2006

Efficient authentication schemes for routing in mobile ad hoc networks

Shidi Xu
University of Wollongong

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

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

List of Tables

List of Figures