

TABLE OF CONTENTS

Candidate Declaration	i
Abstract	ii
Declaration	v
Acknowledgement	vi
Table of Contents	vii
List of Figures	xi
List of Tables	xv
List of Abbreviations	xvi
List of Publications	xviii
Chapter 1: Introduction	1-18
1.1 Internet of Things (IoT)	1
1.2 Significance of IoT	2
1.3 IoT Security Challenges and Requirements	3
1.4 Security Threats against RPL in IoT	7
1.5 Scope of the Research	10
1.6 Problem Statement	11
1.7 Research Contributions	12
1.7.1 Contributions of TDD and SLTD	12
1.7.2 Contributions of TSF-RPL and MLT-IoT	13
1.7.3 Contribution of S-MODEST	15
1.8 Thesis Outline	16
Chapter 2: Background and Literature Survey	19-45
2.1 Fundamentals of IoT	19
2.1.1 IoT Architecture	20

2.1.2 IoT Technologies	21
2.1.3 IoT Applications	22
2.2 IoT Routing	26
2.2.1 Designing Challenges of RPL Routing in IoT	27
2.3 Security in IoT Routing	29
2.3.1 Security Requirements of IoT	30
2.3.2 Trust-based Secure IoT Routing	32
2.4 Literature Survey of Secure IoT Routing	34
2.4.1 Survey of RPL Routing Protocols in IoT	35
2.4.2 Survey Related to Secure IoT Routing Protocols	37
2.5 Survey of Trust-based Secure IoT Routing Protocols	41
SUMMARY	45
Chapter 3: Secure RPL Trust Mechanisms against DDoS Attack over IoT	46-70
3.1 Effect of DDoS Attack in the RPL network	46
3.1.1 Role of Trust in Attack Detection	47
3.2 Trust based DDOS Attack Detection (TDD)	47
3.2.1 TDD Protocol Overview	48
3.2.2 Trust Evaluation and Attack Detection	48
3.3 Performance Evaluation of TDD	50
3.3.1 Simulation Setup and Performance Metrics of TDD	50
3.3.2 Simulation Results of TDD	51
3.4 Subjective Logic-based Trust Mechanism against DDoS (SLTD)	59
3.4.1 SLTD protocol Overview	59
3.4.2 Subjective Logic based Trust Evaluation	60
3.4.3 DDOS Attack Detection	60
3.5 Performance Evaluation of SLTD	61
3.5.1 Simulation Setup and Performance Metrics of SLTD	62

3.5.2 Simulation Results of SLTD	63
SUMMARY	70
Chapter 4: Trust-based RPL Security Solutions against Selective Forwarding Attack over IoT	71-95
4.1 Selective Forwarding Attack and its Effects on RPL Routing	71
4.2 Trust Based Selective Forwarding Attack Detection in RPL (TSF-RPL)	72
4.2.1 System Model of TSF-RPL	73
4.2.2 Trust Evaluation of TSF-RPL	73
4.2.2.1 Neighbor List Maintenance Based on Trust	73
4.2.2.2 Observation of Dropping Packet	74
4.2.3 Current Trust-Based Secure Data Forwarding	75
4.3 Performance Evaluation of TSF-RPL	76
4.3.1 Simulation Setup and Performance Metrics of TSF-RPL	77
4.3.2 Simulation Results of TSF-RPL	78
4.4 Multi-Level Trust-Based Secure RPL over IoT (MLT-IoT)	84
4.4.1 Multi Level Trust Evaluation	85
4.4.2 Selective Forwarding Attack Detection	86
4.5 Performance Evaluation of MLT-IoT	86
4.5.1 Simulation Setup and Performance Metrics of MLT-IoT	87
4.5.2 Simulation Results of MLT-IoT	87
SUMMARY	95
Chapter 5: Game Theory and Dempster Shafer Theory-Based Secure RPL over IoT	96-122
5.1 Impact of Malicious dropping attacks in RPL	96
5.1.1 Role of Game theory Model in RPL Security	97
5.2 Game Model Formulation of S-MODEST	97
5.3 Overview of the S-MODEST	99

5.3.1 Building routing behavior trust on Non-Zero Sum Game Model	101
5.3.2 Utility for Different Strategies and Nash Equilibrium	105
5.4 Malicious Attack Detection by using RPL-Specific Contextual Trust	106
5.4.1 Trusted DODAG Formation using Evolutionary Game Model	108
5.5 Performance Evaluation of S-MODEST	110
5.5.1 Performance Metrics of S-MODEST	111
5.5.2 Simulation Results of S-MODEST	111
SUMMARY	121
Chapter 6: Conclusion and Future Work	123-144
6.1 Conclusions	123
6.2 Future Work	133
References	135-145