Recent Advances in Security in Cognitive Radio Networks

Call for papers

Future generations of wireless communications are expected to provide up to 10 Gbps data speed. Smart Devices will grow up to 34 billion by 2020. Thus, in the light of spectrum scarcity, smart spectral-efficient solutions are highly required. One of those solutions is Cognitive Radio (CR) that allows for opportunistic spectrum sharing among wireless users. Several research organizations have nominated CR as an integral component of the next wireless generations.

The most adopted CR model implies forming CR Networks (CRNs), where a set of CRs cooperate in identifying the unused spectrum. The aims of CRNs include improving the reliability of the spectrum sensing, improving the spectrum usage efficiency, and minimizing the resultant interference at the licensed users.

CRNs are vulnerable to many security threats due to their unique characteristics. Therefore, security protocols in conventional wireless systems cannot attain the same security level in CRNs. A significant amount of research has been dedicated for improving the security in CRNs in its all phases. This special issue will bring together the recent advances in security in CRNs.

Particular topics of interests for this special issue include (but are not limited to):

- Spectrum sensing data falsification attacks in CRNs
- Primary user emulation attacks in CRNs.
- Dependent and cooperating attacks in CRNs.
- Novel attack models in spectrum sensing in CRNs.
- Authentication protocols for CRNs.
- Intrusion detection in CRNs.
- Advances in physical-layer security in CRNs.
- Security and resource-efficiency tradeoff in CRNs.
- Localization mechanisms for incumbent emulation detection.
- Watermarking techniques for primary user authentication in CRNs.
- Reputation-based systems in Cooperative Spectrum Sensing.
- Novel cooperative authentication systems for CRNs.
- Secure geo-location database solutions in CRNs.
- Privacy preservation and data management in CRNs.
- Security issues in Applications of CRNs.
- Security threats in centralized and distributed CRNs.
Interested authors are highly encouraged to send the abstract to the editors by email (emails are listed below) in order to check the consistency with the special issue. Important deadlines are as follows

Paper submission: 1 November 2017
First feedback: 1 February 2018
Final submission: 1 March 2018.

Editors
- Dr. Saud Althunibat, Al-Hussein Bin Talal University, Jordan.
  Email: saud.althunibat@ahu.edu.jo
- Dr. Victor Sucasas, Instituto de Telecomunicacoes, Portugal.
  Email: vsucasas@av.it.pt
- Dr. Talha Faizur Rahman, COMSATS Institute of Information Technology, Pakistan.
  Email: talha_faizurrahman@comsats.edu.pk
- Dr. Senka Hadzic, University of Cape Town, South Africa
  Email: senka.hadzic@gmail.com