

# **TRUST MODELS FOR SOCIAL IOT NETWORKS**

**NISHIT NARANG**



**DEPARTMENT OF ELECTRICAL ENGINEERING**

**INDIAN INSTITUTE OF TECHNOLOGY DELHI**

**APRIL 2022**

# **TRUST MODELS FOR SOCIAL IOT NETWORKS**

*by*

**NISHIT NARANG**

**Department of Electrical Engineering**

Submitted

in fulfilment of the requirements of the degree of Doctor of Philosophy  
to the



**INDIAN INSTITUTE OF TECHNOLOGY DELHI**

**APRIL, 2022**

©Indian Institute of Technology Delhi (IITD), New Delhi, 2022

# **CERTIFICATE**

This is to certify that the thesis titled “Trust Models for Social IoT Networks”, submitted by Nishit Narang, to the Indian Institute of Technology, Delhi, for the award of the degree of Doctor of Philosophy, is a bona fide record of the research work done by him under my supervision.

The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

**Prof. Subrat Kar**

Thesis Supervisor

Department of Electrical Engineering

Place: New Delhi

Indian Institute of Technology, Delhi

Hauz Khas New Delhi 110016

# ACKNOWLEDGEMENTS

I would like to thank Prof. Subrat Kar, an ideal teacher, mentor and supervisor, whose advice and encouragement not only laid down the foundation for my doctoral research, but was instrumental in helping me go through each phase of this experience. I am extremely grateful for his time and guidance and I am proud of working under his supervision.

Dr Amit Nanavati taught the course on Social Network Analysis, which not only ignited minds, but was the first step forward for my research on this topic. It helped me firm up my problem statement and led to my first publication based on the ideas I learnt from this course. I am grateful to him for playing a key part in my research.

Dr Sumantra Dutta Roy, as the Student Research Committee (SRC) Chairman has always been a motivational factor. His guidance and appreciation of the achievements has helped me keep-up my confidence to continuously march towards my goal.

Dr Seshan Srirangarajan and Dr B.S.Panda, as SRC members have been supportive of my work and have always been there to guide and correct my research path. I am extremely grateful to both of them.

I would like to thank my last organization Altran (*now Capgemini Engineering*) and current employer (BITS Pilani) who provided me with the flexibility required to balance official work with research.

Last, but definitely not the least, I would like to thank my family (parents, spouse and son) for believing in me and providing me the space and time I needed to work towards this goal - a dream that I had been long harbouring and been so passionate about. All of this would not have been possible without their support.

# सार

सामाजिक आईओटी (या *साआईओटी*) आईओटी के लिए एक वैकल्पिक वास्तुशिल्प पैटर्न है, जिसमें सामाजिक, व्यावहारिक विशेषताओं वाले आईओटी उपकरण शामिल हैं। एक *साआईओटी*-आधारित सेवा नेटवर्क कम-विलंबता सहयोगी सेवाओं और अनुप्रयोगों को सक्षम करने के लिए आईओटी उपकरणों (सेवा उपयोगकर्ताओं या सेवा प्रदाताओं या दोनों) के बीच सामाजिक सहयोग का उपयोग करता है। विषम उपकरणों के बहु-विक्रेता वातावरण में *साआईओटी*-आधारित सेवा नेटवर्क को लागू करने में एक प्रमुख चुनौती है *विश्वास*। चुनौती एक सेवा उपयोगकर्ता द्वारा स्वायत्त और स्वतंत्र रूप से भरोसेमंद सेवा प्रदाता (ओं) को प्राथमिकता देना और चुनना है। एकल-विक्रेता नेटवर्क मालिकाना विधियों के माध्यम से समस्या का समाधान करते हैं जो बहु-विक्रेता वातावरण के लिए विस्तार नहीं करते हैं। संसाधन-विवश आईओटी उपकरणों वाले नेटवर्क में समस्या को हल करना भी कठिन है। इस थीसिस में, हम एक हाइब्रिड ट्रस्ट प्रबंधन ढांचे का प्रस्ताव करते हैं जो उपयोग करता है *संभाव्य पड़ोस ओवरलैप (पी-एनओ)*, एक ग्राफ-आधारित अवधारणा जिसे हम नोड्स के बीच टाई-स्ट्रेंथ का अनुमान लगाने के साधन के रूप में परिभाषित करते हैं। अनुमानित टाई-स्ट्रेंथ का उपयोग प्रत्येक सेवा उपयोगकर्ता द्वारा सेवा प्रदाताओं की स्वतंत्र प्राथमिकता के लिए एक विधि के रूप में किया जाता है। पड़ोस ओवरलैप अवधारणा समाजशास्त्र में पिछले शोध से उधार ली गई है और हमारे द्वारा निर्देशित सामाजिक नेटवर्क के लिए विस्तारित है। प्रत्येक सामाजिक बंधन में हमारे कार्य में घटित होने की एक संबद्ध संभावना होती है, जिससे *पी-एनओ* परिभाषा प्राप्त होती है।

हमारा प्रस्तावित ट्रस्ट प्रबंधन ढांचा है *हाइब्रिड* दो कारणों से। सबसे पहले, हम दो प्रकार के सामाजिक नेटवर्क - आईओटी डिवाइस मालिकों के ऑनलाइन सोशल नेटवर्क (*ओएसएन* जैसे फेसबुक) और आईओटी उपकरणों के सोशल नेटवर्क (यानी *साआईओटी* नेटवर्क) से उत्पन्न सामाजिक ग्राफ़ पर *पी-एनओ* लागू करते हैं। तदनुसार, दृष्टिकोण विश्वास प्रबंधन के लिए मानव बुद्धि और मशीन कृत्रिम बुद्धि दोनों का उपयोग करता है। *ओएसएन* से आसानी से उपलब्ध डिवाइस मालिकों की सामाजिक टाई-सूचना का उपयोग करने से ग्राफ़ को कम करने में मदद मिलती है

साआईओटी नेटवर्क संचालन शुरू होने पर आरंभीकरण समस्या। दूसरा, ढांचा गतिशील के मिश्रण का उपयोग करता है ( *बातचीत के आधार पर*) और स्थिर ( *ग्राफ आधारित*) विश्वास प्रबंधन के लिए दृष्टिकोण। यह पूरी तरह से स्थिर विधि की तुलना में इसकी उच्च सटीकता से लाभान्वित होते हुए भी एक शुद्ध गतिशील प्रणाली के संसाधन उपरिव्यय को सीमित करने में मदद करता है।

हमारे प्रस्तावित साआईओटी ट्रस्ट प्रबंधन ढांचे की प्रभावशीलता को उजागर करने के लिए, हम इसके प्रदर्शन के सैद्धांतिक और सिमुलेशन-आधारित विश्लेषण दोनों की पेशकश करते हैं। हम साआईओटी सेवा लेनदेन और नेटवर्क संचालन का अनुकरण करने के लिए सार्वजनिक रूप से उपलब्ध सामाजिक नेटवर्क डेटासेट का उपयोग करते हैं। हमारा अध्ययन आईओटी उपकरणों में सीमित भंडारण और कम्प्यूटेशनल संसाधनों की आवश्यकता के दौरान विभिन्न हमले परिदृश्यों को संभालने में प्रस्तावित ढांचे की प्रभावशीलता को दर्शाता है। हम फॉग कंप्यूटिंग और ब्लॉकचैन-आधारित लेजर जैसी अवधारणाओं को शामिल करते हुए, कंप्यूटिंग और स्टोरेज डोमेन में मौलिक वास्तुशिल्प और तकनीकी प्रगति का उपयोग करते हुए, प्रस्तावित ट्रस्ट फ्रेमवर्क को तैनात करने के लिए सिफारिशें भी प्रदान करते हैं।

# ABSTRACT

Social IoT (or SIoT) is an alternate architectural pattern for IoT, which involves IoT devices with social, behavioural attributes. A SIoT-based service network uses social collaboration between IoT devices (acting as service users or service providers or both) to enable low-latency collaborative services and applications. A key challenge in implementing a SIoT-based service network in a multi-vendor environment of heterogeneous devices is *Trust*. The challenge is prioritizing and selecting trustworthy service provider(s) autonomously and independently by a service user. Single-vendor networks solve the problem via proprietary methods that do not scale for multi-vendor environments. The problem is also tougher to solve in networks with IoT devices that are resource-constrained. In this thesis, we propose a hybrid trust management framework that uses *Probabilistic Neighbourhood Overlap (P-NO)*, a graph-based concept that we define as a means for estimating tie-strengths between nodes. Estimated tie-strengths are used as a method for independent prioritization of service providers by each service user. The neighbourhood overlap concept is borrowed from past research in sociology and extended by us for directed social networks. Each social tie has an associated probability of occurrence in our work, leading to the P-NO definition.

Our proposed trust management framework is *hybrid* because of two reasons. First, we apply P-NO on a social graph generated from two types of social networks - the IoT device owners' online social network (like Facebook) and the IoT devices' social network (i.e. the SIoT network). Accordingly, the approach makes use of both human intelligence and machine artificial intelligence for trust management. Using device owners' social tie-information that is readily available from OSNs helps alleviate the graph

initialization problem when the SIoT network operations start. Second, the framework uses a mix of dynamic (*interaction-based*) and static (*graph-based*) approaches for trust management. It helps limit the resource overheads of a pure dynamic system while still benefiting from its higher accuracy than a completely static method.

To highlight the effectiveness of our proposed SIoT trust management framework, we offer both theoretical and simulation-based analysis of its performance. We make use of publicly available social network datasets to simulate SIoT service transactions and network operations. Our study shows the effectiveness of the proposed framework in handling different attack scenarios while requiring limited storage and computational resources in IoT devices. We also provide recommendations for deploying the proposed trust framework, using fundamental architectural and technological advances in computing and storage domains, involving concepts like fog computing and blockchain-based ledgers.

# TABLE OF CONTENTS

CERTIFICATE .....	i
ACKNOWLEDGEMENTS.....	iii
ABSTRACT .....	v
TABLE OF CONTENTS .....	vii
LIST OF TABLES .....	xi
LIST OF FIGURES .....	xiii
ABBREVIATIONS .....	xv
NOTATIONS .....	xvii
1. Introduction .....	1
1.1 Motivation .....	1
1.2 Literature Survey.....	2
1.2.1 Trust Models for OSN, IoT and Service Networks .....	2
1.2.2 Network Models for Social Networks.....	8
1.2.3 Measuring Tie-Strength in Social Networks .....	9
1.3 Limitations of Past Work.....	10
1.4 The focus of Our Research .....	11
1.5 Organization of the Thesis .....	11
2. Classification Of Trust Models .....	15
2.1 Approach 1: Ratings-based Models .....	15
2.2 Approach 2: Opinion-based Models.....	16
2.3 Approach 3: Cross-Integrated Models.....	17
2.4 Limitations of Existing Approaches .....	18
2.4.1 Limitations with Ratings-based Models .....	18
2.4.2 Limitations with Opinion-based Models.....	19
2.4.3 Limitations with Cross-Integrated Models.....	21

2.5	Summary.....	22
3.	SIoT Trust Models Explored.....	25
3.1	Local Preferential Attachment Model.....	25
3.1.1	Overview.....	26
3.1.2	Data Description.....	27
3.1.3	Analysis of Local Distributions.....	30
3.1.4	Experiments and Observations.....	32
3.1.5	Findings.....	36
3.1.6	Summary of Research on Local Preferential Attachment Model.....	37
3.2	Using Device Owners' OSN Ties.....	38
3.2.1	Dataset Description.....	39
3.2.2	Dataset Analysis.....	40
3.2.2.1	Analysis of st-andrews/sassy Dataset.....	40
3.2.2.2	Analysis of thlab_sigcomm2009 Dataset.....	41
3.2.2.3	Analysis of upb_hyccups Dataset.....	43
3.2.3	Summary of Research on Using Device Owners' OSN Ties for SIoT Trust Modelling.....	44
3.3	Using Neighbourhood Overlap.....	45
3.3.1	Data-driven Validation of Hypothesis.....	46
3.3.2	Defining Neighbourhood Overlap for Directed Networks.....	48
3.3.3	Service Provider Prioritization using Neighbourhood Overlap.....	52
3.3.4	Summary of Research on Using Neighbourhood Overlap for SIoT Trust Modelling.....	53
4.	A Hybrid Trust Management Framework for Multi-service SIoT Networks.....	55
4.1	Probabilistic Neighbourhood Overlap (P-NO).....	55
4.2	Hybrid SIoT Trust Management Framework.....	57

4.3	Salient Features of SIoT Trust Management Framework.....	64
4.4	Initialization and Evolution of SIoT Multi-Service Trust Graph .....	69
4.4.1	Initialization Stage .....	69
4.4.2	Evolution Stage.....	70
4.5	Application of Proposed Framework to Bipartite Networks .....	74
4.6	Summary.....	76
5.	Security Assessment of the SIoT Trust Management Framework.....	79
5.1	Theoretical Analysis of Attack Scenarios and Security Measures .....	80
5.1.1	Slandering / Bad-Mouthing Attack .....	80
5.1.2	Sybil Attack .....	81
5.1.2.1	Sybil + Slandering Attack .....	81
5.1.2.2	Sybil + Self-Promoting Attack.....	82
5.1.3	On-Off Attack .....	83
5.1.4	Ballot Stuffing Attack.....	84
5.2	Analysis of Security Measures via SIoT Network Simulation .....	84
5.2.1	Variations in Simulation Environment .....	84
5.2.2	Simulation Procedure.....	86
5.2.3	Simulation Results and Observations.....	89
5.3	Summary of Attack Scenarios and Security Measures	99
6.	Applications and Deployment of SIoT Trust Management Framework.....	101
6.1	SIoT Trust Framework Deployment Modes .....	101
6.2	Blockchain for Storage of Direct-Opinions.....	102

6.3	Data Privacy Management for OSN Data .....	103
6.4	Applications of SIoT Trust Management Framework	106
6.4.1	Social Internet of Vehicles .....	106
6.4.2	Advanced Metering Infrastructure (AMI) .....	107
6.5	Future Work .....	108
6.5.1	Framework Extensions for SIoT Networks with Communities.....	108
6.5.2	Verification on Real-world Networks .....	109
6.5.3	Protocol for Trust Messaging .....	109
7.	References .....	111
8.	List of Papers based on Thesis .....	119
8.1	ACM MobiCom 2018.....	119
8.2	ICTCS 2019 .....	120
8.3	ACM AIMS 2020 .....	121
8.4	Elsevier Computer Communications .....	122
8.5	Complex Networks CNA 2021.....	123
9.	Author Resume.....	125
10.	Index.....	127

# LIST OF TABLES

Table 1: US Patents Tiered Community Structure.....	28
Table 2: Tier-1 (Category-level) Degree Distribution LRT Results .....	32
Table 3: Tier-1 (Category-level) Degree Correlation Results .....	32
Table 4: Tier-2 (Subcategory) Degree Distribution LRT and Degree Correlation Results .....	33
Table 5: Tier-1 (Category-level) Pairwise External Degree Correlation Results .....	34
Table 6: Sample Degree Distribution LRT Results from Subcategory to Category ( <i>across-tiers</i> ).....	35
Table 7: Sample Degree Correlation Results from Subcategory to Category ( <i>across-tiers</i> ) .....	35
Table 8: Sample Degree Correlation Results from Subcategory to Subcategory .....	36
Table 9: Analysis of Experimental Results and Related Findings .....	36
Table 10: Datasets Used to Study Facebook Social Graph Effectiveness in Reflecting Human Relations.....	39
Table 11: Graph Statistics for thlab_sigcomm2009 Dataset .....	42
Table 12: Graph Statistics for upb_hyccups Dataset .....	44
Table 13: Datasets Used for Study of Neighbourhood Overlap in Directed Graphs .....	50
Table 14: Asymmetry Analysis for Directed Graph Datasets .....	51
Table 15: Comparative Analysis of TRM-SIoT and P-NO Approach .....	65

Table 16: Datasets Used to Simulate SLoT Network Transactions  
..... 85

# LIST OF FIGURES

Figure 1: Organization of the Thesis .....	12
Figure 2: Sizes and Affinity Relationship of Categories .....	29
Figure 3: Citation Edge Matrix for USPCN Categories.....	29
Figure 4: Citation Edge Matrix for USPCN Sub-Categories .....	31
Figure 5: Social Graphs from st-andrews/sassy Dataset.....	41
Figure 6: Social Graphs from thlab_sigcomm2009 Dataset .....	42
Figure 7: Social Graphs from upb_hyccups Dataset.....	43
Figure 8: Overlap Graph for st-andrews/sassy Dataset.....	47
Figure 9: Overlap Graph for upb_hyccups Dataset.....	47
Figure 10: Overlap Graph for thlab_sigcomm2009 Dataset .....	47
Figure 11: Neighborhood Overlap in a Service Network Graph .	49
Figure 12: Overlap Graph for SNAP CollegeMsg Dataset .....	50
Figure 13: Overlap Graph for nodobo Dataset.....	51
Figure 14: Hybrid SIoT Trust Management Framework.....	58
Figure 15: HMST Using MSTG and Device Owners' OSN.....	63
Figure 16: Auto-crawling of the SIoT Service Network .....	71
Figure 17: Merging Multiple Bipartite Graphs to generate MSTG .....	75
Figure 18: Augmenting a Bipartite MSTG with Device Owners' OSN ties for Service-User nodes .....	75
Figure 19: Sybil+Slandering Attack.....	82
Figure 20: Simulation of SIoT Service Transactions and Device Assessments with Periodic Interval of 1 Day .....	88
Figure 21: Simulation for upb_hyccups (With OSN Ties) .....	90

Figure 22: Simulation for ubp_hyccups (Without OSN Ties) .....	91
Figure 23: Simulation for st-andrews/sassy (With OSN Ties) ...	92
Figure 24: Simulation for st-andrews/sassy (Without OSN Ties) .....	93
Figure 25: Simulation for ubp_hyccups (OSN Ties Biased in Favour of Malicious Nodes, prob_malicious_nodes = 0.5) .....	94
Figure 26: Simulation for st-andrews/sassy (OSN Ties Biased in Favour of Malicious Nodes, prob_malicious_nodes = 0.5) .....	94
Figure 27: Simulation for ubp_hyccups (OSN Ties Biased in Favour of Benign Nodes, prob_malicious_nodes = 0.8) .....	95
Figure 28: Simulation for st-andrews/sassy (OSN Ties Biased in Favour of Benign Nodes, prob_malicious_nodes = 0.8) .....	96
Figure 29: Simulation for collegeMsg (Without OSN Ties) .....	97
Figure 30: Simulation for nodobo (Without OSN Ties) .....	98
Figure 31: Simulation for thlab_sigcomm2009 (With OSN Ties, prob_malicious_nodes = 0.2) .....	99
Figure 32: Simulation for thlab_sigcomm2009 (Without OSN Ties, prob_malicious_nodes = 0.2) .....	99
Figure 33: Trust Framework Deployment Modes .....	102

# ABBREVIATIONS

<b>AMI</b>	Advanced (or Automated) Metering Infrastructure
<b>FB</b>	Facebook
<b>HMST</b>	Hybrid Multi-service Social Tie-graph
<b>IoT</b>	Internet of Things
<b>LRT</b>	Likelihood Ratio Test
<b>M2M</b>	Machine to Machine
<b>MSTG</b>	Multi-service SIoT Trust Graph
<b>NO</b>	Neighbourhood Overlap
<b>OSN</b>	Online Social Network
<b>PCC</b>	Pearson Correlation Coefficient
<b>P-NO</b>	Probabilistic Neighbourhood Overlap
<b>RSSI</b>	Received Signal Strength Indicator
<b>RSU</b>	Road Side Unit
<b>SIN</b>	Special-purpose Infrastructure Node
<b>SIoT</b>	Social Internet of Things
<b>SIoV</b>	Social Internet of Vehicles
<b>TMS</b>	Trust Management System
<b>USPCN</b>	US Patent citation network
<b>V2V</b>	Vehicle-to-Vehicle
<b>V2X</b>	Vehicle-to-Everything

**VANET**      Vehicular Ad-hoc Network

**WSN**        Wireless Sensor Network

# NOTATIONS

$\mathbf{a} \xrightarrow{S} \mathbf{b}$	It represents an edge from service user node 'a' to service provider node 'b' for service 'S' in a directed service network graph.
$P_S^x$	The set of all (service-provider) nodes whom (the service-user) node 'x' considers <i>trustworthy</i> for the service 'S'.
$U_S^x$	The set of all (service-user) nodes who consider (the service-provider) node 'x' as <i>trustworthy</i> for the service 'S'.
$\mathbf{NO} \{\mathbf{x} \xrightarrow{S} \mathbf{y}\}$	Neighbourhood Overlap (NO) of edge $\{\mathbf{x} \xrightarrow{S} \mathbf{y}\}$ .
$\mathbf{P-NO} \{\mathbf{x} \xrightarrow{S} \mathbf{y}\}$	Probabilistic Neighbourhood Overlap (P-NO) of edge $\{\mathbf{x} \xrightarrow{S} \mathbf{y}\}$ .