A propos du centre ou de la direction fonctionnelle
The Inria Sophia Antipolis - Méditerranée center counts 34 research teams as well as 8 support departments. The center's staff (about 500 people including 320 Inria employees) is made up of scientists of different nationalities (250 foreigners of 50 nationalities), engineers, technicians and administrative staff. 1/3 of the staff are civil servants, the others are contractual agents. The majority of the research teams are located in Sophia Antipolis and Nice in the Alpes-Maritimes. Four teams are based in Montpellier and two teams are hosted in Bologna in Italy and Athens. The center is a founding member of Université Côte d’Azur and partner of the I-site MUSE supported by the University of Montpellier.

Contexte et atouts du poste
This postdoctoral position is hosted at INRIA, Sophia Antipolis and it develops within a close collaboration between INRIA, the University of Sheffield (TUOS) and Princeton University in the broad intersection of information theory, game theory, and artificial intelligence. Mobility between INRIA, the Department of Automatic Control and Systems Engineering at the University of Sheffield, as well as the department of Electrical Engineering at Princeton University, is expected contingent on the evolution of the COVID-19 pandemic. The position is supervised by Samir M. Perlaza and Etian Altman.

Mission confiée
Machine learning relies on exploiting vast amounts of data to learn system parameters that enable the automation of central problems in engineering, science, such as classification, regression, inference and decisions. Tuning the system parameters, which govern the system performance, is carried out under numerous statistical assumptions that find practical justifications in certain applications. Remarkably, a popular assumption is that data, which might be subject to data acquisition impairments, is not subject to malicious manipulation by an attacker that comprises its integrity with the aim of degrading the system performance.

The objective of this postdoc is to study data integrity attacks that capitalize on the existing vulnerabilities of machine learning techniques. The study of this problem demands addressing two important challenges. Firstly, the problem of characterizing the impact of attacking the data that is fed to the machine learning method. To this end, the problem is formulated using information measures that provide quantitative and operationally meaningful metrics for describing the relationship between the training data and the observed data. Secondly, the problem of detecting the attack can be tackled drawing from the links between information theory and statistical inference. By researching these two problems the project will shed light into the vulnerabilities of machine learning techniques and will develop novel attack detection techniques.

Principales activités
The postdoc is expected to be familiar with existing results by the team and in the literature in the design of data injection attacks for tampering with state estimation in cyber-physical systems [1-4]. In the context of this existing know-how at INRIA, the activities during the postdoc are structured across three main threads. The first two focus on the study of attack constructions and the third one aims to distill the knowledge obtained in the other two threads to produce novel attack detection techniques.

1- The tools and insight obtained on the work done for data injection attacks in cyberphysical systems will provide the foundation for investigating data integrity attacks on machine learning processes performing classification, regression, inference and/or decision tasks. In this project, learning parameters such as the loss function, size of data sets, computational complexity will be studied using information theoretic tools that provide characterizations of their impact on the fundamental performance limits.

2- Data integrity attacks have extensively been studied from the perspective of a single attacker possessing complete information. However, many of the learning applications operate on system-of-systems architectures for which scenarios with multiple attackers with access to partial subsystems pose a grave threat. In view of this, a research direction consists in the analysis of distributed attacks across the system with partial information and subject to limited communications channels among the attackers. In this context, the minimum information communication needs to launch a stealth attack are unknown. The motivation for this research follows from the fact that even when there is a single attacker, the sensors or data bases are hierarchically separated, which imposes implementation limitations on globally coordinated attacks.

3- Using the information theoretic models developed during the first part of the postdoc, the focus now shifts to the development of attack detection techniques. Probability of attack detection will be described in terms of the information measures characterizing the attack performance, and in doing so, we will identify the elements of the system that are most susceptible to suffer attacks. Ultimately, the proposed information theoretic framework will be used in the definition of security metrics that recognize and assess the system vulnerabilities that can be exploited by data integrity attacks.


[3] Cristian Genes, Iñaki Esnaola, Samir M. Perlaza, Luis F. Ochoa, and Daniel Coca. "Robust Recovery of...
Compétences
Candidates are expected to have a PhD degree in mathematics or areas related to information theory and game theory. Previous knowledge on information theory and game theory is desirable. The candidate must have a provable level of written and spoken English. Skills in French language are not required.

Avantages
- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural, and sports events and activities
- Access to vocational training
- Social security coverage

Rémunération
Gross Salary: 2653 € per month