# 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>xii</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td></td>
<td>xiii</td>
</tr>
<tr>
<td>LIST OF SYMBOLS AND ABBREVIATIONS</td>
<td></td>
<td>xvi</td>
</tr>
</tbody>
</table>

## 1 INTRODUCTION

1.1 OUTLINE OF WIRELESS SENSOR NETWORK 1
1.2 SECURITY OF WSN 5
   1.2.1 Obstacles for WSN 5
   1.2.2 Security Requirements of WSN 6
   1.2.3 Attacks in WSN 8
   1.2.4 Counter Measures 10
1.3 NEED FOR KEY MANAGEMENT 11
1.4 KEY ESTABLISHMENT 13
1.5 NEED FOR POWER EFFICIENCY 15
1.6 TRUST MANAGEMENT 16
1.7 THESIS OBJECTIVE 18
1.8 PROBLEM FORMULATION 18
1.9 SOLUTION METHODOLOGY 19
   1.9.1 Overall System Architecture 19
1.10 ORGANIZATION OF THESIS 21

## 2 LITERATURE SURVEY

2.1 KEY PREDISTRIBUTION SCHEMES 22
2.2 ENERGY CONSERVATION SCHEMES 32
2.3 TRUST MANAGEMENT SCHEMES 37
2.4 ARCHITECTURES FOR APPLICATION ARENA OF WSN 53
2.5 SUMMARY OF LITERATURE REVIEW 55

3 DUAL KEY OPTIMIZATION 56
3.1 ENACTMENT OF EXISTING PAIRWISE KEY PREDISTRIBUTION 56
  3.1.1 Architecture of Existing Schemes 56
  3.1.2 Probabilistic Pairwise Key Predistribution 57
  3.1.3 Q-Composite Pairwise Key Predistribution 59
  3.1.4 Polynomial Pool based Pairwise Key Predistribution 61
  3.1.5 Security Analysis of Existing Schemes 62
3.2 PROBLEM FORMULATION FOR KEY PRESISTRIBUTION METHODOLOGY 63
3.3 ARCHITECTURE FOR DUAL KEY OPTIMIZATION 63
3.4 RANDOM KEY GENERATION 65
3.5 GROUP CONFIGURATION USING FACTORIAL FUNCTION 66
3.6 PAIRWISE KEY GENERATION AND ESTABLISHMENT 70
3.7 MATHEMATICAL PROOF FOR PAIRWISE KEY ESTABLISHMENT 72
3.8 SECURITY INVESTIGATION ON DKO 91
3.9 EXPERIMENT IMPLEMENTATION 93
3.10 RESULTS AND DISCUSSION 94
3.11 SUMMARY OF DKO 95
4 POWER EFFICIENCY ANALYSIS FOR KEY DISTRIBUTION

4.1 PROBLEM FORMULATION FOR POWER CONSUMPTION OF SENSOR NODES 96
4.2 INTEGRATION OF DKO AND STEM 96
4.3 STEM RUNNING ON TOP OF MAC 97
  4.3.1 State Transition of Stem During Key Predistribution 100
  4.3.2 Analysis of Stem 101
  4.3.3 Power Saving Through Dry Sun of Stem 102
4.4 DISCUSSION ON IMPLEMENTATION AND RESULTS 105
4.5 SUMMARY OF PEAK 108

5 PAIR KEY BASED AUTHENTICATION PROTOCOL FOR AUTHENTICATION IN WIRELESS SENSOR NETWORK 109

5.1 ENACTMENT OF EXISTING TRUST BASED PROTOCOLS 109
  5.1.1 Trust Aware Routing Framework 109
  5.1.2 Trust Based Routing Schemes 113
  5.1.3 Trust Guaranteed Routing 118
  5.1.4 Trust Aware Secure Routing Framework 122
5.2 SECURITY ANALYSIS OF EXISTING TRUST MANAGEMENT SCHEMES 127
5.3 PROBLEM FORMULATION FOR EXISTING TRUST AUTHENTICATION IN WSN 127
5.4 PAIR KEY BASED TRUST AUTHENTICATION PROTOCOL (PTAP) 128
5.4.1 Threshold based Identification of Legitimate Nodes 128
5.4.2 Secret Pairwise key Generation 132
5.4.3 Encryption and Decryption Model 134
5.4.4 Performance Evaluation 135
   5.4.4.1 Simulation model and parameters 135
   5.4.4.2 Performance metrics 136
5.5 RESULTS AND DISCUSSION 137
   5.5.1 Security Analysis of PTAP 141
5.6 SUMMARY OF PTAP 143

6 TRUST AMONG MILITANTS 144
6.1 PROTOTYPE DESIGNING 144
6.2 DKO AND PTAP IN TAM 144
6.3 TAM IN MILITARY SURVEILLANCE ENVIRONMENT 145
6.4 APPLICATION DEVELOPMENT USING TAM 146
   6.4.1 Test Bed Hardware Setup 147
      6.4.1.1 Arduino Microcontroller 147
      6.4.1.2 Zigbee Transmitter 148
   6.4.2 Specification for TAM 148
   6.4.3 Execution Environment of TAM 150
   6.4.4 Future Pinnacles of TAM 153
6.5 SUMMARY OF TAM 153

7 CONCLUSIONS 155
7.1 CONCLUSIONS 155
7.2 FUTURE WORKS 156

REFERENCES 157
LIST OF PUBLICATIONS 166