

CALL FOR PAPERS

Call for Papers for Special Issue on Next Generation Communication and Network Security

Mobile Internet and Computer Communication has become a part of our daily life. People are using mobile Internet and network communication applications such as YouTube, Twitter, Facebook, as well as mobile web and e-mail via mobile communication devices such as smartphones, tablet PCs and embedded mobile devices. Nowadays, cloud computing services that store important and proprietary information on remote machines that are accessible through various networks and mobile internet environments, are also utilized. While such applications may help businesses and also make personal services more efficient, they are vulnerable to attacks, which include various communication and network infringement, system violation, stealing data and obstructing the operations of a business or a person. In addition, the environment of the Next Generation Communications and Networks has raised many issues on heterogeneous communications system and network security, which are vulnerable to various attacks.

This Special Issue will be published by Wiley's Security and Communication Networks (SCN) Journal ([http://onlinelibrary.wiley.com/journal/10.1002/\(ISSN\)1939-0122](http://onlinelibrary.wiley.com/journal/10.1002/(ISSN)1939-0122)) and aims to provide a forum for allowing researchers to report and exchange the current research findings focusing on analysis, design, and applications of **Next Generation Communication and Network Security** in various computer communications systems and networks.

Topics of Interest

This special issue on Next Generation Communication and Network Security in SCN includes (but not limited to) the following topics:

- Trustworthy infrastructures and services for cloud computing;
- Smart mobile device connectivity security vulnerabilities and threats;
- Advanced DDoS detection and mitigation;
- Mobile Web 2.0 and Cross Script attacks;
- User generated content protection;
- Ubiquitous surveillance and privacy-enhancing technologies;
- Cloud-based authentication, single-sign-on, authorization using mobile devices or access control for social networks;
- Security architecture for next generation convergence network;
- Machine-to-machine network security enhancement;
- Advanced Firewalls and intrusion detection/prevention systems;
- Intelligent Active and adaptive defense systems;
- Network Generation Network forensics and fraud detection;
- Security and Privacy models for Pervasive Information Systems.

Instructions for Authors and Review Process

Papers must represent high-quality and previously unpublished works. Original research papers are solicited in all areas of concern (as listed above). All topic-related original submissions will be peer reviewed by at least three experts working in the areas. The guidelines for prospective authors can be found online at [http://onlinelibrary.wiley.com/journal/10.1002/\(ISSN\)1939-0122/homepage/ForAuthors.html](http://onlinelibrary.wiley.com/journal/10.1002/(ISSN)1939-0122/homepage/ForAuthors.html). Prospective authors should submit their papers online at <http://mc.manuscriptcentral.com/scn> and no email submissions will be accepted. When submitting the papers, the authors should make sure to choose "Manuscript type" as "Special Issue," and enter "Running Head" and "Special Issue title" as "SCN-SI-30" and "NGCom-NetSec," respectively, in the SCN Journal Manuscript Central website.

Important Dates

Submission Deadline: 31 August 2011
 Acceptance Notification: 31 October 2011
 Final Papers Due: 15 December 2011
 Publication: 2012

Guest Editors

Taeshik Shon
 Samsung Electronics, Korea
 E-mail: 743zh2k@gmail.com
 Costas Lambrinouidakis
 University of Piraeus, Greece
 Email: clam@unipi.gr
 Xiaobo Zhou
 University of Colorado at Colorado Springs, USA
 Email: zbo@cs.uccs.edu