Contents

Contents ix

List of Figures xi

List of Tables xii

1 Introduction 1

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 Dissertation Organization 3

2 Background and Related Works 4

2.1 Wireless Sensor Network 4

2.1.1 Introduction 4

2.1.2 Security Challenge and Requirements in WSN 5

2.2 Identity based cryptography 6

2.3 Strand Space Model 7

2.4 Related work 7

3 Proposed Work 10

3.1 Network Model and Assumptions 10

3.2 Preliminaries 11

3.3 Proposed Protocol 12

4 Security Proof using Strand Space Model 21

4.1 Introduction 21

4.1.1 Definitions and Theorems 21
4.1.2 Authentication tests 23
4.2 Description: 24
4.3 Formal Analysis of the proposed scheme 25

5 Performance Study **28**
5.1 Simulation Environment 28
5.2 Performance Evaluation 29
5.3 Result Analysis 30

6 Conclusion and Future Work **33**
6.1 Conclusion 33
6.2 Future Work 33

Bibliography **34**

List of Figures

2.1 Wireless sensor network 4

3.1 A Heterogeneous Wireless Sensor Network 11
3.2 Message Exchange during Cluster formation 14
3.3 Cluster Heads send messages to BS which are forwarded by L-sensors 17

4.1 Bundle1 24
4.2 Strand Space format for Bundle 1 25
4.3 Bundle 2 25
4.4 Strand Space format for Bundle 2 25

5.1 Comparison of computation Time between proposed protocol and Yang et al. protocol [21] 30

List of Tables

2.1 Security requirements of wireless sensor networks 5

2.2 Drawbacks of Various Key management Schemes 8

5.1 Simulation Parameters 29

5.2 Computation time for different parameters in Simulation 29

5.3 Comparison between proposed protocol and Yang et al. protocol [21] (Formation of one cluster) 29

5.4 Comparison between proposed protocol and Yang et al. protocol [21] (n=number of L-sensor nodes in one cluster, d=connection degree of each node) 31