

Détection d'anomalies de classification dans l'IoT via Machine Learning

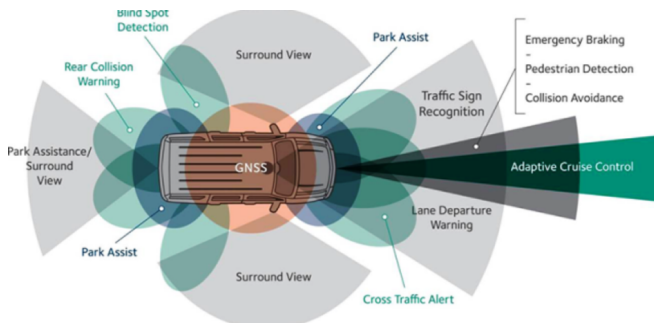
Antoine Urban, Yohan Chaliér

Projet de filière SR2I
Télécom ParisTech

22 juin 2018

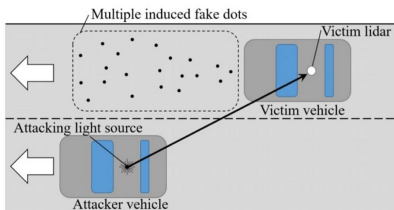
Introduction

La détection d'obstacles : un enjeu de sécurité !

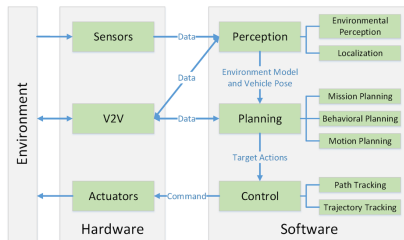


Ensemble des capteurs présents dans le véhicule

Attaques potentielles



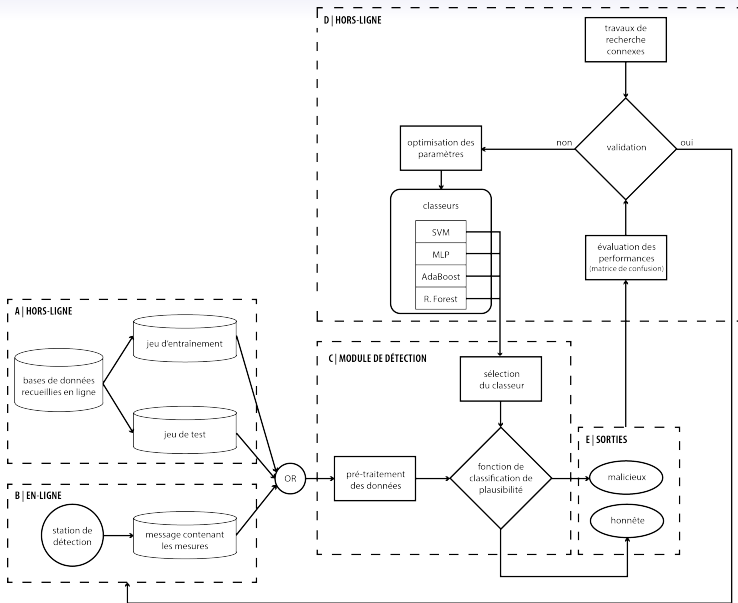
Attaque par aveuglement des capteurs



Attaque par modification

Objectifs

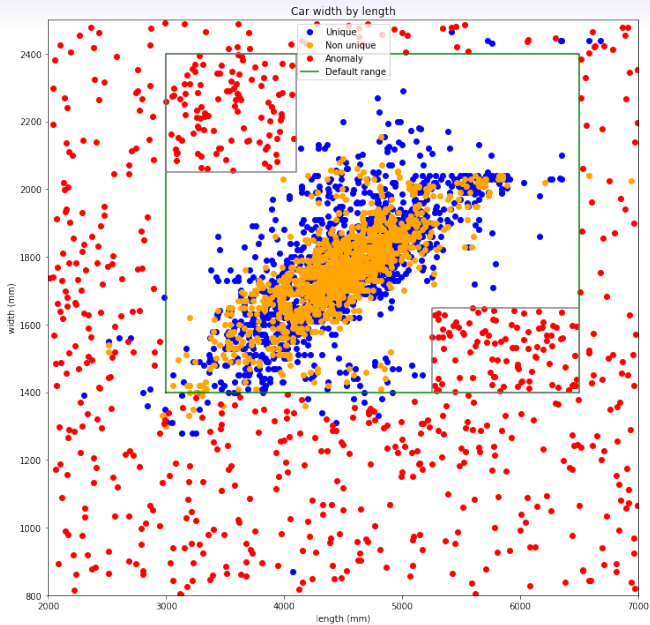
Proposition d'un modèle de classification multi-classes en réalisant un classeur à partir d'un algorithme d'apprentissage supervisé.



Première implémentation

- Extraction des colonnes largeur et longueur de la base de données
- Suppression des redondances
- Définition de zones de décision arbitraires
- Génération des données malicieuses

validité	intervalle de longueur	intervalle de largeur
non-malicieux	3 à 6,5 mètres	1,4 à 2,4 mètres
malicieux	3 à 4,1 mètres	2,05 à 2,4 mètres
malicieux	5,25 à 6,5 mètres	1,4 à 1,65 mètres



Méthodes d'évaluation

Matrice de confusion

		Classe réelle			
		Positif	Négatif		
Classe prédite	Positif	<i>TP</i>	<i>FP</i>	<i>PPV</i>	<i>FDR</i>
	Négatif	<i>FN</i>	<i>TN</i>	<i>FOR</i>	<i>NPV</i>
		<i>TPR</i>	<i>FPR</i>		
		<i>FNR</i>	<i>TNR</i>		

Chargement des bases de données (1/2)

1. Pour chaque jeu de données au format CSV
 - 1.1. Lire les colonnes contenant la longueur et la largeur
 - 1.2. Renommer ces colonnes en "length" et "width"
 - 1.3. Supprimer les lignes incomplètes
 - 1.4. Si nécessaire, convertir les données en flottant et en millimètres
 - 1.5. Ajouter une colonne contenant la classe correspondant au jeu de données considéré
 - 1.6. Appliquer un premier filtre sur la longueur ou la largeur pour supprimer les points extrêmes isolés
2. Fusionner toutes les matrices précédentes en une seule
3. Créer un nouvel objet Detector avec cette matrice en attribut

Chargement des bases de données (2/2)

1. Supprimer les éventuels redondances
2. Ajouter une colonne "odd" à la matrice, initialisée à False
3. **Générer les données malicieuses**
4. Ajouter les données malicieuses à la base de données, en rajoutant la colonne "odd" initialisée à True
5. Remplacer les valeurs des classes (originellement des chaînes de caractères comme "car" ou "human") par des entiers
6. **Séparer la matrice en un jeu d'entraînement et un jeu de test**
7. Renvoyer l'objet Detector ainsi initialisé

Classe Detector

- Pré-traitement
 - clean
 - append_odd_points
 - format
- Interface scikit-learn
 - classify
 - tune_parameters
 - predict
- Affichage
 - plot
 - plot_decision_boudaries

Méthodes d'évaluation

Score F1

Objectif

Maximisation du score F1 comme critère de performance

$$\text{f1-score} = \frac{2 \times (\text{Recall} \times \text{Precision})}{(\text{Recall} + \text{Precision})} = 2 \times \frac{PPV \times TPR}{PPV + TPR} \quad (1)$$

$$\text{Precision} = \frac{TP}{TP + FP} \quad (2)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (3)$$