

SpringerBriefs in Computer Science

Series Editors

Stan Zdonik

Peng Ning

Shashi Shekhar

Jonathan Katz

Xindong Wu

Lakhmi C. Jain

David Padua

Xuemin Shen

Borko Furht

V.S. Subrahmanian

Martial Hebert

Katsushi Ikeuchi

Bruno Siciliano

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

© The Author(s) 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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 802.11TM-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 802.11TM 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 802.11TM or the SIP protocols.

Specifically, for the intrusion detection over the 802.11TM 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

1	Introduction	1
1.1	Selfish Misbehavior Detection in 802.11TM	2
1.2	SIP Layer Attack Detection	4
1.3	Overview of This Book	7
	References	7
2	Real-Time Misbehavior Detection in IEEE 802.11TM: An Analytical Approach	11
2.1	Selfish Misbehavior in 802.11TM	11
2.2	Fair Share Detector Design	12
2.3	Markov Chain Based Analytical Model	14
2.4	Theoretical Performance Analysis	16
2.5	Simulation Results	27
2.6	Summary	33
	References	34
3	Adaptive Misbehavior Detection in IEEE 802.11TM: Based on Markov Decision Process	35
3.1	Adaptive Detector Design	35
3.2	Markov Decision Process Based Modeling	36
3.3	Theoretical Performance Analysis	42
3.4	Simulation Results	46
3.5	Summary	48
3.6	Related Work of Selfish Misbehavior Detection in 802.11TM	49
	References	50
4	SIP Flooding Attack Detection	53
4.1	SIP Flooding Attack	53
4.2	Basic Techniques	55
4.3	Detection and Prevention Scheme Design	56
4.4	Performance Evaluation	63

4.5	Summary	69
	References	69
5	SIP Stealthy Attack Detection and Resource-Drained Malformed Message Attack Detection	71
5.1	Stealthy Attack Detection	71
5.2	Resource-Drained Malformed Message Attack Detection	77
5.3	Summary	83
5.4	Related Work of SIP Layer Attack Detection	83
	References	85