

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:201^

Table of Contents

Publication	i
List of Tables	ii
List of Figures	iii
Acknowledgements	iv
Keywords	v
ABSTRACT	vi
Summary	vii
Notations	ix
1 Chapter 1 Introduction	1
1.1 Wireless Network:	1
1.1.1 Why Wireless network?	2
1.1.2 Elements of a wireless network	3
1.1.3 Wireless Network Scenarios	5
1.1.4 Different Types of Wireless Networks	6
1.2 Wireless Mesh Networks (WMNs)	8
1.2.1 Architecture	10
1.2.2 The advantages of WMNs	12
1.2.3 Wireless Mesh Networks Architecture and design	13
1.2.4 Characteristics of WMNs	14
1.2.5 Applications of WMNs	16
1.3 Network Security	18
1.3.1 Security in Wireless Mesh Networks	18
1.3.2 Challenges	19
1.3.3 Basic Prevention	20
1.3.4 Security goals for WMNs networks	21
1.3.5 Vulnerabilities and Attacks in WMNs	26

1.4	Contributions:	32
2	Chapter 2 Basic concepts	34
2.1	Definitions and Notations	34
3	Chapter 3 Related works	43
3.1	Fundamentals:	43
3.1.1	The Master key approach:	46
3.1.2	The Pairwise key approach:	46
3.1.3	The remaining proposed schemes that our scheme "EARPB "based on:	47
3.1.4	Most closely related work	55
3.1.5	Closely related achievements	72
4	Chapter4 EARPB.....	75
4.1	The phases of our Enhanced Approach	77
4.1.1	Bivariate Polynomial specification and distribution phase	77
4.1.2	Generation and Pre-distribution of Perturbed Polynomials phase	80
4.1.3	Authenticated association (Keys Establishment) phase:	85
4.1.4	Secure path generation phase.....	94
4.2	Network Connectivity	97
4.3	Scalability of the Network.....	98
4.4	Resilience against Node Capture Attack and Traffic analysis attack	99
5	Chapter 5 Conclusion.....	100
6	Bibliography.....	102

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

Table 3.1: Keys in key chain.....	57
Table 4.1: Network Size vs. Number of functions stored on single node.....	99

List of Figures

Figure 1.1: :wireless Network.....	3
Figure 1.2 :Elements of a wireless network	4
Figure 1.3: Single hop & Multi hop fashion	8
Figure 1.4: Wireless Mesh Network	12
Figure 1.5 : Hybrid WMNs.....	16
Figure 2.1: Input, output and properties of hash functions.....	36
Figure 2.2: Symmetric-Key Encryption	40
Figure 2.3:Public-Key Encryption	40
Figure 2.4: A polynomial based scheme for generating pairwise keys.....	41
Figure 2.5: Generating the perturbed polynomial $gu(y)$	42
Figure 3.1: An example of constructed setup key matrix K	57
Figure 3.2 : Illustration of key pool and key matrix.....	61
Figure 3.3: Illustration of preloaded keys in sensors.....	64
Figure 3.4: One-way hash chain	66
Figure 3.5: Selection of Polynomials from a single matrix.....	68
Figure 3.6: Illustrating common functions for two entities.	69
Figure 4.1: Basic Wireless Mesh Network (WMN) Architecture.....	75
Figure 4.2: Showing Distribution of Bivariate Polynomial functions in 3 Dimensional Matrix	78
Figure 4.3: illustrate selection process of perturbed Polynomials from one matrix.....	82
Figure 4.4: Illustrating Common Functions for u & v	83
Figure 4.5: Examples of applying the RPB scheme on Polynomial functions	91
Figure 4.6 :Example of AAA in a WMN	95

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-Raouf 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 Fayed 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. Hatem Baheg 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 in achieving 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 communication overhead. As shown in this thesis the EARP 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