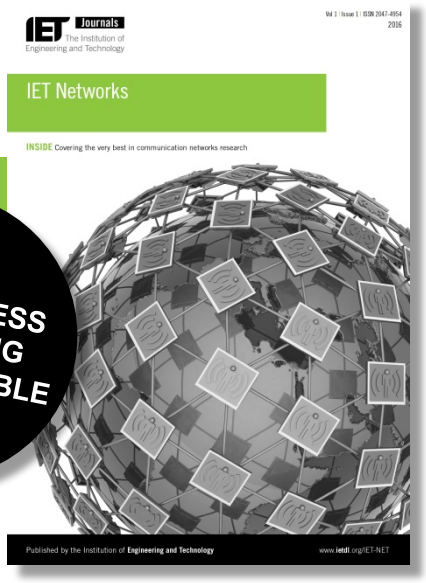
IET Journals
The Institution of Engineering and Technology

IET *Networks*
Call for Papers



OPEN ACCESS PUBLISHING NOW AVAILABLE

SPECIAL ISSUE ON:
Security Architecture and Technologies for 5G

Recently, fifth-generation (5G) communication has attracted attention from academics, industry and government all over the world. 5G drives many new requirements for different network capabilities. However, security is undoubtedly one of the most important cornerstones for 5G development and applications. 5G security challenges have many aspects. Firstly, secure network architectures are required as the basis for 5G to support a huge number of connected devices. Secondly, 5G will migrate or bring in many promising network technologies, such as Software Defined Networking (SDN), Network Functions Virtualization (NFV), Information Centric Network (ICN), Device to Device (D2D), Network Slicing, Cloud Computing/Fog Computing and so on. These technologies should also provide security guarantees for 5G architecture. Thirdly, more and more user data and network traffic will be carried over the 5G network. Big data security should be considered to protect these data, including data privacy, data sources, data analytics and so on. Fourthly, 5G will promote many interesting applications which also require secure support, such as vehicular networks, Internet of Energy (IoE) and VR/AR. We call for survey and research papers in the scope of 5G security. We aim to provide a platform for researchers to further explore the security issues, technologies, and architecture for 5G networks.

Topics of interest include, but are not limited to:

- Innovative security architecture for 5G networks
- 5G core network security
- Secure network slicing for 5G
- Access control security for 5G networks
- Security protocols for 5G networks
- DDoS protection in 5G
- SDN security in 5G networks
- Orchestration of NFV/SDN security in 5G networks
- ICN security
- Device to Device (D2D) security
- Terminal and edge computing security
- Malware attack detection and prevention techniques
- Information sharing and data protection in 5G networks
- Security management in heterogeneous 5G networks
- Big data security in 5G networks
- Securing big data environments
- Big data sources protection
- Big data analytics safeguarding
- Cloud technologies security
- Security for new service delivery models
- Mechanisms to enforce privacy and trust
- Trust models for 5G services
- Security for 5G applications, i.e., vehicular networks, Internet of Energy and VR/AR

All papers must be submitted through the journal's Manuscript Central system:
http://mc.manuscriptcentral.com/iet-net

Publication Schedule:

Submission Deadline:
30 June 2017
Publication:
May 2018

Guest Editors:

Hongke Zhang
Beijing Jiaotong University, China
E: dr.wei.quan@ieee.org;
hkzhang@bjtu.edu.cn

Shui Yu
Deakin University, Australia
E: shui.yu@deakin.edu.au

Chi-Yuan Chen
National Ilan University, Taiwan
E: chiyuan.chen@ieee.org

Wei Quan
Beijing Jiaotong University, China
E: weiquan@bjtu.edu.cn