Annals of Telecommunications

Call for papers
Special Issue on

Security and Privacy in IoT Communication

Nowadays, many Internet-of-Things (IoT) technologies have been established as the building blocks of modern communication services, such as wired/wireless networks, RFID, cloud services, machine-to-machine interfaces, and so on. The modern IoT communication allows billions of objects in the physical world as well as virtual environments to exchange data with each other in an autonomous way so as to create smart environments in many applications, such as automotive, healthcare, logistics, environmental monitoring. However, the modern IoT communication also introduces new challenges in security and privacy. On one hand, considering the modern IoT communication provides global connectivity and accessibility, it is inevitable that the number of attack vectors available to malicious attackers could be incredibly large, such that protecting the information security in modern IoT communication has become a difficult task. On the other hand, the modern IoT communication enables multiple heterogeneous entities located in different contexts to exchange information with each other inherently, in which security mechanisms are supposed to be efficient, interoperable, and scalable during deployment and execution. As a result, there is an increasing demand for development of new approaches to guarantee the security, privacy, integrity, and availability of resources in modern IoT communication.

This feature topic will benefit the research community towards identifying challenges and disseminating the latest methodologies and solutions to security and privacy issues in modern IoT communication technologies. Its objective is to publish high-quality articles presenting open issues, algorithms, protocols, policies, frameworks, standards, and solutions for IoT communication related to security and privacy. All received submissions will be sent out for peer review by at least three experts in the field and evaluated with respect to relevance to the special issue, level of innovation, depth of contributions, and quality of presentation. Reviews and case studies, which address state-of-art research and state-of-practice industry experiences, are also welcomed. Guest editors will make an initial determination of the suitability and scope of all submissions. Papers that either lack originality, clarity in presentation or fall outside the scope of the special issue will not be sent for review and the authors will be promptly informed in such cases. Submitted papers must not be under consideration by any other journal or publication.

Topics of interest include, but are not limited to, the following:

- Secure Data Management in IoT
- IoT Intrusion Detection and Prevention, Firewalls, Packet Filters
- Malware, Botnets, and Distributed Denial of Service in IoT
- IoT Communication Privacy and Anonymity
- IoT Forensics Techniques
- Public Key Infrastructures, Key Management, and Credential Management
- Secure Routing in IoT
- Security & Privacy in Pervasive and Ubiquitous Computing
- Security & Privacy for IoT applications
- Disaster Recovery in IoT Communication and Networks
- Reliability of IoT Communication
- Bootstrapping and supervising privacy and security
- Access control and usage control
- Privacy-by-design and implementation of data protection regulation (e.g. GDPR)
- Resilient IoT communications and services

Guest Editors

- **Jin Li, School of Computer Science, Guangzhou University, China (Lead guest editor)**
- **Mohammed Atiquzzaman, School of Computer Science, University of Oklahoma, USA**
- **Sheng Wen, School of Software and Electrical Engineering, Swinburne University of Technology, Australia**

Papers must describe original research that advances state-of-the-art in the area of cybersecurity and must not be simultaneously submitted to a journal or a conference with proceedings. Papers must be written in excellent English and should not exceed 10 pages. Previously published or accepted conference papers must contain at least 40% new material to be considered for the special issue. A covering letter to the Guest editors clearly describing the extensions made must accompany these types of submissions. All submissions must be made using the instructions available at:

http://annalsoftelecommunications.wp.mines-telecom.fr/how-to-publish/

The authors can directly submit their papers at: https://www.editorialmanager.com/ante/ and must select the menu “Choose Article Type” and then the item “CfP: Security and Privacy in IoT Communication”.

Proposed schedule

Manuscript submission	July 10, 2018
Notification	September 15, 2018
Final revised papers due	November 15, 2018
Online with DOI	As soon as accepted
Printed issue	Early 2019

Published by Springer, *Annals of telecommunications*
is indexed in ISI and Scopus Databases, 2016 Impact Factor: 1.4
2016 *Journal Citation Reports* ® Science Edition (Thomson Reuters, 2017)