Tentative Outline

Thematic Issue Proposal for Recent Advances in Electrical and Electronic Engineering

Secure, Resilient and Green Computing in Wireless Sensor Networks

Guest Editors:

Dr. Rajiv Kumar, Jaypee University of Information Technology, H.P. India.
Dr. Hemraj Saini, Jaypee University of Information Technology, H.P. India.

Aim and Scope:

The previous decades have seen the progression of Wireless Sensor Networks (WSNs) in both scholarly and modern networks. In a WSN, a substantial number of sensor hubs are conveyed and organized to screen or overview focused on territory, with the end goal that the intrigued information can be sensed, processed, stored and collected. Through WSNs, we can connect the physical word and the cyber space, which creates the establishment for growing new smart applications. Numerous potential uses of WSNs have been abused in the fields of natural designing, social insurance, industry, military applications, keen home, and green structures and so on.

To empower the inescapable organization of WSNs, the greatest hindrance is the inconsistency between the different functionalities requested by applications and the restricted vitality supply for sensor hubs. Moreover, because of distributed nature of these networks and their organization in remote zones, these networks are helpless against various security dangers that can antagonistically influence their legitimate working. Securing the WSN needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar or more hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively.

Wireless sensor networks (WSNs) needs better resilience as they may be deployed in failure-prone environments, and WSNs nodes easily fail due to unreliable wireless connections, malicious attacks and resource-constrained features.

Therefore, in this special issue, we look at WSNs, mainly from the perspective of secure, resilient and green computing. Topics of primary interest are centered around secure, resilient and green computing in WSNs, including but not being limited to:

Keywords: Wireless Sensor Network, Green Routing, Resiliency, Green Computing, Denial of Service Attack, Reliable Connection, Distributed Architecture, Secure Computing, Survivability, Routing, Link Metrics, Applications of WSN.

Subtopics

The subtopics to be covered within this issue are listed below:

- Energy harvesting/charging and power management
- Long-life sensor node deployment and topology control
- Energy-efficient communication protocol design
- Scheduling algorithms for sensor networks
- Energy-efficient (or –free) sensing techniques
- New applications of self-sustainable sensor networks
- Data routing, processing and storage strategies
- Network modelling and performance analysis
- Common attacks
- Denial of service attack
- Node compromise
- Impersonation attack
- Protocol-specific attacks
- Attack resilient WSN
- Attack resilient time synchronized WSN

Schedule

Manuscript Submission Deadline: 30th September, 2018
Peer Review Due:30th October, 2018
Revision Due:15th November, 2018
Announcement of Acceptance by Guest Editor:30th November, 2018
Final Manuscript Due: 10th December, 2018

Contact:

Corresponding Guest Editor
Dr. Rajiv Kumar
Associate Professor
Department of ECE
Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh India,
Email: rjv.ece@gmail.com
Web: http://www.juit.ac.in/faculty.php?id=335&dep=ece&page=0

Dr. Hemraj Saini
Associate Professor
Department of CSE & IT
Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh India,
Email: hemraj1977@yahoo.co.in
Web: http://www.juit.ac.in/faculty.php?id=280&dep=cse&page=0