Security and Communication Networks

WILEY | Hindawi

Special Issue on
Security and Privacy for Smart, Connected, and Mobile IoT Devices and Platforms

CALL FOR PAPERS

In recent years, with the rapid development of the smart city paradigm, the Internet of Things (IoT) has raised widespread concern in the whole ICT community. IoT refers to linking the sensors, controllers, machines, people, and things together by using local networks, the Internet, or other communication technologies through a new way to build intelligent things to things network. However, in the near future, the large-scale deployment of the IoT also needs to face many challenges, especially in security and privacy issues for smart, connected, and mobile IoT devices and platforms due to the fact that IoT has different characteristics from the traditional communication networks, related to its specific features and threats. In particular, the security solutions for IoT must provide IoT nodes (things, users, servers, and objects) with data authenticity, confidentiality, integrity and freshness certification, and authorization. In addition, privacy protection must also be considered. Many IoT services and applications may expose sensitive and personal information which may be abused by attackers. The concept of privacy may be different, but it should protect the user's personal identity information and maintain a certain degree of anonymity, nonlinkability, and data confidentiality. Of course, it is also necessary to strike a balance between the availability and the security and privacy protection for IoT.

The special issue will focus on the IoT devices and platforms with respect to security and privacy preserving technologies for speeding up technological progress and attracting more researchers' concerns about the development in this field. In addition, this special issue will include the extended versions of the best papers, which will be presented at the 2nd International Symposium on Mobile Internet Security (MobiSec'17, https://isyou.info/conf/mobisec17/).

Potential topics include but are not limited to the following:

- Advanced IoT security technology and applications
- IoT privacy and trust model
- Security related hardware and platforms in IoT
- Authentication and access control in IoT
- Data processing and privacy in IoT
- Security protocols for IoT
- Semantic approaches for multimedia retrieval applications
- IoT security and privacy issues in cyberphysical systems
- Network security for IoT
- Software security for IoT
- Threat intelligence for IoT
- Lightweight security and cryptographical technology for IoT
- Standardization aspects of IoT security and privacy
- IoT wireless communication technology
- Intrusion detection and tolerant fault tolerance technology for IoT
- Malware detection and prevention technology for IoT
- Cryptographic hardware development for IoT devices

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/spsc/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Karl Andersson, Luleå University of Technology, Skellefteå, Sweden
karl.andersson@ltu.se

Guest Editors
Ilsun You, Soonchunhyang University, Chungcheongnam-do, Republic of Korea
ilsunu@gmail.com

Francesco Palmieri, University of Salerno, Fisciano, Italy
fpalmieri@unisa.it

Submission Deadline
Friday, 23 February 2018

Publication Date
July 2018