

Séminaire 03/07

Implémentation d'une couche de sécurité dans un simulateur ITS

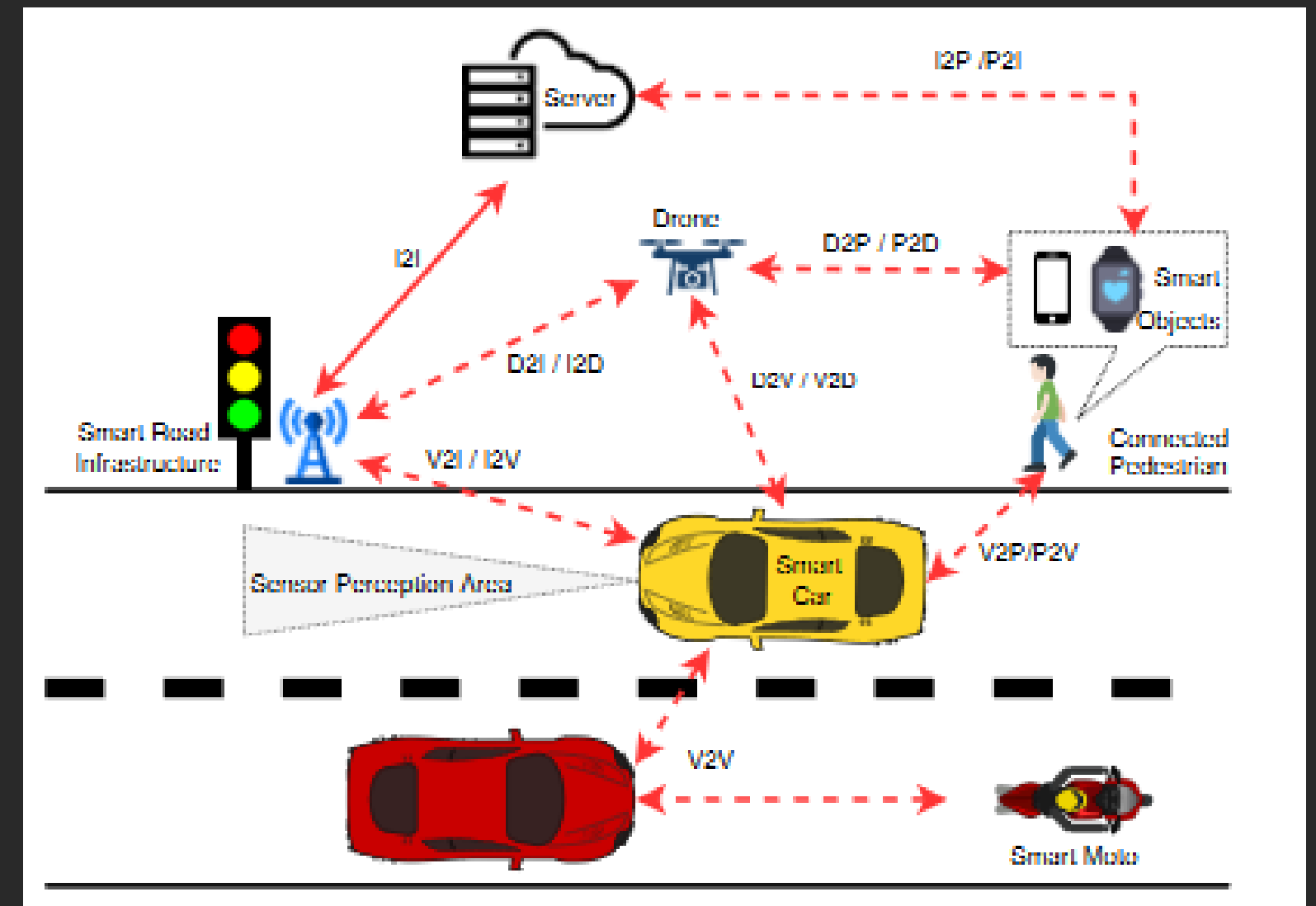


Mathias Kautz
Encadrant: Badis Hammi

ITS (intelligent transport system)

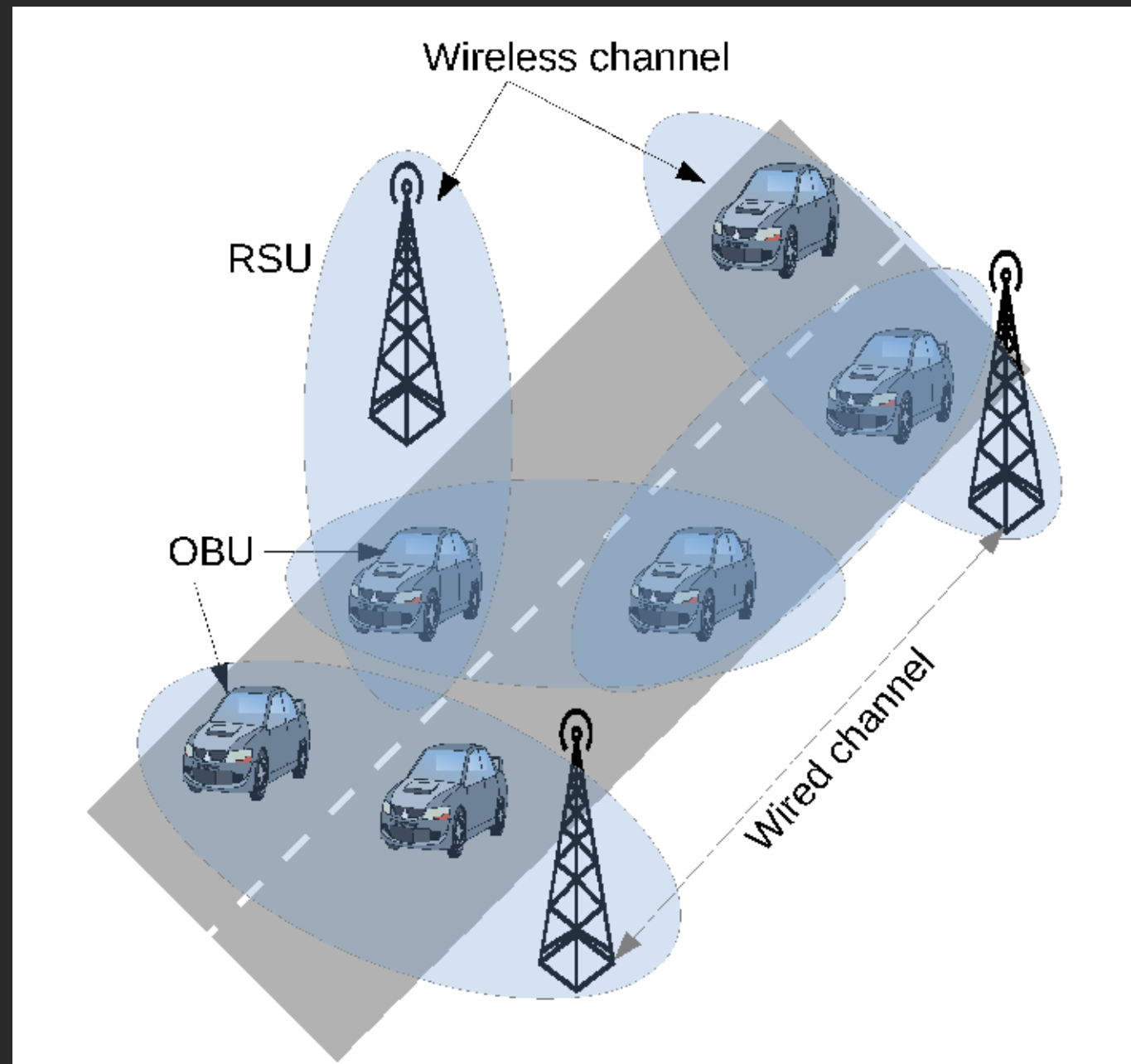
Application des nouvelles technologies au domaine du transport

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



Réseau composé de deux types de noeuds:

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

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

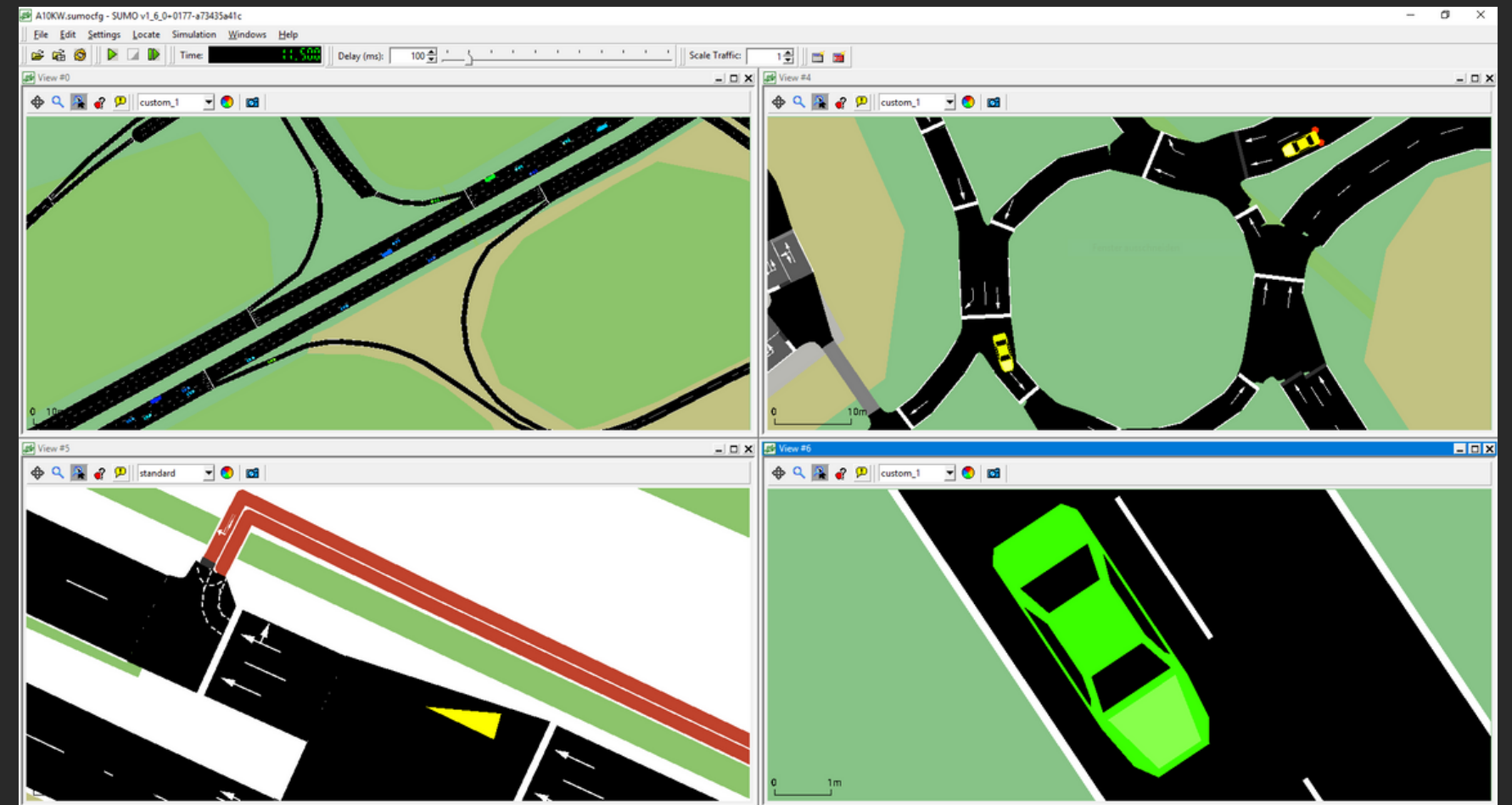
Source: How close are we to realizing a pragmatic VANET solution? A meta-survey

Simulateur de réseaux

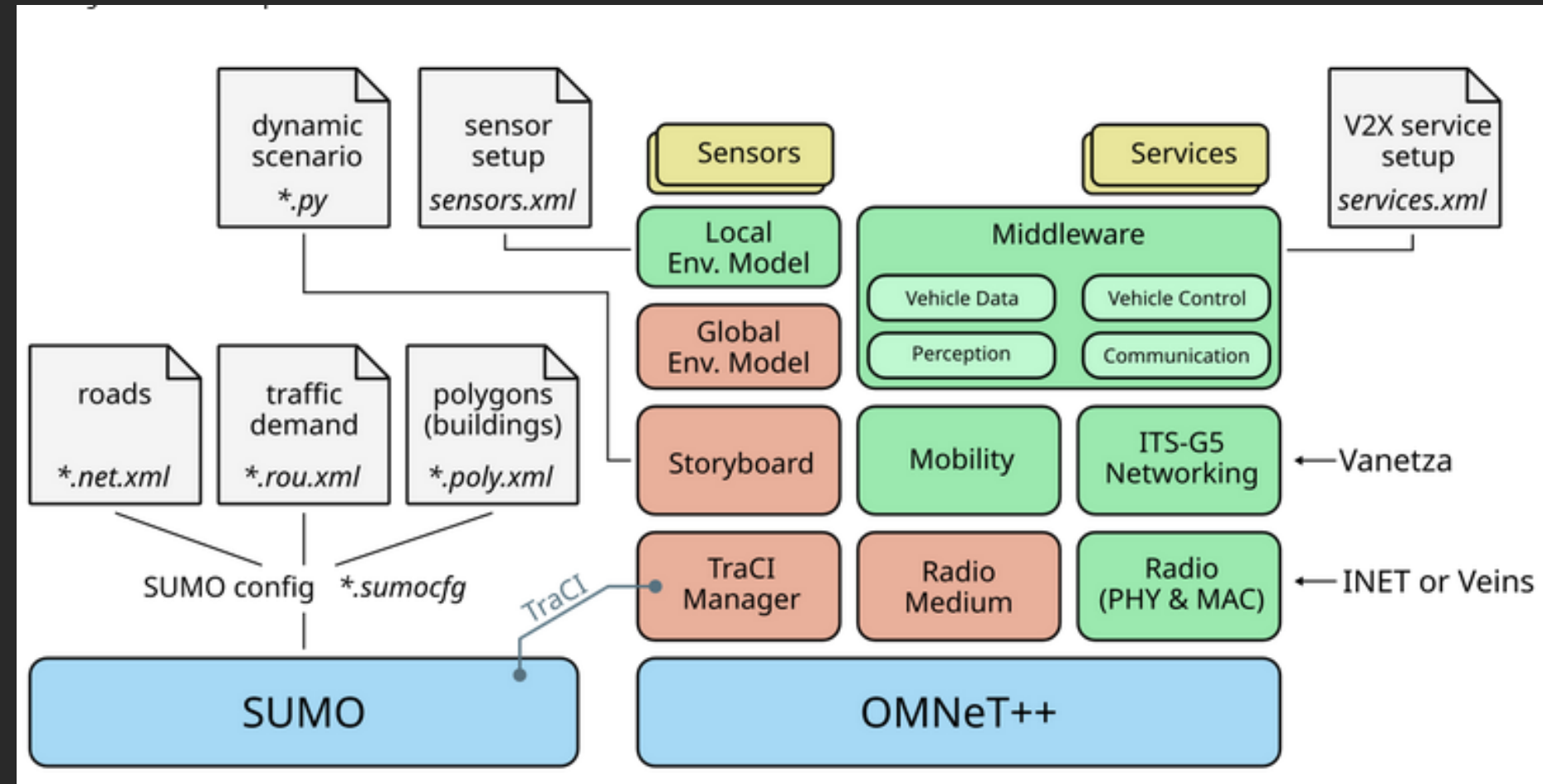
Tests grandeur nature = trop chère

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

Notre projet: réfléchir à l'implémentation d'une couche de sécurité dans un simulateur de ce type



Artery

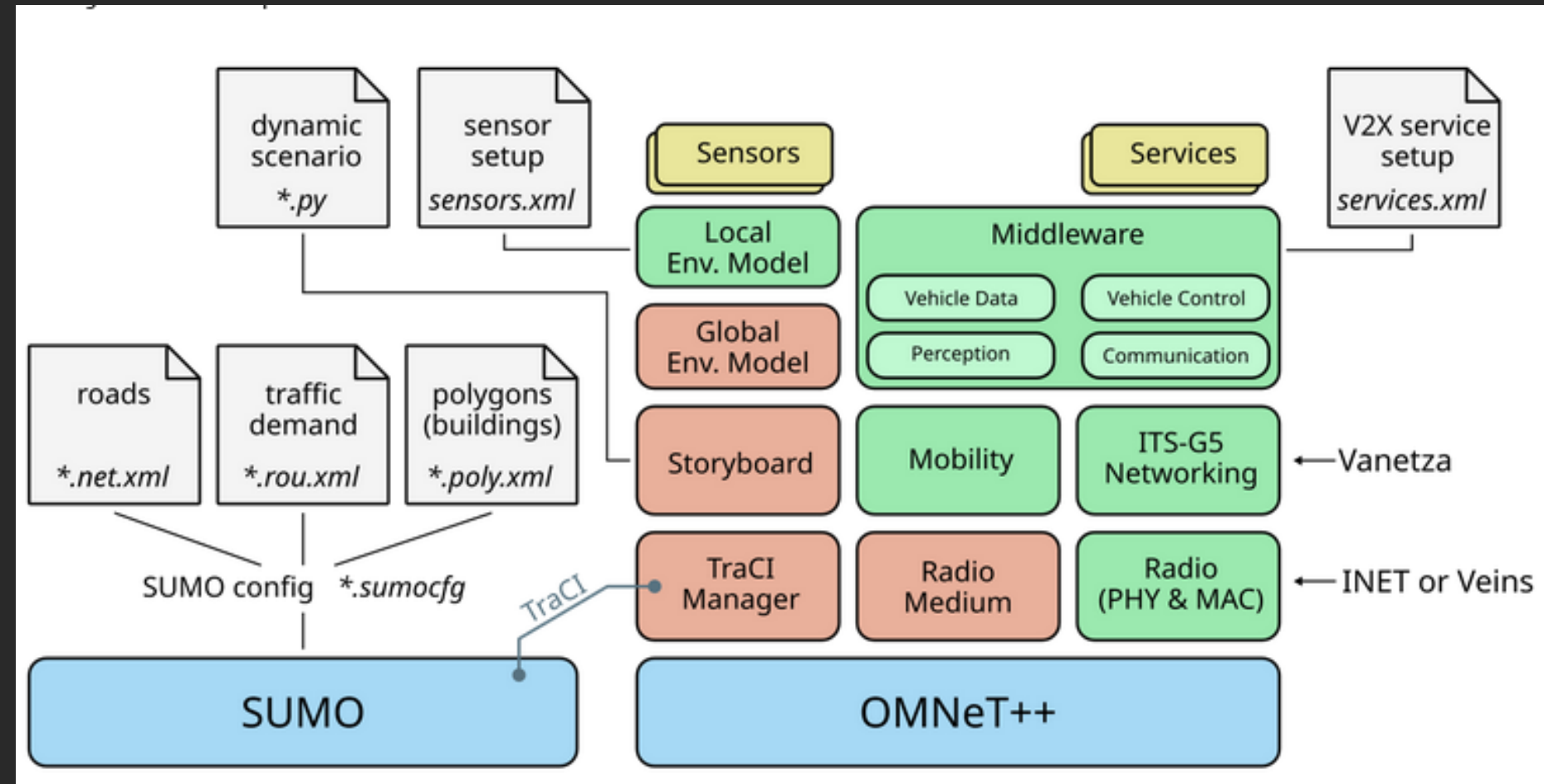


Source: Artery documentation

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

- Extension de Veins
- Open source
- Standard Européen
- Rapide
- Vanetza

Middleware



Source: Artery documentation

Composé de 3 fonctions de base

- Initialize
- Trigger
- Indicate

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

Service : classe dérivant de ITSG5BaseService instanciée dynamiquement par le middleware

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.



Omnet++

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

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 :

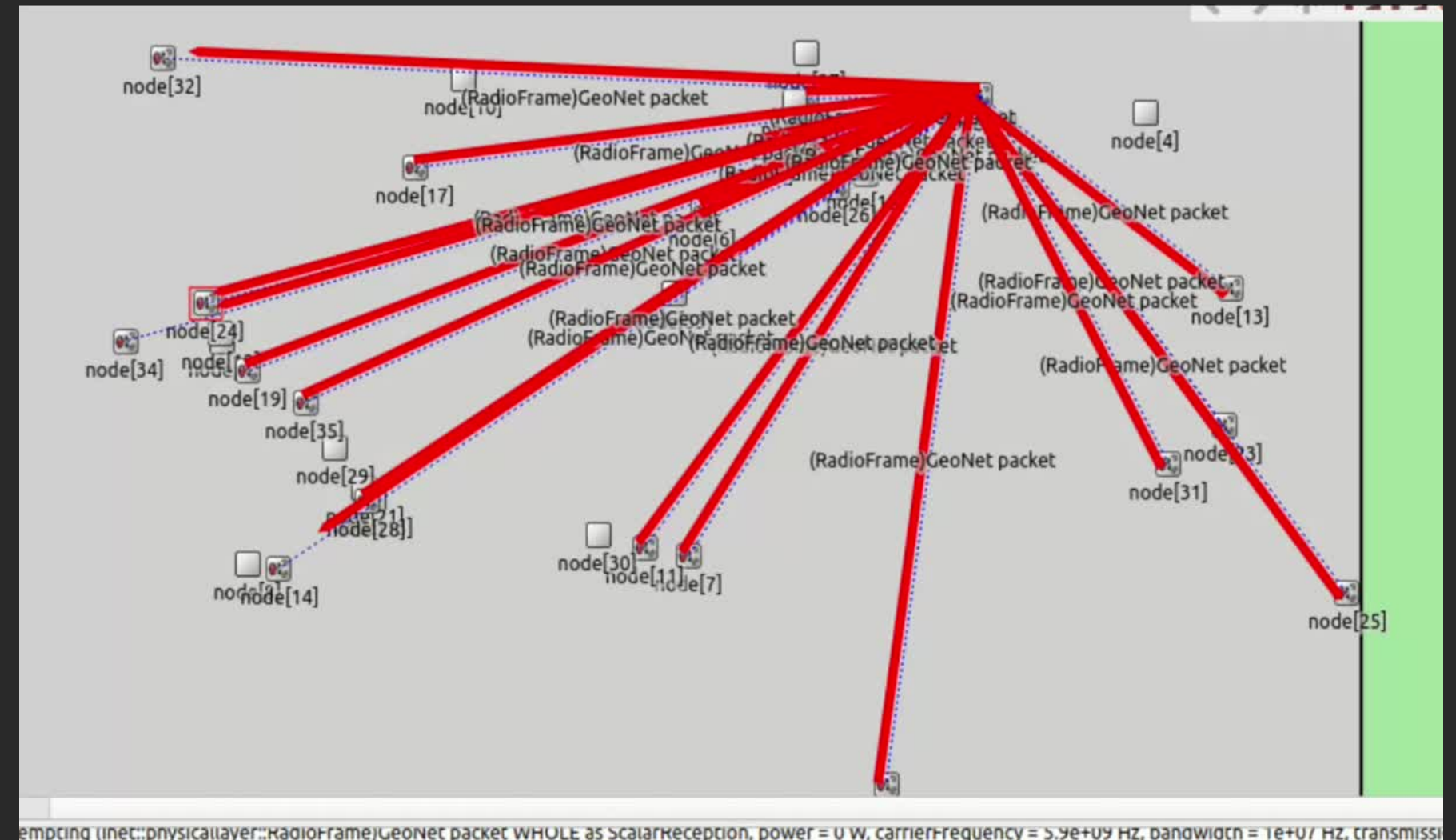
```
class Txcl : public cSimpleModule
{
protected:
    virtual void initialize() override;
    virtual void handleMessage(cMessage *msg) override;
};

Define_Module(Txcl);

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

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

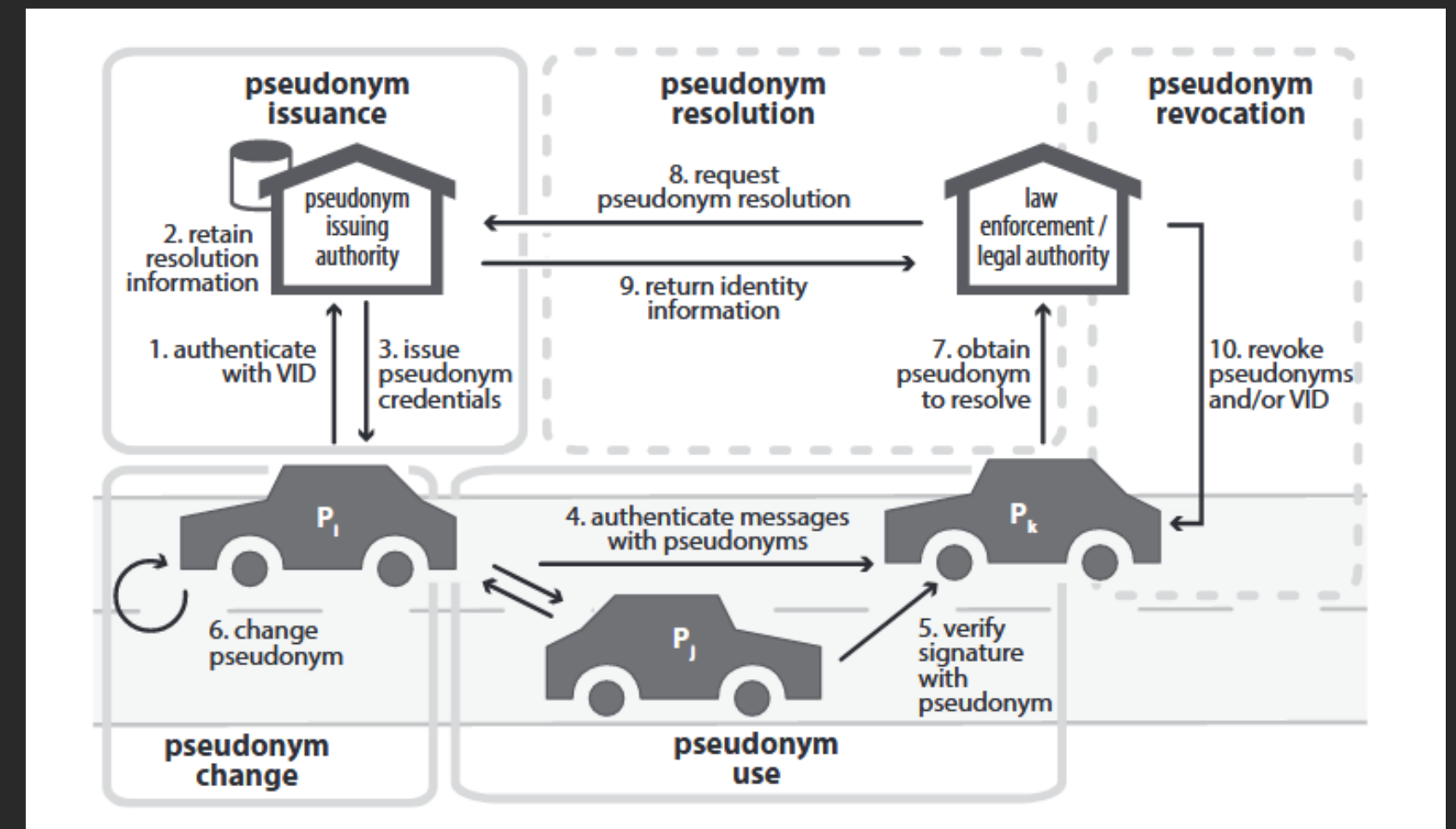
Source: Documentation d'Omnet++ modifié par moi-même



La sécurité dans ces systèmes

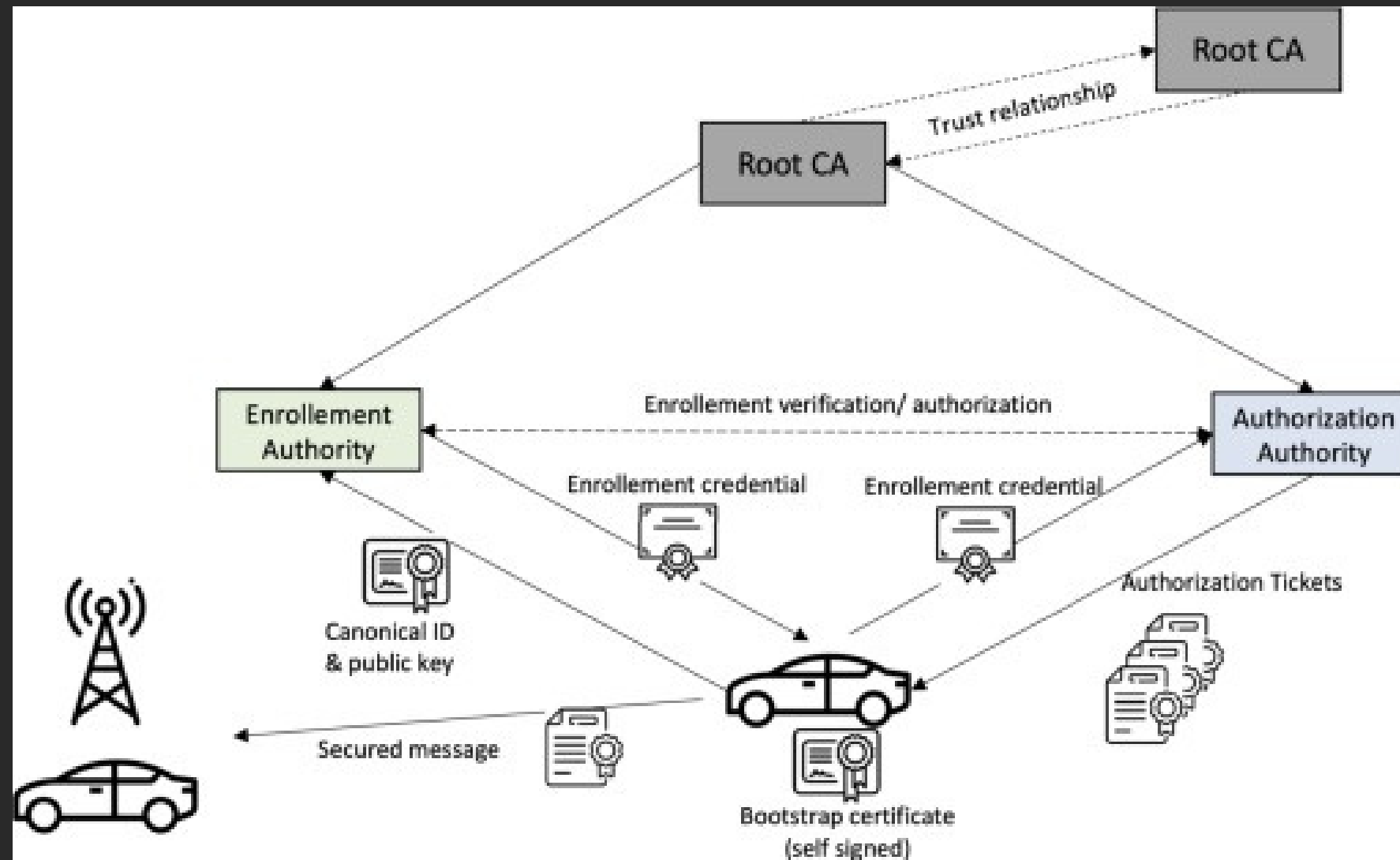
La sécurité est une composante essentielle d'un réseau véhiculaire où une faille de sécurité pourrait avoir une incidence sur la vie des utilisateurs concernés.

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 :

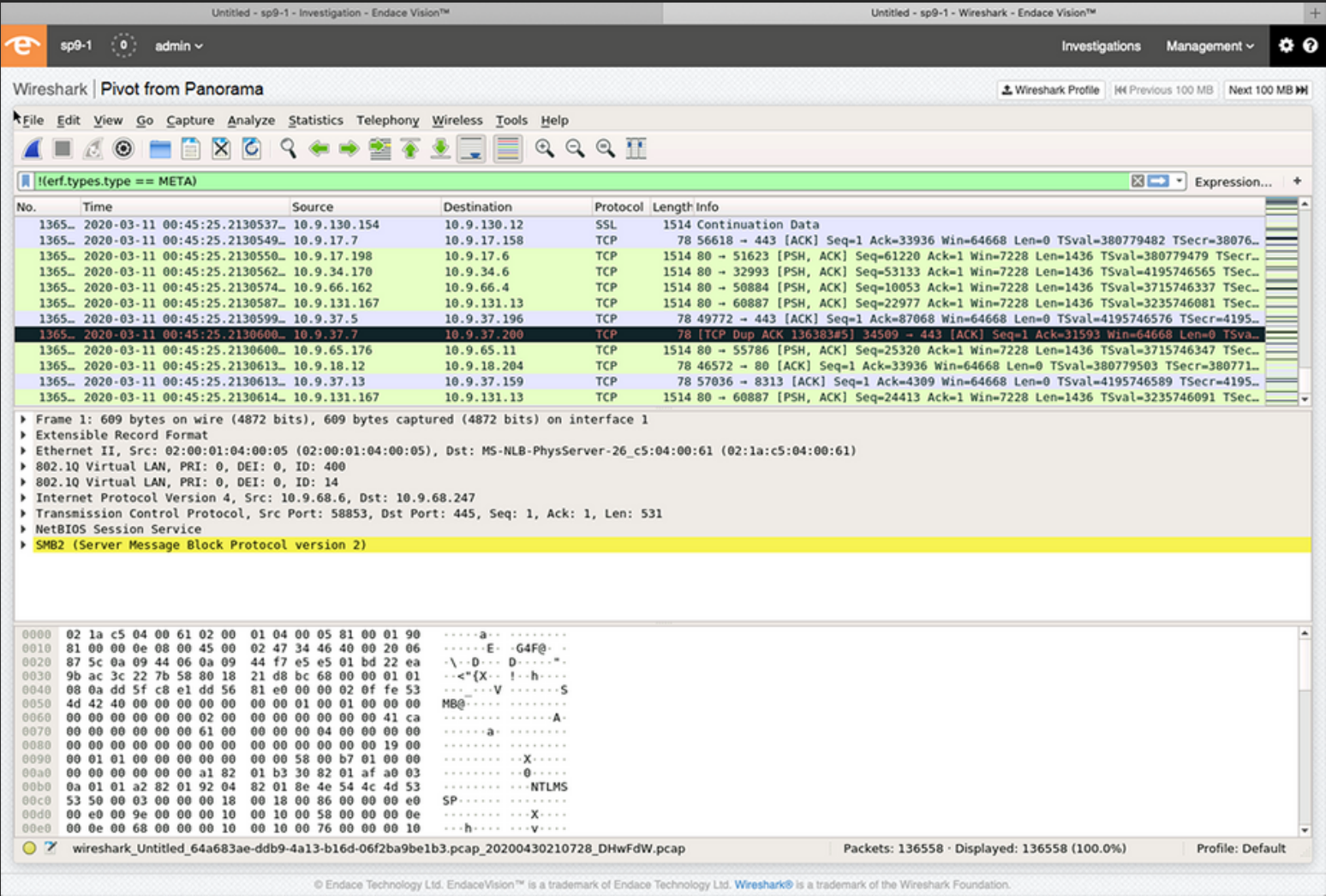
- Root Certification Authority (RCA)
- Long Term Certification Authority (LTCA)
- Pseudonym Certification Authority (PCA)

PcapItsRecorder

Pcap: format de fichier d'enregistrement de packets réseaux (Wireshark)

Recorder inexistant dans artery

Ouf! Packet reader existant sur Wireshark



StaticCertificateLoader

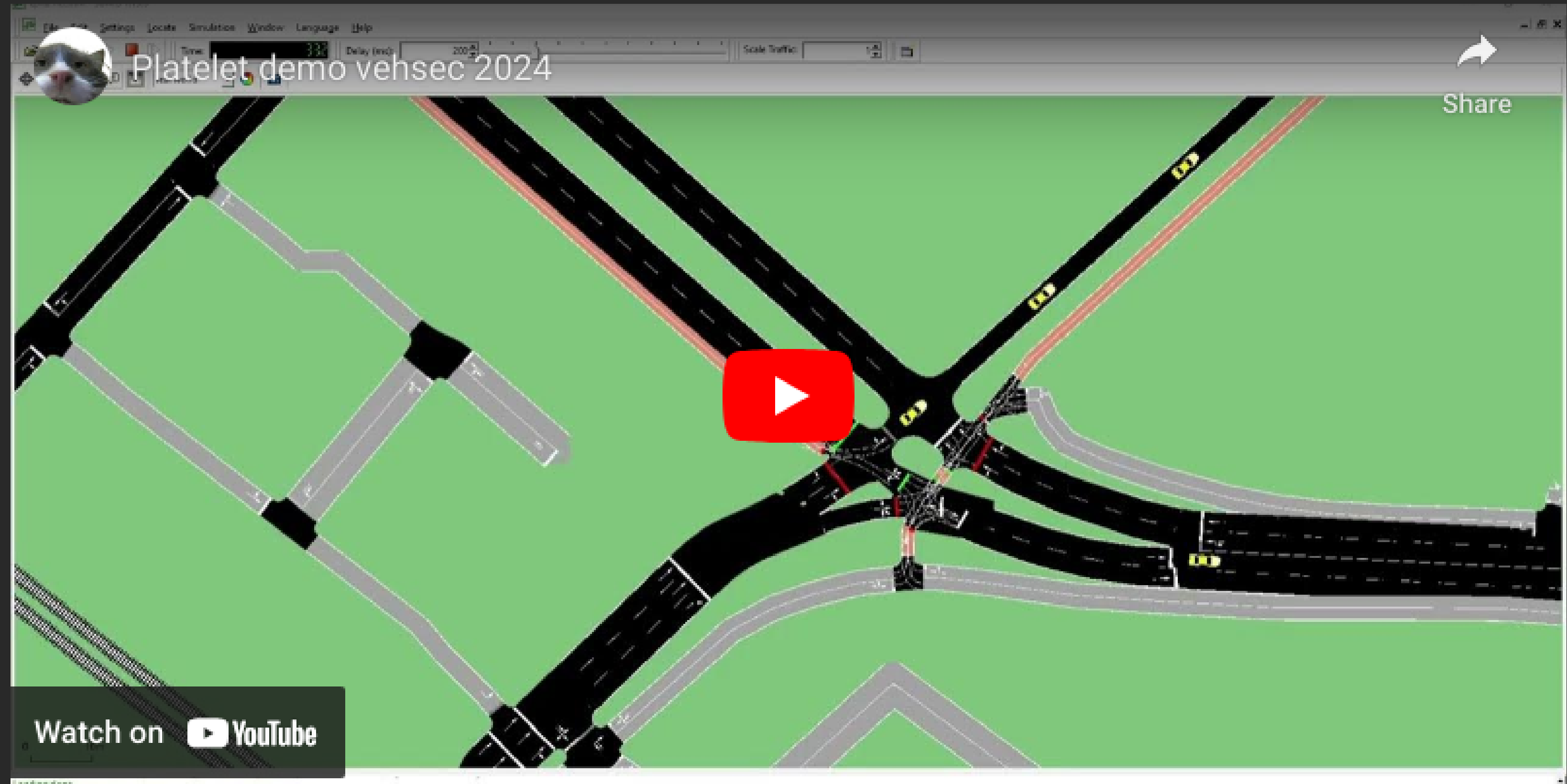
Aucun module de loading de certificat sur Artery

Loader basé sur des fichier certificat généré en amont de la simulation

Garanti l'intégrité et l'authenticité du certificat chargé



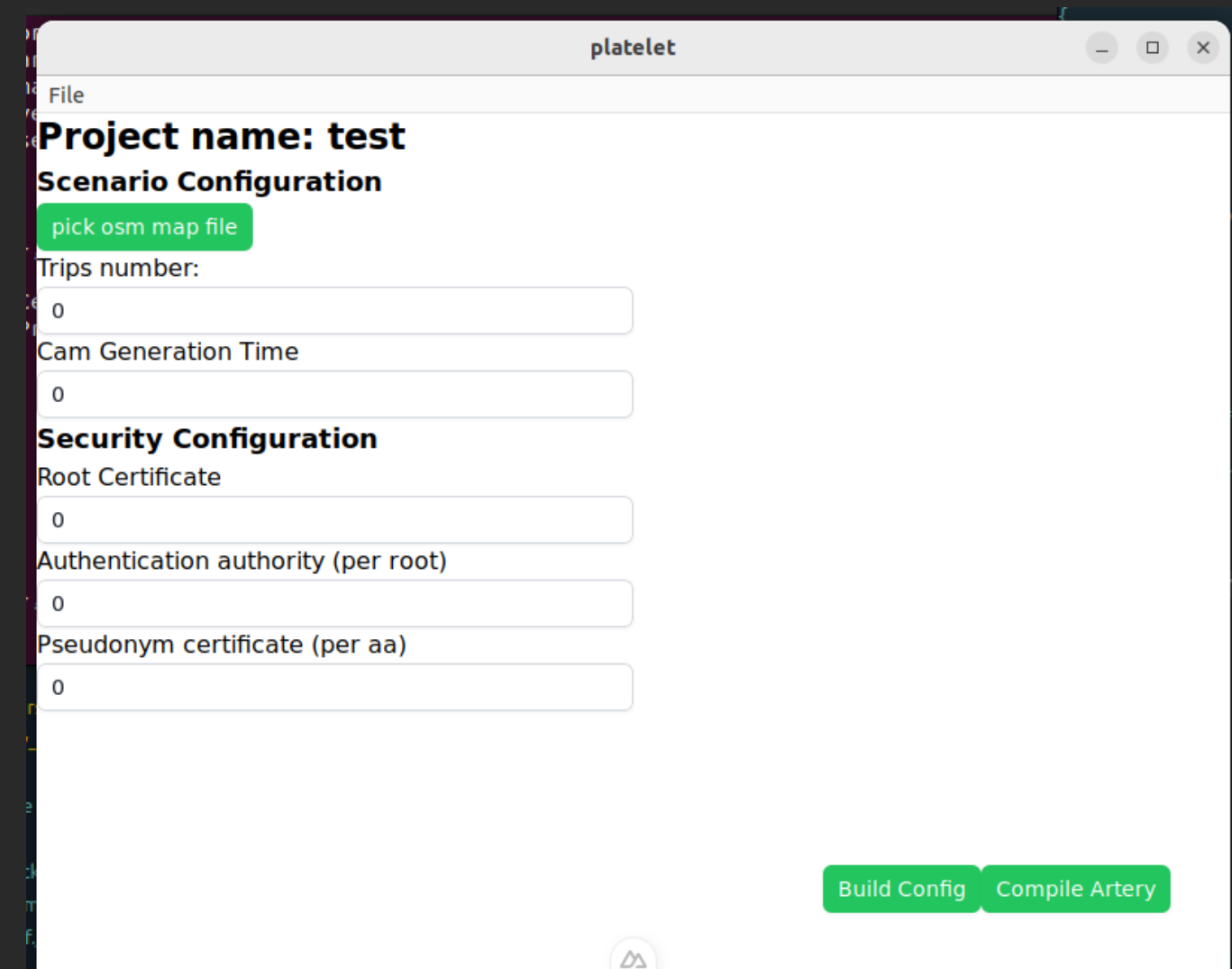
Résumé



Platelet

Objectif : Réunir tout les outils au même endroit

- App Tauri (Rust + Vue3 + Tailwind)
- Créer/Modifier/Supprimer des scénarios
- Config de base (omnetpp, service, etc.)
- Config sécurité



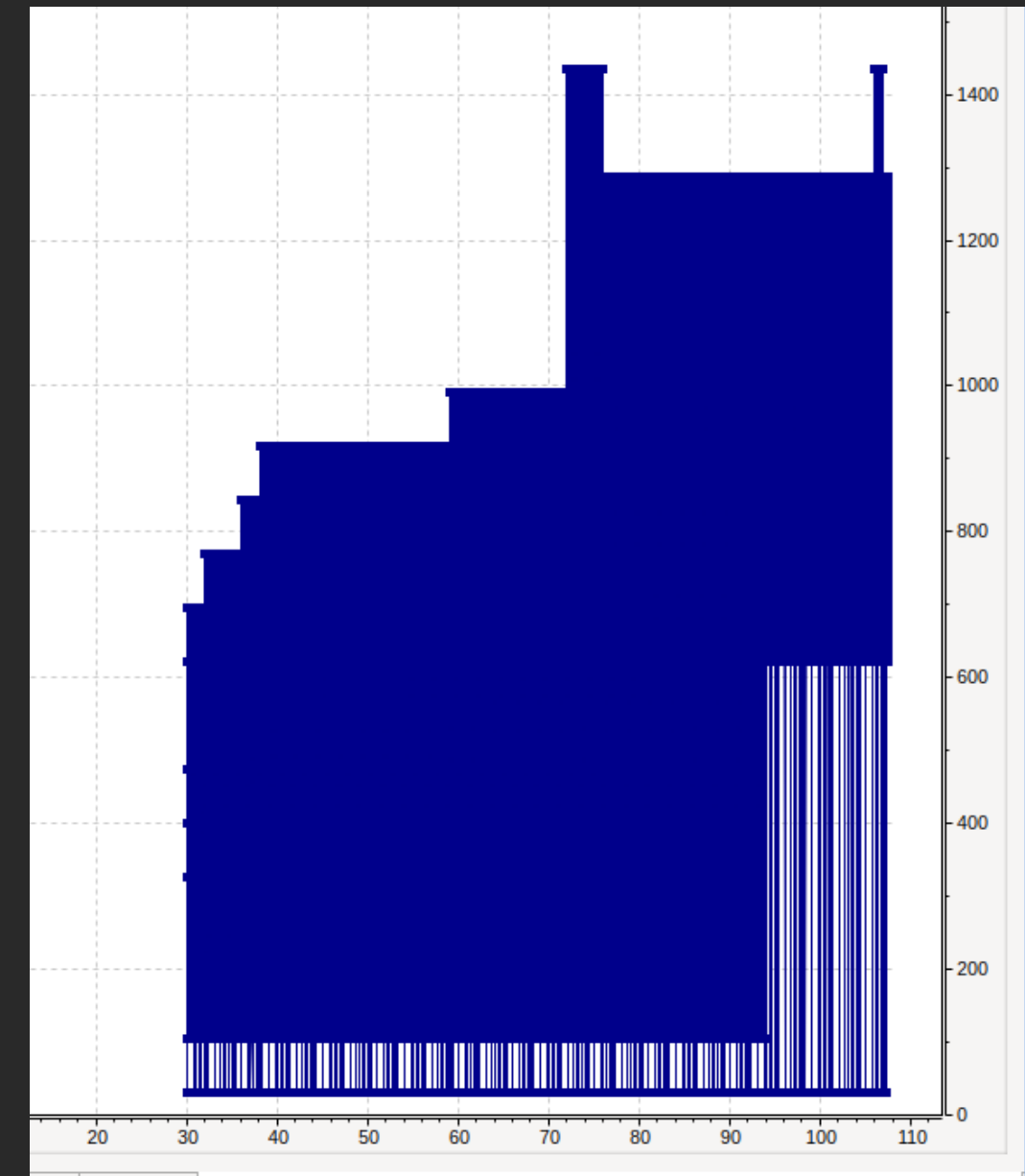
The screenshot shows a web application window titled "platelet". It contains a "File" menu and a "Project name: test" label. Below this is a "Scenario Configuration" section with a green button labeled "pick osm map file". There are two input fields: "Trips number:" with a value of "0" and "Cam Generation Time" with a value of "0". Below these is a "Security Configuration" section with three input fields: "Root Certificate" with a value of "0", "Authentication authority (per root)" with a value of "0", and "Pseudonym certificate (per aa)" with a value of "0". At the bottom right, there are two green buttons: "Build Config" and "Compile Artery".

DDOS

**Simulation d'une attaque DDOS grâce à
Platelet**

**Scénario “exemple” pour le futur
papier**

Prochaine étape l'attaque Sybil



Bibliographie

- Michael Lee, Travis 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