2.7 Etudes transverses

Emilie PETIT - DGITM

Co-financed by the Connecting Europe Facility of the European Union

The contents of this publication are the sole responsibility of InDiD Consortium and do not necessarily reflect the opinion of the European Union.

Qu’est ce que la sous activité 2.7 ?

- *“En lien avec les processus techniques sus mentionnés, et pour résoudre les principaux challenges techniques des C-ITS, les partenaires InDID travailleront sur les sujets techniques transversaux.”*

- A2.7. 1: Nouvelles technologies et hybridation (SG/LTE etc.)
- A2.7.2: Cartographie digitale haute définition
- A2.7.3: Sécurité
- A2.7.4: Amélioration de l’infrastrucure des gestionnaires routiers pour les besoin des véhicules connectés et automatisés

- Le rapport de Milestone 36 établit le bilan du 2.7

GT	Nombre de livrables
2.7.1	4
2.7.2	5
2.7.3	6
2.7.4	12
	27

Co-financed by the Connecting Europe Facility of the European Union

2.7.1 Nouvelles technologies et hybridation (C-V2X & ITS-G5) pour les C-ITS

Toufik AHMED

Badreddine Yacine YACHEUR

INP Bordeaux - LABRI

Co-financed by the Connecting Europe Facility of the European Union

The contents of this publication are the sole responsibility of InDiD Consortium and do not necessarily reflect the opinion of the European Union.

Contexte

- Les communications V2X utilisent majoritairement l'ITS-G5, une technologie de courte portée basée sur le standard IEEE 802.11p.
  Définition d'une nouvelle norme plus performante, IEEE 802.11bd.

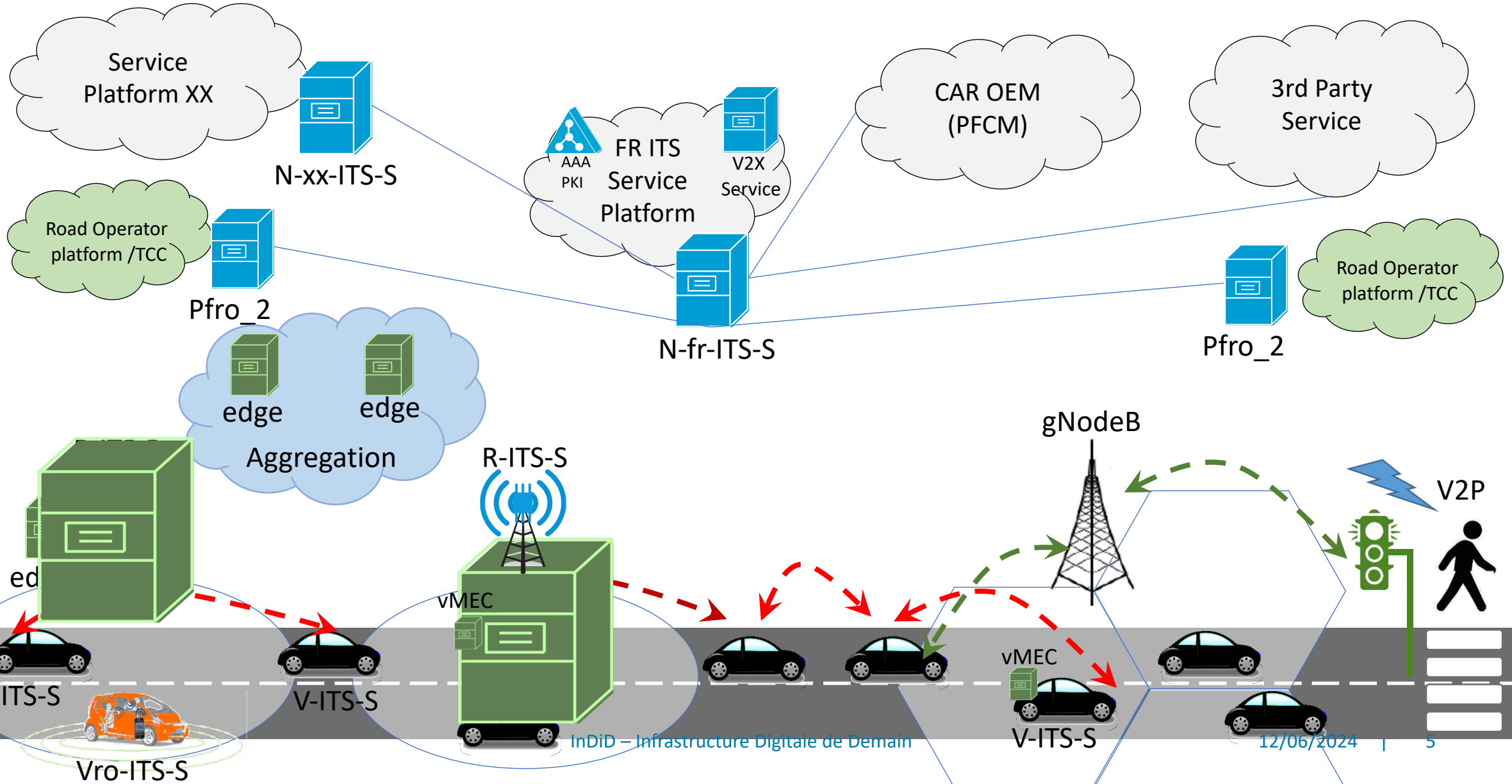
- Un intérêt croissant pour les réseaux cellulaires tels que LTE et 5G (C-V2X)
  Offrir une faible latence, des informations de positionnement très précises, et un débit élevé.

- Evolution des services C-ITS et de leurs besoins
  Moins de latence, plus de bande passante, et une haute fiabilité.

- Besoin d'une source de calculs plus proche du véhicule.
  Définition de la notion de serveur EDGE proche de l'unité de bord de route ou dans le véhicule.

Co-financed by the Connecting Europe Facility of the European Union

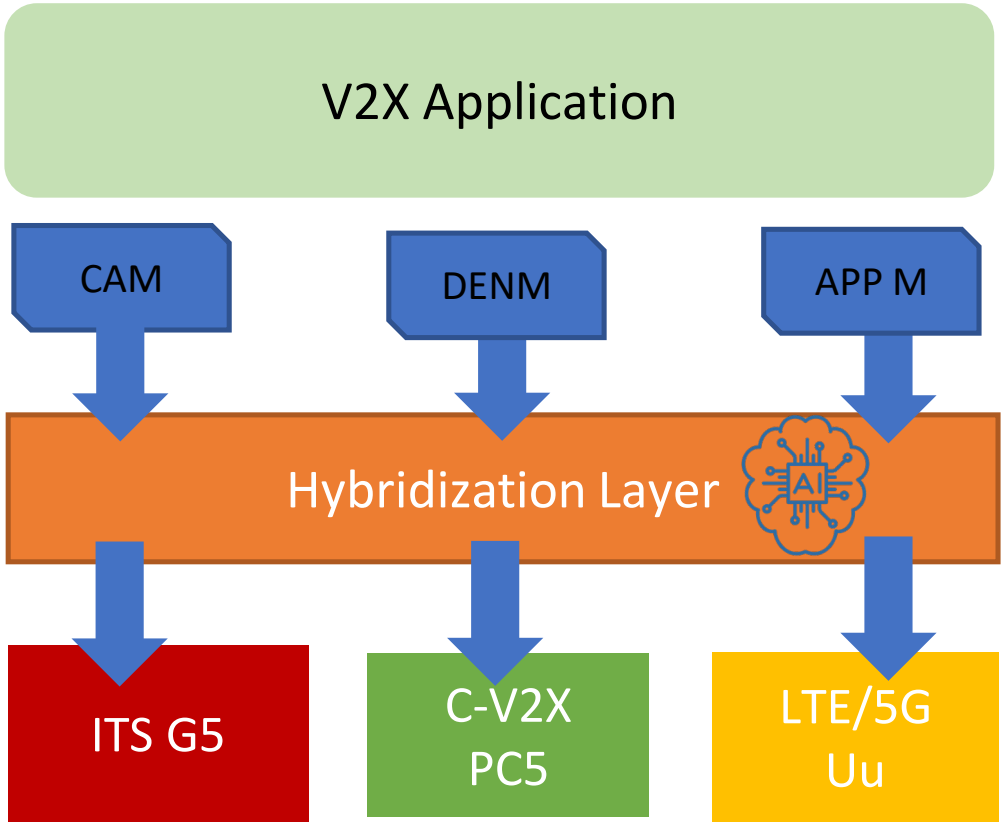
Architecture globale



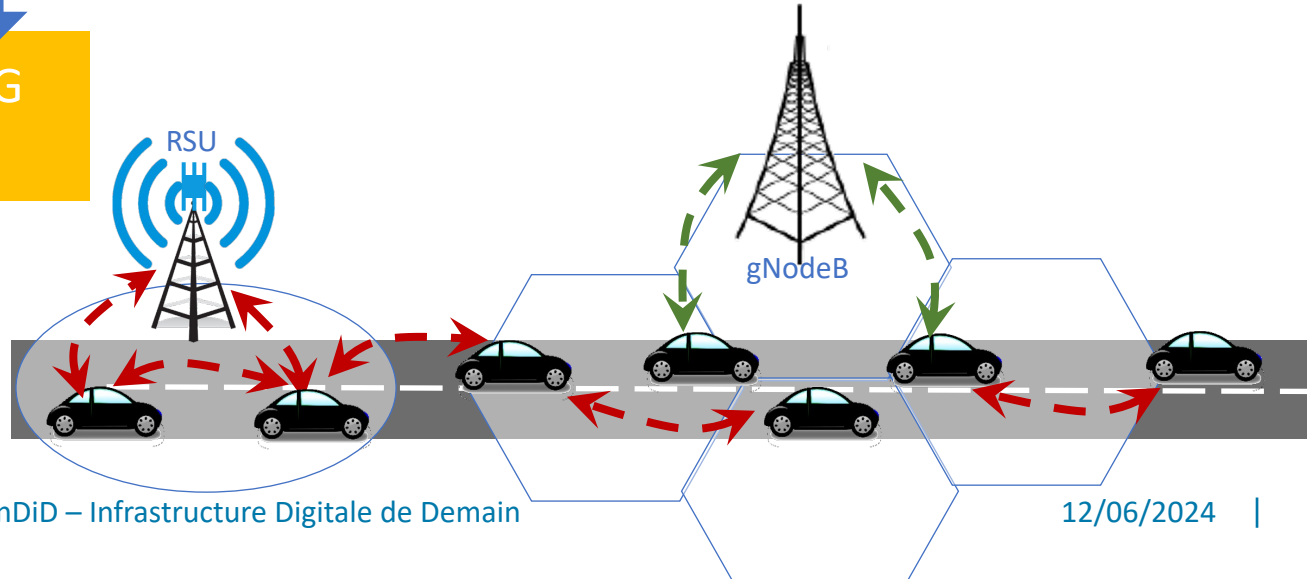
Hybridation des technologies de communication V2X

Co-financed by the Connecting Europe Facility of the European Union

Hybridation des technologies de communication V2X

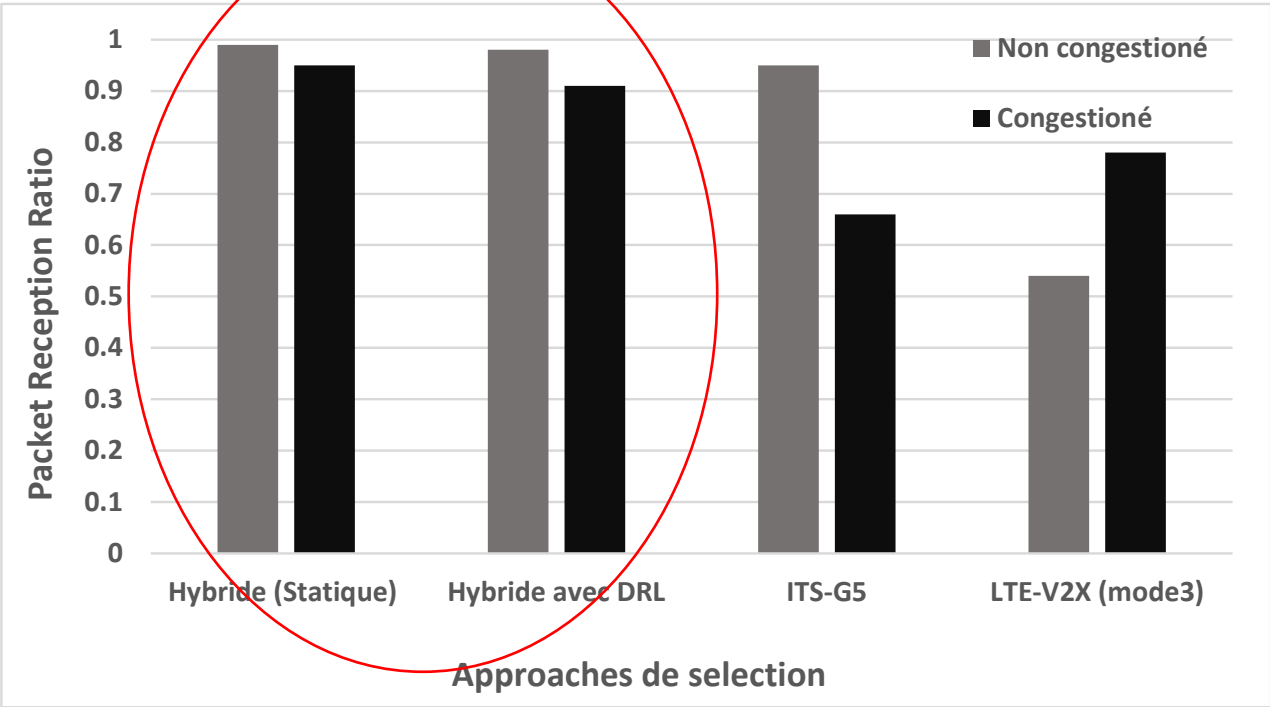


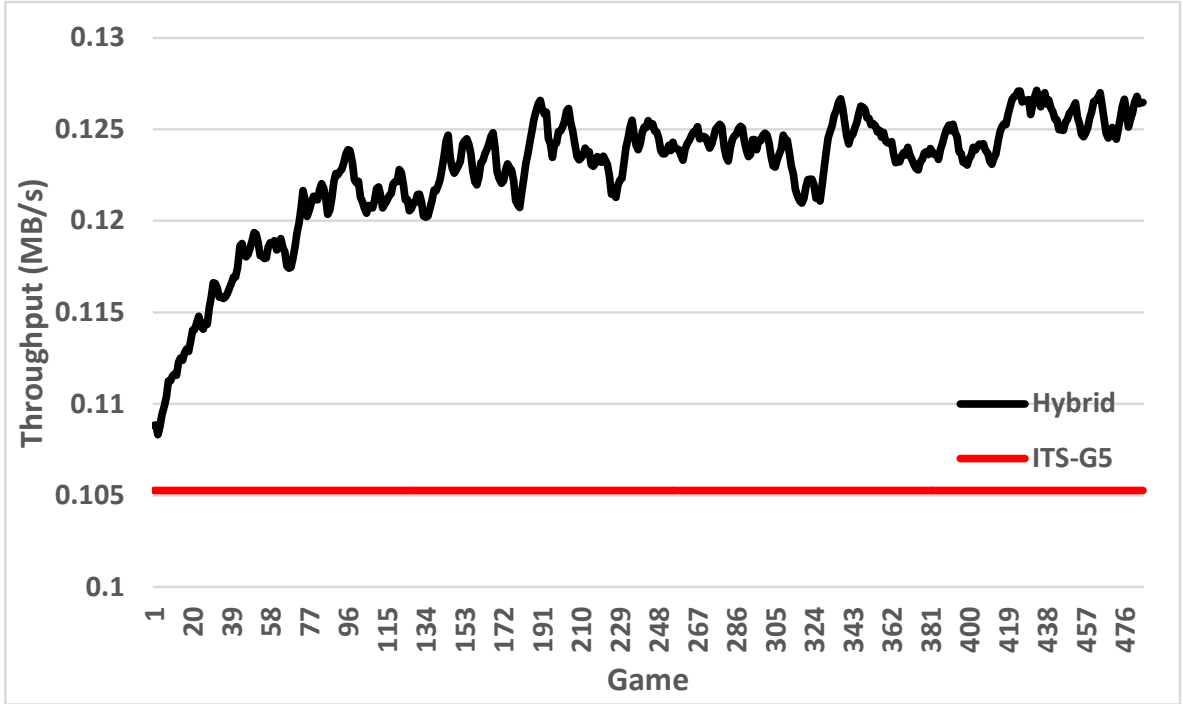
- Mode de communication
  - Hybride redondant
  - Equilibrage de charge
  - Meilleur RAT
- Utilisation de l'IA
  - Apprentissage par renforcement



Co-financed by the Connecting Europe Facility of the European Union

Hybridation des technologies de communication V2X





Amélioration de la fiabilité

Amélioration du débit

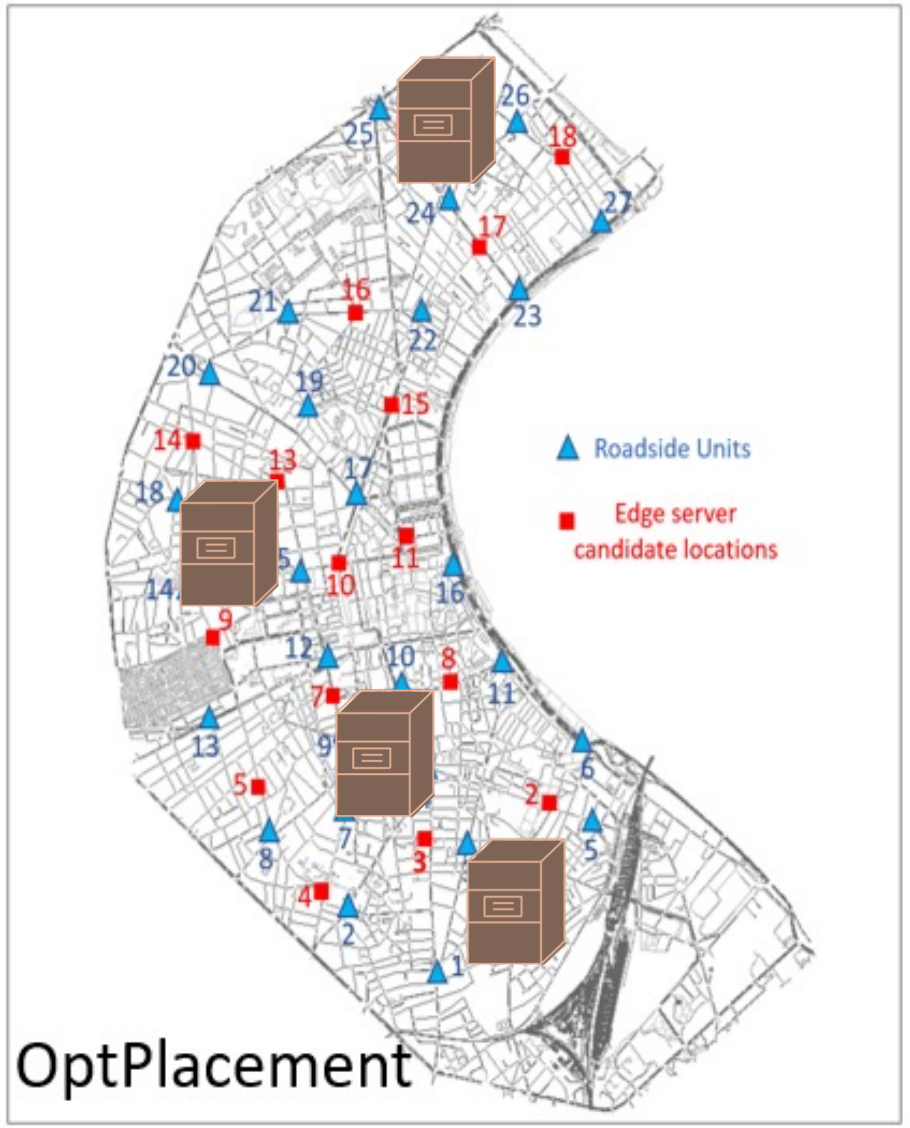
Co-financed by the Connecting Europe Facility of the European Union

Apport de l'Edge dans les réseaux véhiculaires

Co-financed by the Connecting Europe Facility of the European Union

Optimisation du placement des serveurs EDGE

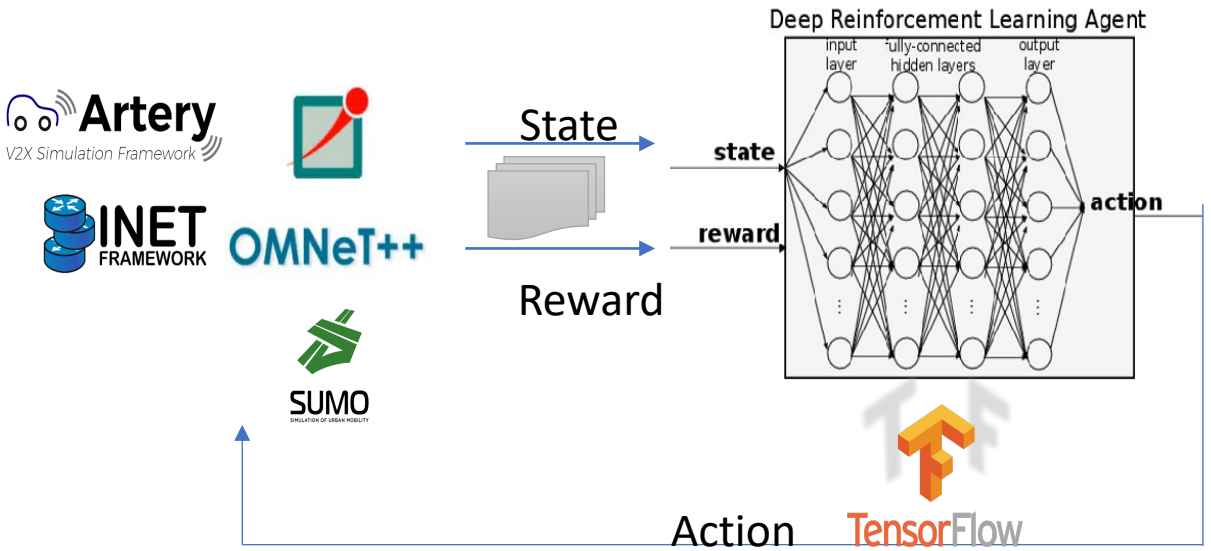
- Choix des emplacements les plus stratégiques sous ces contraintes :
  - Coût
  - Latence
  - Équilibrage de charge
- Utilisation de la programmation linéaire
- Données de trafic depuis Open Data Bordeaux
- OpenStreetMap pour la cartographie de Bordeaux

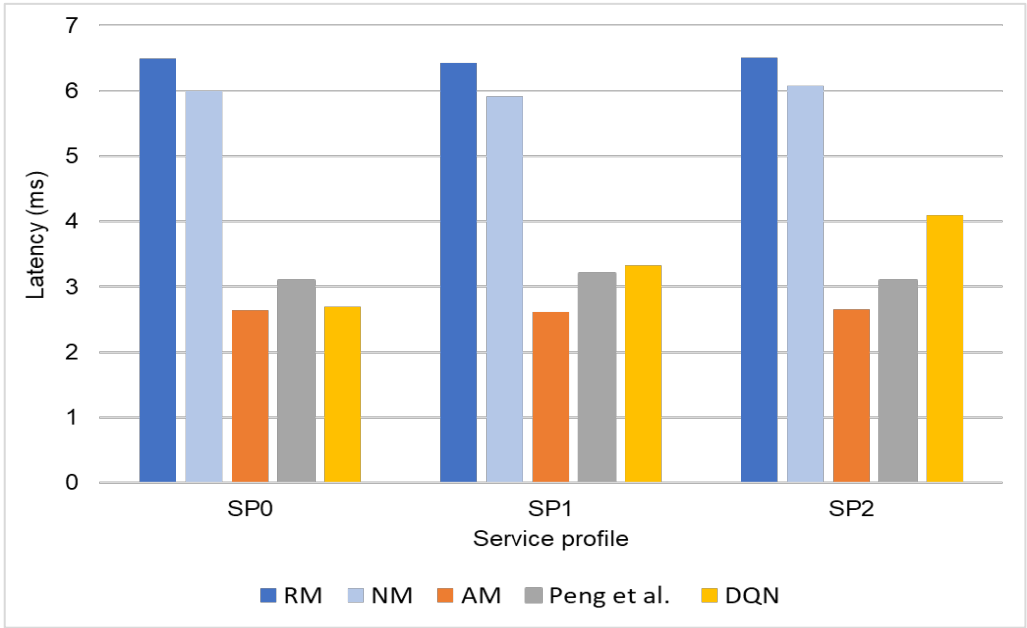


Co-financed by the Connecting Europe Facility of the European Union

Migration de service

- Assurer la continuité du service compte tenu de la mobilité des véhicules
- Utilisation d'une stratégie de migration basée sur l'apprentissage par renforcement profond DRL
- Définition des profils de services selon les exigences des services V2X : latence





Latence

Co-financed by the Connecting Europe Facility of the European Union

La preuve de concept

Co-financed by the Connecting Europe Facility of the European Union

Orientation des véhicules sur une voie de péage

Contexte

- Cas d’usage C4 :

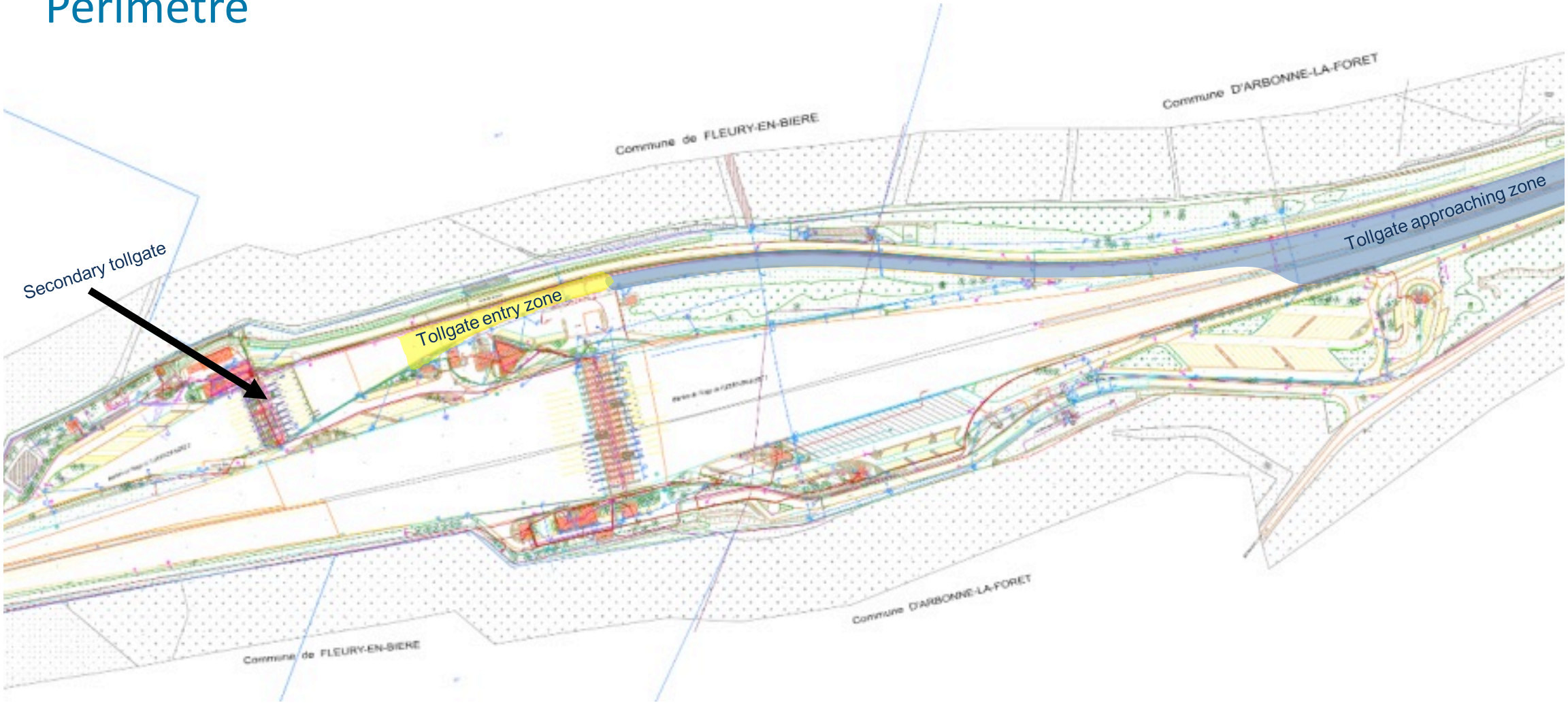
  Gare de péage en approche : orientation des conducteurs

- Bénéfices attendus :
  - Sécurité, confort de conduite à l'approche d'une gare de péage
  - Améliorer la circulation au niveau de la plateforme de péage
  - Amélioration de la fiabilité et de la disponibilité du service pour mieux orienter le véhicule
- Acteurs dans l’architecture :
  - Toll Managment System (ToMS)
  - Unité de bord de route (UBR)
  - Véhicules connectés non autonomes

Co-financed by the Connecting Europe Facility of the European Union

Orientation des véhicules sur une voie de péage

Périmètre



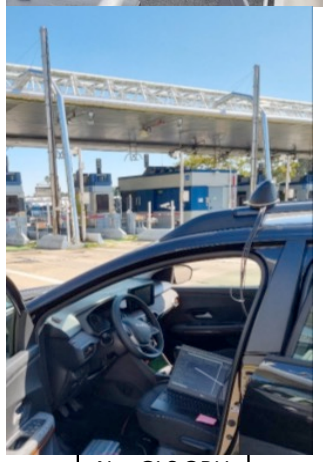
Co-financed by the Connecting Europe Facility of the European Union

Orientation des véhicules sur une voie de péage

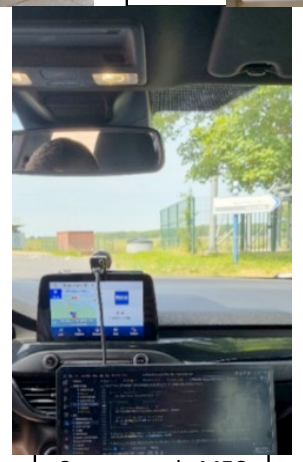
Equipements

RSU

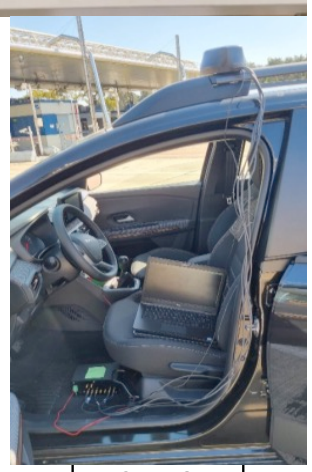
FS



NeoGLS OBU



Camera and vMEC



YoGoKo OBU

Road Side Unit

- Installée sur le toit du bâtiment de supervision
- Malgré sa hauteur de 4 mètres, on a eu une couverture d'un kilomètre

On Board Unit

- Installée à l'intérieur du véhicule
- L'antenne magnétique se fixe sur le toit du véhicule, ce qui garantit une bonne stabilité

Simulateurs

- Le simulateur de trame émule le TOMS et reproduit la transmission de l'IVIM au RSU

Camera embarquée et PC portable comme vMEC

Co-financed by the Connecting Europe Facility of the European Union

Orientation des véhicules sur une voie de péage

Scenarios de tests

Groupe 01 — Scenarios vMEC

- **01** : Orientation du véhicule à l'approche du péage sans utilisation du serveur vMEC
- **02** : Orientation du véhicule à l'approche du péage à l'aide d'un serveur vMEC

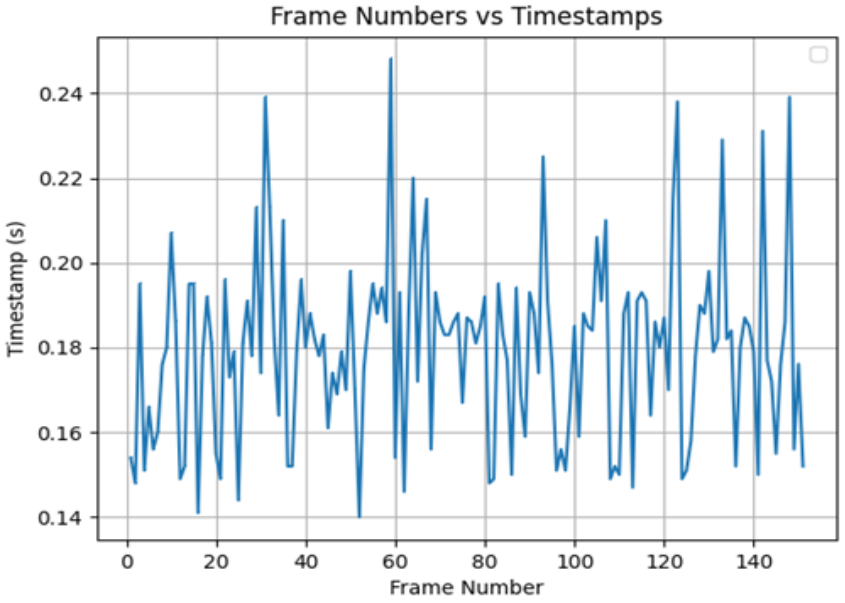
Groupe 02 — Scenarios Hybridation

- **01** : Orientation du véhicule à l'approche du péage sans communication hybride
- **02** : Orientation du véhicule à l'approche du péage avec communication hybride
- **03** : Orientation du véhicule à l'approche du péage avec communication hybride lorsque la couverture ITS-G5 est absente

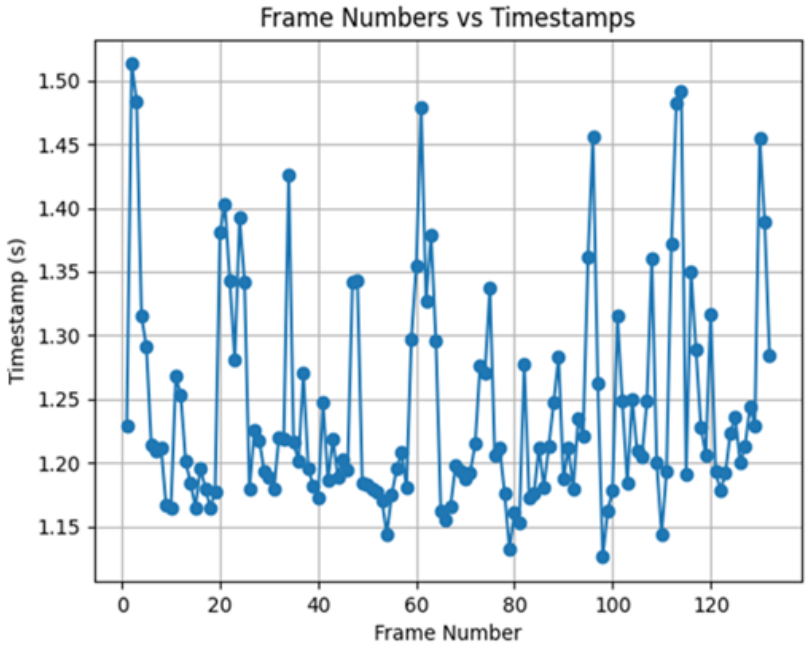
Co-financed by the Connecting Europe Facility of the European Union

Orientation des véhicules sur une voie de péage

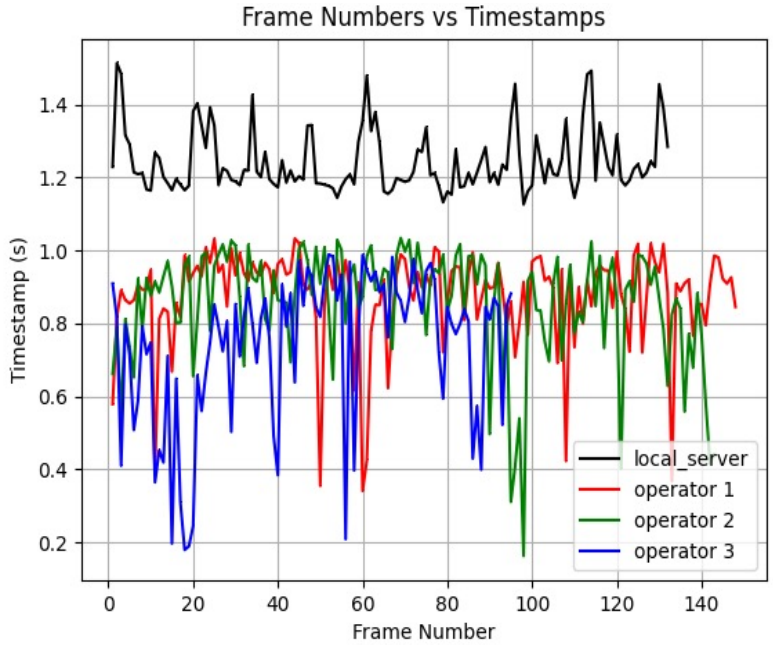
Résultats groupe 1



Sans utiliser le vMEC



En utilisant le vMEC

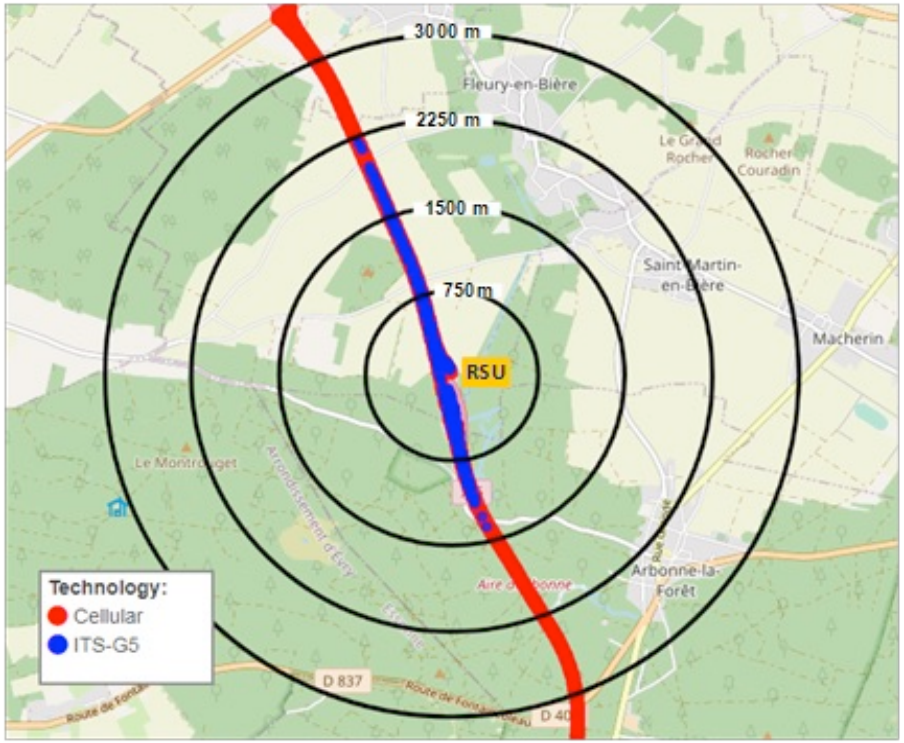


Comparaison entre les approches

Co-financed by the Connecting Europe Facility of the European Union

Orientation des véhicules sur une voie de péage

Résultats groupe 2



Portée des deux technologies

	Paris → Lyon		Lyon → Paris	
	ITS-G5 (%)	Cellulaire (%)	ITS-G5 (%)	Cellulaire (%)
(0, 750]	92.6	99.4	74.5	100
(750, 1500]	75.3	100	32.4	99.6
(1500, 2250]	4.2	99	0	100
(2250, 3000]	0	99.3	0	100

Résultats de fiabilité (PRR)

Co-financed by the Connecting Europe Facility of the European Union

Conclusion

- Optimisation des cas d'usage en utilisant l'hybridation et un placement optimal des sources de calculs EDGE
- Assistance pour les nouveaux services innovants exigeant de meilleures performances
- Évaluation de nouvelles architectures pour les systèmes de transport intelligents coopératifs (C-ITS)

Co-financed by the Connecting Europe Facility of the European Union

Merci pour votre attention

Contact

byacheur@u-bordeaux.fr
tad@labri.fr

Co-financed by the Connecting Europe Facility of the European Union

2.7.2 - CartoHD

Frédérique Williams - IGN

Co-financed by the Connecting Europe Facility of the European Union

The contents of this publication are the sole responsibility of InDiD Consortium and do not necessarily reflect the opinion of the European Union.

Activité du GT 2.7.2

Objectifs (GA)

Définition des éléments nécessaires à l'implémentation d'une cartographie HD opérationnelle dans les futures plateformes des systèmes de transports C-ITS.

Objectifs opérationnels

- Porter et partager la notion CartoHD auprès de l'ensemble des acteurs de l'écosystème
- Fournir les éléments correspondant en entrée des spécifications des services et des messages : en particulier GT2.4 et les POC

Panel d'experts, profils représentatifs :

- des gestionnaires : APRR, SANEF, SNCF, …
- des utilisateurs : Valeo, Vedecom, Transdev
- de la techno/carto : IFFSTAR, UPHF, TOMTOM, IGN, Geosat …

Co-financed by the Connecting Europe Facility of the European Union

Principaux résultats du 2.7.2

Co-financed by the Connecting Europe Facility of the European Union

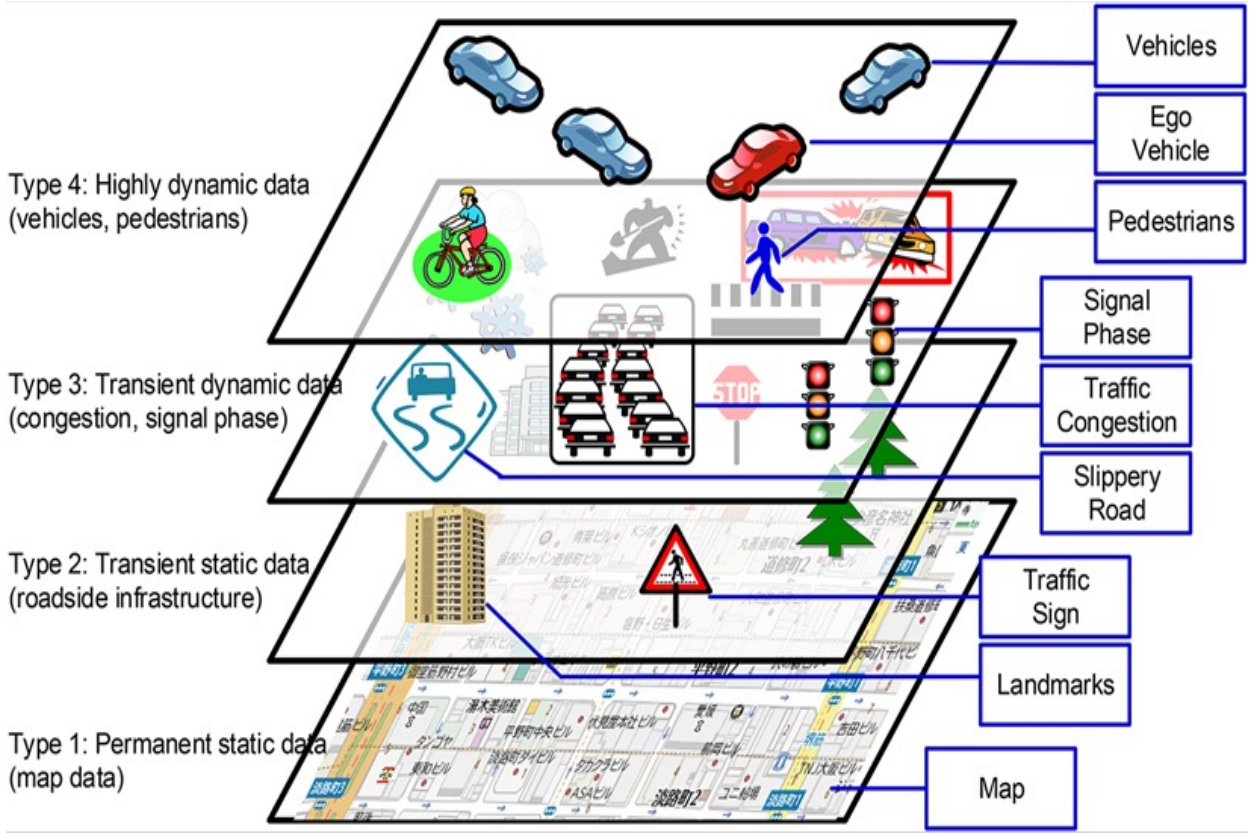
Clarification des concepts CartoHD et état de maturité

(Livrable 1 – Rapport « Etat de l'Art »)

Carto HD = un facteur de fiabilisation

- Notion de "Perception augmentée"
- Un complément aux capteurs pour l'aide à la prise de décision

Local Dynamic Map (LDM)

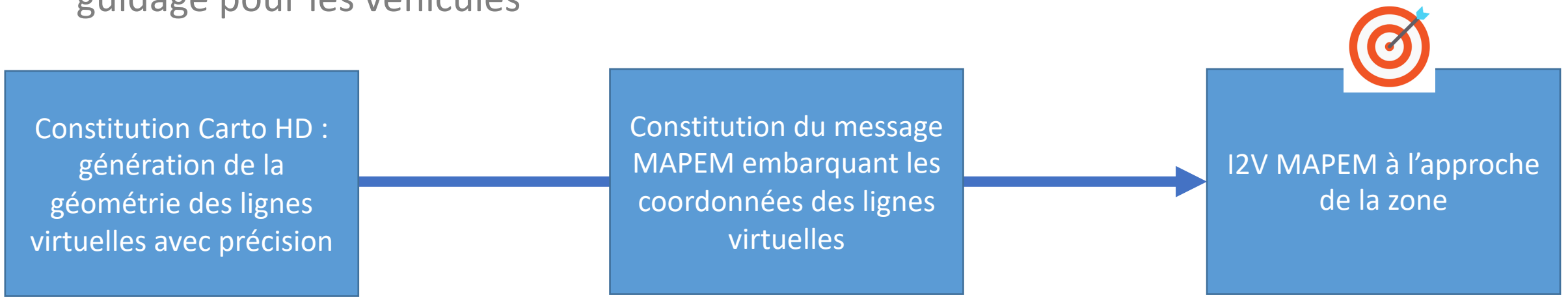


Co-financed by the Connecting Europe Facility of the European Union

Définition d'éléments de spécifications et process CartoHD contexte C-ITS

Contribution au POC « franchissement de la barrière de péage de Fleury»

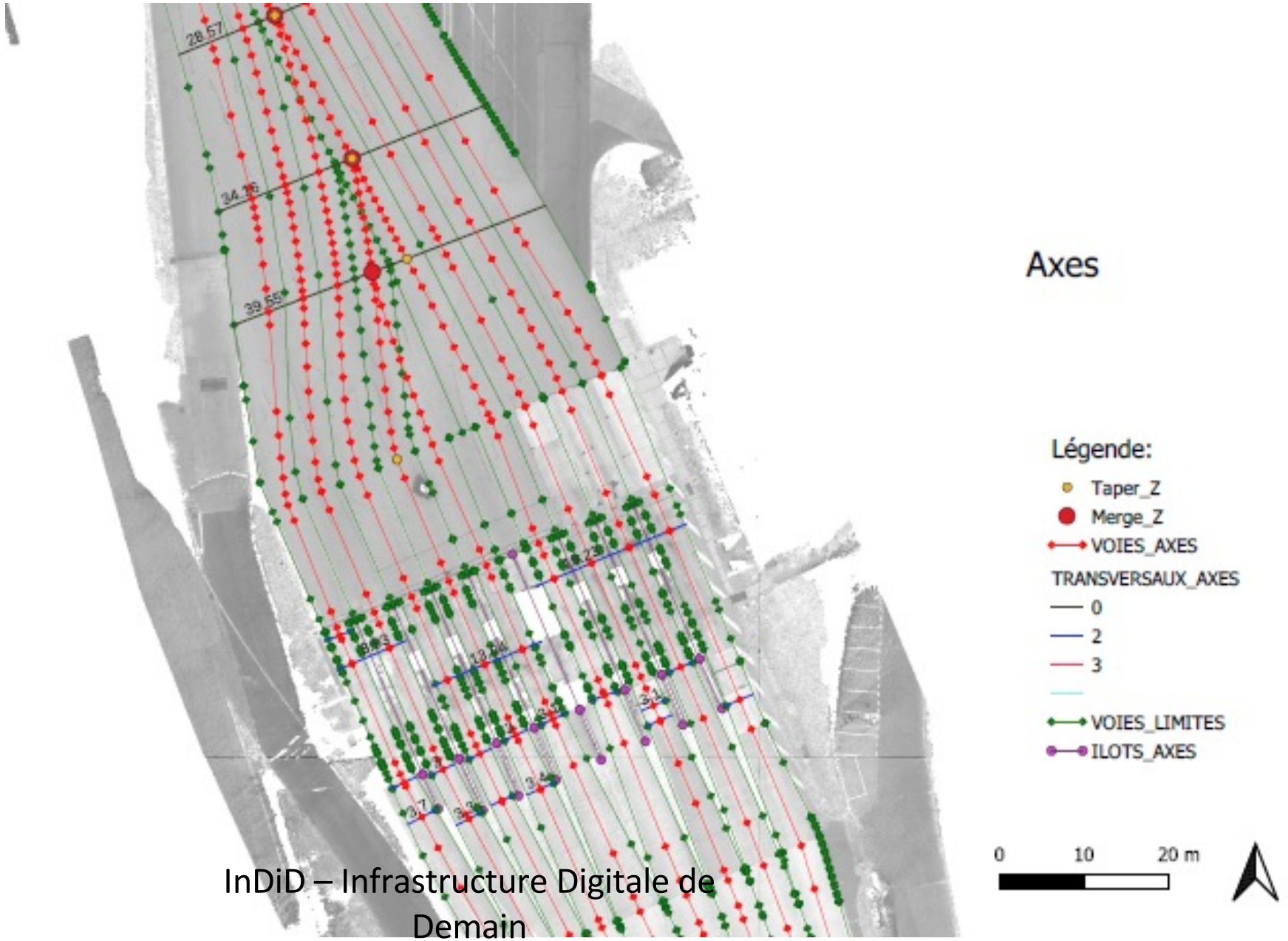
Enjeu : absence de signalisation horizontale sur la raquette signifie pas de lignes de guidage pour les véhicules



Perspectives : extension à d'autres cas d'usages : carrefours complexes, tunnels (opportunité SCALE)

Co-financed by the Connecting Europe Facility of the European Union

Jeu de données carto-MAPEM



Co-financed by the Connecting Europe Facility of the European Union

Rapport sur la gouvernance de la donnée

Des éléments de recommandations confrontés au terrain

- Définition de la gouvernance de la donnée contexte InDiD : importance de la capacité à partager cette donnée dans l'infrastructure au bénéfice d'une optimisation du service
- Dans cette phase du projet, focus sur les aspects techniques et fonctionnels (à partir des travaux des POC)

→ Définition d'un socle d'éléments carto HD

→ Préconisations pour la constitution du MAPEM sur des trajectoires virtuelles pour fiabiliser la conduite automatisée

- Le modèle économique reste à construire

Le projet SCALE représente le cadre désigné pour poursuivre l'analyse sur des cas d'usages supplémentaires (tunnel?) et les aspects économiques.

Co-financed by the Connecting Europe Facility of the European Union

2.7.3 : Sécurité des C-ITS

Rida Khatoun (Telecom Paris)

Co-financed by the Connecting Europe Facility of the European Union

The contents of this publication are the sole responsibility of InDiD Consortium and do not necessarily reflect the opinion of the European Union.

Sécurité des C-ITS

GT 2.7.3

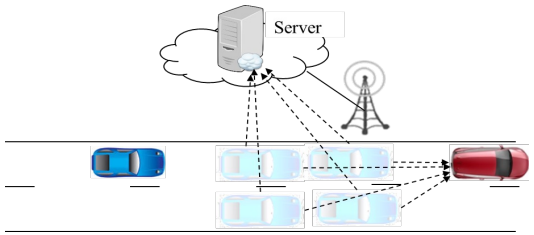
- Taches
  - Tache1 – Sécurité des communications V2X dans un contexte hybride (ITS-G5, LTE-V2X, 5G)
  - Tache2 – Protection contre les attaques DDoS
  - Tache3 – Evaluation des solutions de sécurité
  - Tache4 – Gouvernance PKI
  - Tache5 – Sécurité de bout en bout
- Délivrables
  - Sécurité des Edges : Security for Edge Vehicular Networks
  - Sécurité des communications de bout en bout : End-to-End security in hybrid V2X communication
  - Etat de l'art sur les cyberattaques : State of the art on Cyberattacks in C-ITS : Attacks, taxonomy and Countermeasures
  - Preuve d'un concept de détection : Proof-Of-Concept for a cyberattacks solution in C-ITS
  - Vérification formelle des protocoles de sécurité : Automatic Verification Tools for Cryptographic Protocols
  - Gouvernance PKI : PKI Gouvernance

Co-financed by the Connecting Europe Facility of the European Union

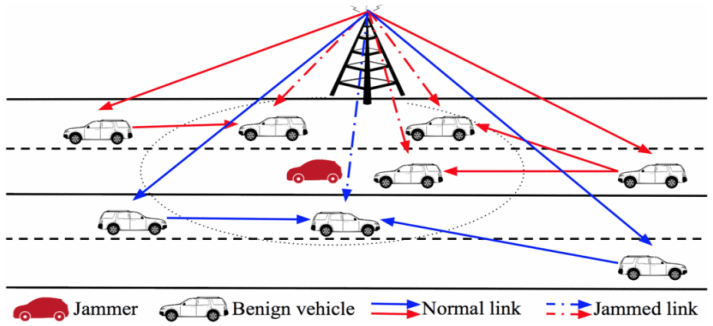
Défis de la cybersécurité des C-ITS

- Catégories des cyberattaques dans les C-ITS
  - Cyberattaques communes avec les réseaux sans fil
  - Cyberattaques spécifiques aux C-ITS

Security challenges	Requirements
Large number of communicating ITS-Stations	Requires quick and efficient treatment of data flows by receivers (vehicles, RSUs and TMEC), in order to make the right decisions.
Different manufacturers and suppliers	Requires standardization of ITS-Stations, applications and processes in order to ensure interoperability between different actors.
High mobility of vehicles	Requires quick adaption in new reception area.
Wireless communication	Requires security solutions for transmitting sensitive data.
Multi-hop transmission mode (V2V communication)	Requires security solutions to guarantee integrity of exchanged messages by authenticating the source of the message.
Dynamic ITS environments	Requires high performance of RSUs to cover all ITS-Stations regardless of the geographical constraints (availability).
Critical time constraints	Requires optimization of processes and security mechanisms in order to receive the useful information in the perfect time.
Very low tolerance of errors, especially messages coming from the TMEC	Requires plausibility and accuracy of information checks, by collecting and comparing data from different sources before taking decisions.
Huge number of ITS applications	Requires setting priorities, and defining security requirements for each application.
Trade-off authentication vs privacy	Requires new authentication approaches that do not reveal the identity of the drivers.
Long life of ITS vehicles	Requires robust security solutions that fit to all possible threats.



A denial of service scenario using a bot of vehicles



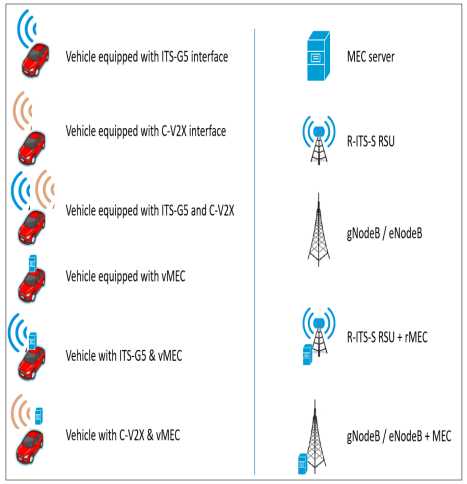
Jamming attack scenario [Gu et al, WiOpt 2018]

	Attacks	Description	Targeted ITS-S
Traditional attacks to wireless communication systems	Denial of Service (DoS) – Flooding	Maliciously and artificially generating a high volume of false messages to disturb the ITS network and equipment.	V-ITS-S R-ITS-S ITSS-C
	Denial of Service (DoS) – Spamming	A high volume of messages introduced intentionally to increase the transmission latency and consume the bandwidth of network	R-ITS-S ITSS-C
	Denial of Service (DoS) – Black hole	A node which drop, misrouting or redirecting message	V-ITS-S R-ITS-S
	Denial of Service (DoS) – Malware	Introduction of malicious software	V-ITS-S R-ITS-S ITSS-C
	Denial of Service (DoS) – Greedy behavior	Saturation of the network by modifying access control or congestion control mechanisms to gain more throughput than other users	V-ITS-S R-ITS-S
	Denial of Service (DoS) – Jamming	Create interference on canal transmission	V-ITS-S R-ITS-S
	Manipulation of messages	Modification or suppression of message fields (loss of information)	R-ITS-S ITSS-C
	Injection of false message	Generate and send false information	V-ITS-S R-ITS-S ITSS-C
	RF Fingerprinting	Distinguish one radio transmitter from another by use of emission profiles	V-ITS-S
	Masquerade	Posting as a legitimate node of the system	V-ITS-S R-ITS-S
	Replay	Sending old message.	R-ITS-S ITSS-C
	Eavesdropping +data analysis	Listen to communication in order to collect and analyze info.	V-ITS-S
Specific attacks to C-ITS	GPS Spoofing	Using GPS simulator to generate radio signals to convince the GPS receiver that it is in an arbitrary location and time.	V-ITS-S
	Location tracking	Collect personal location info.	V-ITS-S
	Sybil attack	Multiplication of fake node (sending multiple message from one node with multiple identities).	R-ITS-S ITSS-C
	Illusion attack	Create a specific traffic situation and sends false traffic warning messages to decoy other drivers believe that a traffic event occurred.	V-ITS-S
	Vehicle Sensor spoofing	Manipulate sensor in order to generate faulty data complying with the implemented protocols	V-ITS-S

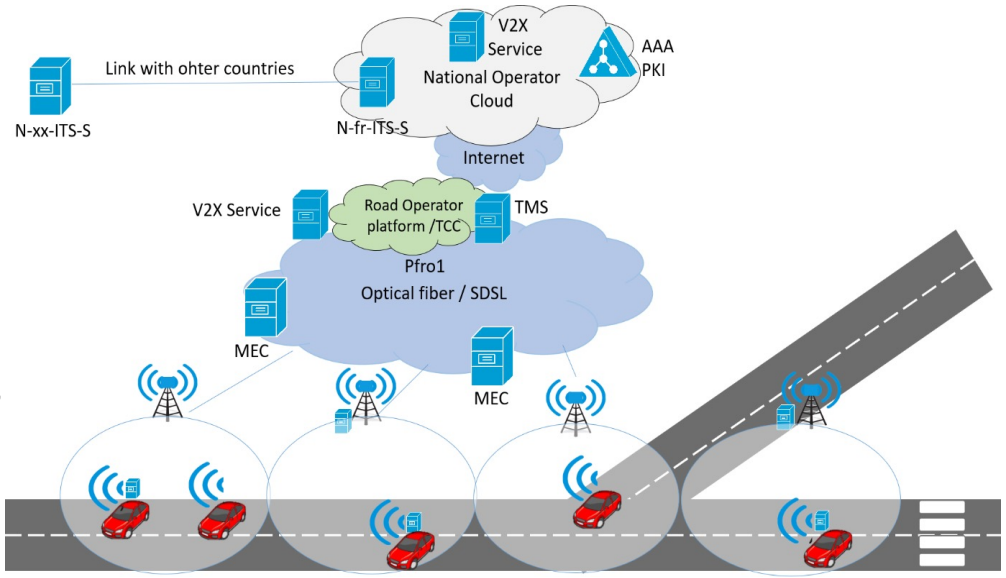
Co-financed by the Connecting Europe Facility of the European Union

Sécurité de l’Edge Computing dans les C-ITS

- Nouvelle architecture pour l’Edge Computing Mobile
  - Composants
    - Serveurs vMEC déployés au sein des véhicules,
    - Serveurs MEC déployés au sein des RSUs
    - Serveurs MEC déployés à autres emplacements fournissant le calcul et le stockage pour les RSUs.
  - Fonctions
    - Interconnexion entre les différents composants du système
    - Connexions V2V/V2I
    - Interconnexion entre les serveurs MEC et les éléments d’hebergement,
  - Recommandations pour INDID : sécurité des données au niveau des Edges avec TPM, IDS au niveau des Edges, …



*MEC: Mobile Edge Computing



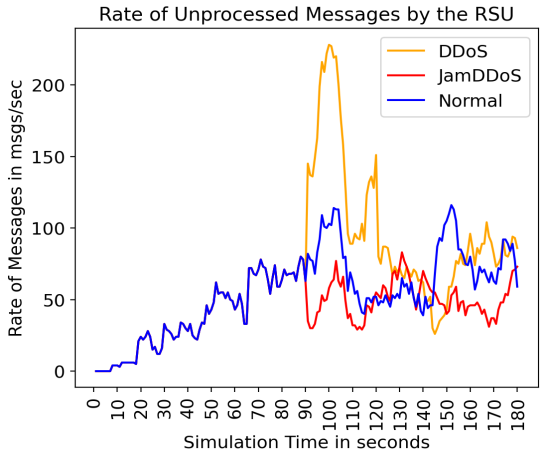
Co-financed by the Connecting Europe Facility of the European Union

Détection des cyberattaques dans les C-ITS

- Etude de l'impact d'une attaque de déni de service distribuée (DDoS) contre les RSU et les V-ITS-S
  - Simulateurs
    - SUMO pour modéliser le trafic
    - OMNeT++ comme gestionnaire du réseau
    - Artery
  - Protocoles: ETSI ITS-G5, GeoNetworking et BTP (Basic Transport Protocol)
  - Environnement
    - Données du trafic sur l'autoroute A1 entre les villes de Paris et Lille
    - Echantillon de 2 km côté de Paris (susceptibilité aux attaques pendant les heures de pointe en raison du volume élevé de voitures).

TABLE II
SIMULATION SCENARIO SET I & II PARAMETERS

Parameter\Case	Normal	DDoS	JamDDoS
Average normal cars	90	90	90
Average attack cars	20	20	20
Attack transmission power	200 mW	200 mW	2 W



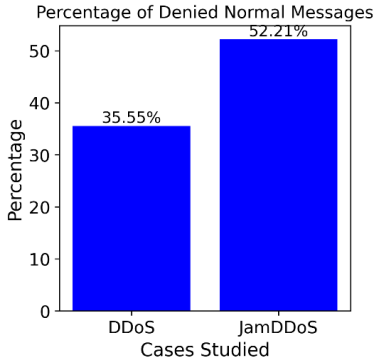
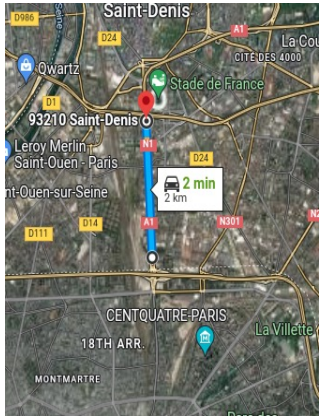


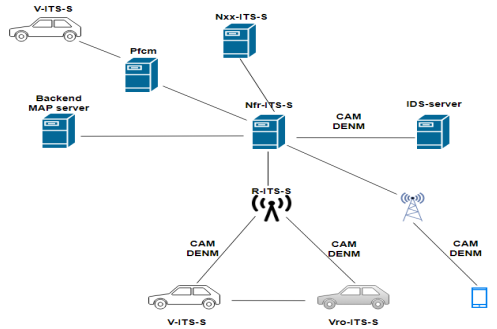
TABLE I
COMMON SIMULATION PARAMETERS

Parameter	Value
Simulation time	180 sec
Attack duration	30 sec (from 90 to 120)
Normal message rate	10 CAMs/sec
Attacker message rate	50 CAMs/sec
Normal transmission power	200 mW (default)
DSRC range	1 km
DCC mechanism	Reactive (1 ms)
Channel name	Control Channel (CCH)
Lane length	2 km
Speed limit	110 km/h
Departure speed	Speed Limit
RSU position	1 km from both ends

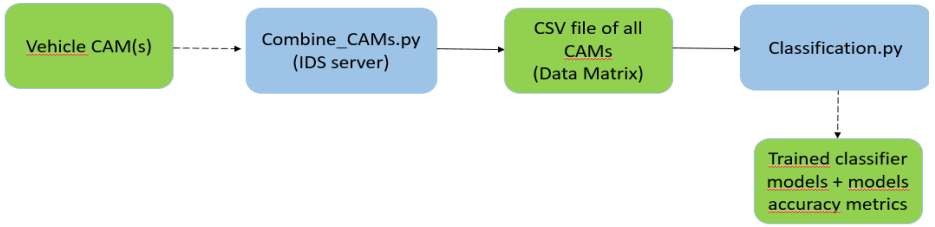


Co-financed by the Connecting Europe Facility of the European Union

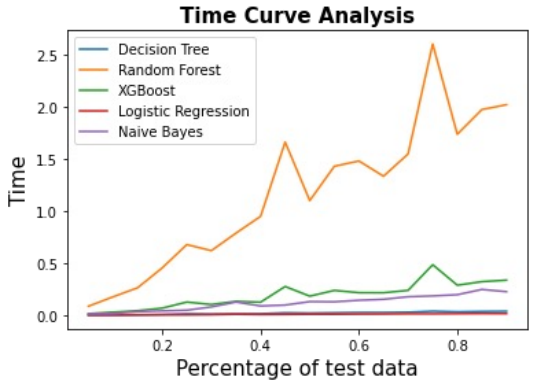
Détection des cyberattaques dans les C-ITS

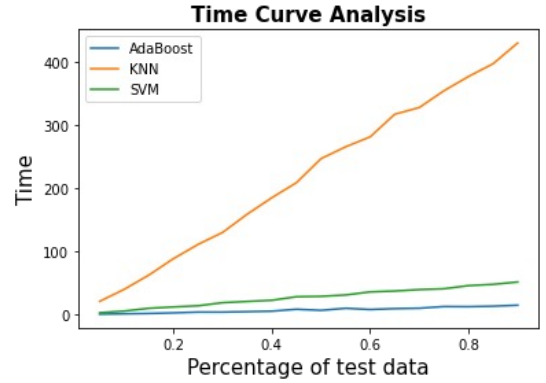


- Approche de détection d'attaques basée sur l'apprentissage (ML)
- Cas d'usage : attaque DDoS et attaque Sybil
  - Le bot V-ITS-S lance une attaque DDoS contre un serveur R-ITS-S.
  - Le bot V-ITS-S utilise des messages CAM.
  - Le jeu de données VeReMi comprend : 5 attaques de falsification de position, 3 densités de véhicules (faible, moyenne et élevée), 3 fréquences d'attaquants (10, 20 et 30 %).
  - Les CAM sont transmis à un IDS pour les analyser.
  - Information: temps de réception des CAM, ID du véhicule, coordonnées du véhicule, erreur de la position du véhicule, temps d'émission, messageID, Pseudo de l'émetteur.



Class/method	Decision tree	Random forest	AdaBoost	XGBoost	KNN	Logistic regression	Naïve Bayes	SVM
DoS attack	0.8656	0.9961	0.9926	0.9995	0.9901	0.9835	0.9804	0.9993
Sybil position attack	0.9773	0.9997	0.9907	0.9993	0.9783	0.9549	0.9237	0.997
Sybil speed attack	0.9877	0.9999	0.9912	1.00	0.971	0.9666	0.9438	0.9994





Co-financed by the Connecting Europe Facility of the European Union

Pour protéger les C-ITS

- Recommandations pour INDID :
  - Déployer et utiliser TLS1.3, VPN IPSEC, ECDHE, ainsi que les WebSocket sécurisées
  - Spécifier formellement les protocoles ainsi que leurs propriétés de sécurité.
  - Employer des mesures de sécurité courantes.
  - Déployer un Système de Détection d'Intrusion (IDS) au niveau des serveurs principaux.
  - Déployer des IDS au niveau des serveurs périphériques (basés sur les signatures et les comportements).
  - Analyser les messages CAM pour la détection d'attaques
    - Impact des cyberattaques prouvé par simulation
    - Attaque Sybil est une menace réelle
    - Bots(un ensemble de véhicules malveillants) représentent une réelle menace
  - Analyser chaque protocole de sécurité à l'aide d'un outil de vérification formel comme ProVerif ou Scyther
  - Appliquer le RGPD et la norme ISO 27000 pour les infrastructures à clés publiques et les cadres de certification

Co-financed by the Connecting Europe Facility of the European Union

2.7.4 – Amélioration de l’infrastructure des gestionnaires

Christelle BERNIER - CEREMA

Emilien BOURDY - URCA

Co-financed by the Connecting Europe Facility of the European Union

Objectifs du 2.7.4: *Road operators' infrastructure enhancement for connected and automated vehicles needs*

- Plusieurs problématiques ont été soulevées par les gestionnaires dans les projets précédents, ou au démarrage d'InDiD :
  - Le gestionnaire dispose d'un équipement centralisé, mais plusieurs sources de données. Comment définir des zones d'agrégation de messages CAM identiques sur plusieurs équipements afin de pouvoir fusionner facilement les données reçues ?
  - Actuellement, la gestion des déviations peut être très complexe chez les gestionnaires (autorisation de dévier réglementaire, ...) et il n'existait pas de messages (en 2019) pour émettre une déviation. Comment transmettre une information de déviation aux usagers ?
  - Le CAM-I de SCOOP est finalement peu utilisé. Comment peut on améliorer le CAM-I ? Est il toujours pertinent dans le contexte actuel ?
  - Comment aider le véhicule à mieux se positionner sur la route ?
  - Est-ce que les données de météorologie dont dispose le gestionnaire sont transmissibles aux usagers ? Si oui comment ?
  - Comment transmettre de manière efficace des données de temps de parcours à l'usager ?
  - Certains nouveaux véhicules scannent les routes et affichent à leur conducteur les vitesses réglementaires. Peut on remonter ces informations aux gestionnaires qui peut ainsi s'assurer de la lisibilité de ses panneaux ?
  - Est il possible d'émettre des messages C-ITS conformes aux spécifications depuis une FLR, qui ne dispose pas d'IHM ?

Co-financed by the Connecting Europe Facility of the European Union

Travaux réalisés

- 12 livrables ont été produits dans le cadre de notre GT.
- Nous avons retenu trois sujets pour ce jour :
  - CAM-I et annonce de service
  - Déviation
  - Agrégation des CAM

Co-financed by the Connecting Europe Facility of the European Union

L’annonce de service

- Dans SCOOP et C-ROADS : utilisation du CAM-I pour annoncer quelques services : mitigation, remontée de logs, connexion à la PKI… Non reconnu au niveau européen
- Ce CAM-I est finalement peu utilisé. Comment peut on améliorer le CAM-I ? Est il toujours pertinent dans le contexte actuel ?
- Enquête menée pour comprendre le besoin des gestionnaires : 13 services identifiés : le CAM-I ne peut pas y répondre.
- Utilisation du SAEM par plusieurs partenaires pour d’autres sujets (platooning, annonce de télépéage)

Décision d’utiliser le SAEM.

SAEM ✔

- Service Announcement Essential Message
- Standard ETSI EN 302 890-1
- Plusieurs services à la fois
  - 270 549 119 en tout
- Annonce de service
  - Possibilité d’en rajouter au besoin
- Services non intégrés au message

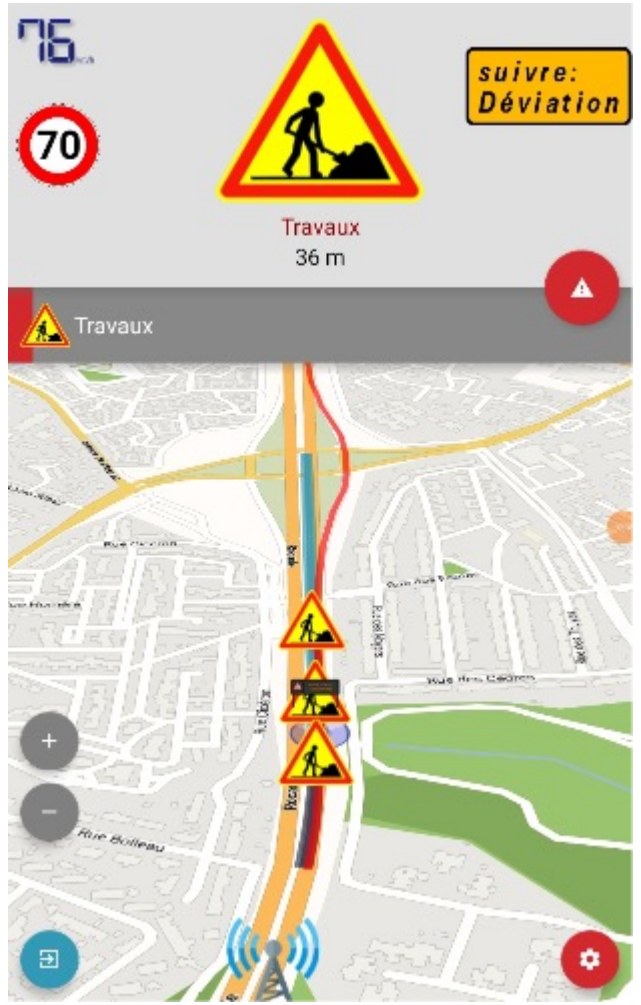
CAM-I ✘

- Cooperative Awareness Message – Infrastructure
- Message Scoop@f - Extension du CAM
- 1 à la fois - 256 en tout
- Limité dans les services existants mais extensible par spécification
- Services intégrés au message
- Non normalisé

Co-financed by the Connecting Europe Facility of the European Union

POC Déviation

- Actuellement, la gestion des déviations peut être très complexe chez les gestionnaires (autorisation réglementaire, impacts sur les routes voisines...) et il n'existait pas de messages C-ITS (en 2019) pour émettre une déviation. Comment transmettre une information de déviation aux usagers ?
- Réponse en deux temps :
  1. Analyse organisationnelle chez les gestionnaires
  2. Définition technique de la déviation :
     - Définition du C-ITS DATEX-II à utiliser (Conformité TIPI)
     - Utilisation du ReroutingManagement
     - Lien IVIM ⟶ DENM et IVIM ↔ IVIM
     - Prototype de C-ITS DATEX-II à l'URCA
- Réalisation d'un POC sur simulateur (URCA) puis en réel sur une UBR de la DIRA (NeoGLS)



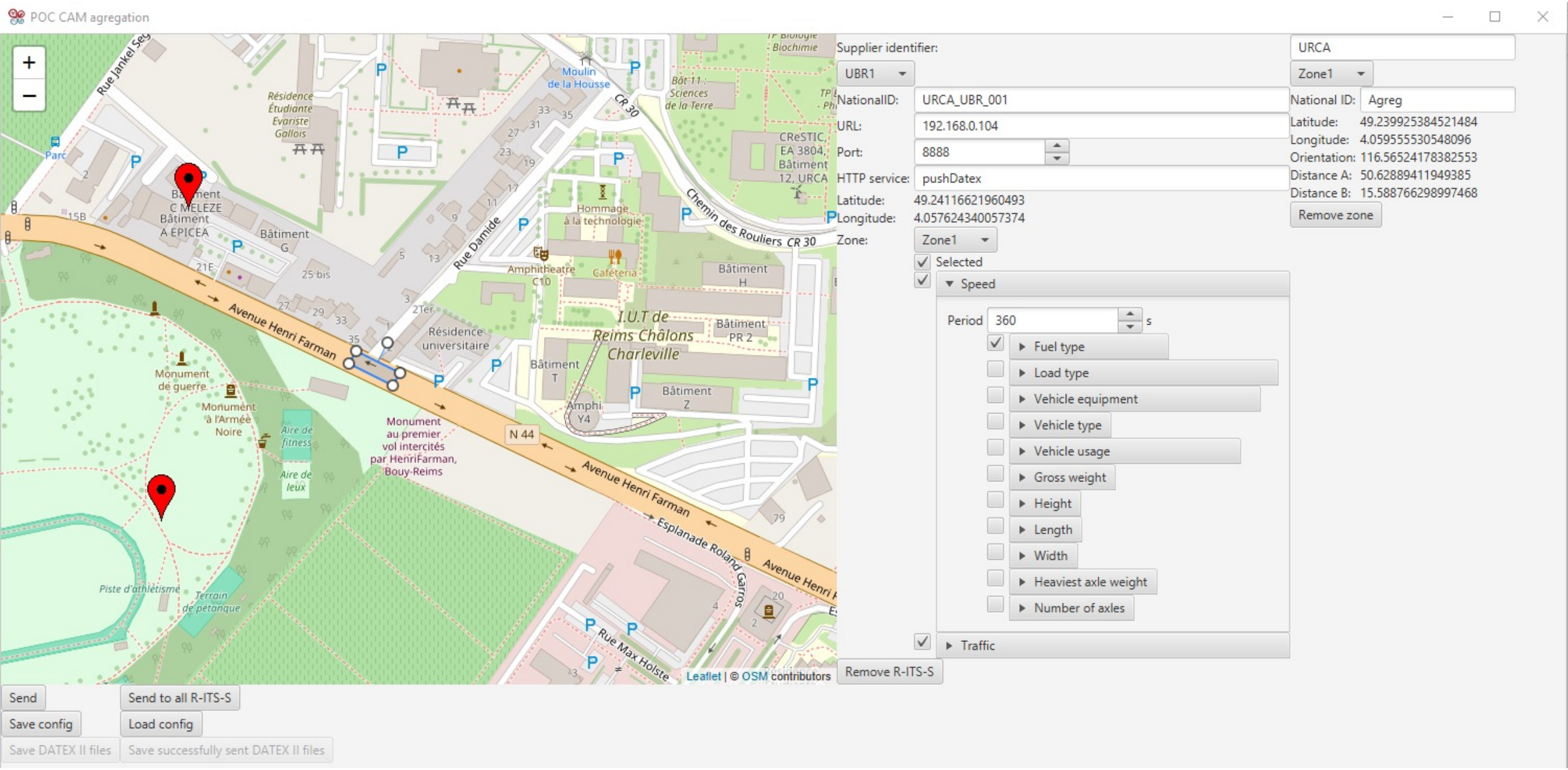
Co-financed by the Connecting Europe Facility of the European Union

Agrégation des CAM

Configurateur externe

- Le gestionnaire dispose d'un équipement centralisé, mais plusieurs sources de données. Comment définir des zones d'agrégation de messages CAM identiques sur plusieurs équipements afin de pouvoir fusionner facilement les données reçues ?
- Configuration de zone d'agrégation des CAM
  - Interne à chaque fournisseur
- Possibilité d'utiliser le C-ITS DATEX-II
  - Nécessite du développement côté gestionnaire
- POC URCA d'un configurateur
  - Configuration des UBR et des zones : avec ou sans classes, type d'agrégation etc.
  - Envoie des C-ITS DATEX-II aux UBR

Co-financed by the Connecting Europe Facility of the European Union


POC CAM agregation
Supplier identifier:
UBR1
NationalID:
URCA_UBR_001
URL:
192.168.0.104
Port:
8888
HTTP service:
pushDatex
Latitude:
49.24116621960493
Longitude:
4.057624340057374
Zone:
Zone1
Selected
Speed
Period
360
s
Fuel type
Load type
Vehicle equipment
Vehicle type
Vehicle usage
Gross weight
Height
Length
Width
Heaviest axle weight
Number of axles
Traffic
Remove R-ITS-S
URCA
Zone1
National ID:
Agreg
Latitude:
49.239925384521484
Longitude:
4.059555530548096
Orientation:
116.56524178382553
Distance A:
50.62889411949385
Distance B:
15.588766298997468
Remove zone
Send
Send to all R-ITS-S
Save config
Load config
Save DATEX II files
Save successfully sent DATEX II files
Leaflet | © OSM contributors
Avenue Henri Farman
N 44
Esplanade Roland Garros
Rue Max Holste
Chemin des Rouliers CR 30
Rue Damide
Rue Jankel Segal
Moulin de la Housse
Résidence Étudiante Evariste Gallois
Bâtiment C MELEZE
Bâtiment A EPICEA
Bâtiment G
Hommage à la technologie
Amphitheatre C10
Cafétéria
Bâtiment H
I.U.T de Reims Châlons Charleville
Bâtiment PR 2
Résidence universitaire
Bâtiment T
Bâtiment Z
Amphi Y4
Monument de guerre
Monument à l'Armée Noire
Monument au premier vol intercités par HenriFarman, Bouy-Reims
Aire de fitness
Aire de jeux
Piste d'athlétisme
Terrain de pétanque
CReSTIC, EA 3804, Bâtiment 12, URCA
Bât 11 : Sciences de la Terre

Conclusion

- Le GT 2.7.4 a pu résoudre plusieurs problématiques soumises par les gestionnaires.

  Toutes les études sont synthétisées dans le livrable « milestone 36 ».

- Chaque sujet nécessite du temps pour être compris, pour adapter les *back offices* des gestionnaires aux services C-ITS, et pour que les gestionnaires s'en emparent.
- Prochaine étape : mise en œuvre et intégration dans le processus Spécifications=>développement=>Tests=> déploiement des résultats pertinents.

Co-financed by the Connecting Europe Facility of the European Union

Annexe 1

Liste des services demandés par les gestionnaires

1. Conditions hivernales
2. Météo
3. Amélioration du positionnement GPS
4. Temps de trajet, parcours
5. Synchronisation temporelle
6. Transfert de données
7. Zone de platooning
8. Restriction permanente de la route pour tout le réseau du gestionnaire
9. Statut des UBR et leur cartographie
10. Envoyer la cartographie HD
11. EDGE computing
12. Mitigation
13. Service accès des voies

Co-financed by the Connecting Europe Facility of the European Union

Merci de votre attention

Co-financed by the Connecting Europe Facility of the European Union