

SpringerBriefs in Optimization

For further volumes:
<http://www.springer.com/series/8918>

My T. Thai

Group Testing Theory in Network Security

An Advanced Solution

 Springer

My T. Thai
Department of Computer and Information
Science and Engineering
University of Florida
Gainesville, FL 32611
USA
e-mail: mythai@cise.ufl.edu

ISSN 2190-8354
ISBN 978-1-4614-0127-8
DOI 10.1007/978-1-4614-0128-5
Springer New York Dordrecht Heidelberg London

e-ISSN 2191-575X
e-ISBN 978-1-4614-0128-5

Library of Congress Control Number: 2011938392

Mathematics Subject Classification (2010):90C31, 68U07, 62P30

© My T. Thai 2012

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden. The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To my parents!

Preface

The idea of group testing is to discover defective items in a large population with the minimum number of tests, where each test, is applied to a subset of items, instead of testing them one by one. Although this powerful theory has been applied to many fields such as medical testing, codes, and multi-access channel communication, its newly emerging application into network security has been only recently discovered. Similar to all the earlier applications of group testing, this new application requires modifications or renovations of the classical group testing models and algorithms, so as to overcome the obstacles of applying the theoretical models to practical scenarios in network security. For example, under which conditions can group testing be constructed and tested on wireless sensor networks?

This monograph presents several new challenges and provides new group testing-based solutions for advanced network security problems. In particular, [Chap. 2](#) presents a solution for Denial-of-Service attacks on the Internet in which a size constraint group testing is required. That is, there is a limit on the number of items in each subset and on the number of total subsets. [Chapter 3](#) provides a solution for reactive jamming attacks in wireless sensor networks. Since the group testing is performed on wireless sensor networks, a careful design of an interference-free group testing, where each test result does not interfere with each other, is required. A more advanced solution for more sophisticated reactive jamming attacks is discussed in [Chap. 4](#). Specifically, [Chap. 4](#) provides a randomized fault-tolerant group testing construction to reduce the computational cost, compared to that using irreducible polynomials on Galois Field. Several challenges in designing a group testing-based solution for advanced reactive jamming attacks are also discussed. A discussion on open problems and suggestions for new solutions for various network security problems are included in the last chapter. We hope that this book will encourage research on the many intriguing open questions and applications of group testing that still remain.

Gainesville, FL, May 2011

My T. Thai

Contents

1	Group Testing Theory	1
1.1	Introduction	1
1.2	Basic Theory and Design	2
1.2.1	Sequential Group Testing	2
1.2.2	Non-Adaptive Group Testing	3
1.2.3	Error Tolerance	7
1.3	Applications in Network Security	9
	References	10
2	Size Constraint Group Testing and DoS Attacks	13
2.1	Overview	13
2.2	Network System Models	15
2.2.1	DoS Attacker Model	15
2.2.2	Victim/Detection Model	15
2.3	Size Constraint Group Testing	17
2.4	Matrix Construction and Latency Analyses	17
2.4.1	Sequential Detection With Packing	17
2.4.2	Sequential Detection Without Packing	20
2.4.3	Partial Non-Adaptive Detection	23
2.5	Detection System Configuration	30
2.5.1	System Overview	30
2.5.2	Configuration Details	31
2.6	Experimental Analysis	34
2.6.1	Configurations	34
2.6.2	Results	36
	References	39

3	Interference Free Group Testing and Reactive Jamming Attacks	41
3.1	Overview	41
3.2	Problem Models and Preliminaries	43
3.2.1	Network Model	43
3.2.2	Basic Attacker Model	44
3.2.3	Maximum Clique	45
3.3	Group-Testing-Based Trigger Node Identification: Preprocessing	45
3.3.1	Node Classification	45
3.3.2	Jamming Range Estimation	46
3.4	Identifying Trigger Nodes Algorithm	47
3.4.1	Interference Free Group Testing Algorithm	47
3.4.2	Non-Adaptive Group Testing Detection Algorithm	48
3.5	Theoretical Analysis	49
3.5.1	Estimation of Trigger Node Upper Bound D_{ij}	49
3.5.2	Correctness of ITN Algorithm	51
3.5.3	Performance Analysis	52
3.6	Experimental Analysis	53
3.6.1	Simulation Setup	53
3.6.2	Results and Analysis	54
	References	58
4	Randomized Fault Tolerant Group Testing and Advanced Security	59
4.1	Advanced Attacker Model	59
4.2	Error-Tolerant Randomized Non-Adaptive Group Testing	60
4.2.1	Construction of Randomized Error-Tolerant (d,z) -Disjunct Matrix	60
4.2.2	Theoretical Analysis	61
4.3	Clique-Independent Set	62
4.3.1	NP-Completeness of CIS in UDGs	62
4.4	Advanced Trigger Node Identification	64
4.4.1	Discovery of Interference-Free Testing Teams	65
4.4.2	Estimation of Trigger Upperbound	68
4.4.3	Analysis of Time Complexity	68
4.5	Advanced Solutions Toward Sophisticated Attack Models	70
4.5.1	Upper Bound on the Expected Value of z	71
4.5.2	Error-Tolerant Asynchronous Testing Within Each Testing Team	74
4.6	Experimental Analysis	75
4.6.1	Overview	75

- 4.6.2 Benefits for Jamming-Resistant Routing 75
- 4.6.3 Improvements on Time Complexity 77
- 4.6.4 Robustness to Various Jammer Models 78
- References 79

- 5 Outlooks 81**
 - 5.1 General Detection Framework Based on Group Testing 81
 - 5.2 Size Constraint Group Testing 82
 - 5.3 Jamming Attacks and Trigger Node Detection 82
 - References 83

- Index 85**