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	**Signature**
Prof.	……………….
Choose an item., University	
Prof.	……………….
Choose an item., University	
Dr.	……………….
Choose an item., University	

.

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

List of Tables

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