TABLE OF CONTENTS

CHAPTER NO. | TITLE | PAGE NO.
--- | --- | ---
ABSTRACT | v
LIST OF TABLES | xvi
LIST OF FIGURES | xvii
LIST OF SYMBOLS AND ABBREVIATIONS | xix

1 INTRODUCTION 1
1.1 THE SENSING PARADIGM 1
1.1.1 Difference between Wireless Adhoc Networks and Sensor Networks 3
1.1.2 Examples of Sensor Nodes 4
1.1.2.1 The “mica mote” family 4
1.1.2.2 Eyer-nodes 5
1.1.2.3 RTiodel 6
1.1.2.4 Scatterweb 7
1.2 TYPICAL SENSOR NETWORK SCENARIO 8
1.2.1 Components of a Sensor Node 9
1.2.2 Layered Architecture of WSN 10
1.2.3 Characteristics Features of WSN 12
1.2.4 Advantages of WSN 13
1.2.5 Limitations of WSN 13
1.2.6 Applications of WSN 14
1.3 WIRELESS SENSOR NETWORK SECURITY 18
1.3.1 Types of Attacks 18
1.4 TYPICAL SECURITY REQUIREMENTS 22

2 LITERATURE SURVEY OF RELATED WORK 39
2.1 BACKGROUND 39
2.2 STAGES OF REPLICAATION ATTACK 41
2.3 GOALS 44
2.4 SECURITY STRATEGIES 45
2.5 REPLICAATION ATTACK DETECTION MECHANISMS 48
2.5.1 Centralized Detection Approaches 49
2.5.1.1 Simple approach 49
2.5.1.2 Local detection (SET) 49
2.5.1.3 With the context of random key predistribution 50
2.5.2 Distributed Detection Approaches 51

3 SYSTEM MODEL AND ASSUMPTIONS 78
3.1 PREAMBLE 78
3.2 SYSTEM MODEL 78
3.2.1 Threat Model 81
3.2.2 Roles of a Node 82
3.2.2.1 Initiator 83
3.2.2.2 Claimer 83
3.2.2.3 Observer 84
3.2.2.4 Witness 84
3.2.3 Replication Attack Mitigation Model 84

4 NODE REPLICAATION ATTACK DETECTION 97
4.1 PREAMBLE 97
4.2 PRELIMINARIES 97
4.3 RANDOMIZED TRUST BASED REPLICAATION DETECTION PROTOCOL 99
4.3.1 Protocol Description 99
4.3.2 RTRADP Algorithm 102
4.3.3 Security Analysis 104
4.3.4 Performance Analysis of RTRADP 107
4.4 MODIFIED RTRADP 110
4.4.1 Simulation Setup and Assumptions 112
4.4.2 Performance Analysis of Modified RTRADP 112
4.5 SUMMARY 116

5 DESIGN CLONE NODE RECOVERY PROTOCOL 117
5.1 INTRODUCTION 117

CHAPTER NO. | TITLE | PAGE NO.
--- | --- | ---
2.5.2.1 Node-to- network broadcasting 51
2.5.2.2 Witness based strategy 51
2.5.2.3 With deployment knowledge 57
2.6 DISTRIBUTED DETECTION APPROACHES 59
2.7 LEGITIMATE CLONE DETECTION MECHANISMS 62
2.8 PREVENTION MECHANISMS 64
2.8.1 Identity-Based Cryptography (IBC) 64
2.8.2 Node Capture Detection 66
2.8.3 Node Addition Prevention 69
2.8.4 Block the Possible Re-Entry of Captured Nodes 70
2.8.5 Proactive Prevention 72
2.9 SELECTION OF TRUST MODEL BASED ON SURVEY 73
2.10 SUMMARY 77
3.1 PREAMBLE 78
3.2 SYSTEM MODEL 78
3.2.1 Threat Model 81
3.2.2 Roles of a Node 82
3.2.2.1 Initiator 83
3.2.2.2 Claimer 83
3.2.2.3 Observer 84
3.2.2.4 Witness 84
3.2.3 Replication Attack Mitigation Model 84

3.3 NETWORK AND ADVERSARY MODEL ASSUMPTIONS 86
3.3.1 Notations 87
3.3.2 Network Model 88
3.3.3 Adversary Model 90
3.3.4 Trust Model 91
3.3.4.1 Malicious behaviour 92
3.3.4.2 Trust quantification process 94
3.3.4.3 Trust computation 95
3.4 SUMMARY 96
4.1 PREAMBLE 97
4.2 PRELIMINARIES 97
4.3 RANDOMIZED TRUST BASED REPLICAATION DETECTION PROTOCOL 99
4.3.1 Protocol Description 99
4.3.2 RTRADP Algorithm 102
4.3.3 Security Analysis 104
4.3.4 Performance Analysis of RTRADP 107
4.4 MODIFIED RTRADP 110
4.4.1 Simulation Setup and Assumptions 112
4.4.2 Performance Analysis of Modified RTRADP 112
4.5 SUMMARY 116
5.1 INTRODUCTION 117

CHAPTER NO. | TITLE | PAGE NO.
--- | --- | ---
1.5 NODE REPLICAATION ATTACK AND ITS DISASTROUS IMPACTS ON WSNs 25
1.6 REPLICAATION ATTACK AND ITS IMPACTS ON SECURITY GOALS OF WSN 26
1.6.1 Security Breaches to Confidentiality 27
1.6.2 Security Breaches to Integrity 27
1.6.3 Security Breaches to Authenticity 28
1.6.4 Security Breaches to Availability 28
1.7 RESILIENT NETWORK 29
1.8 DESIGN CHALLENGES 32
1.9 RESEARCH OBJECTIVES 35
1.10 METHODOLOGY 35
1.11 CONTRIBUTION OF THE THESIS 36
1.12 OUTLINE OF THE THESIS 37

3.3 NETWORK AND ADVERSARY MODEL ASSUMPTIONS 86
3.3.1 Notations 87
3.3.2 Network Model 88
3.3.3 Adversary Model 90
3.3.4 Trust Model 91
3.3.4.1 Malicious behaviour 92
3.3.4.2 Trust quantification process 94
3.3.4.3 Trust computation 95
3.4 SUMMARY 96
4.1 PREAMBLE 97
4.2 PRELIMINARIES 97
4.3 RANDOMIZED TRUST BASED REPLICAATION DETECTION PROTOCOL 99
4.3.1 Protocol Description 99
4.3.2 RTRADP Algorithm 102
4.3.3 Security Analysis 104
4.3.4 Performance Analysis of RTRADP 107
4.4 MODIFIED RTRADP 110
4.4.1 Simulation Setup and Assumptions 112
4.4.2 Performance Analysis of Modified RTRADP 112
4.5 SUMMARY 116
5.1 INTRODUCTION 117

3.3 NETWORK AND ADVERSARY MODEL ASSUMPTIONS 86
3.3.1 Notations 87
3.3.2 Network Model 88
3.3.3 Adversary Model 90
3.3.4 Trust Model 91
3.3.4.1 Malicious behaviour 92
3.3.4.2 Trust quantification process 94
3.3.4.3 Trust computation 95
3.4 SUMMARY 96
4.1 PREAMBLE 97
4.2 PRELIMINARIES 97
4.3 RANDOMIZED TRUST BASED REPLICAATION DETECTION PROTOCOL 99
4.3.1 Protocol Description 99
4.3.2 RTRADP Algorithm 102
4.3.3 Security Analysis 104
4.3.4 Performance Analysis of RTRADP 107
4.4 MODIFIED RTRADP 110
4.4.1 Simulation Setup and Assumptions 112
4.4.2 Performance Analysis of Modified RTRADP 112
4.5 SUMMARY 116
5.1 INTRODUCTION 117

3.3 NETWORK AND ADVERSARY MODEL ASSUMPTIONS 86
3.3.1 Notations 87
3.3.2 Network Model 88
3.3.3 Adversary Model 90
3.3.4 Trust Model 91
3.3.4.1 Malicious behaviour 92
3.3.4.2 Trust quantification process 94
3.3.4.3 Trust computation 95
3.4 SUMMARY 96
4.1 PREAMBLE 97
4.2 PRELIMINARIES 97
4.3 RANDOMIZED TRUST BASED REPLICAATION DETECTION PROTOCOL 99
4.3.1 Protocol Description 99
4.3.2 RTRADP Algorithm 102
4.3.3 Security Analysis 104
4.3.4 Performance Analysis of RTRADP 107
4.4 MODIFIED RTRADP 110
4.4.1 Simulation Setup and Assumptions 112
4.4.2 Performance Analysis of Modified RTRADP 112
4.5 SUMMARY 116
5.1 INTRODUCTION 117

3.3 NETWORK AND ADVERSARY MODEL ASSUMPTIONS 86
3.3.1 Notations 87
3.3.2 Network Model 88
3.3.3 Adversary Model 90
3.3.4 Trust Model 91
3.3.4.1 Malicious behaviour 92
3.3.4.2 Trust quantification process 94
3.3.4.3 Trust computation 95
3.4 SUMMARY 96
4.1 PREAMBLE 97
4.2 PRELIMINARIES 97
4.3 RANDOMIZED TRUST BASED REPLICAATION DETECTION PROTOCOL 99
4.3.1 Protocol Description 99
4.3.2 RTRADP Algorithm 102
4.3.3 Security Analysis 104
4.3.4 Performance Analysis of RTRADP 107
4.4 MODIFIED RTRADP 110
4.4.1 Simulation Setup and Assumptions 112
4.4.2 Performance Analysis of Modified RTRADP 112
4.5 SUMMARY 116
5.1 INTRODUCTION 117
<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE NO.</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>Venn diagram to illustrate the witness characteristics</td>
<td>104</td>
</tr>
<tr>
<td>4.4</td>
<td>Detection rate</td>
<td>108</td>
</tr>
<tr>
<td>4.5</td>
<td>Impact of malicious and trusted witness in detection process</td>
<td>110</td>
</tr>
<tr>
<td>4.6</td>
<td>Modified RTRADP with trusted neighbour</td>
<td>111</td>
</tr>
<tr>
<td>4.7</td>
<td>Detection rate comparison of RED, RTRADP and Modified RTRADP</td>
<td>114</td>
</tr>
<tr>
<td>4.8</td>
<td>Impact of malicious neighbour in the detection process</td>
<td>115</td>
</tr>
<tr>
<td>5.1</td>
<td>The rate of attack detection and legitimate clone detection</td>
<td>121</td>
</tr>
<tr>
<td>5.2</td>
<td>Average detection rates of attack and benign clone detections at initiator</td>
<td>124</td>
</tr>
<tr>
<td>5.3</td>
<td>Sensitivity comparison of BCDW with RTRADP and Modified RTRADP</td>
<td>126</td>
</tr>
<tr>
<td>5.4</td>
<td>Performance comparison of BCDI and BCDW</td>
<td>127</td>
</tr>
<tr>
<td>6.1</td>
<td>Controlled link creation of a replica node with benign neighbours</td>
<td>129</td>
</tr>
<tr>
<td>6.2</td>
<td>Flowchart for prevention protocol</td>
<td>131</td>
</tr>
<tr>
<td>6.3</td>
<td>Block diagram for cache verification and updating</td>
<td>133</td>
</tr>
<tr>
<td>6.4</td>
<td>No. of cloned Nodes Vs Precision and FDR</td>
<td>137</td>
</tr>
<tr>
<td>6.5</td>
<td>No. of cloned Nodes Vs Accuracy</td>
<td>138</td>
</tr>
<tr>
<td>6.6</td>
<td>No. of clonednodes Vs FPR &amp; FPR</td>
<td>139</td>
</tr>
<tr>
<td>6.7</td>
<td>No. of cloned and genuine nodes Vs Precision, Accuracy, FPR and FDR</td>
<td>141</td>
</tr>
<tr>
<td>6.8</td>
<td>Prevention rate with respect to number of cloned nodes</td>
<td>142</td>
</tr>
</tbody>
</table>

**LIST OF SYMBOLS AND ABBREVIATIONS**

**Abbreviations**

- **ATSN** - Agent based Trust model
- **ADC** - Analog to Digital Converter
- **BS** - Base Station
- **BCDI** - Benign Clone Detection at Initiator
- **BCDW** - Benign Clone Detection at Witness
- **B-MEM** - Bloom filter- Memory Efficient Multicast
- **BC-MEM** - Bloom filter and Cell forwarding Memory Efficient Multicast
- **BSN** - Body Sensor Network
- **CPU** - Central Processing Unit
- **C4ISR** - Command, Control, Communications, Computing, Intelligence, Surveillance, Reconnaissance and Targeting
- **CDD** - Cooperative Distributed Detection
- **C-MEM** - Cross Forwarding- memory efficient multicast
- **DAS** - Data Acquisition System
- **DoS** - Denial of Service
- **DFR** - Determining Faulty Readings
- **DM** - Deterministic Multicast
- **DFDi** - Distinguish Forged Data of Illegal
- **DDoS** - Distributed Denial of Service
- **EDD** - Efficient and Distributed Detection
- **EEPROM** - Electrically Erasable Programmable Read-Only Memory
- **ESMIS** - Exclusive Subset Maximal Independent Set
- **xED** - eXtremely Efficient Detection
- **FDR** - False Discovery Rate
- **FN** - False Negative
- **FP** - False Positive
- **FPR** - False Positive Rate
- **FSD** - First Stage Detection
- **GTMS** - Group-based Trust Management Scheme
- **HWSN** - Heterogeneous Wireless Sensor Networks
- **HTCW** - Hybrid Trust computation scheme for Cluster-based WSNs
- **ID** - Identity
- **IBC** - Identity-Based Cryptography
- **IUER** - Inevitability of faults, Understand normal operations, Expect adverse events, Respond to adverse events and conditions
- **JTAG** - Joint Test Action Group
- **LSM** - Line Selected Multicast
- **LKH** - Location-Based Keys
- **MDLC** - Mechanisms based on Data Life Cycle
- **MAC** - Medium Access Control
- **MEM** - Memory Efficient Multicast
- **MIS** - Message Information Table
- **MANET** - mobile ad-hoc networks
- **MTLSD** - Multi-Time-Locational Storage & Diffusion
- **NBBTE** - Node Behavioral strategies: Banding belief theory of the Trust Evaluation algorithm
- **NRA** - Node Replication Attack
- **N2NB** - Node-to-Network Broadcasting
- **NBC** - Nuclear, Biological and Chemical
- **P-MPC** - Parallel Multiple Probabilistic Cells
- **PLUS** - Parameterized and Localized trust management Scheme
- **PPV** - Positive Predictive Values
- **RAM** - Random Access Memory
- **RM** - Random Multicast
- **RAW** - R-Aware Walk
- **RED** - Randomized and Efficient and Distributed protocol
- **RTRADP** - Randomized Trust-based Replication Attack Detection Protocol
- **RDE** - Randomly Directed Exploration
- **RFSN** - Reputation-based Framework for Sensor Networks
- **SRED** - Secure, Randomized and Efficient and Distributed protocol
- **SCADD** - sensor node capture attack detection and defence
- **SPRT** - Sequential Probability Ratio Test
- **SET** - Set
- **SDD** - Simple Distributed Detection
- **SDC** - Single Deterministic Cells
- **SHD** - Single Hop Detection
- **SEPFD** - Sink Enhanced First Stage Detection
- **SEDD** - Storage-efficient EDD scheme proposed
- **TRAWL** - Table-assisted Random Walk
- **TTSN** - Task-based Trust framework for Sensor Networks
TN - True Negative
TP - True Positive
TMBBT - Trust Model based on Bayes Theorem
TMCD - Trust Model based on Communication trust, Data Trust
and Energy trust
UV - Ultra Violet light
UTILE - Unary-Time-Location Storage & Exchange
UAV - Unmanned Arial Vehicle
WAN - Wide Area Network
WSN - Wireless Sensor Network

Symbols

\( K^{-1}(a) \) - a’s private key
\( K(a) \) - a’s public key
\( \{M\} K^{-1}(a) \) - a’s signature on Message M
\( d \) - Average degree of each node
\( B_i \) - Battery life value \((1 - B_{i-1} + 1)\) - represents lifetime of sensor node \(i\)
\( C_i \) - Consistency value of node \(i\), where \(1 < i < k\)
\( CS_i \) - Consistent sensing count of node \(i\)
\( C_{A,g} \) - Cumulative trust of Node A from g witnesses
\( E \) - Edges set
\( \beta_i \) - Forwarding probability, Probability of a neighbour will forward location claim
\( GH_k \) - Global Hit \(k^{th}\) witness
\( G \) - Graph
\( H(M) \) - Hash of Message M
\( ID_a \) - Identity of node \(a\)

\( IS_i \) - Inconsistent sensing count of node \(i\)
\( seed \) - is a number (or vector) used to initialize a pseudorandom number function
\( LH_k \) - Local hit at \(k^{th}\) witness
\( l_a \) - Location of node \(a\)
\( MACK(M) \) - Message authentication code of M with key \(K\)
\( R \) - Number of Replicas
\( N \) - Number of nodes in the network
\( g \) - Number of witness nodes selected by each neighbour
\( \lambda \) - Percentage of malicious nodes (cloned nodes)
\( \Phi_i \) - Probability of compromising or creating a controlled link
\( G_{rand} \) - Pseudo random function
\( P_0 \) - Rate of node replication attack detection
\( clone(i) \) - Replica or clone of node \(i\)
\( S_i \) - Sensing communication value of node \(i\)
\( SF_i \) - Sensing failure count of node \(i\)
\( SS_i \) - Sensing success count of node \(i\)
\( P_s \) - Success rate legitimate clone detection
\( P_{false} \) - The probability of detection when none (or zero) (Honest) honest witness
\( P_{false} \) - The probability of not detecting the attack
\( trust_{thresh} \) - Threshold for Trust factor
\( T_i \) - Trust value for node \(i\)
\( V \) - Vertex set
\( W_i \) - Weight which represents the importance of \(i^{th}\) factor