SPECIAL ISSUE on
Emerging Trends and Recent Advances in Communication Networks Security

GUEST EDITORS
Zhengyi Chai, Tiangong University, China
Mohsen Guizani, Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, UAE

DESCRIPTION
This special issue in Open Computer Science focuses on Emerging Trends and Recent Advances in Communication Networks Security.

The Internet, as the backbone of communication between objects, people, companies, and management, has become a powerful integration platform. The platform provides access to multiple hardware and virtualized resources (servers, networks, storage, applications, connected objects) from cloud computing to IoT infrastructure. It has played an important role in promoting the progress of science and technology. However, interconnecting systems through networks, access to information, different computer technologies, and a combination of all these aspects puts both academic and industrial infrastructure at serious risk. Network systems are subject to various security attacks, such as distributed denial of service, man-in-the-middle attacks, network injection, and malware attacks. The consequences of these attacks are almost always invasive and destructive to computerized systems, and can be fatal if the attack is carried out in the field of smart health devices. Therefore, effective security-based solutions need to be researched to eliminate these risks or counter attacks. Today, intelligent systems for cybersecurity cover a wide range of areas, including smart cities, cyber-physical systems and critical infrastructure, security of vehicles and implantable medical devices, malware research, cryptography, biometrics, human-computer interaction security, secure wireless sensor networks, RFID security, early detection and intervention, and privacy. This special issue will focus on emerging trends and recent developments in communication networks security management. Topics of interest include but are not limited to the following:

- Advances in blockchain and cybersecurity for smart city applications
- Secure and resilient communication and control architecture
- Cryptography, key management, authorization and access control
- Security, reliability and privacy of communication networks
- Security threat and vulnerability assessment and measurement
- Analytics and big data for security management
- Applying next-generation technologies to the security of IoT, cloud computing, wireless and mobile networks
- Configuration and orchestration of security mechanisms
- Security policy specification and management in communication networks
- Complex network algorithms for network security
- Communication network security using artificial intelligence

degruyter.com/comp
Authors are requested to submit their full revised papers complying the general scope of the journal. The submitted papers will undergo the standard peer-review process before they can be accepted. Notification of acceptance will be communicated as we progress with the review process.

HOW TO SUBMIT

Before submission authors should carefully read the Instruction for Authors, available online at: https://www.degruyter.com/publication/journal_key/COMP/downloadAsset/COMP_Instruction%20for%20Authors.pdf

Manuscripts can be written in TeX, LaTeX (strongly recommended) - the journal’s LaTeX template. Please note that we do not accept papers in Plain TEX format. Text files can be also submitted as standard DOCUMENT (.DOC) which is acceptable if the submission in LaTeX is not possible. For an initial submission, the authors are strongly advised to upload their entire manuscript, including tables and figures, as a single PDF file.

All submissions to the Special Issue must be made electronically via online submission system Editorial Manager: http://www.editorialmanager.com/opencs/

All manuscripts will undergo the standard peer-review process (single blind, at least two independent reviewers). When entering your submission via online submission system please choose the option “Special Issue on Emerging Trends and Recent Advances in Communication Networks Security”.

Submission of a manuscript implies that the work described has not been published before and it is not under consideration for publication anywhere else.

The deadline for submissions is December 31, 2022, but individual papers will be reviewed and published online on an ongoing basis.

Contributors to the Special Issue will benefit from:

- critical peer-review
- no space constraints
- quick online publication upon completing the publishing process (continuous publication model)
- better visibility due to Open Access – free, unrestricted and permanent access to all the content
- liberal policies on copyrights (authors retain copyrights) and on self-archiving (no embargo periods)
- promotion of published papers to readers and citers
- long-term preservation – content archiving with Portico

We are looking forward to your submission!

In case of any questions please contact Editorial Office (opencomputerscience@degruyter.com)