SpringerBriefs in Computer Science

Series Editors
Stan Zdonik
Peng Ning
Shashi Shekhar
Jonathan Katz
Xindong Wu
Lakhmi C. Jain
David Padua
Xuemin (Sherman) Shen
Borko Furht
V.S. Subrahmanian
Martial Hebert
Katsushi Ikeuchi
Bruno Siciliano

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

Mohamed M.E.A. Mahmoud
Xuemin (Sherman) Shen

Security for Multi-hop Wireless Networks

Springer

Mohamed M.E.A. Mahmoud
Department of Electrical
and Computer Engineering
Tennessee Technological University
Cookeville, TN, USA

Xuemin (Sherman) Shen
Department of Electronic
and Computer Engineering
University of Waterloo
Waterloo, ON, Canada

ISSN 2191-5768
ISBN 978-3-319-04602-0
DOI 10.1007/978-3-319-04603-7
Springer Cham Heidelberg New York Dordrecht London

ISSN 2191-5776 (electronic)
ISBN 978-3-319-04603-7 (eBook)

Library of Congress Control Number: 2014930297

© The Author(s) 2014
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)

Preface

In multi-hop wireless networks, the mobile nodes should act as routers to relay others' packets. With multi-hop packet transmission, new applications can be enabled, the network performance can be enhanced, and the network can be deployed more readily in developing areas at low cost. However, the involvement of autonomous and self-interested nodes in packet routing can cause serious security vulnerabilities.

Selfish nodes will not relay others' packets because they consume the nodes' resources without direct benefits. They will also make use of the other nodes to relay their packets. This behavior will not only degrade the network connectivity and performance, but also introduce an unfairness problem. Moreover, some irrational attackers will launch *Denial-of-Service* attacks by involving their devices in routes with the intention of dropping packets. The presence of even a small number of attackers will result in repeatedly dropped packets. This can result in failure of the multi-hop communication or at least degrade the network performance in terms of throughput, delay, and packet delivery ratio. In addition, selecting good intermediate nodes to relay packets will have positive impact on route stability and packet delivery ratio. In this brief, we discuss efficient security protocols and schemes that can address these issues in multi-hop wireless networks.

In Chap. 1, we first discuss in detail the security issues addressed by this brief, and then we discuss the challenges for securing the multi-hop wireless networks. Finally, we give an overview of the proposed protocols and schemes to secure the multi-hop wireless networks. In Chap. 2, we present the considered system model including the network and communication models and the threat and trust models. In Chap. 3, we present an efficient incentive scheme to stimulate the selfish nodes to relay others' packets. The scheme uses payment system to charge the nodes that send packets and reward those relaying them. In addition to stimulating cooperation, the scheme can enforce fairness by rewarding the nodes for the consumed resources in relaying others' packets. It can also regulate packet transmission because the nodes pay to get their packets delivered. We first develop a payment model that is specifically tailored to our system model. Then, we discuss an efficient communication protocol to secure the payment with limited use of public

key cryptography. We also discuss a mechanism for submitting the payment data to an off-line trusted party and clearing the payment with minimum overhead. Finally, analysis and measurements will be given to verify our proposals.

In Chap. 4, we first discuss a trust system to evaluate the nodes' competence and reliability in relaying packets in terms of multi-dimensional trust values. Then, we present a mechanism to identify the irrational attackers that drop packets intentionally. A node is identified as malicious once its packet dropping rate measured by the trusted system exceeds a threshold. We also discuss two routing protocols for establishing stable and reliable routes in multi-hop wireless networks. The protocols ensure relaying the packets by those highly trusted nodes having sufficient energy to minimize packet dropping probability. We will show that the integration of routing protocols with the trust and payment systems not only stimulates the nodes to relay others' packets but also maintains route stability and reports correct battery energy level. This is because any loss of trust will result in loss of future earnings. In addition, analysis and simulation results will be given to evaluate these protocols and mechanisms. Finally, we draw some conclusions and future research directions in Chap. 5.

Cookeville, TN, USA Mohamed M.E.A. Mahmoud
Waterloo, ON, Canada Xuemin (Sherman) Shen

Contents

1 Introduction 1
1.1 Security Issues 1
1.2 Motivations and Challenges 3
1.3 Overview on the Proposed Protocols/Schemes 5
1.4 Outline of the Brief 7
References 8

2 System Model 11
2.1 Network and Communication Models 11
2.2 Threat and Trust Models 13
References 14

3 Efficient Incentive Scheme 15
3.1 Payment Model 16
3.1.1 Parties and Relations 17
3.1.2 Charging and Rewarding Policy 20
3.2 ESIP: Communication Protocol with Limited Use of Public Key Cryptography 21
3.2.1 Data Generation and Relay 22
3.2.2 *ACK* Generation and Relay 23
3.3 RACE: Efficient Scheme for Submitting/Processing the Payment Data 25
3.3.1 *Evidence* Composition and Payment-Report Submission 25
3.3.2 Reports Classification 30
3.3.3 Cheaters Identification 31
3.3.4 Credit-Account Update 32
3.4 Security Analysis 37
3.5 Performance Evaluations 42
3.5.1 Replacing Signatures with Hashing Operations 42
3.5.2 Replacing Receipts with Payment Reports 54
References 59

4 Secure Routing Protocols 63
4.1 Trust/Reputation Systems 63
4.1.1 Rating Calculation 63
4.1.2 Trust/Reputation Update 66
4.2 Identification of Malicious Nodes 71
4.3 Reliable and Secure Routing Protocols 73
4.3.1 SRR Routing Protocol 74
4.3.2 BAR Routing Protocol 76
4.4 Evaluations 79
4.4.1 Defence Against Trust Manipulation and Irrational Route Breaking Attacks 79
4.4.2 Evaluations of SRT and WRT Routing Protocols 87
References 92

5 Conclusions and Future Directions 95
5.1 Conclusions 95
5.2 Future Research Directions 97
References 99

List of Figures

Fig. 2.1 The architecture of the multi-hop wireless network 12

Fig. 3.1 The architecture of the proposed security protocols/schemes 16
Fig. 3.2 Payment model's parties and relations 18
Fig. 3.3 The payment rewarding and charging policy. (a) Delivered packets. (b) Undelivered packets 21
Fig. 3.4 The source node shares a key with each node in the route 22
Fig. 3.5 The source and destination nodes' hash chains 22
Fig. 3.6 The exchanged security tags in a session 24
Fig. 3.7 The hop-by-hop security packet-overhead in the Xth data packet and $X > 1$ 24
Fig. 3.8 The formats of the payment *Evidence*s. (**a**) General *Evidence* format. (**b**) Last received packet is data and $1 \leq X \leq N$. (**c**) Last received packet is data and $N < X \leq 2N$. (**d**) Last received packet is *ACK* and $1 \leq X \leq N$. (**e**) The last received packet is *RREP* 26
Fig. 3.9 Aggregated *Evidence* 28
Fig. 3.10 The submission of reports and *Evidences* 29
Fig. 3.11 The worst-case timing of the reports submission and clearance 34
Fig. 3.12 $P(T(n) \leq t)$ versus t at different values of n for model I 35
Fig. 3.13 $P(T(n) \leq t)$ versus t at different values of n for model II 36
Fig. 3.14 The average payment clearance delay for model I 36
Fig. 3.15 The average payment clearance delay for model II 37
Fig. 3.16 The hop-by-hop security packet-overhead of ESIP and signature-based incentive schemes. (**a**) The hop-by-hop security packet-overhead in RSA/DSA based incentive schemes. (**b**) The hop-by-hop security packet-overhead of ESIP 45
Fig. 3.17 The average packet security overhead in ESIP 45
Fig. 3.18 The equivalent route lengths for the same security packet overhead 46

Fig. 3.19 Route length distribution. (**a**) At 15 nodes. (**b**) At 35 nodes. (**c**) At 50 nodes. (**d**) At 100 nodes 47
Fig. 3.20 The ratio of ESIP's cryptographic delay to that of signature-based incentive schemes 48
Fig. 3.21 The average end-to-end packet delay. (**a**) Signature-based incentive schemes. (**b**) ESIP and original DSR 51
Fig. 3.22 The packet delivery ratio versus the number of connections 52
Fig. 3.23 The average throughput versus the number of connections 52
Fig. 3.24 The ratio of ESIP's cryptographic energy to that of the signature-based incentive schemes 53
Fig. 3.25 The impact of node mobility on the end-to-end packet delay 53
Fig. 3.26 The *Evidences*' average storage area at different aggregation levels 56
Fig. 3.27 The *Evidences*' average storage area at different number of aggregated *Evidences* 56

Fig. 4.1 The possible cases for complete and broken routes. (**a**) Complete route. (**b**) Broken route during relaying the *RREP* packet. (**c**) Broken route during relaying he first data packet. (**d**) Broken route during relaying the ith data packet. (**e**) Broken route during relaying the ith *ACK* packet 65
Fig. 4.2 Weighted ratings for two nodes in a broken link. (**a**) $\mathcal{N}_B$ is an honest node. (**b**) $\mathcal{N}_B$ is a malicious node 67
Fig. 4.3 Rating window of $\mathcal{N}_A$ having its latest γ ratings 68
Fig. 4.4 The format of the nodes' certificates 71
Fig. 4.5 A node's state transition diagram 72
Fig. 4.6 The format of *RREQ* and *RREP* packets in *SRR* routing protocol. (**a**) The format of *RREQ* packet. (**b**) The format of *RREP* packet 75
Fig. 4.7 The format of *RREQ* packet in the *BAR* protocol 77
Fig. 4.8 Broadcasting the *RREQ* packet in *BAR* protocol 78
Fig. 4.9 Route selection in the *BAR* protocol 79
Fig. 4.10 The effect of R_m on the reputation system's effectiveness when $\gamma = 50$ 81
Fig. 4.11 The effect of γ on the reputation system's effectiveness 82
Fig. 4.12 The effect of P on $P_i(X)$ when $R_m = 0.5$ 83
Fig. 4.13 The expected drop in the packet delivery ratio due to the malicious nodes 89
Fig. 4.14 *SRR* and *WRT* protocols can improve the packet delivery ratio due to selecting good intermediate nodes 90
Fig. 4.15 *SRR* generates fewer *RREQ* broadcasts because the nodes that cannot satisfy the source node's requirements do not broadcast the packets 91

Fig. 4.16 Routes cannot be established if the source node's trust requirement is not properly determined in *SRR* 92
Fig. 4.17 The route lifetime in our protocols is more than that in *DSR* because of establishing more stable routes 92

List of Tables

Table 3.1 Properties of Web-based applications and cooperation stimulation 17
Table 3.2 Numerical example for the payment reports of $\mathcal{N}_A$ 26
Table 3.3 Numerical examples for fair payment reports 30
Table 3.4 Numerical examples for cheating payment reports 40
Table 3.5 The processing times and energy of the used cryptosystems 44
Table 3.6 Statistics of the simulated network 44
Table 3.7 The average connectivity, route length at different network parameters 46
Table 3.8 The average data packet overhead (bytes) 48
Table 3.9 The required cryptographic operations in ESIP and signature-based incentive schemes 48
Table 3.10 The average packet series size, and cryptographic time and energy ratios 49
Table 3.11 Ninety-five percent confidence interval (C.I.) for mean 50
Table 3.12 The average size of payment receipts, *Evidences*, and reports (bytes) 55
Table 3.13 The distribution of the number of used hash chains 55
Table 3.14 The average amount of submitted payment reports and receipts (KB) 58
Table 3.15 The required cryptographic operations for clearing the payment of 10-min data transmission with node speed of [0, 5] m/s 58
Table 3.16 The required cryptographic operations for clearing the payment of 10-min data transmission with node speed of [0, 10] m/s 58

Table 4.1 Numerical examples for route reliability 74
Table 4.2 Simulation results 84