Advances in Information Security

Volume 73

Series editor
Sushil Jajodia, George Mason University, Fairfax, VA, USA

More information about this series at http://www.springer.com/series/5576

Jiaojiao Jiang • Sheng Wen • Bo Liu • Shui Yu
Yang Xiang • Wanlei Zhou

Malicious Attack Propagation and Source Identification

Springer

Jiaojiao Jiang
Swinburne University of Technology
Hawthorne, Melbourne
VIC, Australia

Bo Liu
La Trobe University
Bundoora, VIC, Australia

Yang Xiang
Digital Research & Innovation Capability
Swinburne University of Technology
Hawthorn, Melbourne
VIC, Australia

Sheng Wen
Swinburne University of Technology
Hawthorne, Melbourne
VIC, Australia

Shui Yu
University of Technology Sydney
Ultimo, NSW, Australia

Wanlei Zhou
University of Technology Sydney
Ultimo, NSW, Australia

ISSN 1568-2633
Advances in Information Security
ISBN 978-3-030-02178-8 ISBN 978-3-030-02179-5 (eBook)
https://doi.org/10.1007/978-3-030-02179-5

Library of Congress Control Number: 2018959747

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

In the modern world, the ubiquity of networks has made us vulnerable to various malicious attacks. For instance, computer viruses propagate throughout the Internet and infect millions of computers. Misinformation spreads incredibly fast in online social networks, such as Facebook and Twitter. Experts say that "fake news" on social media platforms influenced US election voters. Researchers and manufacturers evolve new methods to produce detection systems to detect suspicious attacks. However, how can we detect the propagation source of the attacks so as to protect network assets from fast acting attacks? Moreover, how can we build up effective and efficient prevention systems to stop malicious attacks before they do damage and have a chance to infect a system.

So far, extensive work has been done to develop new approaches, to effectively identify the propagation source of malicious attacks and to efficiently restrain the malicious attacks. The goal of this book is to summarize and analyze the state-of-the-art research and investigations in the field of identifying propagation sources and preventing malicious propagation, so as to provide an approachable strategy for researchers and engineers to implement this new framework in real-world applications. The striking features of the book can be illustrated from three basic aspects:

- A detailed coverage on analyzing and preventing the propagation of malicious attacks in complex networks. On the one hand, a practical problem in malicious attack propagation is the spreading influence of initial spreaders. This book presents and analyzes different methods for influential spreader detection. On the other hand, various strategies have been proposed for preventing malicious attack propagation. This book numerically analyzes these strategies, concludes the equivalences of these strategies, and presents a hybrid strategy by combining different strategies.
- A rich collection of contemporary research results in identifying the propagation source of malicious attacks. According to the categories of observations on malicious attacks, current research can be divided into three types. For each

type, we particularly present one representative method and the theory behind each method. A comprehensive theoretical analysis of current methods is further presented. Apart from the theoretical analysis, the book numerically analyzes their pros and cons based on real-world datasets.
- A comprehensive study of critical research issues in identifying the propagation source of malicious attacks. For each issue, the book presents a brief introduction to the problem and its challenges, and a detailed state-of-the-art method to solve the problem.

This book intends to enable readers, especially postgraduate and senior undergraduate students, to study up-to-date concepts, methods, algorithms, and analytic skills for building modern detection and prevention systems through analyzing the propagation of malicious attacks. It enables students not only to master the concepts and theories in relation to malicious attack propagation and source identification but also to readily use the material introduced into implementation practices.

The book is divided into three parts: malicious attack propagation, propagation source identification, and critical research issues in source identification. In the first part, after an introduction of the preliminaries of malicious attack propagation, the book presents detailed descriptions on areas of detecting influential spreaders and restraining the propagation of malicious attacks. In the second part, after a summary on the techniques involved in propagation source identification under different categories of observations about malicious attack propagation, the book then presents a comprehensive study of these techniques and uses real-world datasets to numerically analyze their pros and cons. In the third part, the book explores three critical research issues in the research area of propagation source identification. The most difficult one is the complex spatiotemporal diffusion process of malicious attacks in time-varying networks, which is the bottleneck of current approaches. The second issue lies in the expensively computational complexity of identifying multiple propagation sources. The third important issue is the huge scale of the underlying networks, which makes it difficult to develop efficient strategies to quickly and accurately identify propagation sources. These weaknesses prevent propagation source identification from being applied in a broader range of real-world applications. This book systematically analyzes the state of the art in addressing these issues and aims at making propagation source identification more effective and applicable.

Hawthorne, Melbourne, VIC, Australia — Jiaojiao Jiang
Hawthorne, Melbourne, VIC, Australia — Sheng Wen
Bundoora, VIC, Australia — Bo Liu
Ultimo, NSW, Australia — Shui Yu
Hawthorne, Melbourne, VIC, Australia — Yang Xiang
Ultimo, NSW, Australia — Wanlei Zhou
September 2018

Acknowledgments

We are grateful to many research students and colleagues at Swinburne University of Technology in Melbourne and the University of Technology Sydney in Sydney, who have made a lot of comments to our presentations as their comments inspire us to write this book. We would like to acknowledge some support from research grants we have received, in particular the Australian Research Council Grant no. LP120200266, DP140103649, and DP180102828. Some interesting research results presented in the book are taken from our research papers that indeed (partially) were supported through these grants. We also would like to express our appreciations to the editors at Springer, especially Susan Lagerstrom-Fife and Caroline Flanagan, for the excellent professional support. Finally we are grateful to the family of each of us for their consistent and persistent supports. Without their support, the book may just become some unpublished discussions.

Hawthorne, Melbourne, VIC, Australia — Jiaojiao Jiang
Hawthorne, Melbourne, VIC, Australia — Sheng Wen
Bundoora, VIC, Australia — Bo Liu
Ultimo, NSW, Australia — Shui Yu
Hawthorne, Melbourne, VIC, Australia — Yang Xiang
Ultimo, NSW, Australia — Wanlei Zhou
September 2018

Contents