



CALL FOR PAPERS

The rapid growth in computation, cognitive networking, dynamic spectrum access, spectrum agility, and hardware miniaturization technologies has led to a major revolution in the wireless sensor networking landscape in recent times. In particular, the introduction of wireless sensor nodes with cognitive radio technologies and dynamic spectrum access capabilities can help to improve spectrum utilization and optimize the dynamic bandwidth and quality-of-service (QoS) requirements of application-specific wireless sensor networks (WSNs). Cognitive radio enabled WSNs require research from multidisciplinary fields including understanding physical systems' operation; how they can be networked in a cognitive and wireless manner; and how these systems can learn and cooperate with one another.

Additionally, the "open" philosophy of cognitive radio WSN paradigm also makes WSNs susceptible to attacks by smart malicious adversaries that could even render the legitimate WSNs resourceless. There are several ways in which the operations of WSNs can be jeopardized. Cognitive disruption through malicious channel fragmentation/aggregation/bonding, Sybil-enabled emulation attacks, or spectrum stealing through induced attacks is just some of the unique mechanisms that can severely cripple the WSNs. In order to defend against these kinds of attacks, it is important to understand how various attacks/attackers work in the first place and thereafter investigate defense mechanisms. The broad diversity of skills required makes this both a challenging and an exciting field of study.

Keeping the above two related challenging issues in emphasis, this special issue will focus on identifying novel and state-of-the-art solutions to problems related to *cognitive WSNs and their survivability*. The goal of this special issue is to bring together researchers and practitioners from academia, industry, and government agencies to focus on understanding modern WSN challenges, security threats, and countermeasures and establishing original contributions and new collaborations in these areas.

Potential topics include, but are not limited to:

- ▶ Robust cognitive radio technology, protocols, and architecture for wireless sensor networks
- ▶ Cross-layer design of cognitive protocols
- ▶ In-building sensing for smart grids
- ▶ Robust and real-time monitoring such as spectrum monitoring and network status monitoring
- ▶ Machine-type communications (MTC) in wireless sensor networks
- ▶ Dynamic spectrum access paradigm in wireless sensor networks
- ▶ Survivability in wireless sensor networks through self-healing
- ▶ Vulnerabilities of sensor integration over commercial systems
- ▶ Learning techniques in adaptive defense
- ▶ Secure cognitive wireless sensor networking in healthcare and for socially assistive functionalities
- ▶ Resilient deployment strategies and self-configuration mechanisms for cognitive WSNs
- ▶ Integration of smart wireless sensor networks with traditional networking solutions and standards
- ▶ Testbed experiments and case studies

Authors can submit their manuscripts via the Manuscript Tracking System at <http://mts.hindawi.com/submit/journals/ijdsn/cre/>.

Lead Guest Editor

Shamik Sengupta, University of Nevada,
Reno, USA
ssengupta@unr.edu

Guest Editors

Walid Saad, Virginia Tech, Virginia,
USA
walids@vt.edu

Abhishek Roy, Samsung Electronics Co.,
Ltd., Seoul, Republic of Korea
abhishek.roy@samsung.com

Manuscript Due

Friday, 17 April 2015

First Round of Reviews

Friday, 10 July 2015

Publication Date

Friday, 4 September 2015