Département de Recherche en Ingénierie des Véhicules pour l' Environnement

EA 1859 research department in vehicle engineering for the environment

Intelligent Vehicle Team

IRT SYtemX
February 23rd, 2017

Sidi Mohammed Senouci
Full Professor

CONFIDENTIAL

Institut Supérieur de l'Automobile et des Transports - 49, rue Mademoiselle Bourgeois - BP 31 58027 Nevers cedex
Téléphone : 03 86 71 50 00 / Fax : 03 86 71 50 01

ISAT in short

- Created in 1991 and part of the Université de Bourgogne, ISAT awards engineering degrees accredited by the Commission des Titres de l'Ingénieur and EUR ACE labeled
- ISAT is a network of over 1,250 engineers
- Each year group takes in 150 students i.e. 650 students total
- ISAT's community counts 50 tenured teachers and 20 administrative & technical clerks
- 8,000 m^2 campus dedicated to teaching, research & student life
- ISAT hosts a research laboratory: DRIVE EA 1859

DRIVE laboratory: organisation

DRIVE

Energy, Propulsion, Electronics Environment

Energy & Propulsion

Pr. Luis Le-Moyne

Intelligent Vehicles

Pr. Sidi M. Senouci

Mechanics & Acoustics for Transport

Durability & Composite Structures

Pr. Shahram Aivazzadeh

Transport Vibration & Acoustics

Pr. Philippe Leclaire

DRIVE laboratory: research scope & resources

Durability & Composite Structures

Transport Vibration & Acoustics

Tomorrow's materials: weight-reduction, performances, comfort & safety

- ✧ **Assemblies**, repairing & bonding
- ✧ Impact-behavior & **life duration**
- ✧ **Wood** & bio-based materials
- ✧ **Acoustic properties** of complex materials
- ✧ **Vibration properties** of multilayers

Energy, Propulsion

Intelligent Vehicle

Energy saving on time & mileage

- ✧ **combustion** optimization
- ✧ **hybrid motorisations**
- ✧ energy-oriented **depollution solutions**
- ✧ **Internet of Vehicles**
- ✧ **V2G** and **G2V**
- ✧ **Network security**
- ✧ **onboard vision** systems

→ **31** researchers/teachers

→ **1** research engineer

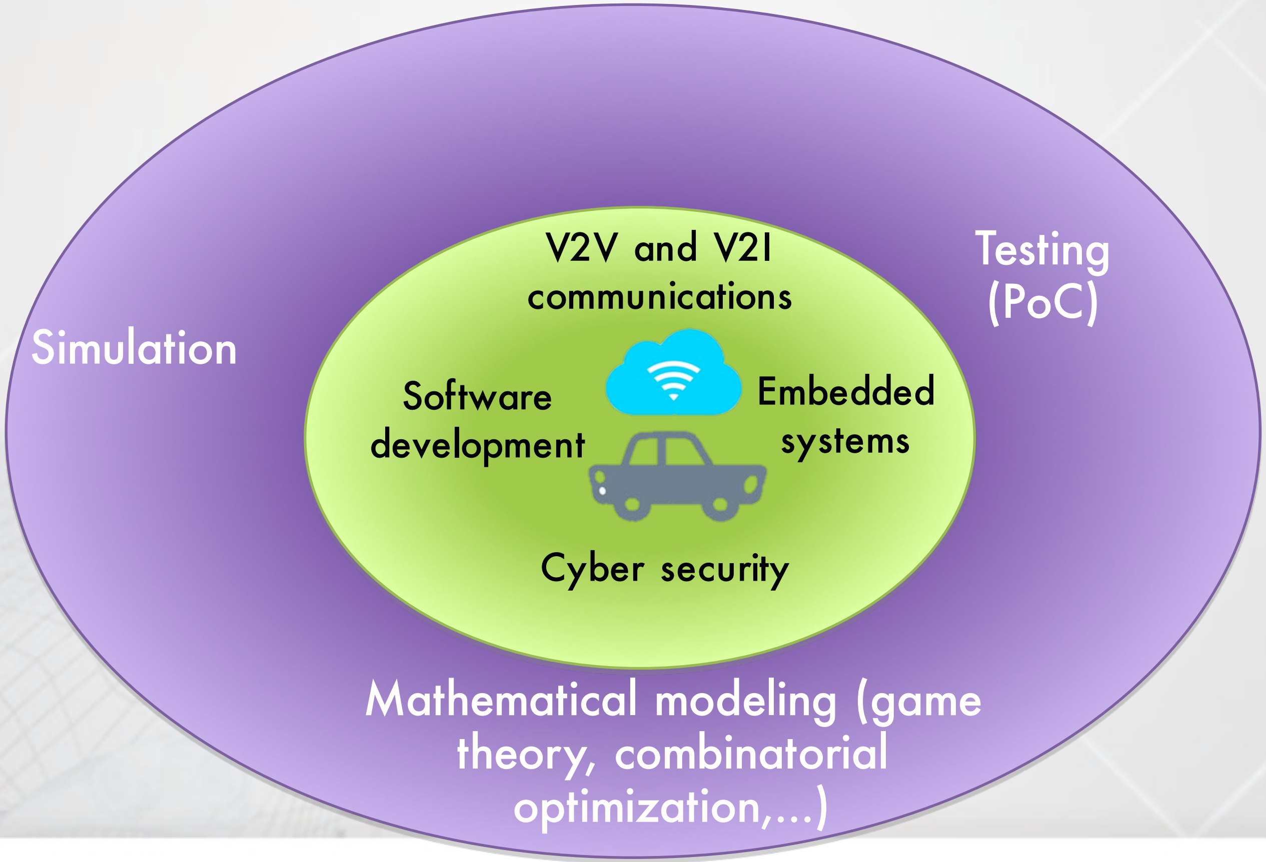
→ **18** PhD candidates (dissertation in progress)

→ **3** postdoctoral students

- **Members :**
- **1** Full professor : SM. Senouci (depuis 9/2010)
- **3** Asociate Professors : P. Brunet (9/2006), E. Aglzim (9/2010)
  A. Kribeche (03/2013)
- **9** PhDs : M.A. Messous, F. Sanchez,
  M. Attia, **I. Allal (CIFRE),**
  K. Dhifallah (CIFRE),
  M. Ramirez (joint PhD, Mexico),
  E. Almeneh (joint PhD, Ethiopia)
  M. Habtamu (joint PhD, Rtiopia)
  A. Arfaoui (joint PhD, Tunisia)
- **1** Postdoc : J. Klami

Vision and scientific approach

Consider the vehicle as an intelligent and communicating entity that interacts with the infrastructure to make the vehicle safer, cleaner and more autonomous




MOBILITY
SUSTAINABILITY
CONNECTIVITY


Axis 2
ICT for a
Sustainable mobility

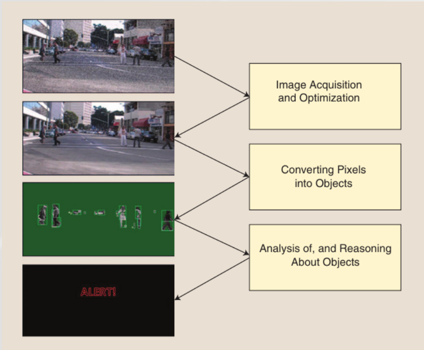

Axis 1
ICT for a
Connected mobility

Scientific axis and associated resources

Axis	Themes	Teachers/Researchers	Ongoing PhDs/postdocs
Axis 1 **ITEA2 CARCODE 2012-2015**	Cooperative data collection Cooperative and secure data exchange/routing Data processing in order to offer services to vehicles (route planning, vehicle tracking, etc.)	S. Senouci P. Brunet A. Kribeche	T. Bouali M.A. Messous F. Sanchez M. Ramirez I. Allal K. Difallah H. Sedjelmaci (postdoc)
Axis 2 **ITEA2 FUSE-IT 2014-2017**	Data collection for better use of electric energy, with an application to the couple SmartGrid - electric vehicles Secure data exchange in the SmartGrid Data processing for better power management for electric vehicles (route planning, electric charging station deployment, etc.)	S. Senouci E. Aglzim	M. Attia H. Sedjelmaci (postdoc) J. Klaimi (postdoc)

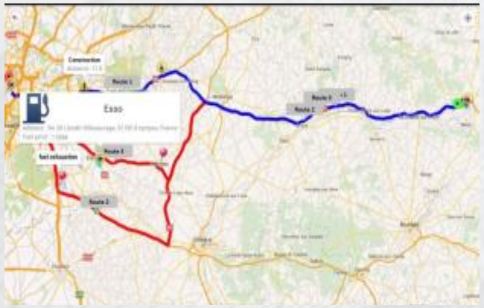
Productions scientifiques 2010-2015

Axis 1



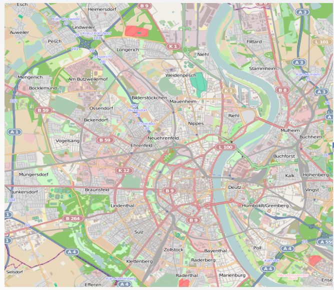
Moving objects detection

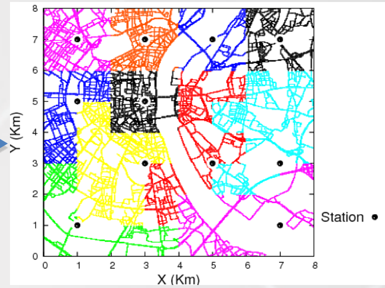
2 autonomous vehicles



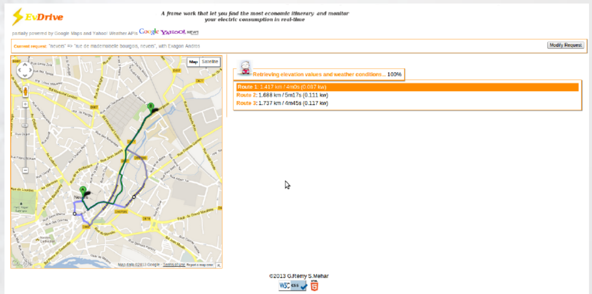
Android Application for route planning

Axis 2





Optimal deployment of charging stations



Web application for route planning for electric vehicles

Energy Efficient Building

Interaction with the economic environement

Axis 1	Axis 2

European project CarCode

- Platform for Smart Car to Car Content Delivery
- January 2013 – December2015
- 3 countries (France – Turkey– Portugal)

CarCoDe

European project FUSE-IT

- Future Unified System for Energy and Information Technology
- October 2014 – October 2017
- 4 countries (France – Belgium – Turkey– Portugal)

FUsEIT

3 contracts with Orage Labs

1. Heterpgenous networks in the context of transport (2010-2013)
2. Energy Efficiency and Quality of Experience of a microcellular networks (2014-2017)
3. Shared resource management in crowd networks (2015-2018)

orange™

Scientific achievements since 2010

- **3 graduated PhD defenses** (G. Rémy, 2013 ; S. Mehar, 2014; T. Bouali, 2016) **+ 5 in 2017**
- **≈25 indexed journal papers** (**at least 3 publications before the PhD viva**)
- 1 patent
- **≈60 international conferences**
- **≈16** national conferences

International recognition since 2010

- **Hosting 20 Phd students** (Mexico, Algeria, Tunisia)
- **Hosting 3 invited professors** (UK, Algeria, Canada)
- Different invitation as speaker in conferences and universities
- **High involvement in IEEE** (Chair of the technical committee IIN, 2014-2015)
- Participation to the organization of ≈40 international conferences

Some partners

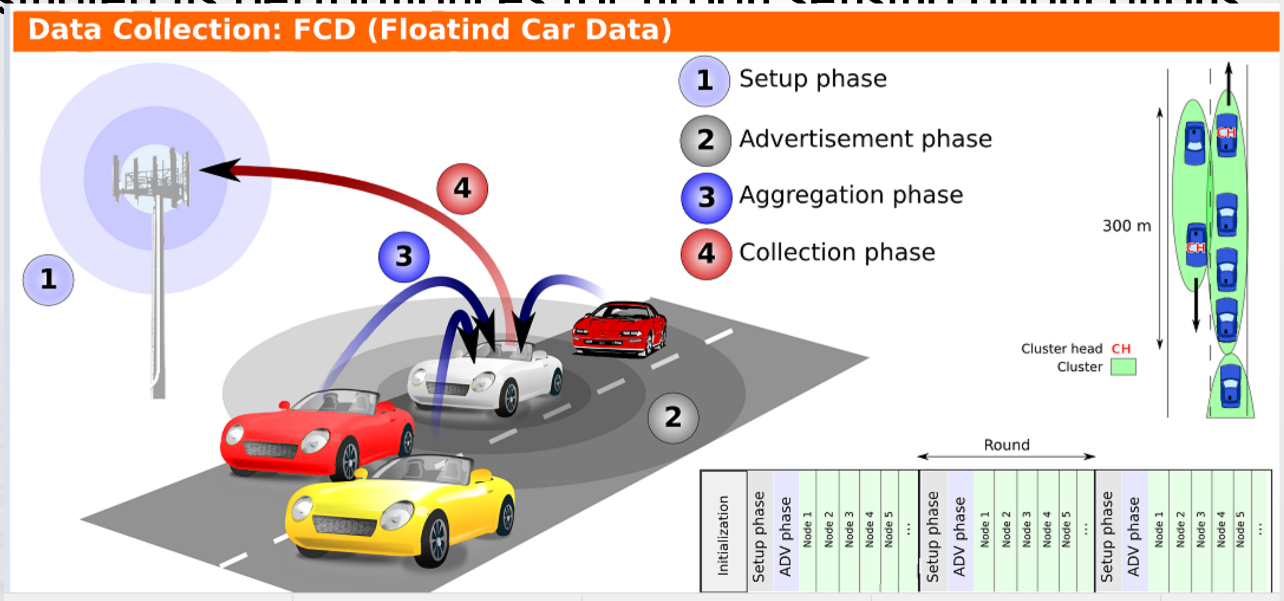
Academics

Industrials

755 k€ since 2010

LTE4V2X:

- A novel framework for a centralized vehicular network organization using LTE
- It takes advantage of a centralized architecture around the eNodeB in order to optimize the clusters management and provide better performances.
- We studied its performances for urban sensing applications.



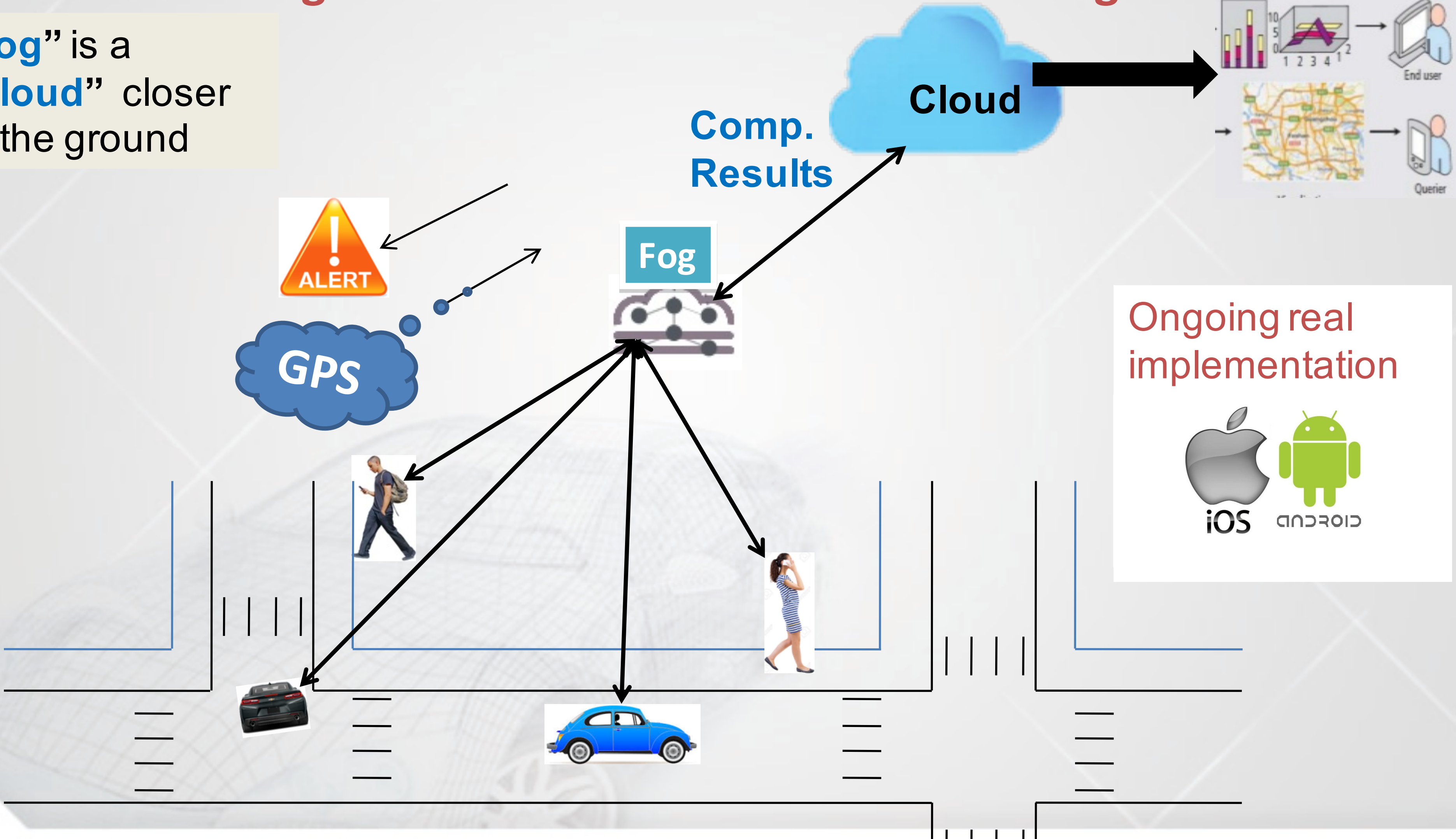
Fog Node Assisted Mobile Crowdsensing

- As European Commission **2015 road safety statistics** depicts **39%** road fatalities are of pedestrians
- Using sensing capabilities of smartphones, we propose Fog Computing based solution to protect vulnerable road users (VRUs) especially pedestrians from accidents
- In this research we propose a **three-tier fog computing based architecture** where **Fog Node** processes delay sensitive data for alerting pedestrians

ICT for connected mobility: Data collection

Fog Node Assisted Mobile Crowdsensing

"**Fog**" is a "**cloud**" closer to the ground

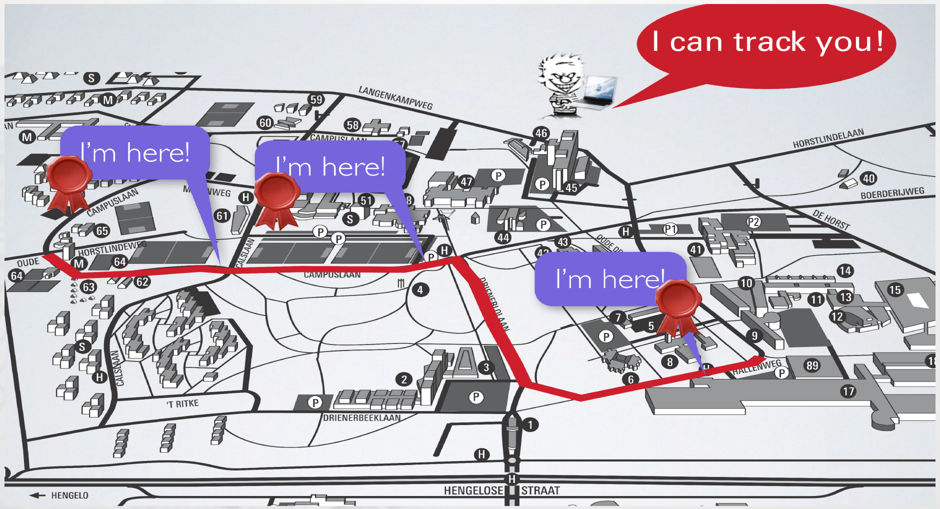


Ongoing real implementation

Towards an Efficient Pseudonym Management and Changing Scheme for Vehicular Ad-Hoc Networks

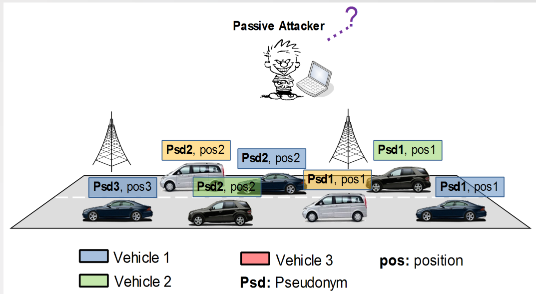
- Why ?
  1. Many VANET's applications need a beaconing mechanism
  2. Safety messages must be authenticated, **but not** encrypted

➔ Location tracking becomes easy (privacy !)



ICT for connected mobility: Privacy

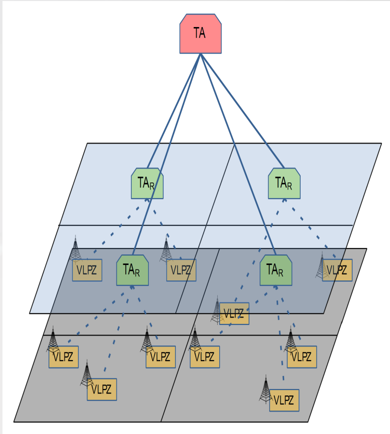
- Pseudonym changing approach: Description
  - Each vehicle have a set of pseudonyms (temporal IDs)
    - Current standards (IEEE 1609.2 and ETSI 102941) are based on a public key infrastructure (PKI), where the pseudonyms represent **a set of certified public keys stored in the vehicle’s OBU**
  - Vehicles change periodically their pseudonyms
  - Only the authorities know the relationship between the real identifier of the vehicle and its pseudonym.



- Pseudonym changing approach: Limitations
  - The pseudonyms could be linked (pseudonym linking attack)
  - The distribution of pseudonyms sets & CRL requires that the VANET area should totally be covered by RSUs
  - ...

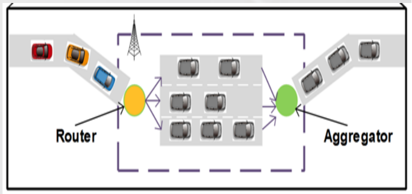
Scheme design

- New efficient pseudonym changing and management scheme based on Vehicular Location Privacy Zone (VLPZ)
  - **Hierarchical structure** that mainly based on **specific zones c**alled Vehicular Location Privacy Zones (VLPZs)
  - The strategy of **changing** of pseudonym and the **distribution** of pseudonyms sets and CRLs are performed inside the VLPZs
  - This scheme also includes a reputation-based mechanism to stimulate vehicles for entering to VLPZs

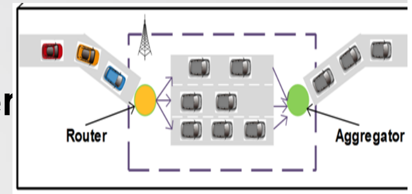


VLPZ-Model

- VLPZ can easily be implemented in the existing roadside infrastructures: gas stations, electric vehicles charging stations, new independent RSUs, etc.
- VLPS = one entry point, one exit point and a limited number of lanes l > 1 and equipped with a RSU



VLPZ-Based Pseudonym Changing Strategy



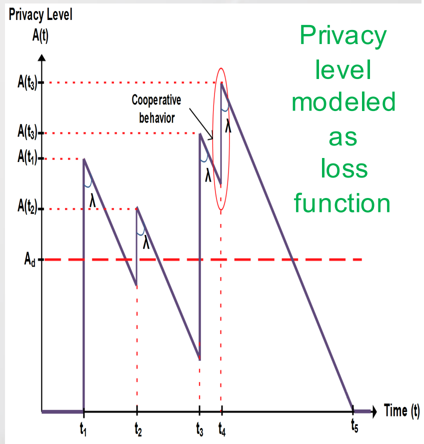
- Vehicles arrive to a VLPZ, one after another, on a one-lane
- Vehicles heads for a **randomly** VLPZ's lane assigned by the router
- Vehicle reside inside a VLPZ for a random period of time
- Vehicles exit a VLPZ through the aggregator with an order different from the entering order

Motivating Vehicles to Enter to the VLPZ

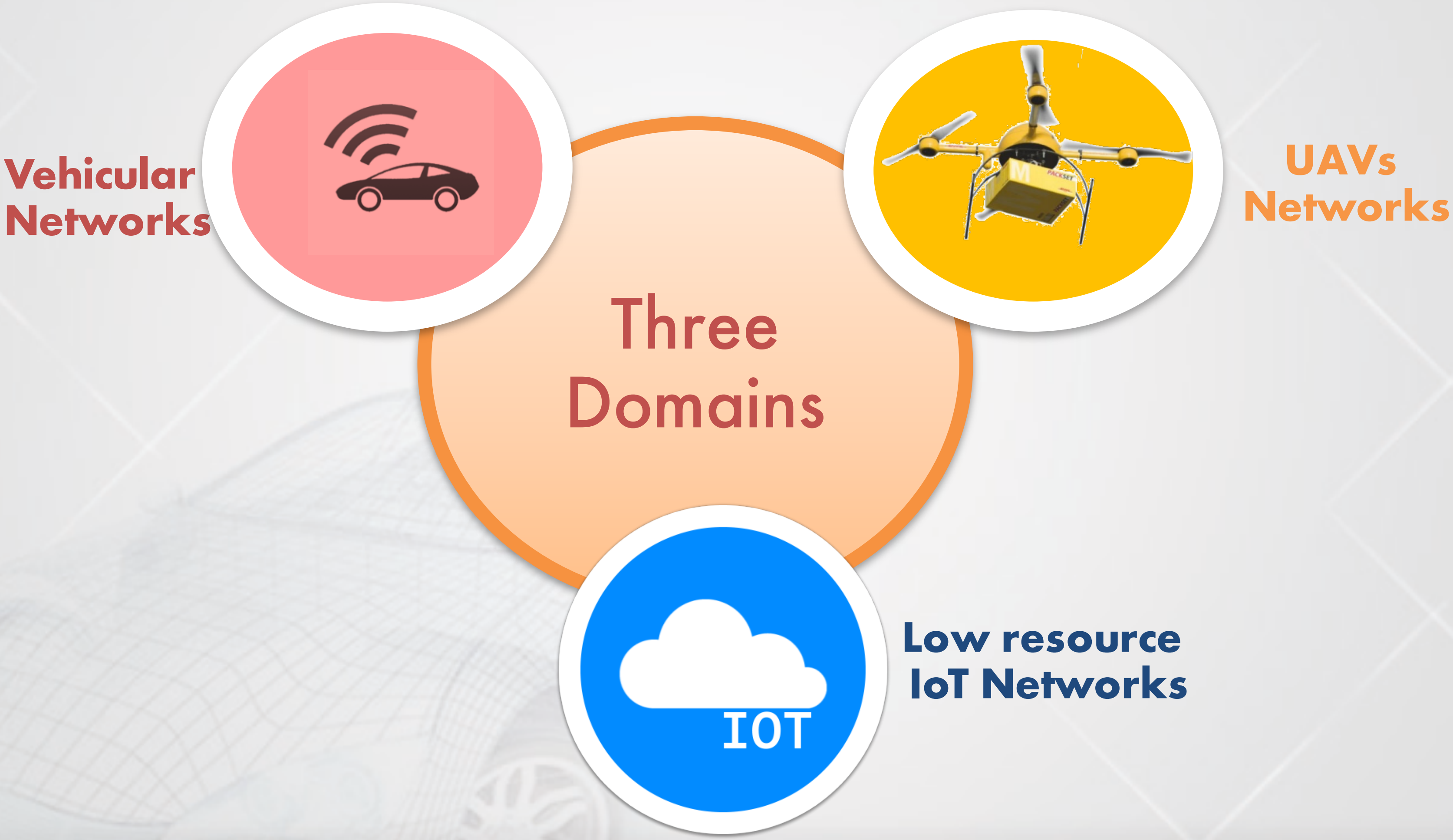
- The privacy level depends on the **capacity** of a VLPZ and its **occupancy**.
  - Vehicles are rational: If a vehicle has reached its desired location privacy level, it will not look to enter a VLPZ again to cooperate with other vehicles

➔ Need for a Reputation Mechanism

- A VLPZ broadcasts invitations to motivate vehicles to enter the VLPZ
- The increase or the decrease of the vehicle's reputation value depends **on its response** and on the **VLPZ occupancy**
- Decision on a vehicle's pseudonym request depends on its reputation value



ICT for connected mobility: Cyber defense



Distributed Intrusion Detection/Prevention

IDS

3 Components

Data Collection Module
Collects data within the radio range of IDS node

→ **Capture Data** →

Detection Module
Analyzes data and Checks the occurrence of a malicious behaviors

→ **Intrusion Events** →

Response Module
Sends an alert to the network administrator when an intrusion occurs

→ **Reaction**

Detection policies

Signature based

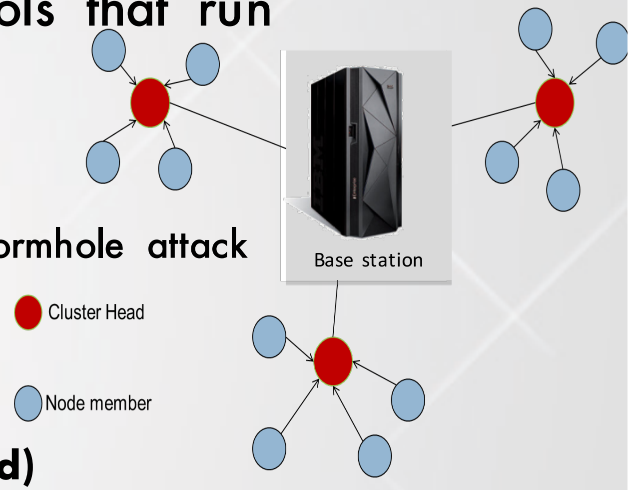
Anomaly-based

Hybrid detection: combine between anomaly-based & signature-based.

Institut Supérieur de l'Automobile et des Transports - 49, rue Mademoiselle Bourgeois - BP 31 58027 Nevers cedex
Téléphone : 03 86 71 50 00 / Fax : 03 86 71 50 01

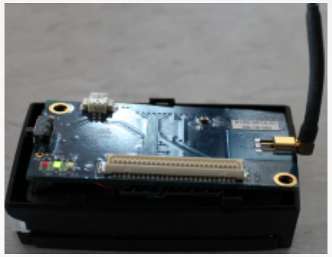
Hierarchical intrusion detection framework for cluster-based wireless sensor networks

- Detection framework composed of different protocols that run hierarchically at three levels:
  1. At low level (IDS agents):
     - **Rule-based detection protocol (4 rules)**
     - 4 Attacks: selective forwarding, Hello flood, Black hole, Wormhole attack
     - Monitoring: PDR, RSSI, etc.
  2. At medium level (CH):
     - **Binary classification detection protocol (SVM based)**
     - **Reputation protocol** used to evaluate the trustworthiness level of its IDSs agents
  3. At high level (BS):
     - Each CH monitors its CH neighbors on the basis of a specification detection protocol with the help of a **vote mechanism** applied at the base station



Hierarchical intrusion detection framework for cluster-based wireless sensor networks

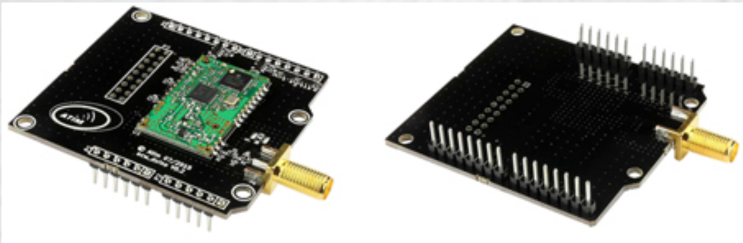

(a)


(b)


(c)

Micaz

Intrusion detection operations: (a) messages send by the cluster member toward cluster-head (red toggle), (b) cluster-head election (green toggle), and (c) IDS's activation and intrusion detection (green and yellow toggles).



Shield radio ARM-N8-LoRaWAN

Hybrid Anomaly Detection for Low-Resource IoT Devices

1- Signature based: Compares the behavior of the analyzed target to a set of predefined rules related to each attack, i.e. ***Signature pattern stored in the IoT device's database. It incurs a low false positive rate.***

2- Anomaly-based: Uses a supervised learning algorithms algorithm to carry out a training, classification and builds a rule related to each new detected attack pattern. Afterward, this rule is stored to be used by the signature detection technique. ***It incurs a high detection rate.***

2- Hybrid: Combination between anomaly and signature detection techniques. **It incurs high detection and low false positive rates.**

The activation of an anomaly detection could generate a high energy consumption

→

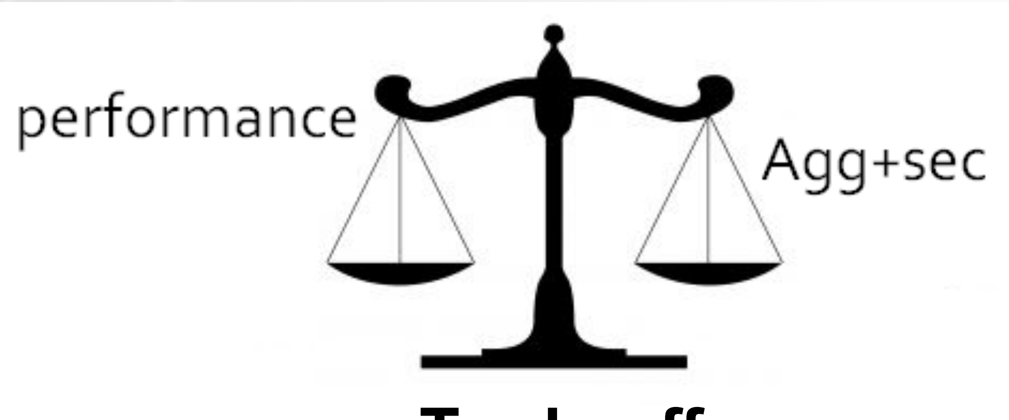
Anomaly detection **activated only when a new attack's signature will be expected to occur**

→

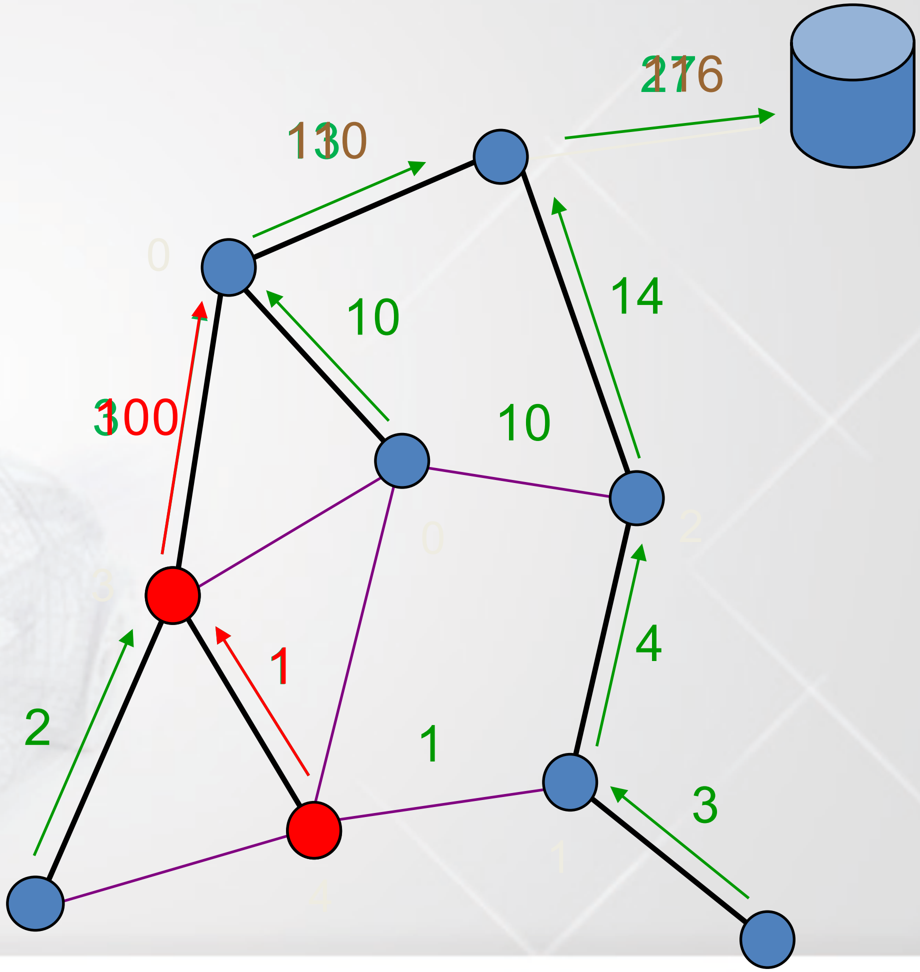
To assure this dilemma, a **Security Game** approach is proposed

Secure Data Aggregation ?

Security ↑ Overhead (Energy) ↓ Aggregation



Trade-off



How to efficiently secure data aggregation ?

SASPKC: Secure Aggregation using Stateful Public Key Cryptography

- Hybrid: **Asymmetric** (Forwarding phase using ECC) and **Symmetric** (Aggregation phase)
- End-to-end Confidentiality and integrity (homomorphism)
- Versatility
- Highlight the advantage of using aggregation

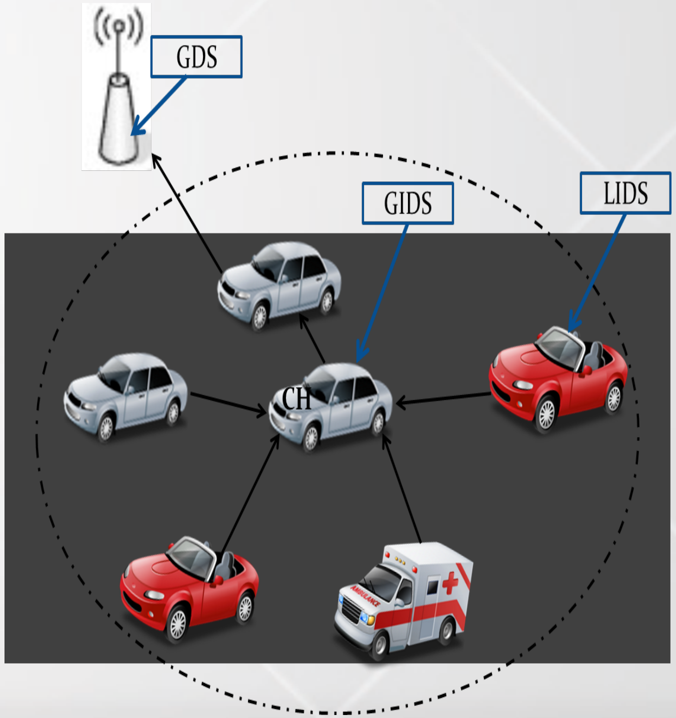
Real implementation

ICT for connected mobility: Cyber defense (Vehicular networks)

Accurate and lightweight intrusion detection framework for vehicular networks

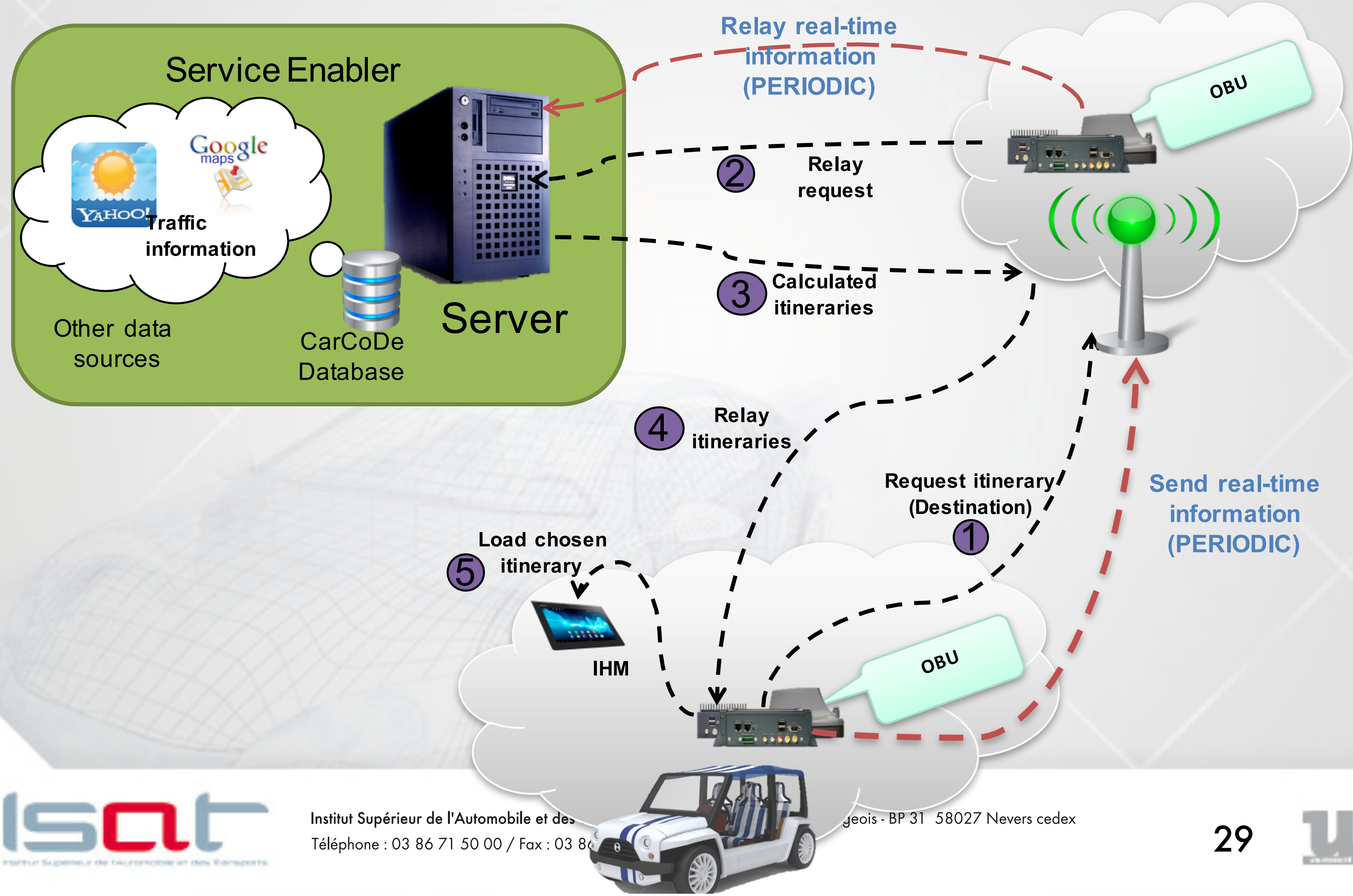
- Vital information managed by the vehicle.
- Need to protect the network against the most dangerous attacks that could occur on such networks
- Need to consider vehicles' characteristics ➔ a **secured clustering** algorithm that considers both **node's mobility** and **network vulnerability during cluster formation**.

- **Local Intrusion Detection System (LIDS)** running at cluster member level that monitors the behaviors of it neighboring vehicles and the cluster-head,
- **Global Intrusion Detection System (GIDS)** running at CH level that monitors the behaviors of its cluster members and evaluates the trustworthiness of monitored vehicles,
- **Global Decision System (GDS)** running at RSU level that computes the Trust-level (TL) related to each vehicle and **categorizes them into an appropriate list according to their TL**.

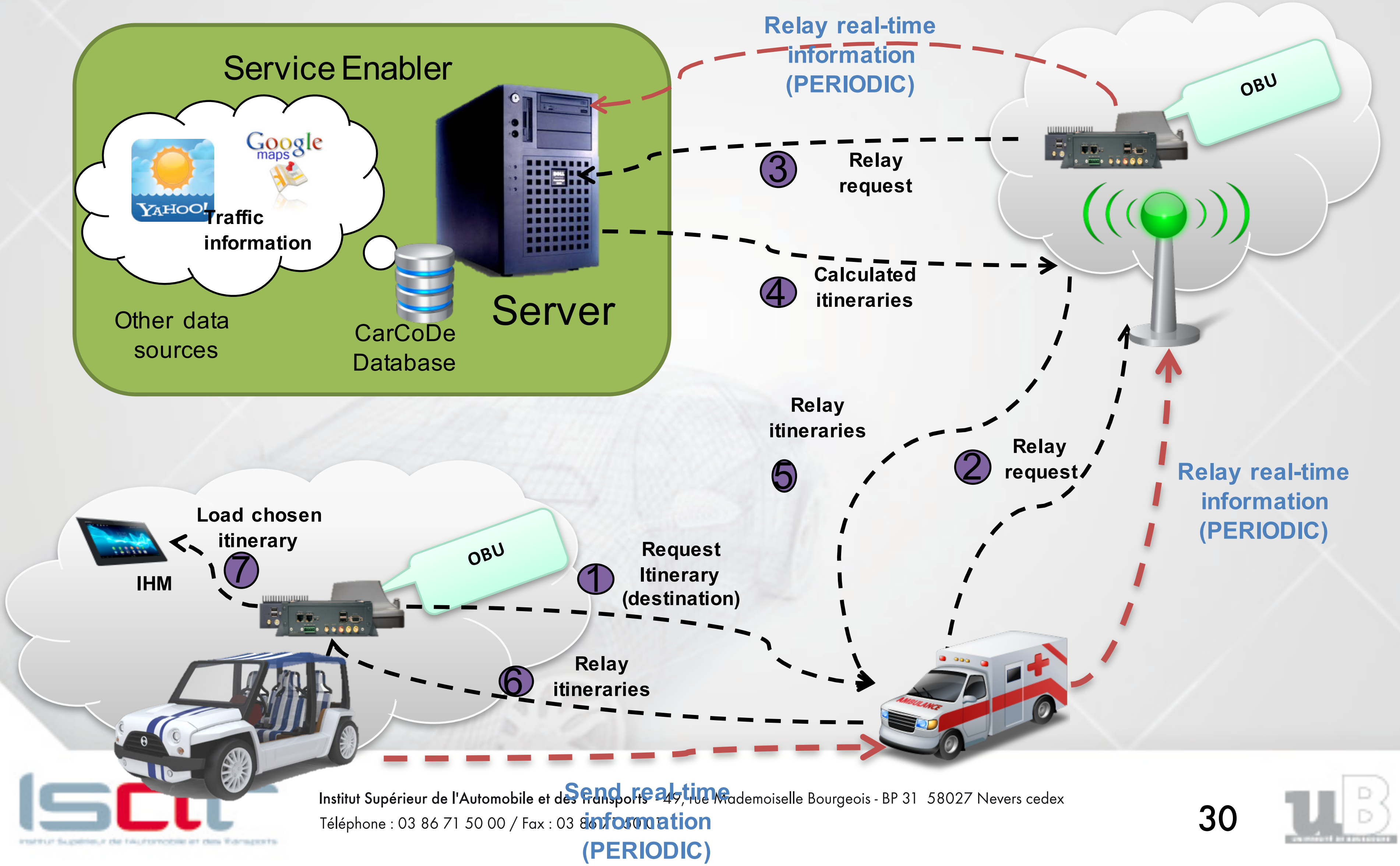


Itinerary planning application: Architecture

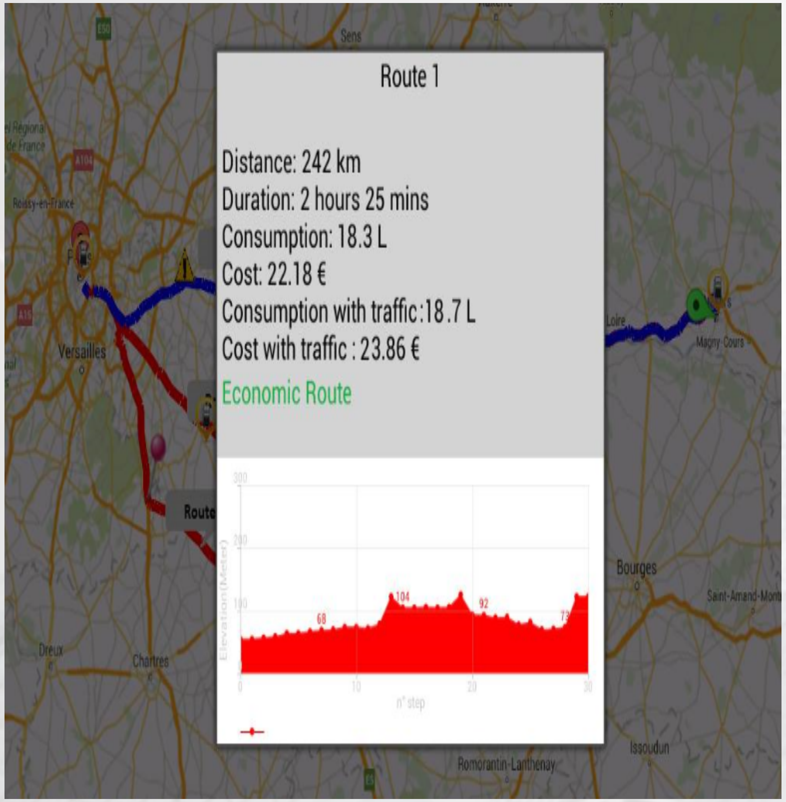
Itinerary planning application: Case of direct communication with infrastructure

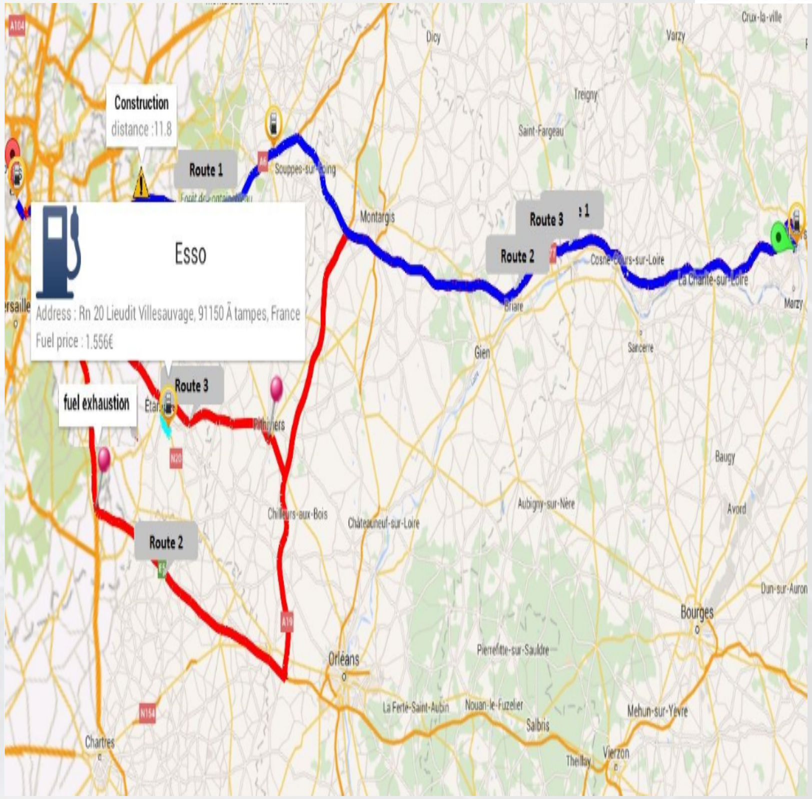


Itinerary planning application: Case of indirect communication with infrastructure



Itinerary planning application: Android application





Electric Vehicles integration in the Smart Grid

- We target the problem of Electric Vehicles (EVs) integration into the SG to avoid electricity intermittence due to the important load that EVs can create
  - We propose at a first level a Bayesian game-theory model that aims to integrate optimally EVs into the SG and **maintain the equilibrium between the offer and the demand**
  - Two players in this game model:
    - The Smart Grid (SG)
    - The Electric Vehicle (EV)
  - Each player has two actions:
    - SG: Deliver/Don't deliver.
    - EV: Charge/Don't charge.
  - Each player has to maximize its gain

An Efficient Intrusion Detection System Against Cyber-Physical Attacks in the Smart Grid

- This work deal with attacks targeting namely the **state estimation** in the smart grid
  - These attacks mislead the state estimation to take the right decisions about the amount of demanded electricity and so the amount of electricity to be produced and how it should be distributed

- Treated attacks:
  - **DoS attack (availability issue):** the attacker prevents the state estimation from useful information that should be sent from the nodes to the control center (blackhole attack, time delay attack, etc.).
    - **Countermeasure:** we use rule based detection and monitor the behavior of the node that should follow a normal distribution
  - **Price manipulation attack (integrity issue):** the attacker alters the announced electricity price (falsified price) in the network and so changes the consumer's behavior
    - **Countermeasure:** we use CUSUM algorithm that detects the granular abnormal changes in the electricity pricing:

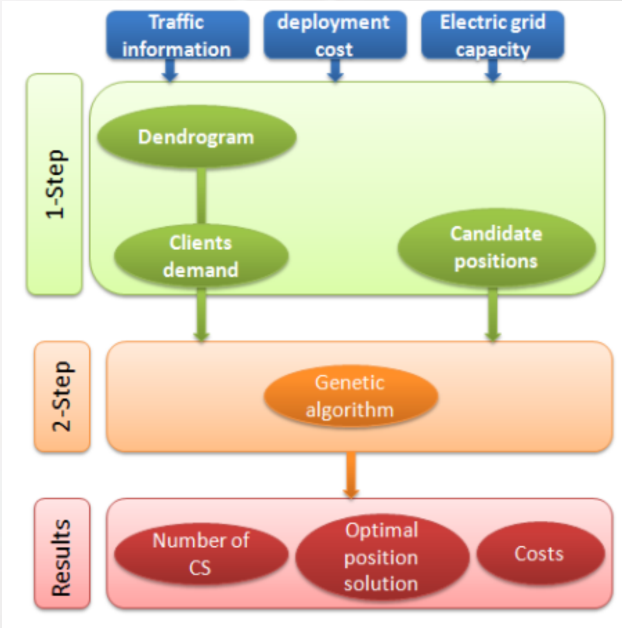
Optimized deployment of electric vehicles' charging stations

- The objective of this work is to optimize the deployment of new charging stations in order to **satisfy** customers **demands**, reduce the **cost** of deployment and allow energy balance

- Problem ?
  - How many charging stations are needed ?
  - Where ?
  - How to assign clients ?

Optimized deployment of electric vehicles' charging stations

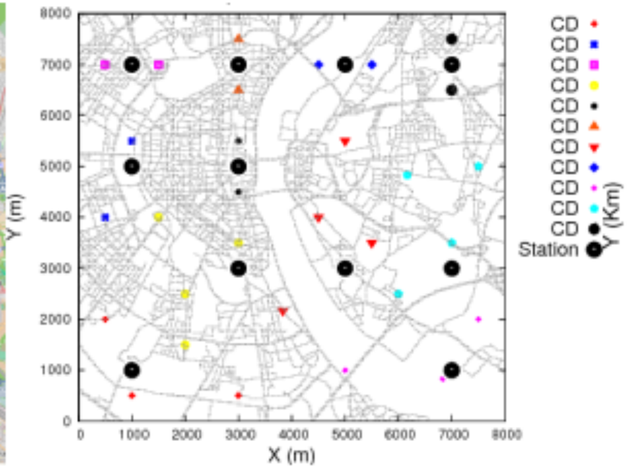
- In our work, we consider :
  - Area traffic density (helps to deduce the energy Demand),
  - The cost of deployment,
  - Transportation cost toward the Charging station,
  - Charging stations capacity (Capacity),
  - Electric grid capability (Total Capacity).

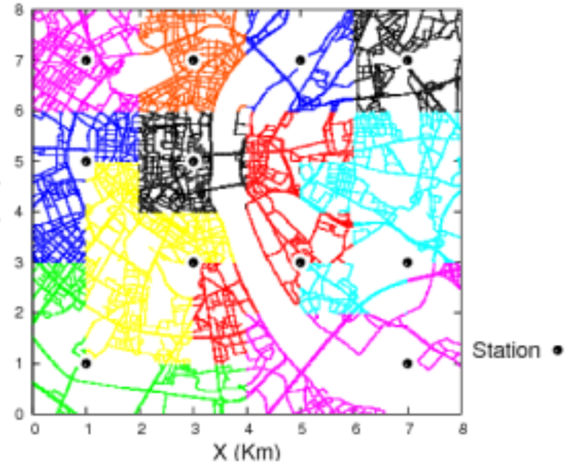


- We model this problem as:
  - Objective function : F =αF1+βF2
    F1: Investment cost, F2: Transport cost
  - Use 2-steps solution
    - Preprocessing
    - Genetic algorithm

Optimized deployment of electric vehicles' charging stations

Tapas cologne real traffic scenario (6 :00 → 8 :00am)





Initial candidates 16 → **Final** candidates **11**

Institut Supérieur de l'Automobile et des Transports - 49, rue Mademoiselle Bourgeois - BP 31 58027 Nevers cedex
Téléphone : 03 86 71 50 00 / Fax : 03 86 71 50 01