

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	v
	LIST OF TABLES	xvi
	LIST OF FIGURES	xviii
	LIST OF SYMBOLS AND ABBREVIATIONS	xxii
1.	INTRODUCTION	1
1.1	NEED FOR SECURITY IN SENSOR NETWORK	2
1.2	ARCHITECTURE OF WIRELESS SENSOR NETWORK	2
1.2.1	Characteristics of WSN	4
1.3	SECURITY CHALLENGES	5
1.3.1	Attacks in WSN	6
1.3.1.1	Common attack	6
1.3.1.2	Denial of Service (DoS) attack	8
1.3.1.3	Node compromise attack	8
1.3.1.4	Impersonation attack	8
1.3.1.5	Routing protocol attack	9
1.3.2	Data Aggregation	11
1.4	CRYPTOGRAPHY IN WSN	11
1.4.1	Symmetric Key Cryptography (SKC)	11
1.4.2	Asymmetric Key Cryptosystem (AKC)	12
1.4.2.1	Key management	14

CHAPTER NO.	TITLE	PAGE NO.
1.5	ELLIPTIC CURVE CRYPTOGRAPHY (ECC)	15
1.5.1	Characteristics of ECC	17
1.5.2	Operations on Elliptic Curves	18
	1.5.2.1 Point addition	18
	1.5.2.2 Point doubling	19
1.5.3	Montgomery Curves	20
	1.5.3.1 Disadvantages of Montgomery	20
	1.5.3.2 Advantages of Montgomery-Form Elliptic curve against timing attack	21
1.5.4	Twisted Edward Curves	23
	1.5.4.1 Twisted Edward addition	24
	1.5.4.2 Twisted Edward doubling	24
	1.5.4.3 Point multiplication	24
1.5.5	Existing Cryptographic Techniques in WSN	27
1.6	NEED FOR THE PROPOSED DYNAMIC SECURE AGGREGATION AND AUTHENTICATION FRAMEWORK	29
1.6.1	Objective of the Research Work	30
1.7	RESEARCH CONTRIBUTIONS	31
1.7.1	Dynamic sliding window Elliptic Curve Cryptography (DswECC)	32
1.7.2	Efficient Key Generation Algorithm - TinyECC-TE	32
1.7.3	Dynamic Secure Aggregation and Authentication (DSAA) Scheme	33
1.7.4	Cluster Based Clone Detection (CBCD)	33
1.8	THESIS OUTLINE	34

CHAPTER NO.	TITLE	PAGE NO.
2.	LITERATURE SURVEY	35
2.1	EXISTING SECURITY SCHEMES IN WSN	35
2.1.1	Hop-by-Hop (HbH) Scheme	35
2.1.2	Encrypted Data Aggregation (EDA) Scheme	36
2.2	EXISTING CRYPTOGRAPHY SOULTIONS FOR WSN	36
2.2.1	Symmetric Key Cryptosystems (SKC) for WSN	37
2.2.1.1	Security analysis of SKC	39
2.2.2	Asymmetric Key Cryptosystems (AKC) for WSN	39
2.2.2.1	Related works on ECC in WSN	41
2.2.2.2	Security analysis of AKC	46
2.2.3	Random Key Cryptosystem (RKC) for WSN	47
2.3	EXISTING KEY MANAGEMENT SCHEMES FOR WSN	48
2.3.1	Key Management Schemes	49
2.4	EXISTING DATA AGGREGATION PROTOCOLS FOR WSN	52
2.5	EXISTING CLONE DETECTION	61
2.6	SIMULATION TOOL	67
2.7	SUMMARY	67

CHAPTER NO.	TITLE	PAGE NO.
3.	LIGHTWEIGHT ELLIPTIC CURVE CRYPTOGRAPHY	68
3.1	PROPOSED DYNAMIC SLIDING WINDOW NON-ADJACENT FORM FOR POINT MULTIPLICATION (DswNAF)	68
3.1.1	Non-Adjacent Form (NAF) for Point Multiplication	69
3.1.2	Width Non-Adjacent Form (wNAF) for Point Multiplication	70
3.1.3	Rule Engine	72
3.2	IMPLEMENTATION IN MICAZ	76
3.2.1	Structure of TinyECC-Twisted Edward (TinyECC-TE)	77
3.2.2	Elliptic curve Integrated Encryption Scheme (ECIES) with Proposed DswNAF	80
3.2.3	Elliptic Curve Diffie Hellman (ECDH) in Micaz	81
3.2.4	Elliptic Curve Integrated Encryption Scheme (ECIES) in Micaz	82
3.3	RESULT AND DISCUSSION	83
3.3.1	Performance Analysis of DswNAF	85
3.3.2	Implementation of TinyECC and TinyECC-Twsited Edward	92
3.3.2.1	Performance analysis of ECDH using Koblitz and Twisted Edward curves	93

CHAPTER NO.	TITLE	PAGE NO.
	3.3.2.2 Performance analysis of ECIES using Koblitz and Twisted Edward curve	96
	3.3.2.3 Memory analysis	98
3.4	SECURITY ANALYSIS OF TINYECC-TE	98
	3.4.1 MITM Attack	101
	3.4.2 Simple Power Analysis (SPA) Attack	103
3.5	SUMMARY	105
4.	A FRAMEWORK FOR DYNAMIC SECURE AGGREGATION AND AUTHENTICATION (DSAA)	107
4.1	PROPOSED DYNAMIC SECURE AGGREGATION AND AUTHENTICATION (DSAA) FRAMEWORK	107
	4.1.1 Sensor Node Deployment and Cluster Formation	110
	4.1.1.1 Node deployment	110
	4.1.1.2 Cluster formation	110
	4.1.1.3 Route update and cost estimation	111
4.2	KEY GENERATION AND KEY EXCHANGE PROCESS IN INTER AND INTRA CLUSTER HEAD	115
4.3	ENCRYPTION / DECRYPTION	116
	4.3.1 Encryption of Sensed Data	117
	4.3.2 Authentication of Sensed Data	118

CHAPTER NO.	TITLE	PAGE NO.
	4.3.2.1 Proposed Scheduler based Combined Secured Hash Algorithm (SCSHA) for WSN authentication	119
	4.3.3 Data Aggregation	121
	4.3.3.1 Encryption	122
	4.3.3.2 Decryption	123
4.4	RESULT AND DISCUSSION	125
	4.4.1 Cluster Formation and Routing	125
	4.4.2 Shared Secret Key Generation using ECDH	128
	4.4.3 Encryption and Decryption of Data	129
	4.4.4 Security Analysis of the Proposed Work	130
	4.4.4.1 Storage requirement	131
	4.4.4.2 Execution timing analysis	131
	4.4.4.3 Energy consumption	132
4.5	ANALYSIS ON PROPOSED SCHEDULER BASED COMBINED SECURED HASH ALGORITHM (SCSHA) FOR WSN AUTHENTICATION	133
	4.5.1 Preimage Attacks	133
	4.5.2 Birthday Attack	133
4.6	SECURITY ANALYSIS ON DSAA	135
	4.6.1 MITM Attack	136
	4.6.2 Node Replication Attack	138
	4.6.3 Impersonation Attack	140
	4.6.4 Replay Attack	140
4.7	SUMMARY	140

CHAPTER NO.	TITLE	PAGE NO.
5.	PROPOSED CLUSTER BASED CLONE DETECTION ALGORITHM	141
5.1	CLONE ATTACK	141
5.2	PROPOSED CLUSTER BASED CLONE DETECTION (CBCD)	143
5.2.1	Clone Detection and Revocation Process	143
5.3	RESULT AND DISSCUSSION OF PROPOSED CBCD	147
5.4	SUMMARY	154
6.	CONCLUSION AND FUTURE WORK	155
6.1	CONCLUSION	155
6.2	SCOPE FOR FUTURE RESEARCH	158
	REFERENCES	159
	LIST OF PUBLICATIONS	177

LIST OF TABLES

TABLE NO.	TITLE	PAGE NO.
1.1	Specification of few currently available sensor boards	4
1.2	Classifications of security attacks that threatening security services in WSN	10
1.3	Level of security obtained between RSA and ECC for different key sizes	15
1.4	Window size vs. number of point additions, doublings, precomputations and memory	27
2.1	Comparison of existing security protocols in WSN	60
3.1	Computation time of various scalar value using wNAF algorithm	85
3.2	Computation time of various scalar value using the proposed DswNAF algorithm	88
3.3	Timing analysis of ECIES	91
3.4	Computational time of ECDH using TinyECC and proposed TinyECC-TE	94
3.5	Comparison of computation time of ECIES using TinyECC and proposed TinyECC-TE	96
3.6	Memory requirement for TinyECC and proposed TinyECC-TE	98
3.7	Notations used in HLPSL code	99
3.8	HLPSL code for communication between two nodes	100

TABLE NO.	TITLE	PAGE NO.
3.9	Computation time of ECDH using Koblitz curves and Twisted Edward curves	105
4.1	Parameters involved for constructing the environment	111
4.2	Control information format (routing table)	112
4.3	Data packet format	114
4.4	Comparison of key agreement scheme based on storage requirement	131
4.5	Execution time for various security algorithms used in proposed work	132
4.6	Energy consumption for various security algorithms in the proposed DSAA	132
4.7	Comparisons of SHA, existing Combined SHA and proposed SCSHA	134
4.8	Security Analysis under MITM attack	138
4.9	Security Analysis under node replication attack	139
5.1	Energy overhead	149

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE NO.
1.1	Node deployment in a hostile environment	3
1.2	Taxonomy of various attacks in WSN	7
1.3	Symmetric key cryptosystem	12
1.4	Asymmetric key cryptosystem	13
1.5	An example for elliptic curve	16
1.6	Geometric addition of elliptic curve points	18
1.7	Geometric doubling of elliptic curve points	19
1.8	Zigbee security suite	28
1.9	Proposed architecture diagram for WSN security	31
2.1	Existing cryptographic techniques	37
2.2	Taxonomy on Elliptic Curve Cryptography	42
2.3	Types of keys used in WSN	48
2.4	Classification of key management schemes for WSN	49
2.5	Taxonomy on data aggregation schemes	54
2.6	Taxonomy on clone detection schemes	62
3.1	Inherent location of the proposed work	69
3.2	wNAF output	71
3.3	Rule engine for selecting window size	73
3.4	Component diagram of TinyECC	77
3.5	Elliptic Curve Diffie Hellman (ECDH) key exchange	81
3.6	Functional diagram of ECIES	83

FIGURE NO.	TITLE	PAGE NO.
3.7	Performance of computation time analysis for wNAF algorithm using various window sizes	86
3.8	Animated output of window controller	87
3.9	Timing analysis of the proposed DswNAF	90
3.10	Execution time of proposed DswNAF in ECIES	91
3.11	Various steps involved in ECDH and its execution time compared with the existing Koblitz curves and Twisted Edward curves	95
3.12	Comparison of computation time of various steps involved in ECIES using Koblitz curves and Twisted Edward curves	97
3.13	Proposed TinyECC-TE Key exchange between two nodes	101
3.14	Proposed TinyECC-TE Key exchange between two nodes with MITM attack	102
3.15	Evaluation of proposed TinyECC-TE under MITM attack	103
3.16	Power trace of addition (S) and doubling (D) operation on ECC	104
4.1	Flow diagram of the proposed Dynamic Secure Aggregation and Authentication (DSAA) framework	108
4.2	Techniques and principles of proposed DSAA	109
4.3	Diagram representing link quality values	114
4.4	Block diagram of block cipher in CBC mode	118
4.5	Proposed design for Combined SHA	119

FIGURE NO.	TITLE	PAGE NO.
4.6	Message scheduler	120
4.7	Sequential diagram of proposed DSAA framework	124
4.8	Simulation of cluster formation in TinyViz	125
4.9	Listener port	126
4.10	Routing table of 38 th node	127
4.11	Packet transmission	128
4.12	ECDH shared secret key generation	128
4.13	Simulated trace file of the sensor data after encryption process	129
4.14	Encryption and decryption of data	130
4.15	Proposed DSAA key exchange mechanism using TinyECC-TE between node to CH and CH to BS	135
4.16	Simulation of proposed DSAA under MITM attack	136
4.17	Evaluation of the proposed DSAA under MITM attack	137
5.1	Cluster formation in WSN	142
5.2	The coherence identification process	144
5.3	Simulation environment with clone node	147
5.4	Entries in the routing table of node 15	148
5.5	Revocation process in clone node 5	149
5.6	Performance analysis of the proposed CBCD algorithm with existing RED algorithm for clone detection	150

FIGURE NO.	TITLE	PAGE NO.
5.7	Performance analysis of the proposed CBCD algorithm with existing RED algorithm for clone detection	151
5.8	Comparison of the energy consumption for the proposed CBCD algorithm and RED algorithm	152
5.9	Detection probability	153
5.10	Time taken for route update	153