Call-for-papers for Special Issue on *Security and Forensics of Internet-of-Things: Problems and Solutions*

Internet-of-Things (IoT) are becoming increasingly prevalent in our society, as the backbone of interconnected smart homes, smart hospitals, smart cities, smart wearables, smart supply chain, and a variety of other smart environments. IoT devices leverage from embedded technologies equipped with sensors and communication capabilities; they are able to broadcast their presence to other objects and interact with them using different protocols. Gartner predicts that, by 2020, 21 billion IoT endpoints will be in use. Along with usability, efficiency, and cost saving benefits, increasingly, the popularity of IoT pose security risks and raise challenges to digital forensics. Aspects such as low processing power and small storage capacity of such IoT devices contribute to their typically poor built-in security and forensics capabilities. Their reliance in the cloud and mobile apps to operate and provide services increase the attack surface, distributing the collection of digital evidence and making reconstruction activities (to answer questions as what, where, when, who, why and how) harder. The high potential for security impact has been demonstrated by the massive DDoS caused by the Mirai botnet in 2016, and subsequent variants which exploit smart cameras and home routers. Security related aspects have been hindering a faster adoption of IoT devices, sharply fostering research on the aforementioned areas of knowledge. This special issue aims to bring the security and digital forensics R&D communities together to advance knowledge of problems and solutions applicable to different smart environments. Topics of interest include, but are not limited to:

- Security architectures and protection mechanisms for IoT
- Threat models and attack strategies for IoT
- Security applications and management of IoT
- Intrusion and malware detection/prevention technologies for IoT
- Cyber physical IoT systems
- Security in Wireless Sensor Networks applied to IoT
- Challenges related to IoT forensics and security
- Privacy and trust in IoT
- Adaptive security in IoT
- Identification/preservation of evidence for DF investigations involving IoT
- Data analysis of IoT for forensic investigation
- Models for risk identification and assessment in IoT networks
- Data ownership and attack simulation methods for IoT networks and devices
- Legal and human aspects of security and forensics of IoT
- Coexistence of different protocols in IoT environments
- Cryptography protocols and algorithms for IoT
- Cybercrimes exploiting IoT
- Trends in specific IoT domains
- Covert communication in IoT

Important dates

Submissions Deadline: **August 15, 2018**
First Reviews Due: November 1, 2018
Revision Due: December 1, 2018
Second Reviews Due/Notification: January 1, 2019
Final Manuscript Due: **February 1, 2019**
Publication Date: 2019

Submission guidelines

All original manuscripts or revisions to the IEEE IoT Journal must be submitted online through IEEE Manuscript Central http://mc.manuscriptcentral.com/iot
Author guidelines and submission information can be found at http://ieee-iotj.org

Guest editors

Virginia N. L. Franqueira, University of Derby, UK
Aleksandra Mileva, University of Goce Delcev, MK
Ville Leppänen, University of Turku, FI
Pedro Inácio, Universidade da Beira Interior, PT
Mauro Conti, University of Padua, IT
Raul H. C. Lopes, Brunel University, JISC & CMS/CERN, UK