



Mineur IOT – Projet 1 : Contrôle du trafic

RAPPORT D'ANALYSE

BENZINA Mohamed-Ali
OUHBAD Omar

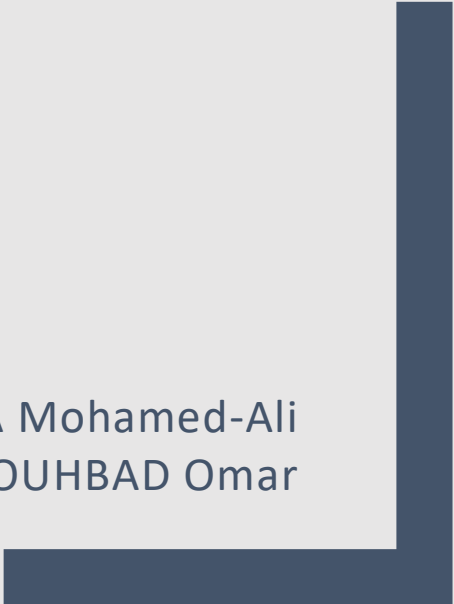


Table des matières

Description du sujet.....	2
Contexte	2
Architecture	3
Schéma	3
Modèles.....	3
Données recueillies	4
Hardware.....	4
Applicatif	4
Technologies utilisées.....	5
Protocole utilisé	5
Sécurité.....	5

Description du sujet

Pour commencer, l'architecture devra être conçue pour gérer un grand volume de données en provenance de nombreux véhicules. Ces données seront périodiques (vitesse, par exemple) et ponctuelles (détection d'accidents, par exemple), et devront être traitées en temps réel pour que les alertes puissent être générées et remontées rapidement. Pour cela, il sera nécessaire de configurer des serveurs de traitement de données de hautes performances pour gérer les flux de données en temps réel.

Une fois les données récupérées, il sera nécessaire de les analyser pour générer les alertes appropriées. L'analyse devra prendre en compte les règles définies dans le projet (par exemple, l'alerte d'accident sera remontée si elle est validée par au moins 2 véhicules et l'alerte d'embouteillage sera remontée si au moins 3 véhicules roulent en dessous de la vitesse autorisée). Il faudra également développer des algorithmes pour traiter ces données et générer les alertes.

Enfin, l'architecture devra inclure une interface utilisateur pour visualiser l'historique des données et des alertes remontées. Il sera également nécessaire de développer des programmes ou sites pour afficher les informations en temps réel. Pour cela, il faudra tenir compte des contraintes d'ergonomie, pour garantir une utilisation intuitive et efficace de l'interface utilisateur.

Contexte

Dans le cadre de ce projet, nous allons imaginer un contexte d'implémentation. Nous prendrons le cas d'une société comme VINCI Autoroutes. Et plus spécifiquement dans le cas de l'autoroute A7. On suppose que le centre de contrôle de l'autoroute se situe à Lyon. Des bornes d'acheminement sont situées tous les 10 kms. Sur 312 km d'autoroutes nous avons donc approximativement 31 bornes. On suppose que les bornes d'acheminement sont connectées au même réseau que celui du centre de contrôle.

Architecture

Schéma

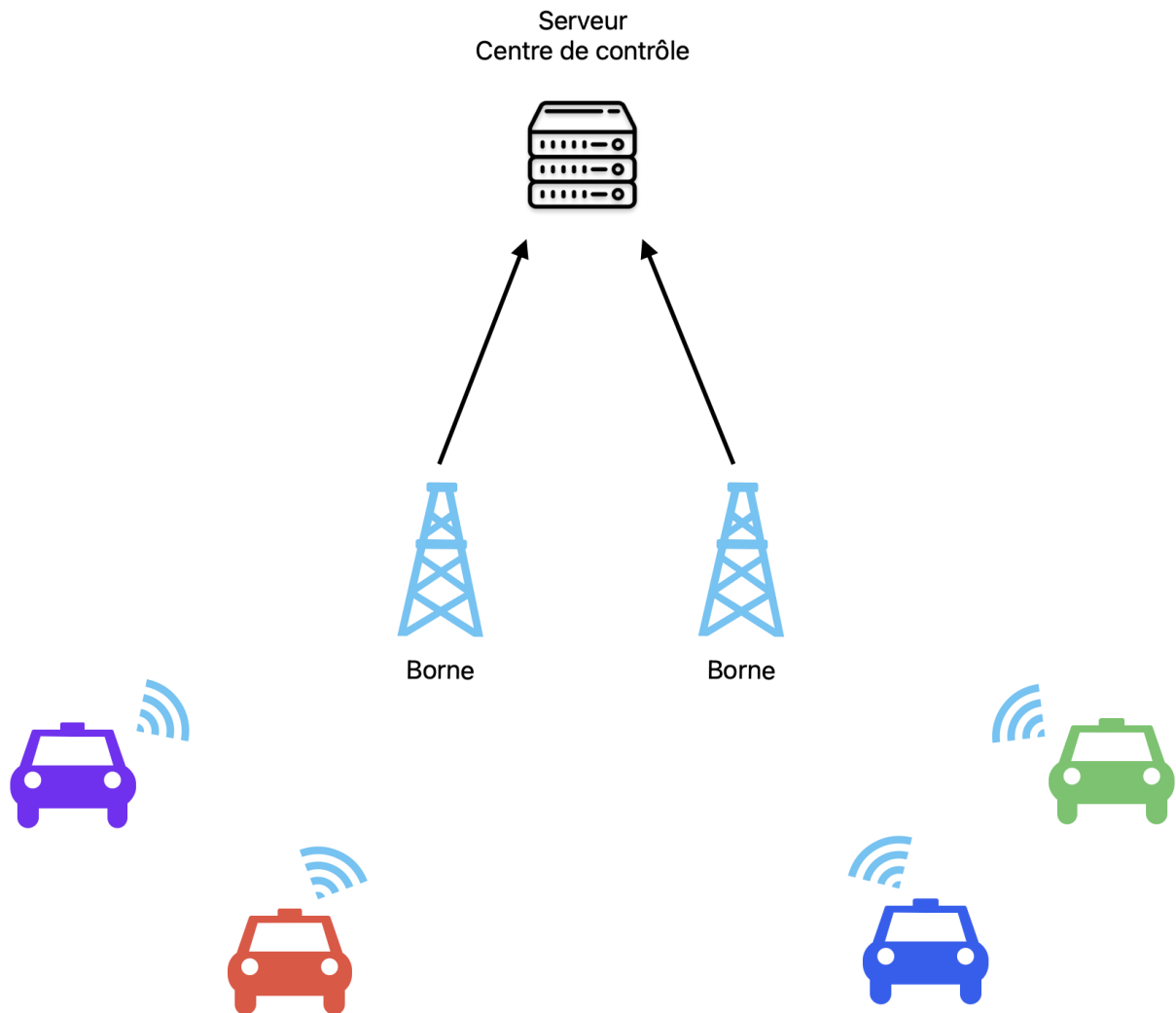


Figure 1 - Schéma de l'architecture du contrôle de trafic

Modèles

Le modèle de transmission choisi est la **communication indirecte par file**.

Le modèle de consommation choisi est le **publish / subscribe**.

Le modèle d'exécution choisi est le **message simple**.

Données recueillies

On aura deux types de données qui seront recueillies.

Le premier type sera des données périodiques. Il s'agira de données qui seront envoyées par les véhicules toutes les secondes. Les données seront les suivantes :

- La vitesse du véhicule qui sera de type « float »
- Les données géographiques qui seront sous la forme de coordonnées GPS (latitude, longitude)
- L'immatriculation du véhicule pour pouvoir identifier la provenance des données

Le deuxième type sera des données ponctuelles. Il s'agira de données qui seront envoyées par les véhicules en fonction d'un événement survenu. Les données seront les suivantes :

- La détection d'un accident qui sera de type « boolean »

Hardware

Un exemple d'hardware qui pourrait être utilisé dans ce projet de contrôle de trafic pourrait être un système embarqué installé dans les véhicules pour collecter les données de vitesse et détecter les accidents. Ce système pourrait inclure :

- Un GPS pour fournir des informations de localisation précises.
- Un capteur d'accélération pour détecter les accidents.
- Un capteur de vitesse pour mesurer la vitesse du véhicule.
- Un module LoRaWAN pour envoyer les données collectées à la borne la plus proche.
- Un microcontrôleur type Esp32 avec une mémoire flash pour stocker quelques données.

Ce système embarqué sera raccordé à la batterie du véhicule.

Applicatif

L'appliquatif de ce projet se compose en trois parties :

- Un programme pour le système embarqué. Situé dans le microcontrôleur, il permettra de détecter les accidents à l'aide des capteurs d'accélération et de vitesse. Il enverra ensuite ces données sous la forme d'un paquet (contenant les données spécifiés dans la partie architecture) à la borne d'acheminement la plus proche.
- Un programme pour les bornes d'acheminement. Il s'occupera de recevoir les données et de les faire parvenir au centre de contrôle.

- Un programme, situé sur le serveur, qui s'occupera de récupérer les données reçues et les stocker en base et les analyser pour faire du monitoring.

Technologies utilisées

Le langage de programmation utilisé sera le Python. Il sera utilisé pour le programme situé sur le serveur et aussi celui situé sur les bornes.

Concernant la représentation des données analysées, nous utiliserons le logiciel de visualisation de données, Grafana. Le logiciel sera hébergé sur le serveur.

Protocole utilisé

Nous utiliserons le protocole MQTT pour la communication entre les bornes d'acheminement et le centre de contrôle.

Sécurité

Sachant la méthode de communication sans fil entre le système embarqué et les bornes d'acheminement, cette partie du système est la plus vulnérable à une attaque et à un vol de données. Cependant LoRaWAN est une norme qui inclut des fonctions de sécurités puissantes.

Les principales fonctions de sécurité incluses dans la norme LoRaWAN sont :

1. Authentification de l'appareil : LoRaWAN utilise une clé d'authentification pour vérifier l'identité des appareils qui se connectent au réseau. Cela permet de s'assurer que seuls les appareils autorisés peuvent accéder au réseau et transmettre des données.
2. Chiffrement des données : LoRaWAN utilise un algorithme de chiffrement pour protéger les données transmises contre la surveillance et l'interception non autorisées. Cela permet de s'assurer que les données sont sécurisées pendant la transmission.
3. Validation de l'intégrité des données : LoRaWAN inclut une validation de l'intégrité des données pour s'assurer que les données reçues n'ont pas été modifiées ou corrompues pendant la transmission.
4. Support de l'authentification mutualisée : LoRaWAN inclut une option d'authentification mutualisée qui permet aux clients de s'authentifier auprès d'un tiers, souvent appelé serveur d'authentification. Cela permet de centraliser la gestion des identités et de faciliter les opérations de gestion des clés.