IEEE VTS Connecting the Mobile World

VTC2015-Fall BOSTON Innovation Meets Tradition

Westin Boston Waterfront Hotel ◆ 6 - 9 September 2015

Second International Workshop on Cognitive Radio and Electromagnetic Spectrum Security

Call for Papers

The autonomous manner in which cognitive radio systems make decisions for a wide range of wireless communications and networking functions, as well as its total dependency on environmental sensory information in order to reach these decisions, makes this technology highly susceptible to attack by a malicious, external entity. At the same time, research activities into identifying potential vulnerabilities in cognitive radio technology and developing robust countermeasures to mitigate these attacks is only now beginning to increase. The purpose of this workshop is to bring together members of the cognitive radio and electromagentic spectrum security community from around the world in order for them to share the latest research findings in this emerging and critical area, as well as exchange ideas and foster research collaborations, in order to further advance the state-of-the-art in security techniques, architectures, and algorithms for cognitive radio communications and networks. Topics of interests include (but are not limited to) the following:

- General security architecture for CR networks
- Cross-layer security design of CR networks
- Secure routing in multi-hop CR networks
- Physical layer security for CR networks
- Geo-location for security in CR networks
- Privacy protection in CR networks
- Security issues for database-based CR networks
- Security in CR networks for the smart grid
- Intrusion detection systems in CR networks
- Truthful Spectrum Auctions
- Authentication methods of primary users
- Primary user emulation attacks and countermeasures
- Defending and mitigating jamming-based DoS attacks in CR networks
- Defending against energy depletion attacks in resource-constrained CR networks
- Attack modeling, prevention, mitigation, and defense in CR systems
- Spectrum sensing data falsification and countermeasures
- Spectrum misusage and selfish misbehaviors and countermeasures
- Unauthorized use of spectrum bands and countermeasures
- Methods for detecting, isolating and expelling misbehaving cognitive nodes
- Eavesdropping attack modeling and analysis in cognitive radio
- Security policies, standards and regulations f or CR networks
- Implementation and testbed for security evaluation in CR systems
- Information-theoretical secrecy capacity of cognitive transmissions

Extended Abstract Submissions:

All 2-page extended abstract submissions must be written in English and must be formatted in standard IEEE 2-column format. The mandatory IEEE template in Microsoft Word and LaTeX format can be found at: http://www.ieee.org/conferences_events/conferences/publishing/templates.html

Only Adobe PDF files will be accepted for the review process. All submissions must be made through the peer review system located at the following URL: https://vtc2015fall.trackchair.com/track/1408

Workshop Chairs:

Xiuzhen (Susan) Cheng, George Washington University, cheng@gwu.edu
Yalin E. Sagduyu, Intelligent Automation Inc., ysagduyu@i-a-i.com
Yi Shi, Intelligent Automation Inc., yshi@i-a-i.com
Shabnam Sodagari, University of Maryland, shabnam@ieee.org
Alexander M. Wyglinski, Worcester Polytechnic Institute, alexw@wpi.edu

Important Dates:

Extended Abstract Submission:
11 April 2015
Acceptance Notification:
11 May 2015
Camera-Ready Papers Submission:
8 June 2015

www.vtc2015fall.org

IEEE