University of Pittsburgh | School of Computing and Information

Proposal Defense

Doctor of Philosophy in Telecommunication and Networked Systems

"On contextual decision making and action enforcing applications in wireless networks and IoT using SDN as a platform"

by **Maryam Karimi**

Date: April 30, 2021
Time: 1:00PM – 3:00PM
Place: https://pitt.co1.qualtrics.com/jfe/form/SV_eWewXEzw1x5C474

Committee:

- Dr. Prashant Krishnamurthy, Professor, School of Computing and Information
- Dr. Martin Weiss, Professor, School of Computing and Information
- Dr. David Tipper, Professor, School of Computing and Information
- Dr. Mai Abdelhakim, Assistant Professor, Department of Electrical and Computer Engineering

Abstract:

The Internet of Things (IoT) is increasingly helping to solve new challenges that can lead to a better quality of life, higher efficiencies and reduced costs. Variety of wearable devices and sophisticated, yet not very expensive connected devices gather different kinds of information (mostly) on their premises about the human body, social activities, etc., and enable people to make decisions or control actions. The complexity of such decisions with performance tradeoffs needs a suitable architecture that can employ data driven decisions for performance improvements. Software defined networks (SDN) and software defined perimeter (SDP) are suitable platforms for implementing the services that require gathering information from the context and performing contextual decision making while managing specific parameters and enforcing actions based on them. This dissertation proposal examines two case studies and proposes a third one toward the dissertation.

In the first case study, we investigate the Interference Management. We explore the use of historical data in WiFi networks to create a classification QoS decision tree that predicts the maximum delay due to specific traffic situations with specific context parameters and makes rapid decisions possible to manage wireless network resources considering quality requirements. We use an agent on each AP for adjusting the OpenFlow network access and gathering necessary context in wireless networks. In the second case study, we investigate contextual integrity verification in IoT. A variety of IoT devices may be required to outsource sensed or generated data to multiple heterogeneous cloud servers. We posit that it is the *Data Owner*'s responsibility to verify whether the stored data remain unchanged. However, the "level" of this verification may be different under different *contexts*. We propose four typically disparate methods of integrity verification and consider the "toll" in terms of time, storage and communication to decide on a suitable data integrity verification process. We adapt the notion of contextual privacy to extract important parameters. In addition to the contextual information that SDN provides we need security context information and a secure infrastructure for authentication and communication; therefore, we propose a secure architecture with integration of SDP and SDN. Finally, we propose the use of Bayesian inference with specific datasets to improve the performance of decision making and automate the detection of how critical each context variable is and how it would affect the probability of choosing an action to be enforced.