

# Contents

<b>Contents</b>	<b>vii</b>
<b>List of Figures</b>	<b>ix</b>
<b>List of Tables</b>	<b>x</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Overview and Problem Statement . . . . .	1
1.2 Motivation . . . . .	2
1.3 Problem Definition . . . . .	3
1.4 Contributions of this work . . . . .	3
1.5 Organization of the thesis . . . . .	4
<b>2 Background and Related Work</b>	<b>5</b>
2.1 Wireless Mesh Networks . . . . .	5
2.1.1 Introduction . . . . .	5
2.1.2 Security Challenges and Issues in WMNs . . . . .	6
2.1.2.1 Security Challenges and Constrains in WMNs . . . . .	6
2.1.2.2 Security Issues in WMNs . . . . .	7
2.2 Identity-Based Cryptography (IBC) . . . . .	8
2.3 Related Works . . . . .	8
<b>3 PAPAN: The protocol</b>	<b>10</b>
3.1 Network Model and Assumptions . . . . .	10
3.2 Security Requirements . . . . .	11
3.3 Preliminaries . . . . .	12

3.4	Proposed Protocol . . . . .	13
<b>4</b>	<b>Performance Study</b>	<b>20</b>
4.1	Simulation Environment . . . . .	20
4.2	Results and Analysis . . . . .	21
4.2.1	Results . . . . .	21
4.2.2	Security Analysis . . . . .	22
<b>5</b>	<b>Conclusion and Future Works</b>	<b>25</b>
5.1	Conclusion . . . . .	25
5.2	Future Works . . . . .	25
	<b>Bibliography</b>	<b>26</b>

# List of Figures

1.1	The three-party roaming authentication structure. . . . .	1
2.1	Architecture of WMNs. . . . .	6
3.1	Network topology of a typical WMN. . . . .	11
3.2	Pairing Based Authentication Protocol with Anonymous Roaming for WMNs . . . . .	14

# List of Tables

1.1	Functionality and Performance Comparison between our Protocol and Related Works . . . . .	3
3.1	Notations and Symbols . . . . .	13
4.1	Computation time of ECSM and Pairing Operations . . . . .	22
4.2	Comparasion of the Time Required for Authentication at the Foreign MG	22
4.3	Comparasion of Computation Time of Our Protocol and Rrelated Works at Roaming MN . . . . .	22
4.4	Computation Cost of Our Protocol at Home MG (HMG), Foreign MG (FMG), Visiting MR and Roaming MN (MN) . . . . .	22