

IEEE ICC 2014 Workshop on *Wireless Physical Layer Security* (WPLS)

Organizing Committee

Eduard Jorswieck, TU Dresden
Zhu Han, Univ. of Houston
Walid Saad, Univ. of Miami
Xiangyun Zhou, ANU

Steering Committee

Matthieu Bloch, Georgia Tech
Ashish Khisti, Univ. of Toronto

Technical Program Committee

Veronica Belmega, ENSEA
Arsenia Chorti, Princeton
Zhiguo Ding, Newcastle Univ.
Dennis Goeckel, UMASS
Xiang He, Microsoft
Y.-W. Peter Hong, NTHU
Jing Huang, Broadcom
Lifeng Lai, WPI
Ingmar Land, UNISA
Jemin Lee, SUTD
Jiangyuan Li, Rutgers Univ.
Ming Li, Utah State Univ.
Zhiwei Li, UC Berkeley
Shih-Chun Lin, NTUST
Jia Liu, Ohio State Univ.
Matthew McKay, HKUST
Behrouz Maham, Univ. of Tehran
Chandra Murthy, IIS
Amitav Mukherjee, Hitachi
Francesco Renna, Univ. of Porto
Aydin Sezgin, RU Bochum
Mikael Skoglund, KTH
Lingyang Song, Peking Univ.
Meixia Tao, SJTU
Xianbin Wang, UWO
Nan Yang, UNSW

Important Dates

Paper Submission: 15 Dec 2013
Acc. Notification: 20 Feb 2014
Camera Ready: 15 Mar 2014
Workshop: 10 Jun 2014

Call for Paper

The emergence of large-scale, dynamic, and decentralized wireless networks imposes new challenges on classical security measures such as cryptography. To this end, researchers have been seeking for new solutions to complement cryptography and significantly improve the overall security of wireless communication networks. One of the most promising ideas is to exploit the physical layer characteristics of the wireless channel such as fading or noise, which are traditionally seen as impediments, for improving the confidentiality of the legitimate communication links. This emerging security technique, known as physical layer security, has drawn considerable attention in the past few years. Beyond securing wireless transmissions of confidential information, physical layer security solutions have been also exploited to provide or enhance the authentication and privacy of legitimate wireless users.

This workshop is part of the 2014 IEEE International Conference on Communications (ICC) to be held in Sydney, Australia between 10 and 14 June. It is expected to bring together academic and industrial researchers in an effort to identify and discuss the major technical challenges and recent results related to physical layer security in wireless networks. Topics of interest include but are not limited to the following:

- Secrecy capacity and rate-equivocation of wireless channels.
- Practical code design for physical layer security.
- Advanced signal processing and space-time secure transmission techniques.
- Secure relaying and cooperative transmission techniques.
- Secure cross-layer design techniques.
- Game theory for wireless physical layer security.
- Secrecy graph and stochastic geometry approaches.
- Advanced physical layer security attacks (e.g., smart eavesdropping or jamming) and their countermeasures.
- Secret key generation and agreement.
- Physical layer authentication.
- Physical layer privacy protection.
- Experimental results on enhancing security at the physical layer.

The workshop will feature the following **keynote speakers**:

- Prof. Aylin Yener
- Prof. João Barros

The workshop accepts only novel, previously unpublished papers. All submissions should be written in English with a maximum paper length of six (6) printed pages (10-point font) including figures without incurring additional page charges (maximum 1 additional page with over-length page charge if accepted) <http://www.ieee-icc.org/authguide.html>

Workshop paper submission:

<https://edas.info/newPaper.php?c=16325&track=44395>