2009

Contribution to securing wireless mesh networks

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

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

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

List of Tables

List of Figures