Future Directions in Connected Autonomous Vehicles and Autonomic Vehicular Networks

gerard.le_lann@inria.fr

1. Introduction

2. WAVE 1.0

3. Motives

4. WAVE 2.0

5. Perspectives

Safety

Efficiency

Privacy

Cybersecurity

Official stance (*headlines, videos, interviews)* from the C-ITS community (BigAuto, New Players, OEMs, …)

Our primary motivations for **autonomous vehicles** (AVs) are **Safety** and **Efficiency**

❖ Safety

Smaller number of accidents and fatalities ► ≈ 1/10

antagonistic goals

[Ex.: 1 fatality per day rather than 9 (France)]

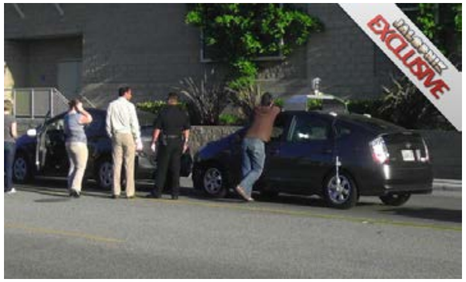
❖ Efficiency

Small inter-vehicular gaps at high velocities (reduce travel times, energy consumption, …), optimal use of asphalt resources

Fairy tales versus facts

☹ AVs have logged million miles without an accident

▶ 2011: Google

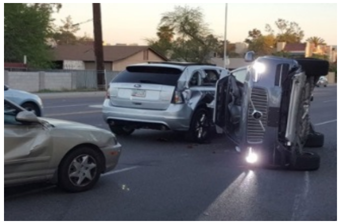


1st fatality
▶ May 2016:
Tesla (radar)

2nd fatality
▶ March 2018:
Volvo/Uber
(lidar)

3rd fatality
▶ March 2018:
Tesla (radar)

Since 2011, dozens/hundreds accidents…



Robotics

Diversified sensors (radars, lidars, infrared, cameras, ultrasonic,…), kinematics, automated learning,…

▶ Not sufficient for safety and efficiency ⇨ **CAVs**

Robotics

Diversified sensors (radars, lidars, infrared, cameras, ultrasonic,…), kinematics, automated learning,…

▶ Not sufficient for safety and efficiency ⟹ **CAVs**

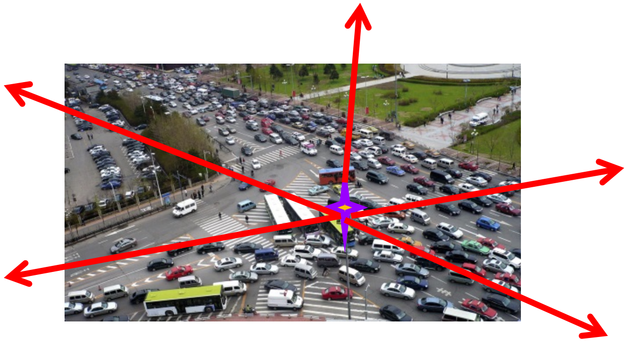
WAVE 1.0

◈ **WAVE (Wireless Access in Vehicular Environment):**
unique technology for V2I and V2V radio telecoms

- *** "Co-operative" Awareness Messages (CAMs ≡ beacons)**
- *** Decentralized Environmental Notification Messages (DENMs)**
- *** Unacknowledged broadcast mode (no co-operation!)**

◈ **Periodic Beaconing + Local Dynamic Maps**

IEEE 802.11p , ETSI ITS G5 standards for connected automated vehicles ≈ 2010



WAVE: omnidirectional wifi
(5.9 GHz, 6 Mbits/s, radius ≈ 300-500 m)

V2I: vehicle-to-infrastructure

for infotainment

V2V: vehicle-to-vehicle

for safety (supposedly)

1) WAVE Protocols

❖ CCH: the only radio channel (among 7) for beacons and DENM messages

❖ Unbounded delays

❖ Unbounded message losses

??

Safety ≡ hard real-time (< 30 ms)
+ ultra high reliability

** CSMA-CA MAC protocol **

* random back-off

* ***average*** delays in heavy traffic ≈ 200 ms

KLEINROCK AND TOBAGI: PACKET SWITCHING IN RADIO CHANNELS:

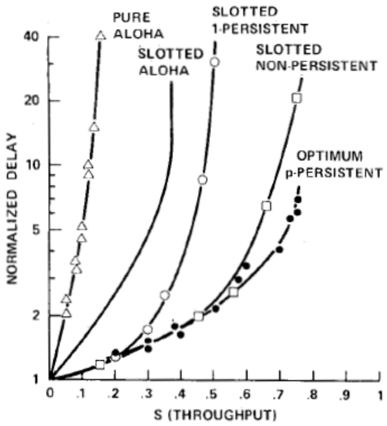
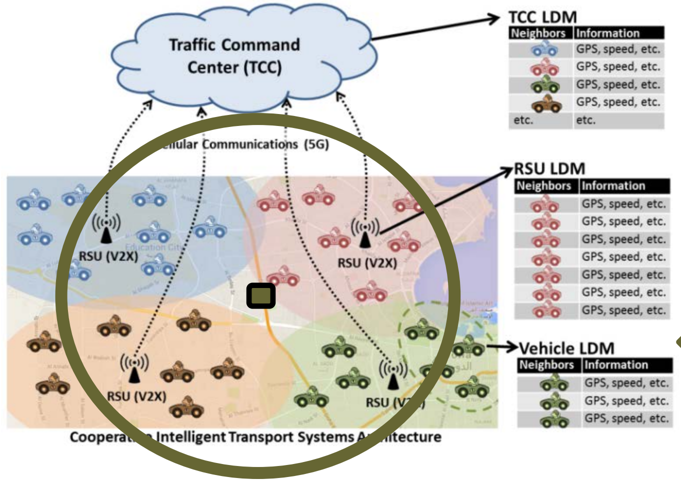


Fig. 12. Throughput-delay tradeoffs from simulation ($a = 0.01$).

Inappropriate for safety/efficiency

2) Periodic Beaconing + LDMs


Traffic Command Center (TCC)
llular Communications (5G)
RSU (V2X)
RSU (V2X)
RSU (V2X)
RSU (V
Cooperat Intelligent Transport Systems A itecture

TCC LDM

Neighbors	Information
	GPS, speed, etc.
	GPS, speed, etc.
	GPS, speed, etc.
	GPS, speed, etc.
etc.	etc.

RSU LDM

Neighbors	Information
	GPS, speed, etc.
	GPS, speed, etc.
	GPS, speed, etc.
	GPS, speed, etc.
	GPS, speed, etc.
	GPS, speed, etc.
	GPS, speed, etc.

Vehicle LDM

Neighbors	Information
	GPS, speed, etc.
	GPS, speed, etc.
	GPS, speed, etc.

Timestamped beacons (CAMs) carry GNSS geodata + velocity + ... are broadcasted periodically (1 to 10 Hz)

► local dynamic maps (diameter ≈ 0.6-1 km)

- ◈ Inaccurate GNSS geodata? Different inaccuracies for different vehicles?
- ◈ Malicious vehicles may lie (false GNSS geodata)
- ◈ LDM: concurrent reads/writes
- ◈ Undelivered beacons (losses)

Inconsistency

$\forall\{X, Y\}\ \ LDM_X \neq LDM_Y$

Beaconing? Useless % safety. Harmful % « pollution »

◈ Very low packet delivery rates

(due to channel contention)

≈ 0.1 at distance ≈ 250 m

≈ 0.95 at distance ≈ 35 m

Considered OK by C-ITS community

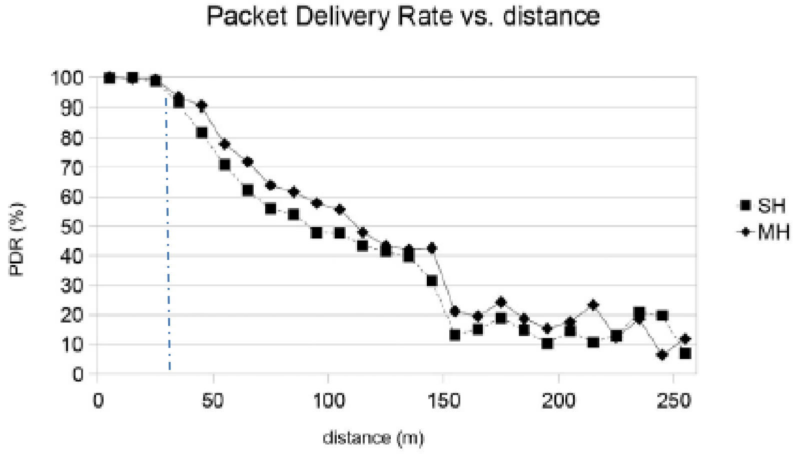


Fig. 12. PDR vs. distance for single- and multi-hop NLOS links in the second measurement campaign.

Safety-critical functions:

proba (success) ≈ 1-10^{-6} / hour (ISO 26262)

Small inter-vehicular gaps? Rely on onboard robotics!

➲ Safety and efficiency gains with WAVE 1.0

% onboard robotics ≈ 0

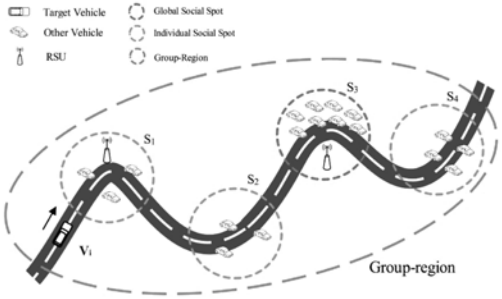
With WAVE 1.0, connected automated vehicles ≡

Smartphones-on-wheels may kill …

With WAVE 1.0, connected automated vehicles ≡

Smartphones-on-wheels may kill ...

❖ **Privacy threats**



Personal data revealed (eavesdropping, tracking)

Hackers Remotely Kill a Jeep on the Highway—With Me in It

❖ **Cybersecurity threats**

Safety compromised by cyberattacks

(masquerading, Sybil attacks, message falsification/suppression, intrusions (viruses, malware, …), injection of bogus data, …)

Privacy

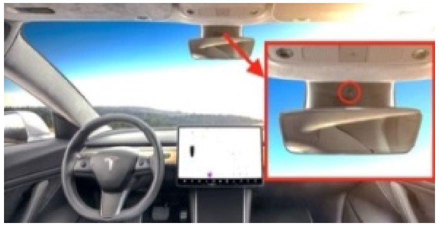
In addition to:

❖ ❖ ❖ ❖ ❖❖ **EXTERNAL** EAVESDROPPING WITH WAVE 1.0 ❖ ❖ ❖ ❖ ❖ ❖

how to combat

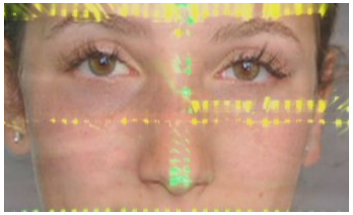
INTERNAL CYBER-ESPIONNAGE?

Janusian justification: for assisted driving (ADAS)



Facial recognition

Continuous cybersurveillance



Who collects, stores, processes, mines, resells, personal data?

Reasons? For how long? Responsibilities in case of hacking?

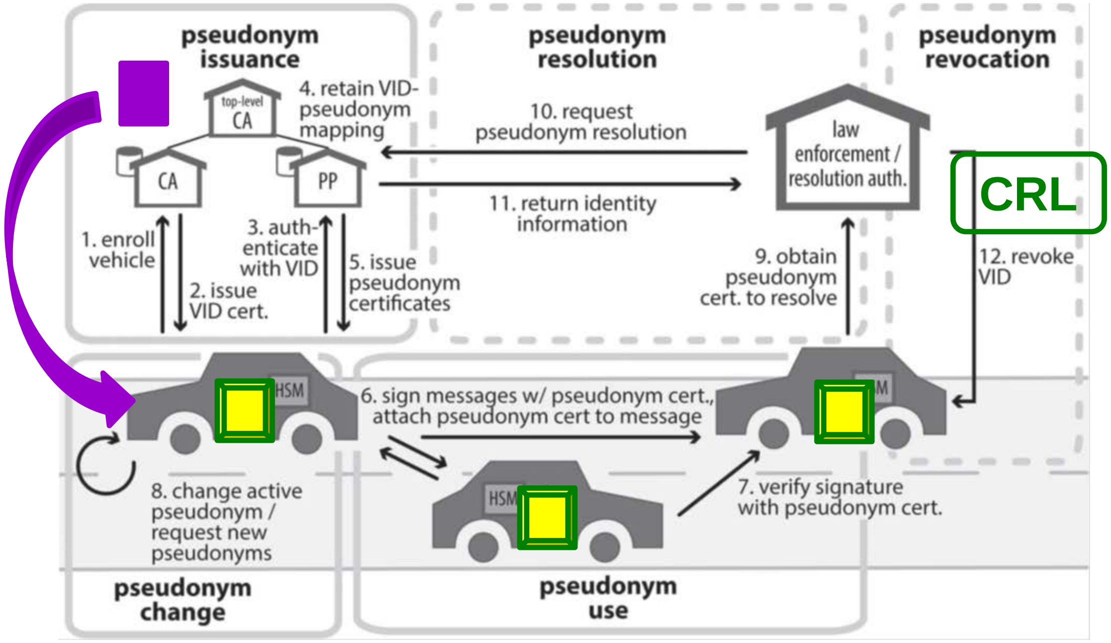
1 long-term reversible certificate 🟪

+

***c* non-reversible short-term credentials/pseudos {key pair, certificate}**

Reversibility mandatory for accountability/auditability

Hardware Sec Module (tamper-proof device) 🟨

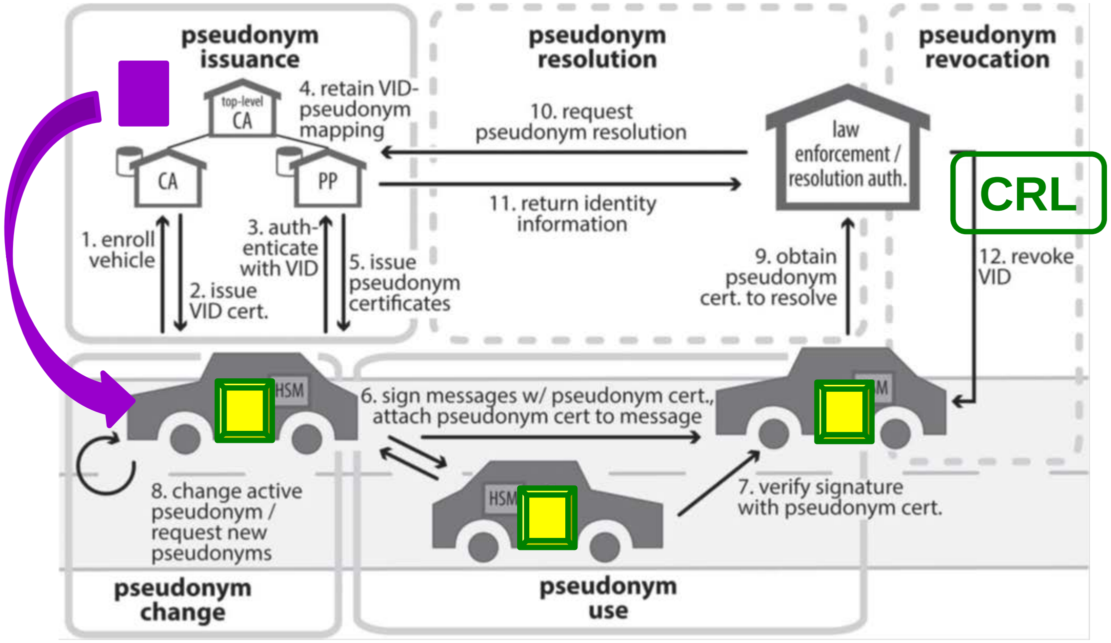


pseudonym issuance
top-level CA
4. retain VID-pseudonym mapping
CA
PP
1. enroll vehicle
2. issue VID cert.
3. auth-enticate with VID
5. issue pseudonym certificates
pseudonym resolution
10. request pseudonym resolution
11. return identity information
law enforcement / resolution auth.
9. obtain pseudonym cert. to resolve
pseudonym revocation
CRL
12. revoke VID
HSM
6. sign messages w/ pseudonym cert., attach pseudonym cert to message
7. verify signature with pseudonym cert.
8. change active pseudonym / request new pseudonyms
pseudonym change
pseudonym use

Courtesy/credit: J. Petit, F. Schaub, M. Feiri, F. Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey", IEEE Com. Surveys & Tutorials, vol. 17, 1st quarter 2015

Cybersecurity

Some open issues with periodic beaconing (1-10 Hz)


pseudonym issuance
top-level CA
CA
PP
4. retain VID-pseudonym mapping
1. enroll vehicle
2. issue VID cert.
3. auth-enticate with VID
5. issue pseudonym certificates
pseudonym resolution
10. request pseudonym resolution
11. return identity information
law enforcement / resolution auth.
9. obtain pseudonym cert. to resolve
pseudonym revocation
CRL
12. revoke VID
HSM
6. sign messages w/ pseudonym cert., attach pseudonym cert to message
7. verify signature with pseudonym cert.
8. change active pseudonym / request new pseudonyms
pseudonym change
pseudonym use

- ❖ c pseudos, each used once for x consecutive beacons
- ❖ c? x?
- ❖ How long before refilling?

- ❖ *c* ↘ 0 ► refilling via Public Key Infrastructures, i.e. V2I telecoms
  ► man-in-the-middle attacks (e.g., suppressions)
- ❖ Revocation of credentials based on denunciations/reporting (cyber space)
  ► malicious adversary coalitions?
  ► CRL management?
- ❖ « Revocation » in physical space (mandatory for safety)?
  C-ITS community mute on that…

≈ 750 Billion US $ in 2030

Big data ≡ big money ...

... falling from the skies

(radio coms in the ether)

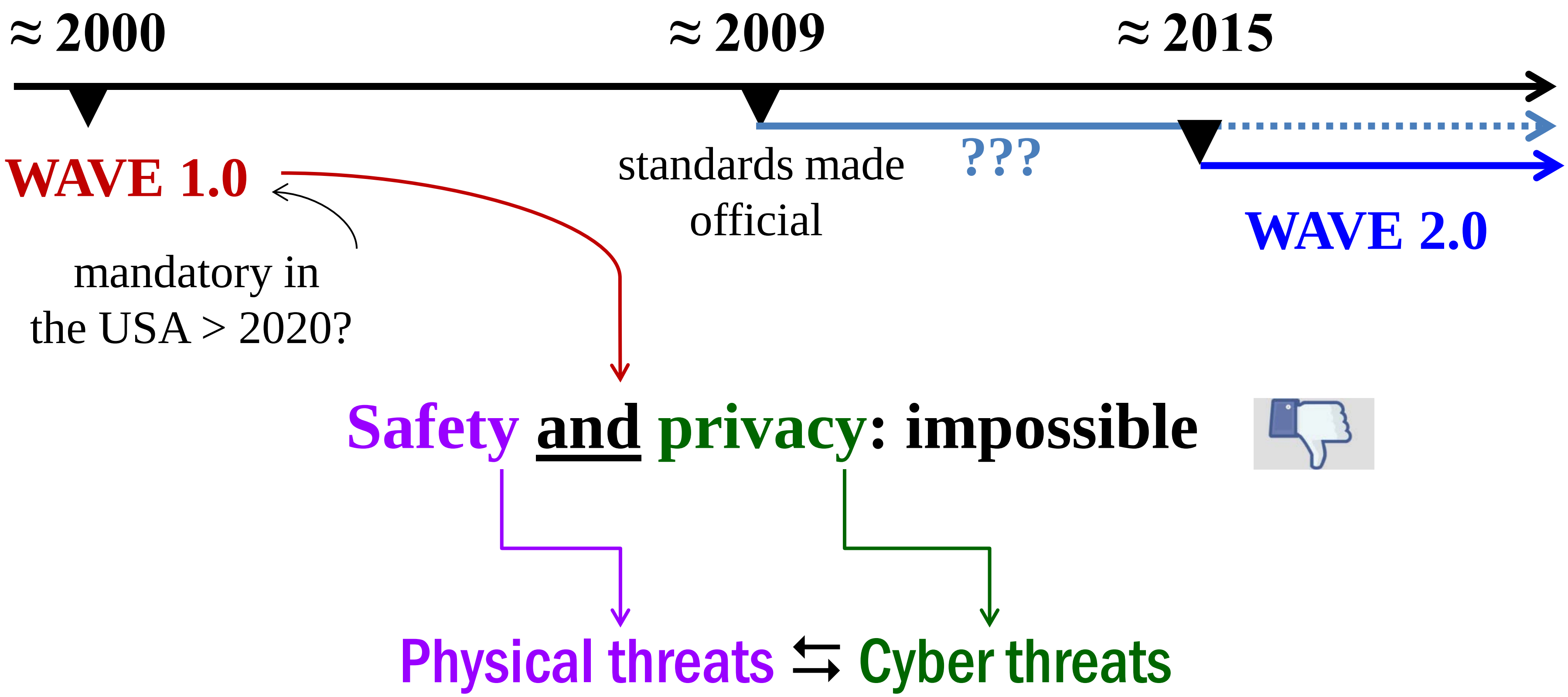
C-ITS' motivations for **CAVs?** **Personal Data!**

In coopetition* with GAFAM and BATX

Big ~~Brother~~ Browser is watching you...

***competitive cooperation**

Technological Waves



≈ 2000

≈ 2009

≈ 2015

WAVE 1.0

mandatory in
the USA > 2020?

standards made
official

???

WAVE 2.0

Safety and privacy: impossible

Physical threats ⇆ Cyber threats

Cyber injuries: personal data hacked, corrupted, ...

Cyber deaths: irreversible loss of personal data, stolen IDs, ...

WAVE 1.0 combated by some US and European lawyers + advocacy groups + scientists + ACLU + EFF + some members of the C-ITS community (5GAA, …) + …

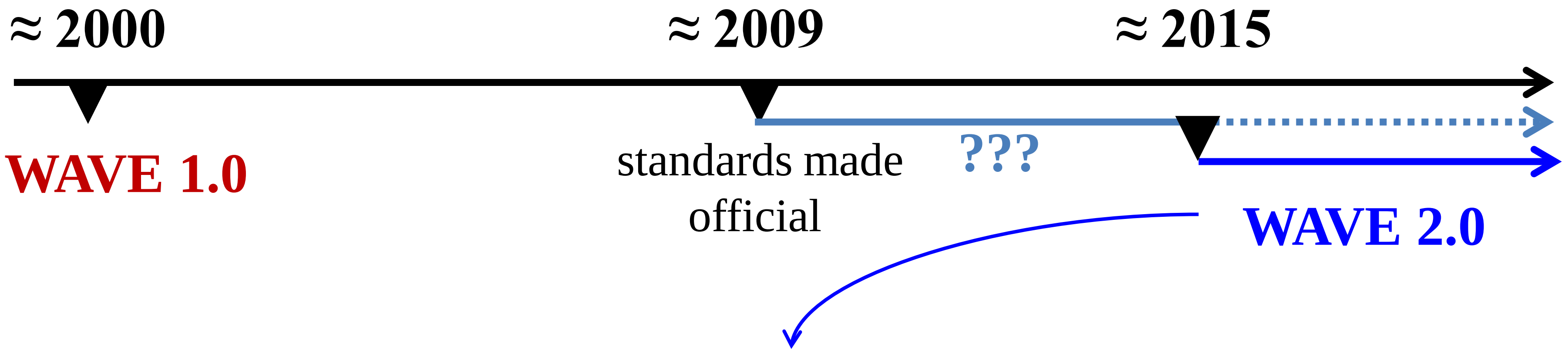
Technological Advances since ≈ 2010

Power controlled MIMO, beamforming, 3GPP/LTE ProSe Direct, 5G NR, optical communications, lane-level positioning, OB tech (kernels, HSMs, …), …

2017 EU WP 29 Resolution, 2018 EU GDPR

WAVE 1.0 ➢ WAVE 2.0

Technological Waves



≈ 2000

≈ 2009

≈ 2015

WAVE 1.0

standards made official

???

WAVE 2.0

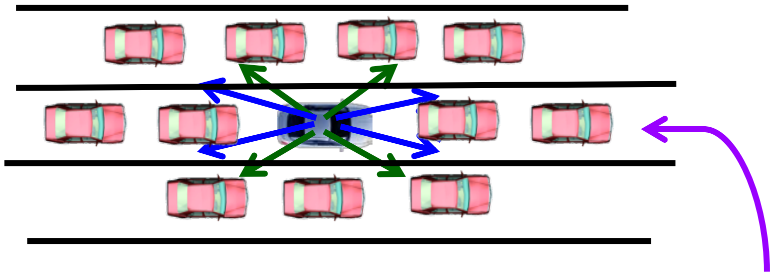
Safety + **efficiency** + **privacy** + **cybersecurity** ***by design***

- ❖ **Remote** eavesdropping/tracking? Unfeasible!
- ❖ **Remote** cyberattacks? Unfeasible!
- ❖ **Nearby** eavesdropping/tracking? Useless (worthless data)! Not worse than human « espionnage » (licence plates in LOS)!
- ❖ **Nearby** cyberattacks? Irrational, easily detected!

Cyberphysical constructs — Short-range radio/optical coms

❒ Vehicular Cells

Neighbor-to-neighbor unicast coms
Range-1 lateral coms (≈ 10 m)
Range-2 longitudinal coms (≈ 50 m)

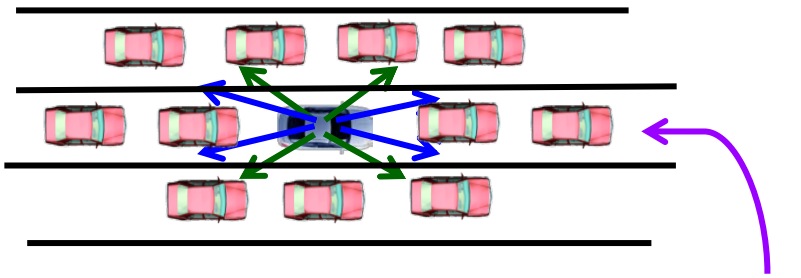


quasi-maximal
Cell

Cyberphysical constructs — Short-range radio/optical coms

❒ Vehicular Cells

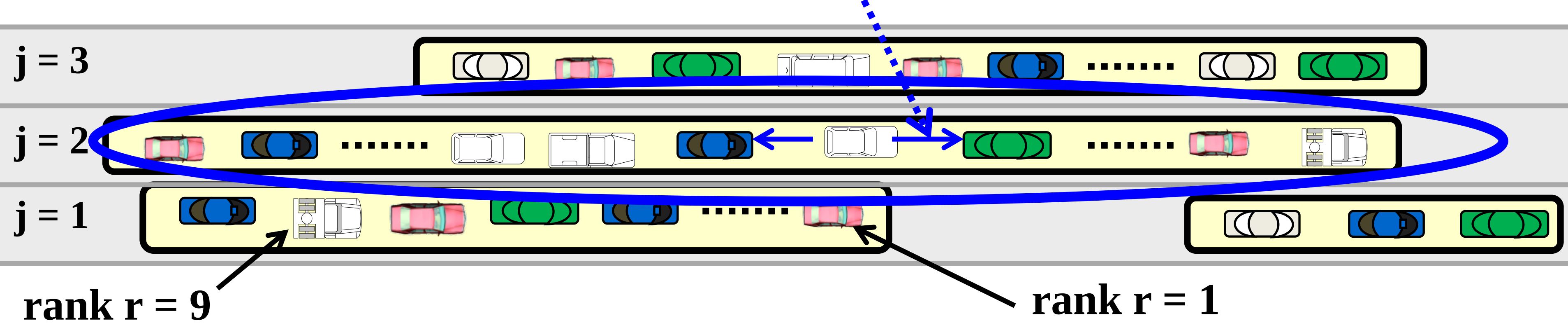
Neighbor-to-neighbor <u>unicast</u> coms
Range-1 lateral coms (≈ 10 m)
Range-2 longitudinal coms (≈ 50 m)



quasi-maximal Cell

❒ Cohorts

Range-2 N2N coms and cohort-wide longitudinal relaying (up/downstream)

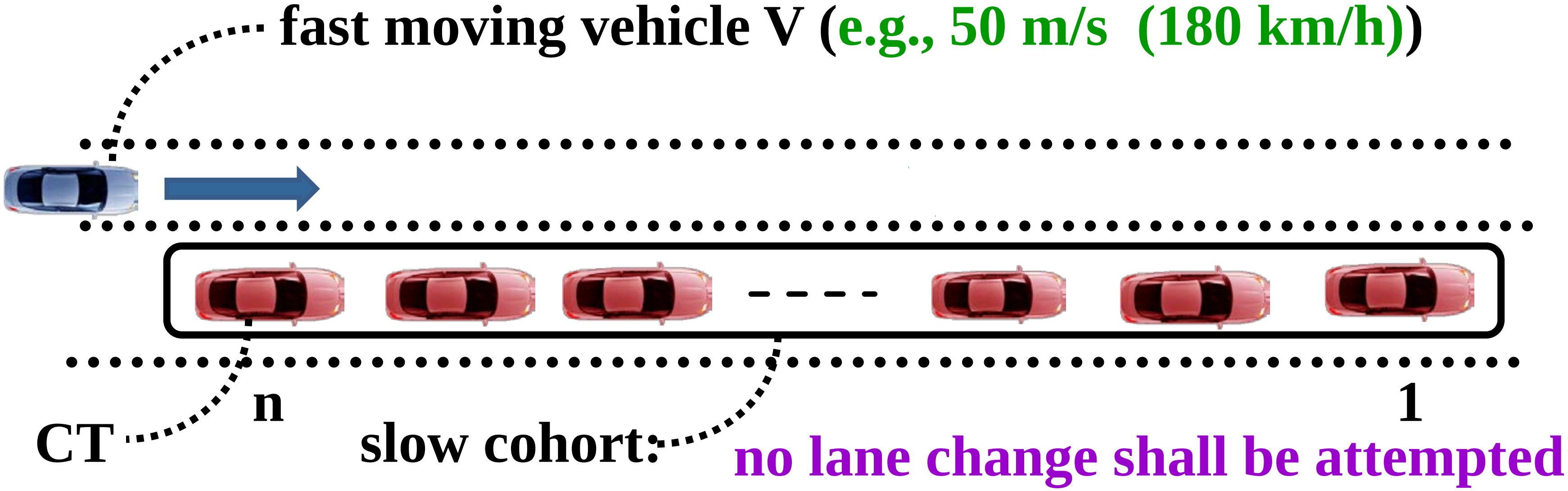


Messages' contents: codes of risk-prone maneuvers, events,…
(no GNSS geodata) // sender ID: pair of integers {r,j}

7,2	0065

Eavesdropping?
Tracking?

Cohort-Wide Dissemination



fast moving vehicle V (e.g., 50 m/s (180 km/h))

CT

n

1

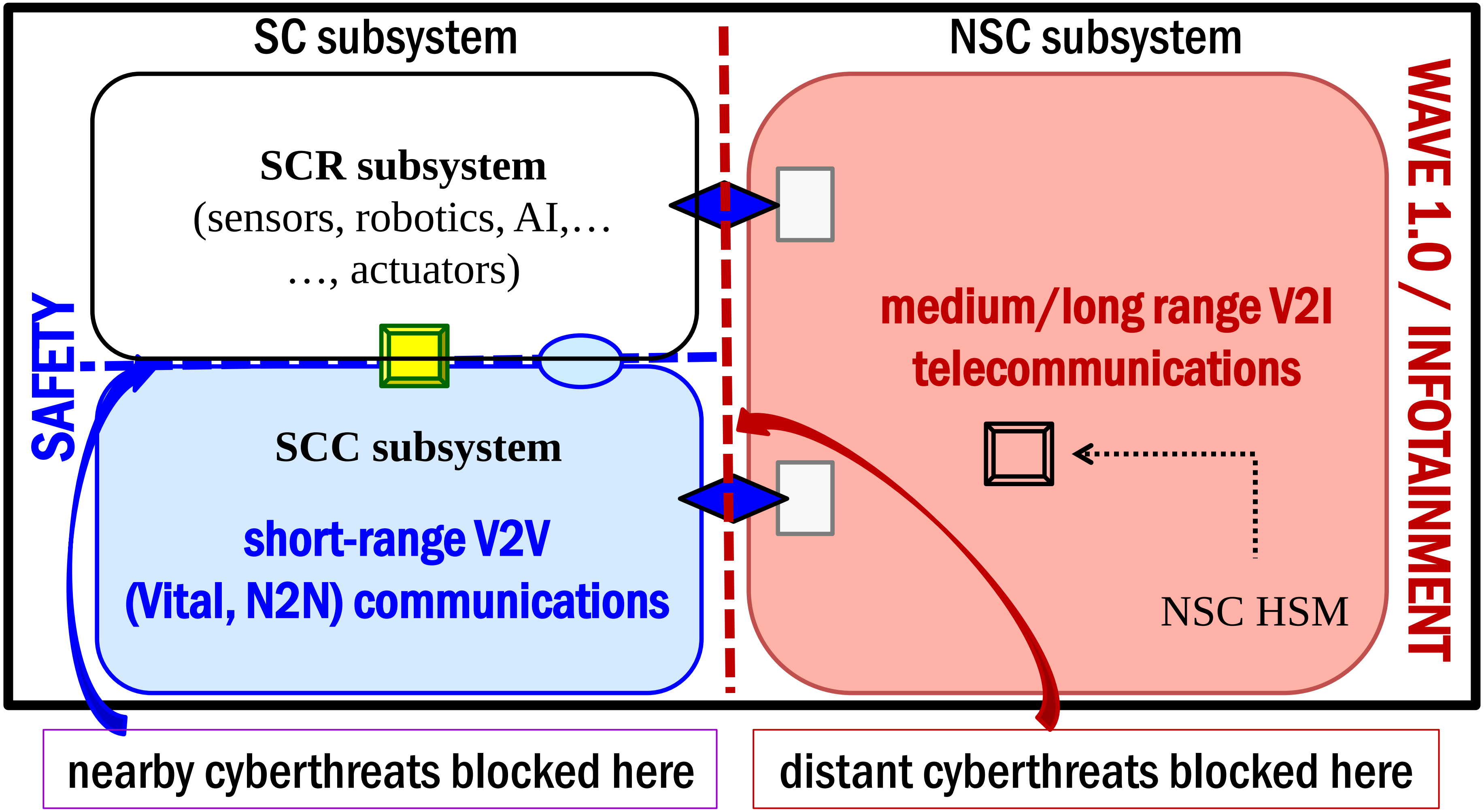
slow cohort: no lane change shall be attempted

- ❖ Robotics alone (vehicle-centric sensing)? No.
- ❖ WAVE 1.0 Bcast? No (unreliable, no timeliness guarantees).
- ❖ **WAVE 2.0? Yes.**

  - CT detects V (robotics or/and lateral com. V to CT)
  - CT initiates dissemination of « **stay in lane** » **N2N message**

$n = 30$ / $\Delta_d(30) = 72$ ms ➔ dist (V) = 3.6 m

WAVE 2.0 Onboard System



SC subsystem

NSC subsystem

SCR subsystem
(sensors, robotics, AI,…
…, actuators)

SAFETY

SCC subsystem

short-range V2V
(Vital, N2N) communications

medium/long range V2I
telecommunications

NSC HSM

WAVE 1.0 / INFOTAINMENT

nearby cyberthreats blocked here

distant cyberthreats blocked here

○ read/write shared memory

🟨 Proactive Sec Module

□ memory written by the NSC subsystem, read by the SC subsystem

◆ secured bridge

WAVE 2.0 and conformance to legislations (privacy)

- ➢ EU GDPR
- ➢ Latest EU WP29 Resolution

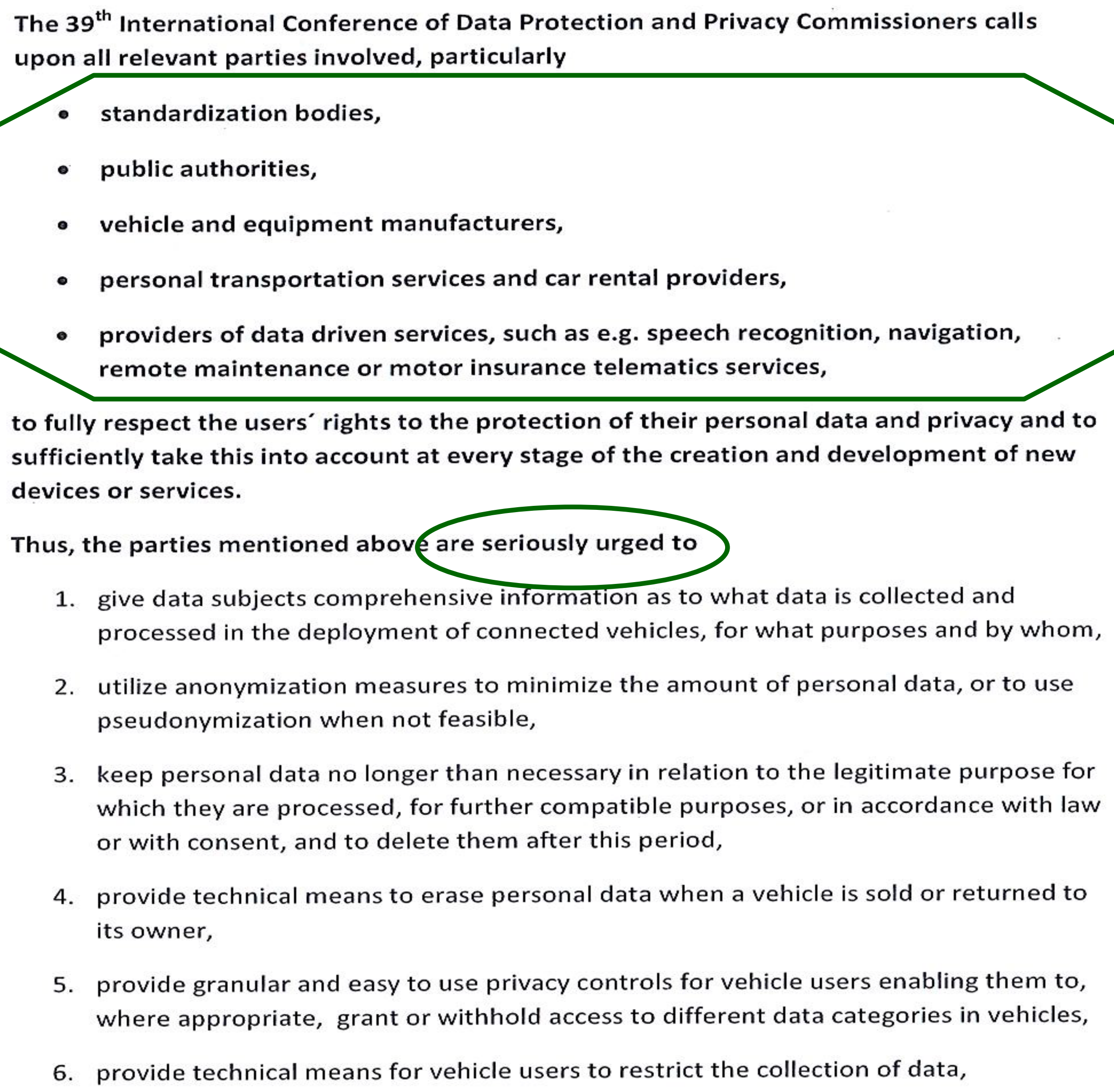
General Data Protection Regulation

❒ Privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

❒ No personal data may be processed unless the data controller or processor has received explicit, opt-in informed consent from the data subject. The data subject has the right to revoke this permission at any time.

❒ …/…

39th International Conference of Data Protection and Privacy Commissioners, Hong Kong, Sept. 2017



The 39th International Conference of Data Protection and Privacy Commissioners calls upon all relevant parties involved, particularly

- standardization bodies,
- public authorities,
- vehicle and equipment manufacturers,
- personal transportation services and car rental providers,
- providers of data driven services, such as e.g. speech recognition, navigation, remote maintenance or motor insurance telematics services,

to fully respect the users´ rights to the protection of their personal data and privacy and to sufficiently take this into account at every stage of the creation and development of new devices or services.

Thus, the parties mentioned above are seriously urged to

1. give data subjects comprehensive information as to what data is collected and processed in the deployment of connected vehicles, for what purposes and by whom,
2. utilize anonymization measures to minimize the amount of personal data, or to use pseudonymization when not feasible,
3. keep personal data no longer than necessary in relation to the legitimate purpose for which they are processed, for further compatible purposes, or in accordance with law or with consent, and to delete them after this period,
4. provide technical means to erase personal data when a vehicle is sold or returned to its owner,
5. provide granular and easy to use privacy controls for vehicle users enabling them to, where appropriate, grant or withhold access to different data categories in vehicles,
6. provide technical means for vehicle users to restrict the collection of data,

Instantiations in CAVs

Mode « cyber-stealth »
(Vital, N2N, F2F coms only, no V2I coms*)

* Handled by NSC subsystems (e.g., eCall, randomized Bcasts (contribution to traffic data), filtered imports by SC subsystems,…)

Mode « no internal cybersurveillance »

Both compatible with anti-theft, accountability/auditability and legitimate cyber-surveillance

Limited modes for public/shared/rental vehicles

Which future motorized society do we want?

WAVE 1.0

Vulnerable to eavesdropping, tracking and cyberattacks.
Fees/billing for V2I coms and PKI.
Safety not (much) better than achieved with OB robotics.

WAVE 2.0

No cyber-espionnage/tracking (options), no remote cyberattacks.
Invulnerability to nearby cyberattacks (irrational, detected).
No charges for N2N coms, for PKI, ≈ 0 for V2I coms.
Highest safety.

Missing crucial technologies (patents, business)

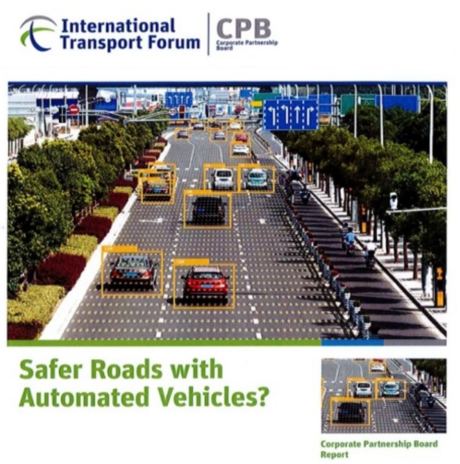
► Security-driven WAVE 2.0 Onboard System Architectures, PSMs

► 5G directional/MIMO short-range power-controlled N2N radio communications (high velocities)

► MAC protocols

- ► Collision-free TDMA % ranking in cohorts (pub. 2016)
- ► Deterministic CDMA
- ► CSMA & deterministic collision resolution

► Optical N2N (passive) communications



International Transport Forum | CPB Corporate Partnership Board

Safer Roads with Automated Vehicles?

Corporate Partnership Board Report

https://www.itf-oecd.org/sites/default/files/docs/safer-roads-automated-vehicles.pdf

OECD