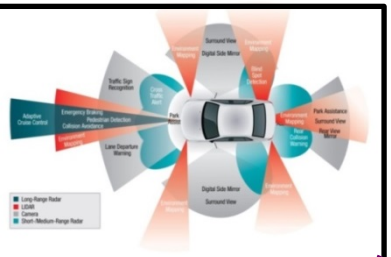
Protection de la vie privée, innocuité et immunité envers les cybermenaces dans les futurs réseaux de véhicules autonomes connectés

But d'innocuité (« safety ») : x fois moins d'accidents
(≈ 90% dus à des fautes humaines), x ≈ 10, efficacité > conduite humaine

vision et « toucher »

capteurs, robotique



parole et ouïe

communications V2V, informatique

véhicules autonomes connectés (VAC)

pas suffisant : accidents dès 2011 (Google cars), 1 mortel en 2016 (Tesla/Mobileye)

cognition et intelligence décisionnelle

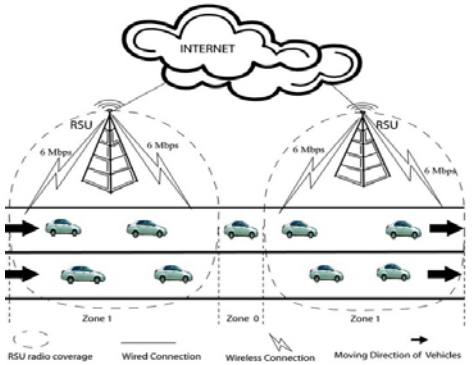
protocoles/algorithmes d'accord explicite connus (code de la route numérisé)

IA et apprentissage « algorithmisé »

WAVE 1.0 : WAVE + balisage périodique

Standards IEEE USA et ETSI Europe élaborés depuis 2004 :

► **Télécommunications wifi V2X, omnidirectionnelles, rayon ≈ 300 m**



réseaux terrestres
RSUs, nœuds 3G/4G/5G

VAC ≡ ordiphone-sur-roues

► **Données critiques (pour l'innocuité, non chiffrées) traitées comme les données personnelles (chiffrées)**

► **Balisage : diffusion {ID du véhicule + position GPS} 1 à 10 fois/s**

► **Nombreuses déficiences**

Évitement d'accidents ? Pas mieux que la robotique !

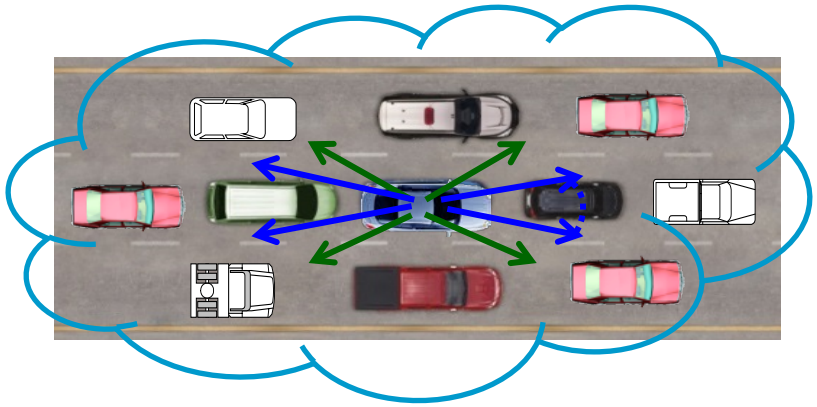
Diffusions vers des inconnus : espionnage, pistage des trajets, cyberattaques ➔ + ou – d'accidents ?

WAVE 2.0 : ~~télé~~ communications V2V

► Accidents ↔ véhicules très/trop proches ↔ communications directes courte portée (antennes adaptatives) pour accords rapides entre VAC spécifiques

optics (cameras, LEDs)

short-range radio (up to ≈ 60 m)



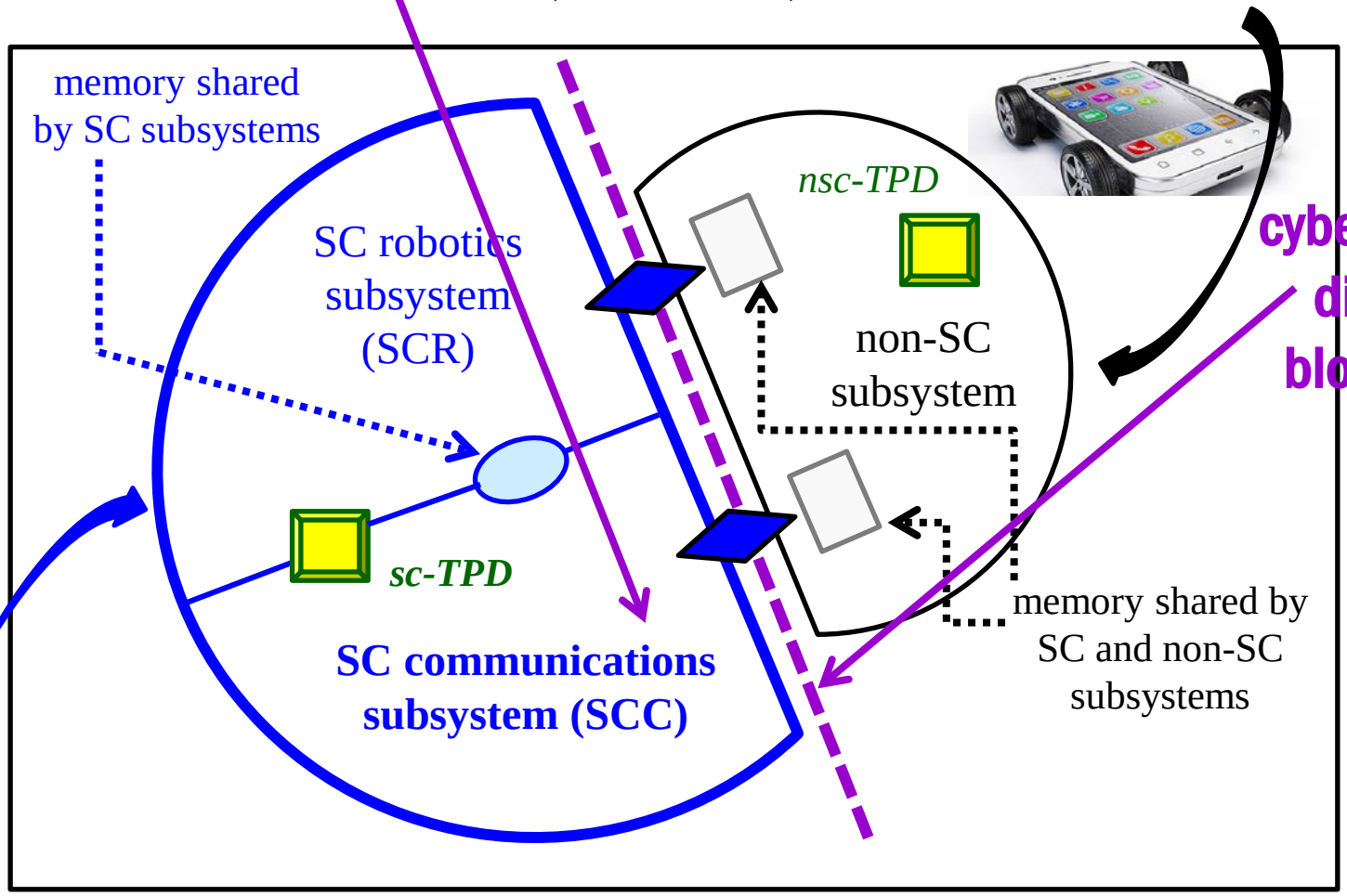
► Les messages critiques (innocuité) ne sont pas des données personnelles (vies humaines en jeu ➔ principe de ségrégation)

L'espionnage doit être impossible (« privacy »), et les cyberattaques (falsification, suppression, injection de leurres, MitM, usurpation d'identité, Sybil, etc.) ne doivent jamais mettre en péril l'innocuité.

cybermenaces rapprochées déjouées par SCC

non safety-critical, and global functionalities

[WAVE 1.1: WAVE, access to telecommunication networks (4G, LTE, 5G), to PKI-based services, to clouds, …]



cybermenaces distantes bloquées ici

WAVE 2.0 on-board system

safety-critical, and local functionalities

tamper-proof device

secured bridge

Pseudonymisation certifiée des émetteurs/véhicules

Réversibilité nécessaire pour l'imputabilité (*liability, accountability*)

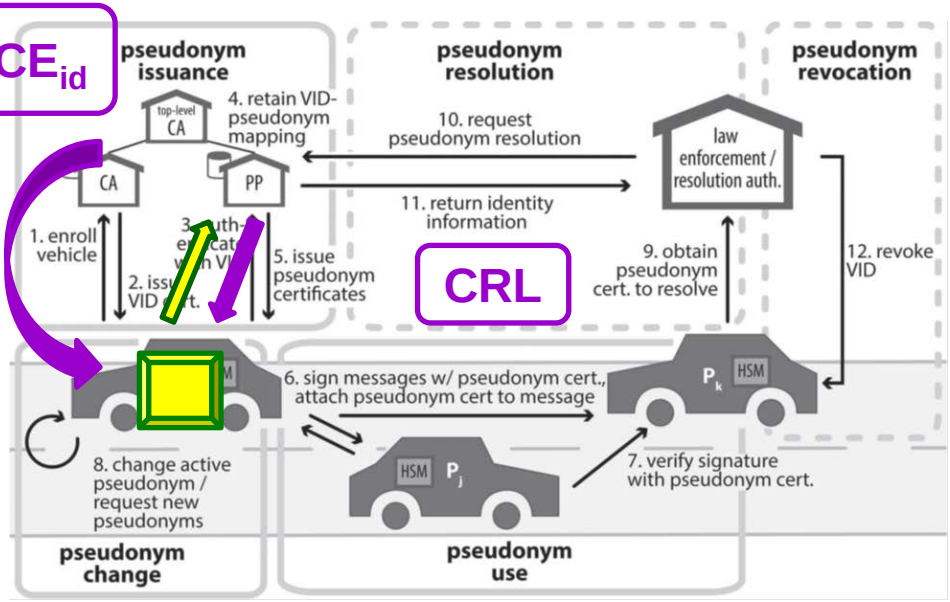
$ID \leftrightarrow CE_{id}$

$CE_{id} \leftrightarrow \{ps, ce_{ps}\}$

TPD (tamper-proof device)

pseudos certifiés

CE_{id} nouveaux $\{ps, ce_{ps}\}$



Courtesy/credit: J. Petit, F. Schaub, M. Feiri, F. Kargl, IEEE Com. Surveys & Tutorials, vol. 17, 1st quarter 2015

Infrastructures à Clés Publiques

Principe % comportement malhonnête :
prévention impossible ➔ identification du VAC et « punition » a posteriori

- **WAVE 1.0 : indissociable du balisage, accès en-ligne [télécoms, ICP] payants**
  Pseudonymie ssi diffusion. Mais si pair-à-pair (entre VAC spécifiques) ?
- **WAVE 2.0 : pas de balisage, pas d'accès ICP en-ligne (coûts nuls)**

IDÉE

Organisation spontanée de VAC au sein de laquelle les véhicules peuvent **se faire confiance** ?

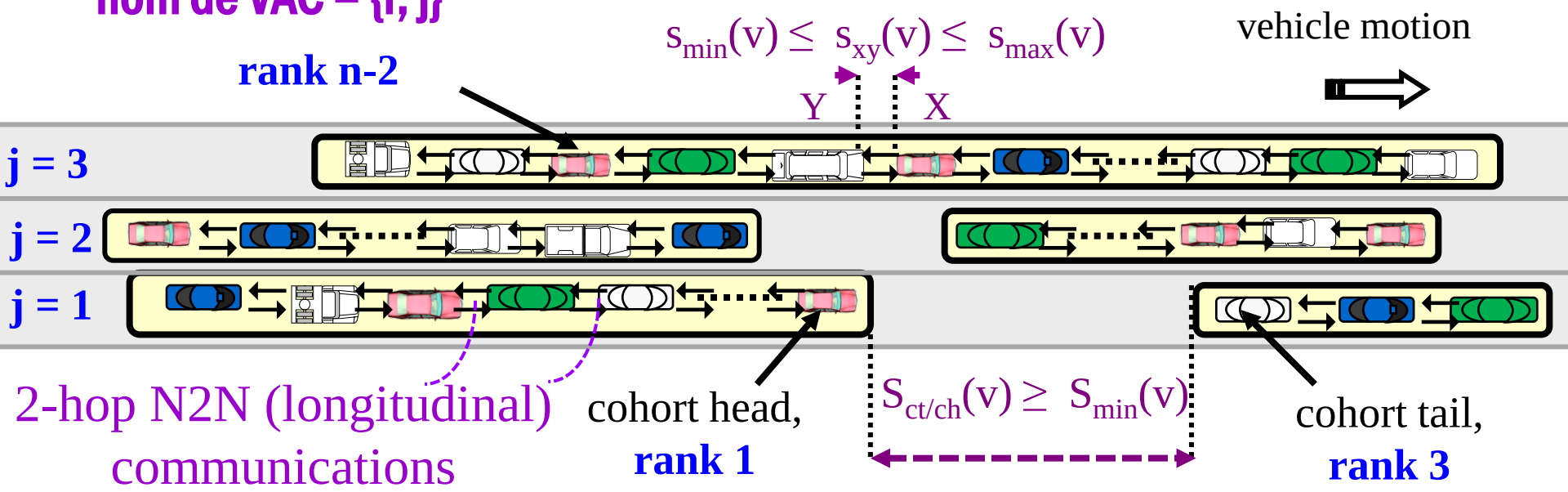
Pseudos utilisés ssi nécessaire.
Anonymisation des émetteurs et destinataires.

Organisation cyberphysique spontanée : cohorte

Formation linéaire ad hoc de VAC // bornes sup de délais

(accès canal, livraisons acquittées de messages, dissémination) ➔ preuves d'innocuité

nom de VAC = {r, j}



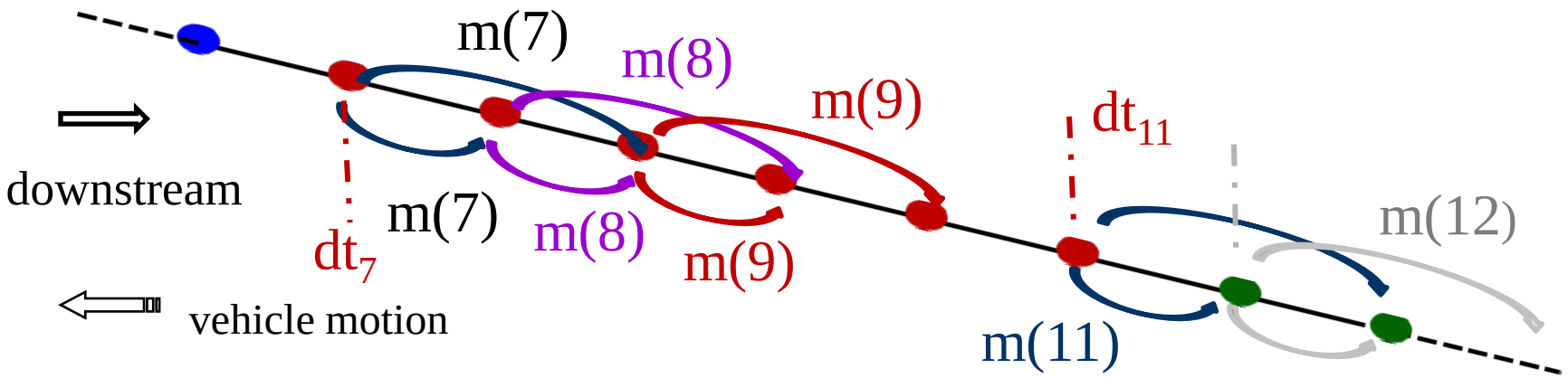
(1) **Authentifier tout véhicule** qui souhaite devenir membre d'une cohorte
➔ 1 {ps, ce_{ps}} consommé en cas de « join »

(2) **Anonymiser les métadonnées des messages SC** émis ensuite par les membres, **sans accéder à des ICP ➔ nom auto-généré = {r, j}**

(3) **Exclusion immédiate de tout véhicule malhonnête ➔ prédicats dans sc-TPD**

- nom de VAC = {r, j}, irréversible, peut changer à tout moment
- contenus des msg : codes non chiffrés (manœuvres possibles) sans coordonnées GPS
- LgSend(msg) : msg livré à 2 voisins

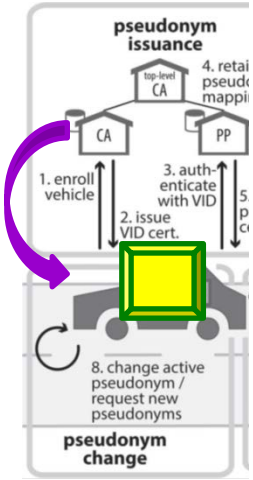
► espionnage inintéressant / traçage impossible,
► détection immédiate de falsification/suppression msg



- protocole MAC : TDMA ➔ rang r ↔ heure UTC d'émission t_r connue
- écoute limitée aux 2 voisins : r qui émet à t_r ne traite que les msg reçus de r-2 et r-1 (down) ou de r+2 et r+1 (up), heures d'émission connues (t_r- 2θ, t_r- θ)

détection immédiate d'usurpation de nom, d'attaque Sybil, MitM, ...

- CE_{id} et pseudonymes certifiés chargés (AC + ICP) dans sc-TPD *uniquement à l'enregistrement/ immatriculation*



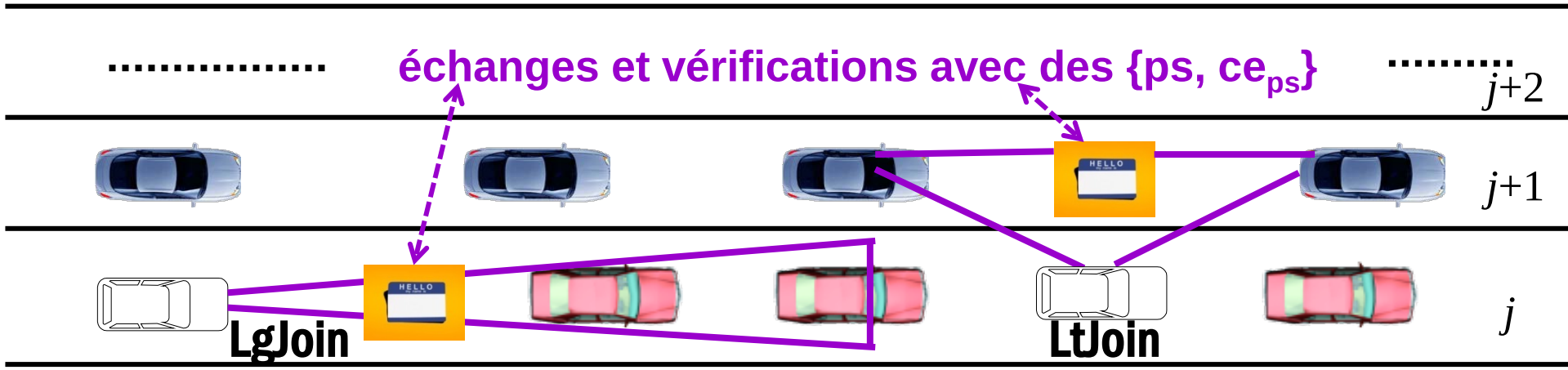
Pseudonymes certifiés réutilisables ad infinitum (retraçage impossible)

- sc-TPD contient des prédicats, violés si comportement malhonnête

Si prédicat violé, exclusion et arrêt physique

- Imputabilité // Sur arrêt, diffusion chiffrée vers les autorités habilitées de : [CE_{id}, position GPS] (+ contenu de sc-TPD ?)

► Authentification ? Au moment d'un LgJoin = demande d'admission dans une cohorte (longitudinal). LtJoin pour admission latérale ou échange de msg.



► Sans aucun accès aux réseaux publics/clouds ou ICP.

Double protection : authentification par pseudo certifié + anonymisation {r, j} de chaque message envoyé

Si attaque, seul « risque » : refus d'admission (cohorte)

Quel choix de société ?

► **Solutions WAVE 1.0** : **surveillance** et **cyberattaques possibles** lors de nos déplacements motorisés, sans avoir d'autre choix que de **payer** (pour être surveillés et attaqués), et **sans garantie d'innocuité** meilleure qu'avec la robotique embarquée.

► **Solutions WAVE 2.0** : **notre mobilité sur roues ne pourra faire l'objet de surveillance ou de cyberattaques**. Solutions à **coûts d'utilisation nuls** comparés à ceux de WAVE 1.0, garantissant également **l'innocuité maximale**.

Déploiement prévu aux USA à partir de 2020