University of Pittsburgh | School of Computing and Information

Proposal Defense

Doctor of Philosophy in Information Science

"**Trust Evolution in IoT Networks with Multiple Attributes**" by **Nuray Baltaci Akhuseyinoglu**

Date: August 30, 2021
Time: 10:00am – 12:00pm
Place: https://pitt.co1.qualtrics.com/jfe/form/SV_3DY2D8oYvJAbg7s

Committee:

- Dr. Prashant Krishnamurthy, Professor, School of Computing and Information
- Dr. Konstantinos Pelechrinis, Associate Professor, School of Computing and Information
- Dr. Amy Babay, Assistant Professor, School of Computing and Information
- Dr. Mai Abdelhakim, Assistant Professor, Department of Electrical and Computer Engineering, Swanson School of Engineering

Abstract:

Internet of Things (IoT) is a communication paradigm comprising millions of devices, a.k.a *things* or *nodes,* growing in number. Things are interconnected smart devices that operate with or without human intervention, such as sensors, actuators, RFID devices, wearable devices, or more powerful computing systems. The heterogeneity of devices, software components, and network infrastructure in IoT leads to increased attack surfaces. One of the significant security threats for IoT is untrustworthy data and operations that may arise due to device compromise, vulnerable transmission medium, or faulty sensors. It is essential to ensure trust in the data and operations in IoT, as it is fundamental for people to overcome perceptions of uncertainty and risk in using IoT services and applications. The lack of trust may have dire consequences for IoT. For example, an attacker compromising an IoT device can generate or report bogus data, boost the reputation of malicious nodes, and ruin that of benign nodes.

There are security mechanisms to defend against external attacks in IoT, such as cryptographic algorithms. Yet, they cannot identify internal attacks as a benign node could turn into a malicious node any time after joining the network through a successful exchange of cryptographic keys and behaving benign for some period. *Trust management* solutions are essential for detecting misbehaving legitimate nodes in IoT when cryptographic measures are not applicable. IoT brings extra challenges to trust management due to ever-changing network topology, heterogeneity in devices and network topology, and limited resources of constrained devices. Promising solutions have been proposed for IoT trust management to address these challenges. Yet, they are limited in accommodating key trust properties and automated trust computation need in IoT environments.

The research in this dissertation proposal focuses on trust evolution in IoT networks drawing upon the research on trust in social sciences. Towards this, we distill significant aspects of trust evolution in social sciences and capture them in solutions for IoT trust management through automated trust computations. More specifically, we propose an automated trust computation framework based on Multi-Attribute Decision Making (MADM) approach and Evidence-based Subjective Logic to account for multi-dimensionality and uncertainty aspects of trust. Also, we propose to extend the trust model of this framework with trust attributes based on our review of social sciences trust literature. We will compare the performance of the two frameworks concerning widely used performance evaluation criteria by the existing IoT trust research. Additionally, we propose to explore trust repair strategies for IoT and a model to reflect these on automated trust computations. Finally, we propose to investigate trust computation issues for multiple IoT network administrative domains and solutions to address them in a trust computation framework.