CALL FOR WORKSHOP PAPERS

SecSDN: The IEEE International Workshop on Secure and Dependable Software-defined Networking for Sustainable Smart Communities

Workshop Scope: The Internet is transforming society to live in the digital age and keep the constituents up-to-date for a better outcome. The digital age is empowering users to adopt Internet-of-Things (IoTs) in various domains like smart homes, smart cities, smart industries, and even an intelligent transportation system. The connected hardware devices (sensors, actuators, gateways, smart meters, switch, and routers) generate and exchange data to enable fast communication among heterogeneous devices. The data is transported to the network through advanced wireless communication technologies and communicated among various domains such as a device to device, the device to cloud, or device to gateway. The IoT plays an important role in guaranteeing the services to the providers but the communication infrastructure is facing challenges in terms of high latency, cost, and energy consumption. Moreover, traditional networking is based on a manual approach; it becomes difficult to handle massive requests simultaneously on the data centres. The issues of interoperability, data consistency, and security are a big concern with traditional networking.

The beauty of SDN technology helps us to isolate the control plane from the data plane and solves the issues through network programmability. The SDN is a centralized approach and easily modify the network topology, and in addition, maintain data consistency and interoperability among heterogeneous IoT devices with the help of automation. Although SDN technology performs resilient and reliable connections in the heterogeneous environment based on secure communication protocols designed by the network programmers still chances of security threats may occur as a single controller is handling the complete network infrastructure. With the widespread adoption of wireless sensors in smart communities, device-to-device communication is susceptible to security vulnerabilities and resulting in devastating attacks on the network controller. The IoT is insecure as sensors may be infected by malware attack have subsequently comprised the control plane. Consequently, ensuring the security and privacy techniques may contribute to defend from security attacks and provide reliable services in smart communities. Moreover, the higher costs, overhead and complexity of traditional cryptographic primitives make it necessary to design lightweight and novel security solutions for SDN in smart communities. The amalgamation of multiple technologies in smart communities makes it further necessary to provide secure communication and computing paradigm.

Addressing the need for a flexible network architecture that adapts to the diverse requirement of end-users in smart communities, this workshop aims to serve as a platform for researchers from academia and industries, to promote the design and development of new ideas, tools and technologies related to Secure and Dependable SDN in Smart communities.

Topics of Interest

- Security and privacy for innovative service delivery models in SDN architecture.
- Lightweight Cryptography in wireless sensors nodes for SDN security.
- Quantum Cryptography in heterogeneous IoT devices for SDN security.
- Secure device-to-device communication in SDN environment.
- Authentication, authorization, and access control (AAA) for SDN security.
- Anomaly detection and prevention mechanisms in smart communities.
- Secure integration of IoT and fog devices for SDN.
- Intrusion detection system and intrusion prevention system for SDN security.
- Heterogeneous system model and trustworthy communication architectures.
- Secure data storage and computing model in SDN.
- Testbed and experimental components tailored to specific SDN security.
- Security threats and vulnerability detection in a heterogeneous environment.
- Blockchain for secure transaction management using SDN in smart communities.
- Deduplication architectures for secure cloud storage in smart communities.
- Security and privacy standardization for SDN in smart communities.
- Dependable control plane optimization for SDN in Smart Communities.

Important Dates:

Submission: **15 July 2020**
Notification: **1 September 2020**
Camera Ready: **1 October 2020**

Workshop Organizer(s):

Gagangeet Singh Aujla, Newcastle University, Newcastle Upon Tyne, UK.
Neeraj Kumar, Thapar Institute of Engineering and Technology, Patiala (Punjab), India.
Mohsen Guizani, University of Qatar, Doha.