Lehrstuhl für Kommunikationsnetze
Prof. Dr.-Ing. Christian Wietfeld

SECURE AND EFFICIENT ROUTING IN HIGHLY DYNAMIC WLAN MESH NETWORKS

DISSERTATION

For the Degree of *Doktor-Ingenieur*
Faculty of Electrical Engineering and Information Technology
TU Dortmund University, Germany

Mohamad Sbeiti
Dortmund, September 2015

Author's Contact Information:
mohamad.sbeiti@tu-dortmund.de
www.paser.info

Thesis Advisor:	**Prof. Dr.-Ing. Christian Wietfeld** TU Dortmund University
Secondary Referee:	**Prof. Dr. Thorsten Holz** Ruhr University Bochum
Thesis Submitted:	April 23, 2015
Thesis Defense:	August 21, 2015

Dortmunder Beiträge zu Kommunikationsnetzen und -systemen

Band 12

Mohamad Sbeiti

Secure and Efficient Routing in Highly Dynamic WLAN Mesh Networks

D 290 (Diss. Technische Universität Dortmund)

Shaker Verlag
Aachen 2016

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Dortmund, Technische Univ., Diss., 2015

Printed in Germany.

ISBN 978-3-8440-4289-4
ISSN 1867-4879

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • e-mail: info@shaker.de

To all people deprived of education.

To Kassem, Sanaa, Malak, Hiyam, Moussa and May
for their endless love and support.

Acknowledgment

Praise be to Allah, lord of the worlds. The beneficent, the merciful.

My utmost gratitude goes to my supervisor, Prof. Dr.-Ing. Christian Wietfeld, for giving me the opportunity to join his group, for letting me participate in several research projects, and for securing financial support to finish this work. He is a professional advisor, from whom I learned not only how to do research, but also to embrace challenges and to always strive for the best. I thank him for his continuous and consistent support, guidance, and encouragement. My discussions with him, even though sometimes difficult, repeatedly inspired me to tackle problems from different and greater perspectives.

I gratefully acknowledge Prof. Dr. Thorsten Holz, Prof. Dr.-Ing. Peter Krummrich, and Prof. Dr.-Ing. Christian Rehtanz for serving as my supervisory committee and for helping me to improve the quality of this thesis by their valuable comments and feedback.

Being part of the communication networks institute (CNI) at the TU Dortmund gave me the opportunity to collaborate with many talented researchers. I would like to express my deep gratitude to all those on the CNI research team, especially Dipl.-Inf. Maike Kuhnert, Dr.-Ing. Andreas Wolff, Dipl.-Ing. Sebastian Subik, and Dr.-Ing. Thang Tran for always finding time whenever I needed an intelligent discussion. Working with them for many years enabled me to conduct quality research. I also thank Dipl.-Inf. Niklas Goddemeier, Dipl.-Inf. Daniel Behnke, Dipl.-Ing. Christoph Ide, and M.Sc. Sebastian Rohde for our successful joint work on several projects and papers. I have greatly benefited from the many interactions and discussions with them.

I am also grateful to the department of electrical engineering and information technology at the Ruhr University Bochum, especially to Prof. Dr.-Ing. Christof Paar, Prof. Dr. Jörg Schwenk, and Dr. Roberto Avanzi, for teaching me IT security, which has been the basis of this thesis.

I also would like to acknowledge Dr.-Ing. Shadi Traboulsi, Dr. Ahmed E.A.A. Abdulla, Dipl.-Ing. Carsten Vogel, Dr. Houssein Assaad, Dr.-Ing. Hassan Sbeyti, Dr. Hassan Hijazi, and Dipl.-Ing. Jakob Pojda for reviewing some papers of mine and for the fruitful discussions we had about different research topics. They always had the kindness to give helpful comments.

I strongly acknowledge the code guru, Dipl.-Ing. Eugen Paul, and Dipl.-Ing. Carsten Vogel for supporting me in implementing my research project, the secure

routing protocol PASER, in simulation and in Linux. I would not have been able to study secure routing in wireless mesh networks as thoroughly without their support. I also thank B.Sc. Jan Schröder, B.Sc. Majuran Rajakanthan, Dipl.-Ing. Mohamad Nehme, and M.Sc. Jonas Hinker for helping me to tackle different security aspects of wireless mesh networks.

On a more personal note, I am deeply indebted to my friends who have always stood by my side. I thank my relatives for their cherish and unwavering support. Gratefully, I thank my parents for their sacrifices, continuous support, care, guidance, and encouragement. I dedicate each and every one of my successes to them. I also thank my sister, May, and my brother, Moussa, for their endless love. Finally, I would like to thank my wife, Hiyam, who cherished me through difficult times and comforted me in stressful situations. Without her genuine love and companionship, I would have taken much longer to finish this work.


overhead
Linux
ARAN
Message
MAC
BATMAN
Communications
operations
time
proactive
Packet
Wireless
mechanisms
routing
Link
HWMPS
packets
Time
Dynamic
Simulation
function
performance
scenario
Available
mobility
WLAN
range
PASER
messages
mobile
first
scenarios
process
Evaluation
discovery
communication
Node
practice
WMNs
frames
Protocol
International
Protocols
dynamic
key
destination
results
set
traffic
access
Performance
information
module
Networks
link
packet
reactive
model
INETMANET
routes
protocols
attacker
topology
number
attack
attacks
delay
authentication
transmission
symmetric
Security
mechanism
volume
security
Implementation
IEEE
HWMP
kernel
802.11s
gateway
use
neighbours
Route
wireless
links
one-hop
chain
simulation
PHY
channel
secure
Online
network
Highly
static
WMN
position
OMNeT++
different
Mobile
Mesh
size
corresponding
approach
throughput
OLSR
data
Mbit/s
Secure
standard
Analysis
rate
scheme
implementation
Key
Network
networks
highly
Conference
framework
route-o-matic
due
cryptographic
hash
UAVs

Abstract

Recent advances in embedded systems, energy storage, and communication interfaces, accompanied by the falling prices of WLAN routers and a considerable increase in the throughput of a WLAN (IEEE 802.11), have facilitated the proliferation of WLAN Mesh Network (WMN) applications. In addition to their current deployments in less dynamic community networks, WMNs have become a key solution in various highly dynamic scenarios. For instance, WMNs are intended to interconnect self-organized, cooperative, and small Unmanned Aerial Vehicles (UAVs) in a wide range of applications, such as emergency response, environmental monitoring, and ad-hoc network provisioning. Nevertheless, WMNs still face major security challenges as they are prone to routing attacks. Consequently, the network can be sabotaged and, in the case of UAV-WMN-supported missions, the attacker might manipulate payload data or even hijack UAVs.
Contemporary security standards, such as the IEEE 802.11i and the security mechanisms of the IEEE 802.11s mesh standard, are vulnerable to routing attacks, as experimentally shown in this research. Therefore, a secure routing protocol is indispensable for making feasible the deployment of WMNs in critical scenarios, such as UAV-WMN-assisted applications. As far as the author of this thesis knows, none of the existing research approaches for secure routing in WMNs have gained acceptance in practice due to their high overhead or strong assumptions.
In this research, a new approach, which is called Position-Aware, Secure, and Efficient mesh Routing (PASER), is proposed. This new proposal defeats more attacks than the IEEE 802.11s/i security mechanisms and the well-known, secure routing protocol Authenticated Routing for Ad-hoc Networks (ARAN), without making restrictive assumptions. It is shown that PASER achieves —in realistic UAV-WMN scenarios— similar performance results as the well-established, non-secure routing protocols Hybrid Wireless Mesh Protocol (HWMP) combined with the IEEE 802.11s security mechanisms. Two representative scenarios are considered: (1) on-demand ubiquitous network access and (2) efficient exploration of sizable areas in disaster relief. The performance evaluation results are produced using an experimentally validated simulation model of WMNs, realistic mobility patterns of UAVs, and an experimentally derived channel model for the air-to-air WMN link between UAVs. The findings of this evaluation are justified by the route discovery delay and the message overhead of the considered solutions.

This research's main aim is to support the broad deployment of a secure routing protocol in highly dynamic WMNs, and the PASER features, presented here, are a major step towards achieving this goal.

Kurzfassung

Der technologische Fortschritt in verschiedenen Bereichen wie eingebetteten Systemen, Energiespeicherung sowie Kommunikationsschnittstellen und -protokollen, hat, unterstützt von sinkenden Preisen für WLAN-Hardware und dem deutlichen Anstieg der Übertragungsraten von WLAN-Technologien (IEEE 802.11), den Grundstein gelegt für die zunehmende Anzahl an Anwendungen von WLAN-Mesh-Netzen (WMNs). Diese haben sich neben der gegenwärtigen Verbreitung quasistatischer, Community-gestützter Funknetze vor allem zu einer Schlüsseltechnologie für hochdynamische Anwendungen entwickelt. Eine solche hochdynamische Anwendung ist beispielsweise die WMN-gestützte Kommunikation selbstorganisierender, miteinander kooperierender unbemannter Kleinflugkörper (UAVs) mit einer grossen Spanne an Einsatzbereichen, wie Bergungs- und Rettungseinsätze, Umweltüberwachung, Präzisionslandwirtschaft oder der Ad-hoc-Bereitstellung mobiler WLAN- und Mobilfunknetze. Mit zunehmendem Einsatz in solch kritischen Bereichen wachsen auch die Anforderungen an die Sicherheit. Gegenwärtige WMN-Technologien stehen hierbei noch vor grossen Sicherheitsherausforderungen, da diese keinen Schutz gegen Routing-Angriffe gewähren. Mithin besteht das Risiko, dass Angreifer Netze sabotieren und im Falle von UAV-Einsätzen Nutzdaten der UAVs manipulieren oder sogar die gesamte Kontrolle über einzelne UAVs übernehmen können.

Wie in dieser Dissertation gezeigt wird, sind derzeitige Sicherheitsstandards wie IEEE 802.11i oder auch die Sicherheitsmechanismen des Mesh-Standards IEEE 802.11s anfällig für Routingangriffe. Um einen sicheren Einsatz von WMNs im sensiblen und kritischen Umfeld wie den erwähnten UAV-WMN-basierten Anwendungsszenarien zu gewährleisten, muss auch das eingesetzte Routingprotokoll entsprechend sicher sein. Soweit dem Autor bekannt, konnte sich unter diesem Gesichtspunkt keine der existierenden Lösungen in der Praxis durchsetzen, da entweder der Overhead der verschiedenen Ansätze zu hoch oder aber die getroffenen Annahmen in Sinne der Sicherheit zu stark und damit in der Praxis lediglich begrenzt umsetzbar sind.

In dieser Arbeit wird ein alternativer, umfassender Ansatz namens Position-Aware, Secure and Efficient mesh Routing (PASER) vorgestellt. Dieses neue Routingverfahren bietet eine höhere Sicherheit gegen Routingattacken als die bestehenden IEEE 802.11s/i-Sicherheitsmechanismen und sogar als das sichere Routingprotokoll Authenticated Routing for Ad-hoc Networks (ARAN), wobei allerdings im Hinblick auf die praktische Einsetzbarkeit auf starke Annahmen verzichtet wird. Es wird gezeigt, dass PASER in realistischen UAV-WMN Szenarien eine vergleichbar hohe Performanz erreicht, wie sie mit dem derzeit weit verbreiteten, aber unsicheren Routingprotokoll Hybrid Wireless Mesh Protocol (HWMP) in Kombination mit den IEEE 802.11s Sicherheitsmechanismen

möglich ist. Zwei repräsentative Szenarien werden hierfür betrachtet: (1) ubiquitärer ad-hoc Netzzugriff und (2) die effiziente Erkundung grösserer Gebiete im Katastrophenschutz. Zur Leistungsbewertung werden ein durch Experimente validiertes OMNeT++-basiertes WMN-Modell mit wirklichkeitsgetreuen UAV-Mobilitätsmustern und eben falls ein aus Experimenten abgeleitetes Kanalmodell für die direkte Funkverbindung zwischen UAVs herangezogen. Bei der Analyse der Ergebnisse werden auch die Verzögerungen der Routenfindung und der Nachrichten-Overhead der Protokolle berücksichtigt.

Diese Arbeit und das in diesem Rahmen erforschte PASER-Verfahren sollen einen wesentlichen Beitrag leisten auf dem Weg zur Entwicklung sicherer, praxistauglicher Routingprotokolle mit dem Ziel einer möglichst hohen Verbreitung eines solchen Protokolls in hochdynamischen WMNs.

Contents