Détection non-supervisée d'anomalies dans le trafic réseau grâce à une approche se basant sur le Double Deep Q-Learning

Bilel Saghrouchni, Frédéric Le Mouël, Bogdan Szanto

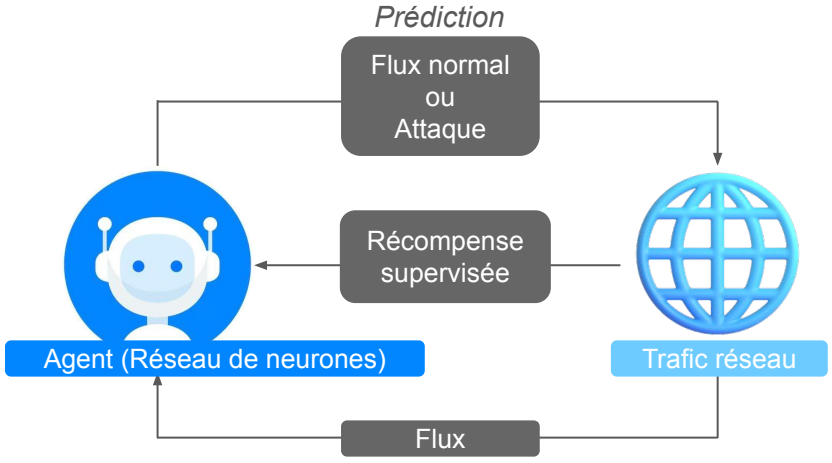
Détection non-supervisée d'anomalies dans le trafic réseau grâce à une approche se basant sur le Double Deep Q-Learning

Bilel SAGHROUCHNI[12] - Frédéric LE MOËL[1] - Bogdan SZANTO[2]
[1]CITI Lab (INSA Lyon) [2]SPIE ICS

Abstract

Les systèmes de détection d'intrusion (IDS) basés sur l'apprentissage profond se sont révélés performants mais peinent à apprendre en continu et à détecter de nouvelles attaques au fil du temps en raison d'une fonction de récompense supervisée basée sur des étiquettes. *[3]*
Dans ce poster, nous présentons une méthode non supervisée d'apprentissage double Q profond (DDQL) qui vise à détecter les attaques et à apprendre de nouveaux comportements grâce une fonction de récompense non supervisée utilisant un score de normalité inspiré de la détection des anomalies du trafic automobile.

Apprentissage par renforcement profond



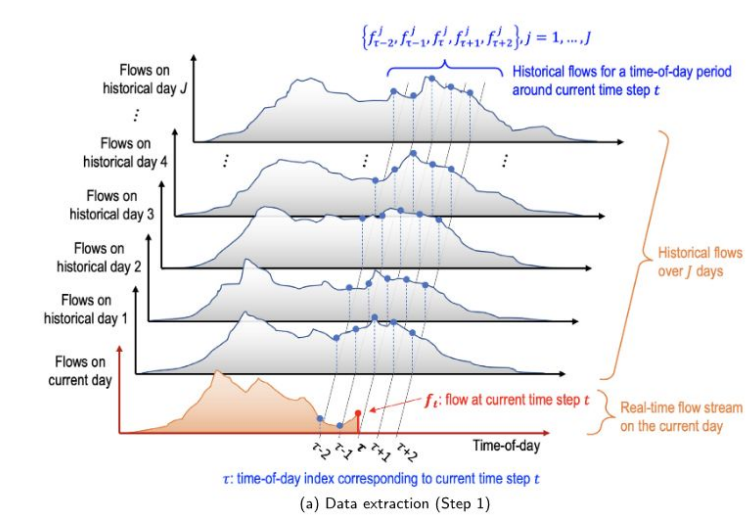
Aujourd'hui, les fonctions de récompenses pour la détection d'intrusion sont supervisées et se base sur un *label*. Cela rend ces solutions inutilisables en conditions réelles, où la nature des flux est inconnue. *[2]*

Score de normalité pour la détection d'intrusion

$$\beta = \frac{tailleCluster}{tailleCluster_{moy}} \cdot \frac{distNormalCluster}{distNormalCluster_{moy}}$$

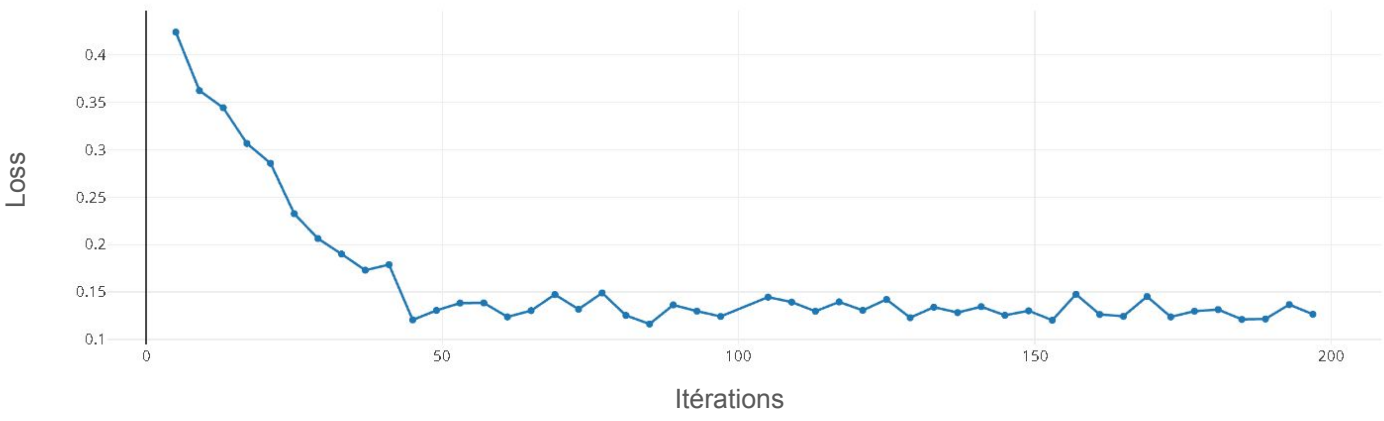
Afin d'utiliser ce score, chaque état (correspondant à un groupement de flux) est clusterisé grâce à l'algorithme KMeans.

Une fonction de récompense basée sur le clustering



Cette approche de détection d'anomalie du trafic automobile définit la récompense en fonction d'un score de normalité caractérisant un cluster de flux normaux (score haut) et un cluster de flux d'attaque (score bas). *[1]*

Résultats



F1 Score moyen	0.96
Accuracy moyenne	0.94

Les expérimentations ont été réalisées avec le dataset NSL-KDD. *[5]*

Références

1. Dan He, "Autonomous anomaly detection on traffic flow time series with reinforcement learning", IEEE Transactions on Neural Networks and Learning Systems, 2023.
2. Manuel Lopez-Martin, "Application of deep reinforcement learning to intrusion detection for supervised problems", IEEE Access, 2020.
3. Imad Tareq, "Deep reinforcement learning approach for cyberattack detection", Journal of Information Security and Applications, 2024.
4. Tom Schaul, "PRIORITIZED EXPERIENCE REPLAY", International Conference on Learning Representations (ICLR), 2016.
5. Gaurav Meena, "A review paper on IDS classification using KDD 99 and NSL KDD dataset", International Journal of Scientific & Engineering Research, 2017.