Channel surveillance strategy and interference reduction in future wireless networks

Mots clés :
- Directeur de thèse : VAN TAM NGUYEN
- Co-encadrant(s) :
- Unité de recherche : Laboratoire Traitement et Communication de l'Information
- École doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal: Divers

Résumé du projet de recherche (Langue 1)

In cooperative spectrum sensing, we will optimize the number of bits allocated to the quantization of local spectrum sensing reports. There is a tradeoff between the accuracy of sensing information, the energy consumption and the network throughput in the selection of the number of bit allocated to quantization. We will optimize the number of quantization bit for reporting spectrum sensing results to obtain maximum secondary network throughput and minimum secondary network energy consumption under the constraint of a low level of primary signal detection. Spectrum sensing suffers from two important security threats: a primary user emulation (PUE) attack and a spectrum sensing data falsification (SSDF) attack. For a PUE attack, we will study a novel method to counter PUE attacks using obligated identification fields available on CR users’ messages and an extra verification on primary signal-occupied timeslots. For an SSDF attack, we will formulate an optimal SSDF attack model, which will be harder to be detected by available methods. In order to achieve a detection strategy for stopping an optimal SSDF attacker, hidden Markov or Q-learning techniques will be adopted to estimate the historical sensing data generation model. Finally a sensing engine will be implemented based on the CR platform coupled with an open source software platform.