Accélérateur
de la transformation
numérique

Privacy in C-ITS: threats, impact and assessment

Farah Sophie HAIDAR, Ph.D

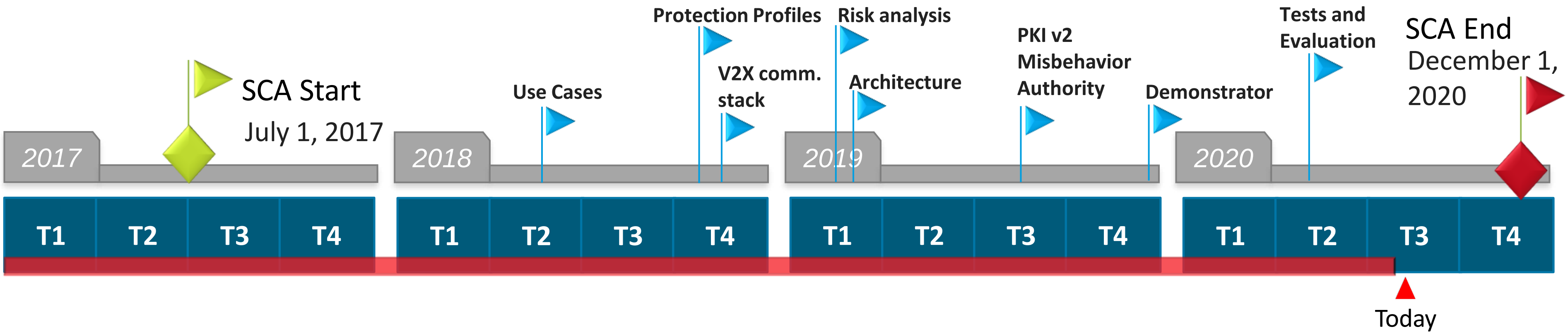
Dr- Research Engineer – IRT SystemX, France

Workshop CyberSec, ITSC 2020, 20-23 September 2020

Outline

- Secure Cooperative Autonomous System (SCA) Project
- Context
- C-ITS Architecture
- Privacy protection in C-ITS
- Tracking attack
- Impact of pseudonym change on safety and security applications
- Conclusion

SCA project overview



Institut Mines-Télécom

SystemX INSTITUT DE RECHERCHE TECHNOLOGIQUE

GROUPE RENAULT

PSA PEUGEOT CITROËN

Valeo

transdev MOBILITY INSPIRED BY YOU

YoGoKo " You Go, We Konnect "

OPPIDA EXPERT EN SECURITE DES SYSTEMES D'INFORMATION

IDNOMIC

TRiALOG

Key challenges

Use cases cooperative autonomous vehicle

- Use cases C-ITS
- Risk analysis
- Performance criteria
- C-ITS privacy

Compliance assessment & Penetration tests

- Protection Profiles
- Test tools development
  - Security conformity
  - Penetration testing
- Dimensioning evaluation in a real case

Crypto-agility & Business continuity

- Misbehavior detection
- Crypto-agility

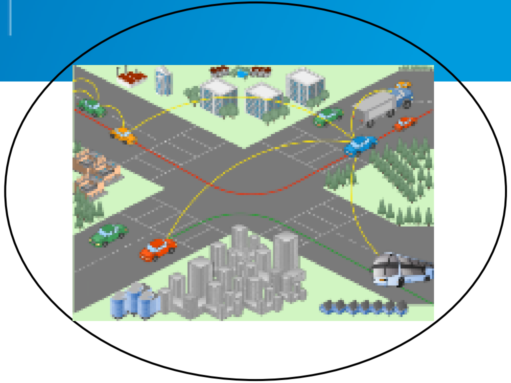
Interoperability & Scalability

- End-to-end hybrid networks security
- Interoperability with C-ITS entities (IoT-like)
- PKI scalability and dynamic dimensioning

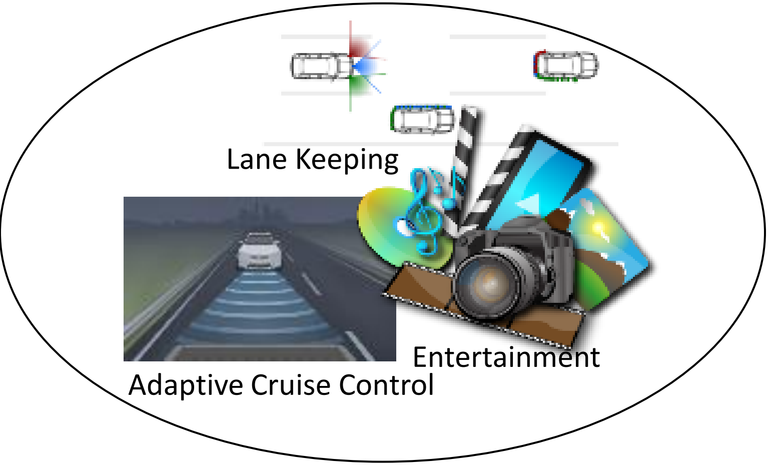
Outline

- Secure Cooperative Autonomous System (SCA) Project
- Context
- C-ITS Architecture
- Privacy protection in C-ITS
- Tracking attack
- Impact of pseudonym change on safety and security applications
- Performance evaluation of pseudonym reloading
- Conclusion

Context of Cooperative Intelligent Transportation System



New Complexity



New Applications

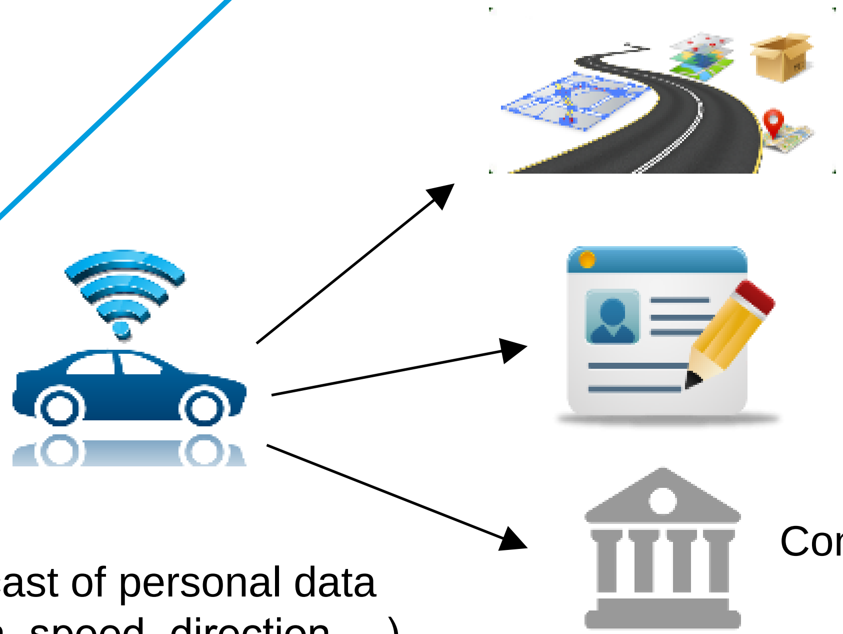
- **Vehicles will communicate and cooperate by exchanging messages between each other and with the infrastructure.**
- **System is open to new applications.**
- **Many potential risks should be taken into account.**

Security and Privacy

Security

- **Authentication**
- Confidentiality
- **Integrity**
- **Non repudiation**
- **« Privacy »**

“Privacy”



Tracking

User profile

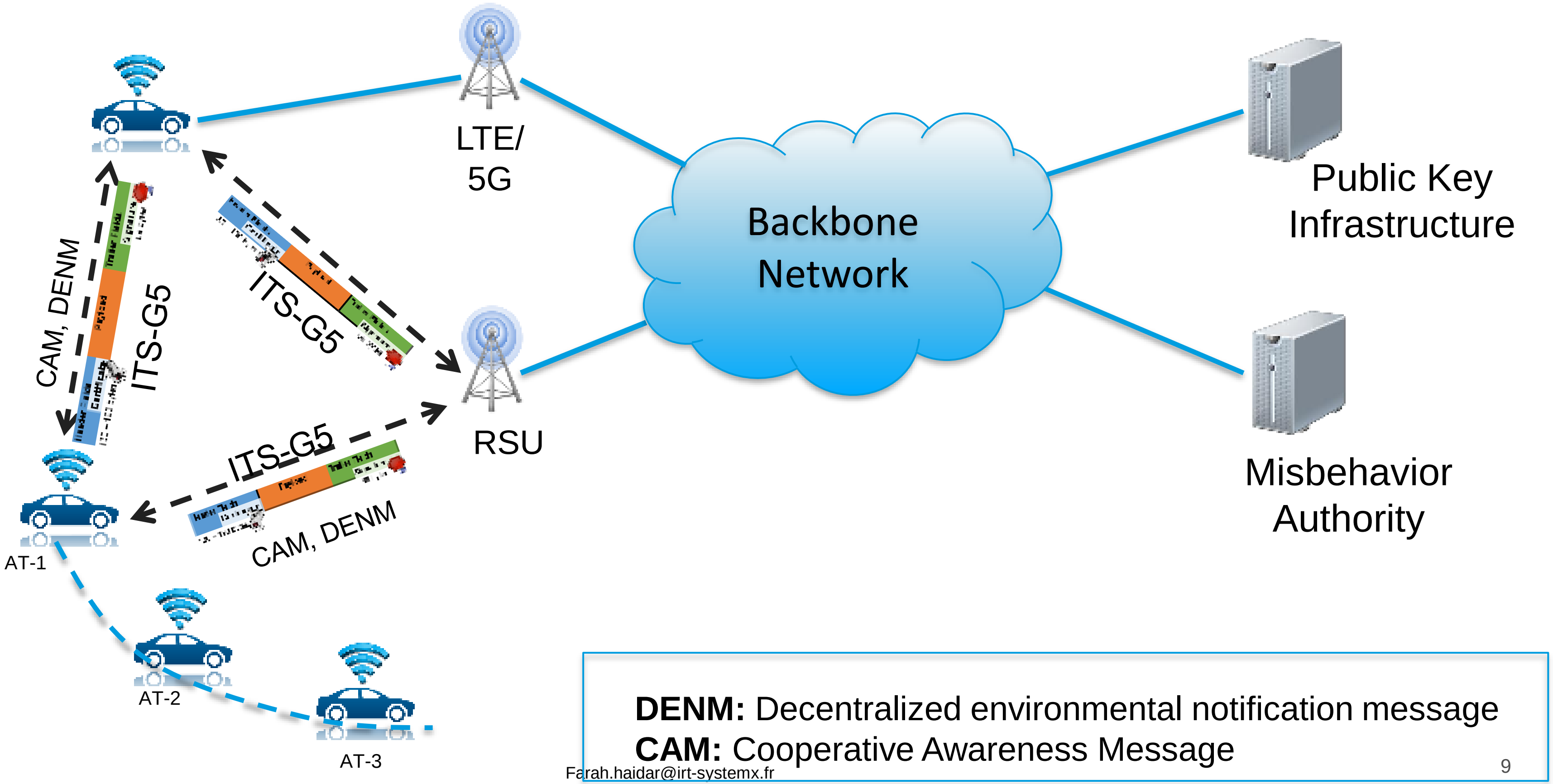
Compliance with regulation

Broadcast of personal data (position, speed, direction,…)

Outline

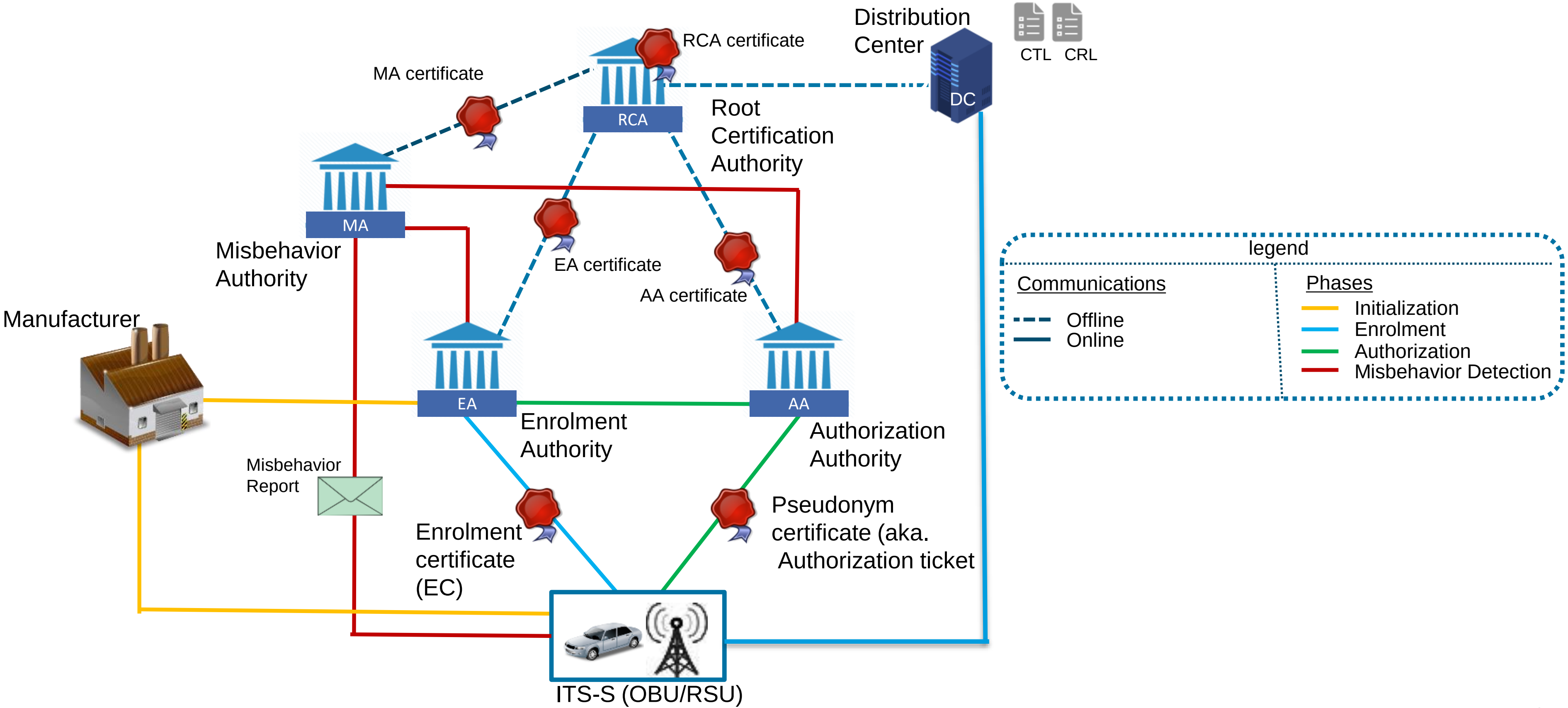
- Secure Cooperative Autonomous System (SCA) Project
- Context
- C-ITS Architecture
- Privacy protection in C-ITS
- Tracking attack
- Impact of pseudonym change on safety and security applications
- Performance evaluation of pseudonym reloading
- Conclusion

Cooperative-Intelligent Transportation System (C-ITS) Architecture



DENM: Decentralized environmental notification message
CAM: Cooperative Awareness Message

Public Key Infrastructure (PKI)



Distribution Center

DC

CTL CRL

RCA certificate

RCA

Root Certification Authority

MA certificate

MA

Misbehavior Authority

EA certificate

AA certificate

Manufacturer

EA

Enrolment Authority

AA

Authorization Authority

Misbehavior Report

Enrolment certificate (EC)

Pseudonym certificate (aka. Authorization ticket

ITS-S (OBU/RSU)

legend

Communications

- - - Offline

— Online

Phases

— Initialization

— Enrolment

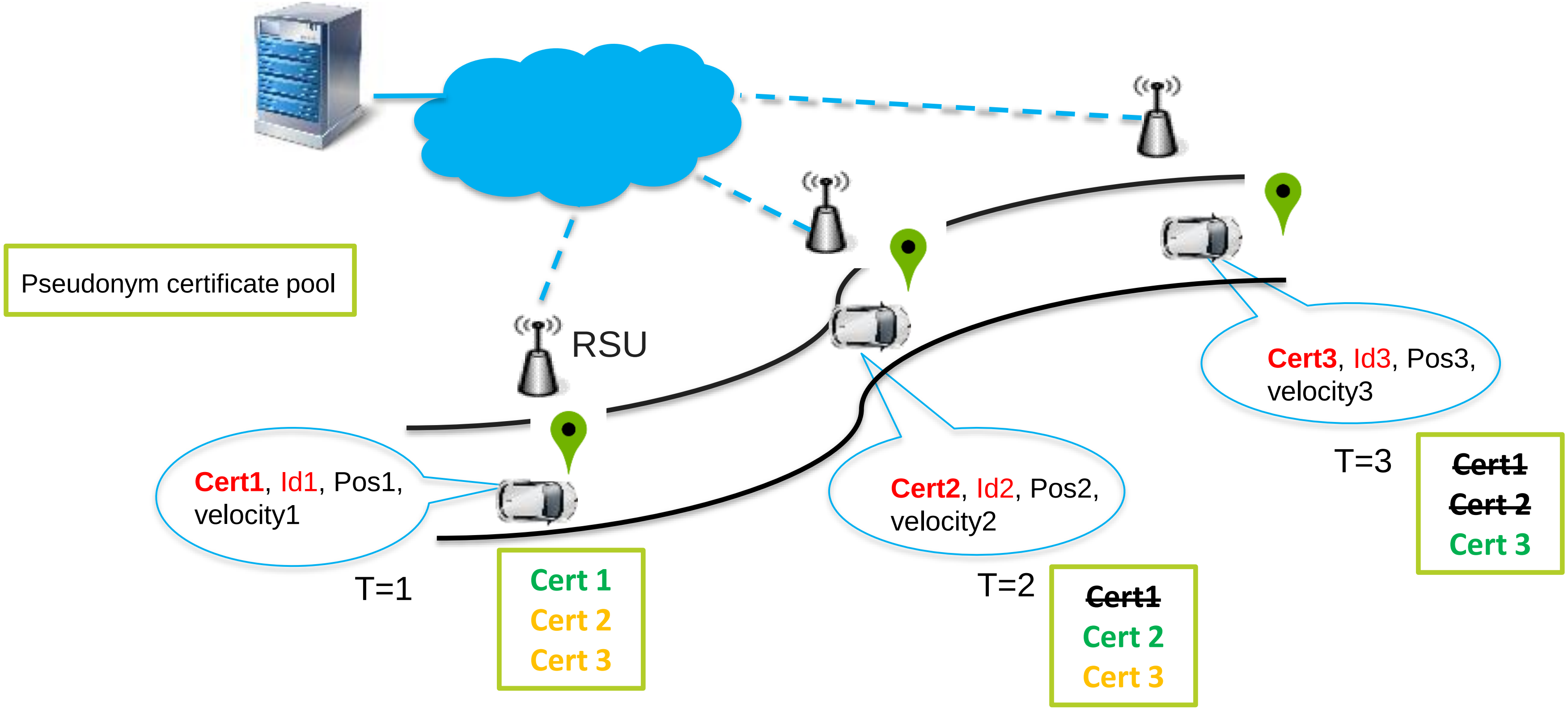
— Authorization

— Misbehavior Detection

Outline

- Secure Cooperative Autonomous System (SCA) Project
- Context
- C-ITS Architecture
- Privacy protection in C-ITS
- Tracking attack
- Impact of pseudonym change on safety and security applications
- Performance evaluation of pseudonym reloading
- Conclusion

Pseudonym certificates change



Public key infrastructure

Pseudonym certificate pool

RSU

Cert1, Id1, Pos1, velocity1

T=1

Cert 1
Cert 2
Cert 3

Cert2, Id2, Pos2, velocity2

T=2

~~Cert1~~
Cert 2
Cert 3

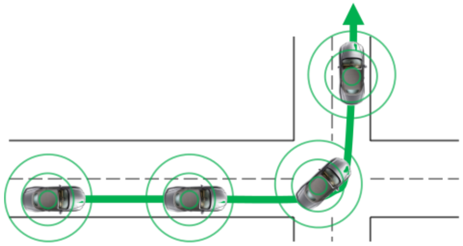
Cert3, Id3, Pos3, velocity3

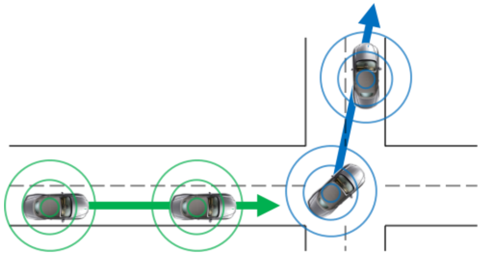
T=3

~~Cert1~~
~~Cert 2~~
Cert 3

Pseudonym change strategies

- Periodic
  - Timer : fixed/random
  - Message number: fixed/random
  - Distance
  - Vehicles density
  - Collaborative
- Periodic with silent period :
  - Fixed/random
  - Depending on the velocity or the direction
- Mix zone
  - Stop CAM on intersections, parkings



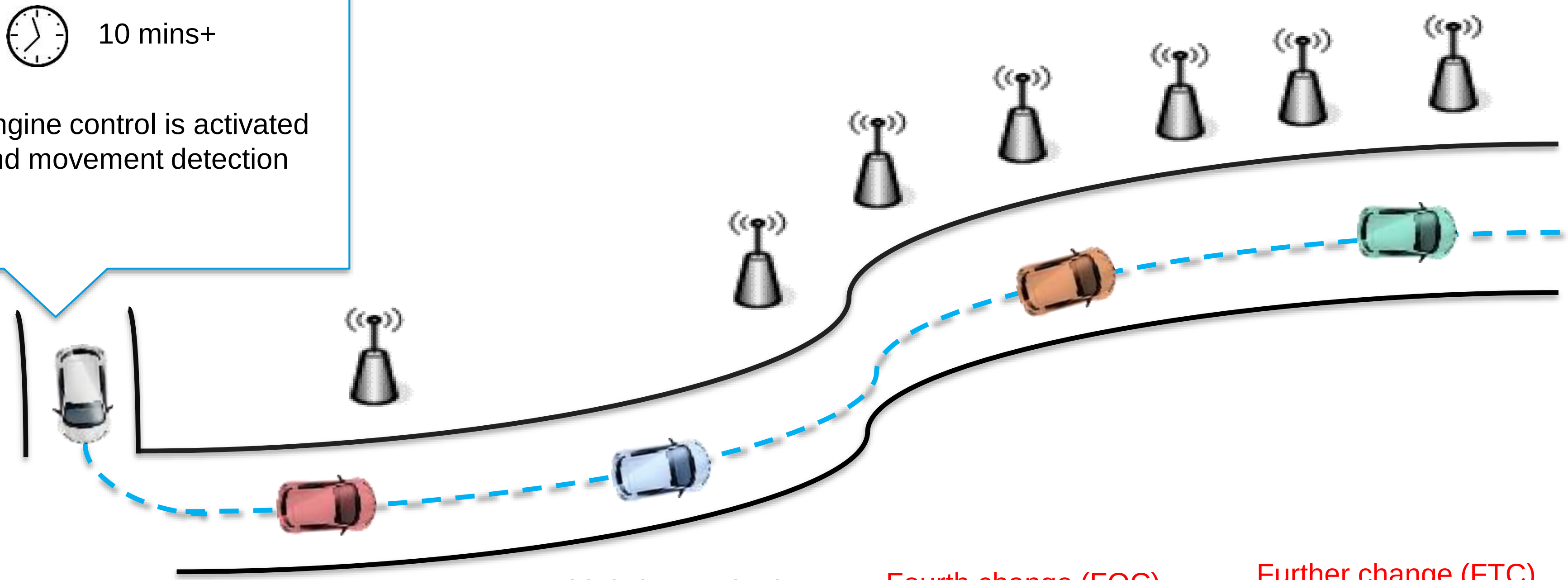


Car2Car Pseudonym Change Strategy

Engine control is deactivated

🕐 10 mins+

Engine control is activated and movement detection



First change (FC)

Second change (SC)

FC + 800 < SC < FC + 1500

Third change (TC)

SC + 800 + 2 to 6 mins (rand)

Fourth change (FOC)

TC + 10000 < FOC < TC + 20000

Further change (FTC)

FOC + 25000 < FTC < FC + 35000

(m)

Outline

Secure Cooperative Autonomous System (SCA) Project

Context

C-ITS Architecture

Privacy protection in C-ITS

Tracking attack

Impact of pseudonym change on safety and security applications

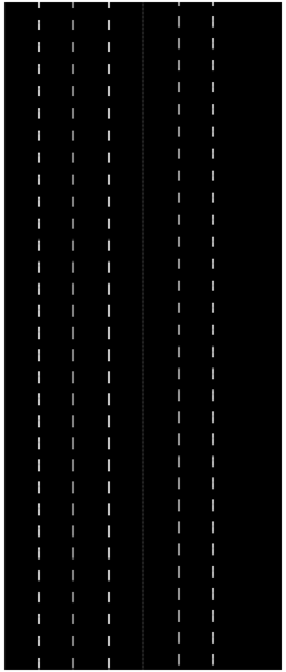
Performance evaluation of pseudonym reloading

Conclusion

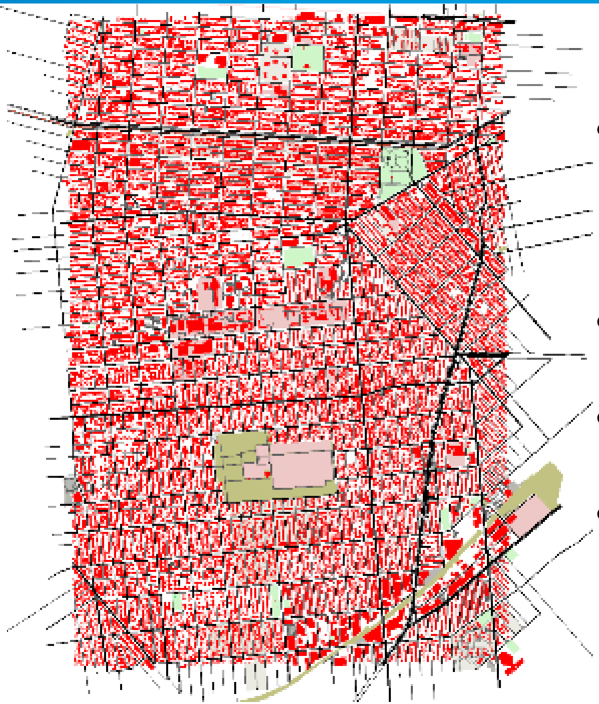
Tracking Attack

- **Simulation of Urban Mobility (SUMO)**
  - Creation of mobility models
- **Omnet++ / Veins**
  - Simulation of V2X communications
- **Tracker**
  - Implementation of tracking attack

Tracking Attack: Simulation Settings



Highway scenario (100km)



Urban scenario (Brooklyn grid)

- **Vehicle density :** medium (1 vehicle/1.5 sec)
- **Type of trips:** random
- **User profile:** normal
- **Velocity:** constant velocity model (30Km/h)

Attacker Profile

Basic attacker

- Prediction

  $X_{t+dt} = X_t + dt * V * \mathrm{Sin}(H)$

  $Y_{t+dt} = Y_t + dt * V * \mathrm{Cos}(H)$

- Filter: creation of candidate list based on plausible range.
- Update: add the potential candidate to the track

Kalman filter attacker

- Prediction

  $x_k = A_{k-1} * x_{k-1} + B_k U_k$

  $P_k = A_{k-1} * P_{k-1} A_{K-1} + Q_{K-1}$

- Update: compare measurements to the predicted state and update covariance noise matrix

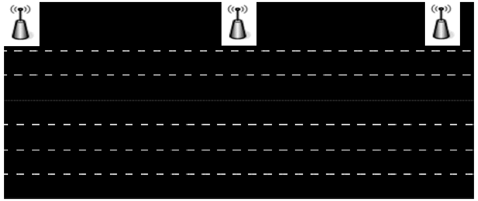
https://en.wikipedia.org/wiki/Kalman_filter

Attacker Types

CDF = 1 means vehicle is not trackable

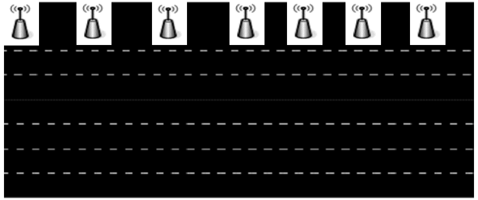
Scenario : highway (100km)

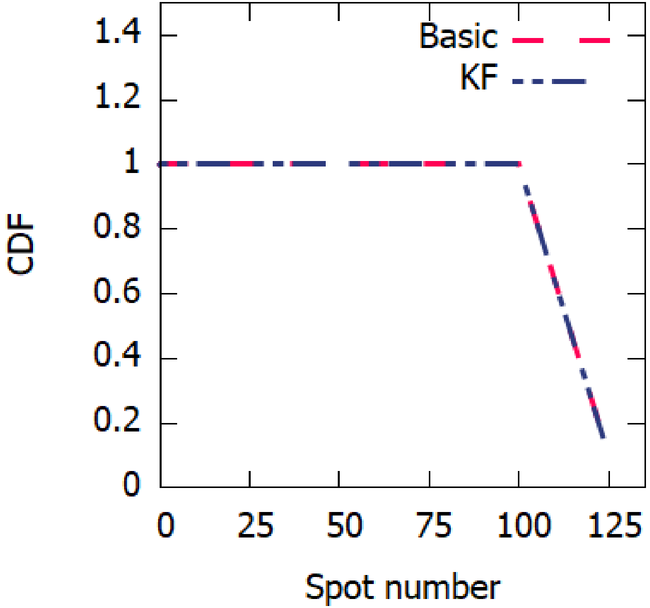
- **Mid-sized-attacker (MDA):** spot number < 125



Uniform distribution

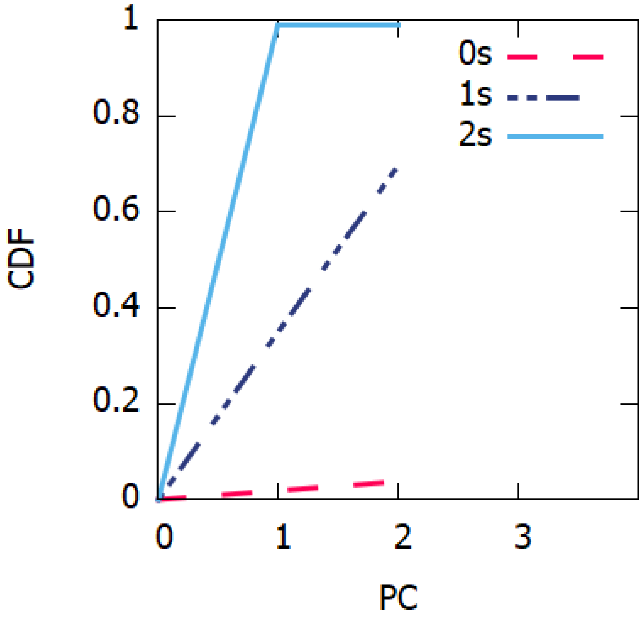
- **Global attacker (GBA):** spot number >= 125





CDF of probability of being Untrackable

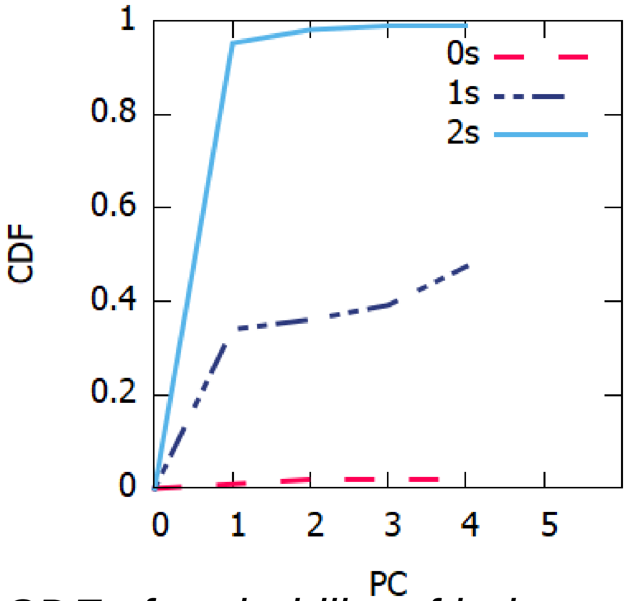
Results of Tracking Attack using Basic/Global Attacker



Silent period = 0
Silent period = 1
Silent period = 2

CDF of probability of being untrackable on urban scenario Using C2C strategy

CDF = 1 means vehicle is not traceable



CDF of probability of being untrackable on highway scenario Using C2C strategy

Outline

Secure Cooperative Autonomous System (SCA) Project

Context

C-ITS Architecture

Privacy protection in C-ITS

Tracking attack

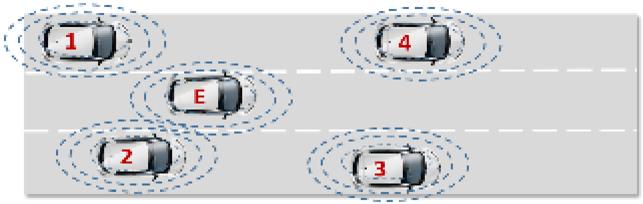
Impact of pseudonym change on safety and security applications

Performance evaluation of pseudonym reloading

Conclusion

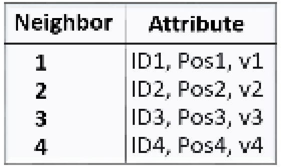
Impact of pseudonym change on Safety applications

- Evaluation of **Cooperative Awareness**
  - Safety applications uses the neighbor table
  - Evaluation of the neighbor table’s consistency

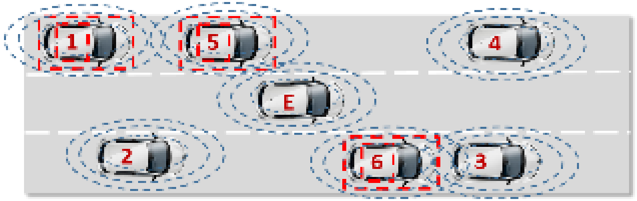


t = t0

Neighbor table of vehicle E at t0

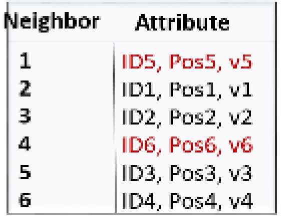


Neighbor	Attribute
1	ID1, Pos1, v1
2	ID2, Pos2, v2
3	ID3, Pos3, v3
4	ID4, Pos4, v4



t = t1

Neighbor table of vehicle E at t1



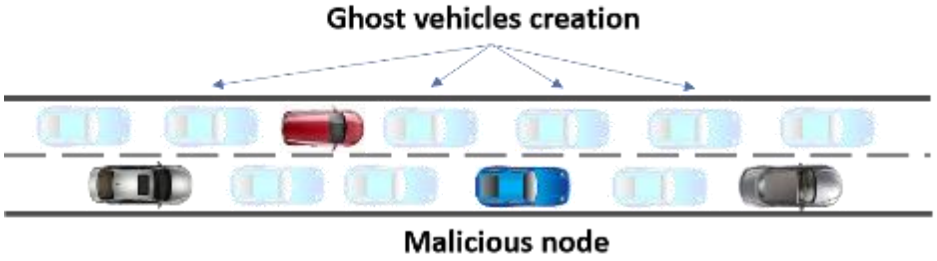
Neighbor	Attribute
1	ID5, Pos5, v5
2	ID1, Pos1, v1
3	ID2, Pos2, v2
4	ID6, Pos6, v6
5	ID3, Pos3, v3
6	ID4, Pos4, v4

Inconsistency of the neighbor table

Vulnerable pseudonym pool

- Sybil attack
  - Having a pool of valid pseudonym open the door to new vulnerabilities
  - An attacker can sign fake messages with valid pseudonym certificates
  - Sybil attack can disturb the system

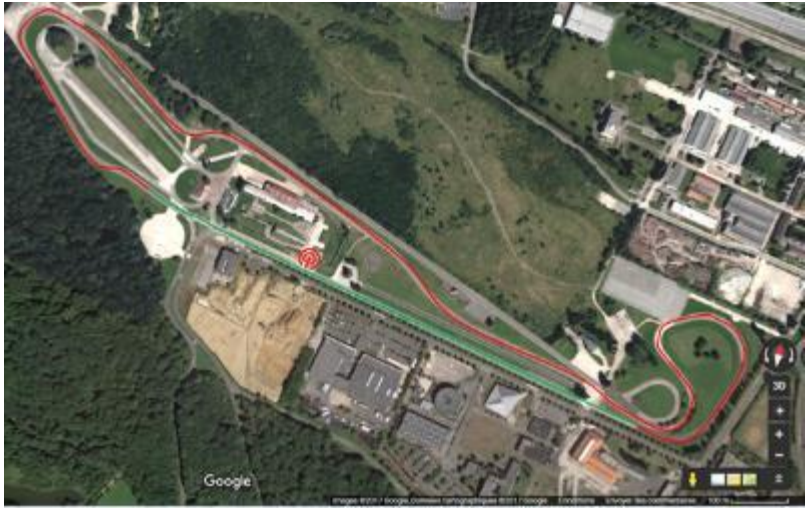
Sybil attack



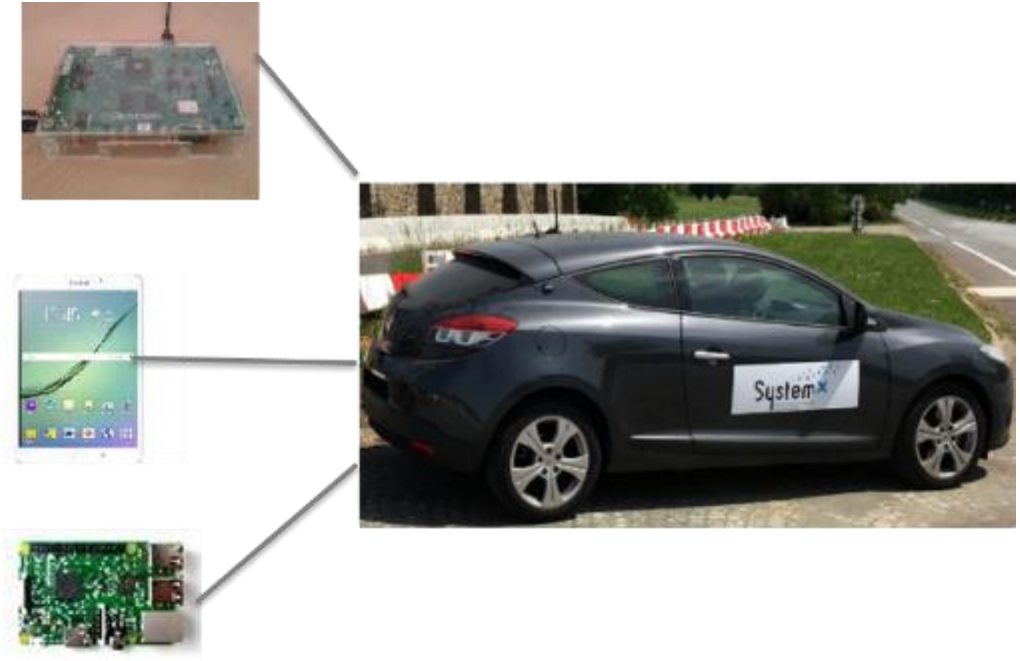
Outline

- Secure Cooperative Autonomous System (SCA) Project
- Context
- C-ITS Architecture
- Privacy protection in C-ITS
- Tracking attack
- Impact of pseudonym change on safety and security applications
- Performance evaluation of pseudonym reloading
- Conclusion

Real Test while Driving



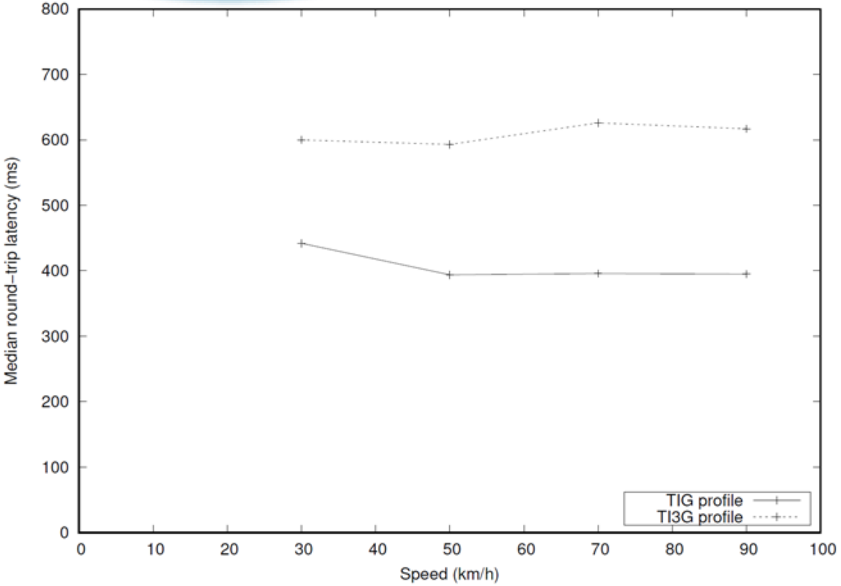
Versailles-Satory test track (green line = RSU coverage)



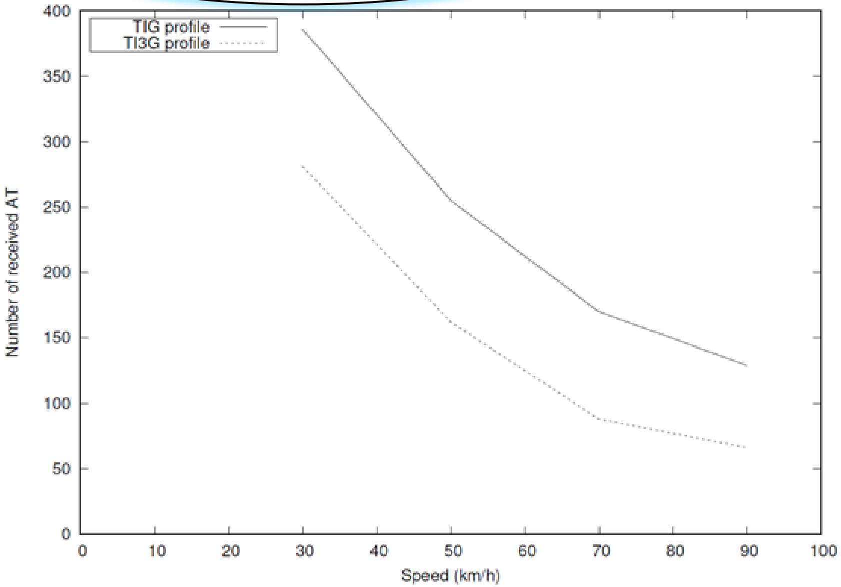
In vehicle equipments

Real Test Results

Median Round trip latency versus speed



Number of received pseudonyms versus speed



Outline

- Secure Cooperative Autonomous System (SCA) Project
- Context
- C-ITS Architecture
- Privacy protection in C-ITS
- Tracking attack
- Impact of pseudonym change on safety and security applications
- Performance evaluation of pseudonym reloading
- Conclusion

Conclusion

- **The use of pseudonym certificates and changing them is the existing solution for privacy protection in C-ITS**
- **Mid sized attacker (basic and intelligent attacker) is unable to track vehicles on highway scenario**
- **Global attacker can track vehicles on highway and on urban scenarios. Adding a silent period can improve the privacy level.**
- **The pseudonym change can disturb the safety appliactions**
- **The pseudonym reloading is feasible in real environment**

Systemx
INSTITUT DE RECHERCHE
TECHNOLOGIQUE

Accélérateur
de la transformation
numérique

Thank you

Farah.haidar@irt-systemx.fr

www.irt-systemx.fr