

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
Waterloo, ON, Canada

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

Security for Multi-hop Wireless Networks

A. M. El-Bendary, M.; Shen, X.S.

2014, XIII, 99 p. 45 illus., 27 illus. in color., Softcover

ISBN: 978-3-319-04602-0