always possible to deploy authentication. This book provides a different approach by using the physical properties associated with wireless transmissions to detect the presence of user spoofing. The book begins by introducing user spoofing in wireless networks, presenting the motivation of the book and summarizing our contributions of the book. After that, we discuss the feasibility of launching user spoofing attacks and their impact on the pervasive wireless environments in Chap. 2. In Chap. 3, we describe the attack detection model that exploits the spatial correlation of Received Signal Strength (RSS) inherited from wireless devices as a foundation. This chapter further presents the performance evaluation of the spoofing attack detection model through experiments in practical environments. In Chap. 4, we deal with the situation when multiple

spoofing attackers are present. We develop a statistical approach to determine the number of attackers, and further show how to localize these adversaries. Both the attacker number determination and adversaries localization methods are evaluated through two wireless testbeds including both Wi-Fi and Zigbee networks. In Chap. 5, we study user spoofing under mobile wireless networks. For many people, mobile devices are becoming the favored portal to their online social lives. Thus, the identity fraud conducted by malicious mobile agents will have detrimental impact on the successful deployment of mobile pervasive applications. We develop the DEMOTE system, which exploits the correlation within the RSS trace based on each devices identity to detect mobile attackers in Chap. 5. The DEMOTE system is evaluated in an office environment in both Wi-Fi and Zigbee networks. In Chap. 6, we provide an overview of the state-of-the-art research. Finally, the conclusions and future directions are presented in Chap. 7.

# Contents

<b>1</b>	<b>Introduction</b> .....	1
1.1	Background and Motivation .....	1
1.2	Contributions .....	2
1.3	Outline of the Book .....	3
	References .....	4
<b>2</b>	<b>Feasibility of Launching User Spoofing</b> .....	5
	References .....	6
<b>3</b>	<b>Attack Detection Model</b> .....	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
<b>4</b>	<b>Detection and Localizing Multiple Spoofing Attackers</b> .....	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**