SEVECOM

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Securing Vehicular Networks

Maxim Raya

Joint work with Jean-Pierre Hubaux et al.

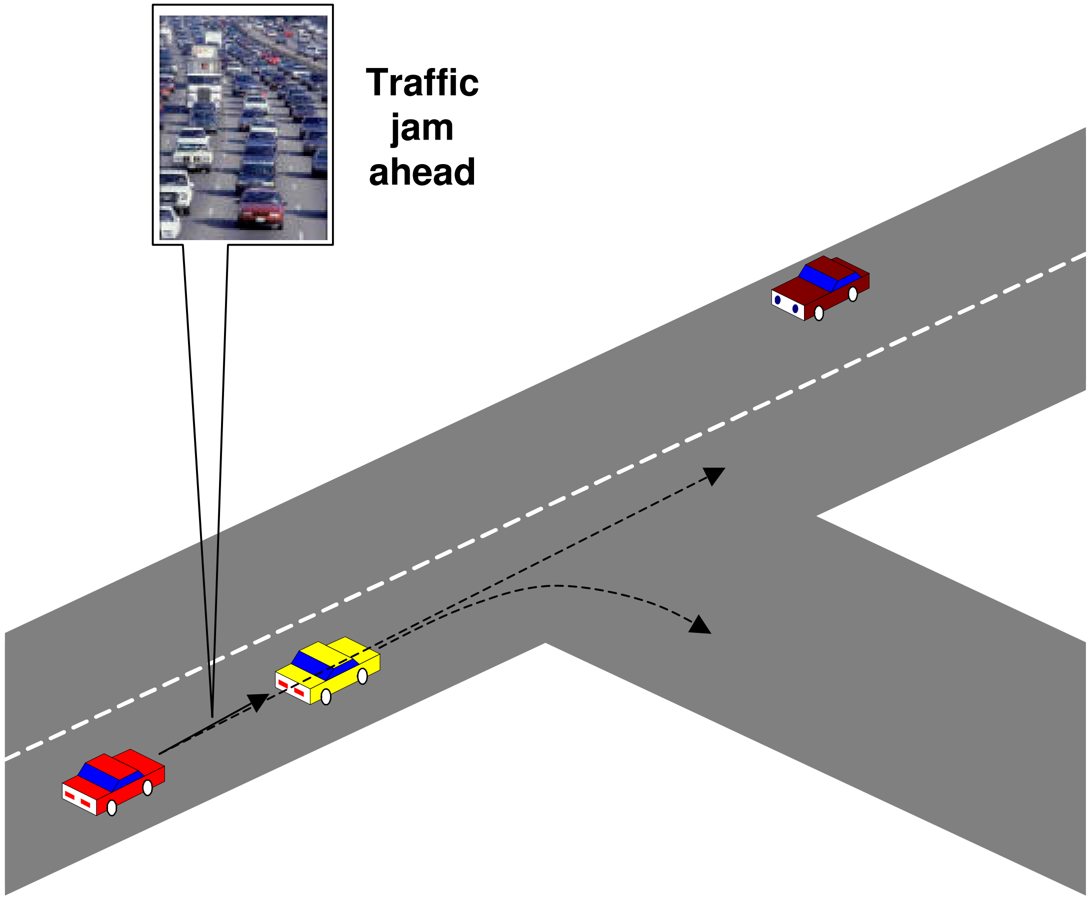
Laboratory for computer Communications and Applications (LCA)

Mobilis 2006

Why is VANET security important?

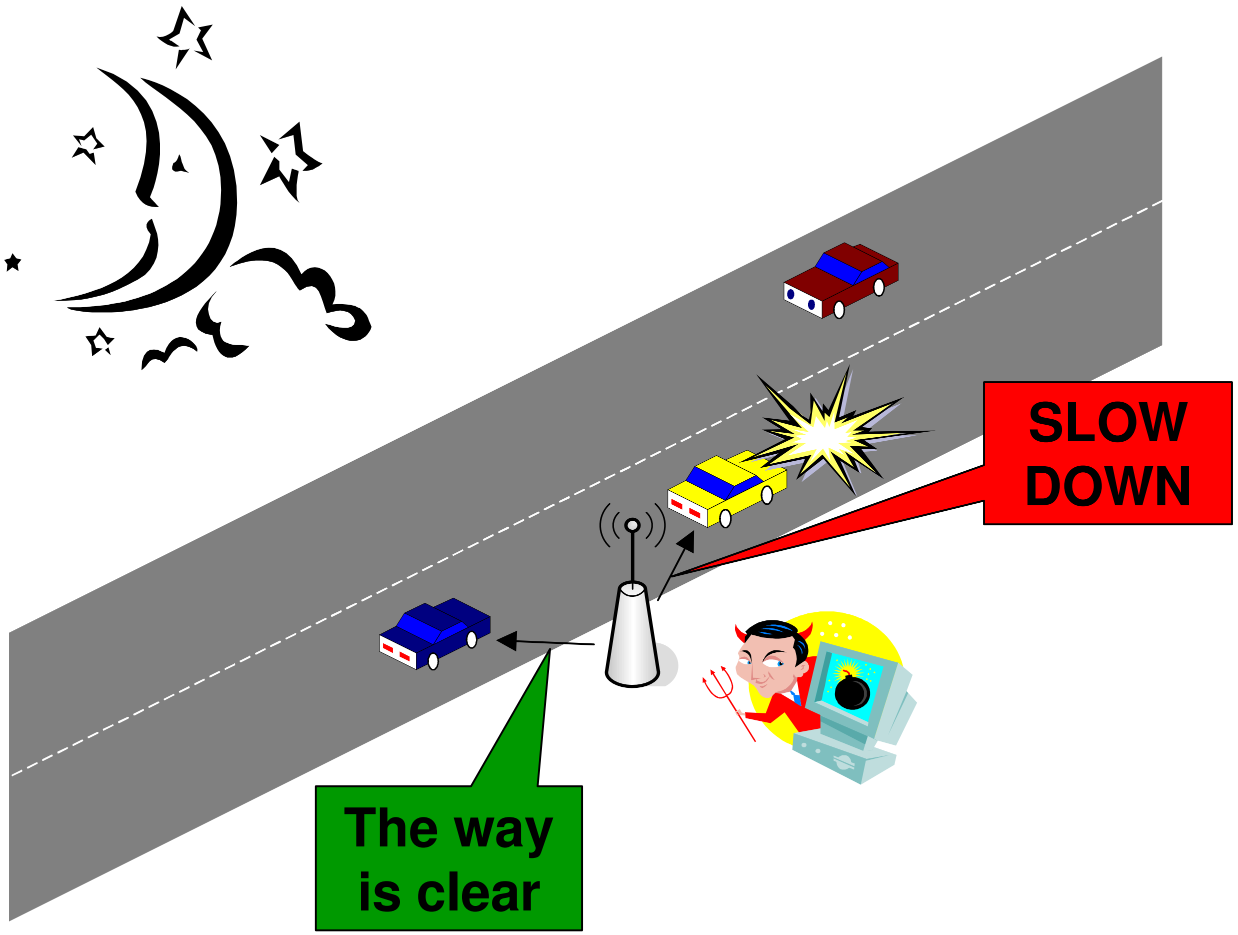
- Large projects have explored vehicular communications: Fleetnet, PATH (UC Berkeley),…
- No solution can be deployed if not properly secured
- The problem is non-trivial
  - Specific requirements (speed, real-time constraints)
  - Contradictory expectations

Attack 1 : Bogus traffic information



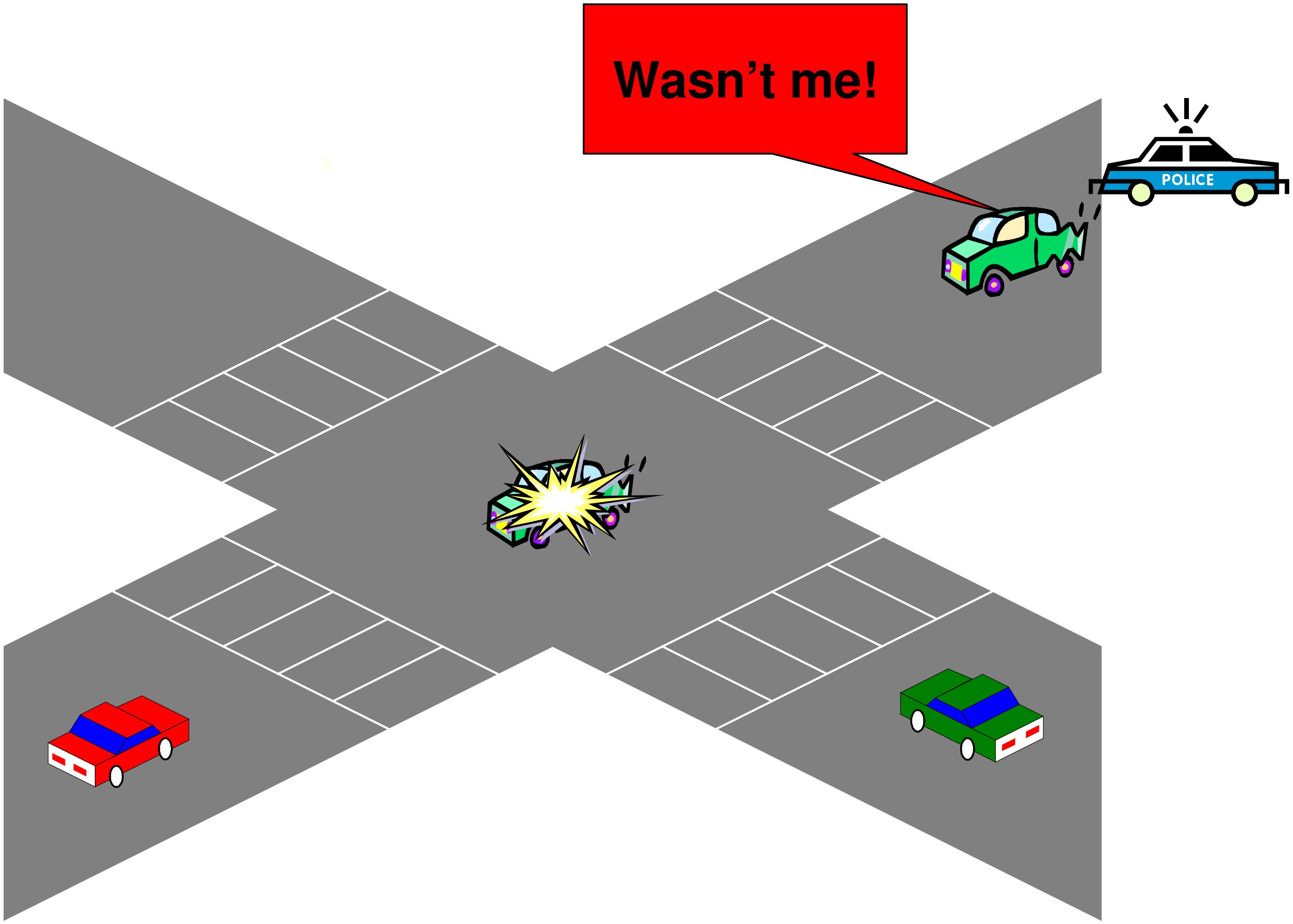
- Attacker: insider, rational, active

Attack 2 : Disruption of network operation



- Attacker: insider, malicious, active

Attack 3: Cheating with identity, speed, or position



- Attacker: insider, rational, active

C2C vs. C2I

- C2C
  - + Immediate response
  - + Faster and easier to deploy
  - + Cheaper
  - + Simpler

  - - Less reliable
  - - Less liable
  - - Local information

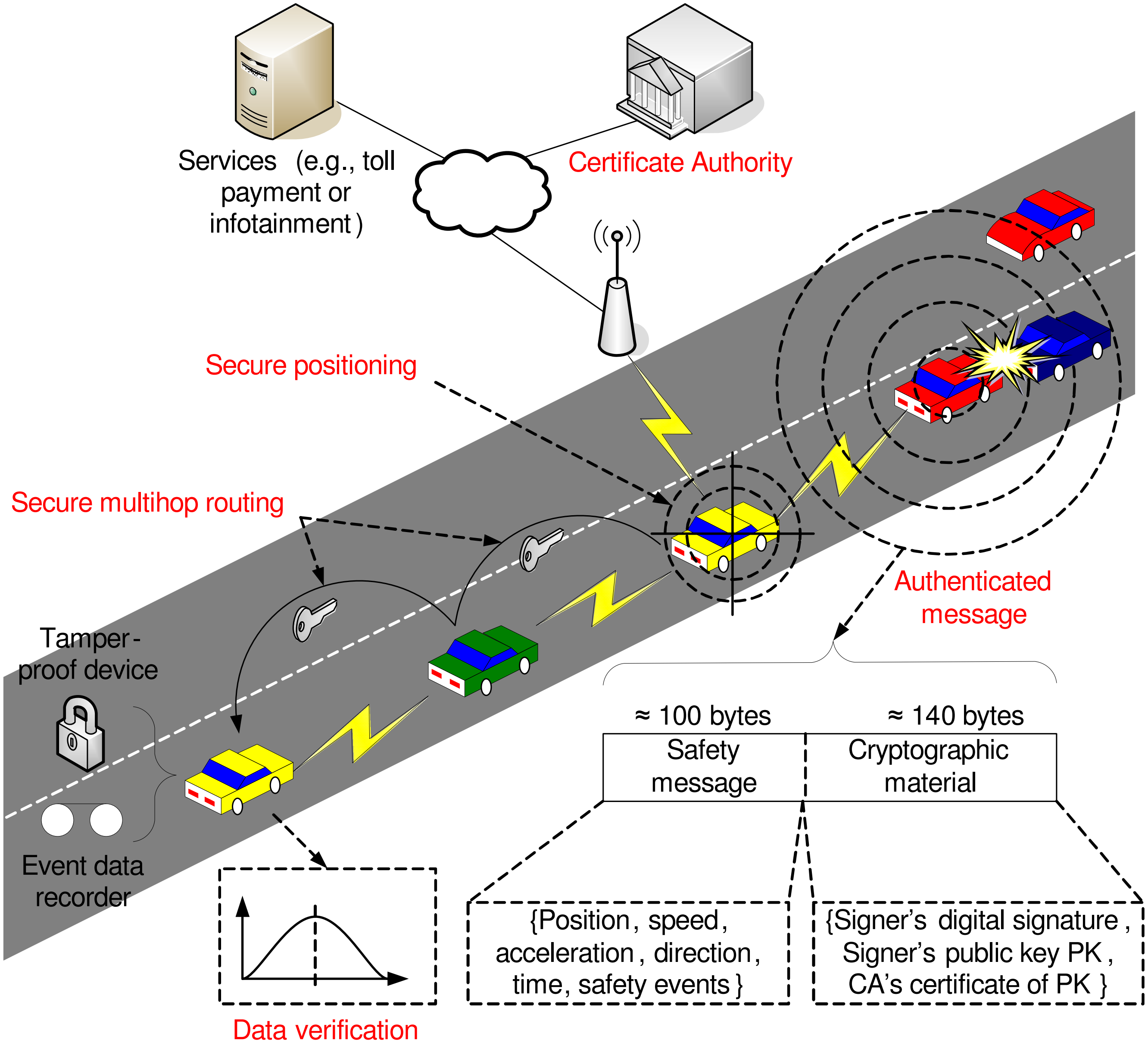
- C2I
  - - Need to contact an authority
  - - Deployment will be gradual
  - - More expensive
  - - Complex management

  - + Authority is trustworthy
  - + Misbehavior can be punished
  - + Global view

Hybrid approach:

VANETs will start in C2C mode then gradually switch to C2I

Security Architecture



Services (e.g., toll payment or infotainment)

Certificate Authority

Secure positioning

Secure multihop routing

Tamper-proof device

Event data recorder

Authenticated message

≈ 100 bytes

Safety message

≈ 140 bytes

Cryptographic material

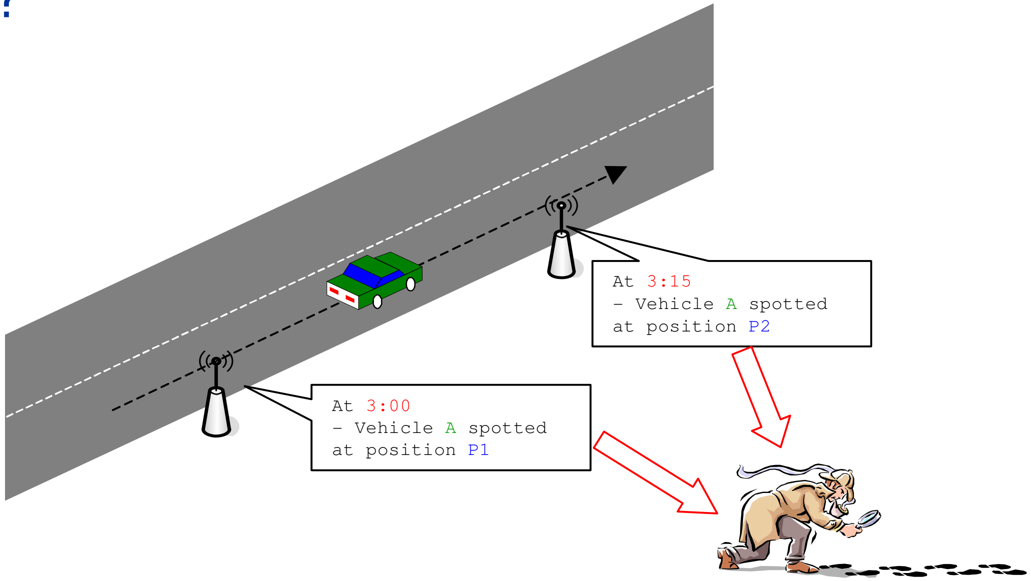
{Position, speed, acceleration, direction, time, safety events}

{Signer's digital signature, Signer's public key PK, CA's certificate of PK}

Data verification

Questions

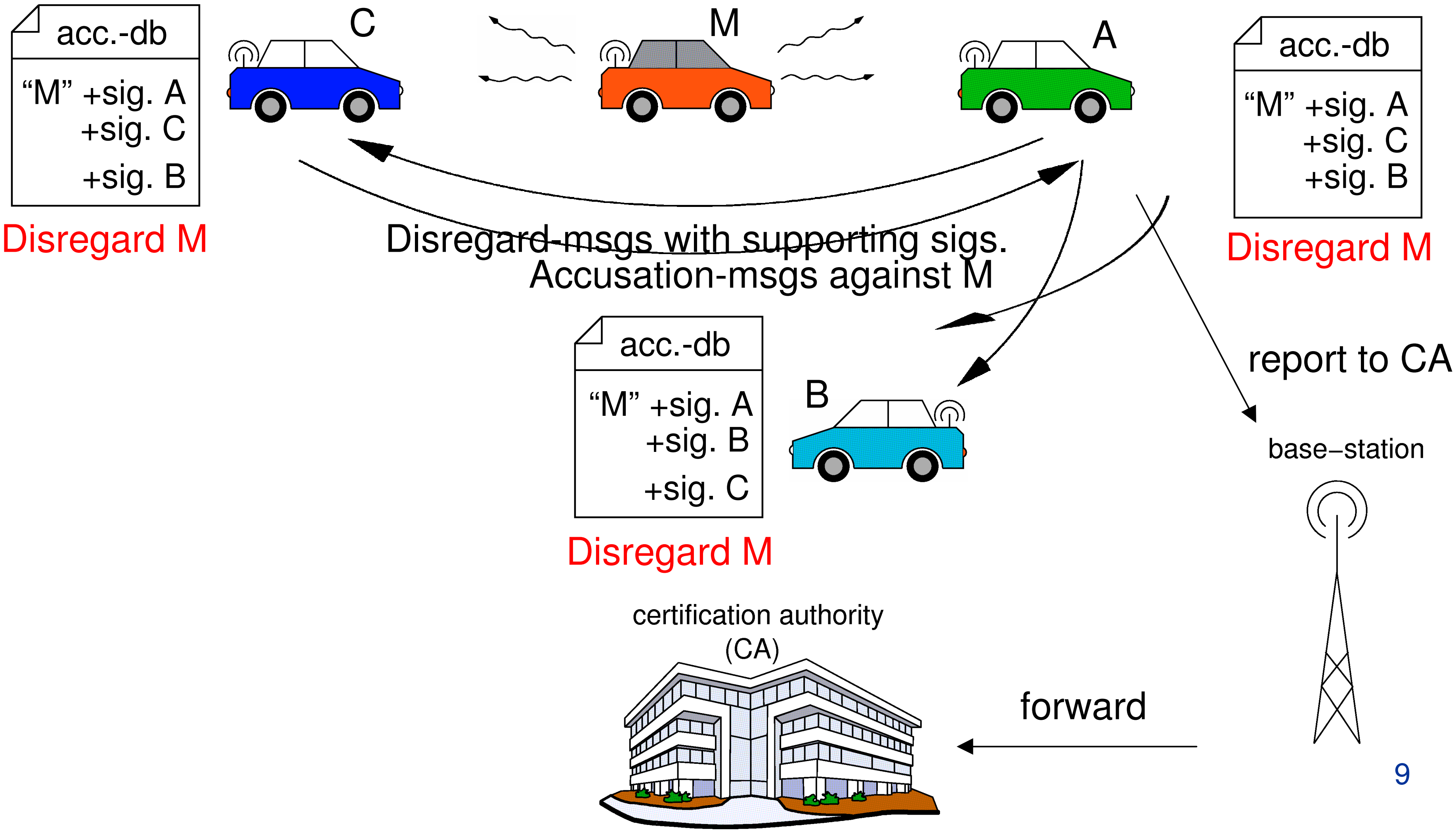
- What applications will be there and who will develop them?
- Certification Authorities: who will manage them and how to make them compatible?
- Costs: who will pay and how much?
- How to verify data correctness, especially position?
- Privacy: how to avoid the Big Brother syndrome and still catch attackers?



At 3:15
- Vehicle A spotted
at position P2

At 3:00
- Vehicle A spotted
at position P1

Certificate Revocation in C2C mode: Distributed Revocation Protocol (DRP)



acc.-db

“M” +sig. A
+sig. C
+sig. B

Disregard M

C

M

A

acc.-db

“M” +sig. A
+sig. C
+sig. B

Disregard M

Disregard-msgs with supporting sigs.

Accusation-msgs against M

acc.-db

“M” +sig. A
+sig. B
+sig. C

Disregard M

B

report to CA

base−station

certification authority
(CA)

forward

Efficient secure aggregation[1]

- VANET security is indispensable but expensive
- De facto security: limited flooding of signed messages

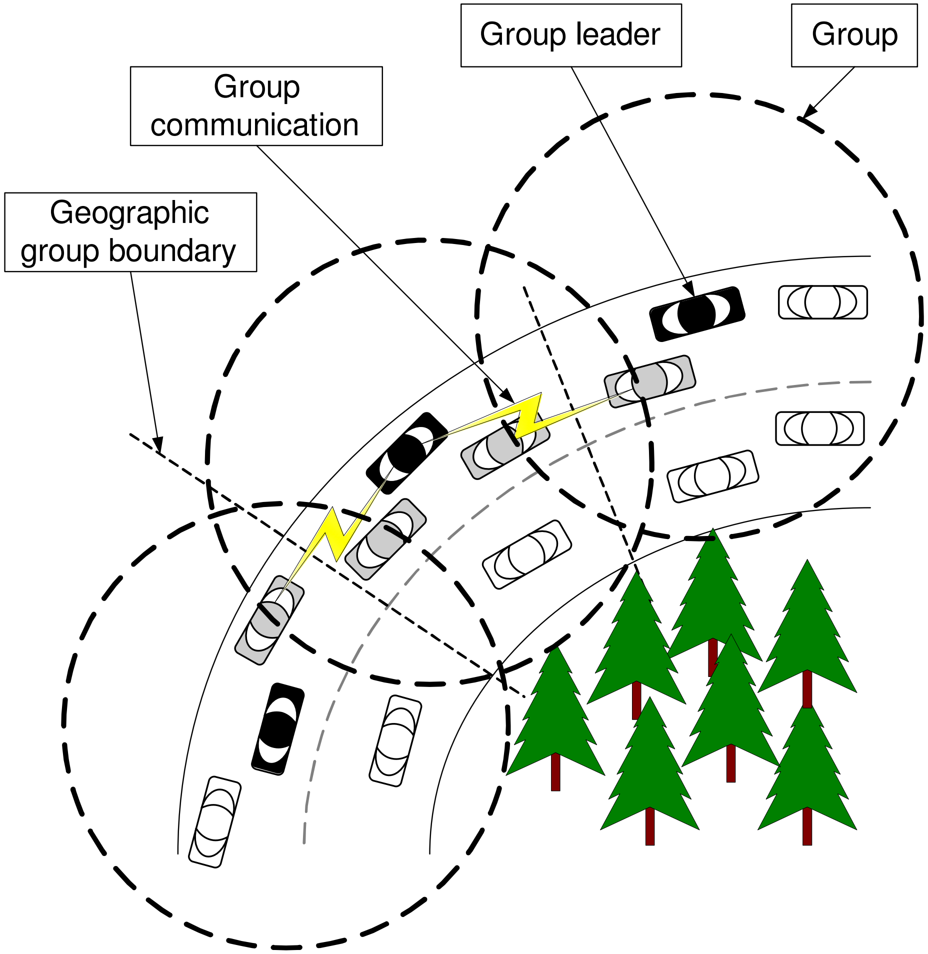
- Since many vehicles broadcast the same event, why not try **aggregation**?

- Can we make it work in VANETs?
- And can we make it **secure**?

- The answer is YES

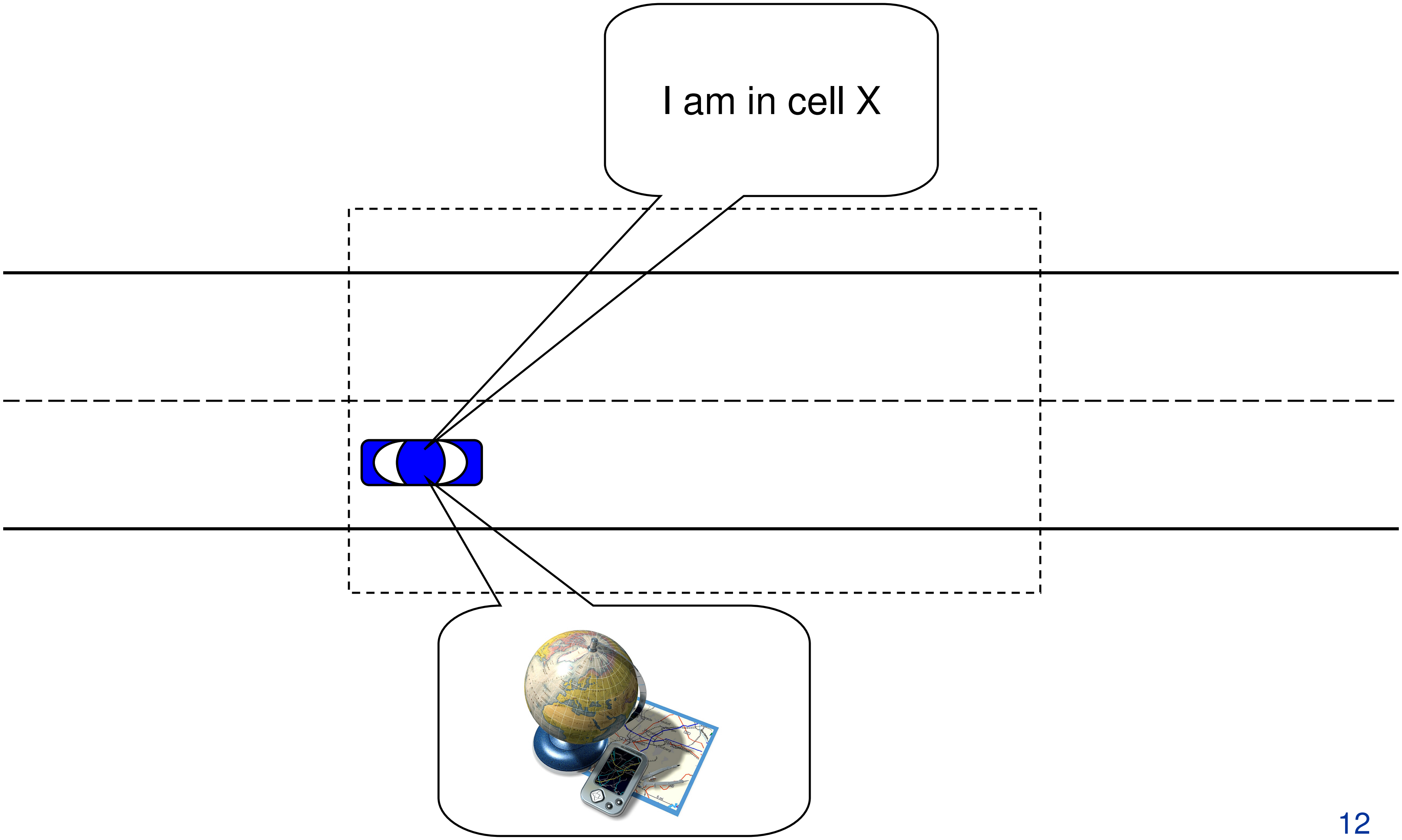
[1] In collaboration with Adel Aziz

The secret of efficient aggregation: groups



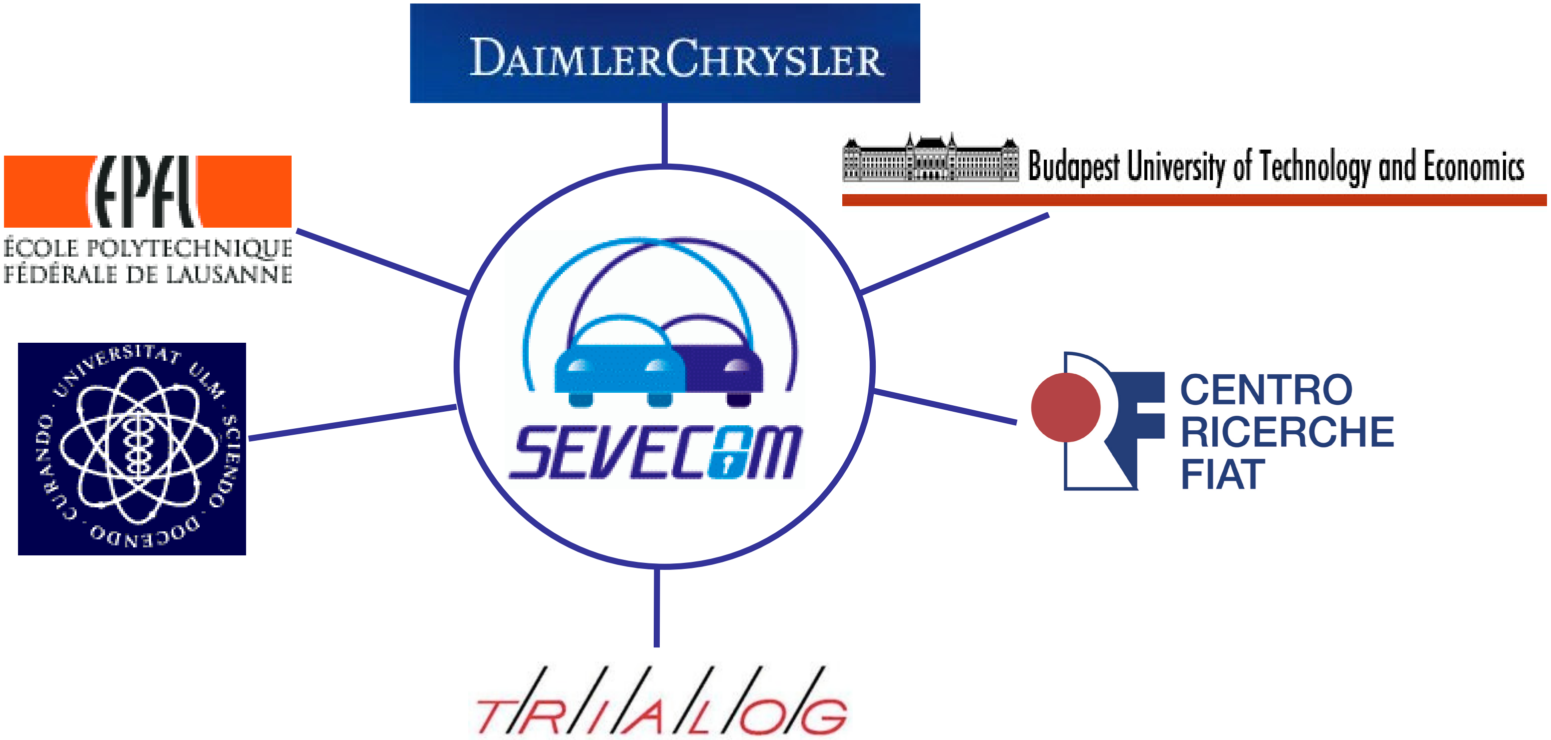
Information is relayed between groups, not individual vehicles

Group formation



SEVECOM
(**SE**cure **VE**hicular **COM**munication)

Objectives: Identification of threats and Specification of a security architecture


DAIMLERCHRYSLER
Budapest University of Technology and Economics
EPFL
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
SEVECOM
UNIVERSITAT ULM · SCIENDO · DOCENDO · CURANDO ·
CENTRO RICERCHE FIAT
TRIALOG

Safety

Information Society and Media

Conclusion

- VANET security is crucial
- Pitfalls
  - Deferment of the security design
  - Security by obscurity
- The presence of an infrastructure is important
- Tradeoffs: privacy vs. liability, security vs. efficiency
- Research is in its beginning, many open problems
- Visit http://ivc.epfl.ch and http://www.sevecom.org