Call for Papers
IEEE Journal on Selected Areas in Communications

"Signal Processing Techniques for Wireless Physical Layer Security"

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 sought novel information theoretic techniques that can secure wireless networks without the need for secret keys. One of the most promising ideas is to exploit the wireless channel physical layer characteristics such as fading or noise, which are traditionally seen as impediments, for improving the reliability of wireless transmission against eavesdropping attacks. Physical layer security has emerged as a key technique for providing trustworthy and reliable future wireless networks and has witnessed a significant growth in the past few years.

To this end, this special issue aims to gather cutting-edge contributions from academia and industry that address and show the latest results on securing wireless networks at the physical layer. This special issue has a particular emphasis on advanced signal processing, information theoretic, and communication techniques that can make the vision of secret wireless transmission using the physical layer characteristics of the wireless channel a reality. Suitable topics for this special issue include, but are not limited to, the following areas:

- Advanced beamforming and other multi-antenna techniques.
- Secure relaying and cooperative transmission techniques.
- Dynamic resource allocation for physical layer security in various communication scenarios which include (but are not limited to) securing multiuser channels (multiple access, broadcast, relay, interference) , dynamic spectrum access, and spectrum-sharing based cognitive radio channels.
- Secure network coding / Byzantine attacks.
- Signal processing techniques for advanced security primitives such as authentication, bit commitment, oblivious transfer, secret sharing, etc.
- Secret key generation from fading channels via public discussion/common randomness.
- Cross-layer design techniques that combine physical layer security and cryptographic algorithms.
- Attacker optimization: jamming and eavesdropping.
- Game theory for wireless physical layer security.
- ▪ Wireless physical layer techniques for enhanced location and signal privacy.
- Experimental results on signal processing for enhancing security at the physical layer.

Prospective authors should prepare their manuscripts in accordance with the IEEE JSAC format described at http://jsac.ucsd.edu/Guidelines/info.html. Authors should submit a PDF version of their complete manuscript to EDAS: http://edas.info. The timetable is as follows:

- Manuscript submission due: August 15, 2012
- First-round reviews due: January 10, 2013
- Acceptance notification/second reviews due: April 10, 2013
- Final manuscript due: May 1, 2013

Guest Editors:
Lead GE: Walid Saad (University of Miami), email: walid@miami.edu
Eduard Jorswieck (TU Dresden), email: Eduard.Jorswieck@tu-dresden.de
Lifeng Lai (University of Arkansas, Little Rock), email: lxlai@ualr.edu

Wing-Kin (Ken) Ma (the Chinese University at Hong Kong), email: wkma@ee.cuhk.edu.hk

H. Vincent Poor (Princeton University), email: poor@princeton.edu
A. Lee Swindlehurst (University of California, Irvine), email: swindle@uci.edu