Seminaire 29/06

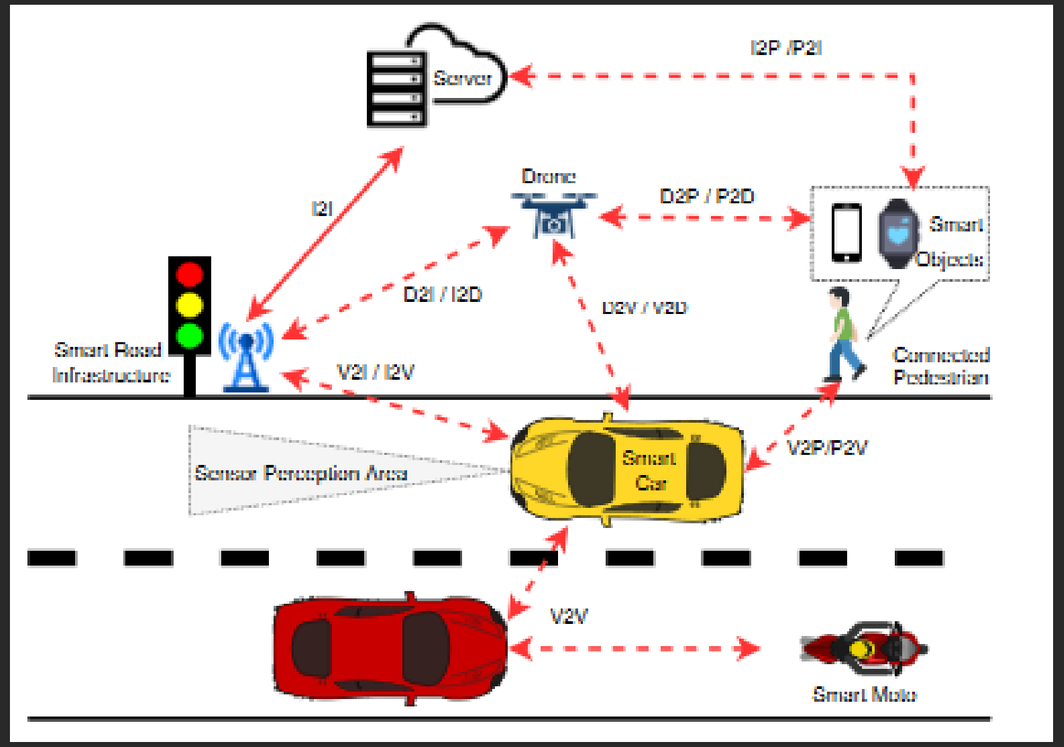
Implémentation d'une couche de sécurité dans un simulateur ITS

Mathias Kautz
Encadrant: Badis Hammi

ITS (intelligent transport system)

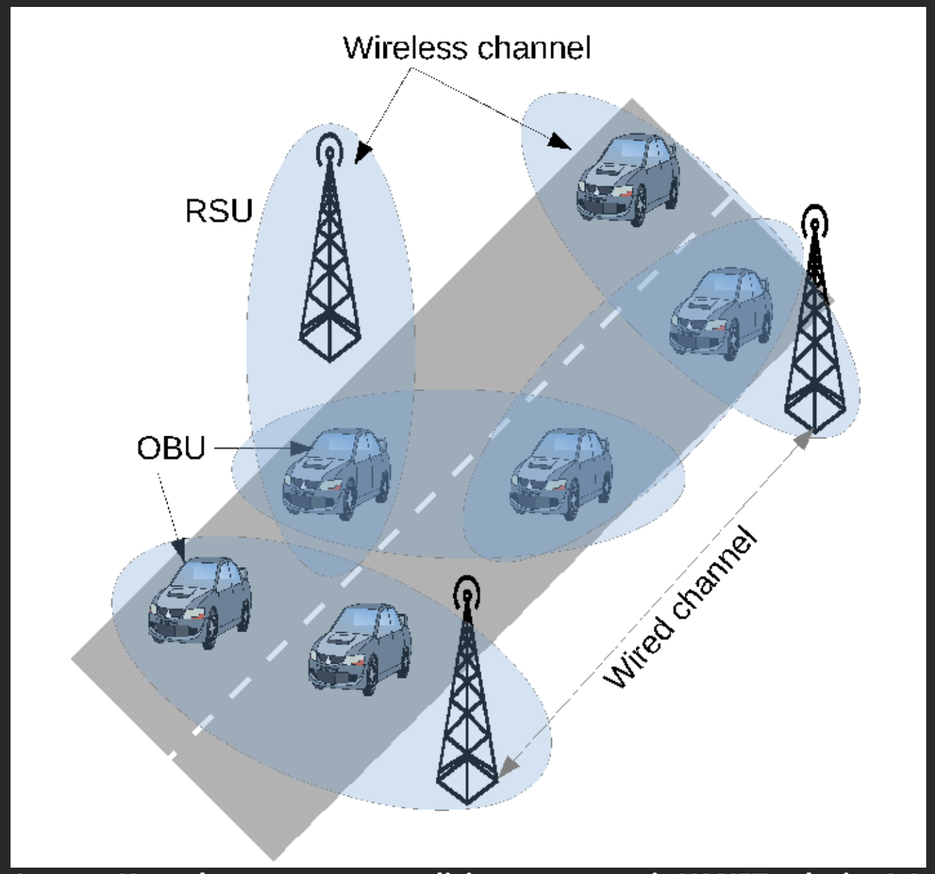
Application des nouvelles technologies au domaine du transport

Dans le contexte d'une ville connectée la présence d'un réseau intervéhiculaire est un point central



Source: PKIs in C-ITS: Security functions, architectures and projects: A survey

C-ITS Network



Source: How close are we to realizing a pragmatic VANET solution? A meta-survey

Réseau composé de deux types de noeuds:

- **Les noeuds RSU (road-side units)**
- **Les noeuds OBU (on-board units)**

Deux types de transmission V2V et V2I

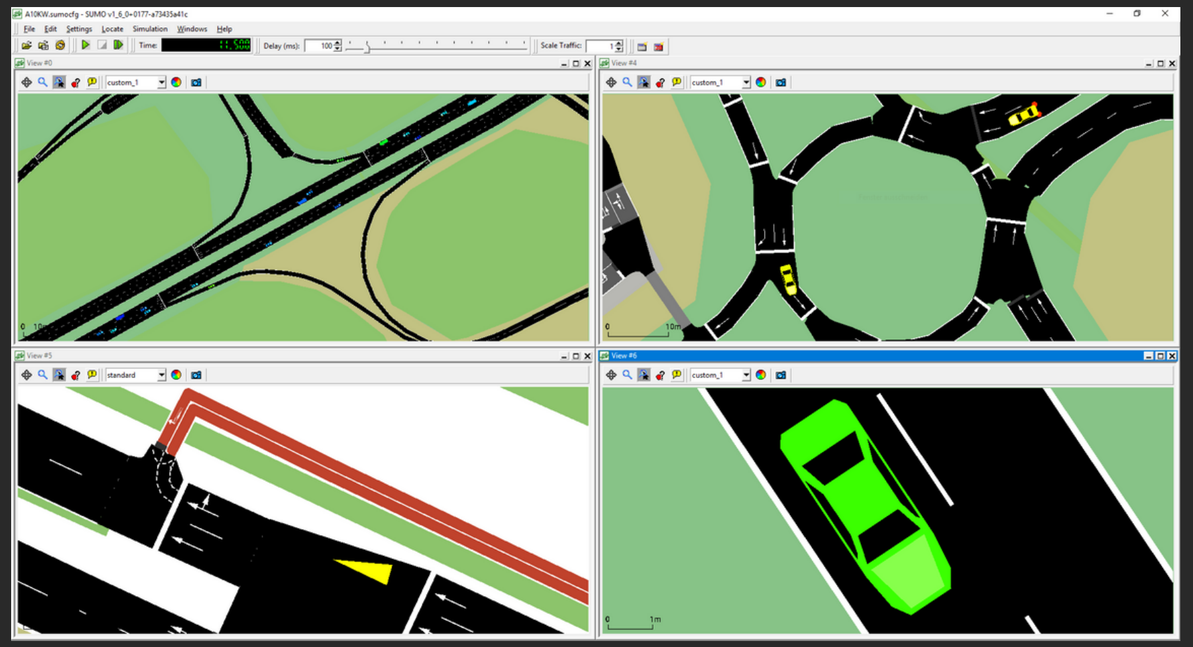
Au départ Ad Hoc mais les solutions récentes se reposent de plus en plus sur des infrastructures existantes (données cellulaires, serveurs centralisés, etc)

Simulateur de réseau

Les entreprises ne peuvent pas se permettre de faire uniquement des tests grandeur nature de leur solution ITS

Il existe donc des simulateurs qui permettent de tester ces solutions dans un environnement numérique

Le but de ce projet est de réfléchir à l'implémentation d'une couche de sécurité dans un simulateur de ce type



Différents simulateurs

Il existe de nombreux simulateur, propriétaire ou open source, qui permettent de simuler des réseaux c-its

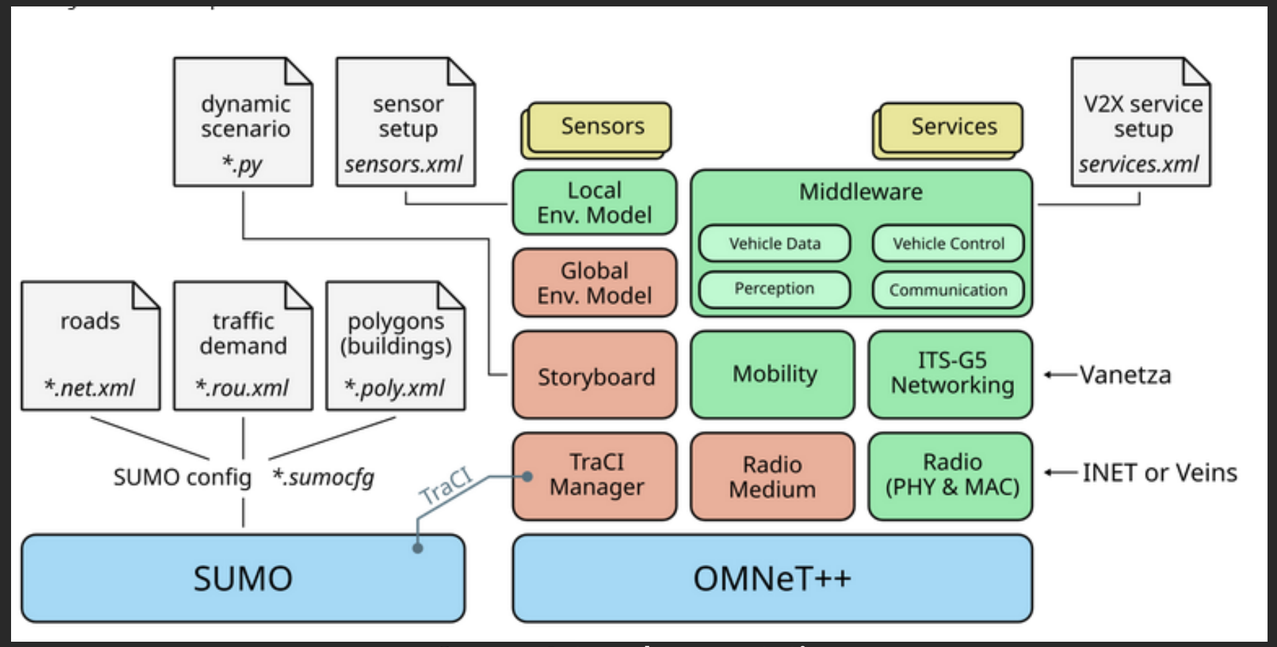
Nous avons choisi de travailler avec artery, car il est moderne, il implémente le standard européen de l'ETSI et surtout, Artery possède déjà des éléments liés à la sécurité.

Artery

Simulateur moderne mettant l'accent sur l'implémentation du standard européen de l'ETSI

Il a commencé comme une extension de Veins qui lui mettait l'accent sur le standard américain WAVES

Il est constitué de deux composant principaux SUMO pour la simulation de trafic et Omnet++ pour la simulation réseaux.



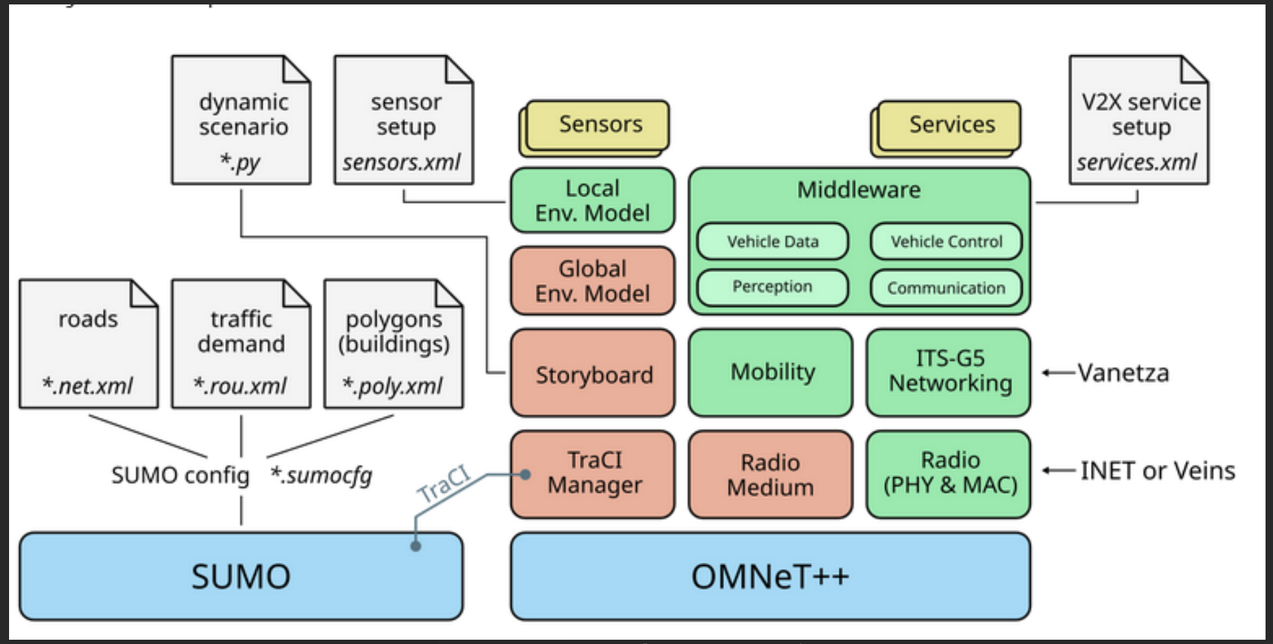
Source: Artery documentation

Lors de son initialisation Artery créé un serveur TRaCI (Traffic Control Interface) qui permet une liaison bidirectionnelle entre Sumo et Omnet++

Middleware

Service : classe dérivant de ITSG5BaseService instanciée dynamiquement par le middleware

Composé de 3 fonctions de base
Initialize : exécuté lors de l'instanciation par le middleware
Trigger : exécuté périodiquement lors de la simulation
Indicate: exécuté lorsque le véhicule reçoit un message



Source: Artery documentation

Les services sont liés aux différents nœuds du réseau en suivant la configuration donnée dans service.xml

SUMO

Simulateur de trafic routier

Basé sur différents fichiers XML pour faire la configuration d'une simulation

Le logiciel permet d'importer des cartes d'OpenStreetMap (OSM) de créer les fichiers de configuration à partir de différents scripts pythons et utilitaires.

J'ai donc pu réaliser une simulation en exportant un morceau d'OSM autour d'EPITA Strasbourg que vous pouvez voir ci-dessus.

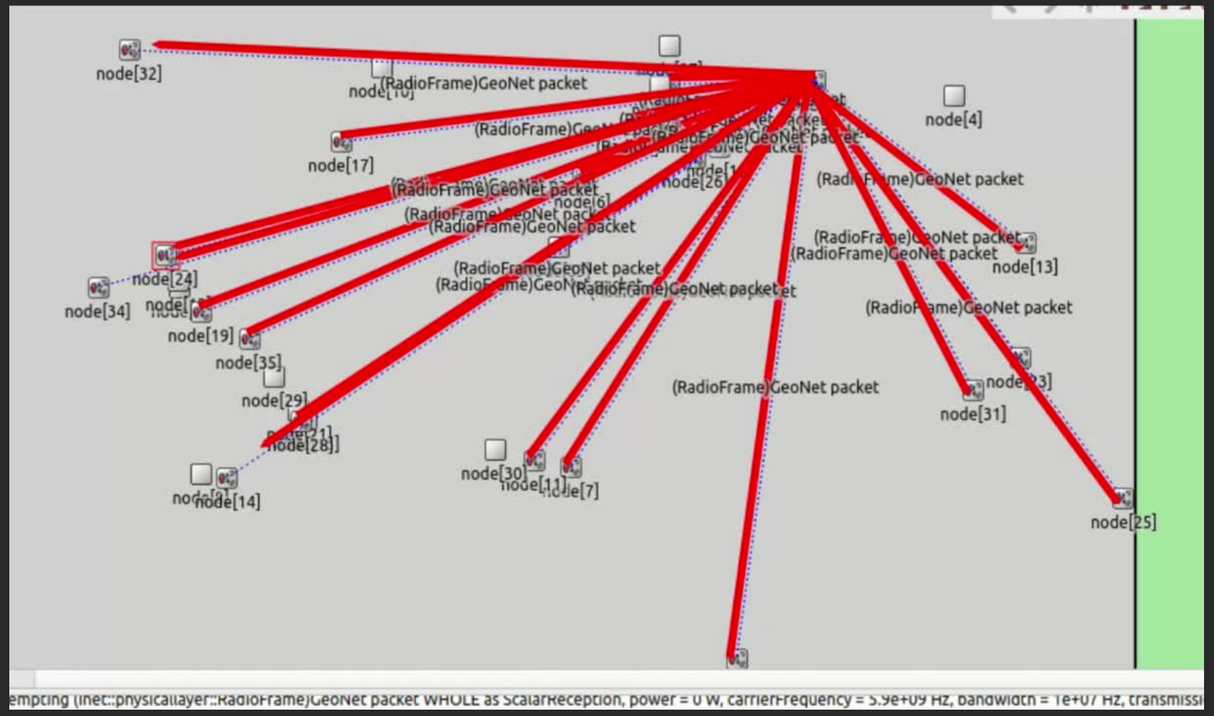
Omnet++

Outil de simulation de réseaux qui permet l'envoie de paquets entre les différents nœuds du réseau.

```
class Txc1 : public cSimpleModule
    {
      protected:
        virtual void initialize() override;
        virtual void handleMessage(cMessage *msg) override;
    };

    Define_Module(Txc1);

    void Txc1::initialize()
    {

        if (strcmp("A", getName()) == 0) {
            cMessage *msg = new cMessage("Hello World!");
            send(msg, "out");
        }
    }

    void Txc1::handleMessage(cMessage *msg)
    {
        send(msg, "out");
    }
```

Source: Documentation d'Omnet++ modifié par moi-même

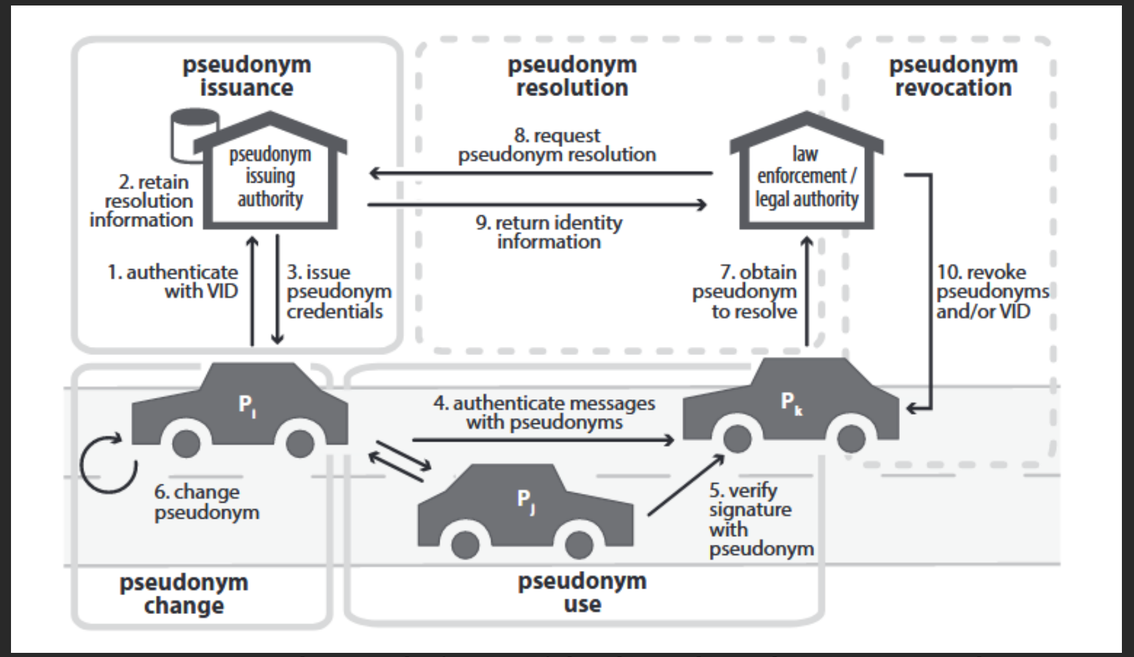
J'ai donc pu, en utilisant des modules fournis par Artery, créer une simulation de réseaux véhiculaire et la couplé à Sumo donnant ce résultat :



La sécurité dans ces systèmes

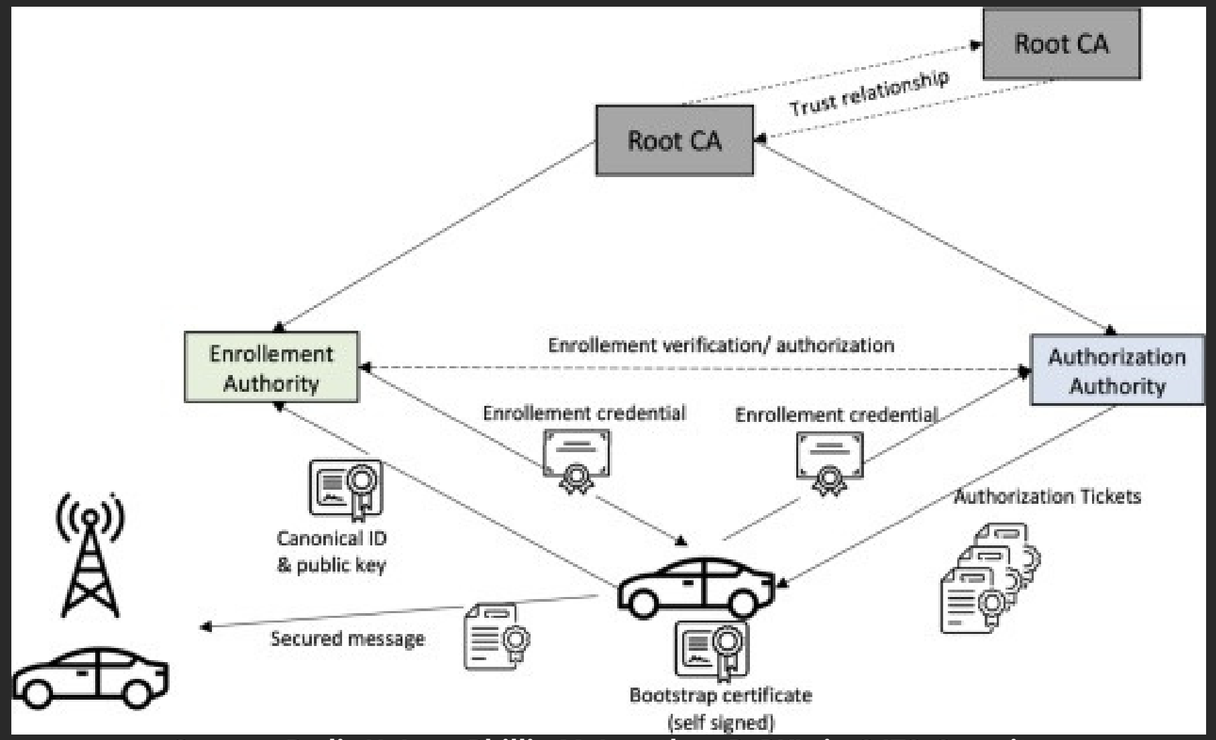
La sécurité est une composante essentielle d'un réseau véhiculaire où une faille de sécurité pourrait avoir une incidence sur la vie des utilisateurs concernés.

Une architecture basée autour d'une PKI est exigé par les différents standard pour apporter une couche de sécurité dans ce réseau



Source : Jonathan P, Florian S, Michael F and Frank K, 2014, Pseudonym Schemes in Vehicular Networks: A survey

Les PKIs dans un réseau ITS



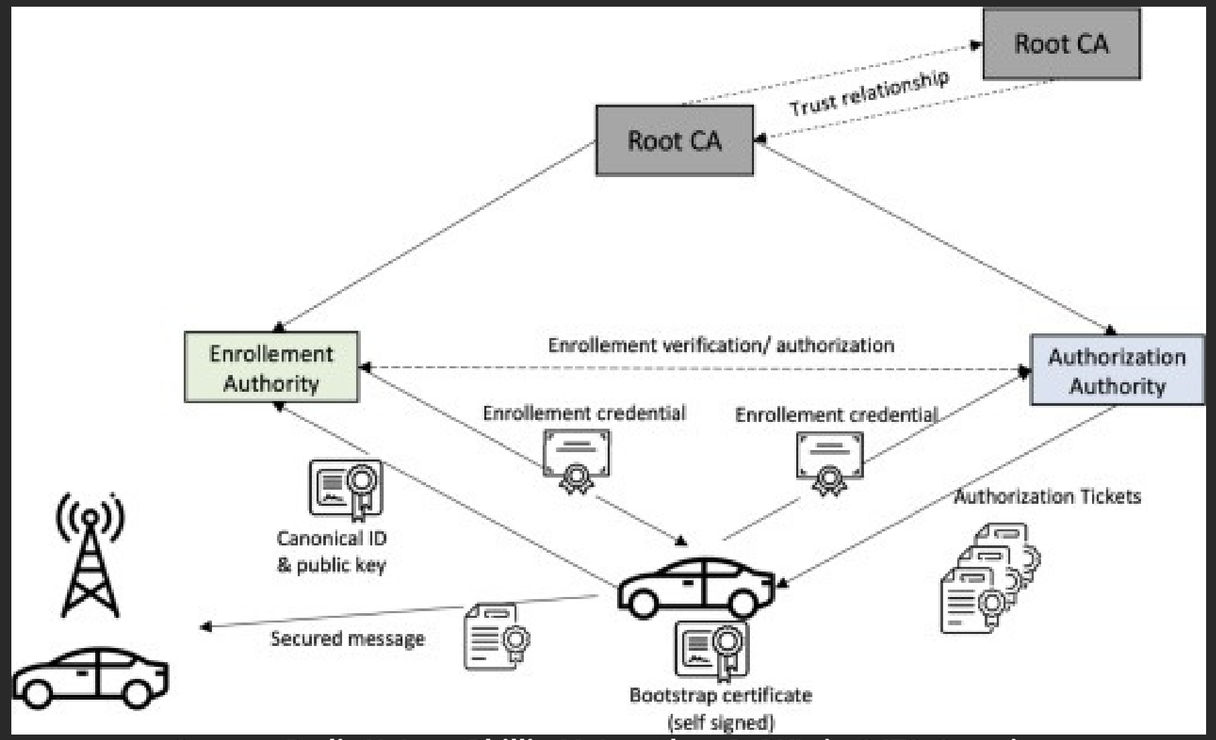
Source : Badis H, Jean-Phillip M, Jonathan P, PKIs in C-ITS: Security functions, architectures and projects: A survey

Il existe plusieurs propositions d'architecture de PKI : j'ai retenu celle de l'ETSI pour cette présentation.

3 types d'autorité dans cette architecture

- Root Certification Authority (RCA)
- Long Term Certification Authority (LTCA)
- Pseudonym Certification Authority (PCA)

Les PKIs dans un réseau ITS



Source : Badis H, Jean-Phillip M, Jonathan P, PKIs in C-ITS: Security functions, architectures and projects: A survey

Root Certification Authority : fournis un certificat autosigné qui permet désigné les autres certificats. C'est la base dans la confiance de cette architecture

Long Term Certification Authority : Fournit un certificat long terme qui donne aux véhicules un droit d'accès au réseau ITS

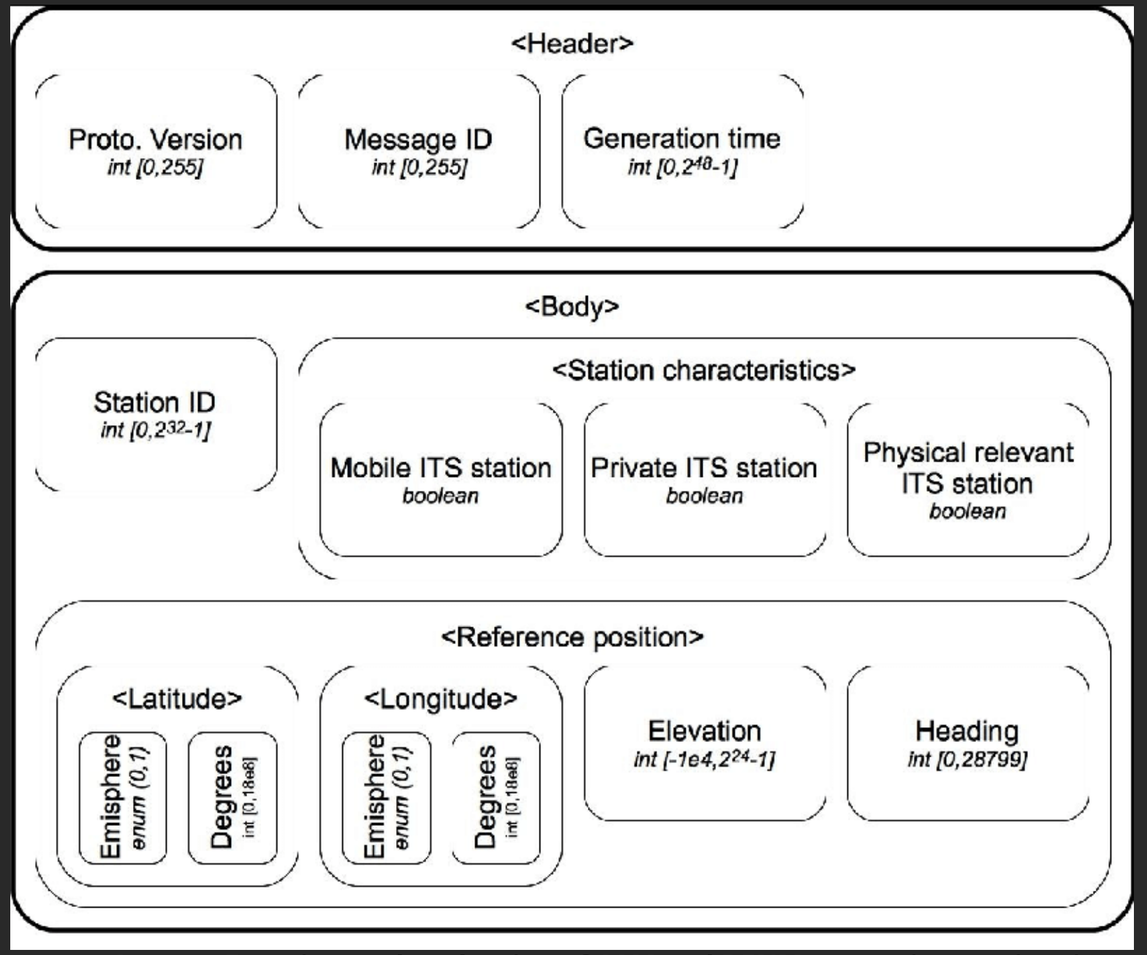
Pseudonym Certification Authority : fournit un certificat donnant des permissions particulières sur le réseau

L'utilisation des certificats

Les messages CAM sont des messages de base du réseau ITS qui sont envoyés très régulièrement à toutes les autres stations ITS proches.

Ils donnent des informations sur la position et la vitesse.

J'ai doté le CaService de la possibilité d'envoyer un Secure Message à la place d'un message CAM simple



Source : Experimental evaluation of CAM and DENM messaging services in vehicular communications

Les secure messages

Utilisé pour envoyé des messages signés et/ou chiffrés dans le réseau ITS

Hachage du certificat -> SHA256
Signature -> ECDSA basé sur la courbe elliptique NIST-P256

Message CAM jamais chiffré toujours signé. Envoi du certificat entier une fois par secondes ou lors de la réception d'une requête

Structure d'un secure message dans le cadre de l'envoi d'un message CAM

CaSignedService

J'ai créé une classe cpp CaSignedService qui dérive de CaService.

Cette classe ré-écrit les fonctions trigger et indicate d'artery tout en utilisant les fonctionnalités de base de CaService pour permettre d'envoyer et de recevoir des secure messages à la place des CAM.

```
CaSignedService::trigger() {
    cam = CaService::createCam();
    securedMessage = createSecuredMessage(cam, certificateProvider.get());
    securedMessage.sign();

    network.send(securedMessage);
}

CaSignedService::indicate(message) {
    if (message.validate()) {
        cam = message.payload;
        updateAwereness(cam);
    }
}
```

Pseudo-code décrivant la logique de la classe CaSignedService

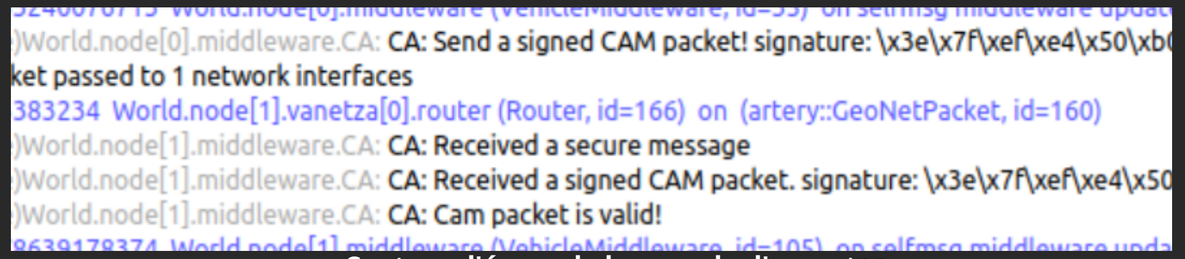
Cette classe s'appuie sur le NaiveCertificateProvider de Vanetza qui n'est pas idéal mais suffisant pour un prototype.

Résultats

Simulation simple : deux voitures sur une route droite qui s'échange des secured messages CAM.

Capture d'écran de la simulation

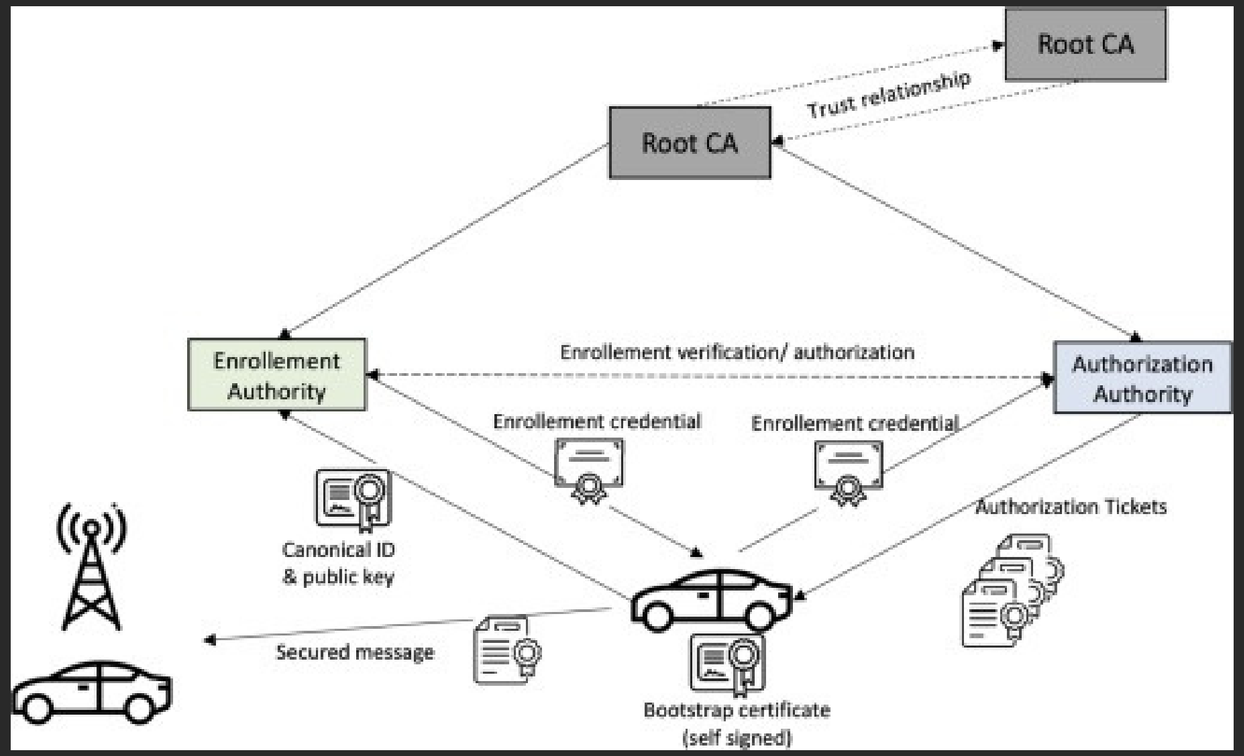
Lorsqu'un message est envoyé ici par node[0] le message est correctement reçu par node[1] avec la signature correspondante et ce message est valide.



Capture d'écran de la console d'omnet++

Ce qu'il reste à faire

- Ajouter des nœuds RSU qui contiennent un dépôt de certificat et permettre aux véhicules d'effectuer des requêtes de certificat sur ces dépôts
- Implémenter l'architecture de PKI proposé avec les différentes autorités et requêtes de certificat



Source : Badis H, Jean-Phillip M, Jonathan P, PKIs in C-ITS: Security functions, architectures and projects: A survey

Bibliographie

- Michael Lee, Travais Atkison, 2021, VANET Applications: Past, Present, and Future
- Badis H, Jean-Philippe M, Jonathan P, 2022, PKIs in C-ITS: Security functions, architectures and projects: A survey
- Agachai S, H.W. Ho, 2017, Smarter and more connected: Future intelligent transportation system
- Jonathan P, Florian S, Michael F and Frank K, 2014, Pseudonym Schemes in Vehicular Networks: A survey
- José S, Fernando P, Antonio M, Antonio F. S., Experimental evaluation of CAM and DENM messaging services in vehicular communications
- Artery Documentation, http://artery.v2x-research.eu/
- Omnet++ documentation, https://omnetpp.org/documentation/
- Vanetza documentation, https://www.vanetza.org/
- Institut européen des normes de télécommunications, ETSI TS 103 096
- Institut européen des normes de télécommunications, ETSI EN 302 637-2
- Institut européen des normes de télécommunications, ETSI TS 102 965