

# Contents

<b>1</b>	<b>Group Testing Theory</b> . . . . .	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
<b>2</b>	<b>Size Constraint Group Testing and DoS Attacks</b> . . . . .	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

<b>3</b>	<b>Interference Free Group Testing and Reactive Jamming Attacks</b>	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
<b>4</b>	<b>Randomized Fault Tolerant Group Testing and Advanced Security</b>	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**



<http://www.springer.com/978-1-4614-0127-8>

Group Testing Theory in Network Security  
An Advanced Solution

Thai, M.T.

2012, XI, 86 p. 24 illus., 17 illus. in color., Softcover

ISBN: 978-1-4614-0127-8