CRESS 2014

The First International Workshop on Cognitive Radio and Electromagnetic Spectrum Security

In conjunction with 2014 IEEE Conference on Communications and Network Security (IEEE CNS 2014)

29 October 2014, San Francisco, CA, USA

Call for Papers

Cognitive radio enables access to broader pools of spectrum and more efficient utilization of current wireless resources and thus plays a key role for the next generation of mobile broadband. Legacy static spectrum allocation, although simple, poses a major obstacle for efficient use of limited wireless resources across time, space, and frequency. This challenge has promoted substantial research and development into cognitive radio technologies with network-level perception, learning, adaptation, and optimization for efficient spectrum utilization. In fact, the latest advances in cognitive radio technology have already started to appear in numerous military and public safety applications, connected vehicle prototypes, and cellular telephony deployments such as 4G LTE-Advanced, e.g., Self-Organizing Network (SON) engines. However, the autonomous manner in which cognitive radio systems make decisions fora 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. Consequently, 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
- 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
- Primary user emulation attacks and countermeasures
- Authentication methods of primary users
- 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 for CR networks
- Implementation and testbed for security evaluation in CR systems
- Information-theoretical secrecy capacity of cognitive transmissions
- 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

Workshop Chairs

Xiuzhen (Susan) Cheng, George Washington University
Yalin E. Sagduyu, Intelligent Automation Inc.
Yi Shi, Intelligent Automation Inc.
Shabnam Sodagari, University of Maryland
Alexander M. Wyglinski, Worcester Polytechnic Institute

Important Dates

Paper Submission Deadline: 25 June 2014
Acceptance Notification: 5 July 2014
Camera-Ready Paper Due: 11 July 2014

cress.ece.wpi.edu