Université de Lorraine - IDMC
Masters SC & TAL – M1
2018-2019

Fiche de projet tutoré / Project form

Anomaly detection with deep learning models

Encadrement / Supervisors

1. LORIA laboratory, SYNALP team
1. main supervisor: Christophe Cerisara (cerisara@loria.fr)
2. other supervisors: Samuel Cruz-lara

Description / Description

1. global project

The objective of this project is to handle a continuous stream of logs, with language data, and train a generative deep learning model on it in an unsupervised way. This model will ideally capture the latent, unknown, normal generative process that produces this stream of observations. For instance, for system logs, the model shall capture the normal, standard sequence of instructions and measures that are executed on the system, without having a direct access to them, but only by observing their output messages.

Then, an anomaly is defined as an abnormal deviation in this process, which is typically due to some failure in the system. The generative model trained so far can be used to detect such anomalies that deviate from the expected predicted behavior.

The whole training process is thus unsupervised, but the main challenges are related to finding the best compromise between closely fitting the training sequence and generalizing to acceptable deviations.

2. biblio. UE 705 (semestre 7)

The literature review will focus on anomaly detection and training predictive generative models, such as the neural language model.

3. réalisation. UE 805 (semestre 8)

The students will choose from their literature review a possible model for anomaly detection, implement it and validate it on system logs datasets.

Informations diverses : matériel nécessaire, contexte de réalisation /
Various information: material, context of realization

Programming in python, with one of the available deep learning toolkits: pytorch or keras.

Use of gitlab to host the code and reports (in markdown or latex).

Livrables et échéancier / Deliverable and schedule

- S7: report on literature review
- S8: model design, implementation and validation; final report.

Bibliographie /References (max. 4-5)

[*il ne s'agit pas de la bibliographie complète qui sera fournie aux étudiants au début du projet mais d'une bibliographie indicative pour aider à cerner le sujet*]

Chalapathy et a., "Anomaly Detection using One-Class Neural Networks", feb. 2018, https://arxiv.org/abs/1802.06360

M. Du et al., "DeepLog: anomaly detection and diagnosis from system logs through deep learning", Proc. ACM CCCS 2017

Radford et al., "Network Traffic Anomaly Detection Using Recurrent Neural Networks", mar. 2018, https://arxiv.org/abs/1803.10769