

# 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 !

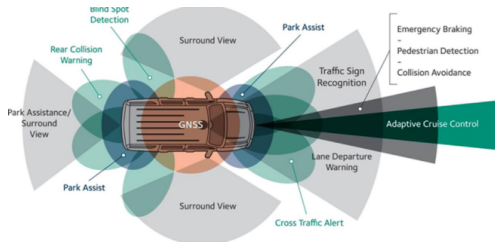
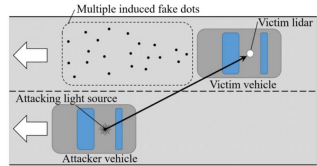


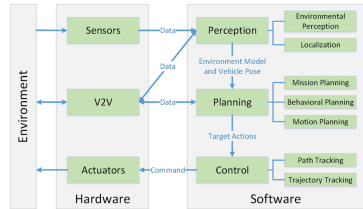
FIGURE – Ensemble des capteurs présents dans le véhicule

# Attaques potentielles

## Attaque par aveuglement des capteurs

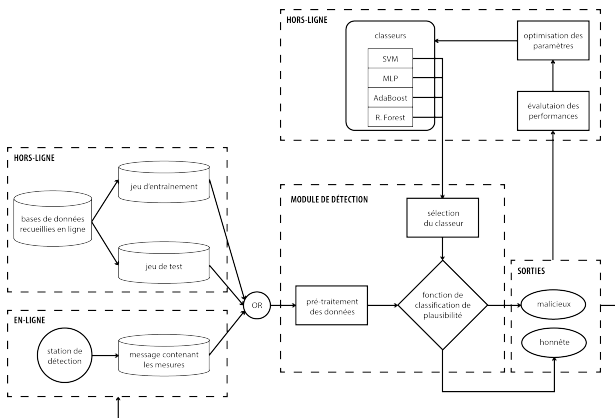


## Attaque par modification



# Objectifs

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



# Méthodes d'évaluation

## Matrice de confusion

		Classe réelle			
		Positif	Négatif		
2*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>		

# Méthodes d'évaluation

## Score F1

**Objectif :** Maximisation du score F1 comme critère de performance

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

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

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