2018-00967 - PhD - Resilient Control in Scale-Free Networks

Level of qualifications required: Graduate degree or equivalent
Function: PhD Position

About the research centre or Inria department
Grenoble Rhône-Alpes Research Center groups together a few less than 800 people in 35 research teams and 9 research support departments.

Staff is localized on 5 campuses in Grenoble and Lyon, in close collaboration with labs, research and higher education institutions in Grenoble and Lyon, but also with the economic players in these areas.

Present in the fields of software, high-performance computing, Internet of things, image and data, but also in simulation in oceanography and biology, it participates at the best level of international scientific achievements and collaborations in both Europe and the rest of the world.

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 (GIAPSA-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 will be performed 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.

Assignment
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 (injection of fake signals replacing the sensor measurements). 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.

Main activities
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,
3. to revisit the optimal control design to attenuate the consequences of possible cyber-physical attacks affecting the most vulnerable nodes.

Benefits package
- Subsidised catering service
- Partially-reimbursed public transport
- Social security
- Paid leave
- Flexible working hours
- Sports facilities

Remuneration
1st and 2nd year: 1 982 euros brut /month
3rd year: 2 085 euros brut / month

General Information
- Theme/Domain: Optimization and control of dynamic systems
- Town/city: Montbonnot
- Inria Center: CRI Grenoble - Rhône-Alpes
- Starting date: 2018-09-10
- Duration of contract: 3 years
- Deadline to apply: 2018-08-15

Contacts
- Inria Team: NeCS
- Recruiter: Perrin Julie / julie.perrin@inria.fr

About Inria
Inria, the French National Institute for computer science and applied mathematics, promotes “scientific excellence for technology transfer and society”. Graduates from the world’s top universities, Inria’s 2,000 employees rise to the challenges of digital sciences. With its open, agile model, Inria is able to explore original approaches with its partners in industry and academia and provide an efficient response to multidisciplinary and application challenges of the digital transformation. Inria is the source of many innovations that add value and create jobs.

Conditions for application
- Defence Security: This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST). Authorization to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.
- Recruitment Policy: As part of its diversity policy, all Inria positions are accessible to people with disabilities.

Warning: you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.