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

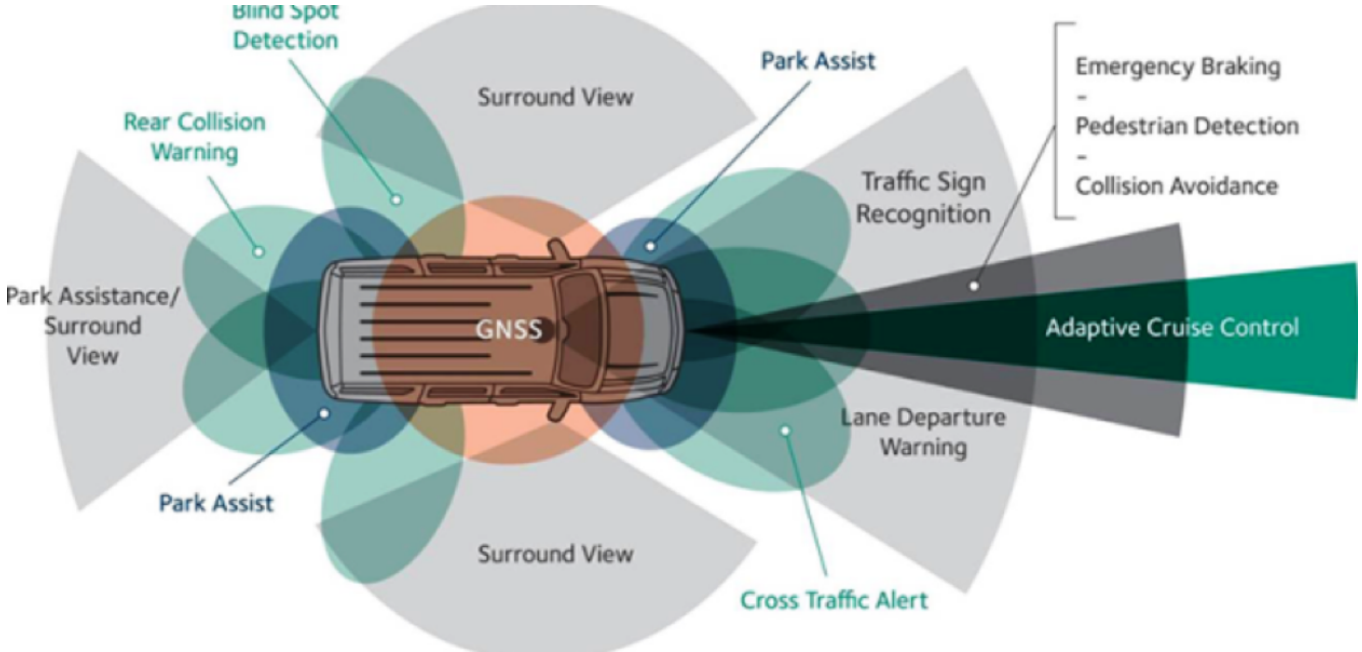
Antoine Urban, Yohan Chalier

Projet de filière SR2I
Télécom ParisTech

22 juin 2018

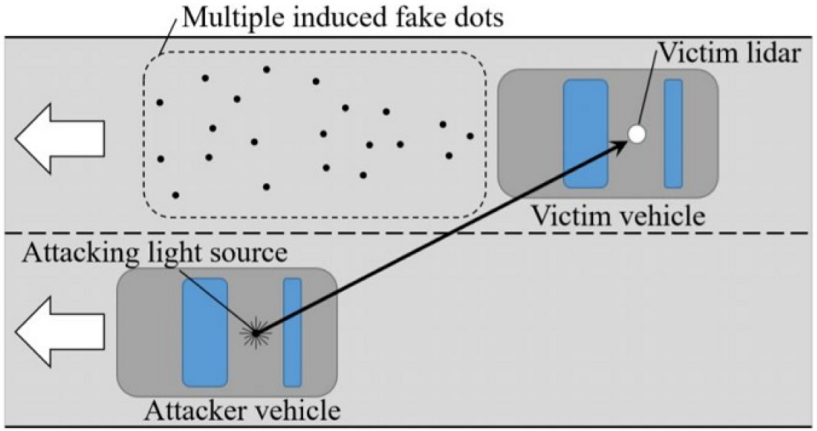
Introduction

La détection d'obstacles : un enjeu de sécurité !

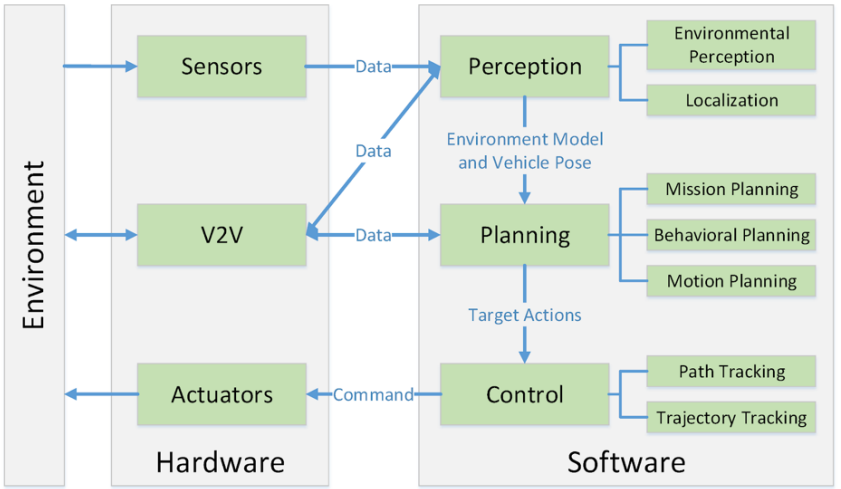


Ensemble des capteurs présents dans le véhicule

Attaques potentielles



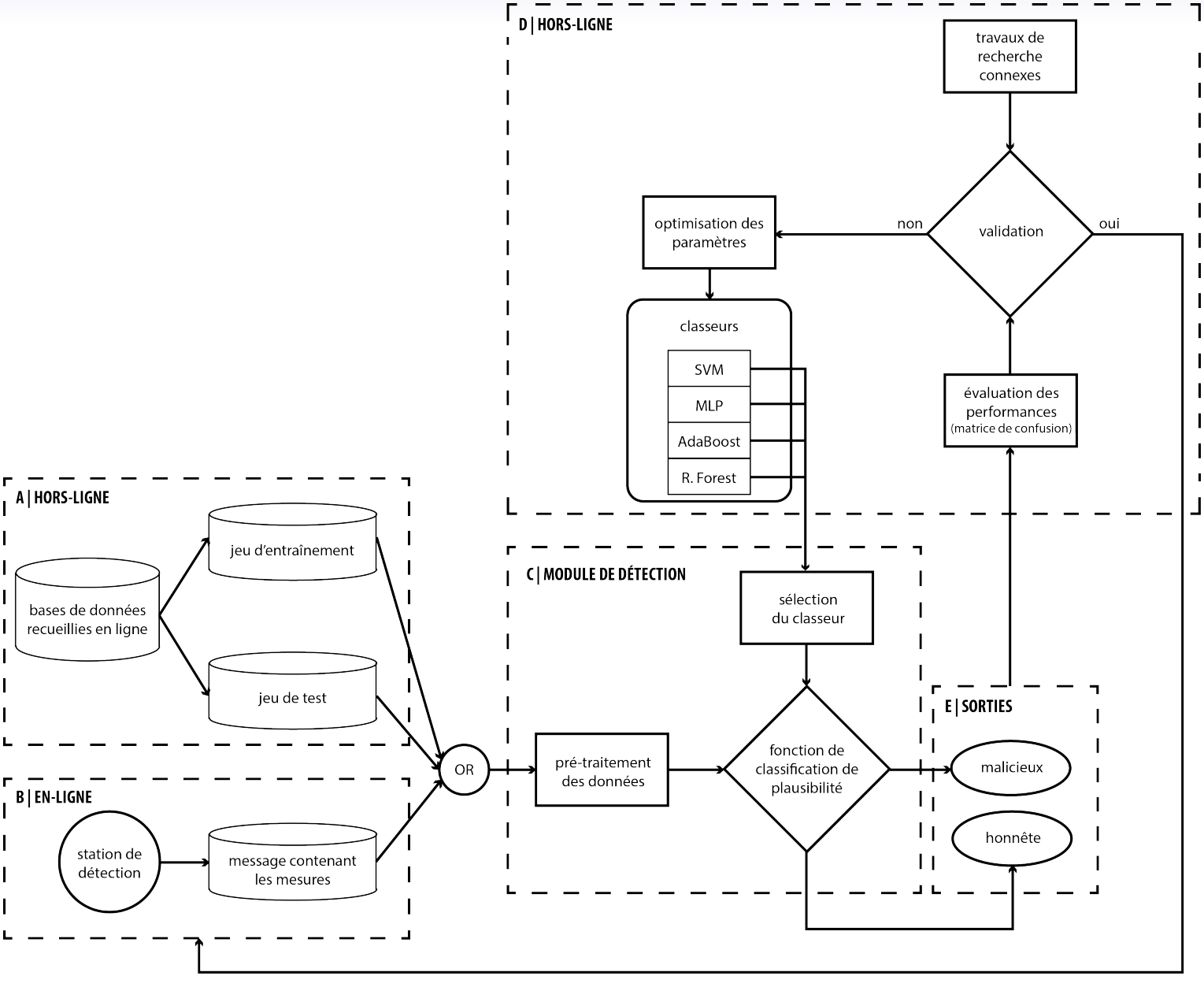
Attaque par aveuglement des capteurs



Attaque par modification

Objectifs

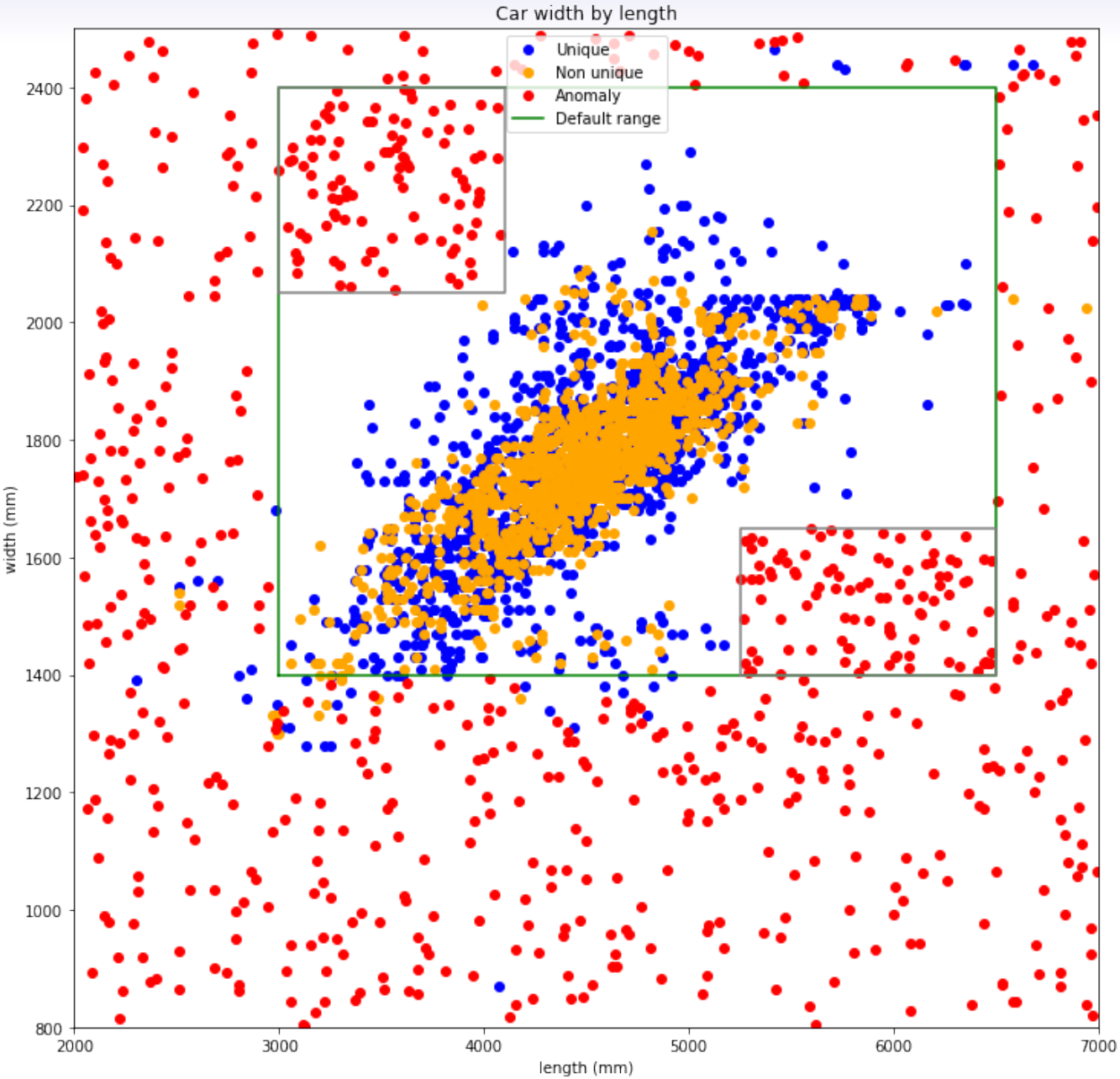
Proposition d'un modèle de classification multi-classes en réalisant un classeur à partir d'un algorithme d'apprentissage supervisé.


D | HORS-LIGNE
travaux de recherche connexes
validation
non
oui
optimisation des paramètres
classeurs
SVM
MLP
AdaBoost
R. Forest
évaluation des performances
(matrice de confusion)
A | HORS-LIGNE
bases de données recueillies en ligne
jeu d'entraînement
jeu de test
C | MODULE DE DÉTECTION
sélection du classeur
OR
pré-traitement des données
fonction de classification de plausibilité
E | SORTIES
malicieux
honnête
B | EN-LIGNE
station de détection
message contenant les mesures

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


Car width by length
Unique
Non unique
Anomaly
Default range
width (mm)
length (mm)
800
1000
1200
1400
1600
1800
2000
2200
2400
2000
3000
4000
5000
6000
7000

Méthodes d'évaluation

Matrice de confusion

		Classe réelle			
		Positif	Négatif		
Classe prédite	Positif	*TP*	*FP*	*PPV*	*FDR*
	Négatif	*FN*	*TN*	*FOR*	*NPV*
		TPR	*FPR*		
		FNR	*TNR*		

Méthodes d'évaluation

Score F1

Objectif

Maximisation du score F1 comme critère de performance

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

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

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