Cyber-Assurance for the Internet of Things, Software-Defined Networks and Fog Computing Architectures

Dr. Tyson Brooks, Chair
Syracuse University
ttbrooks@syr.edu

Dr. Shiu-Kai Chin
Syracuse University
skchin@syr.edu

Dr. Erich Devendorf
Air Force Research Laboratory
erich.devendorf.1@us.af.mil

Description of Mini-Track

The objective of this mini-track is to increase the visibility of current research and emergent trends in Cyber-Assurance theory, application, embedded security and machine-learning for the Internet of Things (IoT), software-defined networks (SDN)/network function virtualization (NFV) and Fog computing architectures based on theoretical aspects and studies of practical applications. Cyber-assurance is the justified confidence that networked systems are adequately secure to meet operational needs, even in the presence of attacks, failures, accidents and unexpected events. Cyber-assurance means that IoT systems, smart internet connected devices (ICD) and networks provide the opportunity of automatically securing themselves against cyber-attacks. The difference is that the concept of cyber-assurance must provide embedded, secure microchips/processors in ICD devices and virtual networks that can continue to operate correctly even when subjected to an attack.

IoT devices using SDN/NFV and Fog computing systems and networks should be able to resist the various security cyber-attacks such as hacking of networks, devices, theft of information, disruption, etc. and be able to continue performing under severe environmental conditions. Through embedded processors and machine learning algorithms over the transmitted information, the miscoding and leaking of information during transmission channels has to monitor any loss, miscoding and leaking of data. Timely adjustments of information with falling quality and automatic switching to the best routing IoT systems by making uses of multi-directional routing is also warranted. Cyber-assurance will need to provide the principles and technologies to unify these systems to deliver the end-state goal of secure IoT systems for greatly enhanced interoperability, scalability, performance, and agility.

The target audience of this mini-track will be composed of researchers, professionals and students working in the field of cyber-security, wireless technologies, information system theory, systems engineering, information security architecture and security system design along with university professors and researchers involved in information assurance, cyber-security, IoT, SDN/NFV and Fog computing related networking. Through the research identified for this track, graduate students, researchers and academics who want to improve contribute their understanding of the latest security developments for the IoT, SDN/NFV and Fog computing. This mini-track will focus on the security needs of these environments, highlighting key issues and identifying the associated security implications so that the general participates can readily grasp the core ideas in this area of research.