Journal of Cyber Security and Mobility

Special Issue on Next Generation Mobility Network Security

http://riverpublishers.com/journal/speical_isseue.php?si=5

CALL FOR PAPERS

The Long Term Evolution (LTE) is the newly adopted standard technology to offer enhanced capacity and coverage for mobility networks, providing advanced multimedia services beyond traditional voice and short messaging traffic for billions of users. This new cellular communication system introduces a substantial redesign of the network architecture resulting in the new eUTRAN (Enhanced Universal Terrestrial Radio Access Network) and the EPC (Enhanced Packet Core). In this context, the LTE Radio Access Network (RAN) is built upon a redesigned physical layer and based on an Orthogonal Frequency Division Multiple Access (OFDMA) modulation, features robust performance in challenging multipath environments and substantially improves capacity. Moreover, a new all-IP core architecture is designed to be more flexible and flatter.

In parallel, the cyber-security landscape has changed drastically over the last few years. It is now characterized by large scale security threats such as massive Distributed Denial of Service Attacks (DDoS), the advent of the Advanced Persistent Threat (APT) and the surge of mobile malware and fraud. These new threats illustrate the importance of strengthening the resiliency of mobility networks against security attacks, ensuring this way full mobility network availability. In this context, however, the scale of the threat is not the key element anymore and traditionally overlooked low range threats, such as radio jamming, should also be included in security studies.

This special issue of the Journal of Cyber Security and Mobility addresses research advances in mobility threats and new security applications/architectures for next generation mobility networks. The main topics of interest of this issue include, but are not limited to, the following:

- LTE RAN security.
- OFDM/OFDMA radio jamming.
- Secure wireless communications under malicious interference/jamming.
- LTE EPC security.
- malware/impact on LTE RAN/EPC.
- Femtocell security threats.
- Detection of attacks against mobility networks.
- Self Organizing Networks (SON) security applications.
- WiFi-cellular interoperability threats and security.
- Mobile device baseband security.

Authors are encouraged to submit original work that has neither appeared in, nor is under consideration for publication in other venues.

IMPORTANT DATES

1) Paper submissions due: March 1st, 2014
2) First review round notifications: March 15th, 2014
3) Revised version due: April 15th, 2014
4) Second review round notifications: May 1st, 2014
5) Final version due: June 1st, 2014
6) Publication: July 2014

AUTHOR INSTRUCTIONS

Please refer to the publisher's website for submission, templates and guideline for manuscript preparation.

- Submission: http://riverpublishers.com/journal/login.php
- LaTeX and Word templates: http://riverpublishers.com/authors.php

Please contact Roger Piqueras Jover $roger[dot]jover[at]att[dot]com$ for questions regarding this special issue.