Ain Shams University
Faculty of Engineering
Department of Electronics and Communication

Secure Communication in Mobile Ad hoc Networks

By

Khaled Mohamed Abd El Mohsen Soliman

Bachelor of Science in Electrical Engineering

(Electronics and Communication)

Faculty of Engineering, Arab Academy for Science,
Technology and Maritime Transport, 2010

A THESIS

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

DEPARTMENT OF ELECTRONICS & COMMUNICATION

Supervised By

Prof. Emad Hegazy
Prof. Ayman Mohammad Bahaa Eldeen Sadeq
Dr. Mohamed Ali Sobh

Cairo, Egypt
March, 2017

Ain Shams University
Faculty of Engineering
Department of Electronics
and Communication

Examiners Committee

Name : Khaled Mohamed Abd El Mohsen Soliman
Thesis : Secure Communication in Mobile Ad hoc Networks
Degree : Master of Science in Electrical Engineering

Name, Title, and Affiliate	Signature
Prof. Sherif El-Kassas Professor of Computer Engineering, The American University in Cairo	.....
Prof. Salwa El-Ramly Professor of Electronics and Communication Engineering, Ain Shams University	.....
Prof. Emad Hegazi (Supervisor) Professor of Electronics and Communication Engineering, Ain Shams University	.....
Prof. Ayman Bahaa-Eldin (Supervisor) Professor of Computer Engineering, Ain Shams University	.....

Date: / /

Abstract

Khaled Mohamed Abd El Mohsen Soliman

Secure Communication in Mobile Ad hoc Networks

Masters of Science dissertation

Ain Shams University, 2017

Mobile Ad hoc Network (MANET) is suffering from diverse security attacks and lack of privacy that affect its performance. In addition, the security measures applied in MANETs such as encryption and key authentication have a number of negative effects on the networks' performance. Cryptographic operations introduce a lot of both CPU and communication overhead. Therefore, routing protocols improvement is representing a great challenge for researchers to overcome the negative effects of security measures. Clustering MANETs is a known technique to lower the routing over-head. It can also be utilized to distribute encryption keys and the authentication process. In this thesis, a new protocol called Secure Clustering and Energy Saver Protocol (SCESP) is proposed to secure communication in MANETs and decrease the consumption of batteries in mobile nodes.

SCESP is aiming to secure the Mobile Ad hoc Networks from spoofing attacks via establishing an intelligent authentication mechanism in addition to decreasing the battery consumption rate to pave the way for applying more security mechanisms. This goal was achieved through developing a novel self-node clustering technique and cluster-based authentication to eliminate the key distribution overhead using smart cards which are consuming less energy than the preinstalled keys on the node itself. In addition, a priority is configured for each node to select the cluster head manually if needed. As proved, The SCESP system has succeeded to enhance the security level of MANETs and decrease the battery consumption resulted from broadcast messages in AODV.

Keywords:

MANETs, Authentication, Security Attacks, PKI, Cryptography, Smart Card, Digital Certificate, Clustering, AODV.

Publications

Khaled Soliman, Ayman M. Bahaa Eldin and Mohamed Sobh, “Energy Aware Secure Clustering in Mobile Ad hoc Networks”, ICCES 2015 10th International Conference on Computer Engineering & Systems, Cairo, Egypt, December 2015.

Acknowledgements

The main pillar of success goes to my supervisors for their efforts to assist me and continuous motivation during the whole period of working in this thesis. Adding to, the great support of my family and friends to pave the way towards achieving my goals and finalize my master's thesis.

In this sense, I would like to thank Prof. Ayman Mohamed Bahaa El-din, Dr. Mohamed Ali Sobh and Prof. Emad Hegazy for their great supervision and guidance to empower my skills and increase my knowledge to achieve the objectives of this thesis.

Statement

This dissertation is submitted to Ain Shams University for the degree of Masters of Science in Electrical Engineering - Electronics and Communication Engineering.

The work included in this thesis was out by the author at Electronics and Communication Department, Ain Shams University.

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

Date : / /2017

Signature :

Name : Khaled Mohamed Abd El Mohsen Soliman

Table of Contents

List of Figures and Illustrations

List of Tables

List of Abbreviations

ABR:	Associativity Based Routing
AODV:	Ad-hoc On-Demand Distance Vector
ATM:	Asynchronous Transfer Mode
CA:	Certification Authority
CAC:	Common Access Card
CCI:	Cluster Contention Interval
CGSR:	Cluster-Head Gateway Switch Routing
CIA:	Confidentiality, Integrity and Availability
DDoS:	Distributed Denial of Service
DestSeqNum:	Destination Sequence Number
DSDV:	Destination Sequenced Distance Vector
DSR:	Dynamic Source Routing
DT:	Distance Table
FWCA:	Flexible Weight Based Clustering Algorithm
IDS:	Intrusion Detection System
IETF:	Internet Engineering Task Force
IKE:	Internet key exchange
IP:	Internet Protocol
LAN:	Local Area Network
LAR:	Location-Aided Routing Protocol
LCA:	Linked Cluster Algorithm
LCT:	Link Cost Table
MAC:	Media Access Control
MANET:	Mobile Ad-hoc Network
MITM:	Man in the Middle attack
MOBIC:	Mobility Clustering Algorithm
MPGC:	Multicast Power Greedy Clustering
MRL:	Message Retransmission List
NS3:	Network Simulator version 3
PDA:	Personal Digital Assistant
PKI:	Public Key Infrastructure

PKIX:	Public Key Infrastructure X.509
RA:	Registration Authority
RERP:	Route reply
RERR:	Route Error
RREQ:	Route Request
RSA:	Rivest-Shamir-Adleman
RT:	Routing table
S/MIME:	Secure/Multipurpose Internet Mail Extensions
SCESP:	Secure Clustering and Energy Saver Protocol
SIM:	Subscriber Identification Module
SSA:	Signal Stability-Based Adaptive Routing
SSH:	Secure Shell
SSL:	Secure Sockets Layer
TCL:	Tool Command Language
TLS:	Transport Layer Security
TORA:	Temporally Ordered Routing Algorithm
WAN:	Wide Area Network
WPR:	Way Point Routing
WRP:	Wireless Routing Protocol
XML:	Extensible Markup Language
ZPR:	Zone Routing Protocol

Chapter One: Introduction

1.1 Motivation

The Mobile Ad hoc Network is facing diverse security vulnerabilities due to the lack of centralization and administration responsible for securing the network from any security threats such as spoofing and denial of service attacks. In addition, the energy factor is one of the major challenges facing the empowerment of MANETs due to battery consumption of mobile nodes. Therefore, there is a great desire to empower the capabilities of MANETs to cope with the modern revolution in information technology and telecommunication.

1.2 Contribution

The proposed system has succeeded to develop an enhanced security framework to decrease the challenging vulnerabilities in MANETs without affecting the communication performance. The security framework proposed is cluster-based authentication technique which is using smart cards to authenticate users to their cluster's heads. In the same time, a new self-node clustering energy aware has been developed to reduce the battery consumption and high utilization of bandwidth.

The new protocol results in comparison with the AODV protocol have shown a great improvement in battery consumption rate as a result of reducing the broadcast messages. This improvement has led to a significant drop of bandwidth utilization and paved the way for the proposed security framework to apply a new security measure to secure communication in MANETs.

1.3 Outline

This thesis is classified into four chapters to present the main pillars of the proposed protocol SCESP and the mechanisms applied for developing the performance and security of MANETs based on the previous endeavors to manage the challenges of MANETs.

Chapter 2 gives a comprehensive background which is addressing the following subjects: MANET's introduction, routing protocols, clustering techniques, security concepts and related work. Chapter 3 introduces the proposed solution SCESP which is divided into 3 parts: self-node clustering, cluster-based authentication and the protocol algorithm.

Afterwards, chapter 4 is showing the simulation results of the developed protocol compared to the default performance of AODV protocol according to the battery consumption of the mobile nodes. Finally, chapter 5 is concluding the thesis and presenting the suggested future work

Chapter Two: Background

2.1 Mobile Ad hoc Networks

2.1.1 Introduction

"Mobile Ad hoc network is a self-organizing wireless network designed for infrastructure-less applications" [1]. This edge is qualifying MANET to have a great role in struggling terrorism in remote areas which are lacking sufficient infrastructure for communication in addition to its uses in battlefields and disaster relief operations.

Securing MANETs is requiring an efficient authentication technique to ensure that only trusted nodes can join the network. As a result, the Public Key Infrastructure (PKI) is the best choice if the nodes can overcome its weaknesses such as routing overhead and battery consumption. These weaknesses have a lower impact when using smart cards as it stores the private key issued by the association who owns this network such as army or police.

This security measure has to be supported by a real improvement in MANETs routing protocols which could be developed by clustering algorithms which divide the network into groups of users to prevent the flood messages of unnecessary packets, avoid wasting network bandwidth and save the mobiles' batteries.

The developed technique is providing a great opportunity to boost the security level of MANETs through centralized administration which provides access to trusted nodes only in each cluster. The head selection could be selected statically as assigning priority for each node or dynamically by selecting the node with the highest number of neighbors.