



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 Ibrahim 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
Arab Academy for Science and Technology and Maritime Transport.

.....
(Examiner)

Prof. Dr. Magdi Mahmoud Mohamed

Electronics and Communications
Engineering Department, Faculty of Engineering, Ain Shams University.

.....
(Examiner)

Prof. Dr. Salwa El-Ramly

Electronics and Communications
Engineering Department, Faculty of Engineering, Ain Shams University.

.....
(Supervisor)

Prof. Dr. Mohamed Ibrahim Shedeed

Chairman of the Board of Science
and Technology Center for Excellence, Ministry of Military Production.

.....
(Supervisor)

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

<i>ABSTRACT</i>	<i>i</i>
<i>LIST OF FIGURES</i>	<i>ii</i>
<i>LIST OF TABLES</i>	<i>iv</i>
<i>LIST OF ABBREVIATIONS</i>	<i>v</i>
<i>LIST OF SYMBOLS</i>	<i>vii</i>

CHAPTER (1): INTRODUCTION

1.1 Problem Statement and Solution Overview.....	1
1.2 Thesis Organization	3

CHAPTER (2): SECURITY IN WIRELESS AD HOC NETWORK

2.1 Introduction.....	6
2.2 Ad hoc Network Definition.....	7
2.3 Ad hoc Networks Classification.....	8
2.3.1 Body Area Network.....	9
2.3.2 Personal Area Network.....	9
2.3.3 Wireless Local Area Network.....	10
2.4 Ad hoc Network Characteristics.....	12
2.4.1 Temporary Network.....	12
2.4.2 Dynamic Network Architecture.....	13
2.4.3 Short-range Network.....	13
2.4.4 Self-organizing Network.....	13
2.4.5 Constrained Devices.....	13
2.4.6 Similar Devices.....	14
2.5 Ad hoc Network Applications	14
2.5.1 Military Tactical Networks.....	14
2.5.2 Personal Area Networks.....	14
2.5.3 Sensor Networks.....	14
2.5.4 Collaborative Networking.....	15
2.5.5 Disaster Area Networks.....	15
2.6 Challenges in Ad-hoc Networks.....	15
2.6.1 No Trusted Third Parity.....	15
2.6.2 Routing Problems.....	15
2.6.3 Absence of Infrastructure.....	16
2.6.4 Roaming Dangerous Environment.....	16
2.6.5 Dynamic Changing Topologies.....	17
2.6.6 Limited Power Resources.....	17
2.6.7 Scalability.....	17
2.7 Security Attacks, Services, and Mechanisms.....	18
2.7.1 Security Attacks.....	18
2.7.2 Security Services.....	20
2.7.3 Security Mechanisms.....	21

Contents

2.8 Security Architecture for Ad-hoc Networks.....	22
2.9 Routing in Ad hoc Networks.....	25
2.9.1 Destination Sequenced Distance Vector.....	26
2.9.2 Dynamic Source Routing.....	26
2.9.3 Ad hoc On-demand Distance.....	28
2.10 Secure Routing in Ad hoc Networks.....	33
2.11 Key Management in Ad hoc Networks.....	33
2.11.1 Two Principles for Ad hoc Key Management.....	34
2.11.2 Key Management Scheme in Ad hoc Networks.....	36
2.12 Summary.....	38

CHAPTER (3): CRYPTOGRAPHY OVERVIEW

3.1 Introduction.....	40
3.2 Cipher System Components.....	40
3.3 Symmetric Key Cryptography.....	42
3.3.1 Advanced Encryption Standard (AES).....	43
3.4 Asymmetric Key Cryptography.....	54
3.4.1 Rivest Shamir Adleman (RSA).....	56
3.5 Authentication Mechanism.....	58
3.5.1 Authentication Functions.....	58
3.5.2 Secure Hash Algorithm (SHA256).....	61
3.5.3 Digital Signature Overview.....	65
3.6 Summary.....	67

CHAPTER (4): PUBLIC KEY INFRASTRUCTURE

4.1 Introduction.....	69
4.2 PKI Definition.....	70
4.3 The Core Components of PKI.....	70
4.3.1 Certification Authority(CA).....	71
4.3.2 Registration Authority(RA).....	72
4.3.3 PKI Repositories.....	73
4.3.4 PKI Users.....	73
4.3.5 Digital Certificate.....	74
4.4 PKI Architectures.....	74
4.4.1 Hierarchical PKI Architectures.....	75
4.4.2 Mesh PKI Architectures.....	76
4.4.3 Bridge PKI Architecture.....	76
4.5 PKI Data Structures.....	78
4.5.1 X.509 Public Key Certificates.....	78
4.5.2 Certificate Revocation Lists (CRLs).....	81
4.6 CA Functions.....	83
4.6.1 Verifying Identity.....	84
4.6.2 Certificate Contents.....	84

4.6.3 Issuing Certificates.....	84
4.6.4 Revoking Certificates.....	86
4.7 PKI Functionality.....	86
4.7.1 Key Generation.....	87
4.7.2 Digital Signatures.....	87
4.7.3 Message Encryption.....	87
4.7.4 Key Distribution.....	88
4.7.5 User Verification.....	88
4.7.6 Message Decryption and Verification.....	89
4.8 Summary.....	89

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

5.1 Introduction.....	91
5.2 Design Framework.....	91
5.2.1 Initialization Phase.....	91
5.2.1 Authorization Phase.....	92
5.3 Certification Authority Design.....	93
5.3.1 Database.....	94
5.3.2 Security Library Classes.....	96
5.3.3 CA Functions.....	97
5.4 Client Design.....	101
5.4.1 Client Components.....	102
5.4.2 Certificate Validation.....	103
5.4.3 Secure File Transmission.....	104
5.5 Software Implementation.....	106
5.6 The Proposed CA Design Analysis.....	116
5.6.1 CA Simulation.....	116
5.6.2 Client Simulation.....	120
5.7 Performance Testing and Evaluation.....	126
5.8 Summary.....	133

CHAPTER (6): CONCLUSIONS AND FUTURE WORK

6.1 Conclusions.....	134
6.2 Future Work.....	136
REFERENCES.....	137
Appendix A.....	140
Appendix B.....	143

LIST OF FIGURES

Figure (2.1)	Wireless Ad-hoc Networks are Conceptually Compared to Traditional Wireless Cellular Networks.....	8
Figure (2.2)	Ad-hoc Networks Classification.....	8
Figure (2.3)	BAN Configuration.....	9
Figure (2.4)	PAN Configuration.....	10
Figure (2.5)	WLAN Configurations: Infrastructure Based.....	11
Figure (2.6)	WLAN Configurations: Ad hoc Network.....	12
Figure (2.7)	Common Network Attacks.....	18
Figure (2.8)	Security Services and the Corresponding Mechanisms.....	22
Figure (2.9)	Security Layer Architecture for MANETs.....	23
Figure (2.10)	Ad-hoc Routing Protocols Hierarchy	24
Figure (3.1)	Simplified Model of Cipher System Components..	41
Figure (3.2)	Simplified Model of Symmetric Encryption.....	42
Figure (3.3)	AES Encryption and Decryption.....	44
Figure (3.4)	AES Data Structures.....	45
Figure (3.5)	AES Encryption Round.....	46
Figure (3.6)	AES SubBytes Operations.....	48
Figure (3.7)	AES ShiftRow Operations.....	49
Figure (3.8)	AES MixColumn Operations.....	50
Figure (3.9)	AES Add Round Key Operations.....	51
Figure (3.10)	AES Key Expansion.....	52
Figure (3.11)	Simplified Model of Asymmetric Encryption.....	55
Figure (3.12)	Summarizes the RSA Algorithm.....	57
Figure (3.13)	Symmetric Encryption.....	58
Figure (3.14)	Public Key Encryption.....	59
Figure (3.15)	Message Authentication Code.....	60
Figure (3.16)	Single Step Processing in SHA2.....	62
Figure (3.17)	Message Digest Generation.....	65
Figure (4.1)	Technical Components and Operational Flow of a PKI.....	71
Figure (4.2)	Hierarchical PKI Architectures.....	75
Figure (4.3)	Mesh PKI Architectures.....	76
Figure (4.4)	Bridge PKI Architecture.....	77

List of Figures

Figure (4.5)	X.509 Public Key Certificate.....	79
Figure (4.6)	X.509 Certification Revocation List.....	82
Figure (4.7)	CA Issuing Certification.....	85
Figure (4.8)	Verifying Sender Identity.....	88
Figure (5.1)	Initialization Phase.....	92
Figure (5.2)	Authorization Phase.....	93
Figure (5.3)	CA Structure	94
Figure (5.4)	Certificate, key Store Handler, and Key Store Information Classes.....	96
Figure (5.5)	Session Key Handler, SHA256, AES192, and RSA Classes.....	96
Figure (5.6)	Key Store File Generation DFD.....	98
Figure (5.7)	Certificate Generation DFD	100
Figure (5.8)	CRL Generation DFD.....	101
Figure (5.9)	Users Database.....	101
Figure (5.10)	Client Structure	103
Figure (5.11)	Validation Process DFD	104
Figure (5.12)	Secure File Transmission Diagram.....	105
Figure (5.13)	CA Application	116
Figure (5.14)	CA Access Control.....	116
Figure (5.15)	New Client Registration.....	117
Figure (5.16)	Key File Generation.....	118
Figure (5.17)	Generating and Issuing Certificate.....	119
Figure (5.18)	New Client Information.....	119
Figure (5.19)	Deactivate User Process.....	120
Figure (5.20)	Client Application.....	121
Figure (5.21)	Client Certificate.....	121
Figure (5.22)	Update Settings at Transmitter.....	122
Figure (5.23)	Revoked Client.....	123
Figure (5.24)	Expired Client.....	124
Figure (5.25)	Transmitter Message.....	125
Figure (5.26)	Receiver Message.....	126
Figure (5.27)	Wireless Ad hoc Network.....	127
Figure (5.28)	Run Time Experiment Results.....	130
Figure (5.29)	Wireless Ad hoc Network.....	131

LIST OF TABLES

Table (2.1)	Comparison Between On-Demand versus Table Driven Based Routing Protocols.....	25
Table (2.2)	Comparison Between DSDV, DSR, and AODV Ad hoc Routing Characteristics.....	32
Table (2.3)	Secure Ad hoc Routing Protocol Comparison.....	33
Table (3.1)	AES Parameters.....	43
Table (3.2)	AES S-Boxes and Inverse S-Boxes.....	48
Table (3.3)	Rcon Constant Round.....	53
Table (3.4)	Arbitrated Digital Signatures Techniques.....	52
Table (5.1)	Client Table.....	95
Table (5.2)	Access Control Table.....	95
Table (5.3)	Wireless Ad hoc Network Clients Parameters.....	128
Table (5.4)	Run Time Experiment of Results.....	129
Table (5.5)	The Parameters of the Client in the Secured Network.....	131
Table (5.6)	Validity Certificate Experiment Results.....	132

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 of 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 field
GHz	G ega H ertz
GPRS	G eneral P acket R adio S ervice
GUI	G raphical U ser I nterface
ID	I dentification
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 N ETwork
MD5	M essage D igest 5

List of Abbreviations

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 E rror
ROTR	R OTate R ight
RREP	R oute R EPlY
RREQ	R oute R EQuest
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	S Hift 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(in ₀ ,.....,in ₁₅)	Input Block Matrix
K	Secret Key
K ₀ ,K ₁ ,K ₂K ₆₃	Additive Constants 32 bit word
K _A , K _B	Public Key of Node A,B
K _{R_b}	Private Key of b
K _{U_a}	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 (ou ₀ ,.....,ou ₁₅)	Output Block Matrix
p	Prime Number
q	Prime Number
S	Substitution box
s (s ₀ ,0.....,s ₃ ,3)	State Array Matrix
T ₁ ,T ₂	Primitive Logical Functions
t ₀t ₇₉	Step Number
v ₂	version 2