Ain Shams University
Faculty of computers and Information sciences
Computer Science Department

SECURE AND EFFICIENT KEY MANAGEMENT IN AD-HOC NETWORKS

Thesis Submitted as a Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy of Computer Science

By

Walid Ibrahim Ibrahim Khedr
Teaching Assistant at Computer Science Department
Faculty of computers and Informatics
Zagazig University

Under Supervision of

Prof. Dr. Ahmed Mohamed Hamad
Dean of Faculty of Information Systems and Computer Science
October 6 University

Prof. Dr. Mohamed Abas Shouman
Dean of the Faculty of Computer and Informatics
Zagazig University

Prof. Dr. Taha Ibrahim El Areef
Prof. of Computer Science
Computer Science Department
Faculty of Computer and Information Sciences
Ain Shams University

Cairo - 2008

To my mother, my late father, my wife, and my children.

ACKNOWLEDGMENTS

Special thanks to my advisor, Prof. Ahmed Mohamed Hamad, for his unfailing support and guidance. I am also grateful to Prof. Mohamed Abbas Shouman and Prof. Taha Ibrahim El Areef for their guidance.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

N_i	The unique ID of node *i*
$G_i^{N_x}$	The unique ID of group *i* led by node N_x
$\lvert G_i^{N_x} \rvert$	Group Size of group *i* led by node N_x
$K_{G_i}^{N_x}$	Group key of group *i* led by node N_x
R	Network leader
K^R	Network global key
KU_R	Network leader's public key
KM_{N_i}	Node N_i 's master key
KU_{N_i}	Node N_i 's public key based on elliptic curve Diffie-Hellman
KR_{N_i}	Node N_i 's private key based on elliptic curve Diffie-Hellman
KT_{N_i}	Node N_i 's termination key. This key is used by node $N_j \in G_k^{N_i}$ when its leader N_i is terminated to find the leader of the group that N_i belongs to
K_{L,N_i}	This is a peer-to-peer shared key between node N_i and its group leader *L*. This key is used to authenticate node N_i to *L*.
WG	The witness group, a group of nodes that witness that *R* is the network leader
T_{N_i}	Total number of nodes leaded by node N_i , equal zero if N_i does not lead any node i.e. non-leader node.
g_i	The undirected graph that represents node *i* and its immediate neighbors. Vertices of g_i represent N_i and its immediate neighbors, and an edge between two nodes exist only if the two nodes are within the transmission range of each other.
J_i	The adjacency matrix of g_i .
Q_i	The set of all cliques in g_i . $Q_i = \{q_1^i, q_2^i, ..., q_m^i\}$
$\lvert q_j^i \rvert$	The size of clique q_j^i of the graph g_i .
$q_{\max}^i$	The maximum clique of the graph g_i , $q_{\max}^i \in Q_i$
$q_{\max}$	The clique with the maximum size among $q_{\max}^i, i = 1,...,n$ where *n* is the number of graphs in the network, i.e.
$E_K(M)$	Encryption of message *M* using key *K*

$D_K(M)$	Decryption of message *M* encrypted by key *K*
$Sign_K(M)$	Signature of message *M* using the key *K*
$Ver_K(M)$	Verification of message *M* signed by key *K*
$\mathbb{Z}_p$	The set of prime integer
((•))	Local broadcast or Group broadcast
((•))	Global Broadcast
━━━━	Connect two nodes within the transmission range of each other and trust each other
- - - - - - - - -	Communication between two nodes out of the transmission range of each other
————	Connect two nodes that trust each other and not necessary within the transmission range of each other.
— — —	Connect two nodes within the transmission range of each other but do not trust each other
	Key establishment using the proposed key exchange algorithm

LIST OF ABBREVIATIONS

ECBD	Elliptic Curve Burmester and Desmedt protocol
MRKT	Mixed-Radix Key Transport protocol
GNY	Gong, Needham and Yahalom logic
KDC	Key Distribution Center
CA	Certificate Authority
PGP	Pretty Good Privacy
TTL	Time to Live
NLR	Node Leave Request
NKU	Network Key Update
KEF	Key Establishment Function
KDF	Key Derivation Function
LRR	Leader Replacement Reply
CREP	Certificate Reply
CREQ	Certificate Request
NJR	Node Join Request
WG	Witness Group
RCR	Root Confirmation Request
KEP	Key Establishment Permission
NLEP	Network Leader Election Protocol
NLCP	Network Leader Confirmation Protocol
NKEP	Network Key Establishment Protocol
GKEP	Group Key Establishment Protocol
RNM	Root Nomination Message
RCM	Root Confirmation Message
MITM	Man in the middle attack
NRR	Node Replacement Request
LRR	Leader Replacement Reply
RTM	Network Leader Termination Message
MREQ	Communication Request
MREP	Communication Reply
KREQ	Key Request
KREP	Key Reply
AREQ	Authentication Request
AREP	Authentication Reply

ABSTRACT

A mobile ad-hoc network (MANET) is a kind of wireless ad-hoc networks, which is a self-configuring network of mobile nodes connected by wireless links the union of which forms an arbitrary topology. These nodes have limited power, computation, and communication capabilities; therefore the use of vastly resource consuming security mechanisms is not possible. Secure and efficient key management in MANETs has been a challenging task for the researchers due to the properties of MANETs like dynamic topologies, use of wireless media, no fixed infrastructure, low-energy constraint devices, limited storage and computation resources. In this thesis we propose a secure, efficient, and authenticated key management protocol for a group of communicating devices in MANETs.

Our proposed key management scheme is based on the concept that each group of nodes within the transmission range of each other can start a key establishment process. These groups can agree on a common key using a transitive authentication technique we developed. We also proposed an authentication protocol, Ad-hoc On Demand Authentication Chain Protocol (AOAC), which allow individual node to authenticate each other and to establish a shared key for peer-to-peer communication, the authentication does not rely on any centralize trusted authority or fixed server and is not based on public key cryptography. The proposed scheme supports dynamic membership operation and considers the dynamic behavior of the network topology. We also developed a key exchange algorithm which is used by our proposed key establishment protocol; it uses elliptic curve cryptography (ECC) and mixed radix conversion (MRC) to improve performance and save computation and communication cost. Our proposed key exchange algorithm is divided into two algorithms: a key agreement algorithm which is used by our proposed key establishment protocol during the setup phase, and a key transport algorithm which is used by our proposed protocol any time a re-keying is needed e.g. node leave or node join. The proposed scheme support dynamic network operations like join and leave operations.

Our key management scheme can be implemented in any network topology as long as the network is connected, only in the setup phase i.e. there is at least one communication link exists to all parties.

1. Introduction

Ad-hoc is adj. Latin shorthand meaning "for this purpose only" [1]. Thus, an ad hoc committee is formed for a specific purpose, usually appointed to solve a particular problem. A mobile ad-hoc network (MANETs) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links—the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad-hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations, etc.

The communication security in ad-hoc networks is commonly based on cryptographic techniques which are based on a shared secret key known by the group of nodes that forms the network. The procedure for creating such a common secret for a group of communicating entities is called group key management. For example, when a group of people are in a closed meeting, they may want to form a private wireless network with their laptops in an ad-hoc manner. There may be no secure channel to connect the computers, and the participants may not have any common means to identify and authenticate each other digitally. This means that they originally do not share any secret keys nor have mutually verifiable public key certificate chains or access to a trusted key distribution center. An eavesdropper might listen to and interfere with their communication, even masquerade as one of them. They would need a group key management protocol, but the nature of ad-hoc networks sets certain special requirements for such a protocol. Another example is a mobile military network, which is both security sensitive and easily exposed to security attacks. Not only the information passing in the network is confidential but the wireless traffic itself can reveal the location of a target to the enemy. The nodes, roaming in hostile environment with little physical protection, might be compromised, which increases the possibility of insider attacks.

From the above examples we can consider ad-hoc networks as dynamic, peer-to-peer networks that do not have a pre-existing infrastructure. They are constructed on the spot. The parties involved might not have a common history. They are often