Détection d'intrusion pour des réseaux embarqués automobiles

Approches d'apprentissage profond pour une meilleure détection

Institut Mines-Télécom

Parties prenantes

TELECOM Paris

IP PARIS

Auteurs

Natasha Alkhatib
Maria Mushtaq
Hadi Ghauch
Jean-Luc Danger

Partenaires

NOKIA

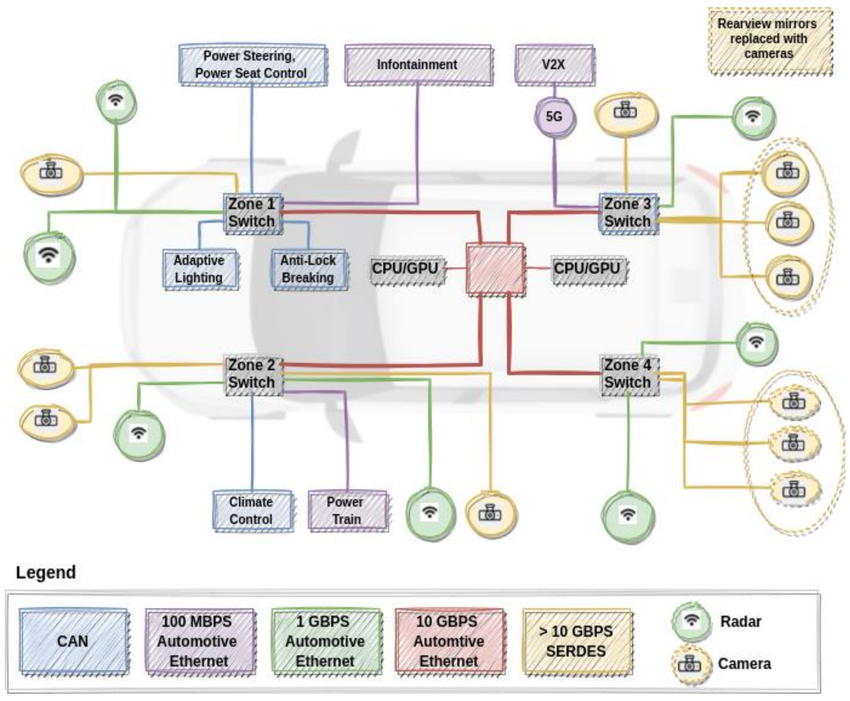
THALES

Valeo
SMART TECHNOLOGY FOR SMARTER CARS

WAVESTONE

Contexte

- **Assurer la sécurité et le divertissement** – des services sophistiqués sont mis en place par les constructeurs automobiles.
- **Complexité croissante des logiciels embarqués** – augmentation de la probabilité d'apparition des vulnérabilités dans ces logiciels.
- **Connectivité étendue des véhicules** – multiplication des interfaces de communication entre le réseau interne et le monde extérieur.
- **Cyberattaques automobiles** – plus de points d'entrées sur les réseaux automobiles embarqués (CAN, FlexRay, MOST, LIN et Ethernet).
- Ces réseaux puissent contenir des vulnérabilités qu'un attaquant peut exploiter.



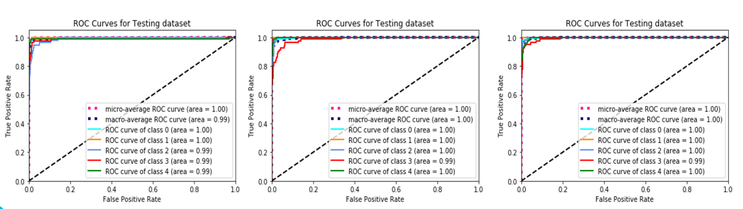
Objectifs

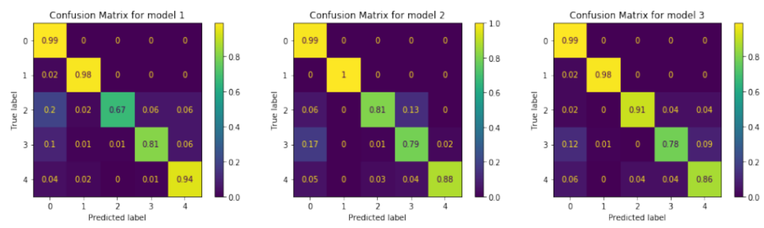
Dans cette thèse, nous utiliserons des techniques d'apprentissage profond pour détecter des intrusions à l'intérieur des différents types de réseaux automobiles embarqués.

- **Données** – Générer et utliliser des ensembles de données contenant différents types s'intrusions sur divers réseaux automobiles embarqués, en particulier Automotive Ethernet (SOME/IP et AVTP) et CAN.
- **Approches basées sur les données** – Construire et comparer différentes techniques de détection d'intrusion supervisées et non supervisées pour la détection d'intrusion en termes de performances et de compléxité de calcul.
- **Solution en temps réel** – Embarquer notre solution dans un calulateur ECU et vérifier son efficacité en temps réel.

Détection supervisée de divers types d'intrusion sur le protocole SOME/IP

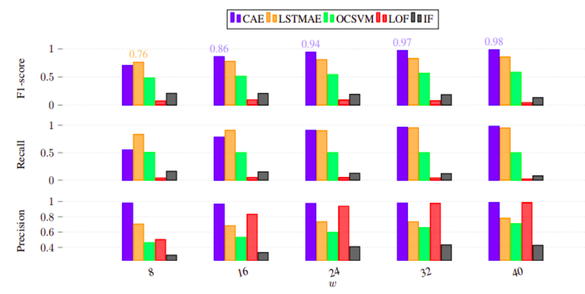
- **Créer une base de donnée composée de traces de paquets SOME/IP normales et anormales.**
- **Développer un modèle supervisé de réseau neuronal récurrent (RNN) pour classer différents types d'attaques.**
- **Divers types d'Intrusions prédites avec succès avec des valeurs F1 et AUC supérieures à 0.8.**





Comparaison de differents techniques non supervisée de détection d'intrusions sur le protocole AVTP

- **Les méthodes deep learning (Autoencoders) vs machine learning.**
- **Meilleure modèle CAE pour différents longueurs de séquences AVTP (0,76<score F1<0,98 et temps de détection = 0.4 s)**



Réference:.

Alkhatib, Natasha, Hadi Ghauch, and Jean-Luc Danger. "SOME/IP Intrusion Detection using Deep Learning-based Sequential Models in Automotive Ethernet Networks." 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2021.

Contact : natasha.alkhatib@telecom-paris.fr

Projet: https://github.com/Alkhatibnatasha/SOMEIP_IDS