Security and Communication Networks

Special Issue on

Security, Privacy, and Blockchain-Based Solutions for IoT in Next Generation and Softwarized Networks

CALL FOR PAPERS

In the Internet of Things, billions of interconnected devices, distributed across remote areas, serve as a baseline for empowering innovative services. In such a distributed, pervasive, and dynamic environment, devices, sensors, networks, and services are exposed to additional threats. The limited capabilities of the involved IoT constrained devices and networks in terms of processing power, storage, and energy make them vulnerable to diverse kinds of threats and attacks.

Moreover, IoT communication protocols and frameworks need to be adapted to service requirements for real-time and critical applications, while considering the associated security and privacy landscape. Several low-power wireless communication protocols and technologies, for both short and wide range, such as NB-IoT, LTE-MTC, Sigfox, 5G, Bluetooth low energy (BLE), and 6LowPAN, are emerging, trying to provide holistic IoT connectivity while handling the associated security aspects. Besides, the IoT can leverage blockchain as well as virtualized and softwarized paradigms and architectures, such as SDN and NFV, in order to endow the IoT with several management and security benefits.

There is a strong need for security and privacy solutions and techniques aimed at providing integral protection for IoT scenarios and networks, by relying, for instance, on SDN/NFV-enabled architectures and/or blockchain. Thus, this special issue aims to solicit high-quality papers reporting on the latest research advances in security and privacy aspects for IoT networks.

Papers will be evaluated based on their originality, presentation, relevance, and contribution to the field of security and privacy in next generation IoT networks, as well as their suitability to the special issue, and for their overall quality. The submitted papers must describe original research that has not been published or currently under review by other journals or conferences. Both theoretical and experimental studies are encouraged. Furthermore, high-quality review papers are also welcomed.

Potential topics include but are not limited to the following:

- Security and privacy solutions based on blockchain for IoT
- Security and privacy in LPWAN (NB-IoT, LTE-MTC, Lora, Sigfox, etc.)
- Security and privacy in 5G-enabled IoT networks
- Attacks detection and prevention systems for IoT networks
- Identity and AAA management for IoT networks
- Security and privacy in Edge and Fog computing networks for IoT
- Network slicing in IoT networks
- Security and privacy for IoT in short and medium range radio access
- Security and privacy in SDN/NFV-enabled IoT networks
- Monitoring, accountability, and forensics in IoT networks and systems
- IoT Botnets and DDoS prevention and mitigation
- Trust management in IoT networks
- Intrusion detection and prevention systems in IoT networks
- Privacy-preserving solutions and challenges for IoT networks
- Countermeasures solutions for IoT networks

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

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

Lead Guest Editor
Jorge B. Bernabe, University of Murcia, Murcia, Spain
jorgebernal@um.es

Guest Editors
Jose M. Alcaraz-Calero, University of the West of Scotland, Glasgow, UK
jose.alcaraz-calero@uws.ac.uk

Khaled Salah, Khalifa University of Science, Abu Dhabi, UAE
khaled.salah@kustar.ac.ae

Julien Bringer, Smart Valor, Zug, Switzerland
julien.bringer@smartvalor.com

Submission Deadline
Friday, 1 February 2019

Publication Date
June 2019