TELECOM Paris

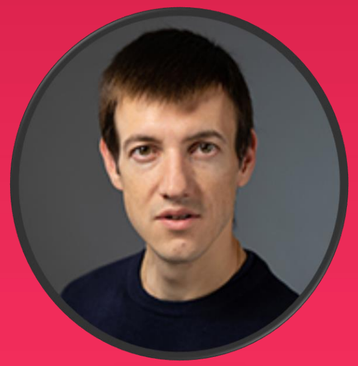
INSTITUT POLYTECHNIQUE DE PARIS

PROGRAMME DES CHAIRES

Anomaly detection in Finance, Connected Vehicles and Industry 4.0

Chairs Webinar on Nov. 3rd, 2022 | 4:30 - 6:00 pm (CET)

16h30 : **Introduction**



16h35 : **Anomaly detection using data depth: multivariate case**

Pavlo Mozharovskyi, Associate Professor at Télécom Paris, Institut Polytechnique Paris
Academic Team Member at Chair - Data Science & Artificial Intelligence

Anomaly detection is a branch of machine learning and data analysis which aims at identifying observations that exhibit abnormal behaviour. Be it measurement errors, disease development, severe weather, production quality default(s) (items) or failed equipment, financial frauds or crisis events, their on-time identification, isolation and explanation constitute an important task in almost any branch of industry and science. By providing a robust ordering, data depth - statistical function that measures belongingness of any point of the space to a data set - becomes a particularly useful tool for detection of anomalies. Already known for its theoretical properties, data depth has undergone substantial computational developments in the last decade and particularly recent years, which has made it applicable for contemporary-sized problems of data analysis and machine learning.
In this article, data depth is studied as an efficient anomaly detection tool, assigning abnormality labels to observations with lower depth values, in a multivariate setting. Practical questions of necessity and reasonability of invariances and shape of the depth function, its robustness and computational complexity, choice of the threshold are discussed. Illustrations include use-cases that underline advantageous behaviour of data depth in various settings.

17h00 : **Identifying and characterizing fraud in bank transactions**

Tiphaine Viard, Associate Professor at Télécom Paris, Institut Polytechnique Paris
Academic Team member- Explainable AI for Anti-Money Laundering

We focus here on the specific domain of bank transactions, where we specifically wish to detect and formally characterize fraudulent behaviours, i.e. bank transfers that are anomalous.
In addition to the common challenges of anomaly detection (lack of annotated data, ever-changing notion of anomaly), banking adds its own: the volume of data is extremely large, and banks have to provide strong justifications for their suspicions.
We will detail this specific context, and formalize an approach based on graph modelling that we develop in the XAI for anti-money laundering chair. We will brush over both the legal and technical standpoints.

17h20 : **How Machine Learning can Protect Connected Cars from Cyberattacks ?**

Rida Khatoun, Associate Professor at Télécom Paris, Institut Polytechnique Paris
Academic Team member at Chair - Connected Cars & Cyber Security

Connected vehicles are witnessing a huge evolution in terms of sensing (i.e., monitoring), processing and communication capabilities. They are increasingly relying on their connectedness to share more information and increase their cooperation and consequently their intelligence. However, the cybersecurity of the connected vehicles is highly critical. In fact, this domain increasingly attracts the attention of attackers. For example, Denial of Service (DoS) attacks are a major threat for vehicular networks. Detecting and identifying the DoS traffic is crucial for defending against such attacks. Machine Learning (ML) algorithms have been extensively adopted in traffic classification and detection of network attacks, namely the DoS attacks. We focus on our research on the use of unsupervised learning algorithms, notably clustering algorithms (e.g. k-means, Clara, DBSCAN and GMM) for detecting DoS attacks. We analyze and compare the detection efficiency of selected UL algorithms using the Vehicular Reference Misbehavior (VeReMi) dataset. The results demonstrates the efficiency of some clustering algorithms for DoS detection; in particular, the Gaussian Mixture Model (GMM) algorithm demonstrates a detection accuracy with more than 95% for all DoS attack traffic categories (DoS, random DoS, and disruptive DoS).

17h40 : **Discussion**

TELECOM Paris

INSTITUT POLYTECHNIQUE DE PARIS

For more information, click on the images below: