IEEE Internet of Things Journal Special Issue on
High-Confidence City IoT for Collaborative Smart City Services

IoT is a critical infrastructure component as well as an enabling technology to support the fast-developing cross-region, cross-application, and diversified collaborative smart city services that require systematic cooperation among multiple smart city systems. Such services put forward the high-confidence demands of city IoT, namely city IoT infrastructures and their offered services should be accountable, expandable, reliable, secure and privacy-savvy, and can self-adapt to accommodate new environments and self-evolve to support emerging applications. Making city IoT high-confidence to assist collaborative smart city services is a nontrivial task, facing the challenges from the physical world, cyber world, and application services. In the physical world, city IoT is an open giant complex system; in the cyber world, IoT data is massive, heterogeneous, and multi-sourced; while the application services are cross-region, cross-application, and diversified. Although enormous amount of effort has been made in both academia and industry all over the world to address these challenges, the solutions are mainly isolated and fragmented, with few jointly considering all the high-confidence features; moreover, accountability/traceability needed by collaborative smart city services is largely ignored.

In this special issue, we look for original work on high-confidence IoT to support collaborative smart city services. Relevant topics include, but are not limited to:

- Expandable and accountable city IoT architectures
- Blockchain enhanced city IoT architectures
- SDN-enabled city IoT architectures
- NFV for dynamic function expansion and adaptation
- Access control to secure the open city IoT environment
- Tee-enabled trusted data collection
- Malicious, damaged, and white-noise data cleaning and extraction
- Intelligent cyber-physical closed loop control
- Spatial-temporal city big data fusion for intelligent decision making
- Migration learning and digital twin technologies
- Cascading failure detection and recovery
- Cascading vulnerability detection and positioning
- Active defense technologies
- Modeling, analysis, and measurement of high-confidence city IoT
- Testbed and empirical studies

Important Dates:

Submission Deadline: March 1, 2020
First Round Review Due: May 15, 2020
Revision Due: July 1, 2020
Acceptance Notification: August 1, 2020
Final Manuscript Due: August 15, 2020
Publication Date: 2020

Submission Guidelines:

All original manuscripts or revisions to the IEEE IoT Journal must be submitted electronically through IEEE Manuscript Central, http://mc.manuscriptcentral.com/iot. Solicited original submissions must not be currently under consideration for publication in other venues. Author guidelines and submission information can be found at http://ieee-iotj.org/guidelines-for-authors/.

Guest Editors:

- Dongxiao Yu, Shandong University, P. R. China (dxyu@sdu.edu.cn)
- Xiuzhen Cheng, The George Washington University, USA (cheng@gwu.edu)
- Falko Dressler, Paderborn University, Germany (dressler@ccs-labs.org)
- Dariusz R. Kowalski, Augusta University, USA (dkowalski@augusta.edu)
- Weifeng Lv, Beihang University, P. R. China (lwf@buaa.edu.cn)