Call for Papers
IEEE Transactions on Information Forensics and Security
Special Issue on Using the Physical Layer for Securing the Next Generation of Communication Systems

Communication technologies are undergoing a renaissance as there is a movement to explore new, clean slate approaches for building communication networks. Although future Internet efforts promise to bring new perspectives on protocol designs for high-bandwidth, access-anything from anywhere services, ensuring that these new communication systems are secure will also require a re-examination of how we build secure communication infrastructures. Traditional approaches to building and securing networks are tied tightly to the concept of protocol layer separation. For network design, routing is typically considered separately from link layer functions, which are considered independently of transport layer phenomena or even the applications that utilize such functions. Similarly, in the security arena, MAC-layer security solutions (e.g. WPA2 for 802.11 devices) are typically considered as point-solutions to address threats facing the link layer, while routing and transport layer security issues are dealt with in distinct, non-integrated protocols like IPSEC and TLS. The inherent protocol separation involved in security solutions is only further highlighted by the fact that the physical layer is generally absent from consideration.

This special issue seeks to provide a venue for ongoing research area in physical layer security across all variety of communication media, ranging from wireless networks at the edge to optical backbones at the core of the network. The scope of this special issue will be interdisciplinary, involving contributions from experts in the areas of cryptography, computer security, information theory, signal processing, communications theory, and propagation theory. In particular, the areas of interest include, but are not limited to, the following:

- Information-theoretic formulations for confidentiality and authentication
- Generalizations of Wyner's wiretap problem to wireless and optical systems
- Physical layer techniques for disseminating information
- Techniques to extract secret keys from channel state information
- Secrecy of MIMO and multiple-access channels
- Physical layer methods for detecting and thwarting spoofing and Sybil attacks
- Techniques to achieve covert or stealthy communication at the physical layer
- Quantum cryptography
- Modulation recognition and forensics
- Security and trustworthiness in cooperative communication
- Fast encryption using physical layer properties
- Attacks and threat analyses targeted at subverting physical layer communications

Manuscript Submission: Manuscripts are to be submitted according to the Information for Authors at http://www.signalprocessingsociety.org/publications/periodicals/forensics/forensics-authors-info/, using the IEEE online manuscript system, Manuscript Central. Papers must not have appeared elsewhere, and must not be in review elsewhere. All papers will be reviewed in accordance with the procedures of the IEEE Transactions. If necessary, the submission date can be moved later based on when the proposal is approved.

Submission deadline: **September 15, 2010**
First Review: December 1, 2010
Revisions Due: January 30, 2011
Final Decision: February 15, 2011
Final manuscript due: March 1,2011
Tentative publication date: June 1, 2011

Guest Editors:

Vincent Poor, Princeton University, (Email: poor@princeton.edu)
Wade Trappe, WINLAB, Rutgers University, (Email: trappe@winlab.rutgers.edu)
Aylin Yener, Pennsylvania State University, (Email: yener@engr.psu.edu)
Hisato Iwai, Doshisha University, Japan, (Email: iwai@mail.doshisha.ac.jp)
Joao Barros, University of Porto, Portugal, (Emal: jbarros@fe.up.pt)
Paul Prucnal, Princeton University, (Email: prucnal@princeton.edu)