SpringerBriefs in Computer Science

For further volumes:
http://www.springer.com/series/10028

Jin Tang • Yu Cheng

Intrusion Detection for IP-Based Multimedia Communications over Wireless Networks

Springer

Jin Tang
AT&T Labs
Warrenville
IL, USA

Yu Cheng
Department of Electrical and Computer Engineering
Illinois Institute of Technology
Chicago, IL, USA

ISSN 2191-5768
ISBN 978-1-4614-8995-5
DOI 10.1007/978-1-4614-8996-2
Springer New York Heidelberg Dordrecht London

ISSN 2191-5776 (electronic)
ISBN 978-1-4614-8996-2 (eBook)

Library of Congress Control Number: 2013949152

Printed on acid-free paper

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

To my wife Huan—Jin
To my wife Yanning and our daughter Annabelle—Yu

Preface

IP-based multimedia communications have become prevailing in recent years. At the same time, with the increasing coverage of the IEEE 802.11™-based wireless networks, IP-based multimedia communications over wireless networks are drawing extensive attention in both academia and industry. However, due to the openness and distributed nature of the protocols involved, such as the session initiation protocol (SIP) and the IEEE 802.11™ standard, it becomes easy for malicious users in the network to achieve their own gain or disrupt the service by deviating from the normal protocol behaviors. This book presents real-time intrusion detection techniques that can quickly track down the malicious behaviors which manipulate the vulnerabilities from either the 802.11™ or the SIP protocols.

Specifically, for the intrusion detection over the 802.11™ protocol, a real-time detector exploiting the nonparametric cumulative sum (CUSUM) test is designed to quickly find a selfish malicious node without any a priori knowledge of the statistics of the selfish misbehavior. While most of the existing schemes for selfish misbehavior detection depend on heuristic parameter configuration and experimental performance evaluation, this book presents a Markov chain-based analytical model to systematically study the CUSUM-based detector, for guaranteed performance in terms of average false positive rate, average detection delay, and missed detection ratio. Further, to achieve better detection performance, by enhancing the FS detector, an adaptive detector is developed with the Markov decision process (MDP). Then based on a reward function defined in this book, an optimal decision policy can be determined to maximize the overall system benefit through a linear programming formulation. The optimal policy also indicates the operation of the adaptive detector, which yields better performance in both false positive rate and detection delay.

For attacks on the SIP layer, this book first focuses on the well-known flooding attack and develops an online scheme to detect and subsequently prevent the attack, by integrating a novel three-dimensional sketch design with the Hellinger distance detection technique. A very challenging attack, the stealthy attack, is also addressed in this book. In a stealthy attack, intelligent attackers can afford a long time to attack the system and only incur minor changes to the system within each sampling period.

A wavelet-based technique is presented to effectively deal with the stealthy attack. Moreover, a new type of malformed message attack, which manipulates both the "Session-Expires" header in the SIP message and openness of wireless protocols to severely drain the network resources, is also addressed.

In summary, this book presents interdisciplinary techniques to achieve an effective real-time intrusion detection system, which interleaves medium access control (MAC) protocol analysis, CUSUM-based detector design, a novel Markovian model for CUSUM detectors, Markov decision process-based performance optimization, sketch-based traffic modeling, and wavelet-based signal processing techniques.

Chicago, IL, USA Jin Tang and Yu Cheng

Contents