Resilient Control in Scale-Free Networks

Supervisors: Carlos Canudas-de-Wit (DR-CNRS, main supervisor), Federica Garin (CR-INRIA),
Application type: PhD student. **Gross salary:** 1757 Euros/month (CNRS official salary for PhD students).
Start: anytime from Sept. 2018. **Duration**: 36 months. **Employer:** CNRS. **Location**: Grenoble, France
Applications: http://scale-freeback.eu/openings/
Required background: Master in control systems engineering or applied mathematics

Context. **Scale-FreeBack** is an ERC Advanced Grant 2015 awarded to Carlos Canudas-de-Wit, Director of Research at the National Center for Scientific Research, (CNRS), during Sept. 2016-2021. The ERC is hosted by the CNRS. The project will be conducted within the NeCS group (which is a joint CNRS (GIPSA-lab)-INRIA team). Scale-FreeBack is a project with ambitious and innovative theoretical goals, which were adopted in view of the new opportunities presented by the latest large-scale sensing technologies. The overall aim is to develop *holistic scale-free control methods of controlling complex network systems in the widest sense, and to set the foundations for a new control theory dealing with complex physical networks with an arbitrary size*. Scale-FreeBack envisions devising a complete, coherent design approach ensuring the scalability of the whole chain (modelling, observation, and control). It is also expected to find specific breakthrough solutions to the problems involved in managing and monitoring large-scale road traffic networks. Field tests and other realistic simulations to validate the theory will be performed using the equipment available at the Grenoble Traffic Lab center (see GTL), and a microscopic traffic simulator replicating the full complexity of the Grenoble urban network. The proposed work will be undertaken in the context of this project.

Topic description.

Vulnerabilities in network systems involve faults and disruptions not only of some system components (sensors and actuators), but also of the communication interconnections. Such faults might be either random intrinsic malfunctions, or malicious external attacks. For example, in an intelligent road infrastructure, intrinsic faults might be the breakdown of some traffic lights, some closed roads for repair work, or failures of some sensors, while an example of external attack is a deception attack, where some roadside access point is shunted, so as to compromise data integrity (injection of fake signals replacing the sensor measurements) and possibly create a congestion compromising the system. Resilient closed-loop control must preserve correct functioning, or at least a graceful degradation, under a variety of possible risks, including malicious attacks exploiting some partial or total knowledge of the system dynamics.

Finding means of detecting and mitigating failures and attacks are the two main goals of this work. Resilient control of cyber-physical systems is a recent topic attracting a growing attention. Most current literature concerns linear network systems, in particular for electrical power-distribution networks. Scale-FreeBack proposes to investigate the resilient control issues arising in traffic networks, and more in general in complex network systems. This work will build upon previous results from the Scale-FreeBack project, where the complexity of controlling large network systems is tackled by controlling aggregated variables (e.g., average densities of some local zones of the traffic network), possibly with evolutionary (i.e., time-varying and state-dependent) aggregations. More specifically, it is proposed: 1) to develop diagnostic tools for detecting anomalies and revealing cyber-physical attacks, 2) to define security metrics for evolutionary networks, and 3) to revisit the optimal control design to attenuate the consequences of possible cyber-physical attacks affecting the most vulnerable nodes.