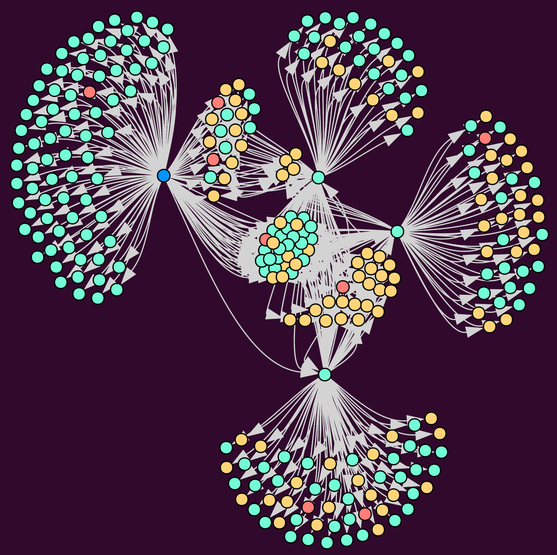
Detecting complex cyberattacks with Graph Deep Learning

Motivation

When a system is represented as a **graph**, new kind of **features** such as **graph topology** and **node interactions** can be leveraged.

These features help Deep Learning models to detect advanced cyber threats such as **DDoS**, **intrusions**, **malwares** or even **APTs**.



***Thesis title**: Graph Deep Learning applied to the detection of cyberattacks and vulnerabilities*

Supervisor: Pr. Khaldoun Al Agha
Advisors: Dr. Nour El Madhoun, Anis Zouaoui

Tristan BILOT
tristan.bilot@lisn.fr

Keywords

PhD subject *Graph representation learning* *Deep Learning* *Cybersecurity* *Network*

Data collection & graph building

Network-based and **host-based** metrics are captured using **sensors**

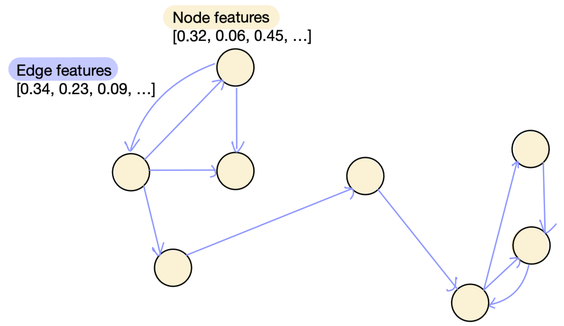
Network flows

source IP, destination IP, nb packets, average packet size, ...

Host metrics & logs

Shell commands, processes, system calls, CPU, RAM, ...

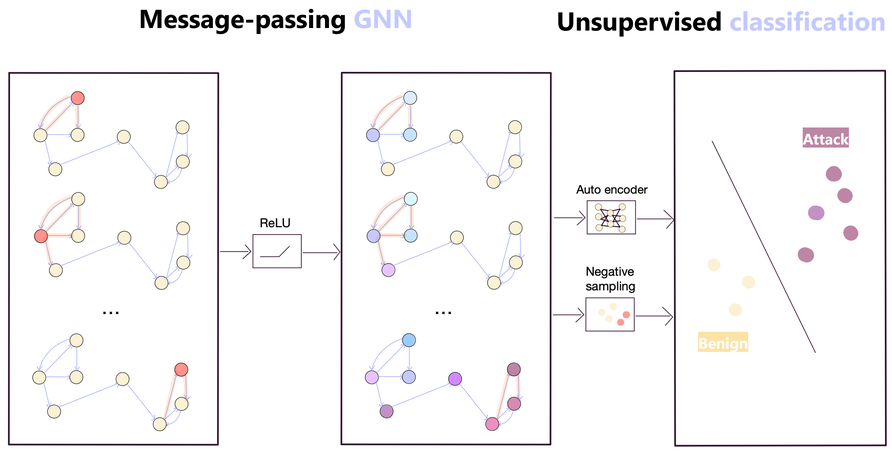
A **heterogeneous graph** is built from these data, using **flow connections**



Graph embeddings & classification

- Graph representation learning and **Graph Neural Networks** are used to extract **node embeddings**
- Temporal GNNs may be used to capture **long-term attack** dependencies

- The **classification** can be done at node-, edge- or graph-level depending on the data
- An ideal **detection system** should be able to classify in near real-time



LISN LABORATOIRE INTERDISCIPLINAIRE DES SCIENCES DU NUMÉRIQUE
université PARIS-SACLAY
cnrs
isep École d'ingénieurs du numérique
IRIGUARD