Security and Communication Networks

Special Issue on **Security, Privacy and Trust Challenges in Mobile Crowdsensing**

CALL FOR PAPERS

Mobile crowdsensing systems (MCS) rely on contributions from mobile devices of a large number of participants or a crowd, where a large group of individuals having mobile devices capable of sensing and computing collectively share data and extract information to measure, map, analyze, estimate, or infer (predict) any processes of common interest. It is advantageous in low deployment cost and vast geographic coverage and has found numerous applications in diverse domains, including transportation, environment monitoring, smart cities, pervasive healthcare, and so on.

However, MCS systems often face the challenge of security, privacy, and trust issues. Motion sensors such as accelerometers and gyroscopes embedded in smartphones play an important role in monitoring our real-world surroundings, which is related to numerous privacy invasion attacks, such as private information leaks related to human behaviours, physical features, and location information. Although users carrying mobile smart devices are willing to participate in the mobile sensing process, they may not disclose their private information like location, voice, and operating record. Additionally, the MCS can easily suffer from side-channel attacks, where physical information leakage during the operation of basic sensors is exploited to deduce the confidential data in mobile crowdsensing applications. Most of the security and privacy issues can be solved with some traditional cryptography methods; however, the heavyweight cryptosystem still cannot be performed on the billions of resource-constrained smart mobile or Internet of Things devices, which restrict the applications in MCS.

The aim of this Special Issue is to solicit original research and review articles to gather recent advanced security, privacy, and trust techniques relevant to the convergence of mobile crowdsensing. In particular, experimental approaches with publicly released code, tools, and data are welcomed.

Potential topics include but are not limited to the following:

- Authentication in mobile crowdsensing
- Lightweight data protection scheme for MCS
- Secure model protection method for AI in MCS
- Hardware security and privacy issues for IoT and mobile devices
- Secure data integrity and validation techniques for MCS
- Privacy computation and processing protocols for crowdsensing
- Secure M2M communication for distributed mobile devices
- Formal security model for cryptographic protocols for MCS
- Future and secure IoT-based data collection methods in MCS
- Trust and reputation system in MCS
- Secure data mining and machine learning in MCS
- Virtualization, security, and management for MCS
- Side-channel attacks and defence methods for MCS
- Blockchain and smart contracts for MCS
- New privacy challenges in MCS

Authors can submit their manuscripts through the Manuscript Tracking System at https://review.hindawi.com/submit?specialIssue=881846.

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

Lead Guest Editor

Ximeng Liu, Fuzhou University, Singapore
snbnix@gmail.com

Guest Editors

Athanasios V. Vasilakos, Luleå University of Technology, Luleå, Sweden
th.vasilakos@gmail.com

Yinbin Miao, City University of Hong Kong, Hong Kong
yinbmiao@cityu.edu.hk

Submission Deadline

Friday, 26 February 2021

Publication Date

July 2021