

Call for Papers: Security in Mobile Wireless Networks

Security has become a primary concern in order to provide protected communication in mobile networks. Unlike the wired networks, the unique characteristics of mobile networks pose a number of non-trivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, highly dynamic network topology and absence of a trusted infrastructure. Ubiquitous roaming impacts on a radio access system by requiring that it supports handover between neighbouring cells and different networks. Also, mobile networks are more exposed to interferences than wired networks. There are several components that contribute to this: adjacent channels, co-channels, Doppler shifts, multipath and fading. This Special Issue (SI) aims to identify and explore the different issues and challenges related to security aspects in mobile networks. What are the impacts (benefits or inconvenience) of mobility on security? What are the appropriate mobility models to have a good level of security? Are Classical IDS approaches appropriate for mobile environments? How can be managed security when Mobility pattern and/or behaviour prediction?

Topics of Interest

The complete security solution should span both layers, and encompass all three security components of prevention, detection and reaction. Topics of interest include, but are not limited to, the following as they relate to mobile networks:

- Secure mobile PHY/MAC protocols.
- Secure mobile routing protocols.
- Security under resource constraints (e.g. energy, bandwidth, memory and computation constraints).
- Performance and security trade-offs in mobile networks.
- Secure roaming across administrative domains.
- Key management in mobile scenarios.
- Cryptographic protocols.
- Authentication and access control in mobile networks.
- Intrusion detection and tolerance in mobile network.
- Trust establishment, negotiation and management.
- Secure mobile location services.
- Secure clock distribution.
- Privacy and anonymity.
- Denial of service in mobile networks.
- Prevention of traffic analysis.

Instructions for Authors and Review Process

Papers must represent high-quality and previously unpublished work. Original research papers are solicited in all areas of Wireless and Networks Security. All submissions will be peer reviewed by at least three experts working in the areas.

The guidelines for prospective authors can be found on-line (<http://www.interscience.wiley.com/journal/security>). Prospective authors should submit their papers online at <http://mc.manuscriptcentral.com/scn>. When submitting the papers, the authors should make sure to choose the Manuscript type as 'Special Issue', and enter the 'Running Head' and the 'Special Issue title' as 'SCN-SI-007' and 'Secure Mobile', respectively.

Important Dates

Papers Submission Deadline: 30 December 2008

Notification of Decisions: 28 February 2009

Final Manuscript Due: 31 March 2009

Guest Editors:

Abderrahim Benslimane,
University of Avignon, France
E-mail: abderrahim.benslimane@univ-avignon.fr

Chadi Assi, Concordia University, Montreal, Canada
E-mail: assi@ciise.concordia.ca

Stamatios V. Kartalopoulos, University of
Oklahoma, USA
E-mail: kartalopoulos@ou.edu

Fred Nen-Fu Huang,
National Tsing Hua University, Taiwan
E-mail: nfhuang@cs.nthu.edu.tw