

TABLE OF CONTENTS

Candidate's declaration.....	i
Acknowledgement	ii
Table of Contents	iii
List of Figures	vii
List of Tables	x
List of Algorithms.....	xi
List of Abbreviations	xii
List of Publications	xv
Abstract.....	xvi
1. INTRODUCTION.....	1-18
1.1. OVERVIEW TO WSNs.....	1
1.1.1. Characteristics of WSNs.....	3
1.1.2. Security Constrains in WSNs.....	4
1.1.3. Security Requirements in WSNs	6
1.1.4. Security Attacks in WSNs	11
1.2. RESEARCH OBJECTIVES	16
1.3. WORK CARRIED OUT	17
1.4. THESIS ORGANIZATION.....	17
1.5. SUMMARY	18
2. LITERATURE SURVEY	19-29
2.1. RELATED WORK ON SECURITY ISSUES AND REMEDIES	19
2.2. RELATED WORK ON DATA AGGREGATION	23
2.3. RELATED WORK ON KEY MANAGEMENT	24
2.4. RELATED WORK ON KEY UPDATION FOR REMOVAL & REPLACEMENT OF COMPROMISED SENSOR NODES.....	25
2.5. RELATED WORK ON FORWARD AND BACKWARD SECRECY	27
2.6. RELATED WORK ON CRYPTOGRAPHY	28

2.7. SUMMARY	29
3. ZSDA: ZONE BASED SECURE DATA AGGREGATION SCHEME FOR CLUSTERED WIRELESS SENSOR NETWORKS.....	30-46
3.1. SYSTEM MODEL.....	30
3.1.1. Cluster Head Selection.....	32
3.1.1.1. Random Cluster Head Selection From Entire Network	32
3.1.1.2. Random Cluster Head Selection From Every Cluster.....	33
3.1.1.3. Presented Random Cluster Head Selection From Every Zone.....	33
3.1.2. Presented Secure Data Aggregation Scheme.....	35
3.1.3. Established Security Capabilities.....	38
3.2. KEY ASSIGNMENT COMPUTATION.....	39
3.2.1. Cluster Key Computation	39
3.2.2. Zone Key Computation.....	40
3.2.3. Sensor Key Computation	42
3.3. ENCRYPTION SCHEME	43
3.4. SIMULATION RESULTS.....	44
3.4.1. Sensor Coverage	44
3.4.2. Energy Consumption	45
3.5. SUMMARY	46
4. VLKM: VIRTUAL LOCATION-BASED KEY MANAGEMENT SCHEME FOR WSNs	47-73
4.1. ISSUES IN KEY MANAGEMENT	47
4.2. KEY MANAGEMENT REQUIREMENTS.....	48
4.3. TYPES OF KEY MANAGEMENT SCHEMES.....	48
4.4. PRESENTED MODEL FOR KEY MANAGEMENT	49
4.4.1. Network Clustering.....	49
4.4.2. Random Locations	51
4.4.3. Virtual Origins	51
4.4.4. Cluster Key	52
4.4.5. Sensor Key.....	54

4.4.6.	Virtual Movements	55
4.4.7.	Key Generation	59
4.4.7.1.	Cluster Key Generation	59
4.4.7.2.	Sensor Key Generation.....	60
4.4.8.	Virtual Location Based Keying Module	62
4.5.	RESULTS	67
4.5.1.	Key Duplication	67
4.5.2.	Key Chain Duplication	69
4.5.3.	Key Uniqueness	70
4.6.	DISCUSSIONS	72
4.7.	SUMMARY	73
5.	KURCS: KEY UPDATION FOR REMOVAL & REPLACEMENT OF COMPROMISED SENSOR NODES.....	74-95
5.1.	KEY REVOCATION SCHEME	74
5.1.1.	Types of Compromised Node Detection and Key Revocation Schemes.....	75
5.1.1.1.	Base Station Initiated Scheme	75
5.1.1.2.	Group Based Scheme	77
5.1.2.	Requirements of Key Revocation Scheme	79
5.2.	CLUSTERING SCHEME.....	79
5.3.	KEY SHARING SCHEMES	82
5.4.	SYSTEM MODEL FOR KEY UPDATION	84
5.4.1.	Types of Keys Used in the Presented Model	86
5.4.2.	Key Generation	87
5.4.3.	Key Updation.....	88
5.5.	PERFORMANCE ANALYSIS	90
5.5.1.	Key Updation Cost.....	90
5.5.2.	Communication Overheads.....	93
5.6.	SUMMARY	95
6.	DESFb:DYNAMIC ENCRYPTION SCHEME TO ACHIEVE FORWARD AND BACKWARD SECRECY IN WIRELESS SENSOR NETWORK.....	96-126

6.1. KEY ISSUE IN SECRECY	96
6.2. KEY GENERATION v/s KEY DISTRIBUTION	97
6.2.1. Issues in key generation	98
6.2.1.1. Forward Secrecy	98
6.2.1.2. Backward Secrecy	99
6.2.1.3. Forward and Backward Secrecy	99
6.3. EXISTING FORWARD & BACKWARD SECRECY SCHEMES	99
6.4. SYSTEM MODEL	102
6.4.1. The Architecture	103
6.4.1.1. Sequence Generator (SG)	104
6.4.1.2. Function Builder (FB)	105
6.4.1.3. Dynamic Encryption Function (DEF)	107
6.5. SIMULATION RESULTS	111
6.6. ANALYTICAL RESULTS AND PERFORMANCE	123
6.7. SUMMARY	126
7. PAIRING BASED ENCODING SCHEMES (PBES) FOR SECURE WSNs	127-162
7.1. PAIRING SCHEME	127
7.1.1. Continuous Pairing Scheme (CPS)	127
7.1.2. Skip Pairing Scheme (SPS)	128
7.2. ENCODING SCHEME	128
7.2.1. Relationship Between Encoding Schemes	131
7.3. RESULTS AND DISCUSSIONS	158
7.4. SUMMARY	162
8. CONCLUSION AND FUTURE DIRECTIONS	163-165
8.1. CONTRIBUTIONS	163
8.2. FUTURE DIRECTIONS	164
REFERENCES	166-173

LIST OF FIGURES

Figure 1.1: Randomly Deployed WSNs	2
Figure 1.2: Characteristics of WSNs	3
Figure 1.3: Security Constrains in WSNs.....	5
Figure 1.4: Security Requirements in WSNs.....	7
Figure 1.5: Normal Communication.....	7
Figure 1.6: Loss of Confidentiality.....	8
Figure 1.7: Loss of Availability	8
Figure 1.8: Loss of Integrity	8
Figure 1.9: Loss of Authenticity	9
Figure 1.10: Non-Repudiation Attack.....	9
Figure 1.11: Replay Attack.....	9
Figure 1.12: Forward and Backward Secrecy	10
Figure 1.13: Attacks on WSNs	11
Figure 1.14: Black Hole Attack	12
Figure 1.15: Selective Forwarding Attack	13
Figure 1.16: Sink Hole Attack	14
Figure 1.17: Sybil Attack	14
Figure 1.18: Worm Hole Attacks.....	15
Figure 3.1: System Model.....	31
Figure 3.2: Selection of Random Cluster Head from Entire Network.....	32
Figure 3.3: Selection of Random Cluster Head from Each Cluster	33
Figure 3.4: Selection of Cluster Head from Each Cluster Area.....	34
Figure 3.5: Random Cluster Head Selection from Same Zone Within Each Cluster	35
Figure 3.6: Data Transfer Scheme without Data Aggregation	35
Figure 3.7: Data Transfer Scheme through Selector.....	37
Figure 3.8: Virtual Cluster Location Updation to Generate a Cluster Key	40
Figure 3.9: Virtual Zone Location Updation to Generate a Zone Key	41

Figure 3.10: Virtual Sensor Location Updation to Generate a Sensor Key.....	42
Figure 3.11: Sensor Coverage With Different Cluster Head Range.....	44
Figure 3.12: Energy Comparison in Direct v/s Presented Data Aggregation Scheme	45
Figure 4.1: Static Cluster Formation.....	50
Figure 4.2: Clustering	50
Figure 4.3: Link Showing Actual and Virtual Locations.....	51
Figure 4.4: Virtual Origin of Network and Cluster.....	52
Figure 4.5: Cluster Virtual Location Mapping	53
Figure 4.6: Sensor Virtual Location Mapping	54
Figure 4.7: Sensor Movement Within Virtual Boundary.....	56
Figure 4.8: Sensor Movement Within Cluster Virtual Boundary	60
Figure 4.9: Two Different Sensors Moving in Same Clusters.....	61
Figure 4.10: Virtual Movement After Origin Mapping	66
Figure 4.11: Key Duplication	68
Figure 4.12: Key Duplication for Different Key Parameters.....	68
Figure 4.13: Number of Two or More Key Match in Series Between Any Two Consecutive Rounds	69
Figure 4.14: Key Chain Duplication for Different Key Parameters	70
Figure 4.15: Keys Uniqueness	71
Figure 4.16: Key Uniqueness for Different Key Parameters	72
Figure 5.1: Key Updation by Base Station in Dynamic Clustering.....	80
Figure 5.2: Key Updation by Base Station in Static Clustering	82
Figure 5.3: Static Clustering With Guard Nodes	84
Figure 5.4: Sensor to Cluster Head to Base Station Communications	85
Figure 5.5: Key Updation by Guard Node in Static Clustering.....	86
Figure 5.6: Energy Consumption in Static Clustering with Compromised Node From Area Wise Spreading in The Entire Network	91
Figure 5.7: Energy Consumption in Static Clustering with Random Compromised Node From Entire Network	92
Figure 5.8: Communication Overheads in Static Clustering With Compromised Node From Area Wise Spreading in The Entire Network	93

Figure 5.9: Communication Overheads With Random Compromised Node From Entire Network	94
Figure 6.1: Key Generation.....	98
Figure 6.2: Affect of Secrete Compromising in Key Generation	98
Figure 6.3: Forward Secrecy.....	98
Figure 6.4: Backward Secrecy	99
Figure 6.5: Forward and Backward Secrecy.....	99
Figure 6.6: Transfer of Key Generation Parameters From Sensor ‘A’ to Sensor ‘B’	100
Figure 6.7: Transfer of Key Generation Parameters From Sensor ‘B’ to Sensor ‘A’	101
Figure 6.8: One Way Hash Function	101
Figure 6.9: Communication Overheads For ‘n’ Sensors in Existing System	102
Figure 6.10: Instruction Sequence Generation For Each Round in WSNs.....	103
Figure 6.11: A System Overview of Dynamic Function Based Forward and Backward Secrecy Scheme	104
Figure 6.12: Static v/s Dynamic Function	108
Figure 6.13: Time complexity to Decode the System.....	124
Figure 6.14: Dynamic Encryption Function with 8 Bit Key v/s Static Encryption Function with 128 Bits Key	125
Figure 7.1: Packet Bits.....	128
Figure 7.2: Continuous Pairing Scheme	128
Figure 3.3: Skip Pairing Scheme	128
Figure 7.4: Relationship between Encoding Schemes.....	132
Figure 7.5: Decimal Number v/s Encoded Numbers in Continuous Pairing.....	147
Figure 7.6: Decimal Number v/s Encoded Numbers in Skip Pairing	158
Figure 7.7: Sensors Physical Connectivity	160
Figure 7.8: Sensors Physical Neighbors	160
Figure 7.9: Sensors Logical connectivity.....	161
Figure 7.10: Sensor Logical Neighbors	161

LIST OF TABLES

Table 3.1: Mapping Table.....	36
Table 4.1: Compute Virtual Location Notations.....	57
Table 4.2: Compute Dynamic Key Notations.....	61
Table 4.3: Key Table for Different Movements	66
Table 6.1: Simulation Results for Different Random Key and Same Packet Input in Each Round	112
Table 6.2: Simulation Results for Same Round Key and Same Packet Input in Each Round.....	118
Table 7.1: Output Produced by Different Encoding Schemes for Continuous Pairing	137
Table 7.2: Output Produced by Different Encoding Scheme for Skip Pairing.....	148
Table 7.3: Algorithms Setting.....	159

LIST OF ALGORITHMS

Algorithm 4.1: Computation of Current Virtual Location for Current Round	58
Algorithm 4.2: Folding Addition	63
Algorithm 4.3: Computation of Dynamic Key for Current Round with Initial Virtual Location and Current Virtual Movement.....	63
Algorithm 6.1: Sequence Generator	105
Algorithm 6.2: Function Builder.....	107
Algorithm 6.3: One stage of Dynamic Encryption Function.....	109
Algorithm 6.4: Same packet same key Algorithm.....	117