

# University of Wollongong - Research Online

## Thesis Collection

Title: Secure communication over mobile ad-hoc network

Author: Zhenfei Zhang

Year: 2009

Repository DOI:

### 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.**

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

2009

## Secure communication over mobile ad-hoc network

Zhenfei Zhang  
*University of Wollongong*

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

Zhang, Zhenfei, Secure communication over mobile ad-hoc network, ME-Res thesis, School of Electrical, Computer and Telecommunications Engineering, University of Wollongong, 2009. <http://ro.uow.edu.au/theses/839>

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](mailto: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.

# Secure Communication over Mobile Ad-hoc Network

A Thesis submitted in partial fulfilment of  
the requirements for the award of the degree

Master of Engineering by Research

from

University of Wollongong

by

Zhenfei Zhang

School of Electrical, Computer and Telecommunications  
Engineering

March 2009

# Declaration

I, Zhenfei Zhang, declare that this thesis, submitted in partial fulfilment of the requirements for the award of Master of Engineering by research, in School of Electrical, Computer and Telecommunications Engineering, University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. The document has not been submitted for qualification at any other academic institution.

# Acknowledgements

I would like to thank Dr. Raad Raad and A.Prof Willy Susilo, my supervisors, for their patient guidance and constant support. I admire Dr. Raad's knowledge in telecommunication and appreciate him taking me into the area of mobile ad hoc networking. I also respect A.P. Susilo's knowledge in cryptography field, and appreciate him guiding me in the right direction.

I would also like to thank my parents, who support me constantly with their love, without which I would never be able to have all my achievements.

# Publications

## **Conference Paper**

Zhenfei Zhang, Willy Susilo and Raad Raad, "Mobile Ad-hoc Network Key Management with Certificateless Cryptography", In Proceeding of the International Conference on Signal Processing and Communication Systems, 2008.

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Motivation . . . . .	1
1.2	The Challenges and Solutions . . . . .	2
1.3	Contribution of Thesis . . . . .	4
1.4	Thesis Structure . . . . .	4
<b>2</b>	<b>Key Management Schemes Review</b>	<b>6</b>
2.1	Pre-established Key Management . . . . .	6
2.1.1	Key Distribution . . . . .	6
2.1.2	Key Exchange . . . . .	8
2.2	Distributed System . . . . .	10
2.2.1	Public Key Cryptography with Distributed System . .	11
2.2.2	ID-based Cryptography with Distributed System . . .	14
2.2.3	Drawbacks of Distributed Models . . . . .	16
2.3	Transitive Trust Model . . . . .	16
2.3.1	Mobility-based Key Management . . . . .	16
2.3.2	Certificate Chain-based Key Management . . . . .	17
2.4	Conclusion . . . . .	21
<b>3</b>	<b>Secure Routing Protocols Review</b>	<b>23</b>



3.1	ARAN . . . . .	23
3.2	SAODV . . . . .	26
3.3	Ariadne . . . . .	28
3.4	SLSP . . . . .	30
3.5	SEAD . . . . .	32
3.6	Conclusion . . . . .	34
<b>4</b>	<b>Certificateless Cryptography over MANET</b>	<b>35</b>
4.1	Certificateless Cryptography . . . . .	36
4.2	Generic Model . . . . .	36
4.2.1	Fully Distributed System . . . . .	38
4.2.2	Partially Distributed System . . . . .	39
4.3	Detailed Scheme . . . . .	40
4.4	Issues and Design Principles . . . . .	44
4.5	Conclusion . . . . .	45
<b>5</b>	<b>Secure Routing Protocol</b>	<b>46</b>
5.1	OLSR . . . . .	46
5.1.1	Basic Mechanism of OLSR . . . . .	46
5.1.2	Remaining Problems of OLSR . . . . .	47
5.2	Reputation System . . . . .	47
5.3	Reputed-OLSR . . . . .	49
5.3.1	Assumptions . . . . .	49
5.3.2	Generic Model . . . . .	49
5.3.3	Detailed Protocol . . . . .	50
5.4	Conclusion . . . . .	56
<b>6</b>	<b>Security Issues</b>	<b>58</b>
6.1	Fake Route Information . . . . .	59

6.2	Man in the Middle . . . . .	59
6.3	ID Stealth . . . . .	60
6.4	Pseudo Spoofing . . . . .	60
6.5	Whitewashing . . . . .	61
6.6	Shilling . . . . .	61
<b>7</b>	<b>Simulation and Results</b>	<b>63</b>
7.1	CL-PKE Over MANET . . . . .	63
7.1.1	Simulation with C . . . . .	63
7.1.2	Simulation with OPNET . . . . .	65
7.2	Rep-OLSR . . . . .	71
7.2.1	Simulation against Whitewashing Attacks . . . . .	71
7.2.2	Simulation with OPNET . . . . .	72
<b>8</b>	<b>Conclusions</b>	<b>78</b>
<b>A</b>	<b>Results of Whitewashing attacks</b>	<b>84</b>
<b>B</b>	<b>Glossary</b>	<b>91</b>

# List of Figures

2.1	Key Distribution in Partially Distributed Model . . . . .	13
2.2	Certificate Graph $G$ [16] . . . . .	18
2.3	3 Steps to Establish a Certificate Chain [16] . . . . .	19
5.1	Network Setup . . . . .	51
5.2	Neighbour Discovery . . . . .	52
5.3	Polling . . . . .	54
5.4	TC Message Forwarding . . . . .	57
7.1	Simulation Results of CL-PKE over MANET with OPNET: 10 Users, Packet Dropped . . . . .	68
7.2	Simulation Results of CL-PKE over MANET with OPNET: 10 Users, Route Discovery Time . . . . .	68
7.3	Simulation Results of CL-PKE over MANET with OPNET: 10 Users, Packet Send . . . . .	69
7.4	Simulation Results of CL-PKE over MANET with OPNET: 10 Users, Packet Received . . . . .	69
7.5	Simulation Results of CL-PKE over MANET with OPNET: 20 Users, Packet Dropped . . . . .	70
7.6	Simulation Results of CL-PKE over MANET with OPNET: 20 Users, Route Discovery Time . . . . .	71

7.7	Simulation Results of CL-PKE over MANET with OPNET:	
	20 Users, Packet Send . . . . .	72
7.8	Simulation Results of CL-PKE over MANET with OPNET:	
	20 Users, Packet Received . . . . .	73
7.9	Simulation Results of Rep-OLSR over MANET with OPNET:	
	20 Users, Routing Delay . . . . .	73
7.10	Simulation Results of Rep-OLSR over MANET with OPNET:	
	20 Users, Hello Message . . . . .	74
7.11	Simulation Results of Rep-OLSR over MANET with OPNET:	
	20 Users, MPR Count . . . . .	75
7.12	Simulation Results of Rep-OLSR over MANET with OPNET:	
	20 Users, Traffic Dropped . . . . .	75
7.13	Simulation Results of Rep-OLSR over MANET with OPNET:	
	20 Users, Traffic Received . . . . .	76
7.14	Simulation Results of Rep-OLSR over MANET with OPNET:	
	20 Users, TC message forward . . . . .	77

# List of Tables

3.1	RREQ and RREP in ARAN . . . . .	25
5.1	MRP Reputation Table, Stage 1 . . . . .	53
5.2	MRP Reputation Table, Stage 2 . . . . .	55
5.3	MRP Reputation Table, Stage 3 . . . . .	56
6.1	Six Types of Attacks . . . . .	58
7.1	Programming Environment for Key Generation . . . . .	63
7.2	Simulation Results of CL-PKE over MANET with C . . . . .	64
7.3	The AODV Parameters . . . . .	67
7.4	Programming Environment for Simulation against Whitewash- ing Attack . . . . .	71

## **Abstract**

A Mobile Ad-hoc Network (MANET) is an ideal network that merely consists of mobile devices without any pre-established infrastructure. However, the secure communication over a MANET is not straightforward. In this thesis, we present a solution for MANET secure communication. Generally speaking, it covers two main areas, namely key management and secure routing.

In the key management area, we present an idea of adopting certificateless public key encryption (CL-PKE) schemes over mobile ad hoc network (MANET), which have not been explored before. In the current literature, there exist two main approaches, namely public key cryptography and identity-based (ID-based) cryptography. Unfortunately, they both have some inherent drawbacks. To avoid these obstacles, Al-Riyami and Paterson proposed certificateless cryptography systems. In this thesis, we adopt Al-Riyami's advantage over MANET. To implement CL-PKE over MANET and to make it practical, we incorporate the idea of Shamir's secret sharing scheme. The master secret keys are shared among some or all the MANET nodes. This makes the system self-organized once the network has been initiated. In order to provide more flexibility, we consider both a full distribution system and a partial distribution system.

In the secure routing area, we present the idea of adopting a reputation system over the optimized link state routing (OLSR) protocol. In the literature, there exist two main routing approaches, namely proactive routing and reactive routing. Several secure reactive routing protocols have been

proposed. However, as far as proactive routing is concerned, few secure protocols are presented, yet they all possess different drawbacks that make them only practical on certain routing protocols. One of major problems is how to determine whether a node is worthy of trust or not. In other networks, for example, peer-to-peer sharing networks, reputation systems are designed to judge users. Unfortunately, they are designed specifically for peer-to-peer systems, while the adoption to MANET is not very straightforward. To this end, we present our Rep-OLSR, which selects routes wisely based on users' former performance by periodically collecting polling results from neighbour nodes.

Finally, we demonstrate that our solution is robust against several types of attacks. We also test our solution with several simulations. The results of the simulations indicate that our solution efficiently secure the communication with little extra traffic compared with pure MANET routing protocols.