Key Management for Vehicular Networks

Maxim Raya and Jean-Pierre Hubaux

Secure Vehicular Communications Workshop

EPFL - 9/11/2006

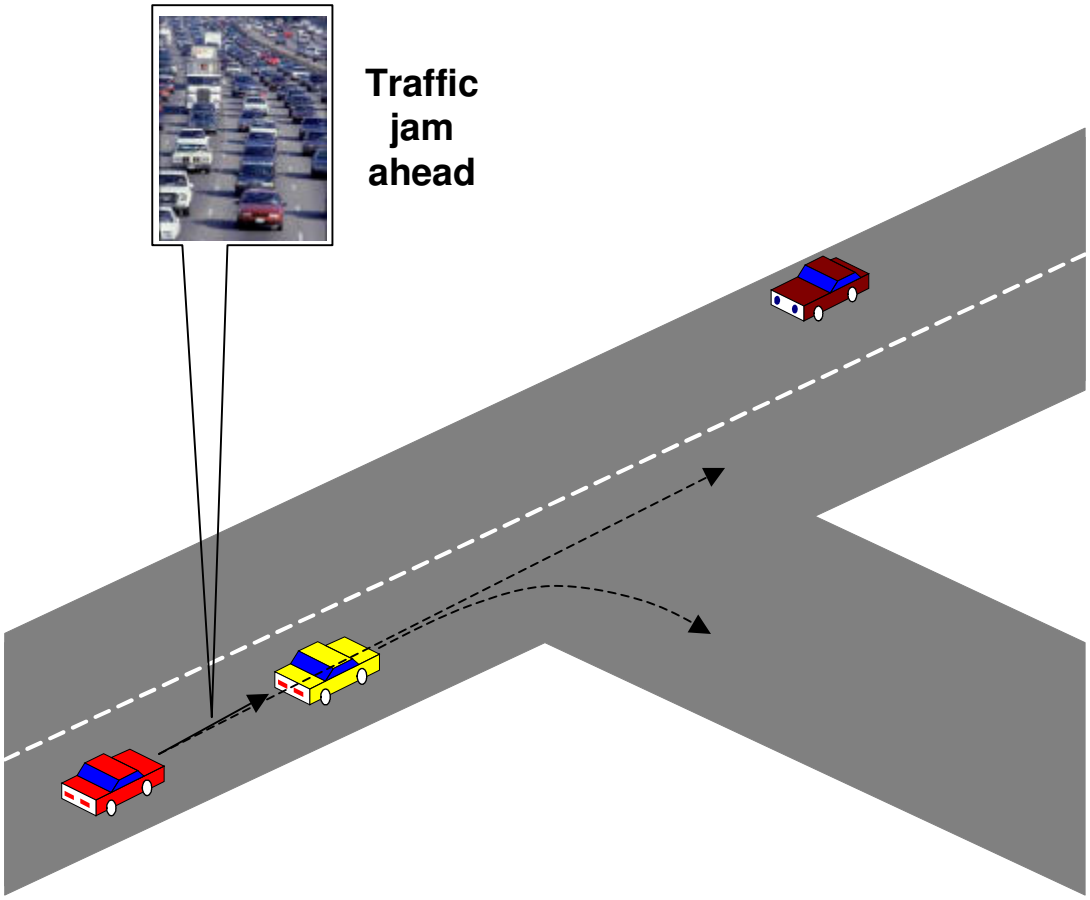
Outline

- Threat model and specific attacks
- Security architecture
- Certificate revocation

Threat model

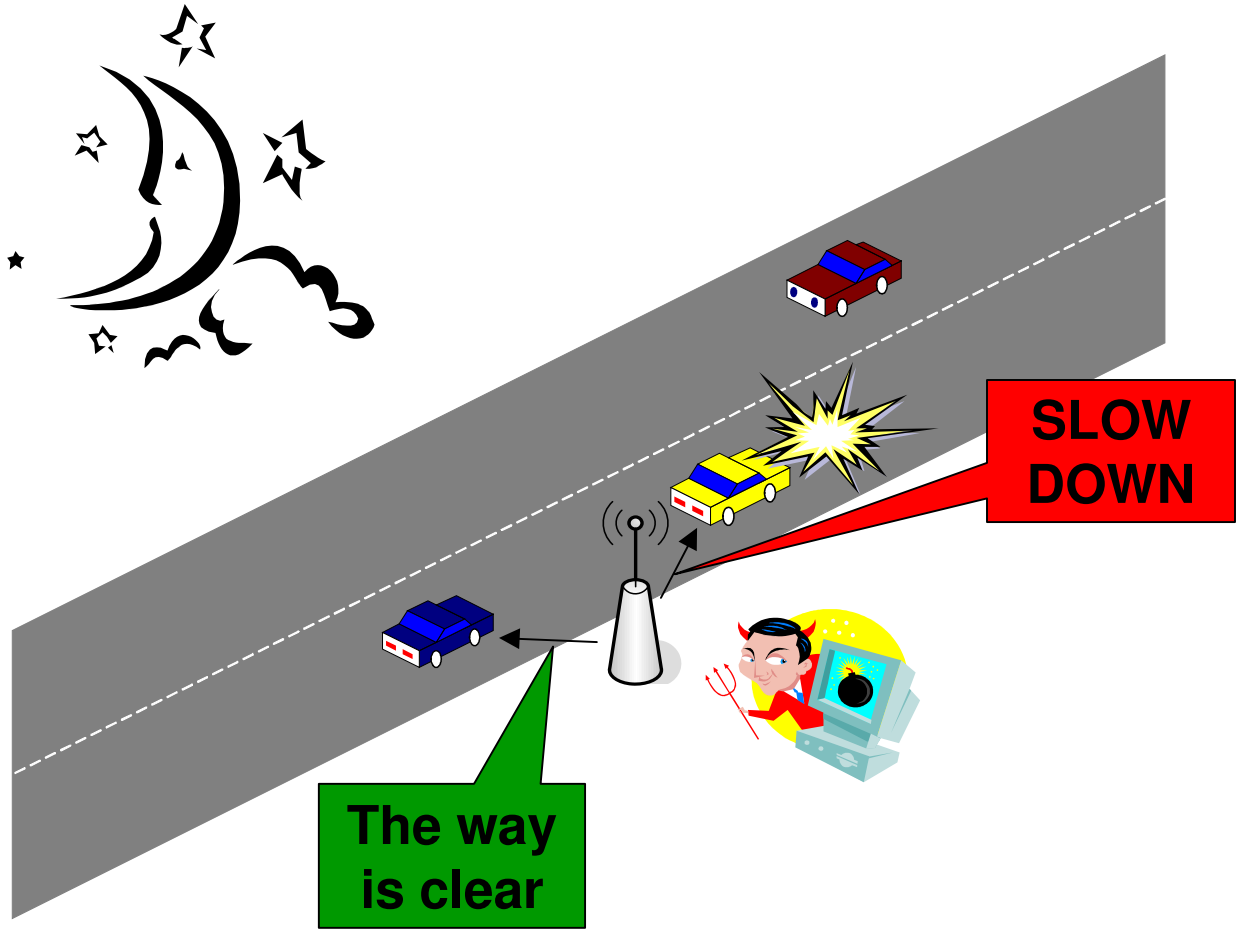
- An attacker can be:
  - Insider / Outsider
  - Malicious / Rational
  - Active / Passive
- Attackers can collude
- The majority of vehicles are honest
- Authorities cannot be compromised

Attack 1 : Bogus traffic information



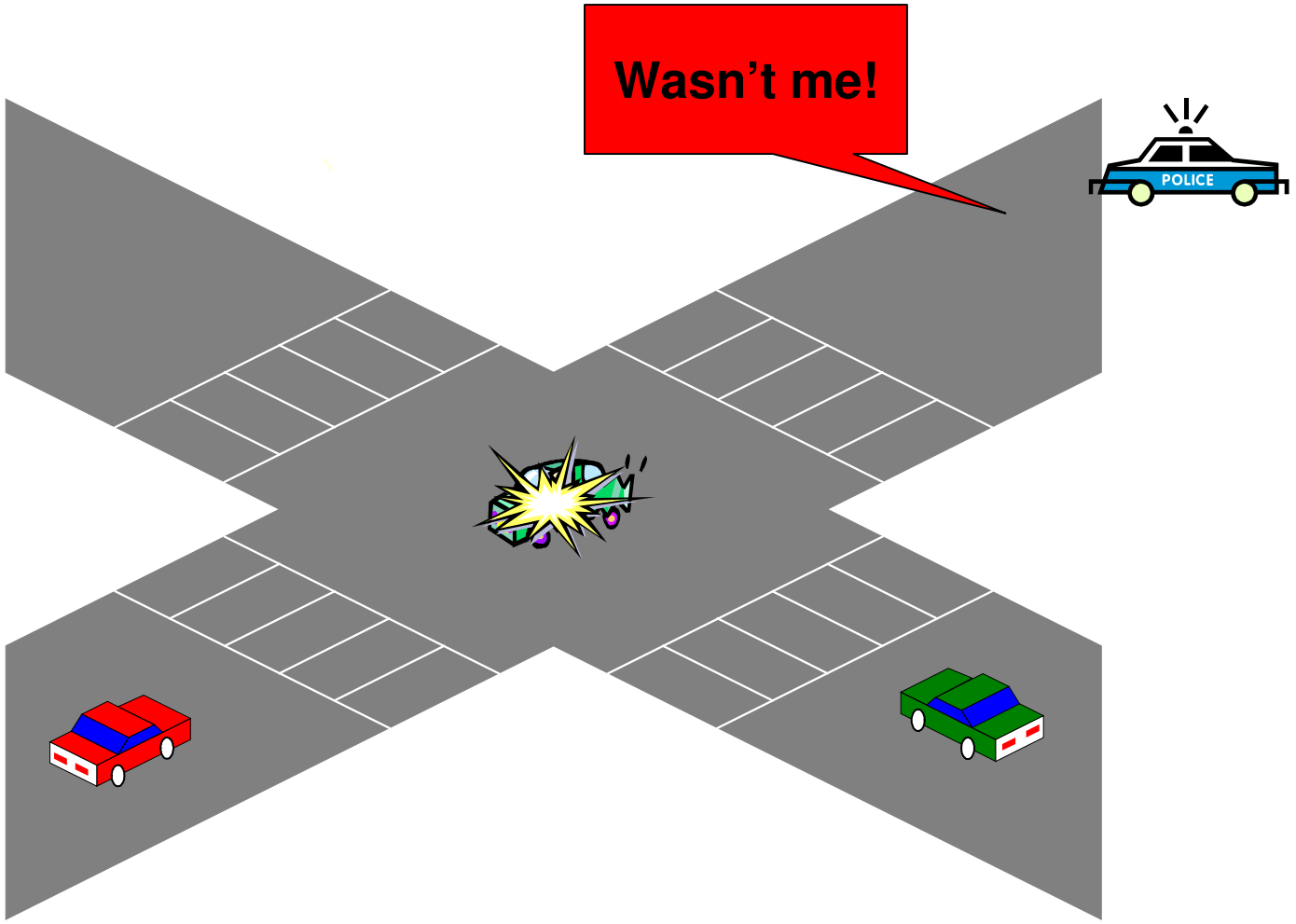
- Attacker: insider, rational, active

Attack 2 : Disruption of network operation



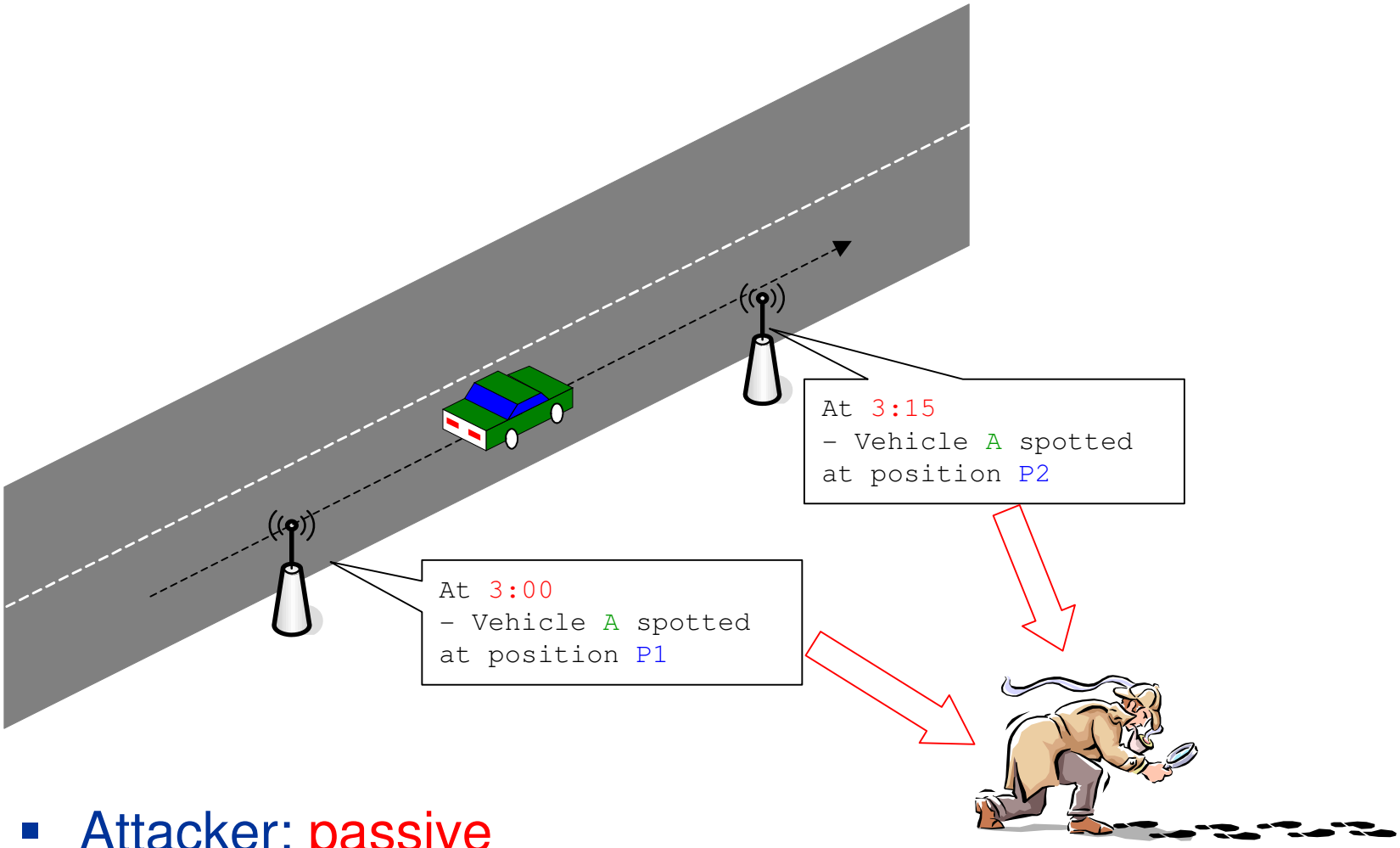
- Attacker: insider, malicious, active

Attack 3: Cheating with identity, speed, or position



- Attacker: insider, rational, active

Attack 4 : Tracking

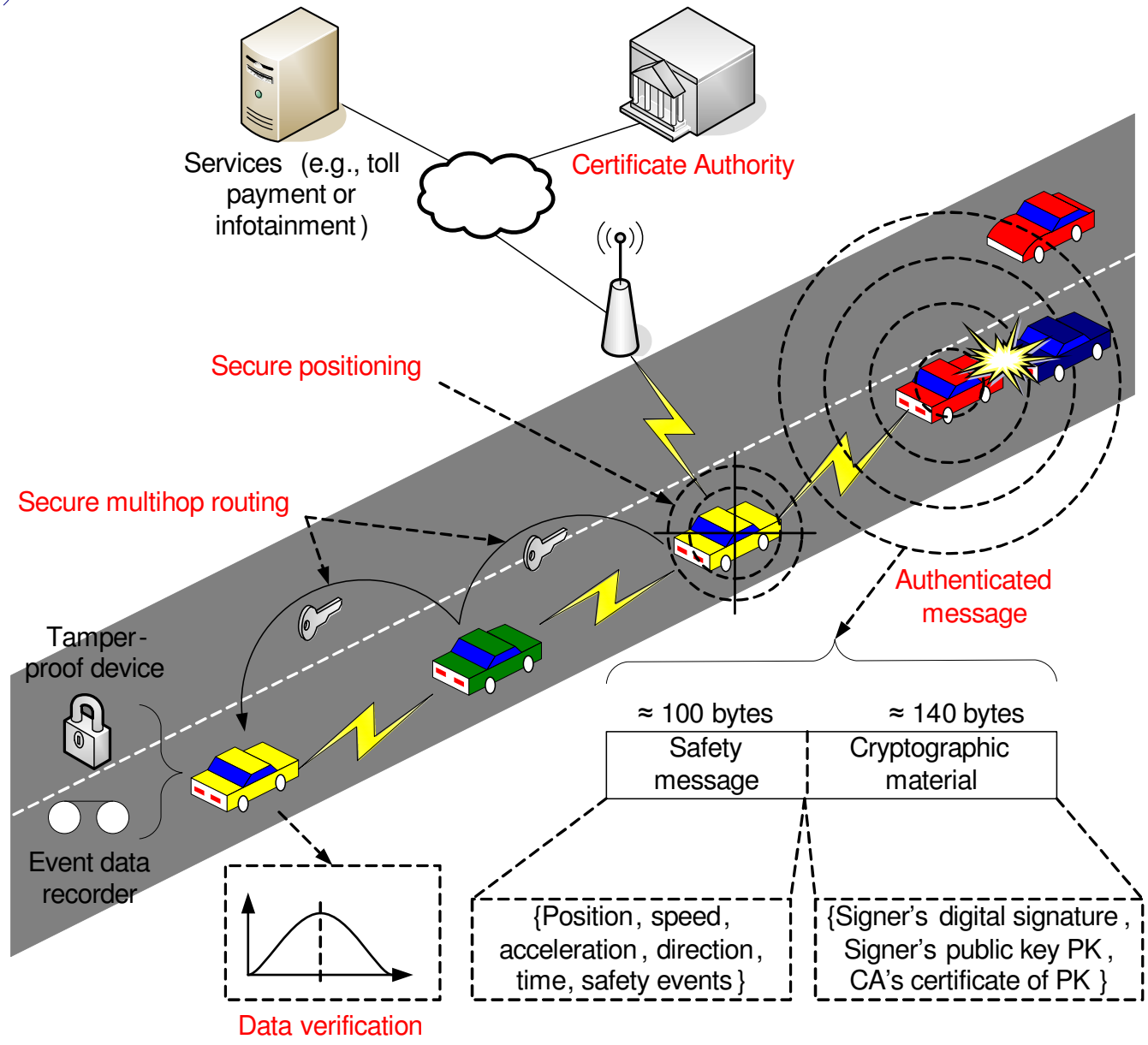


- Attacker: passive
- Big Brother syndrome!

Security system requirements

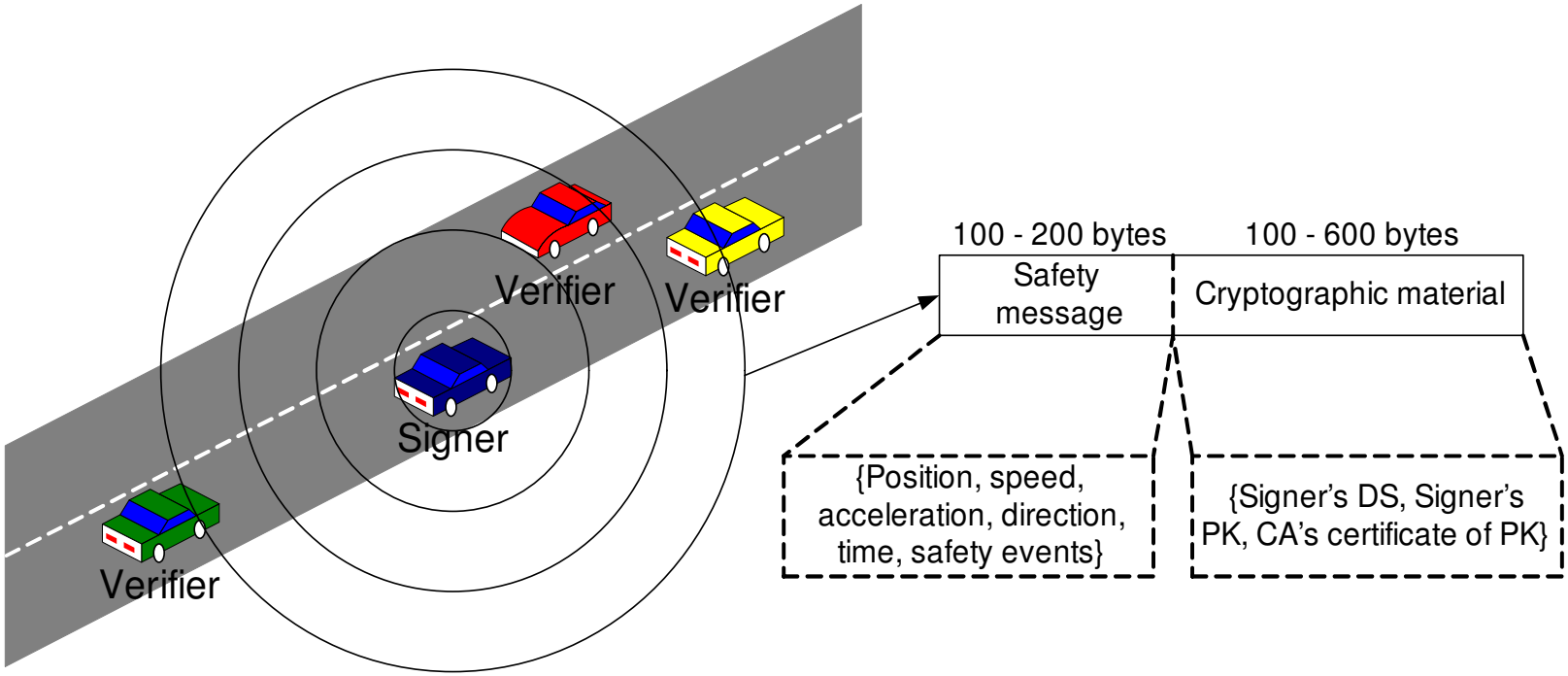
- Sender authentication
- Verification of data consistency
- Availability
- Non-repudiation
- Privacy
- Real-time constraints

Security Architecture

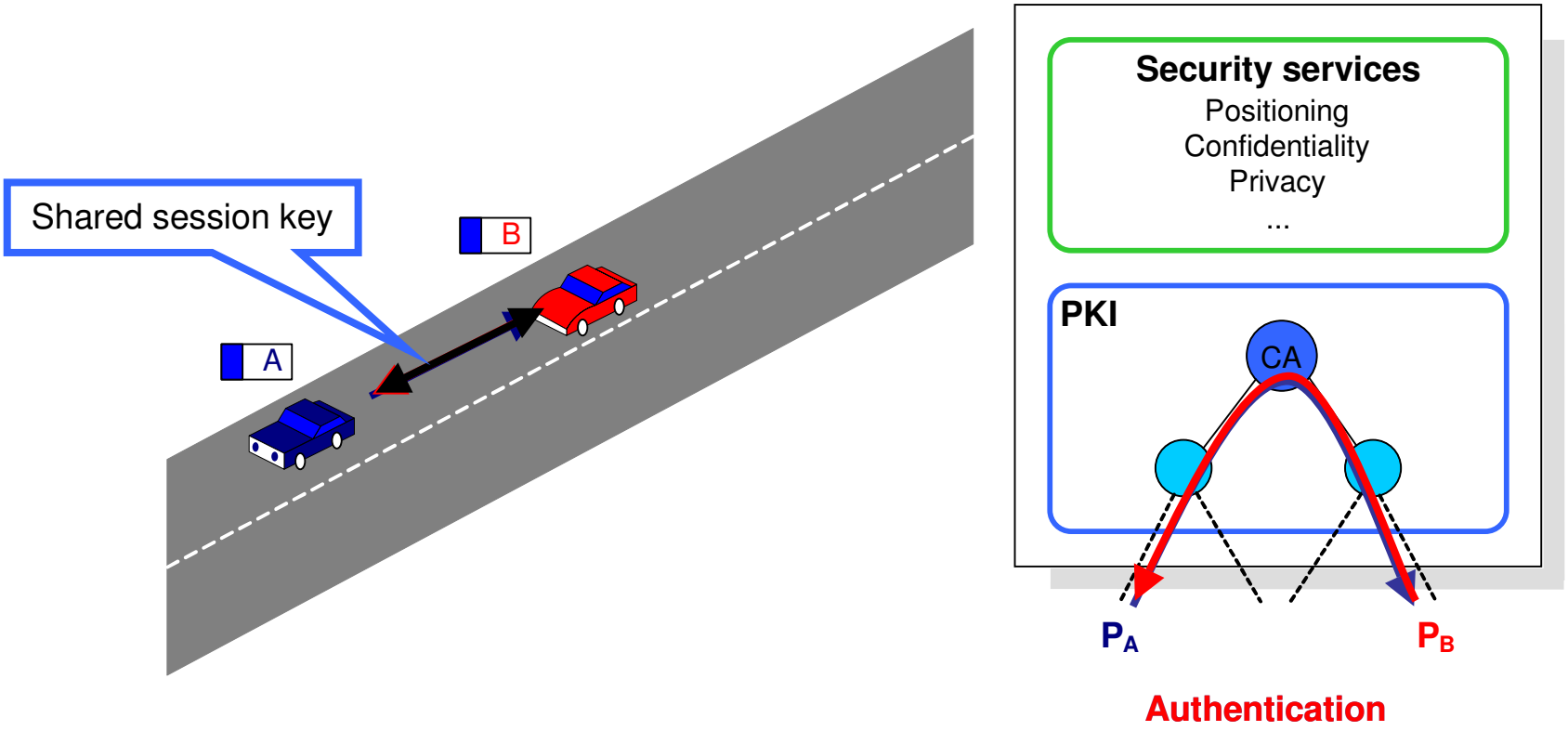


Digital signatures

- Symmetric cryptography is not suitable: messages are standalone, large scale, non-repudiation requirement
- Hence each message should be signed with a DS
- Liability-related messages should be stored in the EDR



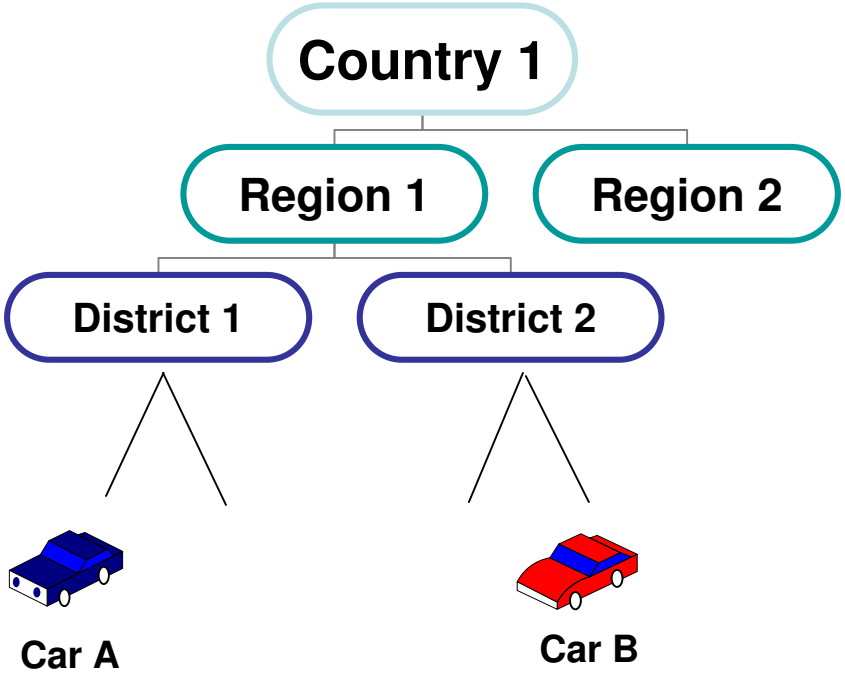
VPKI (Vehicular PKI)



- Each vehicle carries in its **T**amper-**P**roof **D**evice (**TPD**):
  - A unique and certified identity (Electronic License Plate)
  - A set of certified anonymous public/private key pairs
- Mutual authentication can be done without involving a server
- Authorities (national or regional) are cross-certified

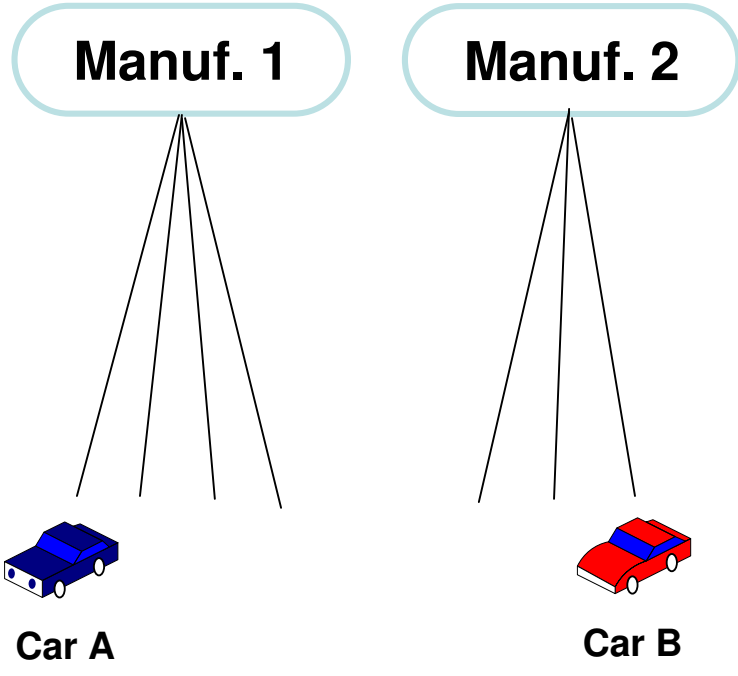
The CA hierarchy: two options

1. Governmental Transportation Authorities



- The governments control certification
- Long certificate chain
- Keys should be recertified on borders to ensure mutual certification

2. Manufacturers



- Vehicle manufacturers are trusted
- Only one certificate is needed
- Each car has to store the keys of all vehicle manufacturers

Anonymous keys

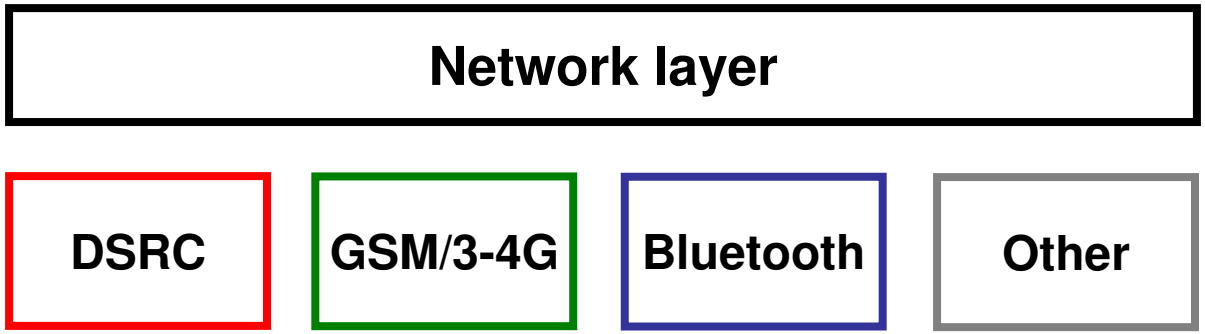
- Preserve identity and location privacy
- Keys can be preloaded at periodic checkups
- The certificate of *V*'s i^{th} key:

$$Cert_V[PuK_i] = PuK_i \mid Sig_{SK_{CA}}[PuK_i \mid ID_{CA}]$$

- Keys renewal algorithm according to vehicle speed (e.g., ˜ 1 min at 100 km/h)
- Anonymity is conditional on the scenario
- The authorization to link keys with ELPs is distributed

DoS resilience

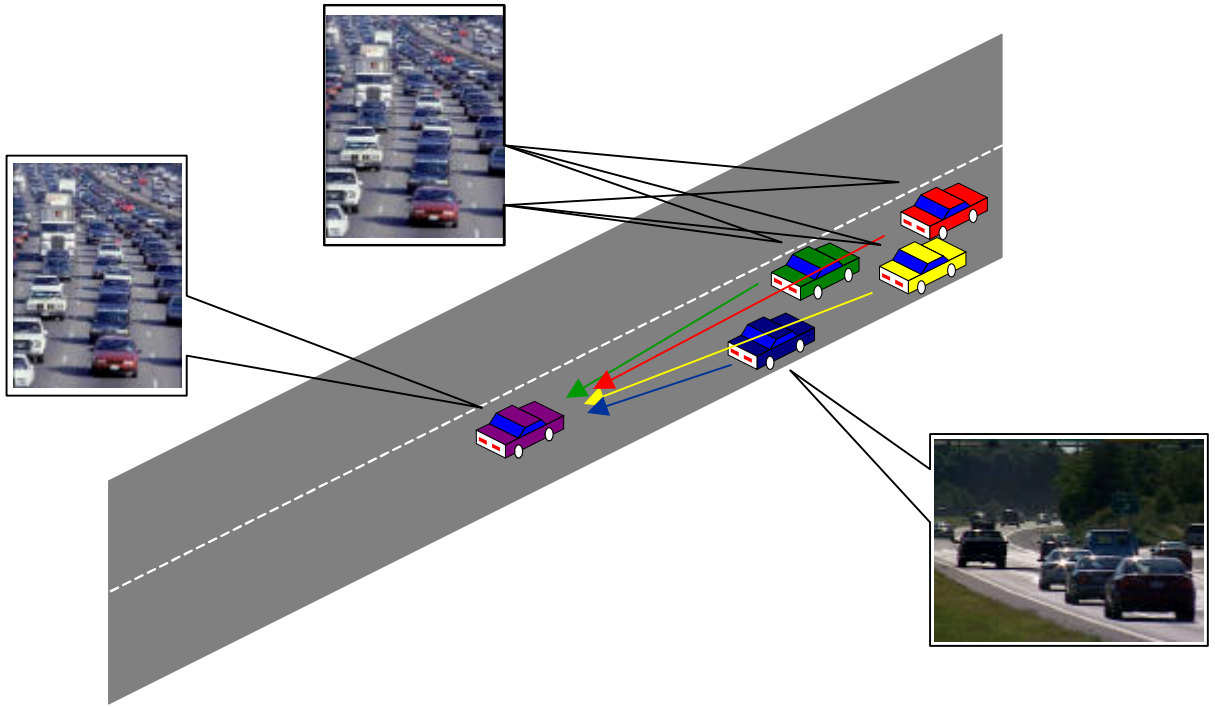
- Vehicles will probably have several wireless technologies onboard
- In most of them, several channels can be used
- To thwart DoS, vehicles can switch channels or communication technologies



- In the worst case, the system can be deactivated

Data verification by correlation

- Bogus info attack relies on false data
- Authenticated vehicles can also send wrong data (on purpose or not)
- The correctness of the data should be verified
- Correlation can help



Security analysis

- How much can we secure VANETs?
- Messages are authenticated by their signatures
- Authentication protects the network from outsiders
- Correlation and fast revocation reinforce correctness
- Availability remains a problem that can be alleviated
- Non-repudiation is achieved because:
  - ELP and anonymous keys are specific to one vehicle
  - Position is correct if secure positioning is in place
- *Formal security analysis* envisioned within the MICS **VerSePro** project (in collaboration with ETHZ)

What PK cryptosystem to use?

- Available options:
  - RSA Sign: the most popular but also has the largest key size
  - ECDSA: the most compact
  - NTRUSign: the fastest in signing and verification
  - Other (XTR, HEC, Braid groups, Merkle trees, …)
- Signature verification speed matters the most
- Further improvements that can help:
  - Vehicles verify only relevant content
  - Several messages may be signed with the same key

Performance comparison

- Key and signature size

PKCS	Key, Sig size (bytes)	T_{tx}(Sig) (ms)
RSA	256	0.171
ECDSA	28, 56	0.019, 0.038
NTRU	197	0.131

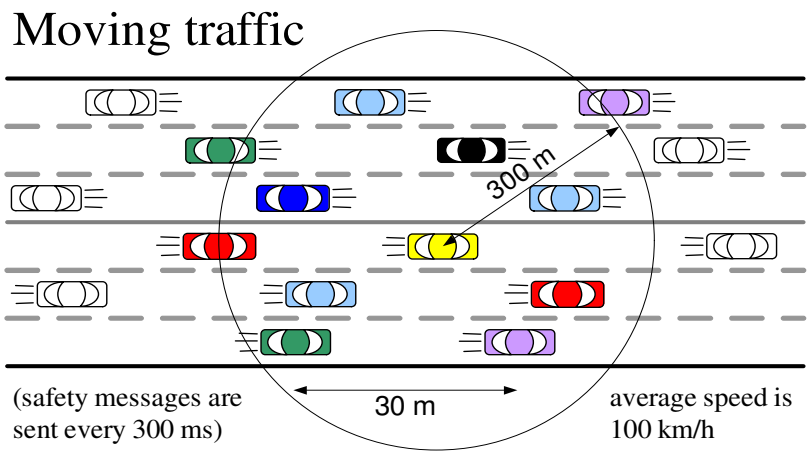
- Signature generation and verification

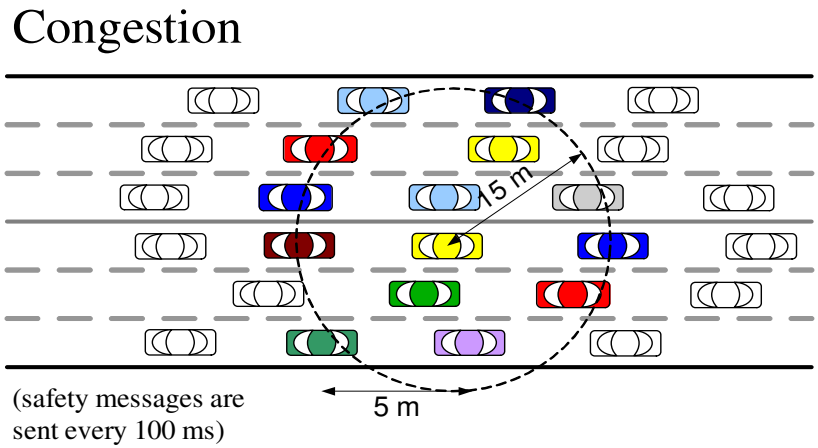
PKCS	Generation (ms)	Verification (ms)
ECDSA	3.255	7.617
NTRU	1.587	1.488

Memory-constrained Pentium II 400 MHz workstation

Performance evaluation

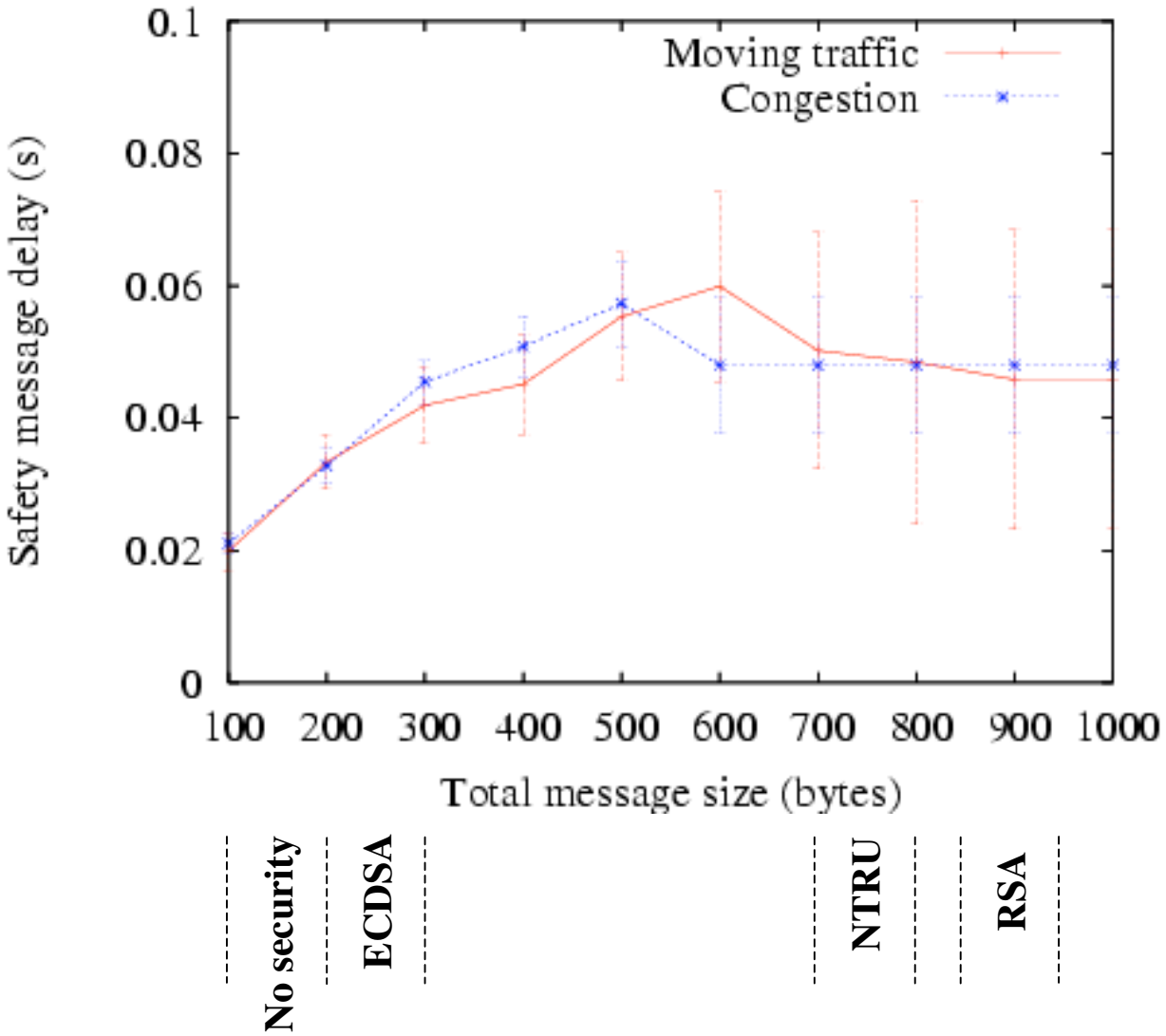
- ns-2 simulations
- Two scenarios drawn from DSRC
- The effect of message size (including the security material) on delay, number of received packets, and throughput is evaluated



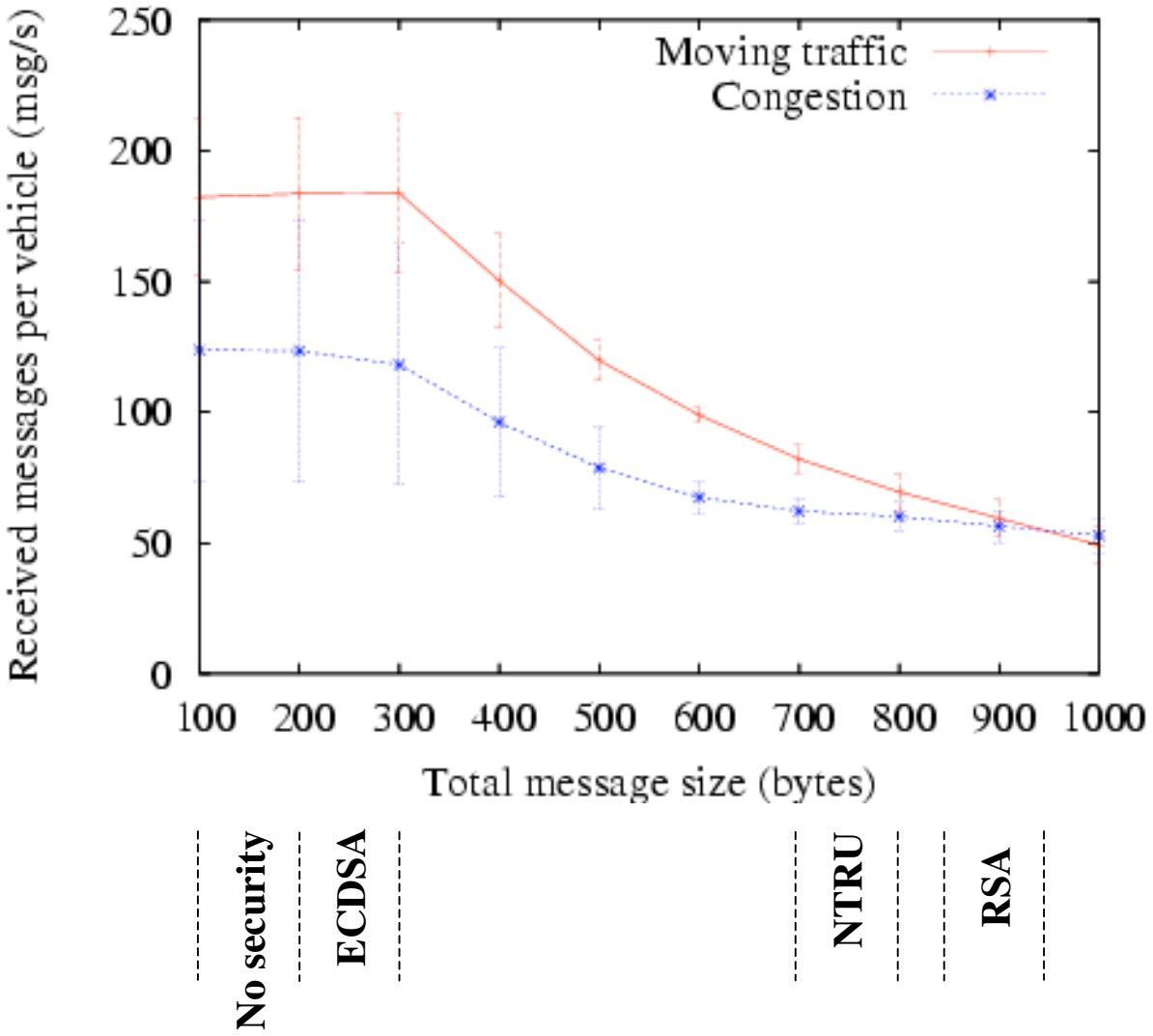


Not to scale

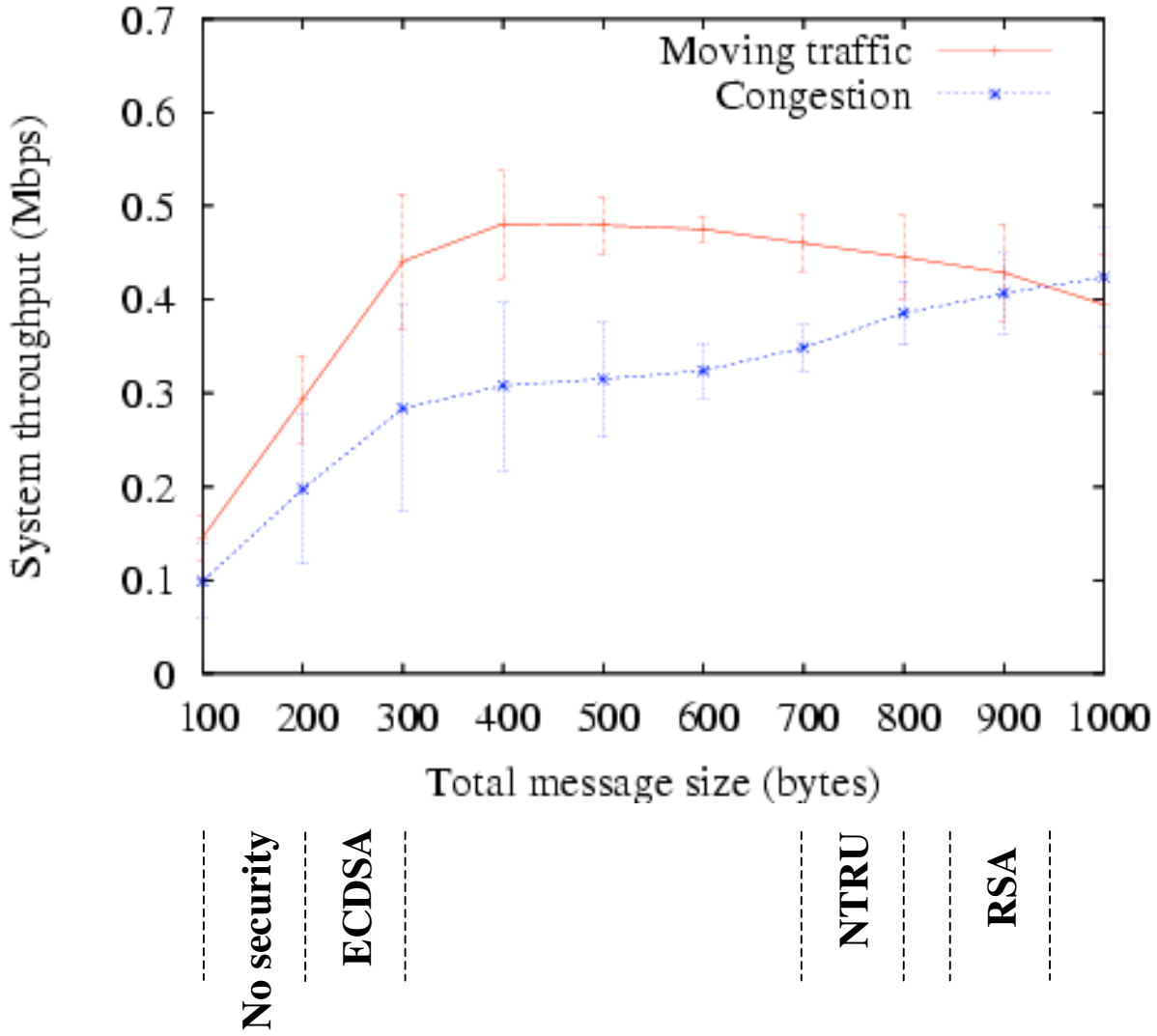
How msg size affects Delay, …



… Number of received packets, …



… and Throughput

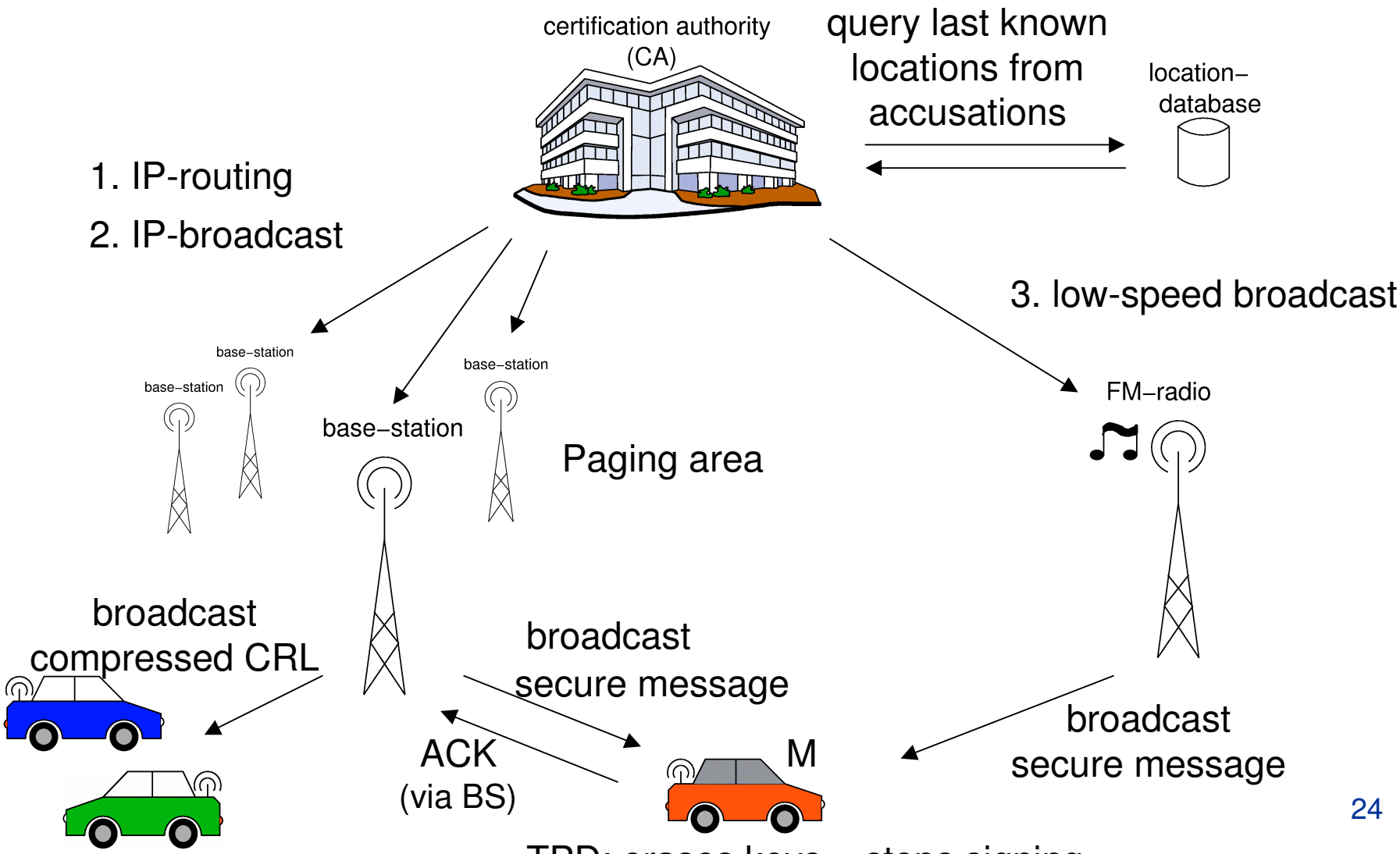


Certificate revocation in VANETs[1]

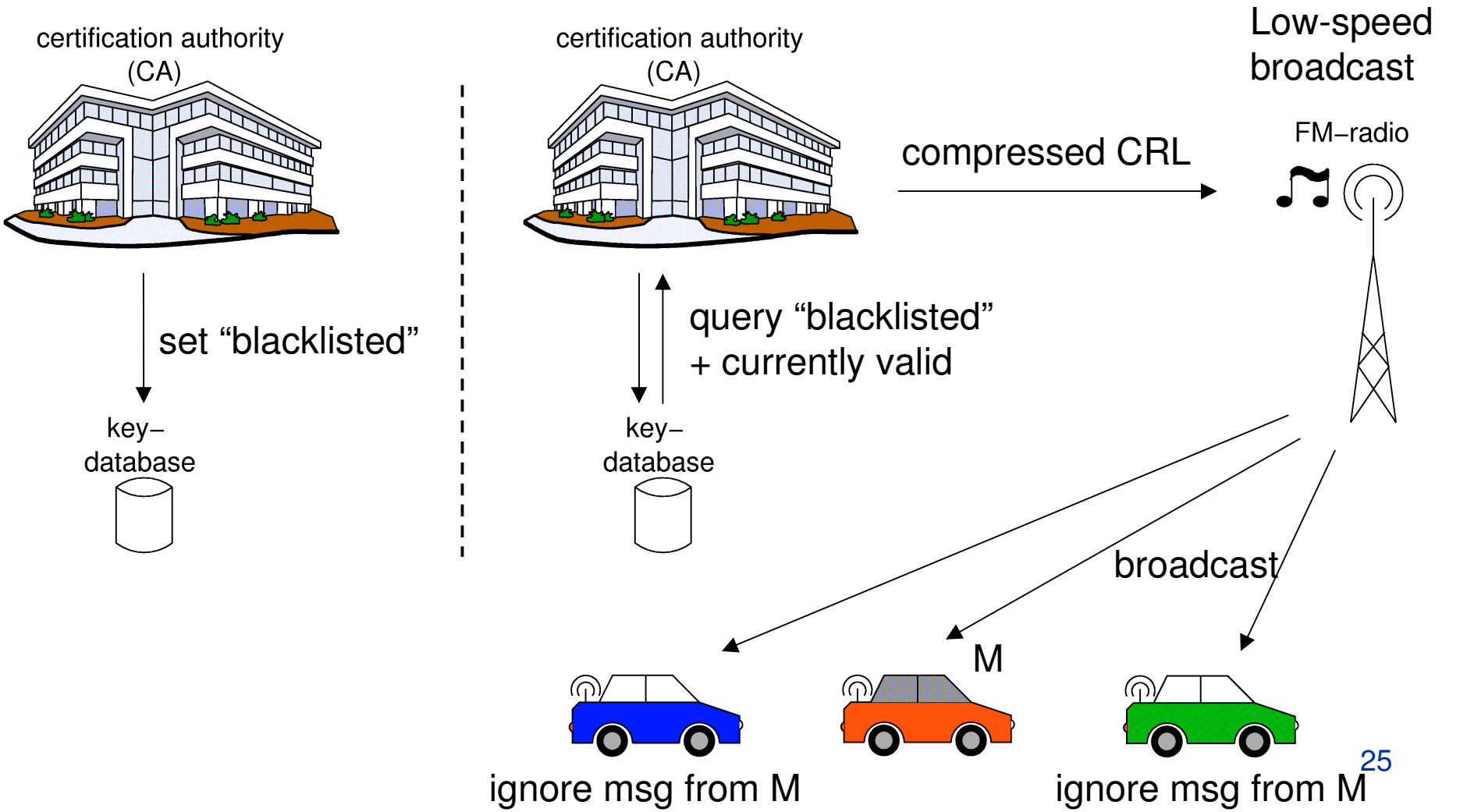
- The CA has to revoke invalid certificates:
  - Compromised keys
  - Wrongly issued certificates
  - A vehicle constantly sends erroneous information
- Using **C**ertificate **R**evocation **L**ists (**CRL**) is not appropriate
- We propose 3 protocols to revoke a vehicle's keys:
  - **R**ev. of the **T**amper-**P**roof **D**evice (**RTPD**): CA revokes all keys
  - **R**ev. by **C**ompressed **CRL**s (**RCCRL**): if TPD is not reachable
  - **D**istributed **R**evocation **P**rotocol (**DRP**): initiated by peers; generates a report to the CA, which triggers the actual revocation by RTPD/RCCRL

[1]In collaboration with Daniel Jungels and Imad Aad

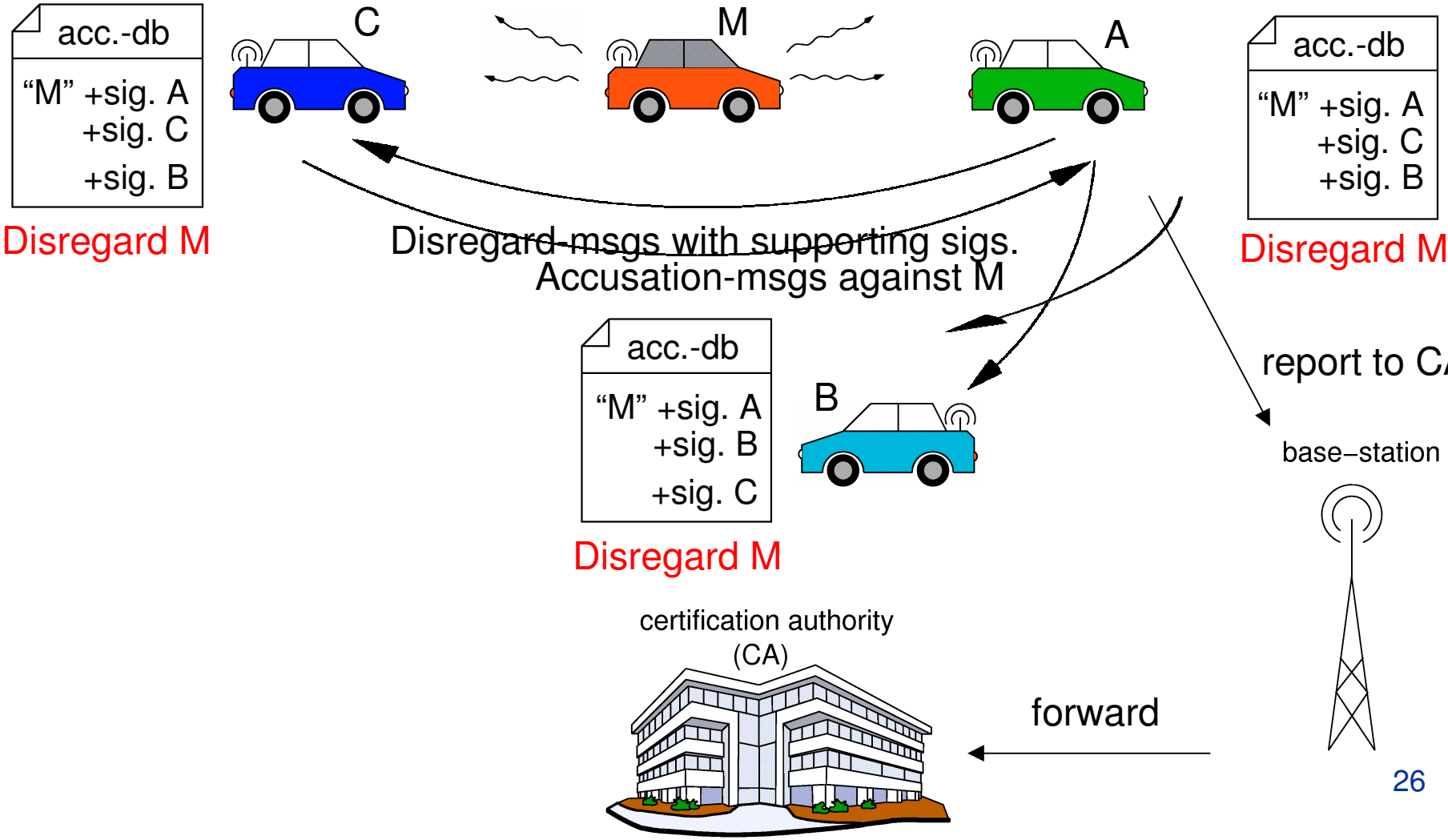
Revocation of the Tamper-Proof Device (RTPD)



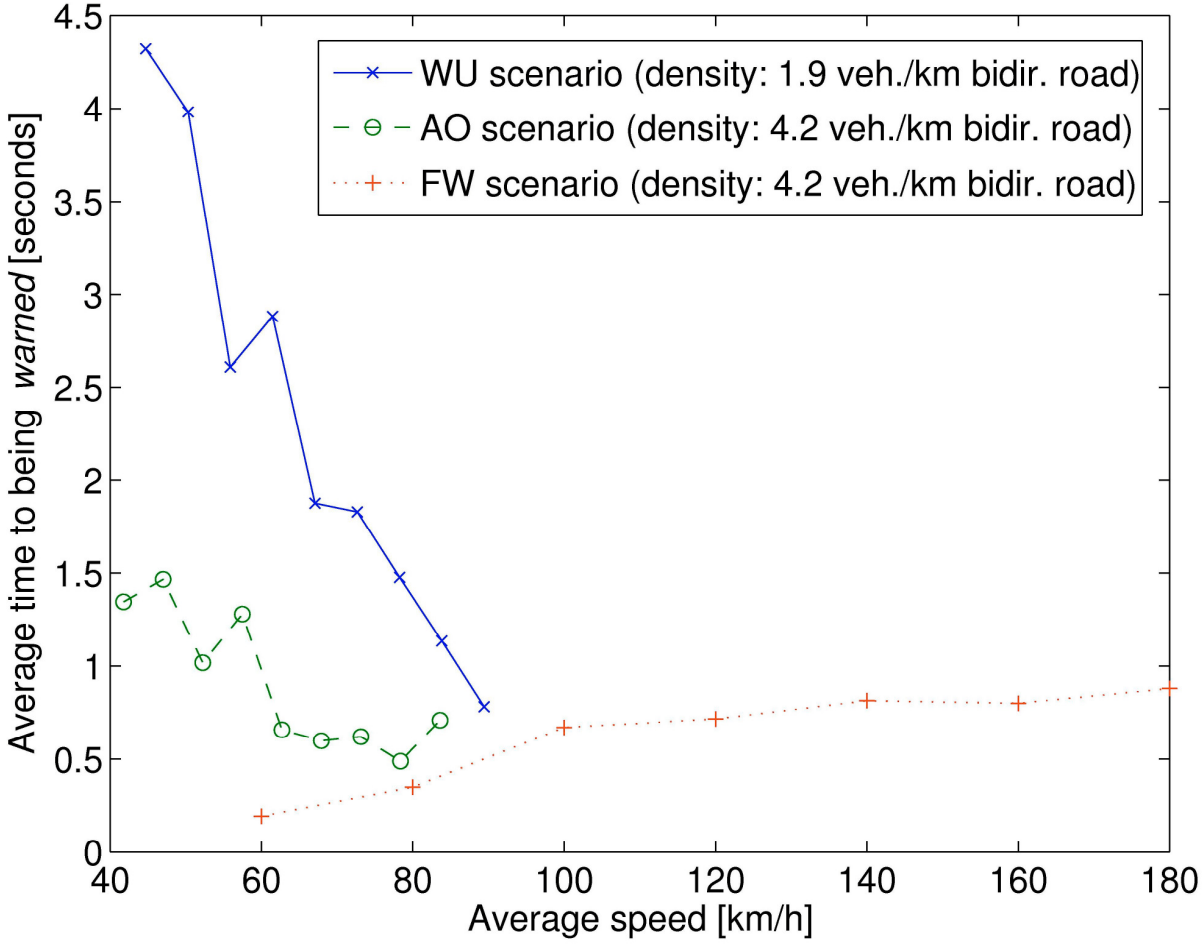
Revocation by Compressed CRLs (RCCRL)



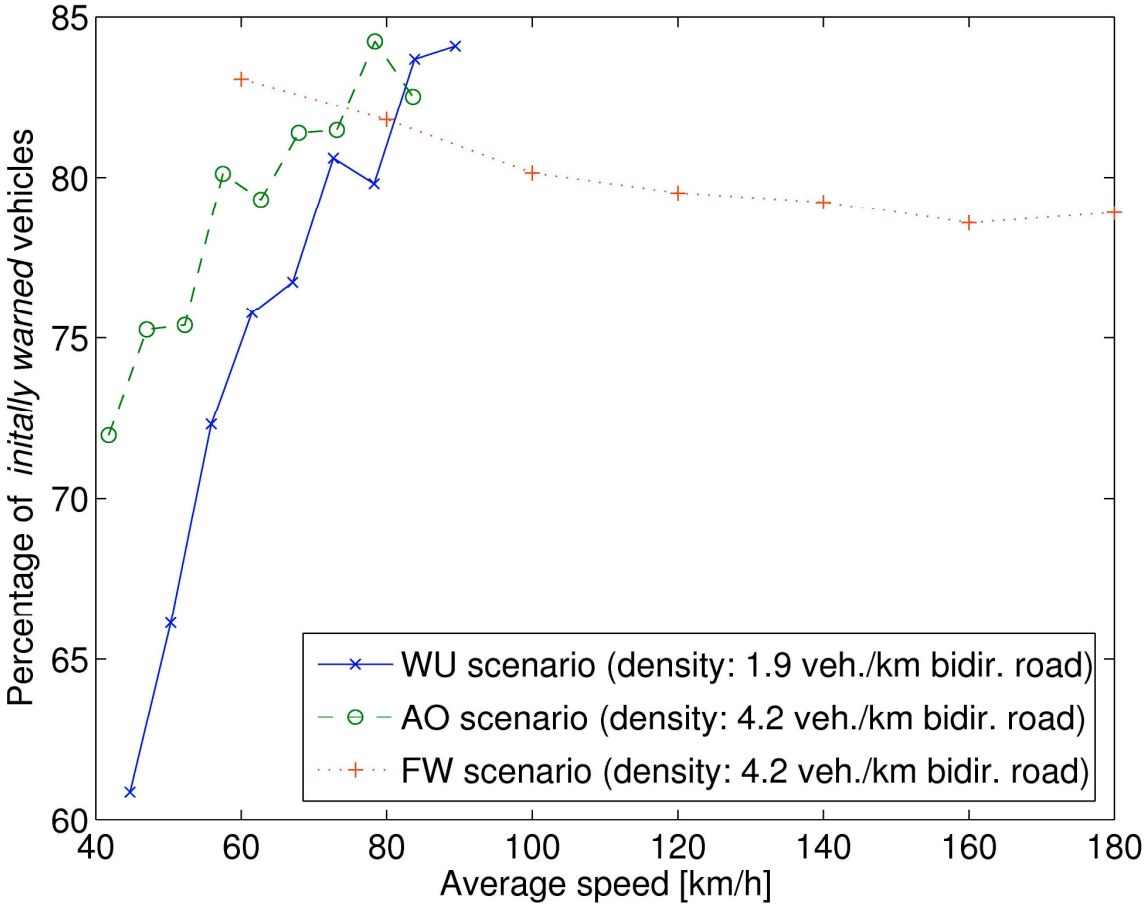
Distributed Revocation Protocol (DRP)



DRP speed


WU scenario (density: 1.9 veh./km bidir. road)
AO scenario (density: 4.2 veh./km bidir. road)
FW scenario (density: 4.2 veh./km bidir. road)
Average time to being warned [seconds]
Average speed [km/h]
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
40
60
80
100
120
140
160
180

DRP coverage



Conclusion

- VANET security is very important
- We presented its main aspects:
  - Threat model
  - Security architecture
- Tradeoffs exist, e.g., between privacy and liability
- The choice of the cryptosystem is crucial
- More info at http://ivc.epfl.ch