International Journal of
Network Management

Special Issue of the International Journal on Network Management (IJNM) on

Security for Emerging Open Networking Technologies

CALL FOR PAPERS

(Publication: September 2017)

Scope of the Special Issue

Emerging open networking technologies and paradigms, such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), and programmable networks, are reshaping the way networks are designed, deployed, and managed. The benefits are manifold, including an unprecedented flexibility for network operation and management, and a favorable environment for delivering innovative network applications and services. However, this paradigm shift brings a multitude of security challenges that have to be addressed in order to provide secure, trustworthy, and privacy-preserving data communication and network services. Addressing these challenges may require not only revisiting existing solutions (e.g., for intrusion detection, privacy preserving, and resilience against attacks), but also designing novel security and resilience schemes tailored to the specific design of open networking technologies and infrastructures.

This special issue of the *International Journal of Network Management* aims to put focus on the state-of-the-art advances, contributions and solutions to security-related challenges arising with emergent open networking technologies. We seek new and unpublished contributions addressing issues in the **Security for Emerging Open Network Technologies** including, but not limited to:

- Secure and resilient design and deployment of open networking technologies
- Privacy-preserving solutions
- Security models and threats
- Security and privacy properties and policies
- Verification and enforcement of security properties
- Trust and identity management
- NFV-based security functions and services
- Security of software-defined infrastructures, protocols and interfaces
- Security and availability management
- Security for Internet of Things
- Intrusion detection, tolerance, and prevention
- Network forensics and auditing
- Detection and resilience against large-scale distributed attacks
- Security of programmable components
- Security-related business and legal aspects
- Security challenges and trends for open networking technologies

Submission Guidelines

Authors must submit their papers in PDF format to http://mc.manuscriptcentral.com/nem. Submissions should not exceed 20 pages (double-space). Author instructions are available here and the LaTeX template can be found here. All submissions will be peer-reviewed. In case of acceptance, the camera-ready version has to take into account reviewers' comments and must follow the template's requirements.

Important Deadlines

Submission Deadline:	*March 1, 2017*
Author Notification:	*May 15, 2017*
Revision Deadline:	*July 1, 2017*
Final Decision:	*August 1, 2017*
Camera Ready:	*August 15, 2017*
Publication:	*September 1, 2017*

Guest Editors

Carol Fung
Virginia Commonwealth University, USA
cfung@vcu.edu

Jérôme François
Inria Nancy Grand Est, France
jerome.francois@inria.fr

Weverton Cordeiro
Federal University of Rio Grande do Sul, Brazil
weverton.cordeiro@inf.ufrgs.br

Mohamed Faten Zhani
École de Technologie Supérieure, Canada
mfzhani@etsmtl.ca