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

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, व्यवहारिक 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

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

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

VANET Vehicular Ad-hoc Network

WSN Wireless Sensor Network

NOTATIONS

'a' $\xrightarrow{S}$ **'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 *trustworthy* for the service 'S'.
U_S^x	The set of all (service-user) nodes who consider (the service-provider) node 'x' as *trustworthy* for the service 'S'.
NO {'x' $\xrightarrow{S}$ **'y'}**	Neighbourhood Overlap (NO) of edge {'x'$\xrightarrow{S}$'y'}.
P-NO {'x' $\xrightarrow{S}$ **'y'}**	Probabilistic Neighbourhood Overlap (P-NO) of edge {'x'$\xrightarrow{S}$'y'}.