

## CANDIDATE'S DECLARATION

---

I hereby certify that the work which is being presented in the thesis, entitled "TRUST BASED SECURED ROUTING MECHANISMS IN INTERNET OF THINGS" in fulfillment of the requirements of the award of the degree of Doctor of Philosophy in Faculty of Computer Science & Engineering and submitted in Maharaja Ranjit Singh Punjab Technical University, Bathinda is an authentic record of my own work carried out during a period from August 2015 to February 2020 under the supervision of Dr. Shaveta Rani, Professor, Giani Zail Singh Campus, College of Engineering and Technology, MRSPTU, Bathinda.

The matter embodied in this thesis has not been submitted by me for the award of any other degree of this or any other University/Institute.

**(Vidhu Kiran)**

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

**(Dr. Shaveta Rani)**

(Supervisor)

Deptt. of Computer Sci. & Engineering

Giani Zail Singh Campus College of Engineering and Technology

Bathinda

The Ph.D. Viva-Voice examination of Vidhu Kiran, Research Scholar, has been held on\_\_\_\_\_

Sign. of Supervisor(s)

Sign.of External Examiner

# ACKNOWLEDGEMENT

---

This phase of life would have been impossible without expressing my gratitude to many people who helped and inspired me during this time. This section is a small effort to convey my gratitude to them. I would like to thank God the most who have made my life bountiful, full of blessings and graces.

First of all I would like to express my profound and heartfelt gratitude to my research supervisor, Prof. (Dr.) Shaveta Rani for her support, understanding and personal guidance. I thank Prof. (Dr.) Paramjeet Singh for his intense endurance and outstanding technical guidance in writing and presenting research.

I would like to give my special thanks to Computer Science and Engineering Department of our organization for their support and continuous guidance. Their inspiring words always motivate me to work on the right path and with positive attitude.

My thesis work would have been incomplete without thanking my sister Navita and my brother Piyush Sharma for always being there in the need of hour. Without them this thesis never came into existence.

My special thanks to my friend Simardeep for helping me in each phase of thesis formatting and for her constant support, love and encouragement.

Last, but not least, I would like to thank to my In-laws family, my husband Pushkar and daughter Mishthi for their love, care, and understanding.

**Vidhu Kiran**

## List of Figures

Figure No.	Name of Figure	Page No.
1.1	Security Challenges of IoT	4
1.2	Block Diagram of Trust-based detection Mechanisms against DDoS Attack	13
1.3	Block Diagram of Trust-based Detection Mechanism against Selective Forwarding Attack	14
1.4	Block Diagram of S-MODEST Model	16
2.1	Layered IoT Architecture	20
2.2	IoT Applications	23
3.1	Number of Attackers Vs. Detection Accuracy for 31 Nodes	52
3.2	Number of Attackers Vs. Detection Accuracy for 41 Nodes	53
3.3	Number of Attackers Vs. Detection Accuracy for 51 Nodes	53
3.4	Number of Attackers Vs. Throughput for 31 Nodes	54
3.5	Number of Attackers Vs. Throughput for 41 Nodes	55
3.6	Number of Attackers Vs. Throughput for 51 Nodes	55
3.7	Number of Attackers Vs. Overhead for 31 Nodes	56
3.8	Number of Attackers Vs. Overhead for 41 Nodes	56
3.9	Number of Attackers Vs. Overhead for 51 Nodes	57
3.10	Number of Attackers Vs. Power Consumption for 31 Nodes	57
3.11	Number of Attackers Vs. Power Consumption for 41 Nodes	58
3.12	Number of Attackers Vs. Power Consumption for 51 Nodes	58
3.13	Number of Attackers Vs. Detection Accuracy for 31 Nodes	63
3.14	Number of Attackers Vs. Detection Accuracy for 41Nodes	64
3.15	Number of Attackers Vs. Detection Accuracy for 51 Nodes	64
3.16	Number of Attackers Vs. Throughput for 31 Nodes	65
3.17	Number of Attackers Vs. Throughput for 41 Nodes	66

3.18	Number of Attackers Vs. Throughput for 51 Nodes	66
3.19	Number of Attackers Vs. Overhead for 31 Nodes	67
3.20	Number of Attackers Vs. Overhead for 41 Nodes	68
3.21	Number of Attackers Vs. Overhead for 51 Nodes	68
3.22	Number of Attackers Vs. Power Consumption for 31 Nodes	69
3.23	Number of Attackers Vs. Power Consumption for 41 Nodes	69
3.24	Number of Attackers Vs. Power Consumption for 51 Nodes	70
4.1	Number of Attackers Vs. Detection Accuracy for 31 Nodes	79
4.2	Number of Attackers Vs. Detection Accuracy for 41 Nodes	79
4.3	Number of Attackers Vs. Detection Accuracy for 51 Nodes	79
4.4	Number of Attackers Vs. Throughput for 31 Nodes	80
4.5	Number of Attackers Vs. Throughput for 41 Nodes	80
4.6	Number of Attackers Vs. Throughput for 51 Nodes	81
4.7	Number of Attackers Vs. Overhead for 31 Nodes	81
4.8	Number of Attackers Vs. Overhead for 41 Nodes	82
4.9	Number of Attackers Vs. Overhead for 51 Nodes	82
4.10	Number of Attackers Vs. Power Consumption for 31 Nodes	83
4.11	Number of Attackers Vs. Power Consumption for 41 Nodes	83
4.12	Number of Attackers Vs. Power Consumption for 51 Nodes	84
4.13	Number of Attackers Vs. Detection Accuracy for 31 Nodes	88
4.14	Number of Attackers Vs. Detection Accuracy for 41 Nodes	88
4.15	Number of Attackers Vs. Detection Accuracy for 51 Nodes	89
4.16	Number of Attackers Vs. Overhead for 31 Nodes	89
4.17	Number of Attackers Vs. Overhead for 41 Nodes	90
4.18	Number of Attackers Vs. Overhead for 51 Nodes	90
4.19	Number of Attackers Vs. Power Consumption for 31 Nodes	91
4.20	Number of Attackers Vs. Power Consumption for 41 Nodes	91
4.21	Number of Attackers Vs. Power Consumption for 51 Nodes	92
4.22	Number of Attackers Vs. Energy Consumption for 31 Nodes	92

4.23	Number of Attackers Vs. Energy Consumption for 41 Nodes	93
4.24	Number of Attackers Vs. Energy Consumption for 51 Nodes	93
4.25	Number of Attackers Vs. Throughput for 31 Nodes	94
4.26	Number of Attackers Vs. Throughput for 41 Nodes	94
4.27	Number of Attackers Vs. Throughput for 51 Nodes	95
5.1	Performance Evaluation of S-MODEST by Varying the Network Area in terms of Detection Accuracy	112
5.2	Performance Evaluation of S-MODEST by Varying the Network Area in terms of Throughput	113
5.3	Performance Evaluation of S-MODEST by Varying the Network Area in terms of Normalized Overhead	114
5.4	Performance Evaluation of S-MODEST by Varying the Network Area in terms of energy consumption	114
5.5	Performance Evaluation of S-MODEST by Varying the Number of Attackers in terms of Detection Accuracy	115
5.6	Performance Evaluation of S-MODEST by Varying the Number of Attackers in terms of Throughput	116
5.7	Performance Evaluation of S-MODEST by Varying the Number of Attackers in terms of Normalized Overhead	117
5.8	Performance Evaluation of S-MODEST by Varying the Number of Attackers in terms of Energy Consumption	117
5.9	Performance Evaluation of S-MODEST by Varying the Number of Attackers in terms of Routing Enforcement	118
5.10	Performance Evaluation of S-MODEST by Varying the Data Interval in terms of Detection Accuracy	119
5.11	Performance Evaluation of S-MODEST by Varying the Data Interval in terms of Throughput	120
5.12	Performance Evaluation of S-MODEST by Varying the Data Interval in terms of Normalized Overhead	120

5.13	Performance Evaluation of S-MODEST by Varying the Data Interval in terms of Energy Consumption	121
------	--	-----

## List of Tables

<b>Table No.</b>	<b>Name of Figure</b>	<b>Page No.</b>
2.1	Comparison of Various Types of RPL attacks over IoT	30
2.2	Comparison of Various Types of RPL Routing protocols for IoT	35
2.3	Comparison of Various types of Secure IoT Routing Protocols	40
2.4	Comparison of Various Trust approaches of RPL routing and IoT	43
3.1	Simulation Parameters for TDD Mechanism	51
3.2	Simulation Parameters of SLTD	62
4.1	Simulation Parameters of TSF-RPL	77
4.2	Simulation Parameters of MLT-IoT	87
5.1	Elements of Game model of IoT Environment	98
5.2	Elements of Game model of IoT Environment	98
5.3	Utility in a Non-Zero Sum Game Model	105
5.4	Utility in an Evolutionary Game Model	109
6.1	Performance Results of TDD Mechanism and Packet Frequency-based DDoS detection	124
6.2	Performance Results of SLTD mechanism and Intrusion detection without Subjective Logic	125
6.3	Performance Results of TSF-RPL and Trust-based RPL network	127
6.4	Performance Results of MLT-IoT and Existing NBTD Mechanism	129
6.5	Performance Results of S-MODEST and SecTrust Model in terms of Network Area	130
6.6	Performance Results of S-MODEST and SecTrust Model in terms of Number of Attackers	131
6.7	Performance Results of S-MODEST and SecTrust Model in terms of Data Interval	132

## List of Abbreviations

6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
C	Cooperative
CLT	Collaborative lightweight trust-based
CM	Connected Members
COLIDE	COLlaborative Intrusion DEtection
DIO	DODAG information object
DODAG	Destination Oriented Directed Acyclic Graph
DoS	Denial of Service
DT	Direct Trust metric
FI	Failed Interactions
GTMS	Group-Based Trust Management Scheme
IBC	Identity Based Cryptography
IoE	Internet of Everything
IoT	Internet of Things
IP	Internet Protocol
MLT-IoT	Multi Level Trust Based Secure RPL over IoT
NBTD	Neighbor Based Trust Dissemination
NC	Non-Cooperative
NE	Nash Equilibrium
PCs	Personal Computers
PDA	Personal Digital Assistants
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
RPL	Routing Protocol for Low Power and Lossy Networks
RV	Rank Variance
SBIDS	Sink-Based Intrusion Detection System



SI	Successful Interactions
SLTD	Subjective Logic based Trust Mechanism against DDoS
SMRP	Secure Multi-Hop Routing Protocol
TDD	Trust based DDOS Attack Detection
TSF-RPL	Trust Based Selective Forwarding Attack Detection in RPL
TSRF	Trust-Aware Secure Routing Framework
Wi-Fi	Wireless Fieldity
WSN	Wireless Sensor Network