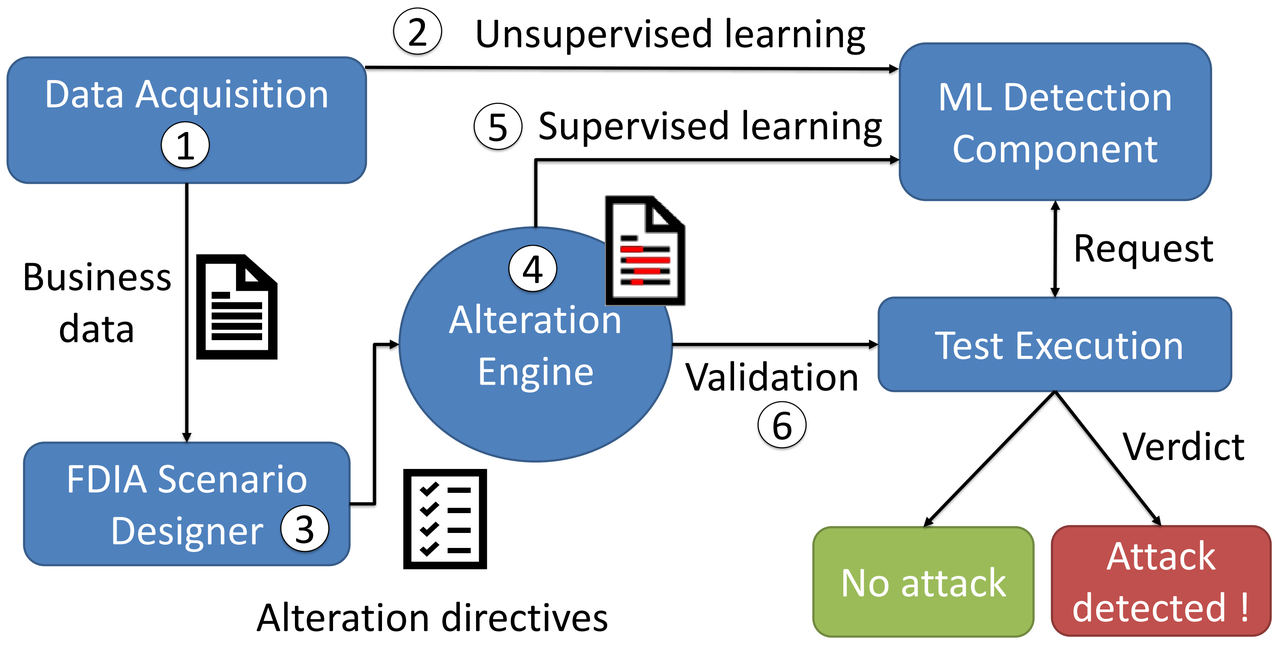
GeLeaD : *Generate Learn and Detect*

Objectif du projet

Le but du projet GeLeaD est de proposer des méthodes de détection des FDIA (*False Data Injection Attacks*) basées sur des composants de *Machine Learning* (ML). L'originalité des travaux réside dans la génération automatique des données destinées à l'entraînement et/ou à la validation des composants de détection.

Architecture générale de l'approche



1. L'approche consiste à récupérer massivement les données métier au sein d'un domaine via des capteurs ou de bases de données de données existantes.
2. À partir de ces données il est possible d'entraîner un composant ML afin qu'il apprenne une représentation du domaine issue de données réelles. On parle alors d'apprentissage non supervisé.
3. Sur ces données, il est également possible de concevoir des scénarios d'attaques FDIA grâce à un langage dédié.
4. Ces scénarios peuvent être exécutée afin de produire des données altérées de manière à simuler les traces que laisserai une cyberattaque.
5. Les données altérées peuvent alors être labellisées afin d'entraîner un composant ML à détecter des types précis d'attaques. On parle alors d'apprentissage supervisé.
6. Les données peuvent également être utilisée pour évaluer l'efficacité d'un composant ML de détection préalablement entraîné.

La détection des cyberattaques

Apprentissage non supervisé

Détection via un score d'anomalie

- Association d'un score à une séquence de messages (fenêtre de détection)
- « Apprentissage » d'un seuil caractérisant les données sans attaques.

Apprentissage supervisé

Détection via la classification en deux classes : attaqué / non-attaqué :

- Classification du dernier message d'une séquence de messages.
- Classification d'une séquence de messages (fenêtre de détection)

Architecture répandues pour la classification de séries temporelles :

- *Long Short-Term Memory* (LSTM)
- *Convolutional Neural Network* (CNN)
- *CNN-LSTM*
- Etc.

Actuellement deux domaines d'applications

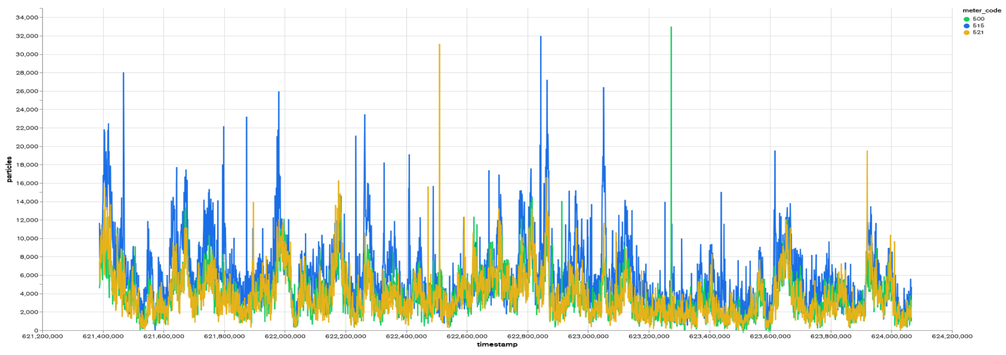
Intelligent Parking System (IPS)

Données métier issues des kiosques IPS :

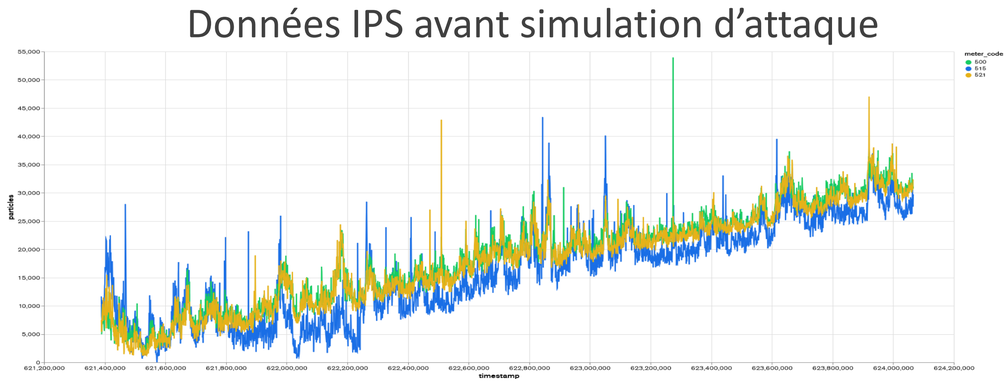
- Niveau de pollution
- Température
- Humidité
- Niveau de bruit

Kiosque IPS

Exemple d'altération :



Données IPS avant simulation d'attaque

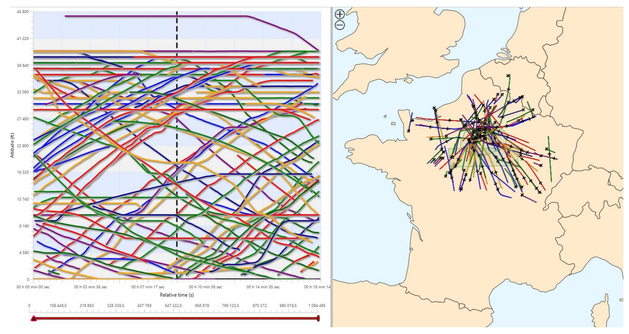


Données IPS après simulation d'attaque

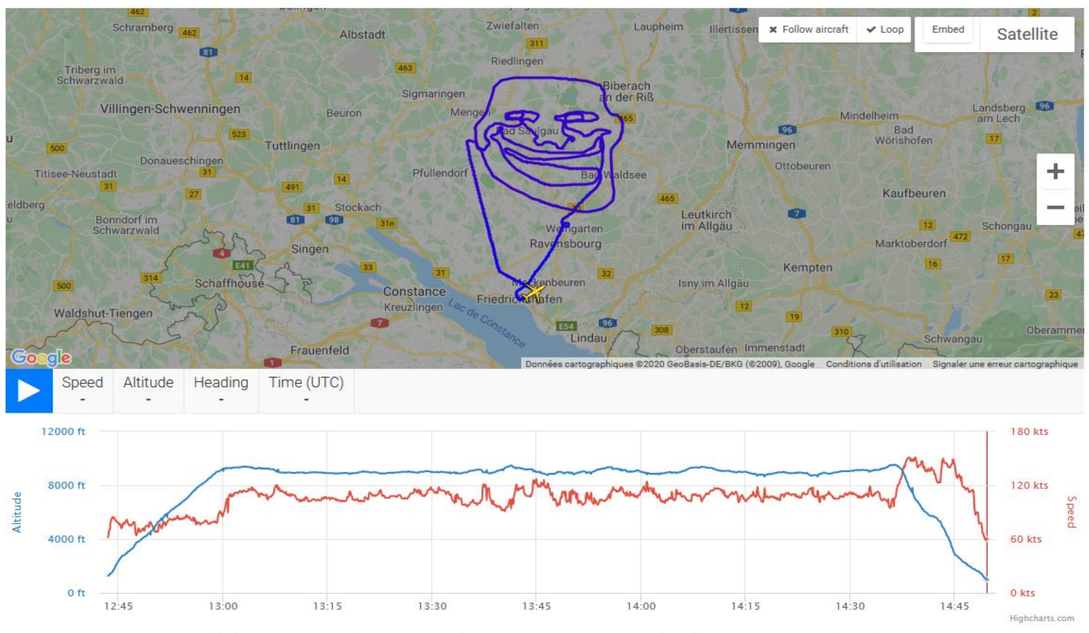
Air Traffic Control (ATC)

Données métier issues des avions via le protocole ADS-B :

- Position 3D de l'avion
- Vitesse au sol
- Direction
- Vitesse ascensionnelle
- Statut (*squawk*)
- Etc.



Exemple d'altération :



« Trollface » dessinée via une altération de la trajectoire

ANR ASTRID - GeLeaD

Coordinateur du projet :

Raphaël COUTURIER

raphael.couturier@univ-fcomte.fr

INSTITUT FEMTO-ST

15 B AVENUE DES MONTBOUCONS

25030 BESANÇON CEDEX

www.femto-st.fr

UBFC UNIVERSITÉ BOURGOGNE FRANCHE-COMTÉ

Smartesting® Cognitive Test Automation

femto-st SCIENCES & TECHNOLOGIES

PROJET FINANCÉ PAR L'ANR - PROJECT FUNDED BY THE ANR