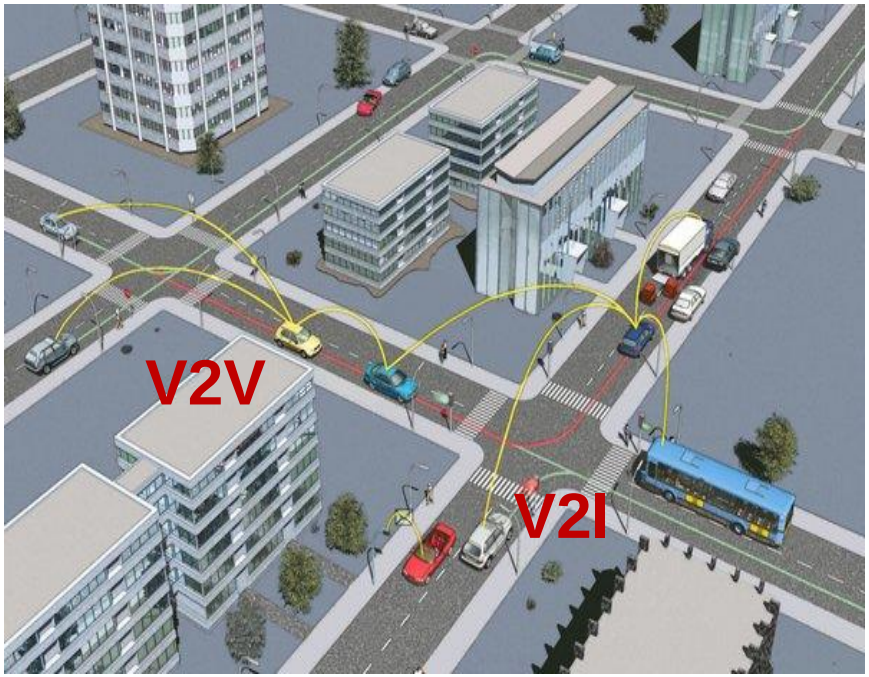
La voiture connectée: Comment sécuriser les communications V2X ?

Houda Labiod
houda.labiod@telecom-paristech.fr

Equipe SdR (Sécurité des Réseaux)
Département INFRES, Telecom ParisTech

Colloque scientifique IMT - 10 Novembre 2017 – Telecom ParisTech

Les systèmes de transport intelligents , C-ITS



Les systèmes ITS utilisent les technologies de l'information et des communications pour développer et améliorer tous types de systèmes de transport

Objectifs des systèmes C-ITS: améliorer la sécurité, améliorer la gestion du traffic, ….

203 millions de voitures connectées en 2022

La voiture connectée au sein d'un réseau véhiculaire hybride maillé de grande échelle

- **Une combinaison de technologies sans fil**
  - ITS-G5 (IEEE 802.11p)/11/15.4, 3G/4G/5G, Bluetooth, NFC, …..
- **Plusieurs types de communications**
  - Vehicle-to-Anything (V2X)
  - V2V, V2I, I2V, V2P, P2V, C-V2X
  - I2I and P2I
- **Caractéristiques**
  - Communications multi-sauts
  - Topologie dynamique
  - Déconnexions fréquentes
  - Système complexe
    - acteurs, stations hétérogènes
  - Grande échelle, Mobilité élevée
- **Cas d'usages variés**
  - ETSI C-ITS Release 1, Day 1 et Day 1,5
  - ETSI C-ITS Release 2, C2C Day 2

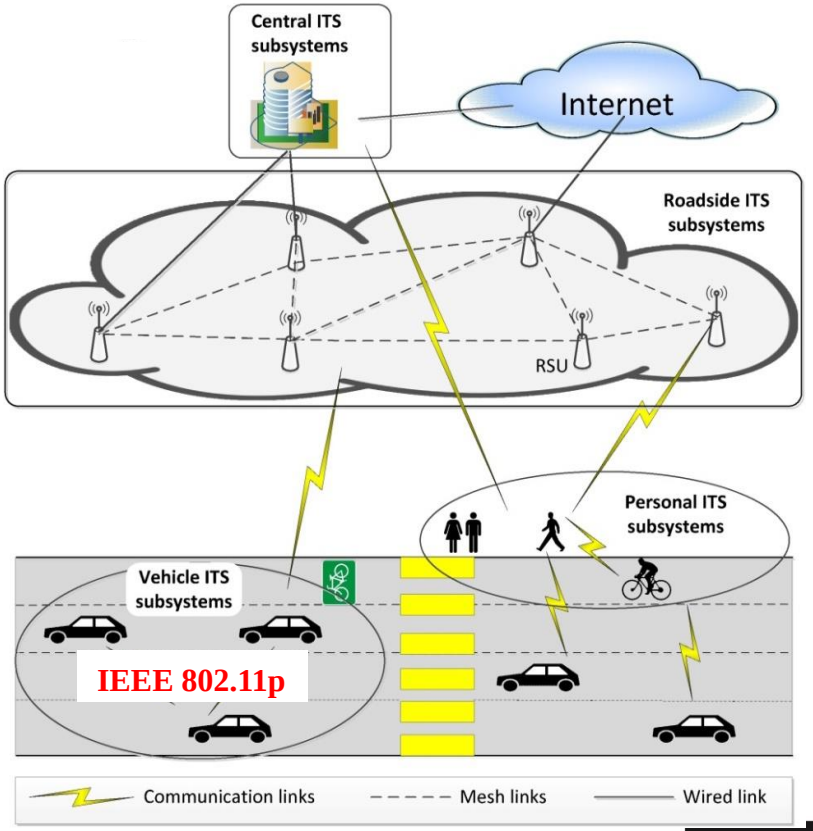


Fig. 1: Architecture V-Mesh.

Cybersécurité

Interfaces multiples de communication

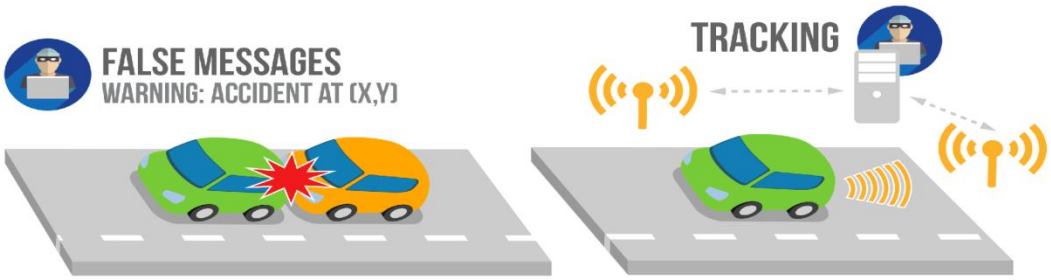
ITS-G5, Wi-Fi, Bluetooth, NFC, 4G, USB, OBD…

Faiblesses / Failles

Augmentation forte de la complexité des systèmes et des logiciels embarqués

Cyber attaques

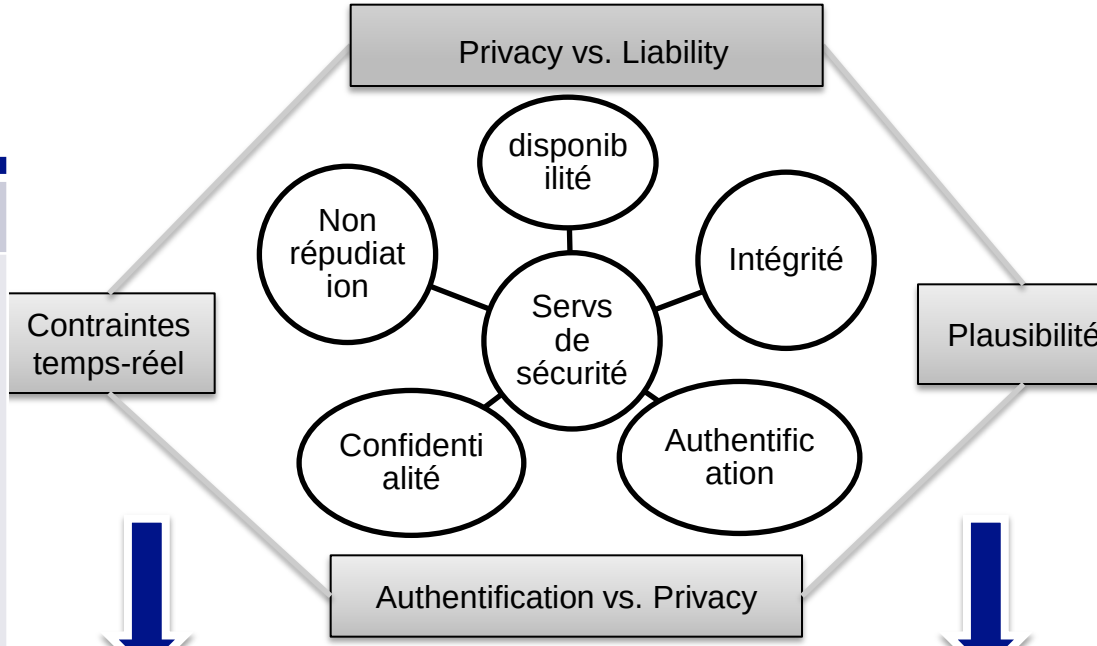
- sur le véhicule (système embarqué)
- Sur l'infrastructure (système débarqué)



https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/).

Questions clés

Threats		Impacted Objectives						
		Confidentiality	Integrity	Availability	Authenticity	Plausibility	Accountability	Privacy
Denial of Service	Flooding							
	Spamming							
	Black hole							
	Malware							
	Wormhole							
	Greedy behaviour			Y				
	Blackmailing							
	fault injection							
	Reflection attack							
	Jamming							
Manipulation of messages			Y		Y	Y		
Masquerade			Y		Y			
Illusion attack				Y		Y		
Sybil attack					Y			
Replay			Y					
Insertion of information (injection)			Y					
Eavesdropping		Y						Y
Traffic analysis		Y						Y
Repudiation							Y	
RF Fingerprinting		Y			Y			Y
Sensor spoofing			Y	Y		Y		
Sensor Jamming				Y				



- Comment sécuriser le système?
- Comment protéger les messages échangés?
- Comment faire confiance dans les messages reçus ?
- Comment garantir la protection de la vie privée?

- Architecture de sécurité de bout-en-bout
  - sécuriser les communications V2X
- Systèmes C-ITS avec confiance
  - gérer les info identification de sécurité, clés
- Compromis entre scalabilité, sécurité, sûreté , performance et coût
- Assurer la protection des données personnelles

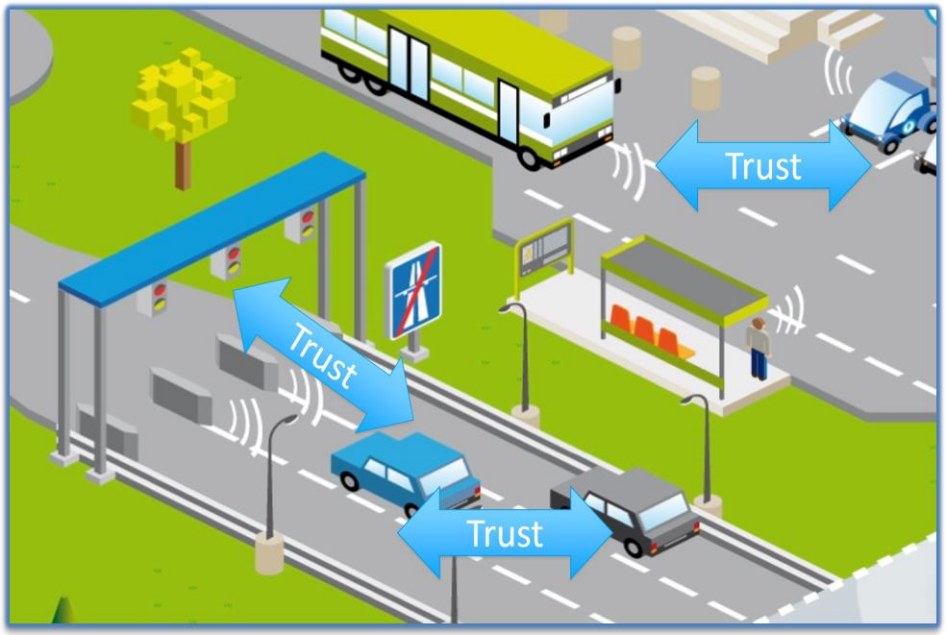
La confiance doit être au coeur du système
Architecture de sécurité de bout-en-bout

Les véhicules envoient et recoivent les messages via ITS-G5

- L'information est diffusée sans acquittement
- Données véhicule (vitesse, position, trajectoire), données perception dynamique de l'environnement

PKI
Authentification

PKI
Intégrité



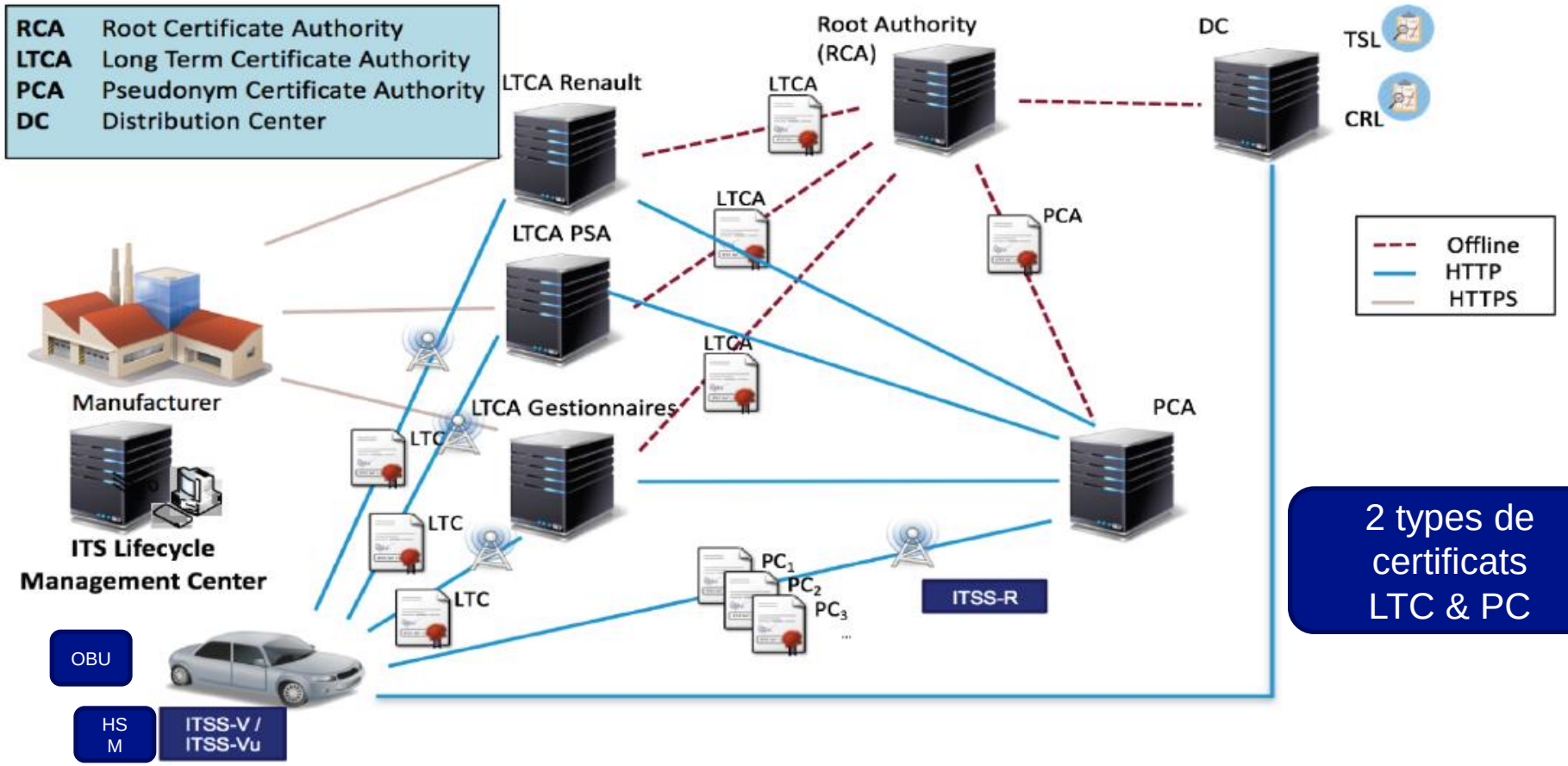
PKI
Autorisation

PKI
Confidentialité

- Messages de données signés selon le standard ETSI 103 097
- Messages anonymes avec un support de changement de certificats pseudonymes délivrés par une infrastructure nationale PKI via RSU ou pas pour rendre le suivi difficile

PKI

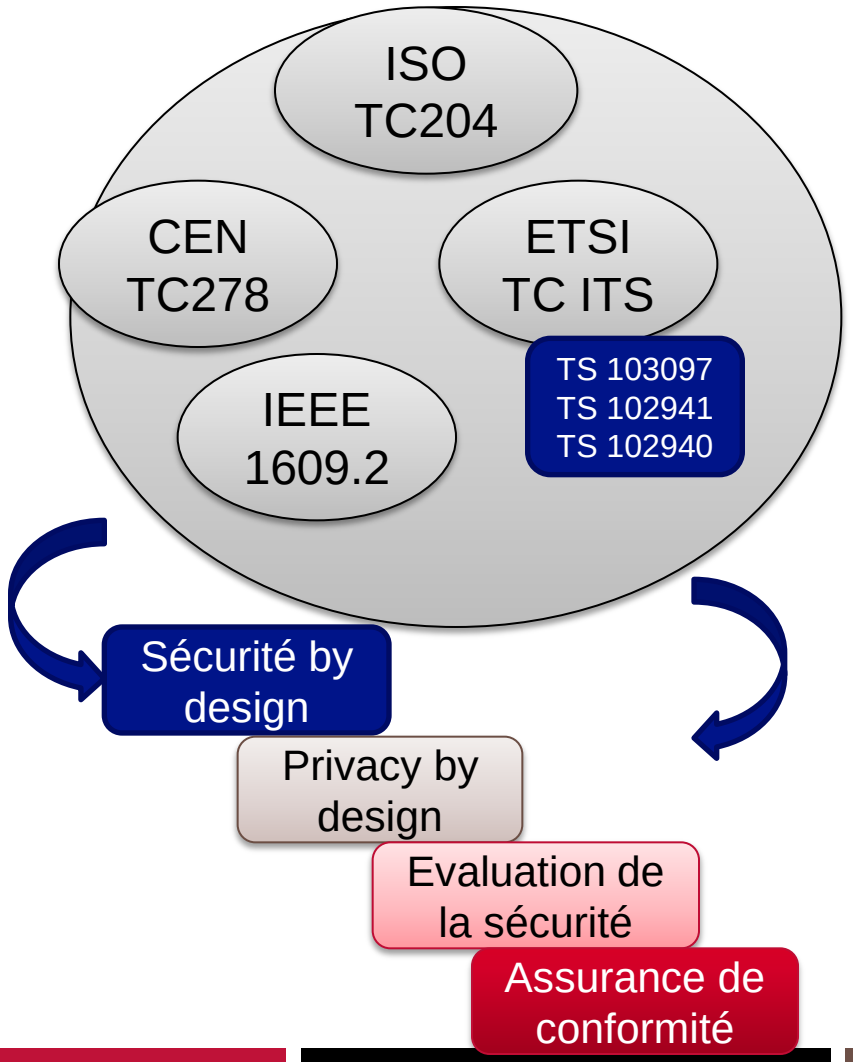
Modèle de confiance basé sur une chaîne de certification hiérarchique



2 types de certificats LTC & PC

ETSI, C2C, IEEE 1609.2, EU C-ITS platform trust model, SCOOP@F PKI

Standards sécurité: un état des lieux



- **Sécurité de bout-en-bout**
  - Architecture V2X sécurisée
  - Protocoles de communications sécurisés
  - Privacy
- **Sécurité des communications V2X hybrides**
  - 4G/LTE/5G, LTE-V2X, LTE-D2D, ITS-G5, 5GV2X
  - Protocoles de mobilité IP, Modèle et mécanismes de confiance
  - Privacy, QoS
- **Cryptographie légère, temps-réel et cryptoagilité**
  - Mise à jour à distance de la sécurité, stockage sécurisé
- **Privacy**
  - Anonymisation, pseudonymisation, stratégie de changement de pseudonymes
- **Révocation**
- **Détection de comportements anormaux, malicieux**
- **Scalabilité**
- **Intéropérabilité**
  - Architecture de communication, confiance
- **Standardisation**

Equipe SdR

- SdR (Sécurité des Réseaux) – depuis Mars 2015

Permanents	PhDs	Postdocs	REs
4 Prof., 1 MCF, 1 IR, 1 CA	13 (current)	4	2

Research Topics

Cybersecurity & Cyberdefense

- Trust (vehicular networks, MANETs, Mesh, connected objects, smartgrids)
- Large scale attack/intrusion detection
- Security on demand

Security architectures, security of data exchanges and applications (design, implementation, validation & optimisation)

- Cloud Computing, ICS (Industrial Control Systems)
- Internet of Things
- Wireless networks (vehicular networks, cooperative networks,…)

2016-2017: 60 publications, 4 PhDs (defended)

C-ITS, Connected & Autonomous vehicles

Research topics

- V2X security
- PKI vs. PKI-less
- Privacy
- Revocation
- Misbehavior detection, intrusion detection
- Resilience by design
- Cooperation Vehicular-cellular
- Mobility and connectivity analysis
- Routing, clustering, dissemination
- Security data analytics

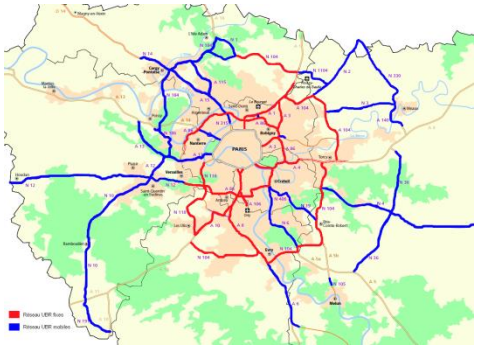
Pre-deployments projetcs SCOOP@F, InterCor and C-Roads

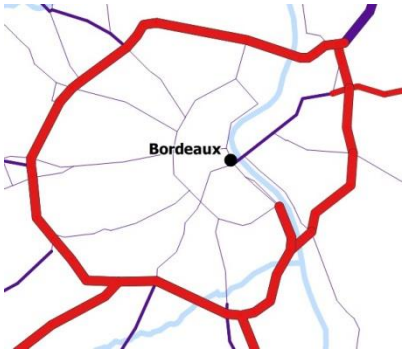
- **French collaboration**
  - IRT SystemX: Projects ISE & SCA.
  - L2S: Project D2D4V2X
  - VeDeCoM
- **International collaboration**
  - NTU (Singapour) : 1 PhD, defense in Septembre 2017.
  - NUS (Singapour) – privacy analysis of data traffic, NUS-Singtel Cybersecuirty lab.
- **Bilateral collaboration**
  - Renault, PSA, Orange, IMT-atlantique
  - **Chaire C3S**
- **Standardization**
  - ETSI, IETF, C-ITS Platform

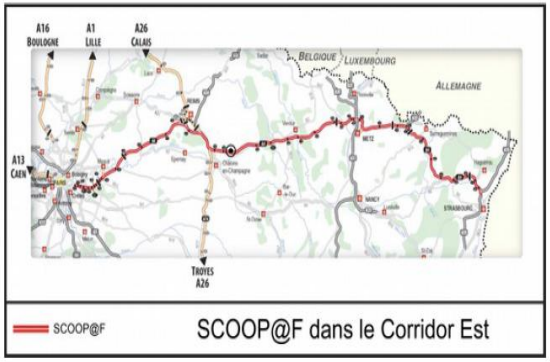
Pre-deployments projetcs SCOOP@F, InterCor and C-Roads

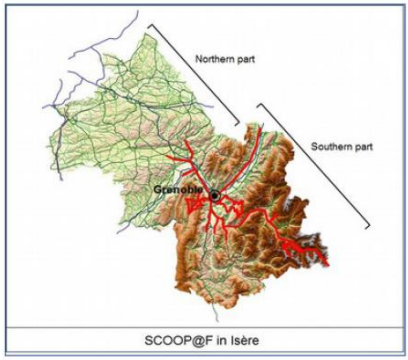
- **SCOOP@F part 1: 2014-2018**
  - Priority Services
  - Wireless communications ITS-G5 (IEEE 802.11p)
- **SCOOP@F part 2: 2016-2018**
  - New services
  - Hybrid Communications Cellular/ITS-G5
  - Crossed tests with other EU Member States
  - Cooperation with ongoing European pilot projects and the EU C-ITS platform
- **2000 vehicles, 350 RSUs, 2000 km**
- **Budget: 20 millions € funded by EU**

ANSSI, CNIL

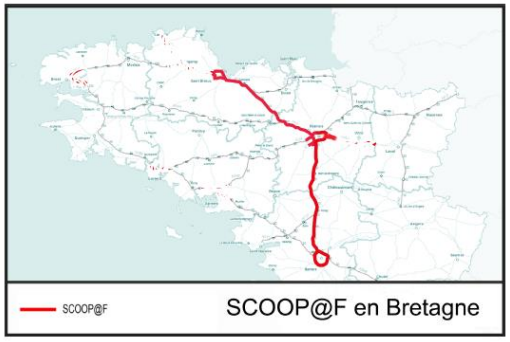








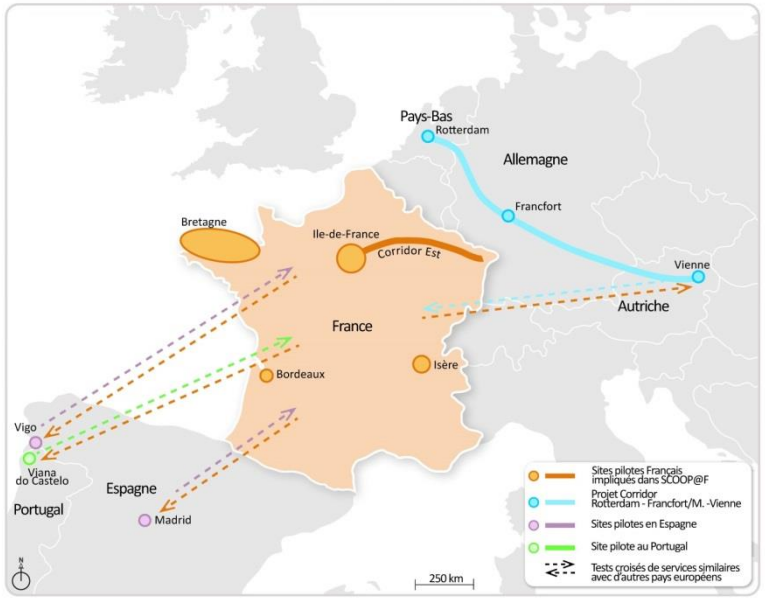
5 pilot sites
(different types of roads)



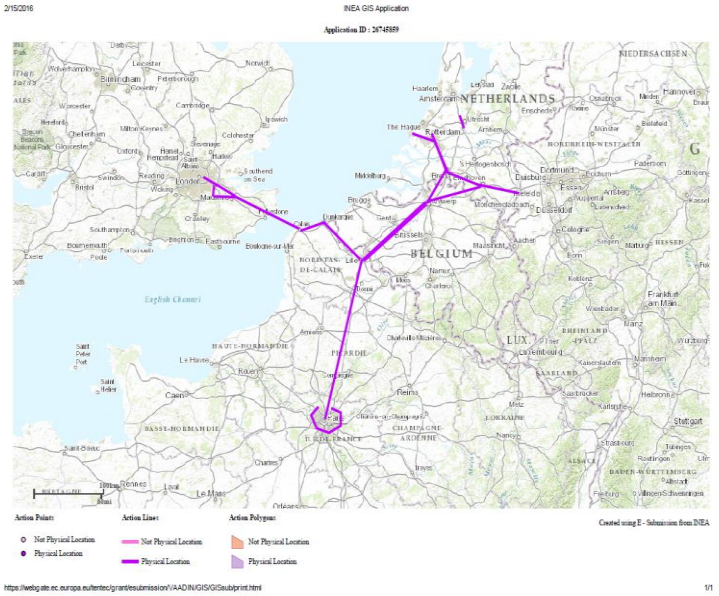
www.scoop.developpement-durable.gouv.fr/en

European partnerships

Crossed tests



SCOOP@F2



InterCor

Trusted and Secure Communications in Vehicular Mesh networks

- **Participator: Heng Chuan Tan**
- **Status: Joint PhD Télécom ParisTech & NTU (graduate at Sep. 2017)**
- **Target: trusted and secure V2V, V2I communications**
- **Research issues**
  - Defend Badmouthing attack, Ballot-stuffing attack, overhearing attacks and modification attacks in V-Mesh networks
  - Low-latency key management for vehicular networks to replace PKI

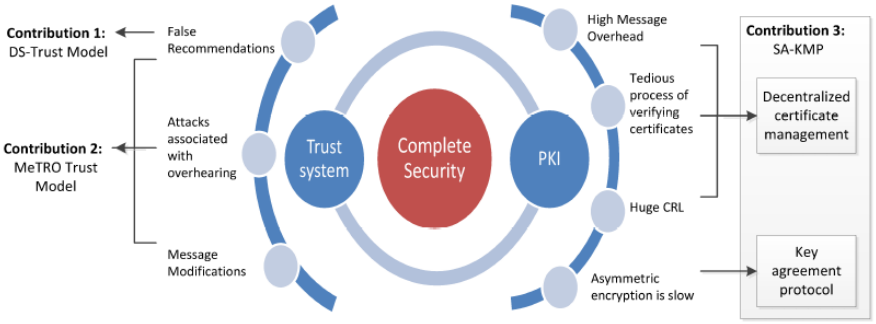


Fig. 1: Framework of trusted and secure communications in V-Mesh networks

- **Contribution**
  - Two trust models: DS-Trust, MeTRO
  - Key management protocol: SA-KMP

Publications	Journals	Conferences
published	2	3
In preparation /under review	1	

Representative work:

H. C. Tan, M. Ma, H. Labiod, P. H. J. Chong, and J. Zhang, "A Nonbiased Trust Model for Wireless Mesh Networks", International Journal of Communication System, 2016.

H. C. Tan, M. Ma, H. Labiod, A. Boudguiga, J. Zhang, and P. H. J. Chong, "A Secure and Authenticated Key Management Protocol (SA-KMP) for Vehicular Networks", IEEE Transactions on Vehicular Technology, 65(12):9570-9584, 2016.

Clustering in vehicular networks

- **Participator: Mengying Ren**
- **Status: Joint PhD in Télécom ParisTech & UTT (to be graduated at Feb. 2018)**
- **Target: establish robust infrastructures between vehicles**
- **Research issues**
  - Clustering in VANET to guarantee long CH/CM duration
  - Analysis of the impact of each component in clustering procedure
- **Contribution**
  - Mobility-based clustering
  - Unified Framework of clustering

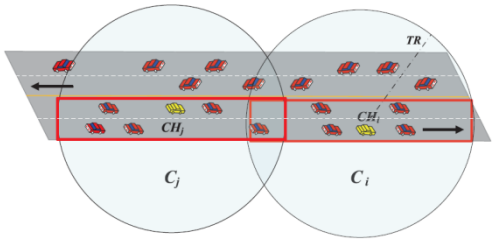


Fig. 2: Examples of clusters in vehicular networks

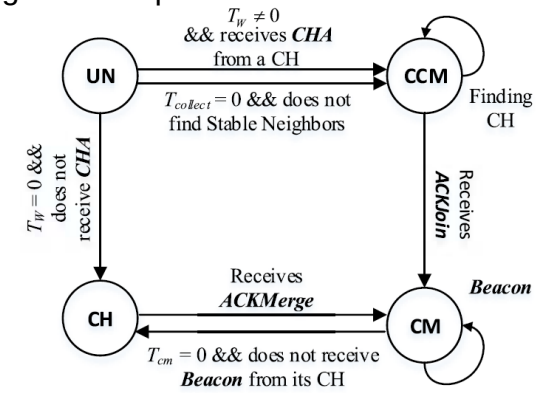


Fig. 3: State transition graph of clustering

Representative work:

M.Y. Ren, Jun Zhang, L. Khoukhi, H. Labiod, and V. Vèque, "A Unified Framework of Clustering Approach in Vehicular Ad hoc Networks", accepted by IEEE Transactions on Intelligent Transportation Systems , 2017

M.Y. Ren, L. Khoukhi, H. Labiod, Jun Zhang, and V. Vèque, "A Mobility-based Scheme for Dynamic Clustering in Vehicular Ad -hoc Networks (VANETs)", accepted by Vehicular Communications , 2017

Publications	Journals	Conferences
Journals	2	6
In preparation /under review	2	

Data dissemination in vehicular networks

- **Participator: Jun Zhang**
- **Status: Postdoc researcher**
- **Target: enable high-speed transmission in vehicular networks**
- **Research issues**
  - Information dissemination via evolutionary game theory (EGT)
  - Offloading in hybrid LTE-vehicle networks
  - Mobility pattern prediction for vehicles
  - Analytical model for clustering in vehicular networks
  - Privacy-aware data delivery in hybrid D2D-V2V networks
- **Contribution**
  - EGT-based information dissemination scheme
  - Joint active time and flow selection model for cellular content retrieval through ITS
  - Simulator-independent clustering algorithms comparison framework
  - Machin learning based link duration prediction

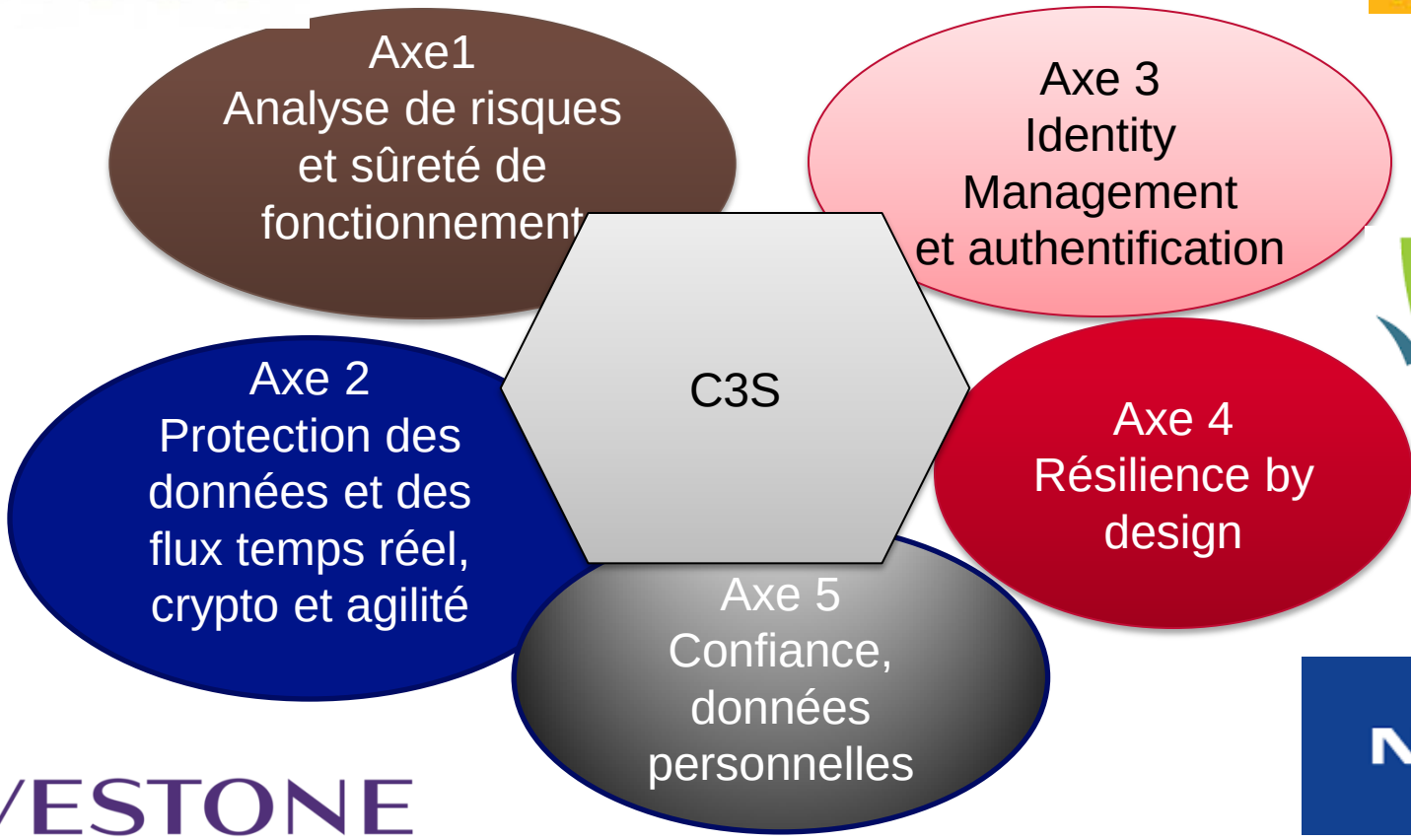
Publications	Journals	Conferences
Journals	5	9

Representative work:

Jun Zhang, Mengying Ren, Houda Labiod, and Lyes Khoukhi, " Link Duration Prediction in VANETs via AdaBoost", in IEEE GLOBECOM 2017

Jun Zhang, Vincent Gauthier, Houda Labiod, Abhik Banerjee, and Hossam Afifi, "Information Dissemination in Vehicular Networks via Evolutionary Game Theory", in IEEE ICC 2014

Axes Chaire C3S



https://chairec3s.wp.imt.fr/