



AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Electronics Engineering and Electrical Communications

Efficient Security Protocols For Next Generation Wireless Networks

A Thesis submitted in partial fulfillment of the requirements of the degree
of
Doctor of Philosophy in Electrical Engineering
(Electronics Engineering and Electrical Communications)

by

Mohamed Abdel Aziz El-Bashary
Master of Science in Electrical Engineering
(Electronics Engineering and Electrical Communications)
Military Technical College, 2001

Supervised By
Prof. Dr. Adel El-Hennawy
Prof. Dr. Wagdi Anis
Dr. Ahmed Abdel Hafez

Cairo - (2016)



AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Electronics and Communications

Efficient Security Protocols For Next Generation Wireless Networks

by

Mohamed Abdel Aziz El-Bashary

Master of Science in Electrical Engineering
(Electronics Engineering and Electrical Communications)
Military Technical College, 2001

Examiners' Committee

Name and Affiliation

Prof.

Choose an item., University

Prof.

Choose an item., University

Dr.

Choose an item., University

Signature

.....

.....

.....

Date: 30 July 2016

Statement

This thesis is submitted as a partial fulfillment of Doctor of Philosophy in Electrical Engineering Engineering, Faculty of Engineering, Ain shams University.

The author carried out the work included in this thesis, and no part of it has been submitted for a degree or a qualification at any other scientific entity.

Mohamed Abdel Aziz El-Bashary

Signature

.....

Date: 30 July 2016

Researcher Data

Name:	Mohamed Abdel Aziz El-Bashary
Date of birth:	25/06/1968
Place of birth:	Cairo
Last academic degree:	Master of Science in Electrical Engineering
Field of specialization:	Communications
University issued the degree:	Military Technical College
Date of issued degree:	2001
Current job:	Officer Engineer in the Armed Forces

Thesis Summary

A Mobile Ad hoc Network (MANET) is a self organized and self configuring network composed of mobile nodes that are connected wirelessly. MANET has very particular features such as high mobility, multi-hop routing and the absence of any fix infrastructure. The wireless nodes operate as communication end-points as well as routers, enabling multi-hop wireless communication. Many practical applications are being developed for the use of mobile ad hoc networks in both military and civilian environments.

MANETs pose unique challenges, including limited power resources, low computation capabilities, limited storage capacity, less communication bandwidth, and more vulnerable to security attacks. The above mentioned constraints make security a challenge in MANETs.

Key management is a basic part of any secure communication that provides confidentiality, integrity and availability of the network. It supports the generation, distribution, storing, protection, and maintenance of keying material between authorized parties. Key management schemes should achieve robustness, key freshness, forward and backward secrecy, scalability, availability and efficiency. Key management protocols are classified into symmetric, asymmetric, group, and hybrid. Group key management is a point of interest for researchers with the growing usage of mobile devices and the rising of multicast communication.

In this research, first, a survey among the well known key management schemes in MANETs will be conducted to evaluate the security strength. Second, a new group key management scheme for MANETs will be proposed. The proposed key management scheme resolves the security holes in the studied schemes, and it is suitable to be deployed in the limited resources MANETs as well. Finally, the performance of the proposed novel scheme will be studied and analyzed in terms of security strength, memory storage, communication overhead, power consumption, simplicity, and scalability.

Key words: MANET, Group key management, security, multicast, Scyther.

Acknowledgment

First of all thanks to ALLAH Who helps me to accomplish this work.

I would like to express my sincere gratitude to my advisors Prof. Dr. Wagdy Anis, and Dr. Ahmed Abdel Hafez for the continuous support of my PhD study and related research, for their patience, motivation, and immense knowledge. Their guidance helped me in all the time of research and writing of this thesis.

I place on record, my sincere thank to the soul of Prof. Dr. Adel El-Hennawy, for his valuable guidance and encouragement, who passed away before completion of this work.

Besides my advisors, I would like to thank the rest of my thesis committee: Prof. Dr. Salwa El-Ramly and Prof. Dr. A. Hameed Gaafar for their insightful comments and encouragement.

My sincere thanks also go to Dr. Mohamed Mahmoud, Dr. Hesham Dahshan, Eng. Ahmed Hasan and Dr. Haitham Dawood, who provided me all their support and experience. Without their precious support it would not be possible to conduct this research.

I must express my very profound gratitude and appreciation to my mother, to my wife and to my beloved daughters for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Finally, I would like to express, my sense of gratitude to one and all, who directly or indirectly, have lent their hand in this venture.

This Thesis is dedicated to the Spirit of My Father, Abdel Aziz El-Bashary.

July 2016

Table of Contents

List of Figures	i
List of Tables	iii
List of Abbreviations	iv
List of Symbols	vi
CHAPTER 1: INTRODUCTION	1
1.1. General Overview	1
1.2. Motivation and Goals of the Study	2
1.3. Contribution of the Work	3
1.4. Organization of the Thesis	5
CHAPTER 2: MOBILE AD HOC NETWORKS (MANETS)	7
2.1. Overview of Wireless Ad hoc Networks	7
2.2. The Characteristics of Wireless Networks	8
2.3. Mobile Ad-Hoc Network Applications	10
2.4. MANET Architecture	10
2.4.1. Enabling Technologies:	11
2.4.2. Networking	12
2.4.3. Middleware and Applications:	12
2.5. Routing Protocol	12
2.5.1. Proactive Protocols	13
2.5.2. Reactive Protocols	15
2.5.3. Hybrid Protocols	17
2.6. Performance	17
2.7. Vulnerabilities of Routing Protocols	18
2.8. Attacks in Ad Hoc Networks	19
2.8.1. Passive attacks	20
2.8.2. Active attacks	20
2.9. Security Mechanisms	24
2.10 Auto Configuration	27
2.10.1 Conflict Detection Protocols	28
2.10.2 Protocols Avoiding Conflicts	29
2.10.3 Auto-Configuration and Security	29
CHAPTER 3: KEY MANAGEMENT IN AD HOC NETWORKS	31
3.1. Introduction	31
3.2. Characteristics of Key Management Schemes	33
3.2.1. Confidentiality	34
3.2.2. Key Authentication	34
3.2.3. Key Confirmation	34
3.2.4. Key Freshness	34
3.2.5. Resistant to Known Key Attacks (KKA)	35

3.2.6.	Forward Secrecy	35
3.2.7.	Backward Secrecy	35
3.2.8.	Key Independence	35
3.2.9.	Availability	35
3.2.10.	Survivability	35
3.2.11.	Robustness	36
3.2.12.	Efficiency	36
3.2.13.	Scalability	36
3.3.	Trust Models	36
3.3.1.	Centralized Trust Model	36
3.3.2.	Web-of-Trust Model	40
3.3.3.	Decentralized Trust Model	41
3.3.4.	Hybrid Trust Model	41
3.4.	Key Management Schemes in MANETs	41
3.5.	Asymmetric Key Management Schemes	42
3.5.1.	Secure Routing Protocol	42
3.5.2.	Ubiquitous and Robust Access Control	44
3.5.3.	Mobile Certificate Authority	45
3.5.4.	Self-organized Key Management	45
3.5.5.	Secure and Efficient Key Management	47
3.6.	Symmetric Key Management Schemes	48
3.6.1.	Distributed Key Pre-distribution Scheme (DKPS)	48
3.6.2.	Peer Intermediaries for Key Establishment (PIKE)	49
3.7.	Group Key Management Schemes	50
3.7.1.	Centralized Group Key Management Protocols	52
3.7.2.	Decentralized Group Key Management Protocols	53
3.7.3.	Distributed Group Key Management Protocols	53
3.8.	Discussion	53
	CHAPTER 4: A COMPARATIVE STUDY FOR GROUP KEY MANAGEMENT IN MANET	55
4.1.	Introduction	55
4.2.	Centralized Group Key Management Protocols	57
4.2.1.	With Keys Pre-distribution	57
4.2.2.	Without Keys Pre-distribution	60
4.3.	Decentralized Group Key Management Protocols	62
4.3.1.	Enhanced BAAL Protocol	63

4.3.2.	Dual Encryption Protocol (DEP)	64
4.3.3.	BALADE Protocol	65
4.3.4.	Other Protocols	67
4.4.	Distributed Group Key Management Protocols	67
4.4.1.	Chiang-Huang (C-H) Protocol	67
4.4.2.	Hierarchical, Simple, Efficient, and Scalable Group Key Management (HSESGK) Protocol	68
4.4.3.	Mobility Based Key Management protocol (MBKM)	73
4.4.4.	Other Protocols	76
4.5.	Discussion	77
4.5.1.	Centralized Group Key Management Schemes	78
4.5.2.	De-centralized Group Key Management Schemes	82
4.5.3.	Distributed Group Key Management Schemes	83
4.5.4.	Comparison of the Group Key Management Protocols	84
CHAPTER 5: A NEW EFFICIENT AND SECURE KEY MANAGEMENT SCHEME FOR MOBILE AD HOC NETWORKS		89
5.1.	Introduction	89
5.2.	The Proposed Scheme	89
5.2.1.	Cluster Formation	90
5.2.2.	Cluster Head (CH) Selection	91
5.2.3.	Group Key Generation and Distribution	92
5.2.4.	Cluster Group key Kc	92
5.2.5.	Cluster Head Group key KCH	93
5.2.6.	Session Key Ks	93
5.2.7.	Joining of a New Node	94
5.2.8.	Leaving of an Existing Node	95
5.2.9.	Message Flow of the Proposed Scheme	95
5.3.	Environment of Experiments	95
5.4.	Simulation Results	99
5.4.1.	Basic Performance Metrics	99
5.4.2.	Experiments Results	99
5.4.3.	Additional Performance Metrics	106
5.5.	Discussion of Simulation Results	109

CHAPTER 6: VERIFICATION OF THE PROPOSED PROTOCOL	112
6.1. Introduction	112
6.2. Scyther Tool	113
6.2.1. Verification of Claims	115
6.2.2. Automatic Claims	115
6.2.3. Characterization\	115
6.3. The Model Description	116
6.4. Properties Specifications	118
6.5. Formal Verification	119
6.6. Proposed Protocol Verification	120
6.6.1. Node (N1) Role	121
6.6.2. The First Cluster Head Role	122
6.6.3. The Second Cluster Head Role	123
6.6.4. The Second Node Role	124
6.7. Conclusion	125
CHAPTER 7: CONCLUSION AND FUTURE WORK	126
7.1. Conclusion	126
7.2. Suggestions for Future Work	130
REFERENCES	131

List of Figures

- Figure 2.1: MANET Architecture
- Figure 2.2: Range of Communication Technologies
- Figure 2.3: Passive Attack
- Figure 3.1: Categories of TTPs
- Figure 3.2: Establishment of Session Key Using KDC
- Figure 3.3: Components of a PKI
- Figure 3.4: The System Private Key
- Figure 3.5: An Example Of Certificate Chain
- Figure 3.6: Server Group Structure in SEKM
- Figure 3.7: Illustration of PIKE scheme
- Figure 3.8: The IP Multicast Model
- Figure 4.1: Classification of Group Key Management Protocols in MANETs
- Figure 4.2: Key Distribution Tree Based in the K-Means Algorithm
- Figure 4.3: The Group Key Generation and Distribution in Enhanced BAAL
- Figure 4.4: The Group Key Generation and Distribution in BALADE
- Figure 4.5: A Key Graph for C-H Protocol
- Figure 4.6: MANET Based on Clustering
- Figure 4.7: Double Multicast (Blue and Red) Trees Structure for a Cluster
- Figure 4.8: Blue Trees Point of View for Constructing Itself
- Figure 4.9: Red Trees Point of View for Constructing Itself
- Figure 4.10: Double Multicast (Blue and Red) `Trees Structure among Cluster Heads
- Figure 4.11: The Main Idea of the Compared Key Management Schemes.
- Figure 5.1: The Cluster Model in MANET
- Figure 5.2: The Message Flow of the Proposed Scheme
- Figure 5.3: PDP versus Number of Nodes (at 5 m/sec)
- Figure 5.4: Overheads versus Number of Nodes (at 5 m/sec)
- Figure 5.5: Packet Drop versus number of nodes (at 5 m/sec)
- Figure 5.6: PDP versus Speed (at 10 nodes)
- Figure 5.7: Overheads versus Speed (at 10 nodes)
- Figure 5.8: Packet Drop versus Speed (at 10 nodes)
- Figure 5.9: PDP versus No of Nodes for the Proposed Scheme at Different Speeds
- Figure 5.10: Overheads versus No of Nodes for the Proposed Scheme at Different Speeds
- Figure 5.11: Packet Drop versus No of Nodes for the Proposed Scheme at Different Speeds
- Figure 5.12: NRL versus No of Nodes for the Proposed Scheme at Different Speeds.

- Figure 5.13: Average Hop Count versus No of Nodes for the Proposed Scheme at Different Speeds.
- Figure 5.14: E-E Delay versus No of Nodes for the Proposed Scheme at Different Speeds.
- Figure 5.15: PLP versus No of Nodes for the Proposed Scheme at Different Speeds
- Figure 6.1: GUI of Scyther Tool
- Figure 6.2: Protocol Verification Flow Chart
- Figure 6.3: First Node Claims Result
- Figure 6.4: Cluster Head Claims Result
- Figure 6.5: Second Cluster Head Claims Result
- Figure 6.6: Second Node Claims Result

List of Tables

Table 2.1:	Attack of Network Layers
Table 3.1:	EBS Matrix
Table 4.1:	EBS Matrix
Table 4.2:	Comparison of Centralized Protocols
Table 4.3:	Comparison of Decentralized Protocols
Table 4.4:	Comparison of Distributed Protocols
Table 5.1:	Simulation Parameters of the Proposed Scheme
Table 5.2:	Various Performance Metrics for Different No. of Nodes at 5 m/s
Table 5.3:	Various Performance Metrics for Different No. of Nodes at 20 m/s
Table 6.1:	Protocol Verification Message Types

List of Abbreviations

5G	5th Generation
ACK	Acknowledgment
AKMP	Adaptive Key Management Protocol
AODV	Ad Hoc On Demand Distance Vector
AP	Access Point
ARQ	Automatic Repeat Request
ARQ	Automatic Repeat Request
BAN	Body Area Network
CA	Certificate Authority
CAN	Content Addressable Network
CBR	Constant Bit Rate
CFF	Cover-Free Family
CGK	Cluster Group Key
CH	Cluster Head
CM	Cluster Member
CR	Challenge-Response
CREP	Confirmation Reply
CREQ	Request for Confirmation
DCDP	Dynamic Configuration and Distribution Protocol
DCF	Distributed Coordination Function
DDHCP	Distributed Dynamic Host Configuration Protocol
DEP	Dual Encryption Protocol
DHCP	Dynamic Host Configuration Protocol
DKPS	Distributed Key Pre-distribution Scheme
DoS	Denial of Service
DSDV	Destination-Sequenced Outdistances Vector
DSR	Dynamic Source Routing
EBS	Exclusion Basis System
FEC	Forward Error Correction
GC	Global Controller
GDH	Group Diffie Hellman
GLC	Group of Local Controllers
GPS	Global Positioning System
GUI	Graphical User Interface
H&O	Hypercube and Octopus
IARP	Intra Zone Routing Protocol
IERP	Inter-Zone Routing Protocol
IKA	Initial Key Agreement
IoT	Internet of Things
KDC	Key Distribution Center
KEK	Key Encryption Key

KKa	Known Key Attacks
KS	Key Server
LAN	Local Area Network
LC	Local Controller
LKH	Logical Key Hierarchy
LKHW	Logical Key Hierarchy for Wireless sensor network
M2M	Machine-to- Machine
MAC	Medium Access Control
MAN	Metropolitan Area Network
MANET	Mobile Ad Hoc Network
MBKM	Mobility Based Key Management
MCH	Main Cluster Head
MOCA	Mobile Certificate Authority
MPR	Multi-point Relay
NRL	Normalized Routing Load
NS-2	Network Simulator -2
OLSR	Optimized Link State Routing
PAN	Personal Area Network
PDP	Packet Delivery Percentage
PFS	Perfect Forward Secrecy
PHY	Physical Layer
PIKE	Peer Intermediaries for Key Establishment
PLP	Packet Loss Percentage
RA	Registration Authority
RREP	Route Reply
RREQ	Route Request
RRER	Route Error
SEKM	Secure and Efficient Key Management
SGK	Subgroup Key Server
SHA	Secure Hash Algorithm
SPDL	Structured Programming Descriptive Language
SSD	Secure Shared Key Discovery
TC	Topology Control
TCP	Transport Control Protocol
TEK	Traffic Encryption Key
TTP	Trusted Third Party
URSA	Ubiquitous and Robust Access Control
VANET	Vehicular Ad Hoc Network
WAN	Wide Area Network
WMN	Wireless Mesh Network
ZRP	Zone Routing Protocol