FNSSC`2017

Workshop on Future Networks for
Secure Smart Cities

IEEE IM™

*To be held jointly to **IFIP/IEEE International Symposium on Integrated Network Management** (Lisbon, May 2017)*

ifip
IEEE

Scope

Future Smart Cities are expected to carry massive amount of extremely sensitive data related to residents' private life. Just to mention a few, information about transportation, health care, public administration, education will be constantly collected and processed in order to provide citizens with essential services on a daily basis. This trend rises widespread concerns about the security of the infrastructure used to gather and analyze those data.
Traditional computer networks seem to lack all the necessary features to smoothly implement the required mechanisms to protect the infrastructure and the transferred data therein. In fact, inherent characteristics of traffic, network topologies and devices present in Smart Cities make the design and implementation of security mechanisms extremely challenging.
Although common good practices are followed by devices manufacturers and vendors, the integration of different devices still presents a number of issues with regard to interconnectivity, communication, applicability, security and privacy. Moreover, many of the devices classified into the Internet of Things have limited resources (from the point of view of computing power and storage), which makes the execution of complex communication and security mechanisms difficult.
An interesting, yet unexplored, research area lays at the intersection of novel network paradigms, like the Software-Defined Networking (SDN) and the Information-Centric Networking (ICN). Those novel approaches considerably extend the toolkit available to network operators by enhancing control and data-plane logics. Novel paradigms may solve new challenges of security and data privacy, energy-consumption concerns and issues related to massive interconnectivity of objects and services.
The Workshop on "Future Networks for Secure Smart Cities" (fnssc.itl.waw.pl) provides a forum for discussions on the potential of novel networking paradigms for the development of Smart Cities. It brings together industry and academia, engineers and researchers to propose solutions as well as to identify open security challenges in the design and maintenance of solutions in urban environments.

Topics of Interest

The workshop invites submissions of unpublished works proposing architectures and mechanisms to improve the security of services provided within Smart Cities. Topics of interest include (but not limited to):

- Architectures for security monitoring in urban environments
- Interconnection of existing services in Smart Cities
- Trust management schemas
- SDN control plane application for anomalies detection in traffic scenarios
- Security and energy-saving improvements for SDN/ICN protocols
- Solutions for interconnectivity and security in smart buildings
- Advanced fault tolerance and resiliency mechanisms
- Lightweight secure solutions to interconnect sensor networks in urban zones
- Threats and countermeasures of massive interconnectivity
- Use cases for SDN and ICN in Smart Cities
- Integration of SDN and ICN protocols

Submission Instructions

Prospective authors are invited to submit original, unpublished works for publication in the IEEE IM 2017 proceedings and for presentation in the workshop.
Please, follow the same instructions as for IM Technical Papers (IEEE 2-column style to be included in IEEE Xplore). However, in order to undergo the single-blind review process, submissions must have a maximum length of 6 pages (including title, abstract, all the tables and figures and references).
Papers should be submitted through JEMS by selecting *IM 2017 – FNSSC 2017* track.

Important Dates

Paper registration: ~~Dec 15, 2016 (Thursday)~~ extended Jan. 15, 2017
Paper Submission: ~~Dec 19, 2016 (Monday)~~ extended Jan. 15, 2017
Notification of acceptance/rejection: Jan 30, 2017 (Monday)
Camera ready: Feb 15, 2017 (Wednesday)