DOCTORAL INPhINIT FELLOWSHIPS PROGRAMME – INCOMING - CALL 2020

PhD POSITION IN ADVERSARIAL MACHINE LEARNING AT THE ICMAT FOR THE INPhINIT PROGRAMME

Job Position title: PhD in Adversarial Machine Learning

Research project/ group description

The DataLab at the Statistics, Probability and Operations Research (SPOR) group covers a broad range of topics including data science and engineering, machine learning, optimal control, risk analysis, game theory, decision analysis and Bayesian methods. SPOR supports the whole spectrum of evidence based decision making, from mathematical foundations, to data analysis, to inference, to analysis, to decision support, with applications in fraud detection, security, cybersecurity, epidemiology, insurance, and social robotics, to name but a few. Our DataLab provides statistical support to other CSIC institutes and non-academic partners, with emphasis on big data and large scale analytics in grand challenge scientific and business applications. We have research links with groups at Duke, Paris-Dauphine, Aalto, CNR-IMATI, George Washington, IBM Research and others where research visits may be performed.

The PhD position will focus on a complex problem motivated by a societally relevant decision in the area of adversarial machine learning. The candidate is expected to cover the whole spectrum of activities involved in solving complex real problems, from data analysis, to building appropriate models and estimating them, to using such models to support forecasts and decisions, sometimes, even, to developing software to support the above tasks. The candidate will also collaborate in consulting opportunities arising through the DataLab.

Job position description

Machine Learning (ML) and Artificial Intelligence have had recent major successes in areas such as automatic translation or autonomous vehicle design. As a fundamental underlying hypothesis, all these developments rely on the use of independent identically distributed data for both the training and test phases. In this project, the PhD candidate will consider machine learning problems in relation with security, specifically in relation with one major socio-economical problem: fake news detection. From a methodological point of view, they form part of what is called adversarial machine learning (AML), which questions the previous iid data hypothesis in at least three directions which motivate this project:

- The presence of adversaries ready to modify the data to obtain a benefit.
- The distributions in the training and test phases may be different and frequently imbalanced.
- Attacks may vary over time.

The prevailing paradigm in this field is game theory, with its entailed common knowledge hypothesis. However, from a fundamental point of view, such hypothesis is not sustainable in our incumbent applications, as the adversaries tend to hide and conceal information. As a recent alternative, the field of adversarial risk analysis emerges (ARA).

The global objective of this project is to provide a new paradigm for adversarial machine learning which takes into account the presence of adversaries, of imbalanced classes and of concept drift and develop them methodologically and conceptually to solve problems in relation with fake news detection.

The PhD candidate will work on this project and is also expected to participate in the group activities (seminars, courses, conferences, etc.), and have regular meetings with his/her supervisor.

Group Leader: Prof. David Ríos Insua

Email: david.rios@icmat.es

David Rios´s website: https://www.icmat.es/drios

Other relevant websites:

Website of the SPOR Group: https://www.icmat.es/spor/

Website of the ICMAT´s group on Statistics, Probability and Operations Research: https://www.icmat.es/research/groups/group3

Links to the INPhINIT 2020 Incoming Open Call:

Programme description: https://obrasociallacaixa.org/en/investigacion-y-becas/becas-de-la-caixa/doctorado-inphinit/incoming

Application website: https://www.lacaixafellowships.org/index.aspx

Programme rules here.

PhD position finder: https://hosts.lacaixafellowships.org/finder