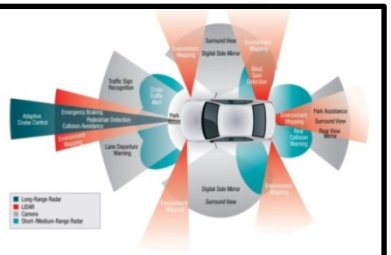
Safe Automated Driving and Cyber-Security on Highways*
Beyond Today's Connected Autonomous Vehicles

- Safety goal: divide accident rates by x, x ≈ 10 (≈ 90% due to human faults)
- Efficiency goal: asphalt utilization ratios > with human driving

vision and « touch »

sensors, robotics



insufficient : accidents since 2011 (Google cars), 1 fatal crash in 2016 (Tesla/Mobileye)

speech and hearing

IV communications, informatics

connected autonomous vehicles (CAVs)

cognition and decisional intelligence

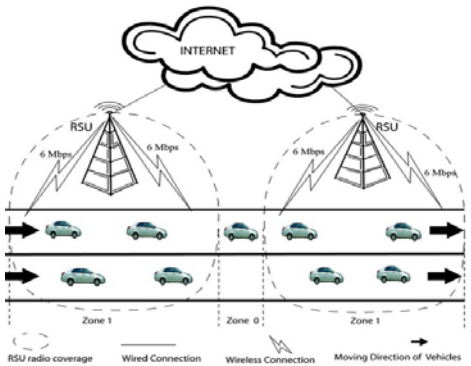
protocols + algorithms for explicit IV agreement (deterministic driving rules)

AI and algorithmic learning

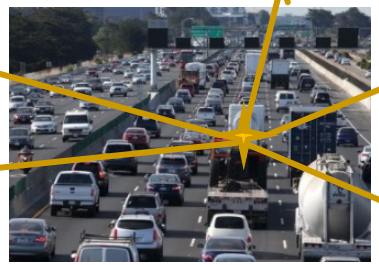
*** and elsewhere**

WAVE 1.0 : WAVE + beaconing + auth + PKIs for cert & pseudos

[1] 1st floor (ground level) ≡ WAVE (US and European standards ≈ 2010)



terrestrial nodes
(RSUs, 3G/4G/5G relays)



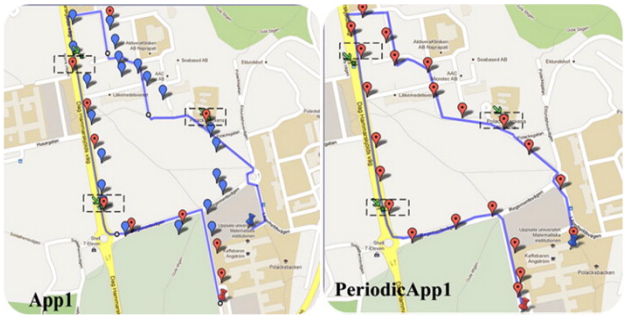
≈ 300 m

CAV ≡ smartphone-on-wheels

- ► Wifi telecommunications
- ► Channel access delays: no upper bounds, large average values
- ► No guaranteed message deliveries

Safety & efficiency?
≈ 0 improvement % robotics.

[2] 2nd floor ≡ periodic beaconing (1-10 Hz), with GPS coordinates ➔ LDMs



WAVE 1.0 : WAVE + beaconing + auth + PKIs for cert & pseudos

Broadcasts heard by unknown distant vehicles/nodes

- ➢ silent eavesdropping & tracking,
- ➢ cyberattacks ➔ - or + accidents ?

➲ **Additional goal: Cyber-Security (Privacy, Trust, Immunity to Cyberattacks)**

---

[3] 3rd floor ≡ vehicle authentication & {pseudonyms + certificates} <u>imported on-the-move</u> from cloud-based PKIs

[1 + 2 + 3] ➔

---

[1]: soon obsolete with 5G (5GAA) and next-gen IVCs (radio & optics)

[2]: useless + impossibility results (no beaconing)

[3]: OK if …

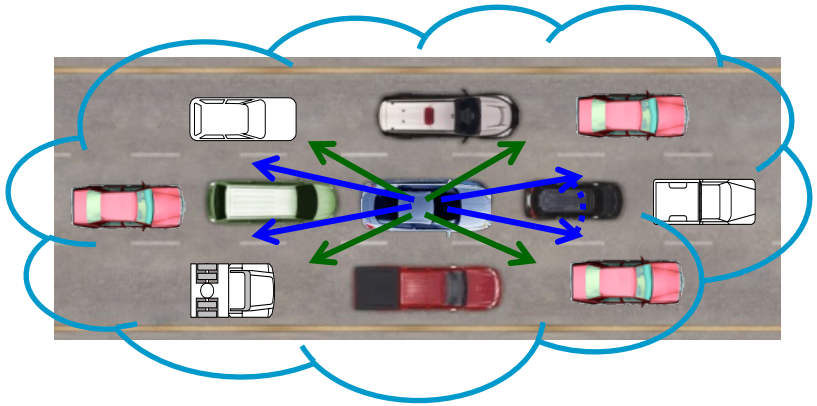
➔ **WAVE 2.0**

WAVE 2.0 : V2V ~~tele~~ communications + {auth & cert & pseudos}

❶ Safety & efficiency: short-range directional IVCs suffice

optics (cameras, LEDs)

short-range radio (up to ≈ 40 m)



- accidents ↔ vehicles (very) close to each other
- distant emergency conditions ?

❷ Safety in life-critical systems: the fundamental Segregation Principle

❸ Cyberthreats shall never undermine safety

❶ *See publications for protocols, agreement algorithms, and worst-case bounds*

λ: worst-case upper bound of <u>channel access delays</u>

Δ_d: worst-case upper bound of <u>string-wide ack'ed message dissemination delays</u>

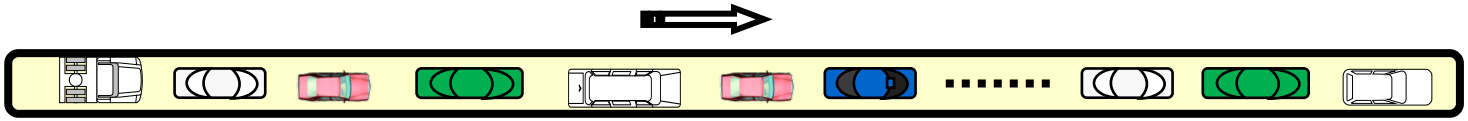
Δ_a: worst-case upper bound of <u>string-wide or inter-string agreement delays</u>

(Δ's for non malicious faults) *σ = smallest asphalt slot ≈ 7 m*

BM_0: a **MAC protocol** is acceptable only if **dist travelled in λ << σ**

BM_1: a string-wide **ack'ed message dissemination algorithm** is acceptable only if **dist travelled in $\Delta_d < \sigma$**

BM_2: a string-wide or inter-string **agreement algorithm** is acceptable only if **dist travelled in $\Delta_a <$ 2σ**



Safety ≡ cyber-synchronization (« cooperation ») prior to risk-prone maneuvers

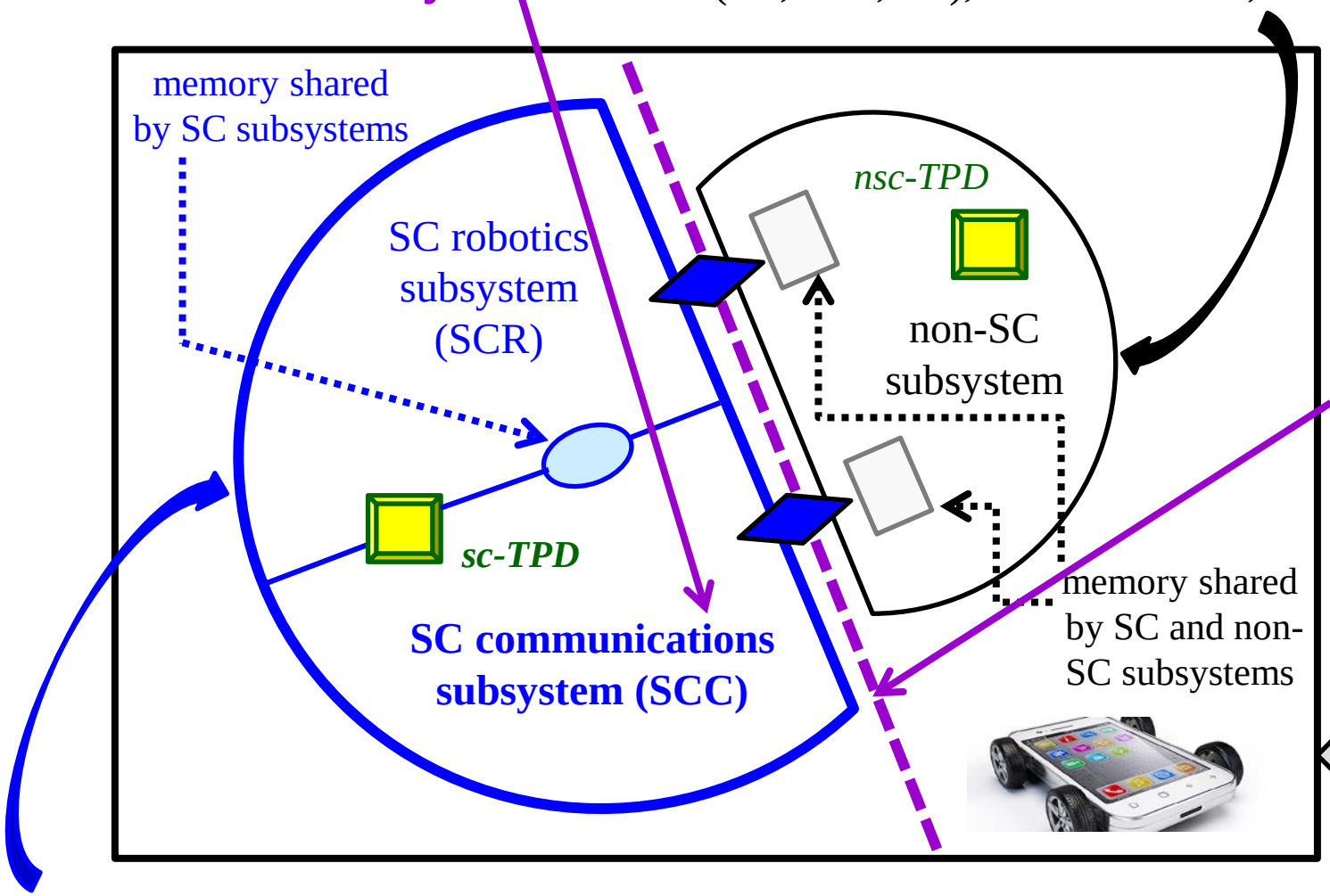
Problems in Cyber-Physics ➔ cyber-physical constructs needed ➔ cohorts ❹

❷ ❸

close cyber-surveillance and attacks: thwarted by SCC

non safety-critical and global functionalities

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



remote cyber-surveillance and attacks: blocked here

WAVE 2.0 on-board system

safety-critical and local functionalities

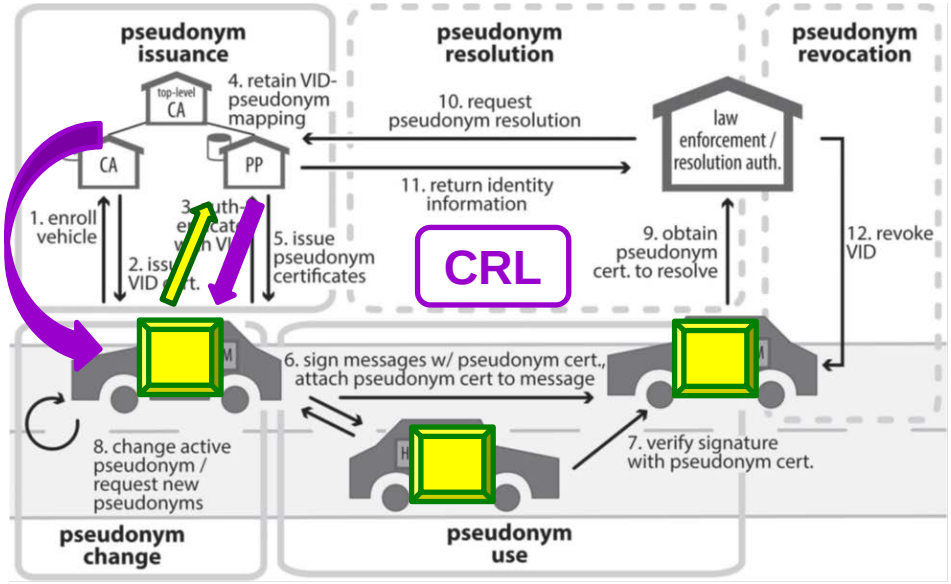
tamper-proof device

secured bridge

Authentication and certified pseudonymity

Reversibility needed for non-repudiation, liability, accountability

Registration & authentication:
ID ↔ CE_{id}
Pseudos & certificates{ps, ce_{ps}}



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

Replenishment: **CE_{id}**

New {ps, ce_{ps}} from Public Key Infrastructures

TPD (tamper-proof device)

- **Attacks: MitM, suppression, spoofing, …**
- **Tracking still feasible even if pseudos changed frequently**
- **Paying services (telecoms, PKI)**

WAVE 2.0 → no replenishment

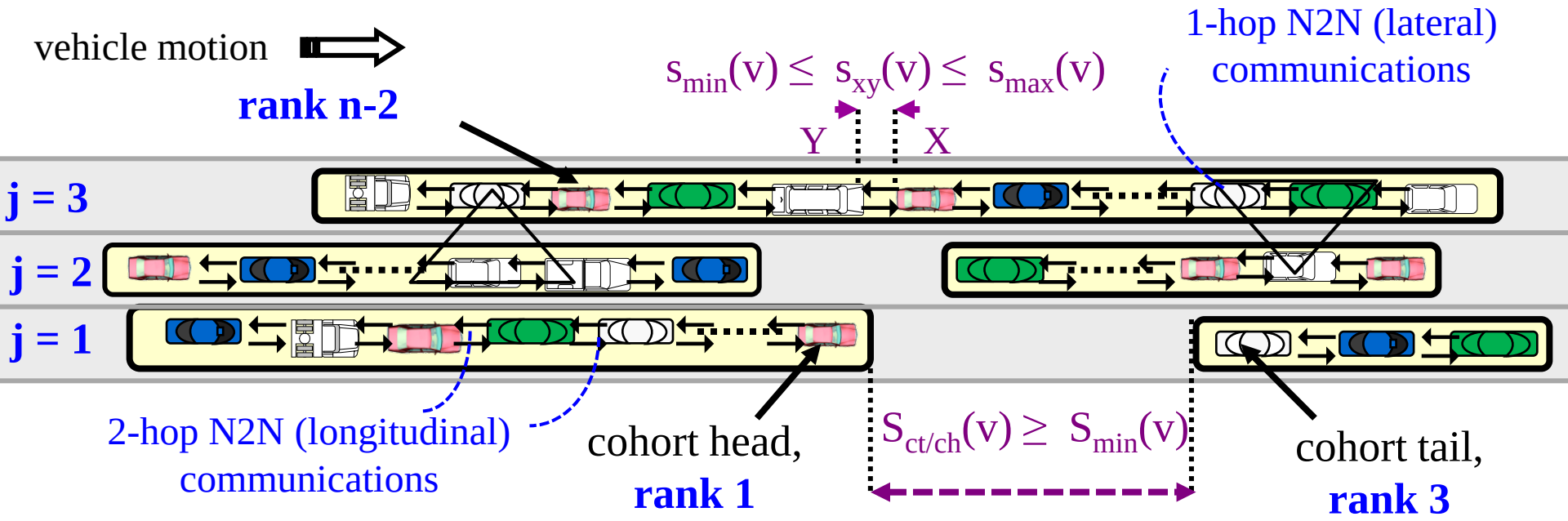
4 Cohorts: spontaneous formations of CAVs in Cyber-Physics

➲ **Safety proofs (physical space)**

➲ **Cohort members can trust each other (cyber space)**

- ❖ **A certified pseudo utilized only for …**
- ❖ **Member name ≡ {r, j} ➔ non reversible anonymity**

➢ **double obfuscation**



Safety and Cyber-Security with WAVE 2.0

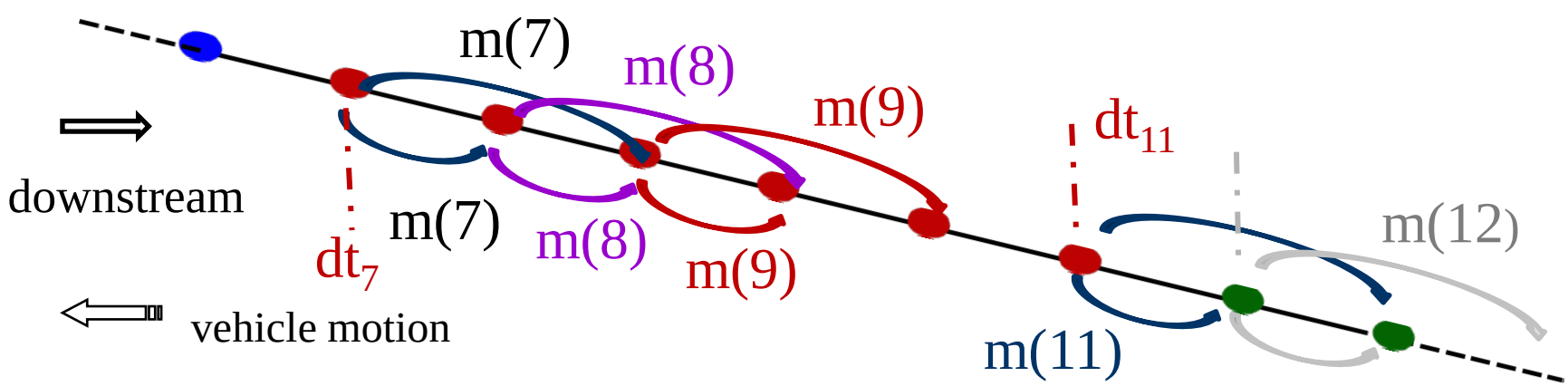
► Remote cyberattacks from unknown sources cannot compromise safety

► Close eavesdropping and tracking: unfeasible and useless

► Close cyberattacks (msg falsification/suppression, masquerading, injection of bogus data, Sybil attack, ...): detected in 0 delay, cannot compromise safety

Predicates in sc-TPD

► If predicate violated, vehicle excluded/halted, and [CE_{id} + GPS location + encrypted contents of sc-TPD] broadcast to authorities



Which Society Do We Want?

WAVE 1.0 solutions:

- **Potential exposition to cyber-surveillance and cyberattacks while travelling on wheels**
- **Having to pay (for being possibly spied on and cyberattacked)**
- **Safety no better than with on-board robotics**

WAVE 2.0 solutions:

- **Connected autonomous vehicles are safe privacy-preserving harbors: highest safety despite cyberattacks, no eavesdropping or tracking (option offered by OB systems)**
- **No fees due to telcos or PKIs**

Deployment planned starting 2020 in the USA (NHTSA)