

University of Wollongong
Research Online

University of Wollongong Thesis Collection
1954-2016

University of Wollongong Thesis Collections

2009

Contribution to securing wireless mesh networks

Shams Ud Din Qazi
University of Wollongong, shams@uow.edu.au

Follow this and additional works at: <https://ro.uow.edu.au/theses>

University of Wollongong

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material.

Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Recommended Citation

Qazi, Shams UD, Contribution to securing wireless mesh networks, MCompSc-Res thesis, School of Computer Science and Software Engineering, University of Wollongong, 2009. <http://ro.uow.edu.au/theses/792>

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

NOTE

This online version of the thesis may have different page formatting and pagination from the paper copy held in the University of Wollongong Library.

UNIVERSITY OF WOLLONGONG

COPYRIGHT WARNING

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.



Contribution to Securing Wireless Mesh Networks

A thesis submitted in fulfillment of the
requirements for the award of the degree

Masters by Research

from

UNIVERSITY OF WOLLONGONG

by

Shams Ud Din Qazi

School of Computer Science and Software Engineering
June 2009

© Copyright 2009

by

Shams Ud Din Qazi

All Rights Reserved

Dedicated to
My Parents

Declaration

This is to certify that the work reported in this thesis was done by the author, unless specified otherwise, and that no part of it has been submitted in a thesis to any other university or similar institution.

Shams Ud Din Qazi
June 3, 2009

Abstract

A wireless mesh network (WMN) comprises of mesh access points (MAPs)/mesh routers and mesh clients (MCs), where MAPs are normally static and they form the backbone of WMNs. MCs are wireless devices and dynamic in nature, communicating among themselves over possibly multi-hop paths, with or without the help of MAPs. Security has been a primary concern in order to provide protected communication in WMNs due to the open peer-to-peer network topology, shared wireless medium, stringent resource constraints and highly dynamic environment. These challenges clearly make a case for building multi-layer security solution that achieves both wide-range protection and desirable network performance.

In this thesis, we attempt to provide necessary security features to WMNs routing operations in an efficient manner. To achieve this goal, first we will review the literature about the WMNs in detail, like WMN's architecture, applications, routing protocols, security requirements. Then, we will propose two different secure routing protocols for WMNs which provide security in terms of routing, data and users as well.

The first protocol is a cross-layer secure protocol for routing, data exchange and Address Resolution Protocol (ARP) problems (in case of LAN based upon WMNs). Our protocol is a *ticket-based ad hoc on demand distance vector* (TAODV) protocol, a secure routing protocol that is based on the design of the Ad Hoc on demand distance vector (AODV) protocol. Due to the availability of a backbone, we incorporate the Authentication Server (AS) for the issuance of tickets which are further used for secure routing, transfer of public keys and MAC addresses in one single step. By incorporating the public keys, source and destination can easily generate their shared secret key based upon Fixed Diffie-Hellman key exchange protocol for data encryption and decryption. Our protocol is secure against both active as well as passive attacks.

The second proposed protocol is to “achieve user anonymity in WMNs”. This

protocol is also ticket-based protocol. The ticket is issued by Network Operator (NO) which provides user anonymity, user authentication and data confidentiality/privacy throughout the WMN. Our protocol is inspired by the blind Nyberg-Rueppel digital signature scheme. In this protocol NO issues tickets to valid users only and these users can then use these tickets to access Internet or to access services provided by Internet Gateway (IGW). IGW can only verify these tickets whether tickets are valid or not but can not check “Identity of ticket holder”. This way, user anonymity has been achieved along with user authentication and data privacy throughout WMN.

Acknowledgements

First of all, I would like to thanks A/Prof Dr Yi Mu and A/Prof Dr Willy Susilo, my supervisors, for their guidance and constant support during my study. I must evidence their wealth of knowledge in the field of security and cryptography. I also appreciate their efforts in guiding me in the field of network security, especially in the area of cryptography.

I am grateful to University of Sciences and Technology, Pakistan for providing me this opportunity to pursue my higher studies in University of Wollongong by giving financial support.

I would like to thanks all of my research group members especially Xinyi Huang, Wei Wu and Siamak Fayyaz Shahandashti, for their help in learning cryptography. I would also like to thank all staff of Centre for Computer and Information Security Research and the School of Computer Science and Software Engineering.

Finally, I would like to thanks my parents, for their relentless support throughout my entire life with their love and guidance. Without them, I would never be able to have all my achievements.

Publications

1. Shams Qazi, Yi Mu and Willy Susilo. *Securing Wireless Mesh Networks with Ticket-Based Authentication*. 2nd International Conference on Signal Processing and Telecommunication Systems, ICSPCS'2008.

Contents

Abstract	v
Acknowledgements	vii
Publications	viii
1 Introduction	1
1.1 Background	1
1.2 Problem Description	2
1.3 Our Contribution	3
1.4 Thesis Structure	4
2 Wireless Mesh Networks Basics	5
2.1 Introduction	5
2.2 Network Architecture	7
2.2.1 Infrastructure WMNs	9
2.2.2 Client WMNs	10
2.2.3 Hybrid WMNs	11
2.3 Characteristics of WMNs	12
2.3.1 Multi-Hop Wireless Network	12
2.3.2 Support for Ad Hoc Networking	12
2.3.3 Mobility Factor	12
2.3.4 Access of Multiple Networks	13
2.3.5 Dependence of Power Consumption	13
2.3.6 Compatibility with Existing Wireless Networks	13
2.4 Applications of WMNs	13
2.4.1 Broadband Home Networking	14

2.4.2	Community and Neighborhood Networking	14
2.4.3	Enterprise Networking	15
2.4.4	Metropolitan Area Networks	16
2.4.5	Transportation Systems	17
2.4.6	Building Automation	17
2.4.7	Health and Medical Systems	17
2.4.8	Security Surveillance Systems	18
2.5	Routing Protocols	18
2.5.1	Ad-Hoc on Demand Distance Vector (AODV) Protocol	20
2.5.2	Dynamic Source Routing (DSR) Protocol	22
2.6	Security Requirements	24
2.6.1	General Security Requirements	24
2.6.2	Security Requirements for WMNs	27
2.7	Existing Secure Routing Protocols	29
2.7.1	ARAN	29
2.7.2	SAODV	30
2.7.3	SAR	30
2.8	Evaluation of Existing Secure Routing Protocols	32
2.8.1	ARAN	32
2.8.2	SAODV	33
2.8.3	SAR	33
2.9	Summary	33
3	Cryptography Basics	35
3.1	Introduction	35
3.2	Cryptography	36
3.2.1	Secret or Symmetric Key Cryptography	36
3.2.2	Public or Asymmetric Key Cryptography	37
3.3	Diffie-Hellman Key Exchange Protocol	38
3.3.1	Algorithm	39
3.4	Digital Signatures	40
3.4.1	General Scheme	40
3.4.2	Security Requirements for Digital Signature Schemes	42
3.5	Nyberg-Rueppel Signature Scheme	43
3.6	Blind Signatures	43

3.6.1	Functions	44
3.6.2	Protocol	44
3.6.3	Properties	45
3.7	Blinding the Nyberg-Rueppel Digital Signature	45
3.8	Summary	46
4	Ticket based Ad-Hoc On Demand Distance Vector Protocol	48
4.1	Introduction	48
4.2	Protocol Design	49
4.2.1	Notations	51
4.2.2	Setup	51
4.2.3	Proposed Run	52
4.2.4	In Case of New MAP	53
4.2.5	In Case of New MC	54
4.2.6	Communication Between Different MCs	55
4.2.7	Address Resolution Protocol Security	58
4.3	Security Analysis	58
4.4	Summary	60
5	Achieving User Anonymity in WMNs	62
5.1	Introduction	62
5.1.1	Anonymity and Its Importance	62
5.1.2	Application Scenario	63
5.2	Protocol Design	65
5.2.1	Notations	66
5.2.2	Registration of New Mesh Client	66
5.2.3	Ticket Generation Process	67
5.2.4	Proposed Run	69
5.2.5	Ticket Verification Process	72
5.2.6	Ticket Uniqueness Checking	73
5.3	Security Analysis	73
5.4	Summary	75
6	Conclusions	76
A	Glossary	79

List of Tables

1.1	Security issues related to each layer	3
3.1	Diffie-Hellman Key Exchange Algorithm	39
4.1	Certificate	52
4.2	Ticket	53

List of Figures

2.1	Wireless Mesh Network Architecture	6
2.2	Examples of mesh routers: (a) Conventional wireless router [1] and (b) Advanced Risc Machines (ARM)[2]	8
2.3	Infrastructure Wireless Mesh Network Architecture	9
2.4	Client Wireless Mesh Network Architecture	10
2.5	Hybrid Wireless Mesh Network Architecture	11
2.6	WMNs for broadband home networking	15
2.7	WMNs for community networking	16
2.8	Route Discovery in AODV Protocol	21
2.9	Route Discovery in DSR Protocol	23
2.10	Man-in-the-middle attack	27
2.11	Security Aware Routing Protocol	31
3.1	Secret or Symmetric Key Cryptography	37
3.2	Public or Asymmetric Key Cryptography	38
3.3	General Digital Signature Scheme	41
3.4	Verification of Digital Signature	42
4.1	Wireless Mesh Network with Authentication Server	50
4.2	Communication Process in Wireless Mesh Network	56
5.1	ISP using WMN for extension of Internet to users in remote area	63
5.2	Military Operation using WMN for communication	64
5.3	Internet extension using WMN	70