Security and Communication Networks

# Special Issue on
# Security Measurements of Cyber Networks

WILEY | Hindawi

CALL FOR PAPERS

Cyber networks facilitate and expedite the development of information and communication technologies and digital economies. Indeed, cyber networks are becoming fundamental to many aspects of our lives, both working and social. However, as networks become larger, heterogeneous, and pluralistic, evaluation of the security of cyber networks becomes increasingly difficult. Attacks and intrusions upon cyber networks can have serious impacts from personal-level to national-level security. As such, there is a rising need to understand, and measure, network security for a range of requirements and standards and in the context of different network scenarios. Although many prior studies have been dedicated to network intrusion detection, malware detection, and security threat defense, a generally accepted security measurement framework is still absent. Such a system is urgently required for the rapid identification of security holes, assessment of potential threats, and implementation of efficient fixes.

Several pertinent questions exist for security measurement theories and methods in terms of security-related data collection, composition, analytics, and processing. This is especially true for detecting security threats and measuring cyber network security in a quantified, precise, and efficient manner: (i) How may we adaptively collect related data for security measurement in the context of large-scale heterogeneous networks, in a generic and pervasive way? (ii) How may we compose and fuse collected big data for economic data storage and transmission, as well as efficient data processing, for precise security threat detection and judgment? (iii) How may we protect valuable data, preserve privacy, and effectively control its access? (iv) How may we aggregate and mine security-related data to finally measure the security of the whole network in a quantified manner? These open and interesting issues are now attracting significant attention.

This Special Issue will bring together recent advances on security data collection and analysis; detection of malware, virus, and network intrusion; and network system protection, in the context of network security assessment and measurement. It welcomes original and innovative research on theories, methodologies, schemes, algorithms, and tools related to security measurements of cyber networks, from academia, industry, and government. Inquiries about potential review articles should be directed to the Special Issue Editor in Chief.

Potential topics include but are not limited to the following:

- Theories, frameworks, and tools for security measurement
- Network security data collection, transmission, processing, and analysis
- Network security data fusion, composition, and mining
- Big data security and trust
- Malware, virus, and intrusion detection
- Network system protection
- Security data access control
- Security in heterogeneous networks and complex systems
- Cyber hacking and protection
- Network security simulation and toolkits
- Standards for network security measurement
- Assurance methods for network security
- Network data trust management

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/smcn/.

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

**Special Issue Editor in Chief**
Zheng Yan, Xidian University, Xi'an, China; Aalto University, Aalto, Finland
*zheng.yan@aalto.fi*

**Guest Editors**
Yuqing Zhang, University of Chinese Academy of Sciences, Beijing, China
*zhangyq@nipc.org.cn*

Raymond Choo, University of Texas at San Antonio, San Antonio, USA
*raymond.choo@utsa.edu*

Yang Xiang, Deakin University, Melbourne, Australia
*yxiang@swin.edu.au*

**Submission Deadline**
Friday, 12 January 2018

**Publication Date**
June 2018