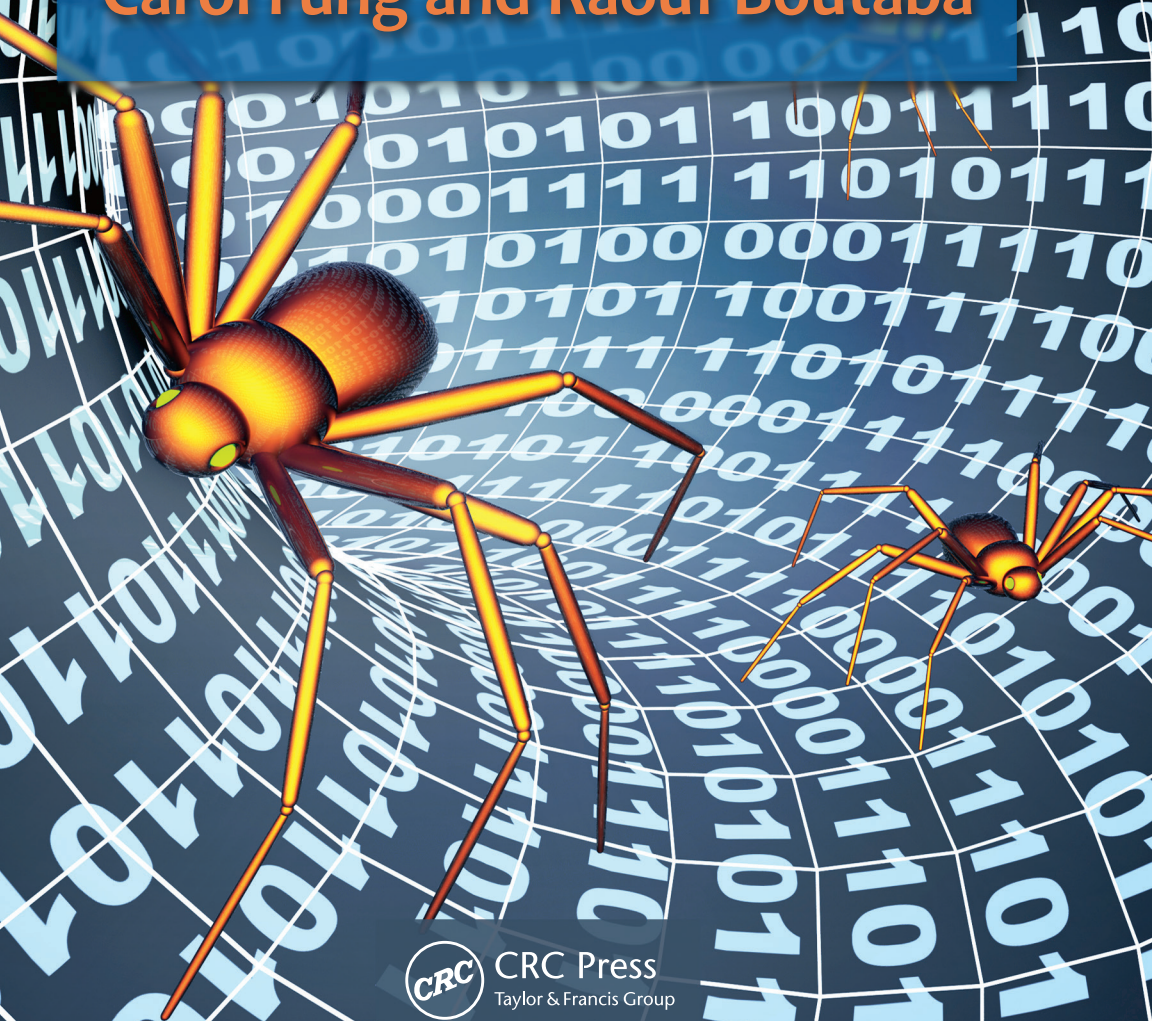


# Intrusion Detection Networks

A Key to Collaborative Security

---

Carol Fung and Raouf Boutaba



CRC Press  
Taylor & Francis Group

AN AUERBACH BOOK

# **Intrusion Detection Networks**

**A Key to Collaborative Security**

This page intentionally left blank

# Intrusion Detection Networks

A Key to Collaborative Security

Carol Fung and Raouf Boutaba



CRC Press

Taylor & Francis Group

Boca Raton London New York

---

CRC Press is an imprint of the  
Taylor & Francis Group, an **informa** business

AN AUERBACH BOOK

CRC Press  
Taylor & Francis Group  
6000 Broken Sound Parkway NW, Suite 300  
Boca Raton, FL 33487-2742

© 2014 by Taylor & Francis Group, LLC  
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works  
Version Date: 20131108

International Standard Book Number-13: 978-1-4665-6413-8 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access [www.copyright.com](http://www.copyright.com) (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

**Trademark Notice:** Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

**Visit the Taylor & Francis Web site at**  
**<http://www.taylorandfrancis.com>**

**and the CRC Press Web site at**  
**<http://www.crcpress.com>**

---

# Contents

---

<b>List of Figures</b> . . . . .	<b>xiii</b>
<b>List of Tables</b> . . . . .	<b>xvii</b>
<b>Preface</b> . . . . .	<b>xix</b>
<b>About the Authors</b> . . . . .	<b>xxi</b>
<b>SECTION I: INTRODUCTION</b>	<b>1</b>
<b>SECTION II: CYBER INTRUSIONS AND INTRUSION DETECTION</b>	<b>7</b>
<b>2 Cyber Intrusions</b> . . . . .	<b>9</b>
2.1 Introduction . . . . .	9
2.2 Overview of Cyber Intrusions . . . . .	10
2.2.1 Malware . . . . .	10
2.2.2 Vulnerabilities Exploitation . . . . .	11
2.2.3 Denial-of-Service Attack . . . . .	12
2.2.4 Web-Based Attacks . . . . .	13
2.2.5 DNS Attack . . . . .	14
2.2.6 Organized Attacks and Botnets . . . . .	15
2.2.7 Spam and Phishing . . . . .	15
2.2.8 Mobile Device Security . . . . .	17
2.2.9 Cyber Crime and Cyber Warfare . . . . .	17
2.3 A Taxonomy of Cyber Intrusions . . . . .	18
2.4 Summary . . . . .	18

<b>3</b>	<b>Intrusion Detection</b>	<b>21</b>
3.1	Intrusion Detection Systems	22
3.1.1	Signature-Based and Anomaly-Based IDSs	22
3.1.2	Host-Based and Network-Based IDSs	22
3.1.3	Other Types of IDSs	24
3.1.4	Strength and Limitations of IDSs	24
3.2	Collaborative Intrusion Detection Networks	25
3.2.1	Motivation for IDS Collaboration	25
3.2.2	Challenges of IDS Collaboration	25
3.3	Overview of Existing Intrusion Detection Networks	26
3.3.1	Cooperation Topology	26
3.3.2	Cooperation Scope	27
3.3.3	Collaboration Type	27
3.3.4	Specialization	28
3.3.5	Cooperation Technologies and Algorithms	28
3.3.5.1	Data Correlation	28
3.3.5.2	Trust Management	29
3.3.5.3	Load Balancing	29
3.3.6	Taxonomy	29
3.4	Selected Intrusion Detection Networks	29
3.4.1	Indra	29
3.4.2	DOMINO	30
3.4.3	DShield	31
3.4.4	NetShield	31
3.4.5	CIDS	32
3.4.6	Gossip	33
3.4.7	Worminator	34
3.4.8	ABDIAS	34
3.4.9	CRIM	35
3.4.10	ALPACAS	35
3.4.11	CDDHT	35
3.4.12	SmartScreen Filter	35
3.4.13	CloudAV	36
3.4.14	FFCIDN	36
3.4.15	CMDA	36
3.5	Summary	37

## **SECTION III: DESIGN OF AN INTRUSION DETECTION NETWORK** **39**

<b>4</b>	<b>Collaborative Intrusion Detection Networks Architecture Design</b>	<b>41</b>
4.1	Introduction	42
4.2	Collaboration Framework	42
4.2.1	Network Join Process	44
4.2.2	Consultation Requests	45

4.2.3	Test Messages . . . . .	46
4.2.4	Communication Overlay . . . . .	46
4.2.5	Mediator . . . . .	46
4.2.6	Trust Management . . . . .	46
4.2.7	Acquaintance Management . . . . .	47
4.2.8	Resource Management . . . . .	47
4.2.9	Feedback Aggregation . . . . .	47
4.3	Discussion . . . . .	48
4.3.1	Privacy Issues . . . . .	48
4.3.2	Insider Attacks . . . . .	48
4.4	Summary . . . . .	49
<b>5</b>	<b>Trust Management . . . . .</b>	<b>51</b>
5.1	Introduction . . . . .	52
5.2	Background . . . . .	53
5.3	Trust Management Model . . . . .	55
5.3.1	Satisfaction Mapping . . . . .	55
5.3.2	Dirichlet-Based Model . . . . .	56
5.3.3	Evaluating the Trustworthiness of a Peer . . . . .	57
5.4	Test Message Exchange Rate and Scalability of Our System . . . . .	59
5.5	Robustness against Common Threats . . . . .	60
5.5.1	Newcomer Attacks . . . . .	60
5.5.2	Betrayal Attacks . . . . .	60
5.5.3	Collusion Attacks . . . . .	61
5.5.4	Inconsistency Attacks . . . . .	61
5.6	Simulations and Experimental Results . . . . .	61
5.6.1	Simulation Setting . . . . .	61
5.6.2	Modeling the Expertise Level of a Peer . . . . .	62
5.6.3	Deception Models . . . . .	63
5.6.4	Trust Values and Confidence Levels for Honest Peers . . . . .	63
5.6.5	Trust Values for Dishonest Peers . . . . .	64
5.6.6	Robustness of Our Trust Model . . . . .	66
5.6.7	Scalability of Our Trust Model . . . . .	69
5.6.8	Efficiency of Our Trust Model . . . . .	69
5.7	Conclusions and Future Work . . . . .	71
<b>6</b>	<b>Collaborative Decision . . . . .</b>	<b>73</b>
6.1	Introduction . . . . .	74
6.2	Background . . . . .	75
6.3	Collaborative Decision Model . . . . .	75
6.3.1	Modeling of Acquaintances . . . . .	77
6.3.2	Collaborative Decision . . . . .	79
6.4	Sequential Hypothesis Testing . . . . .	80
6.4.1	Threshold Approximation . . . . .	83
6.5	Performance Evaluation . . . . .	84



6.5.1	Simulation Setting . . . . .	85
6.5.1.1	Simple Average Model . . . . .	85
6.5.1.2	Weighted Average Model . . . . .	86
6.5.1.3	Bayesian Decision Model . . . . .	86
6.5.2	Modeling of a Single IDS . . . . .	86
6.5.3	Detection Accuracy and Cost . . . . .	88
6.5.3.1	Cost under Homogeneous Environment . . . . .	89
6.5.3.2	Cost under Heterogeneous Environment . . . . .	89
6.5.3.3	Cost and the Number of Acquaintances . . . . .	90
6.5.4	Sequential Consultation . . . . .	92
6.5.5	Robustness and Scalability of the System . . . . .	95
6.6	Conclusion . . . . .	96
<b>7</b>	<b>Resource Management . . . . .</b>	<b>97</b>
7.1	Introduction . . . . .	97
7.2	Background . . . . .	98
7.3	Resource Management and Incentive Design . . . . .	100
7.3.1	Modeling of Resource Allocation . . . . .	100
7.3.2	Characterization of Nash Equilibrium . . . . .	103
7.3.3	Incentive Properties . . . . .	105
7.4	Primal / Dual Iterative Algorithm . . . . .	107
7.5	Experiments and Evaluation . . . . .	110
7.5.1	Nash Equilibrium Computation . . . . .	110
7.5.2	Nash Equilibrium Using Distributed Computation . . . . .	111
7.5.3	Robustness Evaluation . . . . .	114
7.5.3.1	Free-Riding . . . . .	114
7.5.3.2	Denial-of-Service (DoS) Attacks . . . . .	115
7.5.3.3	Dishonest Insiders . . . . .	115
7.5.4	Large-Scale Simulation . . . . .	117
7.6	Conclusion . . . . .	117
<b>8</b>	<b>Collaborators Selection and Management . . . . .</b>	<b>119</b>
8.1	Introduction . . . . .	120
8.2	Background . . . . .	121
8.3	IDS Identification and Feedback Aggregation . . . . .	122
8.3.1	Detection Accuracy for a Single IDS . . . . .	123
8.3.2	Feedback Aggregation . . . . .	124
8.4	Acquaintance Management . . . . .	126
8.4.1	Problem Statement . . . . .	126
8.4.2	Acquaintance Selection Algorithm . . . . .	128
8.4.3	Acquaintance Management Algorithm . . . . .	130
8.5	Evaluation . . . . .	132
8.5.1	Simulation Setting . . . . .	132
8.5.2	Determining the Test Message Rate . . . . .	132
8.5.3	Efficiency of Our Feedback Aggregation . . . . .	134

8.5.4	Cost and the Number of Collaborators . . . . .	135
8.5.5	Efficiency of Acquaintance Selection Algorithms . . . . .	136
8.5.6	Evaluation of Acquaintance Management Algorithm . . . . .	137
8.5.6.1	Convergence . . . . .	137
8.5.6.2	Stability . . . . .	139
8.5.6.3	Incentive Compatibility . . . . .	141
8.5.6.4	Robustness . . . . .	141
8.6	Conclusion and Future Work . . . . .	142

## SECTION IV: OTHER TYPES OF IDN DESIGN 145

<b>9</b>	<b>Knowledge-Based Intrusion Detection Networks and Knowledge Propagation . . . . .</b>	<b>147</b>
9.1	Introduction . . . . .	148
9.2	Background . . . . .	150
9.3	Knowledge Sharing IDN Architecture . . . . .	151
9.3.1	Network Topology . . . . .	151
9.3.2	Communication Framework . . . . .	152
9.3.3	Snort Rules . . . . .	153
9.3.4	Authenticated Network Join Operation . . . . .	154
9.3.5	Feedback Collector . . . . .	154
9.3.6	Trust Evaluation and Acquaintance Management . . . . .	155
9.3.7	Knowledge Propagation Control . . . . .	156
9.3.8	An Example . . . . .	157
9.4	Knowledge Sharing and Propagation Model . . . . .	157
9.4.1	Lower Level – Public Utility Optimization . . . . .	159
9.4.2	Upper Level – Private Utility Optimization . . . . .	161
9.4.3	Tuning Parameter $R_{ij}$ . . . . .	162
9.4.4	Nash Equilibrium . . . . .	164
9.4.5	Price of Anarchy Analysis . . . . .	165
9.4.6	Knowledge Propagation . . . . .	166
9.5	Bayesian Learning and Dynamic Algorithms . . . . .	167
9.5.1	Bayesian Learning Model for Trust . . . . .	168
9.5.1.1	Dirichlet Learning Model for Knowledge Quality . . . . .	168
9.5.1.2	Credible-Bound Estimation of Trust . . . . .	168
9.5.2	Dynamic Algorithm to Find the Prime NE at Node . . . . .	169
9.6	Evaluation . . . . .	171
9.6.1	Simulation Setup . . . . .	172
9.6.2	Trust Value Learning . . . . .	172
9.6.3	Convergence of Distributed Dynamic Algorithm . . . . .	176
9.6.4	Scalability and Quality of Information (QoI) . . . . .	176
9.6.5	Incentive Compatibility and Fairness . . . . .	177
9.6.6	Robustness of the System . . . . .	179
9.7	Conclusion . . . . .	180