**Mathematics Department**
**Faculty of Science**
**Computer Science Division**
**Ain Shams University**


# *New security techniques for wireless networks*

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE M.SC. DEGREE
(COMPUTER SCIENCE)
SUBMITTED TO
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
AIN SHAMS UNIVERSITY
CAIRO, EGYPT

**Presented By**

**WalaaAbd El Hakim Abd El Ghany Elsalhy**

**Supervised By**

**Prof. Emeritus. Fayed Fayek Mohamed Ghaleb**
Basic Professor Emeritus of mathematics,
Department of Mathematics,
Faculty of Science, Ain Shams University

**Prof. Ahmed Mohamed Khedr**
Professor of Computer Science,
Department of Mathematics,
Faculty of Science, Zagazig University

Cairo-2018

**Faculty of Science**

# APPROVAL SHEET

## New security techniques for wireless networks

M.Sc. *Thesis Submitted by*

**WalaaAbd El Hakim Abd El GhanyElsalhy**

***Thesis Supervisors***

**Prof. Emeritus. Fayed Fayek Mohamed Ghaleb**
Basic Professor Emeritus of mathematics,Department of Mathematics, Faculty of Science, Ain Shams University.

**Prof. Ahmed Mohamed Khedr**
Professor of Computer Science, Department of Mathematics, Faculty of Science, Zagazig University.

### Examination Committee

**Prof. AtefZakiGhalwash**
Professor of Faculty of Computer and Information Sciences, Helwan University.

**Prof. Aboul Ella Hassanien El -Etefy**
Professor of Faculty of Computer and Information Sciences Faculty , Cairo University.

**Date of Examination**

**Ain in Shams University**

Author: WalaaAbd El Hakim Abd El GhanyElsalhy

Title: New Security Techniques for Wireless Networks

Division: Computer Science

Department: Department of Mathematics

Faculty: Faculty of Science

Degree: M.Sc.

Year:201٨

# Table of Contents

# Publication

Walaa El-salhy, Fayed F M Ghaleb and Ahmed M Khedr. Article: Using a Random Perturbation-based Scheme for establishing Authentic Associations in Wireless Mesh Network. *International Journal of Computer Applications* 94(20):18-22, May 2014.

# List of Tables

# List of Figures

# Acknowledgements

*I acknowledge my deep gratitude to ALLAH the most beneficent and most merciful, who helped me complete this work on a level that I hope will please the reader.*

*First of all I would like to thank my dear family, Mother, Father ,my husband Dr. Mohamed El-Mahdi, brothers Omar &Mohamed, my uncle Abd El-Raoof and his wife whose kindness, care and never ending support and encouragement made me the person I am today.*

*Special thanks are due to my supervisors; Prof. Emeritus. Fayed Fayek Mohamed Ghaleb at the Faculty of Science, Ain Shams University and Dr. Ahmed Mohamed Khedrat the Faculty of Science,Zagazig university who constantly guided me in elaborating this thesis, assisted me in understanding and analyzing problems, and continuously provided support and valuable comments.*

*I would also like to thank Dr. HatemBaheg who learns me a lot.*

*Finally I would like also to thank all my friends specially Nermin El-Ansary ,Abd Allah Adel &Marwa Mohamed who pushed me either directly or indirectly to finish this work in the moments I thought it never will.*

## Keywords

Authentication, Pairwise, Key Establishment, Bi-variate Polynomial, Random Perturbation, Hash function, wireless Networks,Mesh Network, Mesh Routers,Mesh clients, Polynomial, Network Security, Mobile Clients, Scalability.

# ABSTRACT

Establishing an Authentic Association among entities in Wireless Mesh Networks WMN is a nontrivial problem and the architecture of WMN is relatively new and lacks a robust secure scheme .In this paper, we develop a Polynomial Based scheme which provides pair-wise connectivity, low communication, marginal storage overhead and high scalability while making on the fly Authentic Association feasible by using random perturbation based (RPB) scheme. New Proposed scheme is not only observed to be resilient against both traffic analysis and node capture attacks but also it is more secure , only requires a small storage space and has a little communication overhead.

# Summary

The actual different level of mobility associated with Mesh Clients offers much more flexibility within Wireless Mesh Networks (WMNs). The architecture of WMNs is comparatively new and lacks a robust secure scheme, so establishing an Authentic Association (AA) amongst entities in WMN is actually nontrivial problem. This thesis develops a Polynomial Based scheme (PBs)which provides pair-wise connectivity by using random perturbation based (RPB) scheme. New scheme (EARPB)is Proposed to combine the advantages of (PBs) and (RPB) schemes. These advantages are summarized inachieving pair-wise connectivity, low communication, marginal storage overhead and high scalability. It is not only performed to be resilient against both traffic analysis and node capture attacks but also it guarantees that any two nodes can directly establish a pairwise key without exposing any secret to other nodes . Even though many nodes have been actually compromised, the pairwise keys shared by non-compromised nodes remain highly secure. The proposed scheme incurs low computation and communicationoverhead.As shown in this thesis the EARPB scheme provides all these distinguished features without relying on public key cryptography.

The thesis is described as follows:

**Chapter one** gives a brief background about the security and wireless mesh networks concepts that will be used during the thesis.

**Chapter two** gives a survey on the terminologies that have been used in this thesis.

**Chapter three** gives a brief survey on w related works of our scheme.

**Chapter four** proposes five proposes (EARPB) Enhanced Approach with a Random Perturbation-Based Scheme.

**Chapter five** gives the conclusion and the future works.

## Notations

The following are some Acronyms with a short explanation used in this thesis.

| Acronym | Explanation |
|---|---|
| AA | authenticated association |
| AAA Server | authentication, authorization and accounting |
| AP | Access point |
| CIA | Colluding Injected Attack |
| DDoS | distributed denial of service |
| DoS | Denial of Service |
| DRAM | dynamic random access memory |
| EARPB | Enhanced Approach with a Random Perturbation-Based Scheme |
| EPKEM | efficient pairwise key establishment and management scheme |
| IGW | Internet Gateway |
| Id | identified |
| KDC | key distribution center |
| KGS | Key Generation Server |
| Mac | message authentication code |
| MANETs | Mobile ad hoc networks |
| MCs | Mesh Clients |
| MRs | Mesh Routers |

| | |
|---|---|
| NICs | network interface card |
| NP | nondeterministic polynomial time |
| PDA | personal digital assistant |
| PBS | Polynomial Based Scheme |
| RF | Radio frequency |
| ROM | Read-only memory |
| SRAM | static random access memory |
| STA | Station |
| VANET | vehicular ad hoc network |
| WAP | wireless access point |
| WHA | Wormholes Attacks |
| WiMax | Worldwide Interoperability for Microwave Access |