2.7 Transversal studies

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.

What is 2.7 subactivity – Transversal studies

- *« In conjunction with the aforementioned technical processes, and to face the major technical challenges of C-ITS, cross-cutting technical topics will be addressed by InDiD partners. »*

- A2.7. 1: New technologies and hybridisation (SG/LTE etc.)
- A2.7.2: DTI - Digital HD maps
- A2.7.3: Security
- A2.7.4: Road operators' infrastructure enhancement for connected and automated vehicles needs

- Milestone 36 report summarize all 2.7 sub-activity results.

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 New Technologies and Hybridization (C-V2X & ITS-G5) for C-ITS

Toufik AHMED

Badreddine Yacine YACHEUR

Université de 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.

Context

- V2X communications utilize ITS-G5, a short-range technology based on the IEEE 802.11p standard.

  Introduction of a new, more efficient standard, IEEE 802.11bd.

- A growing interest in cellular networks such as LTE and 5G (C-V2X)

  Providing low latency, highly accurate positioning information, and high throughput simultaneously.

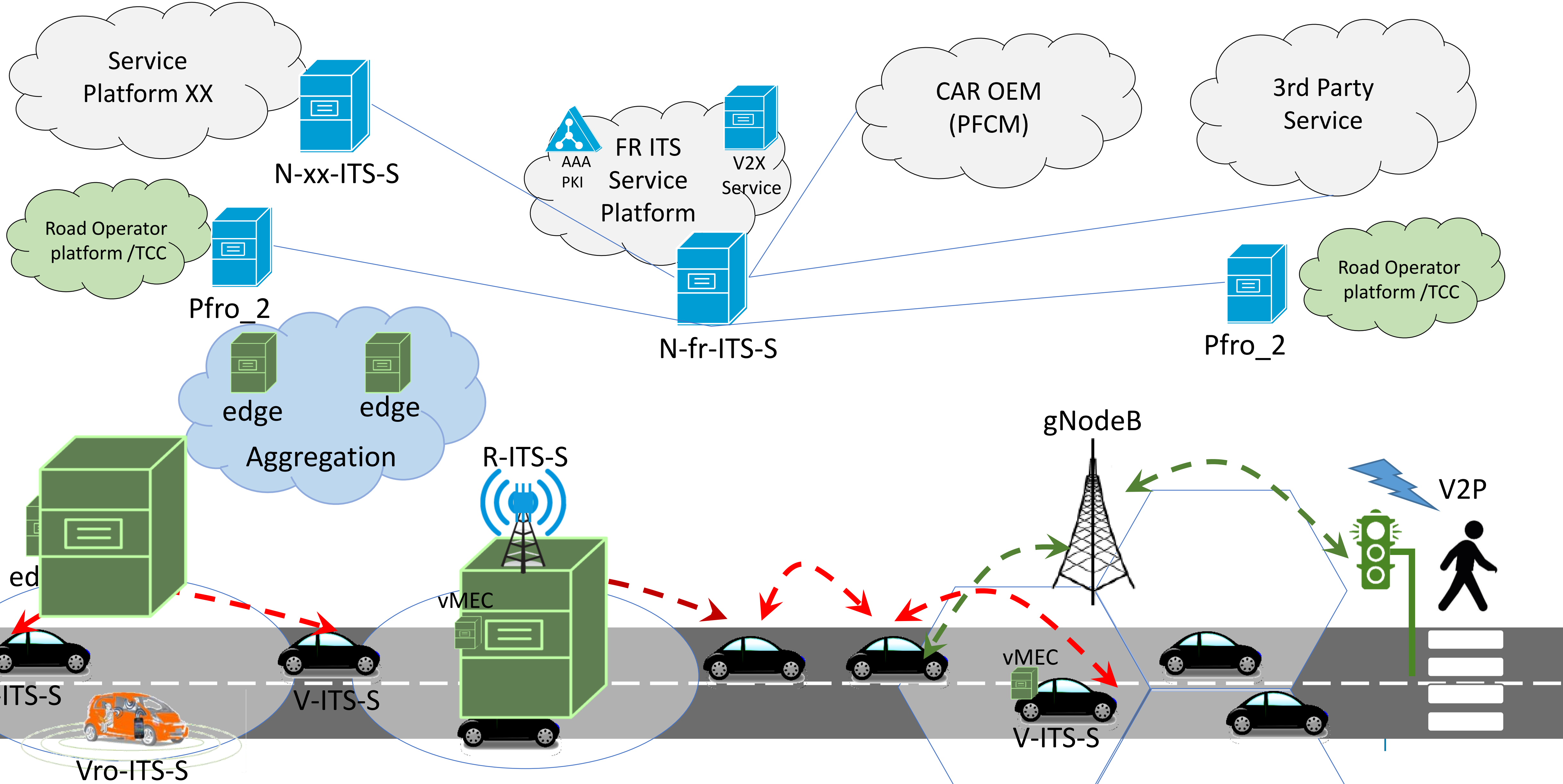
- Evolution of C-ITS services and their requirements Less latency, bandwidth, and reliability.

- Need for computational resources closer to the vehicle.

  Introduction of the concept of an EDGE server located near the roadside unit or within the vehicle.

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

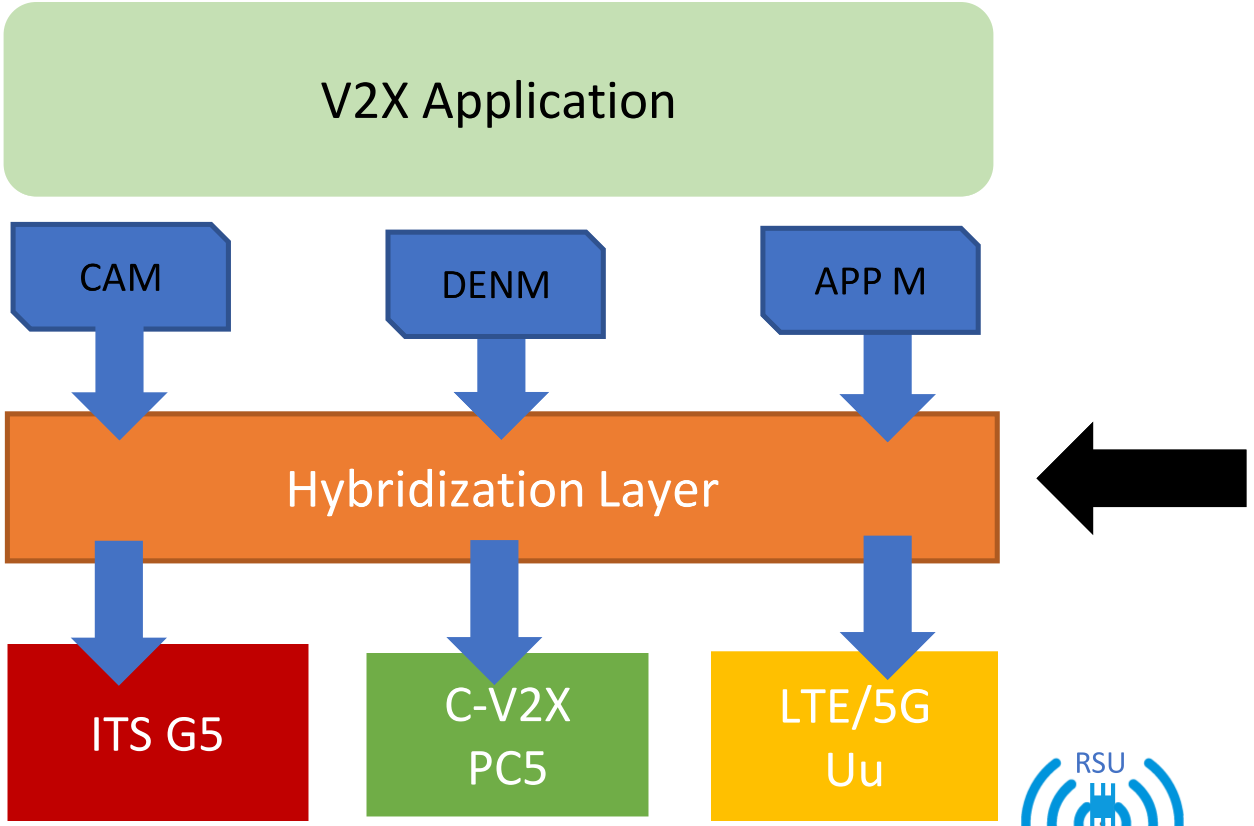
Global architecture



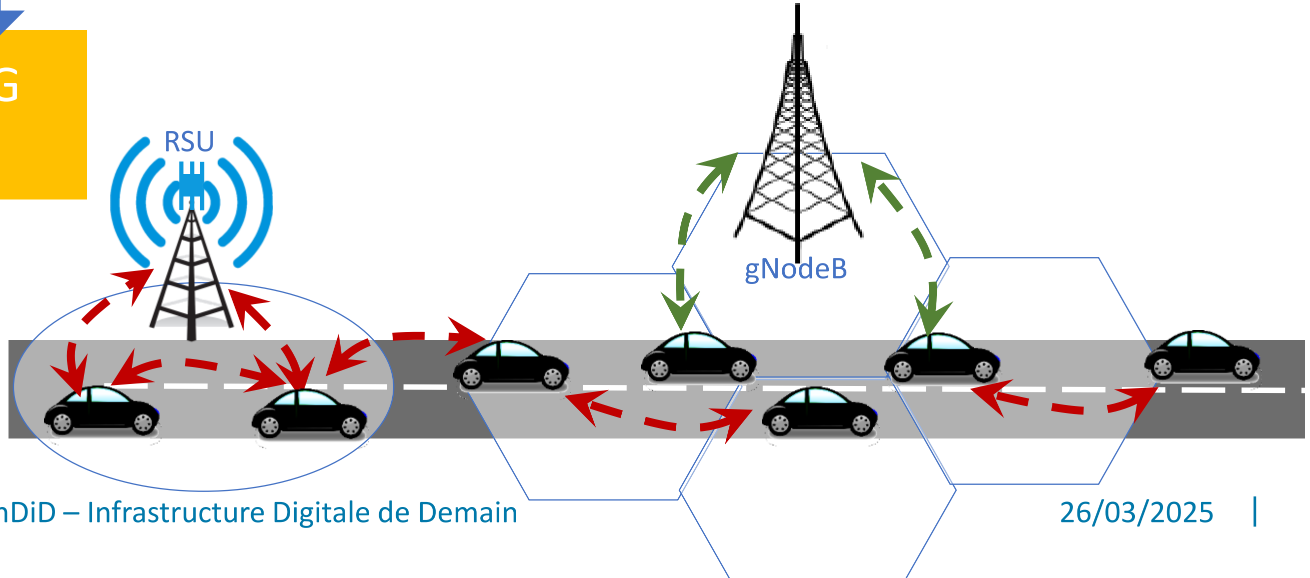
Hybridization of V2X communication technologies

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

Hybridization of V2X communication technologies

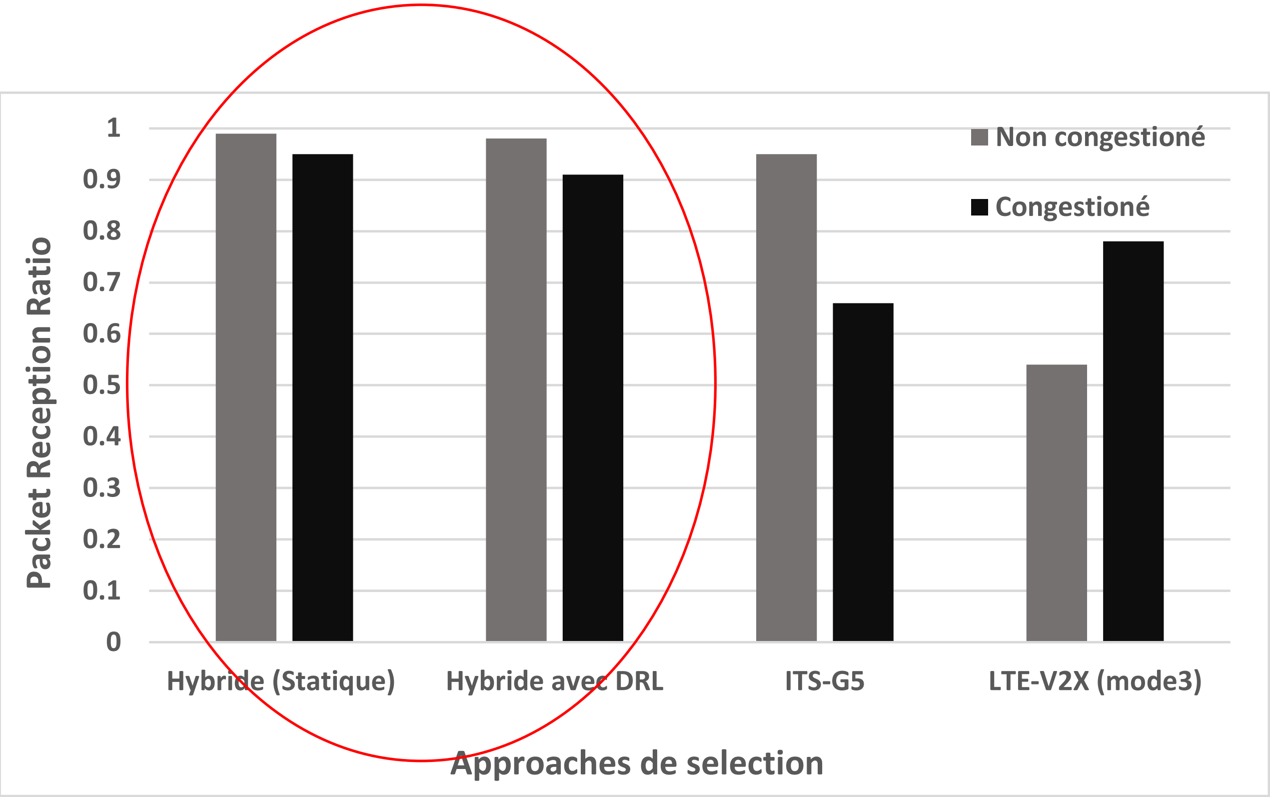


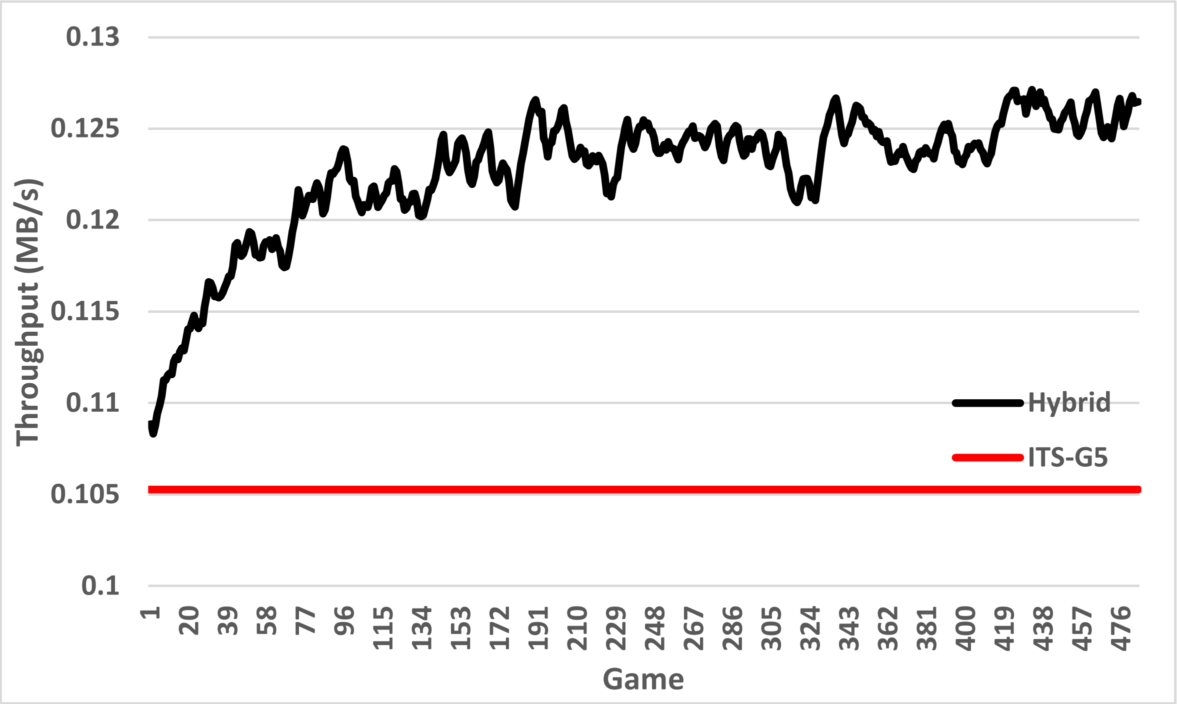
- Communication modes
  - Hybrid redundant
  - Load balancing
  - Best RAT
- Use of AI
  - Deep reinforcement learning



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

Hybridization of V2X communication technologies





Improved reliability

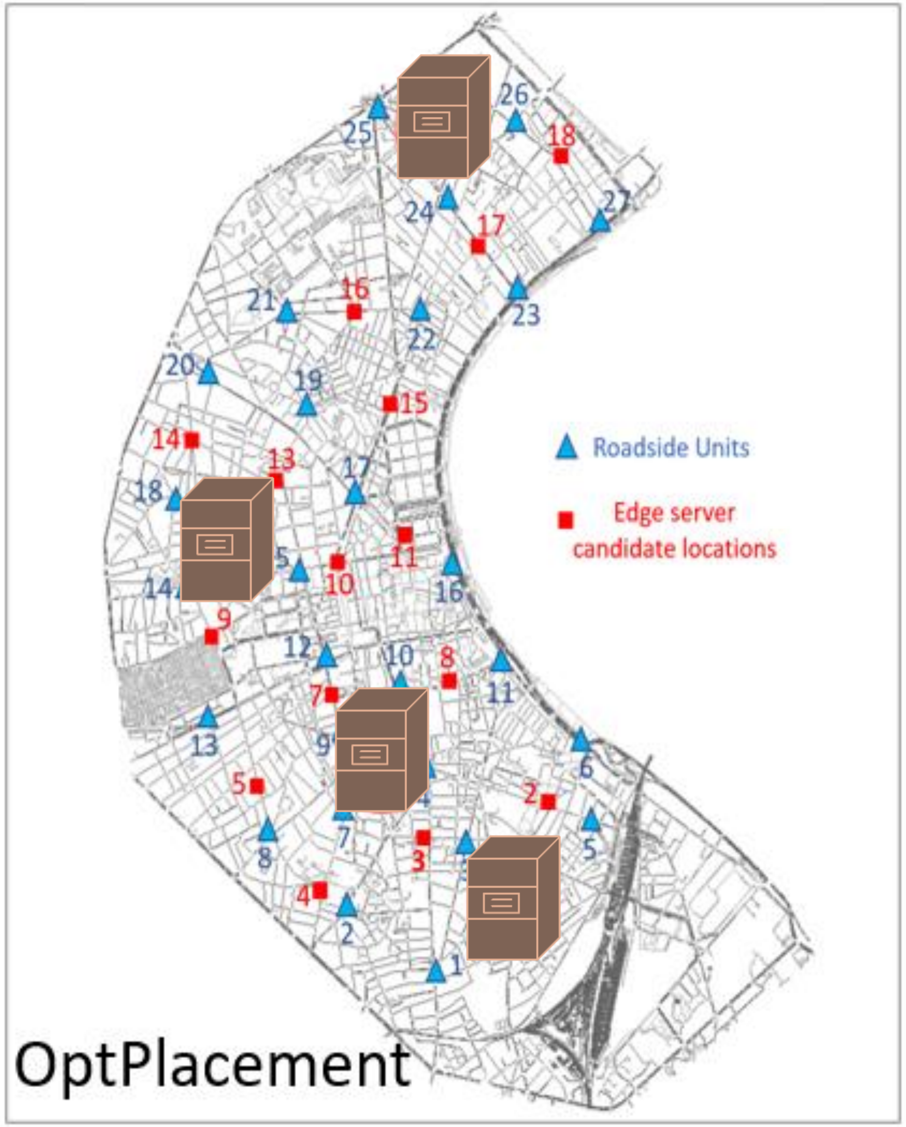
Improved throughput

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

The Edge's contribution to vehicular networks

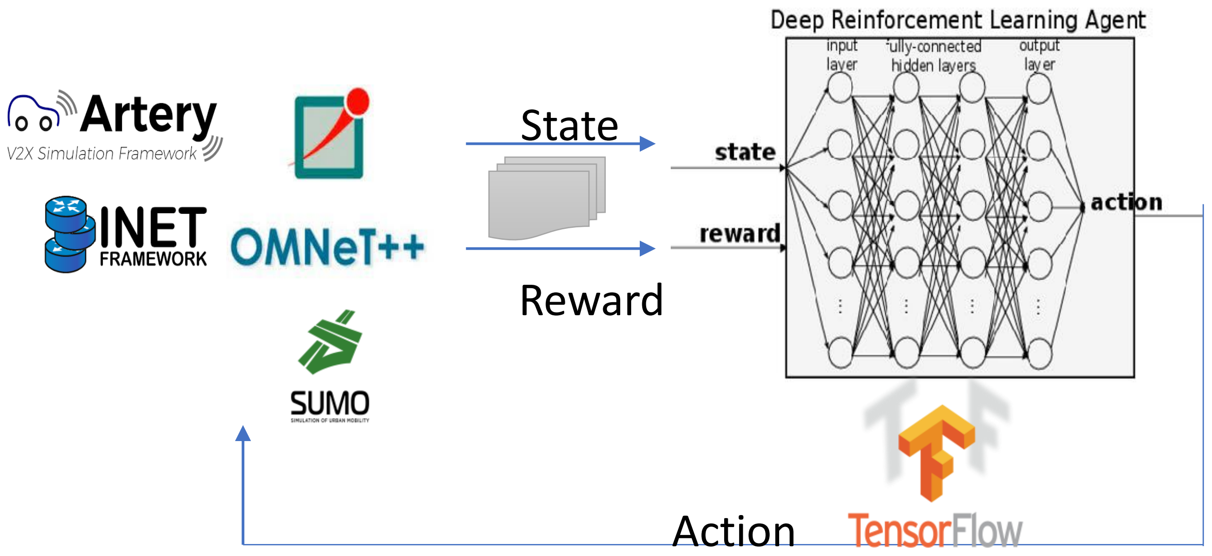
Optimizing EDGE server placements

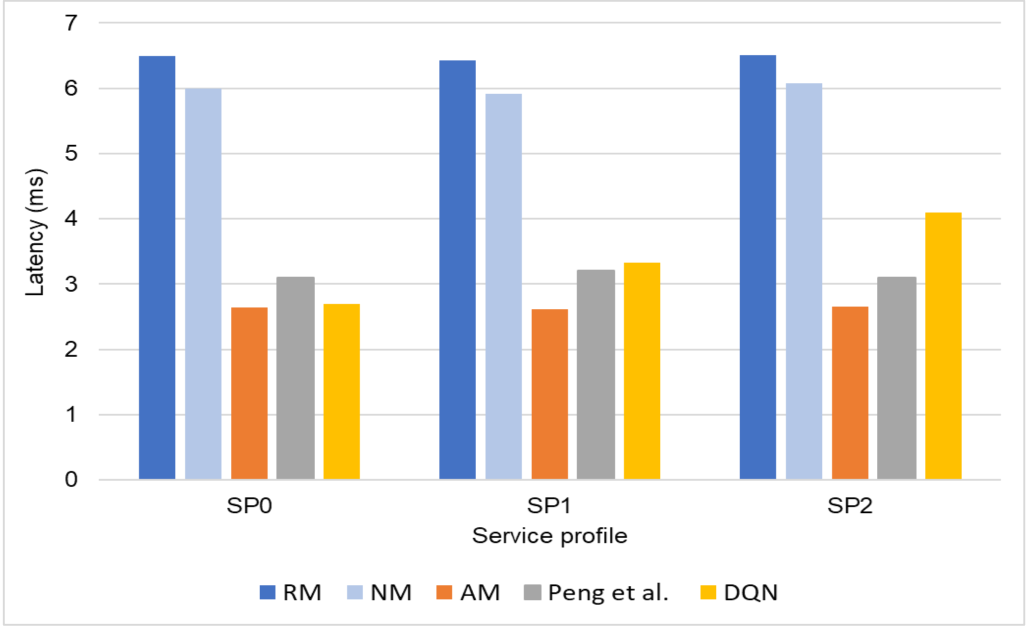
- Choice of the most strategic locations under constraints
  - Cost
  - Latency
  - Load balancing
- Use of linear programming
- Traffic data from Open Data Bordeaux
- Open street Map for mapping Bordeaux



Service migration

- Ensure continuity of service given vehicle mobility
- Use of a migration strategy based on deep reinforcement learning (DRL)
- Definition of service profiles according to V2X service requirements: latency





Latency

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

Proof of concept

Orientation des véhicule sur une voie de péage

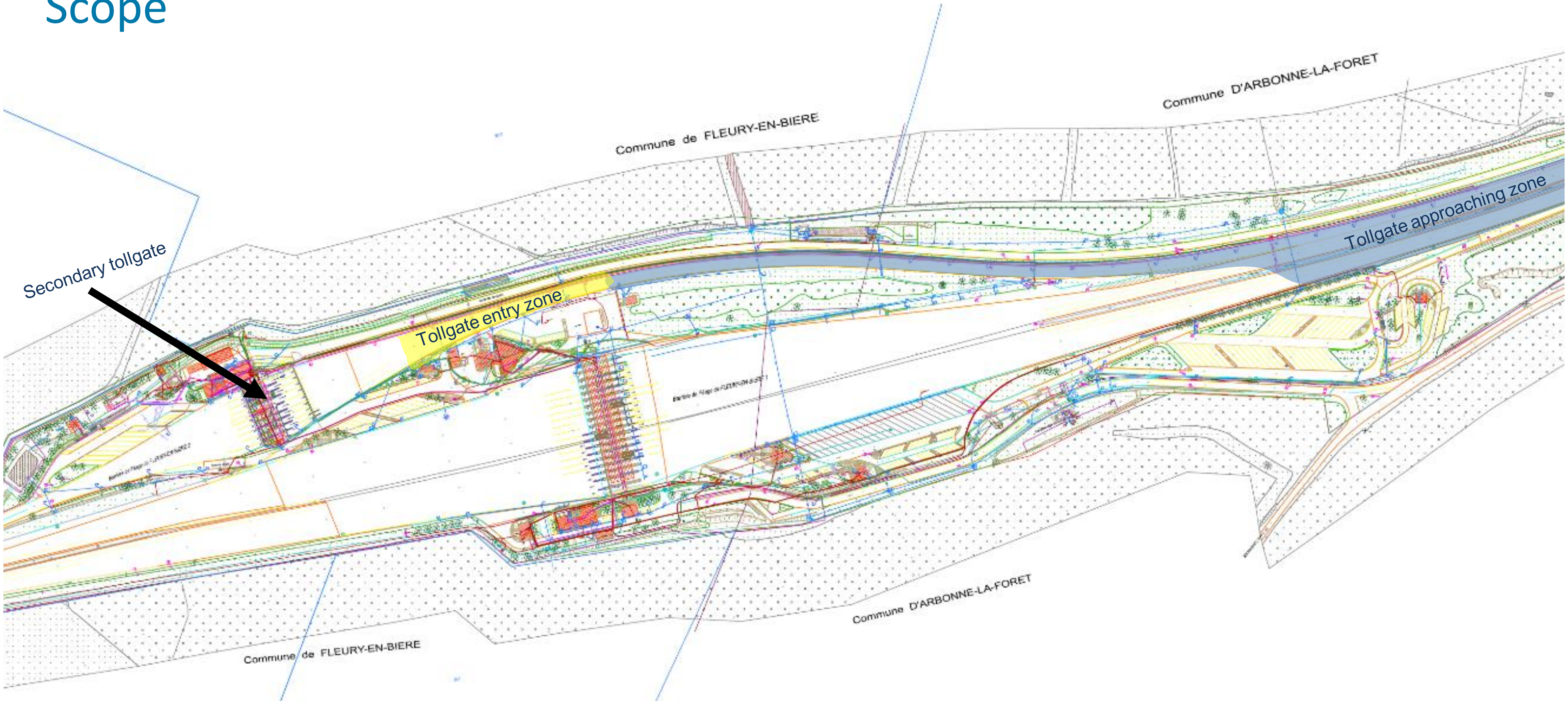
Context

- Use case C4
  - Approaching toll station: driver orientation
- Expected benefits :
  - Safety, driving comfort when approaching a toll station
  - Improve traffic flow at the toll station
  - Test hybridization and use of vMEC to improve vehicle orientation
- Actors in the architecture :
  - Toll Managment System (ToMS)
  - Roadside unit (UBR)
  - Non-autonomous connected vehicles

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

Vehicle orientation on a toll station

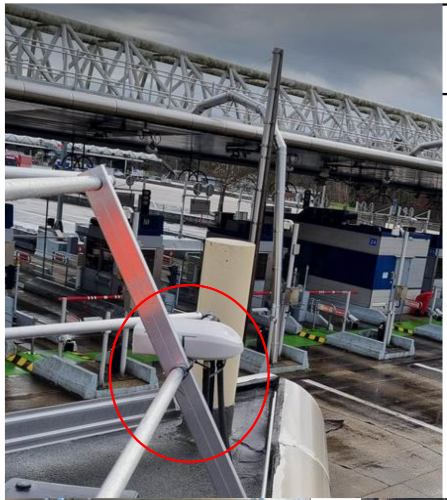
Scope



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

Vehicle orientation on a toll station

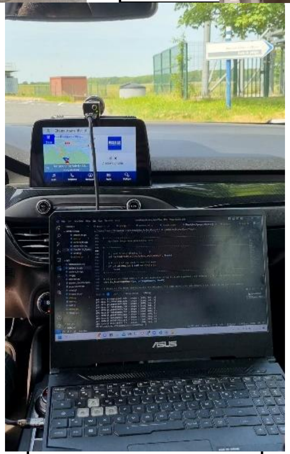
Equipements



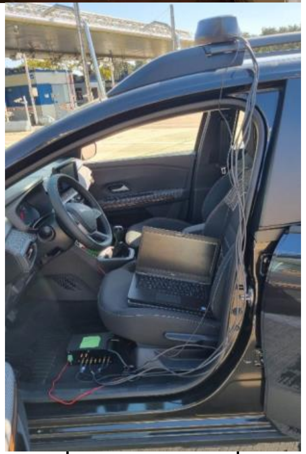
RSU

FS

NeoGLS OBU



Camera and vMEC



YoGoKo OBU

Road Side Unit

- Installed on the roof of the supervision building
- Despite its 4-meter height, we had a coverage of one kilometer

On Board Unit

- Installed inside the vehicle
- The magnetic antenna is fixed to the vehicle roof, ensuring stability

Simulators

- The frame simulator emulates TOMS and reproduces
- IVIM transmission to the RSU.

On-board camera and laptop PC as vMEC

Vehicle orientation on a toll station

Test scenarios

Group 01 – **vMEC Scenarios**

- 01 – Orientation of the vehicle approaching the toll station without using the vMEC server
- 02 – Vehicle guidance on approach to toll station using a vMEC server

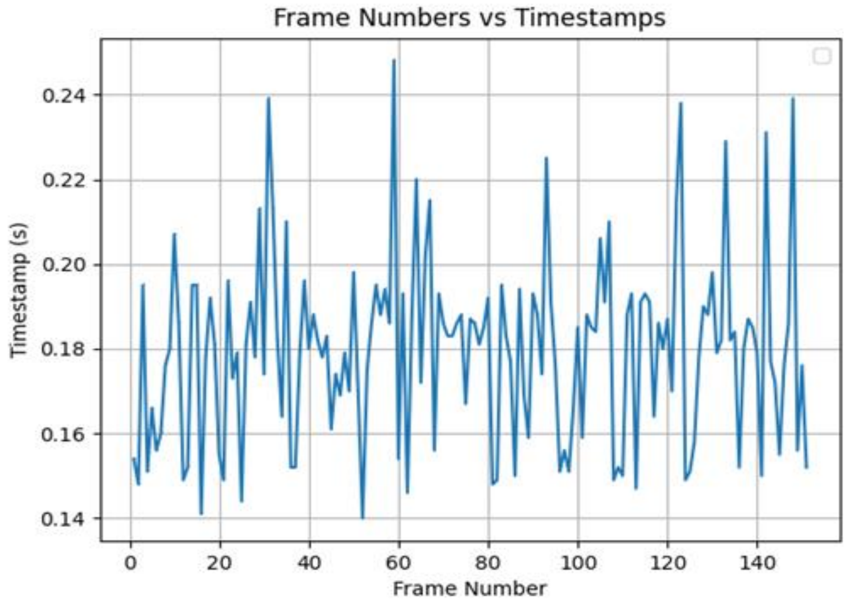
Group 02 – **Hybridization scenarios**

- 01 – Vehicle orientation on approach to toll station without hybrid communication
- 02 – Vehicle guidance on toll approach with hybrid communication
- 03 – Vehicle guidance on toll approach with hybrid communication when ITS-G5 coverage is lower

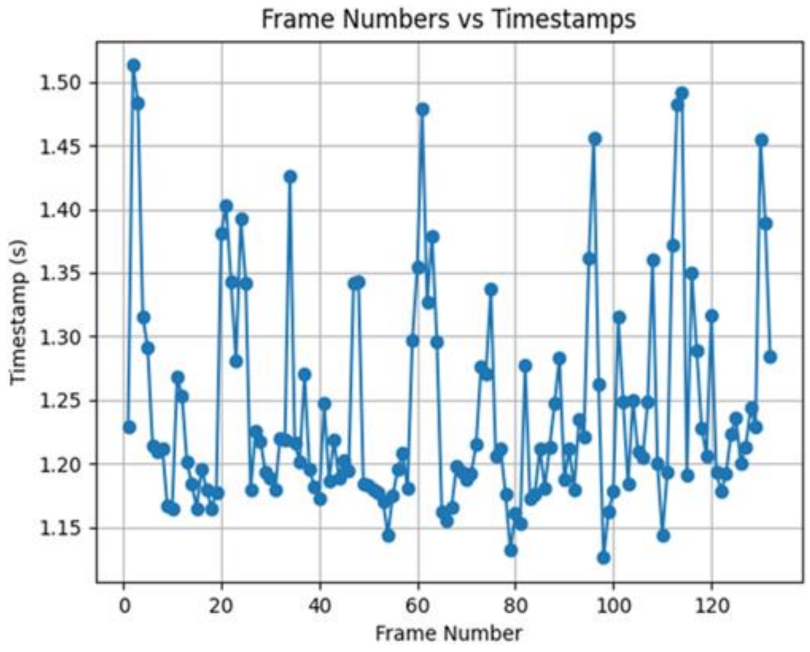
Co-financed by the Connecting Europe Facility of the European Union

Vehicle orientation on a toll station

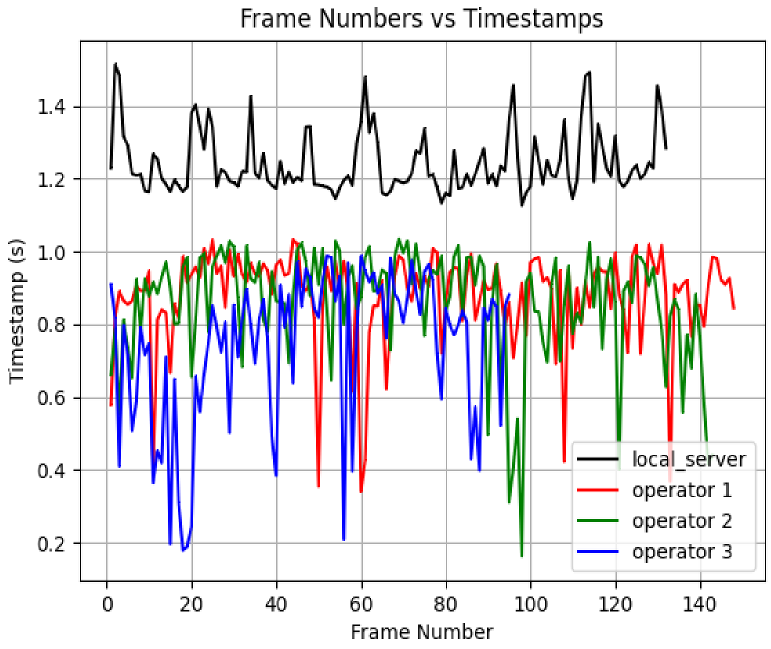
Group 1 results



Without using vMEC



Using vMEC

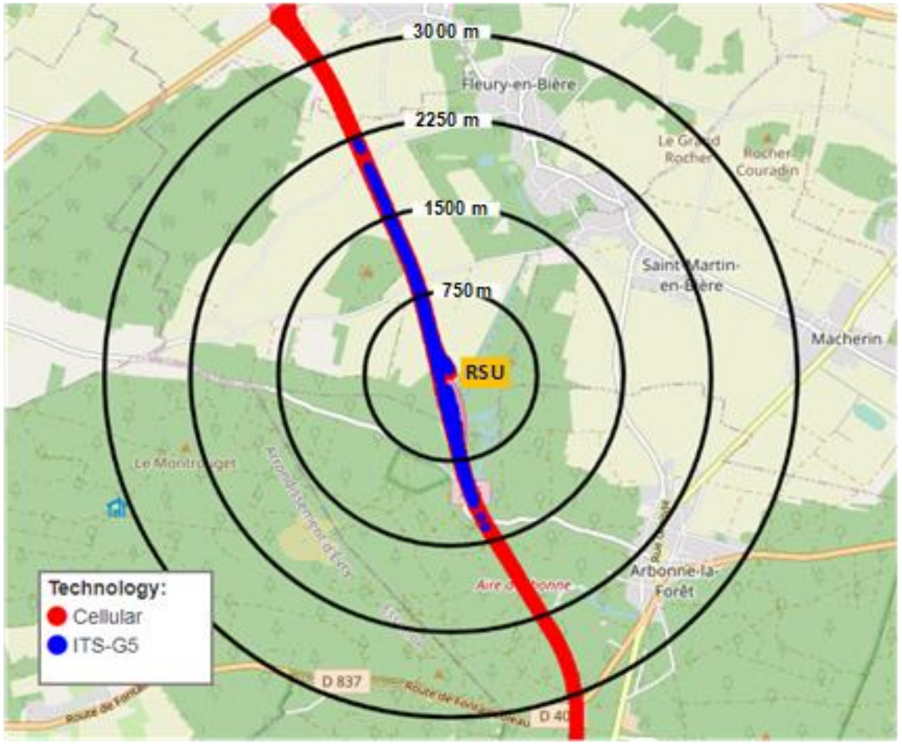


Comparison of approaches

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

Vehicle orientation on a toll station

Group 2 results



Range of both 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

Reliability results (PRR)

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

Conclusion

- Optimization of use cases using hybridization and optimal placement of EDGE calculation sources

- Support for innovative new services requiring improved performance

- Evaluation of new architectures for cooperative intelligent transport systems (C-ITS)

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

Thank you for your attention

Contact

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

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

2.7.2 HD maps

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.

WG 2.7.2 activities

Objectives (GA) :

Characterize the optimisation of the service and safety with the integration of geographic data into InDiD architecture

Specify the characteristics of the minimum set of a cartographic data infrastructure necessary for the experimental deployment of new use cases (Day 1.5 and beyond) and the associated governance aspects.

The working group defined its roadmap around the two main goals :

- Enhance HDMAPS concepts and stakes amongst the stakeholders
- Provide concrete inputs to the other WG defining specs of services and messages

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

Main achievements

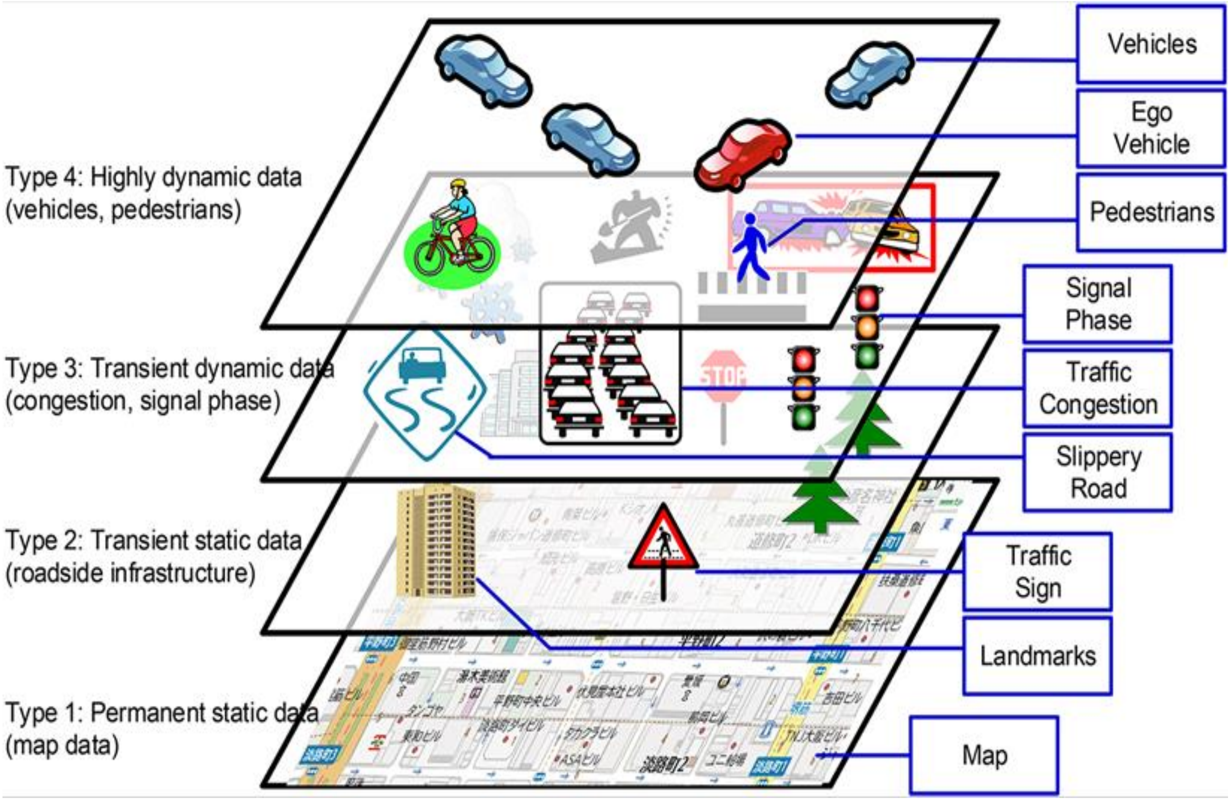
HDMAPS concepts clarification and acculturation

Report 1 – State of the art

HDMAPS = safety enhancement

- "Augmented Perception"
- Redundant sensor providing enhanced environmental information

Local Dynamic Map



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

Core HDMAPS specs enabling MAPEM generation

Contribution to POC «Crossing the Toll barrier »

The challenge :
absence of markings in the relevance zone → no guidance lanes for the AV

HDMAPS dataset : virtual lines high precision definition

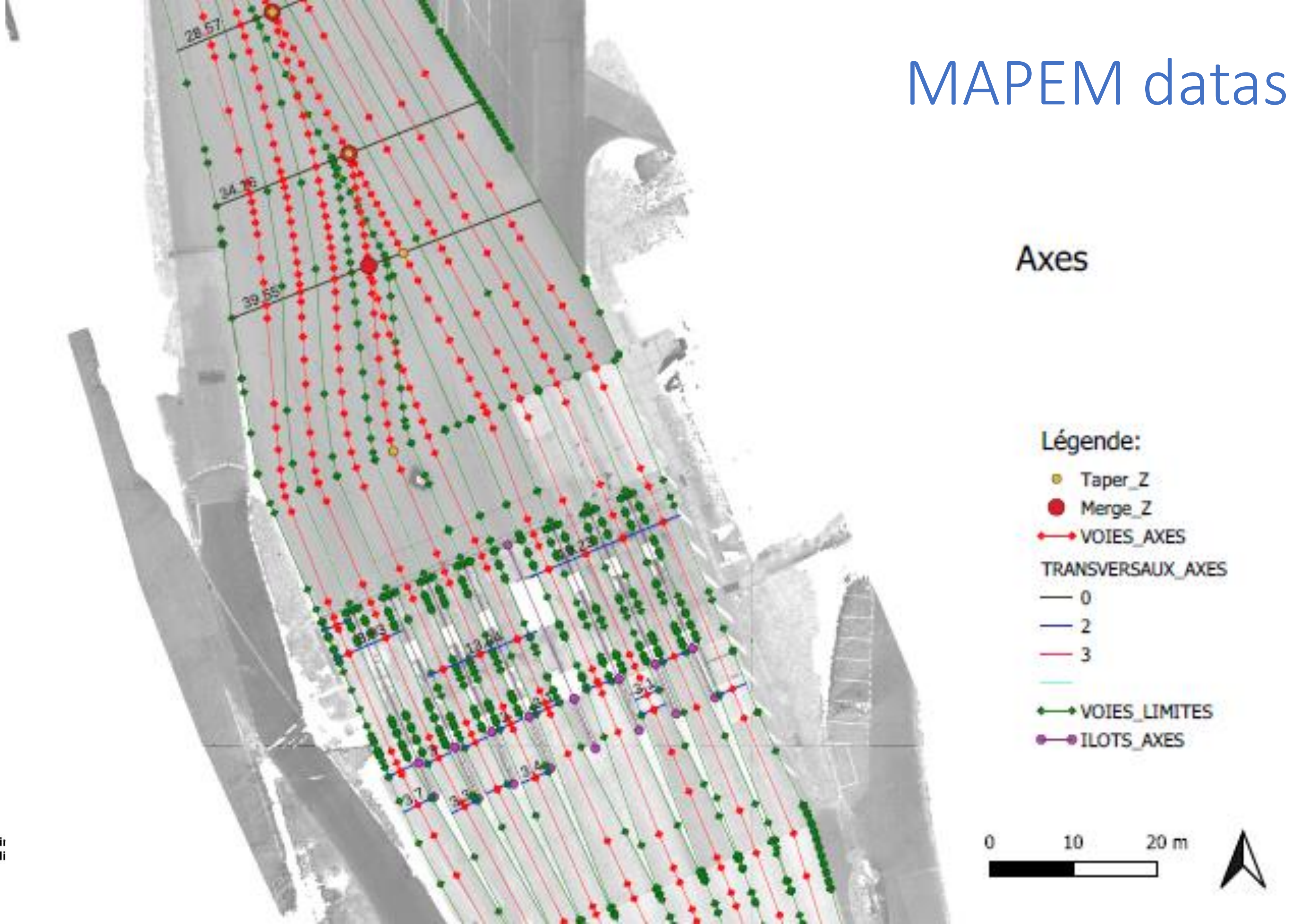
→ MAPEM message : convert geographic lanes into MAPEM specification

→ I2V MAPEM : the road operator send precise trajectory

Perspectives : define the process / extend to other uses cases (SCALE)

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

MAPEM dataset



Co-fi
Facili

Cartographic Data Governance first recommendations

Terrain proof keys of guidance

- Data governance definition : InDiD context, focus on the notion of a shared cartographic infrastructure enabling all the actors to benefit from it.
- Technical and feasability aspects considered in first phase
- retex POC : Core HDMAPS + basic operational elements
- Economic model : to be further considered

The follow-up project SCALE would represent the adequate framework to further consider additional use-cases and the business model aspects.

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

2.7.3 : Security of C-ITS

Rida Khatoun (Telecom Paris)

Towards secured C-ITS

GT 2.7.3

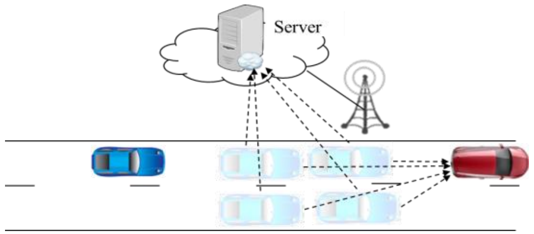
- Tasks
  - Task#1 – Trusted and Secure V2X Communications in a hybrid context (ITS-G5, LTE-V2X, 5G)
  - Task#2 – Protection against Denial of Service (DoS) attacks
  - Task#3 – Security evaluation methodology
  - Task#4 – Security governance
  - Task#5 – Terminals security
- Livrables
  - Security for Edge Vehicular Networks
  - End-to-End security in hybrid V2X communication
  - State of the art on Cyberattacks in C-ITS : Attacks, taxonomy and Countermeasures
  - Proof-Of-Concept for a cyberattacks solution in C-ITS
  - Automatic Verification Tools for Cryptographic Protocols
  - PKI Gouvernance

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

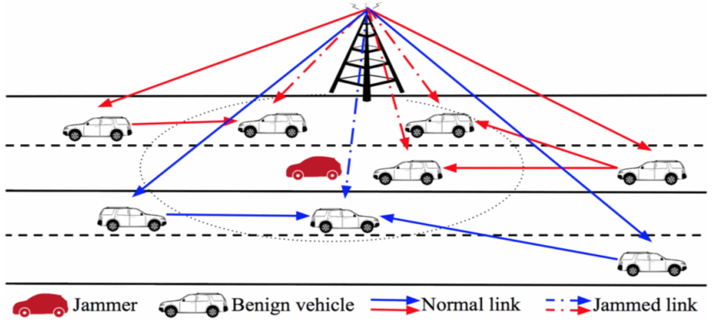
Security challenges in C-ITS

- Categories of potential cyberattacks against C-ITS systems
  - Common attacks to wireless communication systems
  - Specific attacks to C-ITS systems

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



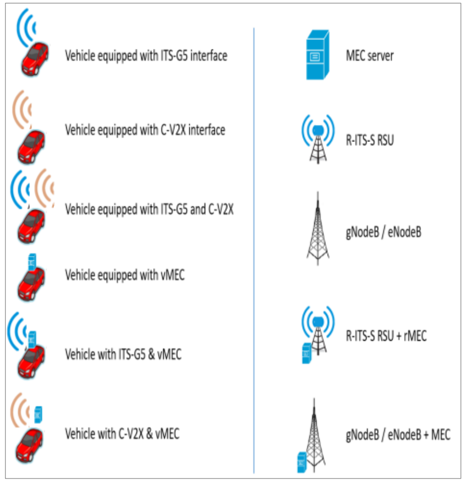
Jamming attack scenario [Gu et al, WiOpt 2018]

		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
		Spamming	A high volume of messages introduced intentionally to increase the transmission latency and consume the bandwidth of network	R-ITS-S ITSS-C
		Black hole	A node which drop, misrouting or redirecting message	V-ITS-S R-ITS-S
		Malware	Introduction of malicious software	V-ITS-S R-ITS-S ITSS-C
		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
		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

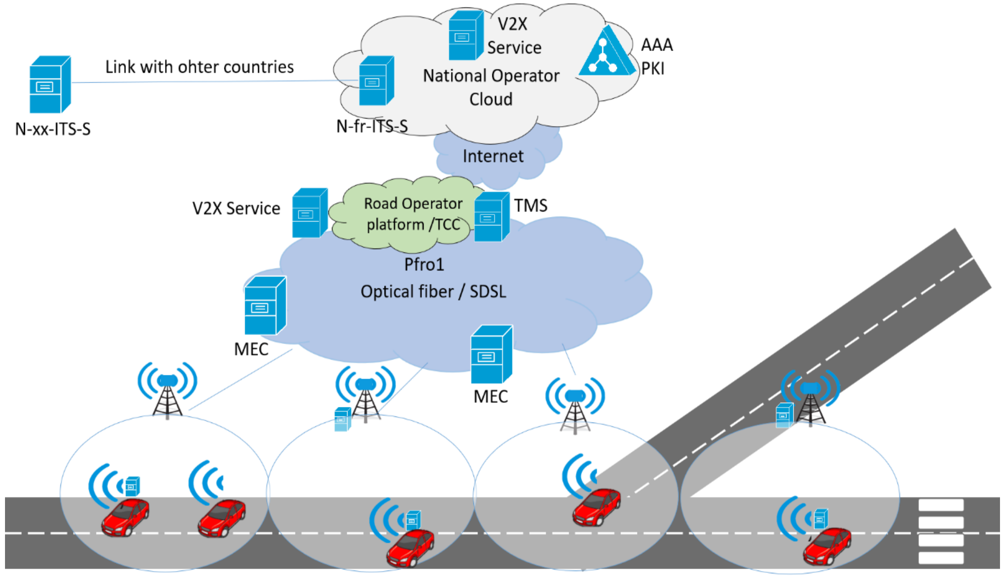
Co-financed by the Connecting Europe Facility of the European Union

Security for Edge Vehicular Networks

- **New Mobile Edge Computing-based architecture**
  - Components
    - vMEC servers deployed on vehicles,
    - MEC servers deployed on RSUs
    - MEC servers deployed in other locations and provide computing and storage resources to multiple RSUs.
  - Functions
    - Interconnection between the different components of the system
    - V2V/V2I connections
    - Interconnection between MEC servers and the hosting elements,
  - Recommendations for InDiD : Data security at the edge level with TPM, IDS at edge, …



*MEC: Mobile Edge Computing



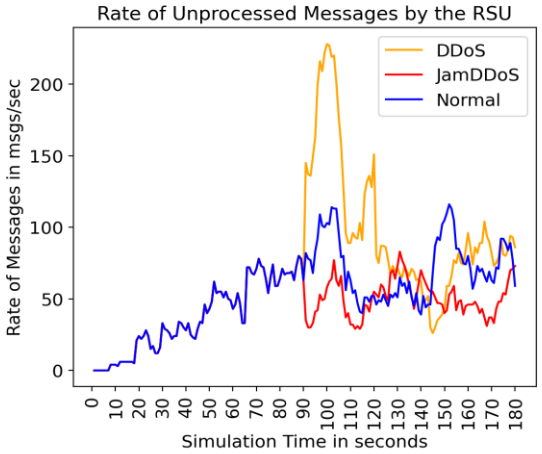
Co-financed by the Connecting Europe Facility of the European Union

Cyberattacks detection in C-ITS

- Study of the impact of Distributed Denial of Service on RSU and V-ITS-S
  - Simulators
    - SUMO for traffic modeling
    - OMNeT++ as a network manager
    - Artery
  - Protocols: ETSI ITS-G5, GeoNetworking et BTP (Basic Transport Protocol)
  - Environment
    - Traffic data on the A1 highway between the cities of Paris and Lille
    - 2 km sample on the Paris side (susceptibility to attacks during rush hours due to the high volume of cars)

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



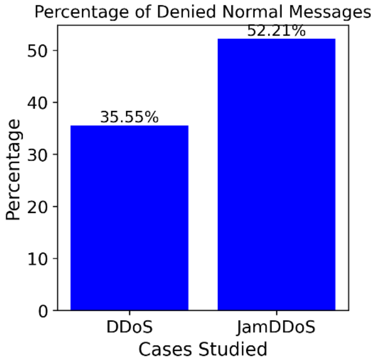
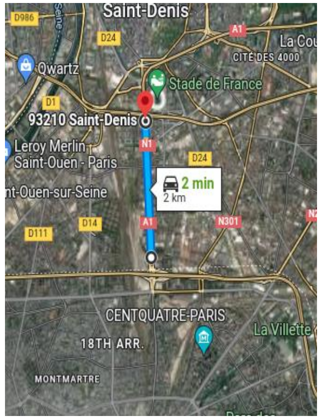


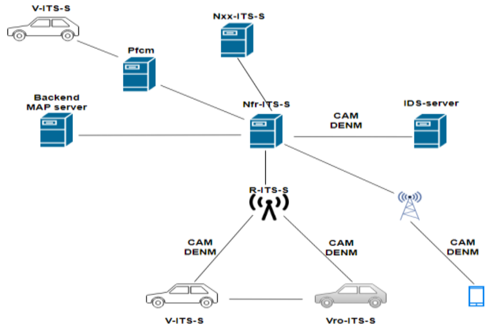
TABLE I
COMMON SIMULATION PARAMETERS

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

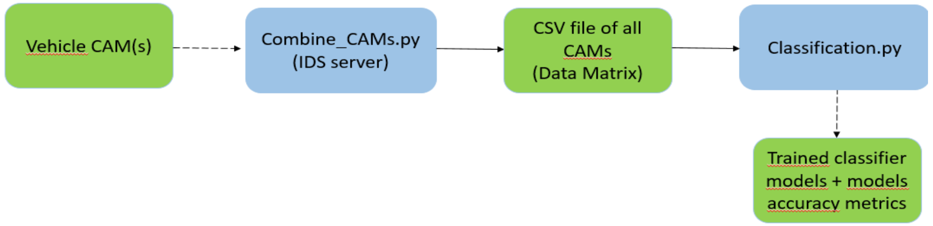


Co-financed by the Connecting Europe Facility of the European Union

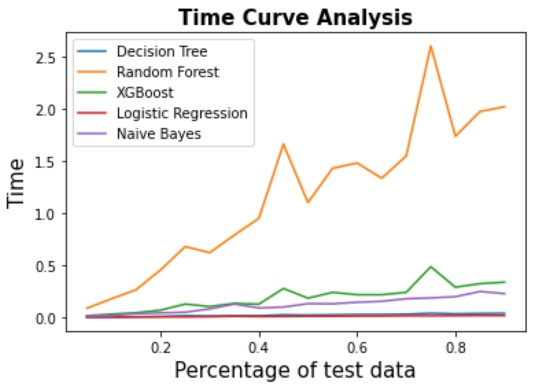
Cyberattacks detection in C-ITS

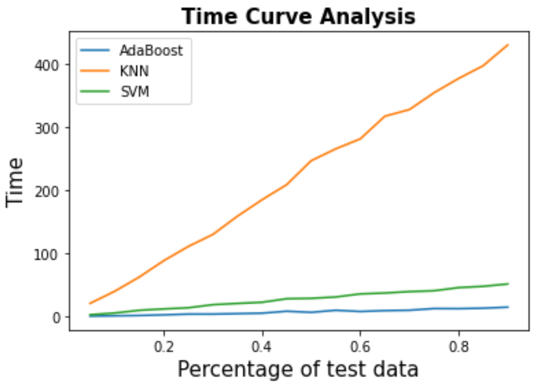


- ML-based intrusion and attacks detection approach
- Use case: DDoS & Sybil attack
  - V-ITS-S bot launches a DDoS against an R-ITS-S
  - V-ITS-S bot utilizes CAM messages
  - VeReMi dataset : 5 position falsification attacks, 3 vehicle densities (low, medium, and high), 3 attacker frequencies (10, 20, and 30 %)
  - CAMs are forwarded to an Intrusion Detection System (IDS) server for analysis
  - Information: Received time of CAM, Vehicle's ID, coordinates of the vehicle's position
  - Vehicular position error, sendTime, sender, senderPseudo, messageID, vid_start_time



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

To protect C-ITS

- Recommendations for INDID:
    - TLS1.3, VPN IPSEC, ECDHE, secure WebSocket
    - Use expressive formal language for specifying protocols and their security properties
    - Use common security measures
    - Deploy an Intrusion Detection System (IDS) at the high level servers
    - Deploy IDSs at the edge servers (signature-based and behavior-based)
    - CAMs messages analysis for attack detection
        - Cyberattacks proved by simulation
        - Sybil attack is a dangerous one
        - BotVehicles (a set of malicious vehicles) are a real threat
    - Promote security assessment
    - Analyze each security protocol using a formal verification tool such as ProVerif or Scyther
    - Apply GDPR and ISO 27000 for PKI and certification frameworks

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

2.7.4 – Road operator's infrastructure enhancement

Christelle BERNIER - CEREMA

Emilie BOURDY - URCA

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

- Many problematics from road operators with previous projects at the beginning of InDiD:
  - Road operator has centralized equipment, but many data sources. How can we define identical aggregation zones of CAM on several equipment to easily merge received data?
  - Currently, deviation management is very hard to road operators (regulatory deviation authorization, …) and there was no defined messages (in 2019) to send a deviation. How can we transmit this deviation information to users?
  - SCOOP’s CAM-I is finally not much used. How can we improve CAM-I? It is still relevant in the actual context?
  - How can we improve vehicle’s positioning?
  - Can meteorological data from road operator be transmitted to users? If yes, how?
  - How can me transmit travel time efficiently to users?
  - Some new vehicles scan roads and print speed limits to road users. Can we upload these data to road operators to ensure visibility of these road signs?
  - Is it possible to send C-ITS messages conform to specifications from trailers, which has no HMI?

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

What is done

- 12 deliverables wrote in this WG
- Three of them will be discuss today:
  - CAM-I and service announcement
  - Deviation
  - CAM aggregation

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

Service announcement

- In SCOOP and C-ROADS: use of CAM-I to annonce services (mitigation, log upload, PKI connection). Unrecognized in the European level.
- CAM-I are not much used. How can we improve CAM-I? Is it still pertinent in the actual context?
- Survey to understand road operator’s needs: 13 identified services: CAM-I cannot do.
- SAEM used by other partners (platooning, electronic toll collection system)
- Decision to use SAEM.

SAEM

- Service Announcement Essential Message
- ETSI EN 302 890-1 standard
- Many services at the same time
  - 270 549 119 in all
- Service announcement
  - Possibility to add others if needed
- Services are not in the message

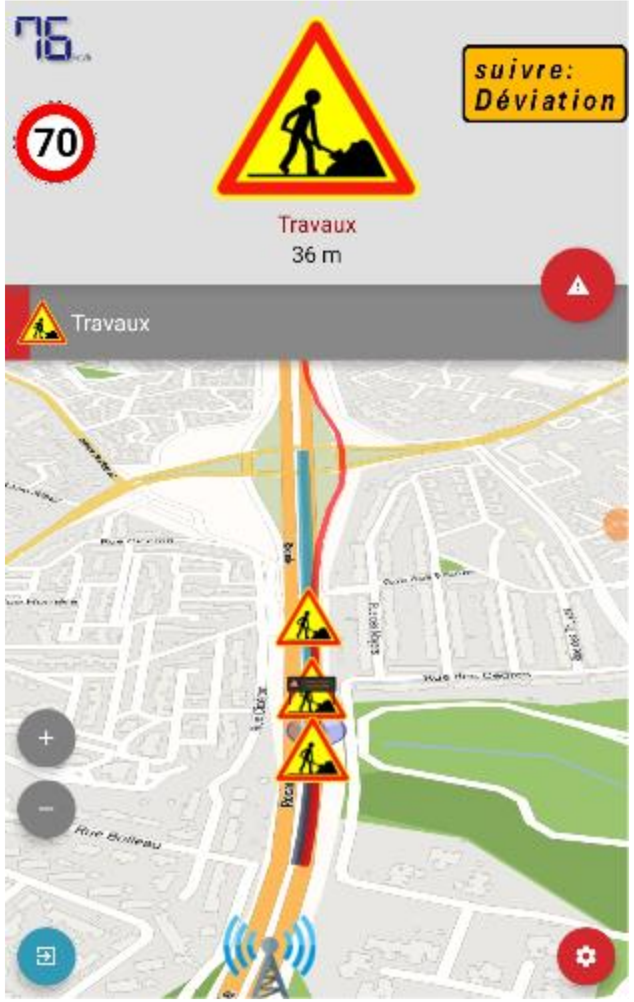
CAM-I

- Cooperative Awareness Message – Infrastructure
- Scoop@f message – CAM extension
- 1 at a time - 256 in all
- Limited by existing services but extensible
- Services are integrated to the message
- Non standard

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

Deviation POC

- Currently, deviation management may be very hard for road operators (regulatory authorization, impact on neighbor's road, …) and there were no defined C-ITS message (in 2019). How can we transmit deviation information to users?
- Two phases answer:
  1. Organisational analysis by road operators
  2. Technical definition of the deviation:
     - C-ITS DATEX-II definition (conformance to TIPI)
     - Use of ReroutingManagement
     - IVIM ⟶ DENM and IVIM ↔ IVIM connection
     - C-ITS DATEX-II prototype from URCA
- POC from simulation (URCA) then on road with DIRA's RSU (NeoGLS)



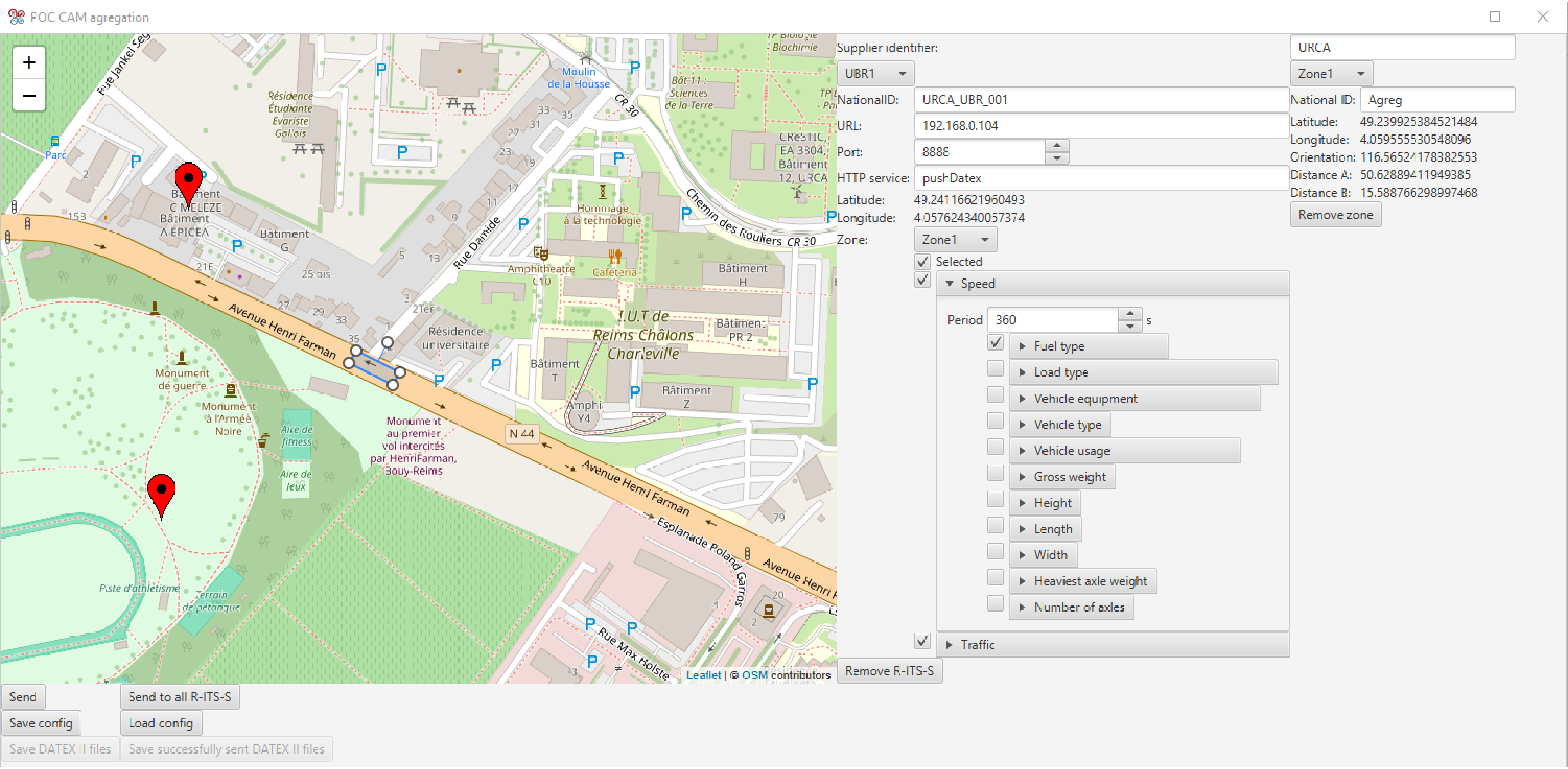
Co-financed by the Connecting Europe Facility of the European Union

CAM aggregation

External setting tool

- Road operators have centralized equipment, but many data sources. How can we define CAM aggregation zones identical for many equipment in order to easily merge received data?
- CAM aggregation area configuration
  - Internal to each provider
- Possibility to use C-ITS DATEX-II
  - Road operator’s side development is needed
- POC of external setting tool from URCA
  - Zones and RSU configuration: with or without classes, aggregation type, etc.
  - Send of C-ITS DATEX-II to RSU

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



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

Conclusion

- 2.7.4 WG solved many problematics from road operators.

  All studies are synthetized in the “milestone 36” deliverable.
- Every subject need time to be understood, adapt road operator’s back office to C-ITS services, and for road operator to take them.
- Now it is to implement these services.

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

Appendix 1

List of services requested by road operators

1. Winter conditions
2. Meteorological data
3. GPS positioning improvement
4. Travel time, route
5. Temporal synchronisation
6. Data upload
7. Platooning
8. Permanent restriction on road for all road operator network
9. RSU’s positioning and status
10. HD cartography download
11. EDGE computing
12. Mitigation
13. Lane access service

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

Thank you for your attention