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

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 intefere 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