Programme de la réunion du vendredi 27 Novembre 2020
Session commune des GT « Sûreté / Surveillance / Supervision (S3)» et « Vérification et Synthèse des Systèmes Cyber-Physiques (VS-CPS)»
dans le cadre des Journées Nationales de l'Automatique, JNA 2020

De l'utilisation de la parcimonie en Automatique : applications au diagnostic et à la cybersécurité.
J-P Barbot (LS2N & Quartz) en collaboration avec S. Derbel, M. Makni, I. Mrad, S Nateghiboroujeni et W. Torki.
Abstract: Dans cette présentation dans un premier temps des techniques du traitement du signal et plus généralement d'optimisation sous contraintes en pseudo norme zéro sous hypothèse parcimonieuses sont rappelées. Ensuite, on propose comment utiliser celles-ci en automatique et en donne une application au diagnostic et une application à la détection des ``cyberattacks''.

Exploitation de test statistique d'hypothèses afin de concevoir des méthodes adverses, application à la dissimulation d'information.
Rémi Cogranne - LM2S-Université de technologie de Troyes
Résumé : Un test statistique est, comme son nom l'indique, généralement utilisée pour rejeter une ou plusieurs hypothèse et en accepter une concurrente. Cependant, contrairement aux méthodes d'apprentissage statistique, il est parfois possible de donner une expression des performances de tels tests.
Cela est souvent présenté comme une garantie ou une confiance que l'utilisateur peut placer dans le système. Dans cette présentation, nous allons montrer que dans un contexte "adverseriel" en vogue, disposer d'une expression quant à la performance d'un test permet également de concevoir une méthode visant justement à minimiser cette performance. Cela peut alors permettre à un adversaire de concevoir une méthode avec une "indétectabilité" garantie la plus grande possible. Nous appliquerons cette approche à la dissimulation d'informations dans les images (stéganographie et stéganalyse).

Towards secure state estimation of cyber-physical systems in the bounded- error framework
Nacim Ramdani (Univ. Orléans, PRISME) en collaboration avec Djahid Rabehi (PRISME) and Nacim Meslem (GIPSA-lab).
Abstract: Autonomous robots and most today's critical infrastructures are cyber-physical systems (CPS) that operate in highly networked environments as they need to communicate remotely with control and management systems. This feature makes them more vulnerable to cyber-attacks. For instance, a scenario of importance is posed by a malicious adversary that can arbitrarily corrupt the measurements of a subset of (remote) sensors in the CPS. Because sensor measurements data are used to generate control commands, corrupted measurements data will lead to corrupted commands, thus critically affecting the behaviour of the CPS. From a control theory perspective, one needs to develop algorithms and architectures for the detection of cyber-attacks on either sensors or actuators, and the mitigation of their impact on the resilience and the overall performance of the CPS. State-of-the-art methods often consider active attack detection, control algorithms that work directly with encrypted sensor data, or secure state estimation methods that show resilience when sensors are under cyber-attacks. In this talk, first, I will briefly review recent literature on cyber-security from the perspective of control theory. Then, I will describe our approach to secure state estimation, a secure interval state estimator for linear continuous-time systems with discrete-time measurements subject to both bounded-error noise and cyber-attacks. The interval state estimator is modelled as an impulsive system, where impulsive corrections are made periodically using measurement. The approach includes a new selection strategy that can endow the state estimation with resiliency to attacks, when assuming that only a subset of the whole set of sensors can be attacked although this subset is unknown a priori.