AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Electronics and Communications Engineering Department

Design of a Proposed Certification Authority for Ad Hoc Wireless Networks

A Thesis submitted in
partial fulfillment of the requirements for the Degree of
Master of Science in Electrical Engineering.

Submitted by

Rania Sobhy Abdel Moniem

B.Sc. in Electrical Engineering
(Electronics and Communications Engineering, Cairo University, 2002)

Supervision by

Prof. Dr. Salwa Hussein EL Ramly
Department of Electronics and Communications Engineering
Faculty of Engineering, Ain Shams University

Prof. Dr. Mohamed Ibrahem Shedeed
Chairman of the Board of
Science and Technology Center for Excellence

Dr. Tarek Abdel Mageed Abdel Aziz
Communication Security Consultant,
EG-MOD.

EGYPT, CAIRO
2009

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Electronics and Communications Engineering Department

JUDGMENT COMMITTEE

Name: Rania Sobhy Abdel Moniem
Thesis: Design of a Proposed Certification Authority for Ad hoc Wireless Networks
Degree: Master of Science in Electrical Engineering

NAME, TITLE, AND AFFILIATION **SIGNATURE**

Prof. Dr. Khaled Ali Shehata …………………
College of Engineering and Technology (Examiner)
Arab Academy for Science and Technology and Maritime Transport.

Prof. Dr. Magdi Mahmoud Mohamed …………………
Electronics and Communications (Examiner)
Engineering Department, Faculty of Engineering, Ain Shams University.

Prof. Dr. Salwa El-Ramly …………………
Electronics and Communications (Supervisor)
Engineering Department, Faculty of Engineering, Ain Shams University.

Prof.Dr. Mohamed Ibrahem Shedeed …………………
Chairman of the Board of Science (Supervisor)
and Technology Center for Excellence, Ministry of Military Production.

Date: …/…/……….

Communication Department
Faculty of Engineering
Ain Shams University
Cairo - 2009

EGYPT, CAIRO
2009

Acknowledgments

I would like to exploit this chance to render my gratitude and thanks to whoever helped me in preparing my thesis. First, all gratitude is due to ALLAH, who made this success possible and affordable.

Many thanks go to my supervisor *Prof. Dr. Salwa El-Ramly* who provided me with all the needed information, data and guided me to use all appropriate resources that allowed me to put this thesis in its final form.

My best thanks go to my supervisor *Dr. Mohamed Shedeed* for being kindhearted father who granted me a lot of advice and guidance. He dedicated a lot of his own time supporting me and trying to get rid of all the obstacles I met in my way.

Special thanks go also to my supervisor *Dr. Tarek abdel Megeed* who encouraged, helped and supported me throughout the hard times I met in preparing this thesis from the very beginning to the end. I should thank him for countless interesting discussions and for attending countless practice talks without a complaint.

I am also grateful to by Dr. Nabil Hamdy. He also well interested me in the topic of networks security. I'm very proud to be one of his students.

Last but not the least; my thanks and appreciation to all of *my friends and colleagues* who have extended their helping hand in one way or another and provided several valuable suggestions without which this thesis would not have been accomplished.

My love goes to *my family* for being a partisan, taking my side, providing me the opportunity to pursue my dreams and supporting me through my study.

Thanks a million for our Minister, the Minister of state of the Military Production for permitting us to continue our post-graduate studies, providing us with all the materialistic and morale facilities that helped us to complete our work without any hardships.

EGYPT, CAIRO
2009

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Electronics and Communications Engineering Department

STATEMENT

This Dissertation is submitted to Ain Shams University in partial fulfillment of the Degree of Master of Science in Electrical Engineering (Electronics and Communications Engineering).

The work include in this thesis was received by author at the Department of Electronics and Communications Engineering, Faculty of Engineering, Ain Shams University, Cairo, Egypt.

No part of this thesis was submitted for a degree or qualification at any other university or institution.

Name: Rania Sobhy Abdel Moniem

Signature: …………………………..

Date: ……/……../………

EGYPT, CAIRO
2009

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Electronics and Communications Engineering Department

CURRICULUM VITAE

Name	:Rania Sobhy Abdel Moniem
Date of birth	: 21/6/1979
Place of birth	: Egypt, Giza.
Nationality	: Egyptian
First university degree	: B.Sc. in Electrical Engineering (Electronics and Communications Engineering, Cairo University, 2002)
Certification date	: May, 2002.

Name: Rania Sobhy Abdel Moniem

Signature: ………………

Date: ……/……../………

EGYPT, CAIRO
2009

Thesis Abstract

Rania Sobhy Abdel Moniem, " Design of a Proposed Certification Authority for Ad hoc Wireless Networks", Master of Science in Electrical Engineering, Ain Shams University, Faculty of Engineering, Electrical Department, Electronics and Communications Engineering, 2009.

Abstract

A wireless ad hoc network is a network where a set of mobile devices communicates among themselves using wireless transmission without the support of fixed or stationary infrastructure. The open and dynamic operational environment of ad hoc network composes it vulnerable to various network attacks and poses a great challenge to system security designers for many reasons. In order to achieve a high level of security and privacy for the Ad-hoc network, digital signature is used. It is used to maintain the data confidentiality, user authentication and to prevent any unauthorized person to access to the network.

In this thesis, a proposed certification authority for wireless ad hoc network is designed, which consist of database contains all the information needed for the generation and issuance of digital certificates in addition to the registration authority to register the information of the clients in the network. Also renewal digital certificates mechanism, certificate revocation mechanism, and key management mechanism.

The basic components of the proposed certification authority is aimed to provide a strong authentication and secure file transmission for wireless ad hoc network by issuing digital certificates to the participants to achieve privacy, access control, integrity, and confidentiality of data over the network.

We use simulation software to implement the proposed CA and clients through a virtual wireless ad hoc network. The CA generates and issues digital certificates for clients and also verifies its digital signature to check the validation of the client’s certificates. Finally, there are several experiments and tests done to verify the performance of wireless network against unauthorized user.

CONTENTS

CHAPTER (1): INTRODUCTION

CHAPTER (2): SECURITY IN WIRELESS AD HOC NETWORK

CHAPTER (3): CRYPTOGRAPHY OVERVIEW

CHAPTER (4): PUBLIC KEY INFRASTRUCTURE

CHAPTER (5): DESIGN AND IMPLEMENTATION OF A PROPOSED CERTIFICATION AUTHORITY FOR WIRELESS AD HOC NETWORK

CHAPTER (6): CONCLUSIONS AND FUTURE WORK

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AES	**A**dvanced **E**ncryption **S**tandard
ANSI	**A**merican **N**ational **S**tandards **I**nstitute
AODV	**A**d hoc **O**n-demand **D**istance **V**ector
ARAN	**A**uthenticated **R**outing **A**d hoc **N**etworks
BAN	**B**ody **A**rea **N**etwork
CA	**C**ertification **A**uthority
CPU	**C**entral **P**rocessing **U**nit
CRL	**C**ertificate **R**evocation **L**ist
CTS	**C**lear **T**o **S**end
DAP	**D**irectory **A**ccess **P**rotocol
DFD	**D**ata **F**low **D**iagram
DoS	**D**enial **o**f **S**ervice
DSA	**D**igital **S**ignature **A**lgorithm
DSDV	**D**estination **S**equenced **D**istance **V**ector
DSR	**D**ynamic **S**ource **R**outing
DSS	**D**igital **S**ignature **S**tandard
EE	**E**nd **E**ntity
FIPS	**F**ederal **I**nformation **P**rocessing **S**tandards
gcd	**G**reatest **C**ommon **D**ivision
GF	**G**aussian **f**ield
GHz	**G**ega **H**ertz
GPRS	**G**eneral **P**acket **R**adio **S**ervice
GUI	**G**raphical **U**ser **I**nterface
ID	**ID**entification
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
IP	**I**nternet **P**rotocol
ISM	**I**ndustrial, **S**cientific and **M**edical
ISO	**S**everal **I**nternational **O**rganization
ITU	**I**nternational **T**elecommunication **U**nion
LAN	**L**ocal **A**rea **N**etwork
LDAP	**L**ightweight **D**irectory **A**ccess **P**rotocol
MAC	**M**essage **A**uthentication **C**ode
MANET	**M**obile **A**d hoc **NET**work
MD5	**M**essage **D**igest **5**

mod	**M**odular **A**rithmetic
OSCP	**O**nline **C**ertificate **S**tatus **P**rotocol
PAN	**P**ersonal **A**rea **N**etwork
PDA	**P**ersonal **D**igital **A**ssistants
PKCS	**P**ublic **K**ey **C**ryptography **S**tandard
PKG	**P**ublic **K**ey **G**enerator
PKI	**P**ublic **K**ey **I**nfrastructure
RA	**R**egistration **A**uthority
RERR	**R**oute Error
ROTR	**ROT**ate **R**ight
RREP	**R**oute **REP**ly
RREQ	**R**oute **REQ**uest
RSA	**R**ivest **S**hamir **A**delman
RTS	**R**equest **T**o **S**end
SEAD	**S**ecure **L**ink **S**tate **P**rotocol
SODV	**S**ecure **A**d hoc **O**n-demand **D**istance **V**ector
SHA	**S**ecure **H**ash **A**lgorithm
SHR	**SH**ift **R**ight
SQL	**S**tructure **Q**uery **L**anguage
SRP	**S**ecure **R**outing **P**rotocol
SSH	**S**ecure **S**hell
SSL	**S**ecure **S**ocket **L**ayer
TCP	**T**ransmission **C**ontrol **P**rotocol
TTP	**T**rust **T**hird **P**arty
UMTS	**U**niversal **M**obile **T**elecommunication **S**ystem
WLAN	**W**ireless **L**ocal **A**rea **N**etwork
WPAN	**W**ireless **P**ersonal **A**rea **N**etwork
WRP	**W**ireless **R**outing **P**rotocol
ZRP	**Z**one **R**outing **P**rotocol

LIST OF SYMBOLS

A,B,C,D,E,F,G,H	32 bit Registers for MD buffer
C	Cipher Text
D_K	Decryption Algorithm using a key
d	Public Key
E_K	Encryption Algorithm using a key
e	Private Key
g	Function for Expand Key
H(x)	Hash Code of Message
h	Hash Value
in(in0,…….,in15)	Input Block Matrix
K	Secret Key
K0,K1,K2…….K63	Additive Constants 32 bit word
KA, KB	Public Key of Node A,B
KR_b	Private Key of b
KUa	Public Key of b
k	Arbitrary Integer
(k,n)	Threshold Parameters
L	Number of Fixed Size Blocks
M	Plain Text
n	Product of Prime Numbers
out (ou0,…..,ou15)	Output Block Matrix
p	Prime Number
q	Prime Number
S	Substitution box
s (s0,0….…..,s3,3)	State Array Matrix
T1,T2	Primitive Logical Functions
t0……t79	Step Number
v2	version 2