# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER NO.</th>
<th>TITLE</th>
<th>PAGE NO.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td></td>
<td>xv</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td></td>
<td>xvi</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td></td>
<td>xix</td>
</tr>
</tbody>
</table>

## 1 INTRODUCTION

1.1 WIRELESS SENSOR NETWORKS 1
   1.1.1 Characteristics 1
   1.1.2 Applications 3
   1.1.3 Security 5
   1.1.4 Lifetime 6

1.2 TOPOLOGY MAINTENANCE PROTOCOLS 7
   1.2.1 Attacks on TMPs 9

1.3 NEED FOR SECURE TMP ALGORITHMS IN WSN 10

1.4 RESEARCH MOTIVATION 12

1.5 RESEARCH OBJECTIVES 14

1.6 CONTRIBUTIONS 15

1.7 ORGANIZATION OF THE THESIS 16

1.8 SUMMARY 17

## 2 LITERATURE REVIEW 18

2.1 INTRODUCTION 18

2.2 TOPOLOGY MAINTENANCE PROTOCOLS 18
2.2.1 Centralized Approach 19
2.2.2 Distributed Approach 22
2.2.3 Hybrid Approach 32
2.3 AUTHENTICATION IN WSN 33
2.4 VARIOUS AUTHENTICATION PROTOCOLS IN WSN 34
2.5 CHALLENGES IN SECURE TOPOLOGY MAINTENANCE ALGORITHMS 53
2.6 SUMMARY 53

3 SECURE ENERGY CONSERVING SLOT-BASED TOPOLOGY MAINTENANCE PROTOCOL 55
3.1 INTRODUCTION 55
3.2 NETWORK ASSUMPTION 56
3.3 NETWORK INITIALIZATION 58
3.4 SECS-TMP STATES 58
  3.4.1 Sleeping State 59
  3.4.1.1 Significance of $\alpha$ 61
  3.4.2 Electing State 61
  3.4.3 Operating State 64
3.5 TIME SLOT AND TIME FRAMES 64
3.6 BS FUNCTIONALITIES IN SECS-TMP 68
3.7 SECURITY ANALYSIS OF SECS-TMP 71
  3.7.1 Resilience to Clone Attack 71
  3.7.2 Resilience to Sybil Attack 74
  3.7.3 Resilience to Replay Attack 74
  3.7.4 Resilience to Sleep Deprivation Attack and Network Substitution Attack 75
CHAPTER NO. | TITLE | PAGE NO.
---|---|---
3.8 | SIMULATION RESULTS OF SECS-TMP | 75
  3.8.1 Lifetime Analysis with respect to the BS Arrival | 76
  3.8.2 Network Lifetime Analysis with respect to Operating Nodes | 80
  3.8.3 Network Lifetime Analysis with respect to Configuration Parameter $\alpha$ | 81
  3.8.4 Attack Detection Analysis | 83
  3.8.5 Memory Consumption | 85
  3.8.6 Energy Consumption | 86
3.9 | SUMMARY | 88

4 | LIGHT WEIGHT SECURE SLOT-BASED TOPOLOGY MAINTENANCE PROTOCOL (LWSS-TMP) | 89
  4.1 INTRODUCTION | 89
  4.2 NETWORK DEPLOYMENT AND INITIALIZATION | 91
    4.2.1 Authentication Request / Response | 93
  4.3 LWSS-TMP STATES | 95
    4.3.1 Sleeping State | 96
    4.3.2 Node-to-Node (N2N) Electing State | 96
    4.3.3 Operating State | 100
      4.3.3.1 Pairwise Key Generation and MAC Calculation | 100
      4.3.3.2 Ranking Algorithm | 101
  4.4 SECURITY ANALYSIS OF LWSS-TMP | 105
    4.4.1 Resilience to Clone Attack | 105
5 SECURE HYBRID SLOT-BASED TOPOLOGY MAINTENANCE PROTOCOL (SHS-TMP) 118

5.1 INTRODUCTION 118
5.2 NETWORK INITIALIZATION 120
5.3 SHS-TMP OVERVIEW 120
  5.3.1 Sleeping State 122
  5.3.2 BS-Sensing State 122
  5.3.3 BS-Electing State 123
  5.3.4 Node-to-Node (N2N) Electing State 123
  5.3.5 Operating State 124
5.4 SECURITY ANALYSIS OF SHS-TMP 124
  5.4.1 Resilience to Clone Attack 125
  5.4.2 Resilience to Sybil Attack 125
  5.4.3 Resilience to Replay Attack 126
  5.4.4 Resilience to Sleep Deprivation and
       Network Substitution Attacks 126
5.5 SIMULATION RESULTS OF SHS-TMP 127
<table>
<thead>
<tr>
<th>CHAPTER NO.</th>
<th>TITLE</th>
<th>PAGE NO.</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.1</td>
<td>Network Lifetime Analysis</td>
<td>127</td>
</tr>
<tr>
<td>5.5.2</td>
<td>Comparison of Energy Consumption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
<td>132</td>
</tr>
<tr>
<td>5.5.3</td>
<td>Memory Consumption Analysis</td>
<td>134</td>
</tr>
<tr>
<td>5.6</td>
<td>SUMMARY</td>
<td>136</td>
</tr>
<tr>
<td>6</td>
<td>CONCLUSION AND FUTURE WORK</td>
<td>137</td>
</tr>
<tr>
<td>6.1</td>
<td>CONCLUSION</td>
<td>127</td>
</tr>
<tr>
<td>6.2</td>
<td>FUTURE WORK</td>
<td>139</td>
</tr>
</tbody>
</table>

REFERENCES 140

LIST OF PUBLICATIONS 147