

University of Wollongong - Research Online

Thesis Collection

Title: Efficient authentication schemes for routing in mobile ad hoc networks

Author: Shidi Xu

Year: 2006

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

2006

Efficient authentication schemes for routing in mobile ad hoc networks

Shidi Xu

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

Xu, Shidi, Efficient authentication schemes for routing in mobile ad hoc networks, M.Comp.Sc. thesis, School of Information Technology and Computer Science, University of Wollongong, 2006.
<http://ro.uow.edu.au/theses/517>

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.



Efficient Authentication Schemes for Routing in Mobile Ad Hoc Networks

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

Master of Computer Science by Research

from

UNIVERSITY OF WOLLONGONG

by

Shidi Xu

School of Information Technology and Computer Science
June 2006

© Copyright 2006

by

Shidi Xu

All Rights Reserved

Dedicated to
my parents

Declaration

I, Shidi Xu, declare that this thesis, submitted in partial fulfilment of the requirements for the award of Master of Computer Science by research, in the School of Information Technology and Computer Science, 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.

Shidi Xu
June 22, 2006

Publication

Journal Paper

Shidi, Yi Mu, Willy Susilo. “Authenticated AODV Routing Protocol Using One-Time Signature and Transitive Signature Schemes”, *Journal of Networks*, pp. 47-53, Volume 1, Issue 1, 2006.

Conference Paper

Shidi Xu, Yi Mu, and Willy Susilo. “Secure AODV Routing Protocol Using One-Time Signature”, *In Proceedings of the International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, pp. 288-297, Springer, 2005.

Shidi Xu, Yi Mu, and Willy Susilo. “An Efficient Authentication Scheme for MANET Routing”, *In Proceedings of the 1st International Workshop on Security in Ubiquitous Computing Systems*, pp. 854-863, Springer, 2005.

Shidi Xu, Yi Mu, and Willy Susilo. “Online-Offline Signatures and Multisignatures for AODV and DSR Routing Security”, *Accepted in the 11th Australasia Conference on Information Privacy and Security (ACISP’06)*, 2006.

Abstract

Mobile ad hoc network (MANET) has been generally regarded as an ideal network model for group communications. However, the security deployment for MANET routing operations is problematic. Firstly, existing secured routing protocols are deficient in achieving both authentication efficiency and full scale of security. In addition, the diversity of routing protocols presents difficulties in the generalisation of the security design. The most possible candidate solution, the digital signature, has far from been properly implemented from an ad hoc point of view.

In this thesis, we are motivated to provide necessary security features to MANET routing operations in an efficient manner. Considering the feasibility of utilising digital signatures in MANET, we incorporate the notion of the online/offline signature scheme in our design, where the computational overhead is shifted to the offline phase. We also make use of the one-time signature scheme, which is efficient in computation, and the multisignature scheme, which is especially suitable for group authentication. Then, we observe the specialities of different routing protocols (AODV-ad hoc on-demand distance vector routing and DSR-dynamic source routing), as well as the similarities between above signature schemes.

In our design, we exploit the efficiency and the adaptability of signature schemes. As our contributions, we propose two authentication schemes to secure AODV and DSR protocol respectively. For AODV protocol, our ID-based online/offline signature schemes enhance the authentication performance by properly balancing the computational overhead, whereas the one-time signature scheme achieves the same objective by making trade-offs between computation power and memory storage. For DSR protocol, we provide a generic construction from ID-based online/offline signature schemes to ID-based multisignature schemes, so that the installation over AODV can be transformed to offer the same level of security for DSR. Our scheme is *unique*, in the sense that a single ID-based online/offline signature scheme can be applied to both AODV and DSR routing protocols.

Acknowledgements

I would like to thank Dr. Yi Mu and Dr. Willy Susilo, my supervisors, for their patient guidance and constant support during my study. I admire their wealth of knowledge in security and cryptography, and appreciate them taking me into the area of cryptography.

I am also grateful to Dr. Joonsang Baek. I appreciate his instruction on security proof methods, which helped me a lot in my later study.

I greatly appreciate Professor John Fulcher for his help in the English expression of this thesis, and the support received from all the staff in the School of IT and CS, University of Wollongong.

Finally, I would like to thank my parents, who support me constantly with their love. Without them, I would never be able to have all my achievements.

Contents

Publication	v
Abstract	vi
Acknowledgements	vii
1 Introduction	1
1.1 Motivation	1
1.2 The Challenges	2
1.3 The Solutions	3
1.4 Thesis Structure	4
2 MANET Preliminaries	6
2.1 Mobile Ad Hoc Networks	6
2.2 MANET Routing Protocols	7
2.2.1 AODV Routing Protocol	8
2.2.2 DSR Protocol	10
2.2.3 Other Routing Protocols	12
2.3 MANET Routing Security Requirements	13
2.3.1 Threats and Countermeasures	14
2.3.2 Security Requirements	16
2.4 Secure Routing protocols	17
2.4.1 ARAN Authentication Scheme	17
2.4.2 Other Secure Protocols	19
2.5 Summary	20
3 Cryptographic Preliminaries	22
3.1 Cryptography Basics	22
3.1.1 One-Way Functions	22

3.1.2	Cryptographic Hash Functions	24
3.1.3	Hash Chain	26
3.1.4	Random Oracle model	28
3.1.5	Elliptic Curve Cryptology Basics	30
3.1.6	Bilinear Pairing	31
3.2	Digital Signature Schemes	33
3.2.1	Generic Scheme	33
3.2.2	Security Requirements for Digital Signature Schemes	35
3.3	One-time Signature Schemes	35
3.3.1	Generic Scheme	36
3.3.2	Detailed Schemes	36
3.4	Identity based Signature Schemes	39
3.4.1	Generic Scheme	39
3.4.2	Security Arguments	40
3.5	Online/Offline Signatures	41
3.5.1	Constructions Based on One-time Signatures	41
3.5.2	Other Construction Approaches	42
3.6	Multisignature Schemes	43
3.6.1	Constructions based on RSA	43
3.6.2	Accountable Subgroup Multisignature Scheme	44
3.6.3	Security Arguments	46
3.7	Summary	47
4	ID-based Online/Offline Signature Schemes	48
4.1	Generic Scheme	48
4.2	Security Arguments	49
4.3	A Concrete Construction	50
4.3.1	Analysis	51
4.3.2	Security Proof	51
4.4	A Better Construction	54
4.4.1	Analysis	54
4.4.2	Security Proof	55
4.5	Summary	58
5	ID-based Multisignature Schemes	59
5.1	Generic Scheme	59

5.2	Security Arguments	60
5.3	Generic Construction of IBMS from IOS	61
5.3.1	The Scheme	62
5.3.2	Security Arguments	63
5.4	A Concrete Construction	63
5.4.1	Security Analysis	65
5.4.2	Efficiency Comparison	68
5.5	Summary	69
6	Authentication Schemes for MANET Routing Operations	70
6.1	AODV Security Considerations	70
6.2	Authentication Schemes for AODV	73
6.2.1	A Scheme based on ID-based Online/offline Signatures	73
6.2.2	A Scheme based on One-time Signatures	75
6.2.3	Key Chain Construction	76
6.2.4	The Scheme	76
6.2.5	A Feature for Gratuitous Route Reply	79
6.3	Authentication Scheme for DSR Using ID-based Multisignatures	82
6.3.1	DSR Security Considerations	82
6.3.2	Installation of IBMS over DSR	84
6.4	Summary	86
7	Conclusions and Future Work	88
A	Glossary	91
	Bibliography	93

List of Tables

5.1	ID-based Signatures Efficiency Comparison	68
5.2	ID-based Multisignatures Efficiency Comparison	69
A.1	Glossary	92

List of Figures

2.1	The Route Discovery Process for AODV Protocol	9
2.2	The Route Discovery Process for DSR Protocol	11
2.3	ARAN <i>RDP</i> Packet Propagation	18
2.4	ARAN <i>REP</i> Packet Propagation	19
3.1	Hash Chain Construction	27
3.2	Digital Signature Scheme	34
5.1	Generic Construction of IBMS	62
6.1	A Possible Attack in SAODV	72
6.2	IOS based Authentication Scheme for AODV Route Request Processing	74
6.3	HORS One-time Signature Scheme	77
6.4	Key Chain Construction	78
6.5	HORS based Authentication Scheme for AODV Route Request process- ing	80
6.6	IASM signature generation process in DSR	85
6.7	Detailed Algorithm for DSR <i>RREQ</i> packet	87