Panos Papadimitratos

Senior Researcher, EPFL

Geneva, 5-7 March 2008

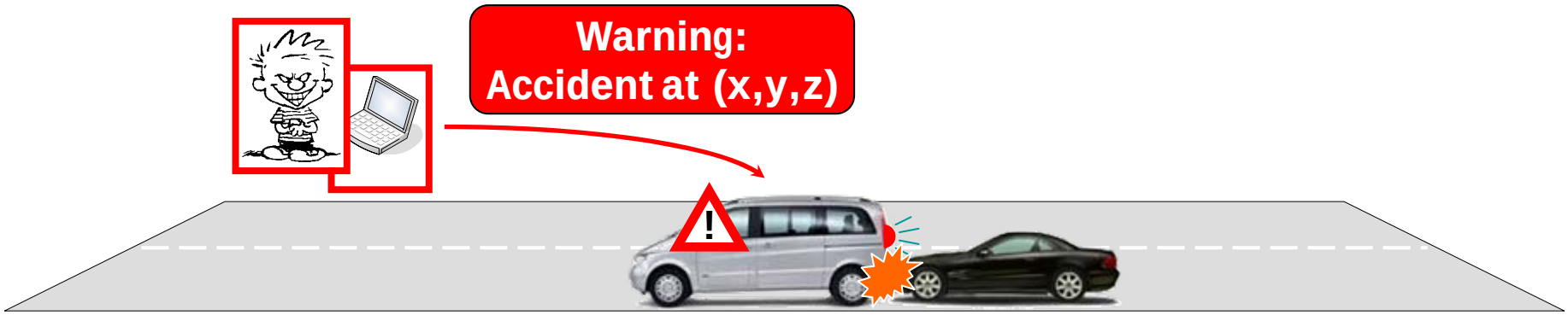
ISO IEC ITU International Telecommunication Union

Secure Vehicular Communication Systems: Towards Deployment

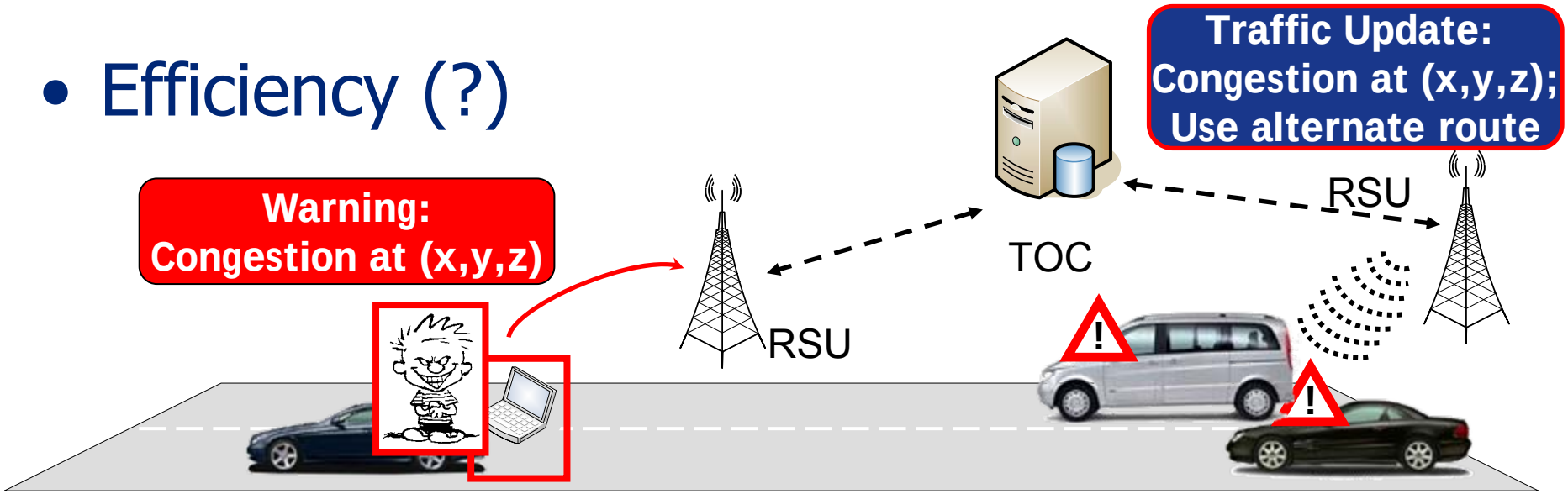
•The Fully Networked Car
•Geneva, 5-7 March 2008

Security and Privacy for VC?

- Safety (?)

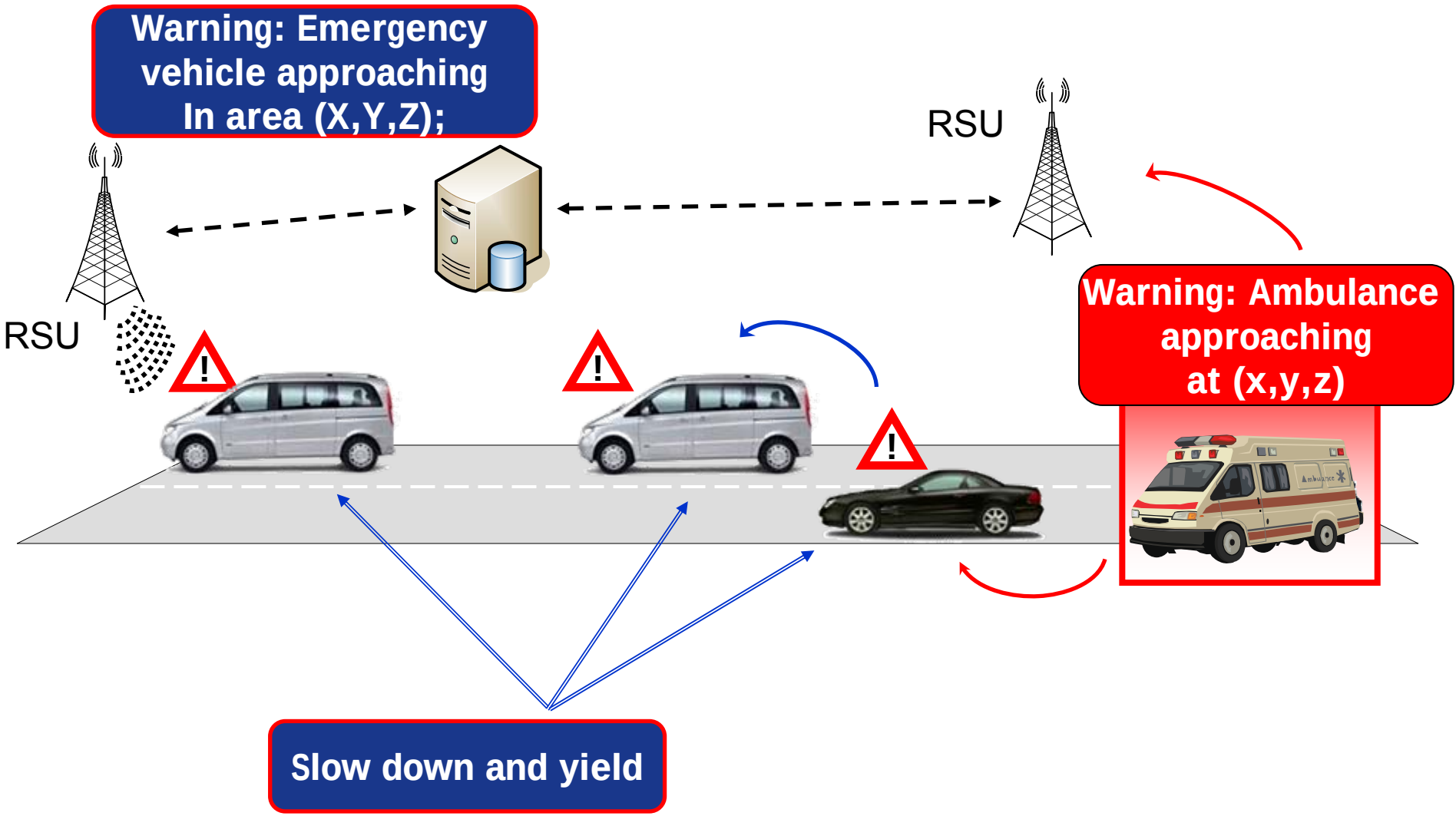


- Efficiency (?)



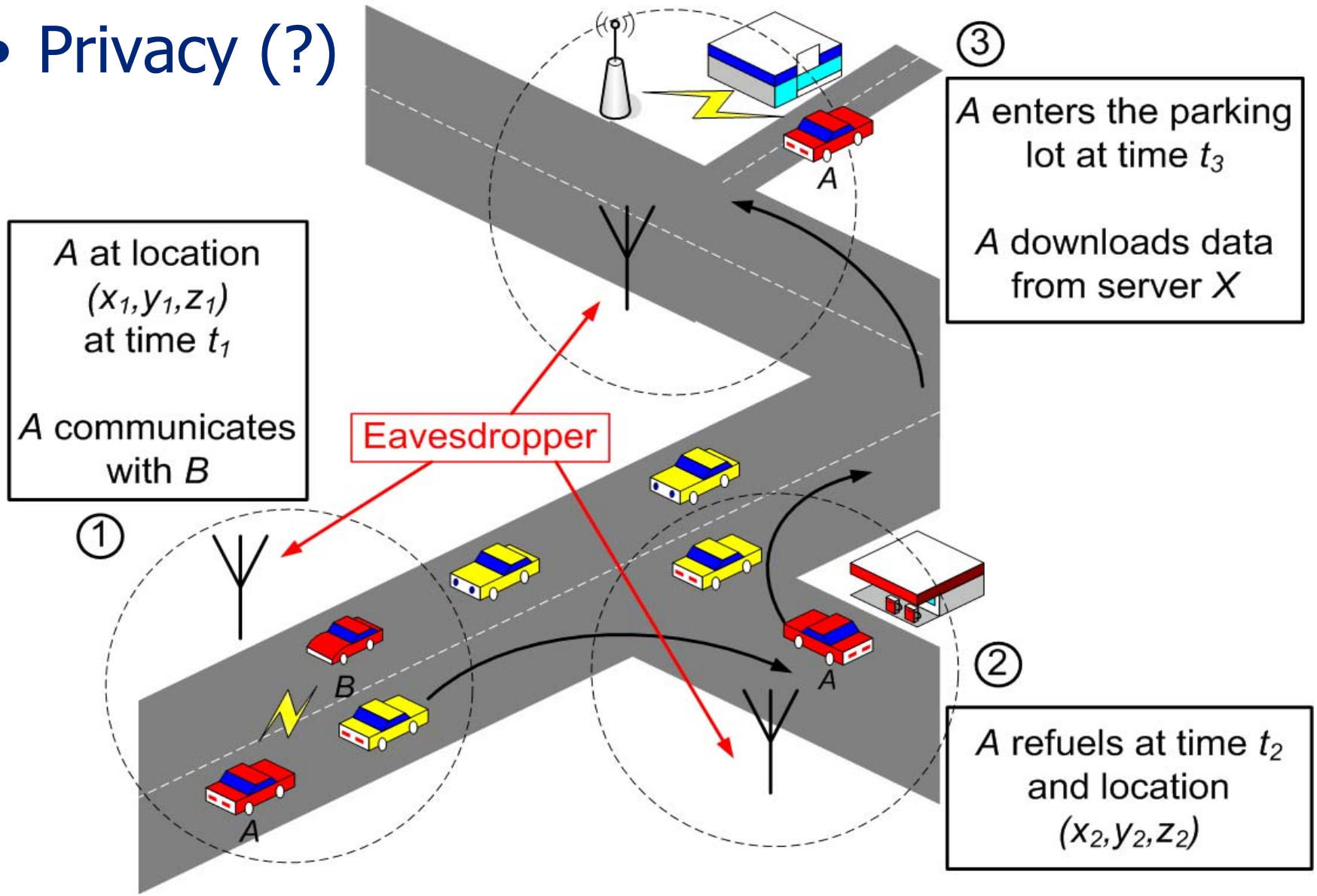
Security and Privacy for VC? (cont'd)

- Efficiency (?)

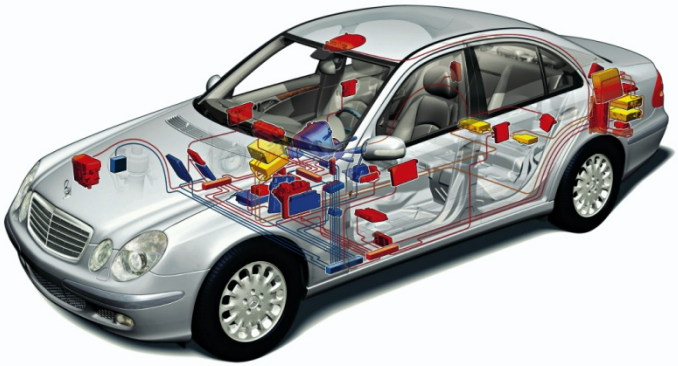


Security and Privacy for VC? (cont'd)

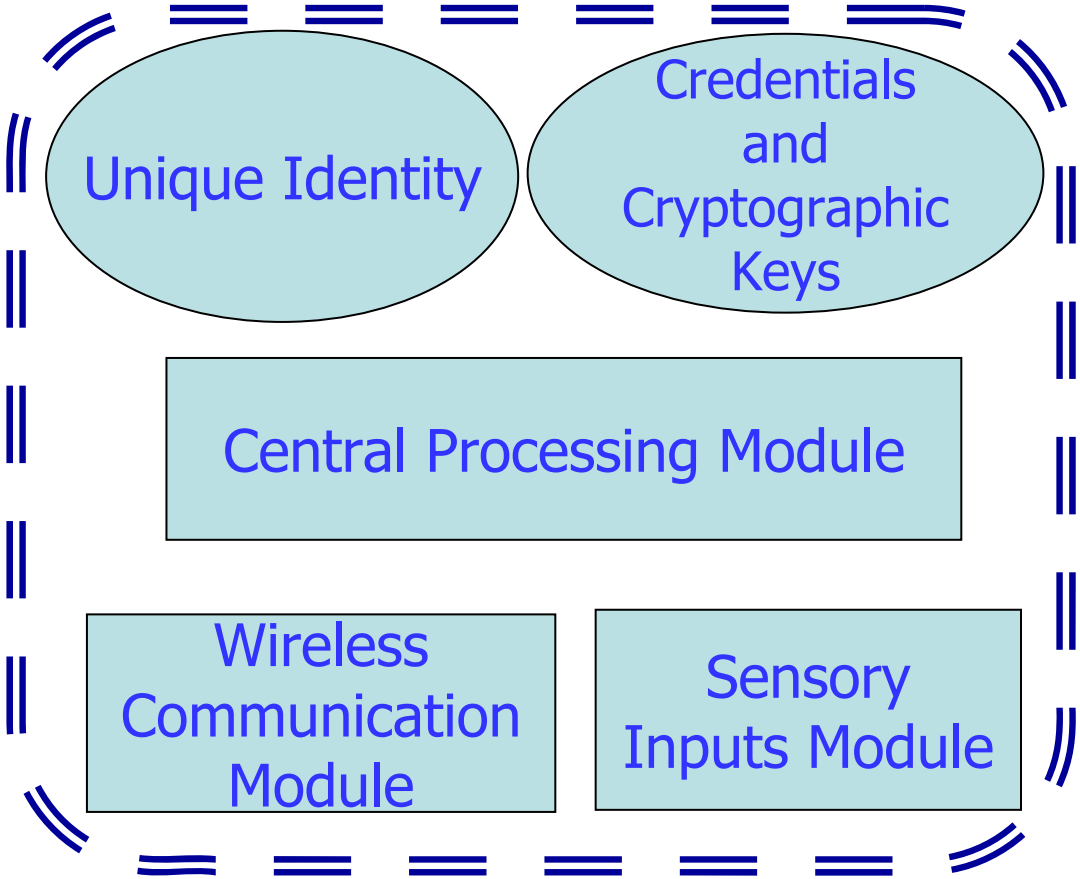
- Privacy (?)



Secure VC system entities



Abstract view of a vehicle in a (secure) vehicular communications system

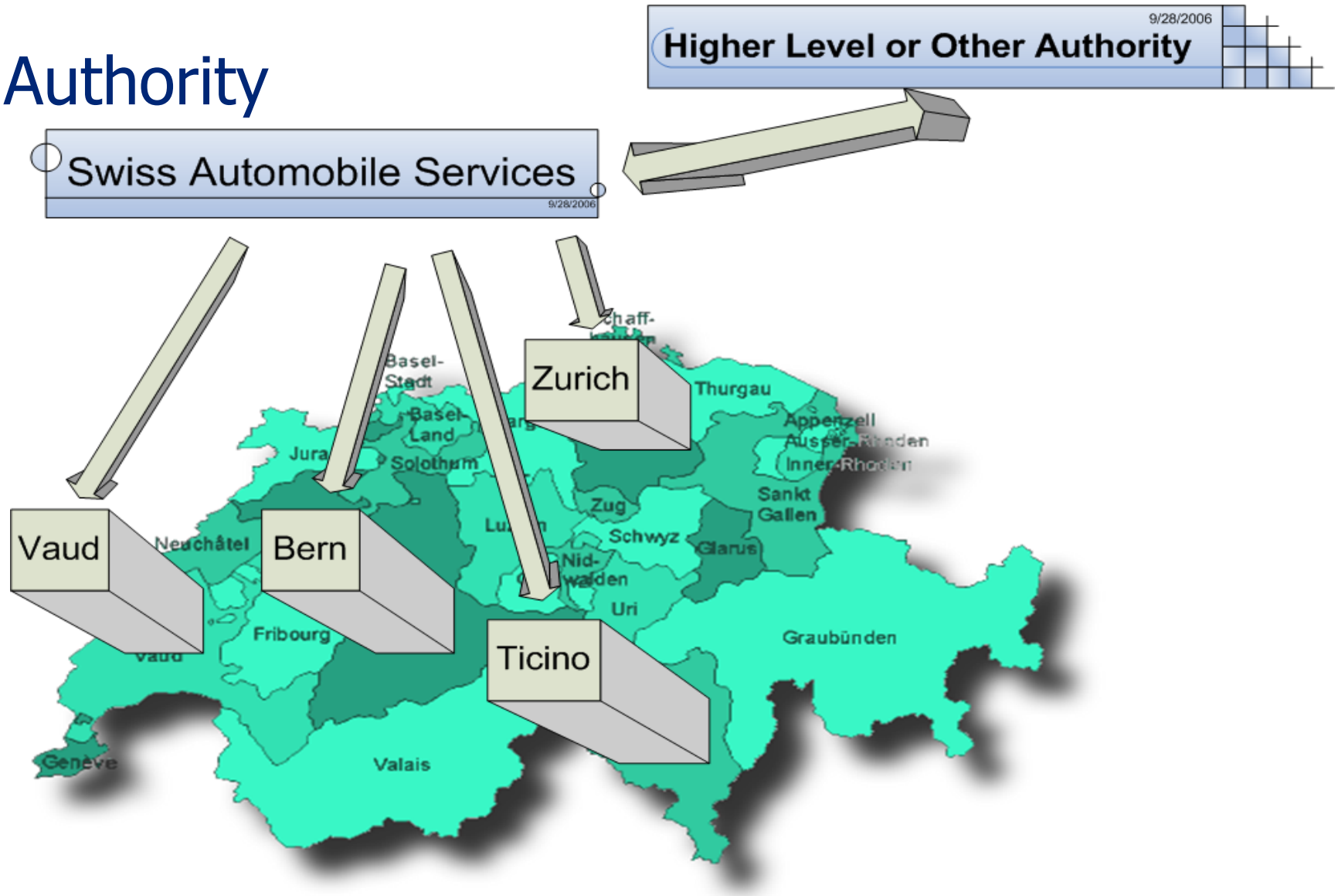


Secure VC system entities (cont'd)

- Node V
  - Identity
    - Integration of pre-VC and VC-specific identifiers
    - Long-term
  - Cryptographic keys
    - Public/private K_V / k_V
  - Credential
    - Certificate $Cert_{CA}$ (V, K_V, A_V, T)
      - A_V: attributes of node V
      - T: lifetime

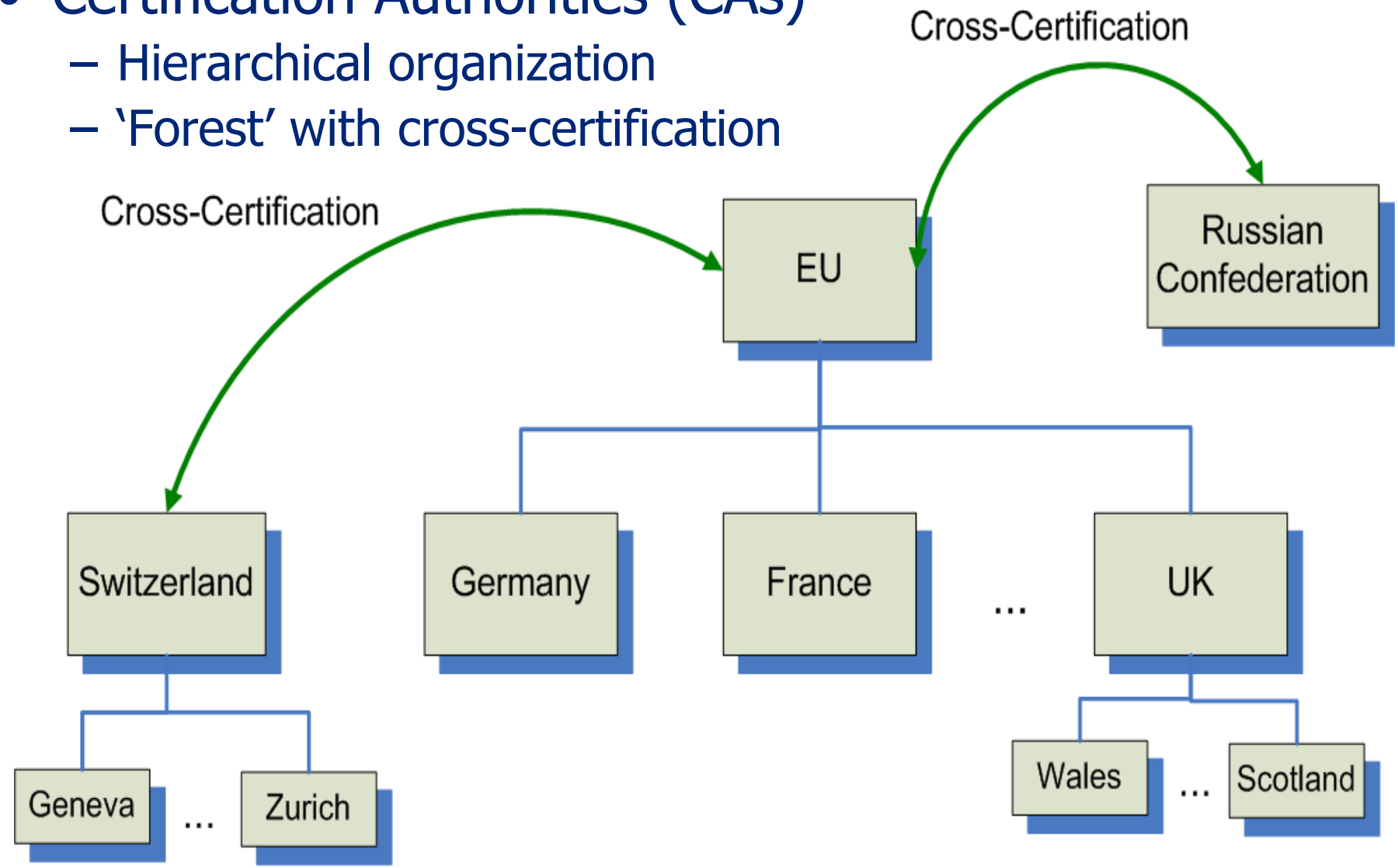
Secure VC system entities (cont'd)

- Authority

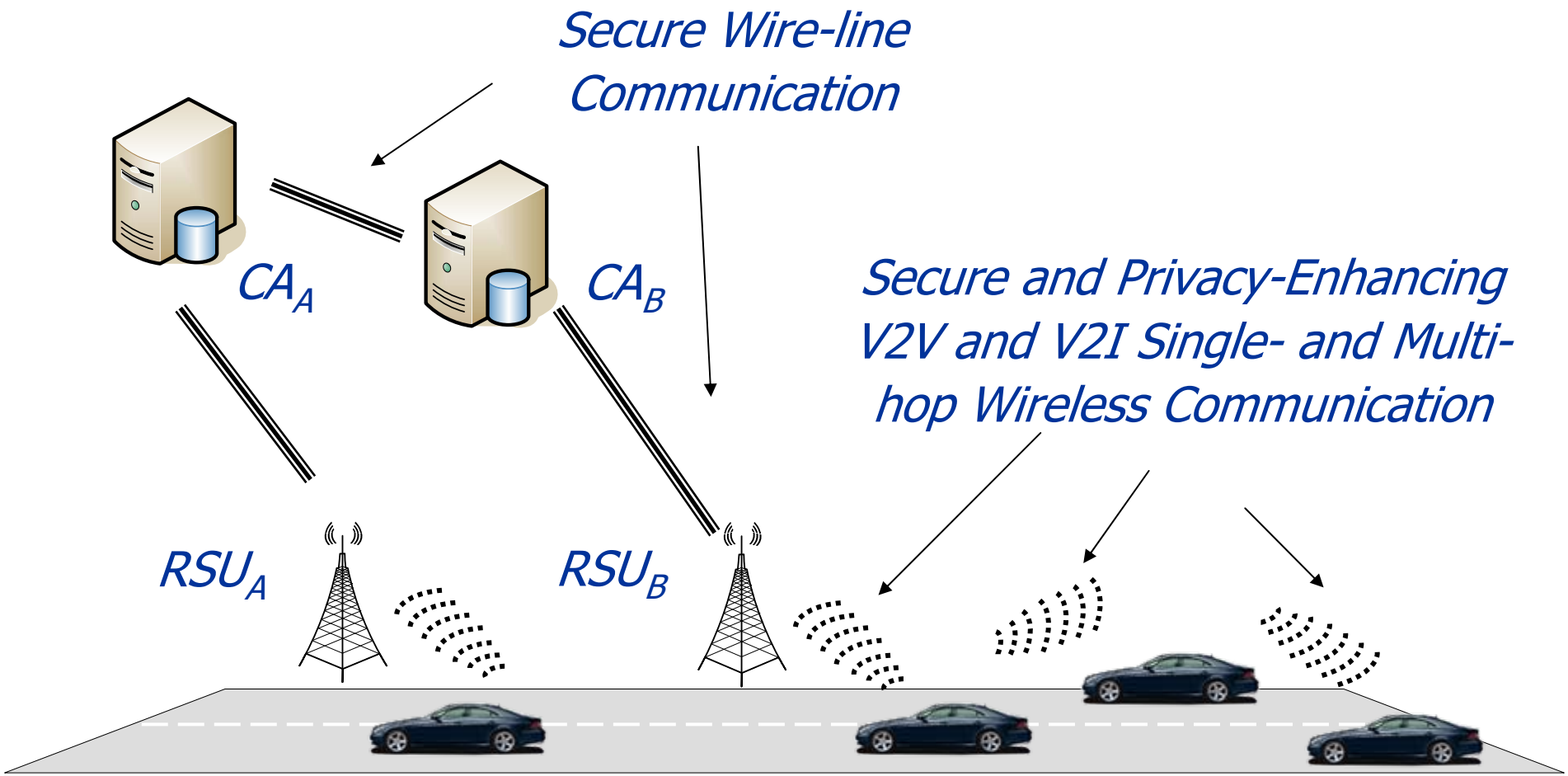


Secure VC system entities (cont'd)

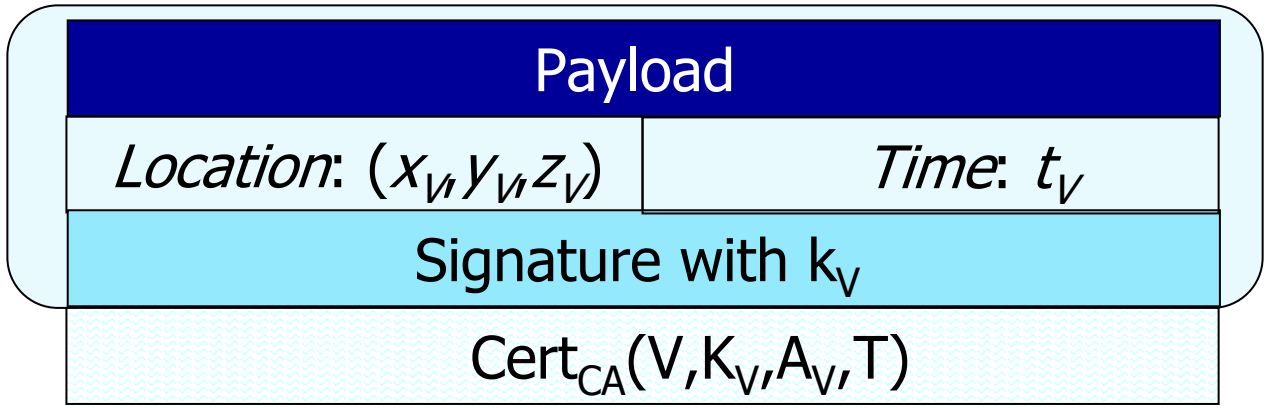
- Certification Authorities (CAs)
  - Hierarchical organization
  - 'Forest' with cross-certification

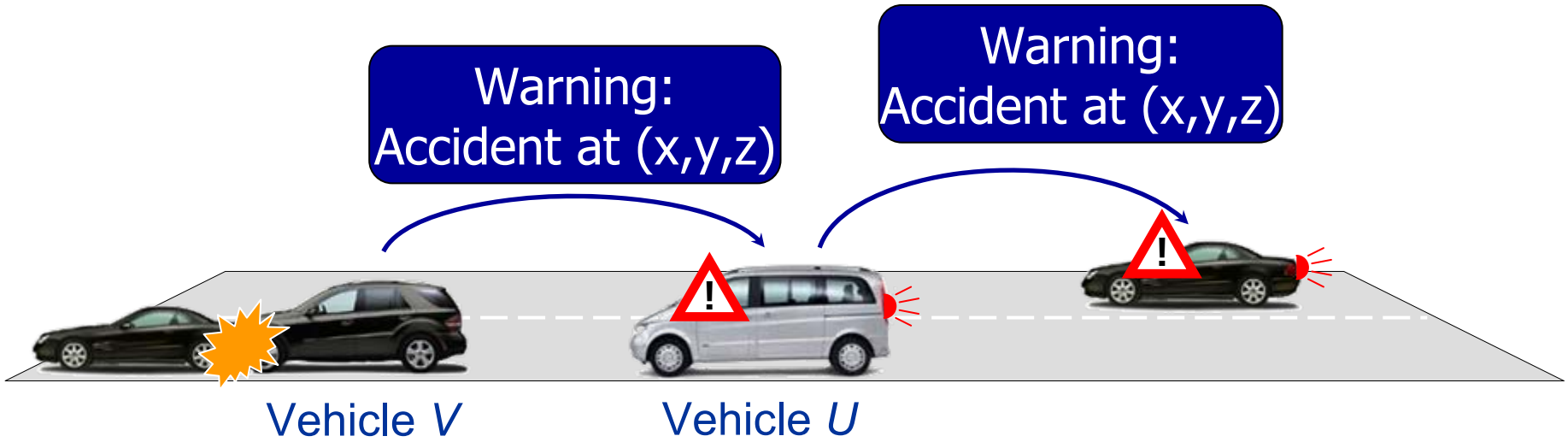


Secure vehicular communication



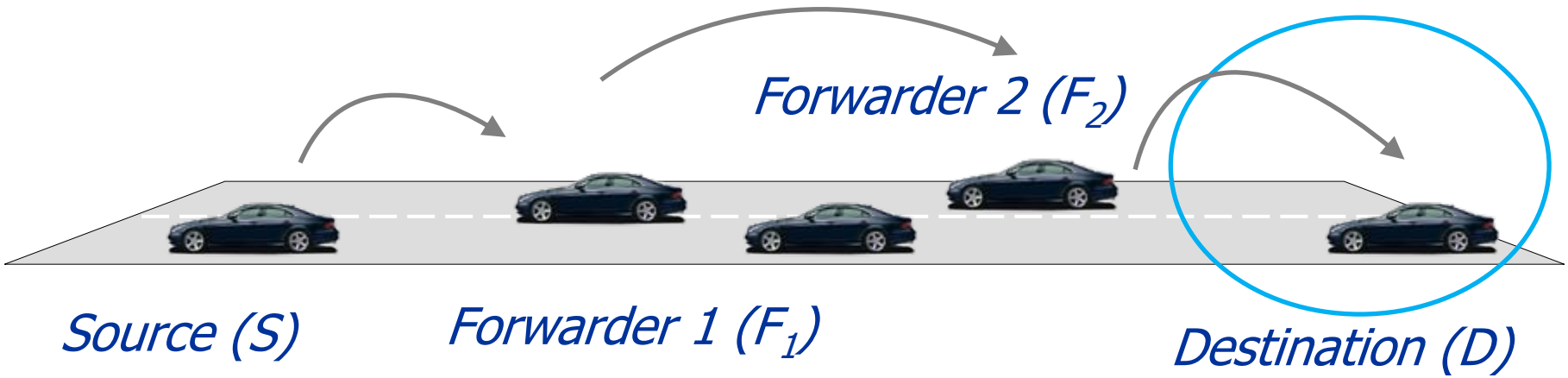
Secure communication



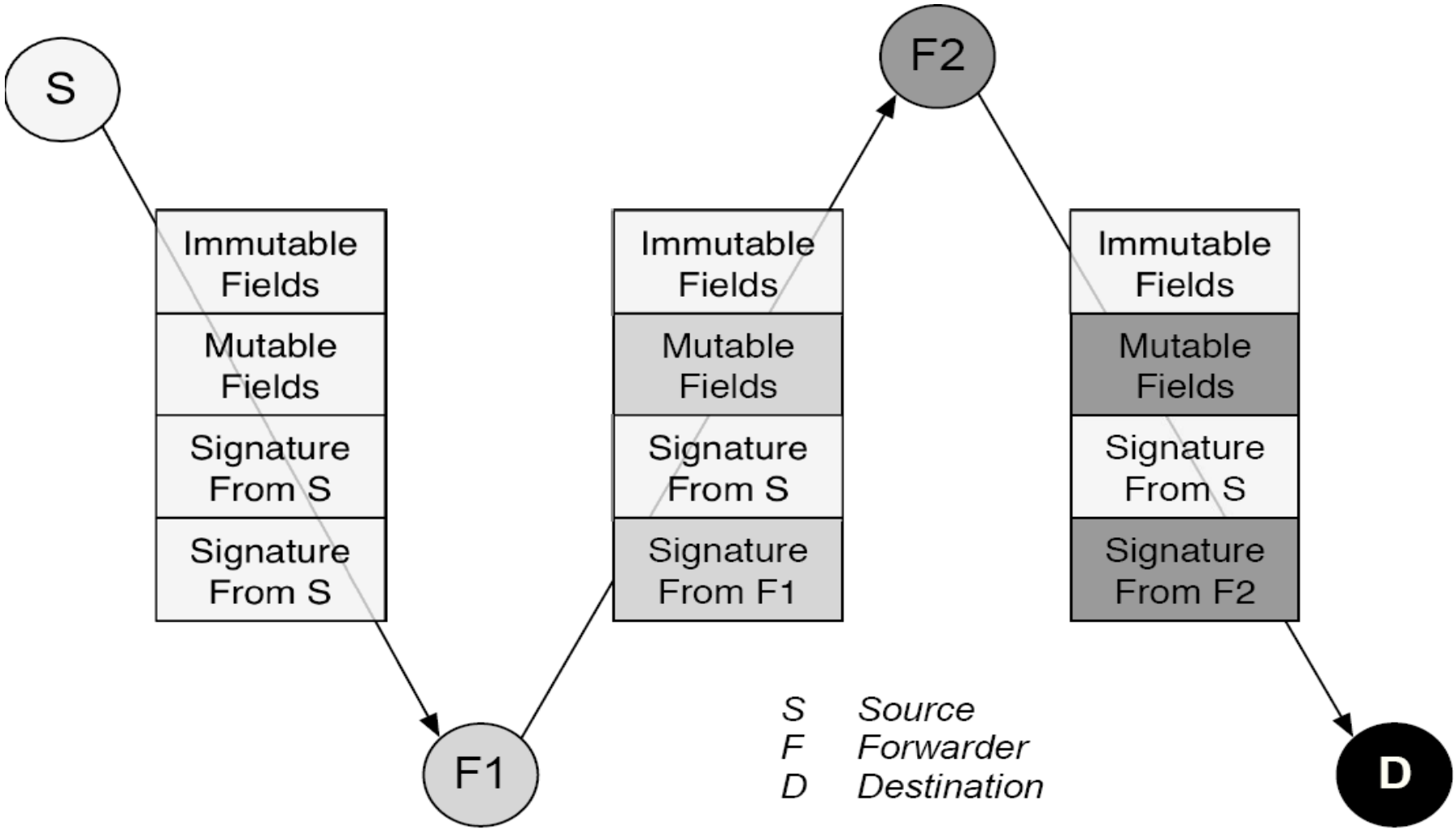


Secure Geo-Cast (cont'd)

- Position-based routing
  - Relaying nodes (forwarders) also send packets to the geographically closest node to the destination (location)



Secure Geo-Cast (cont'd)



C. Harsch, A. Festag, and **P. P.**, "Secure Position-Based Routing for VANETs," IEEE VTC 2007-Fall

Pseudonymous authentication

- At least the same degree of privacy achieved nowadays, before vehicular communications
- Ideally, anonymous and authentic communications, but:
  - High processing and communication overhead
  - Often, messages from the same vehicle should be linkable
- Requirement: messages generated by a given vehicle can be linked at most over a protocol-selectable period of time
  - The shorter this period, the harder to track a vehicle becomes

Pseudonymous authentication (cont'd)

- **Pseudonym**
  - Certified public key
  - Certificate has no identifying information
- Equip vehicles with **multiple** pseudonyms
  - Alternate among pseudonyms over time (and space)
  - Sign message with the private key corresponding to pseudonym
  - Append current pseudonym to signed message

Pseudonymous authentication (cont'd)

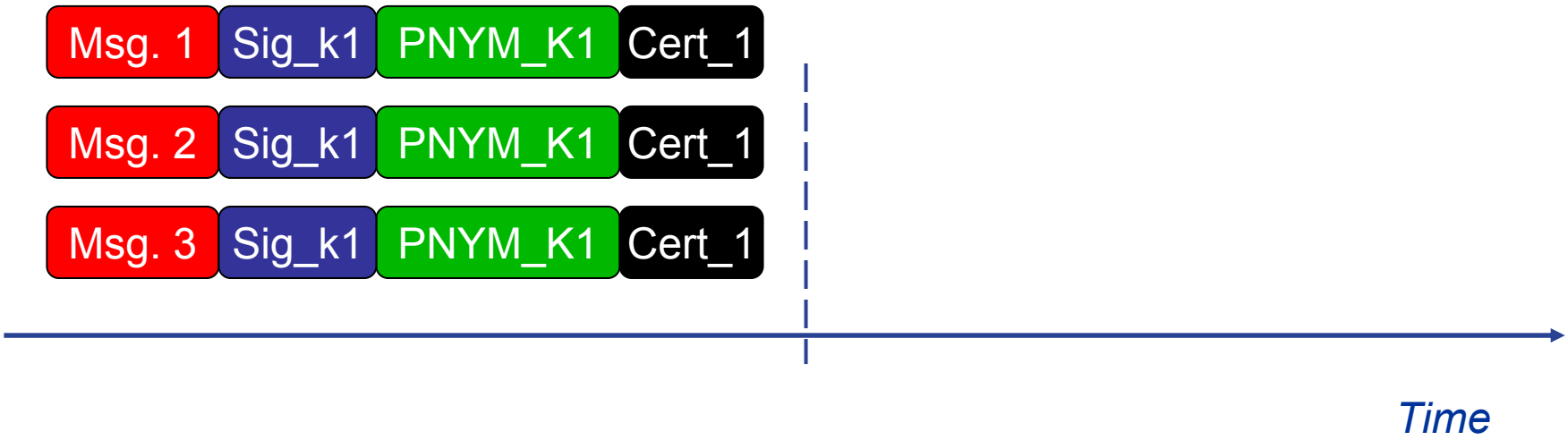
- Pseudonym format

PSNYM-Provider ID	PSNYM Lifetime
Public Key K_i	
PSNYM-Provider Signature	

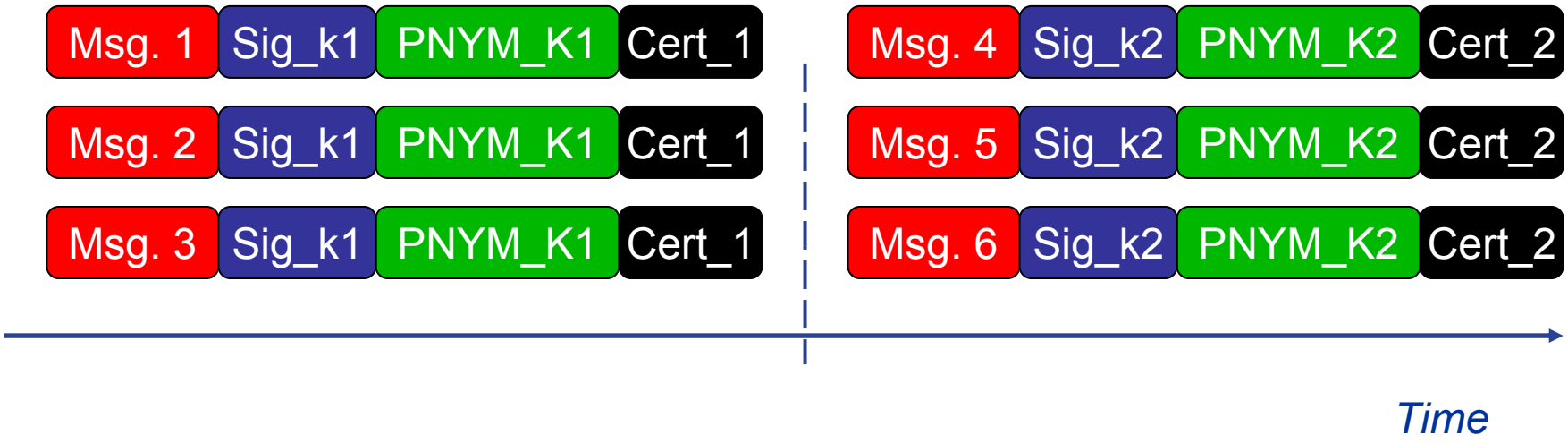
- Supplying vehicles with pseudonyms
  - Sufficient in number
  - Periodic 'refills'
- Pseudonym provider: a trusted third party

P. P., L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, M. Raya, "Architecture for secure and private vehicular communications," ITST 2007

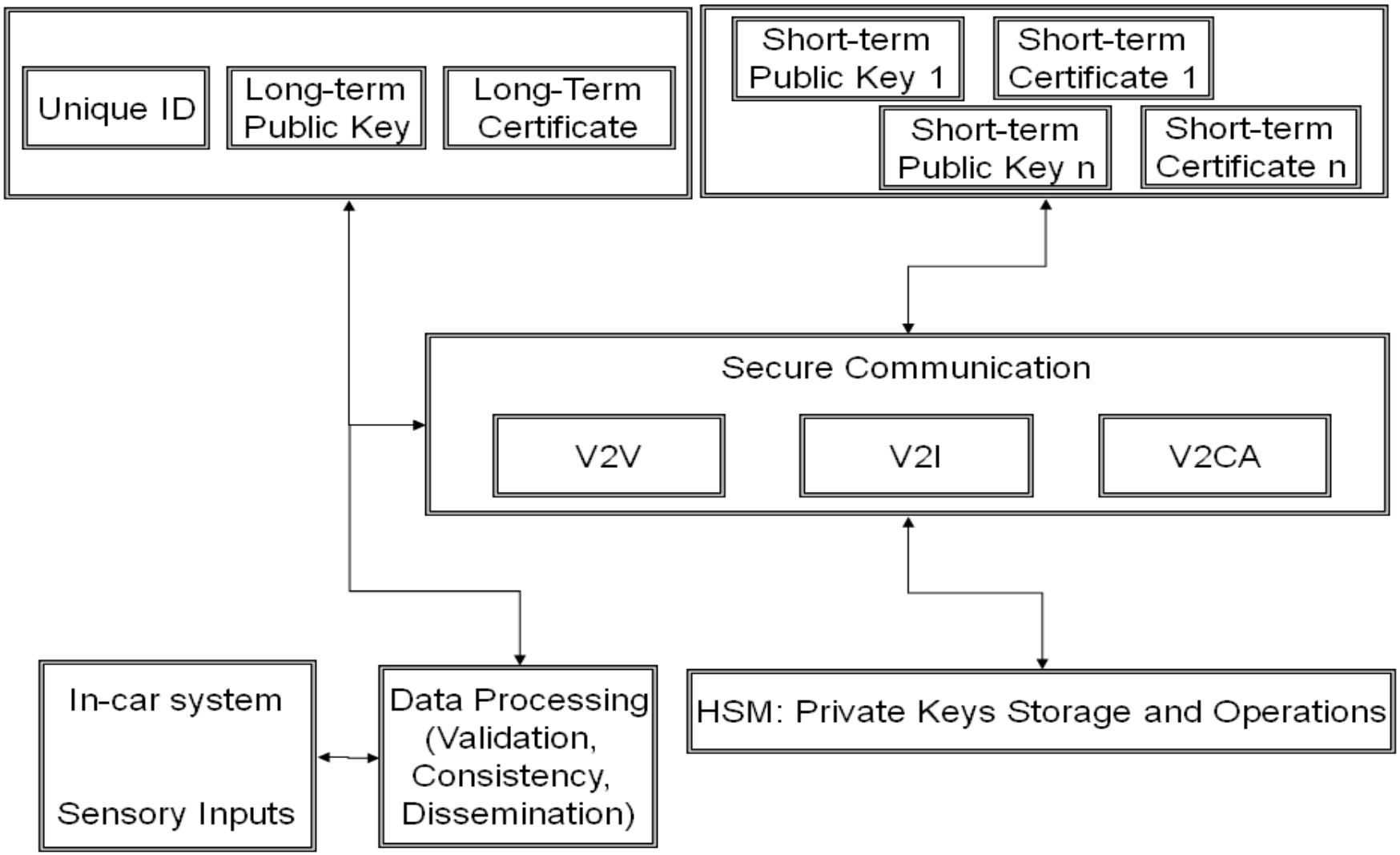
Pseudonymous authentication (cont'd)



Pseudonymous authentication (cont'd)



Secure VC: system overview



Are secure VC systems practical?

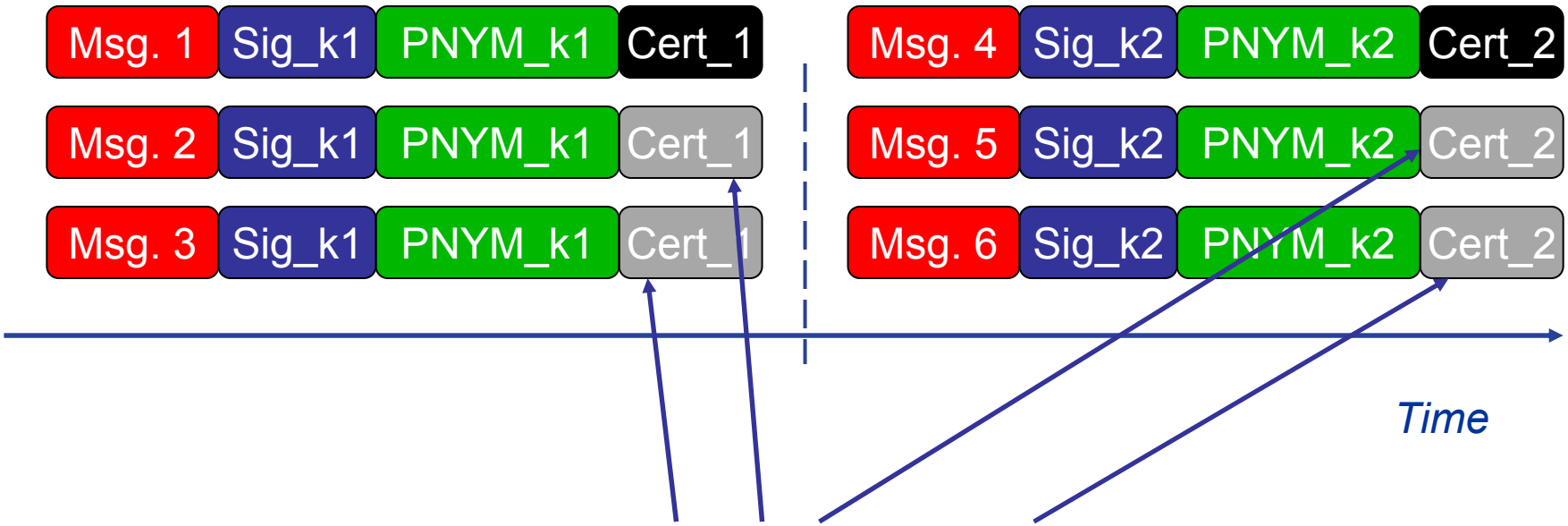
- Can security protocols run, along with the VC protocol stack, on the embedded computing units?
- Are security architectures easy to manage?
- Can a secured vehicular communication system be as effective as one without security?

Are secure VC systems practical? (cont'd)

- Lesson 1: More on-board processing power
- Lesson 2: Careful use of strong security
  - Communication optimizations
  - Adaptation to operational requirements
- Lesson 3: Impact of security on VC-enabled applications
- Lesson 4: Security is perceived as a constraint

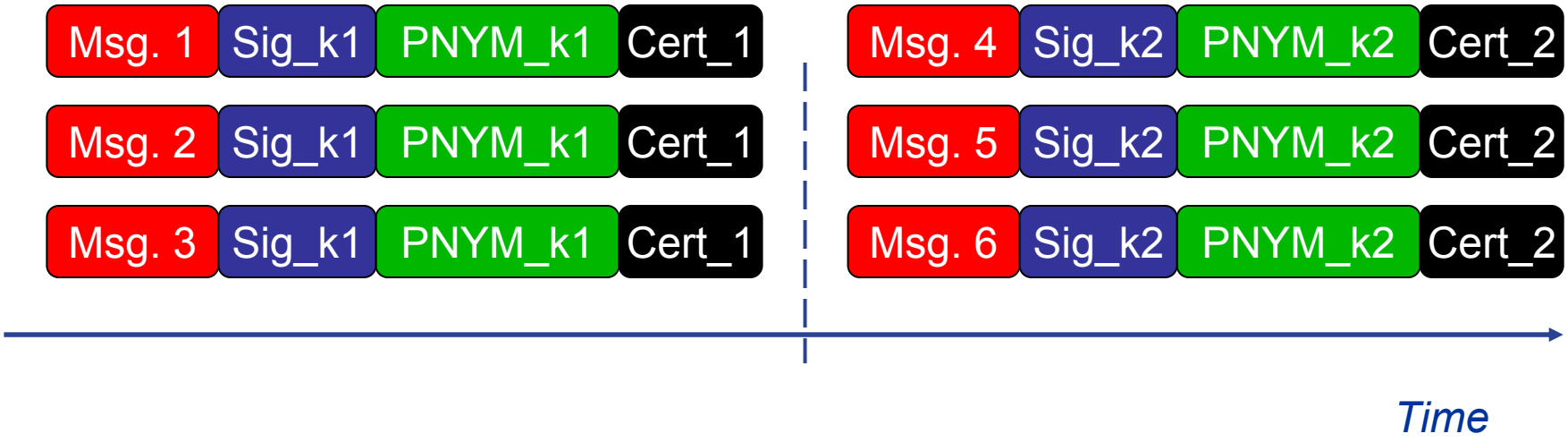
P. P., "On the road - Reflections on the Security of Vehicular Communication Systems," IEEE ICVES, Columbus, OH, USA, Sept. 2008

Reducing SVC cost - Optimization (1)

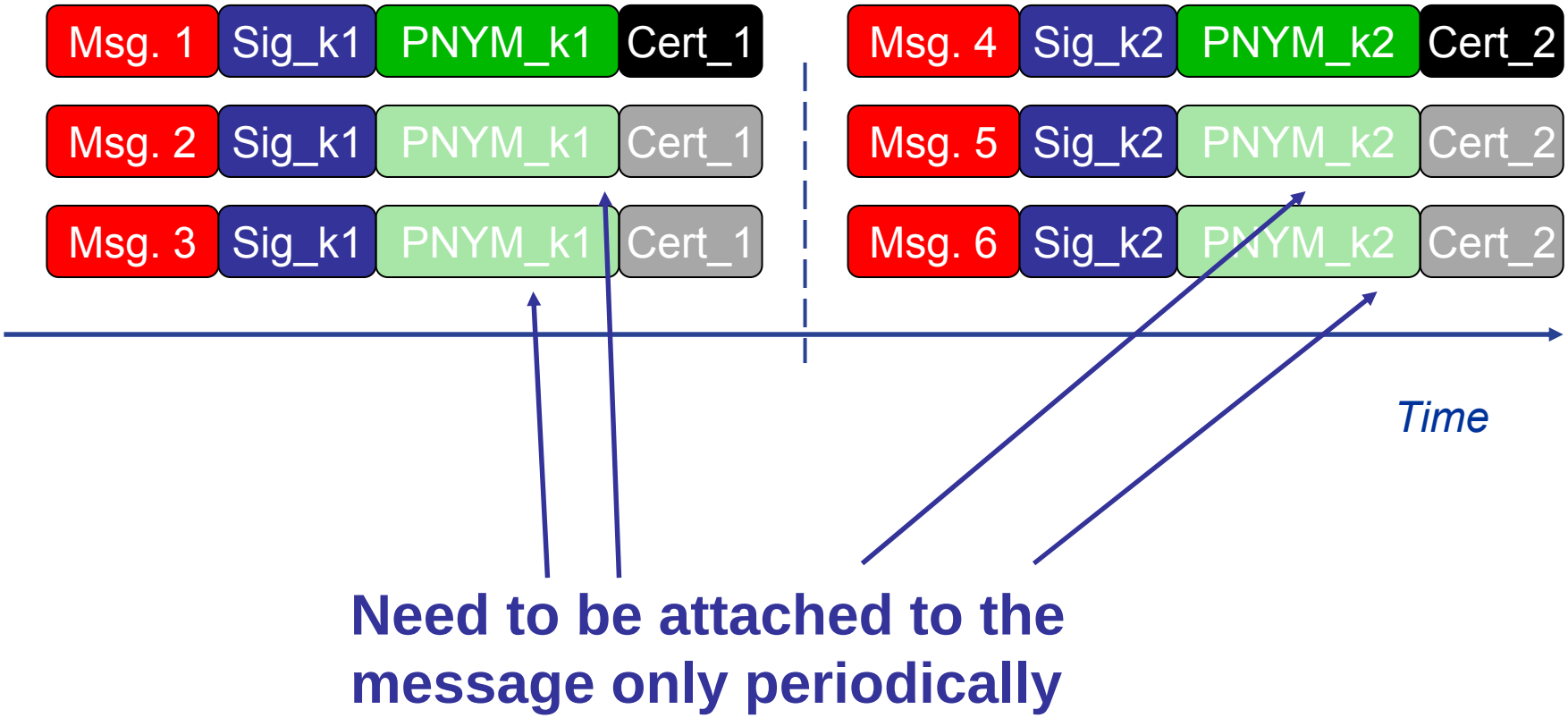


Need to be generated / validated only once per pseudonym lifetime

Reducing SVC cost - Optimization (2)

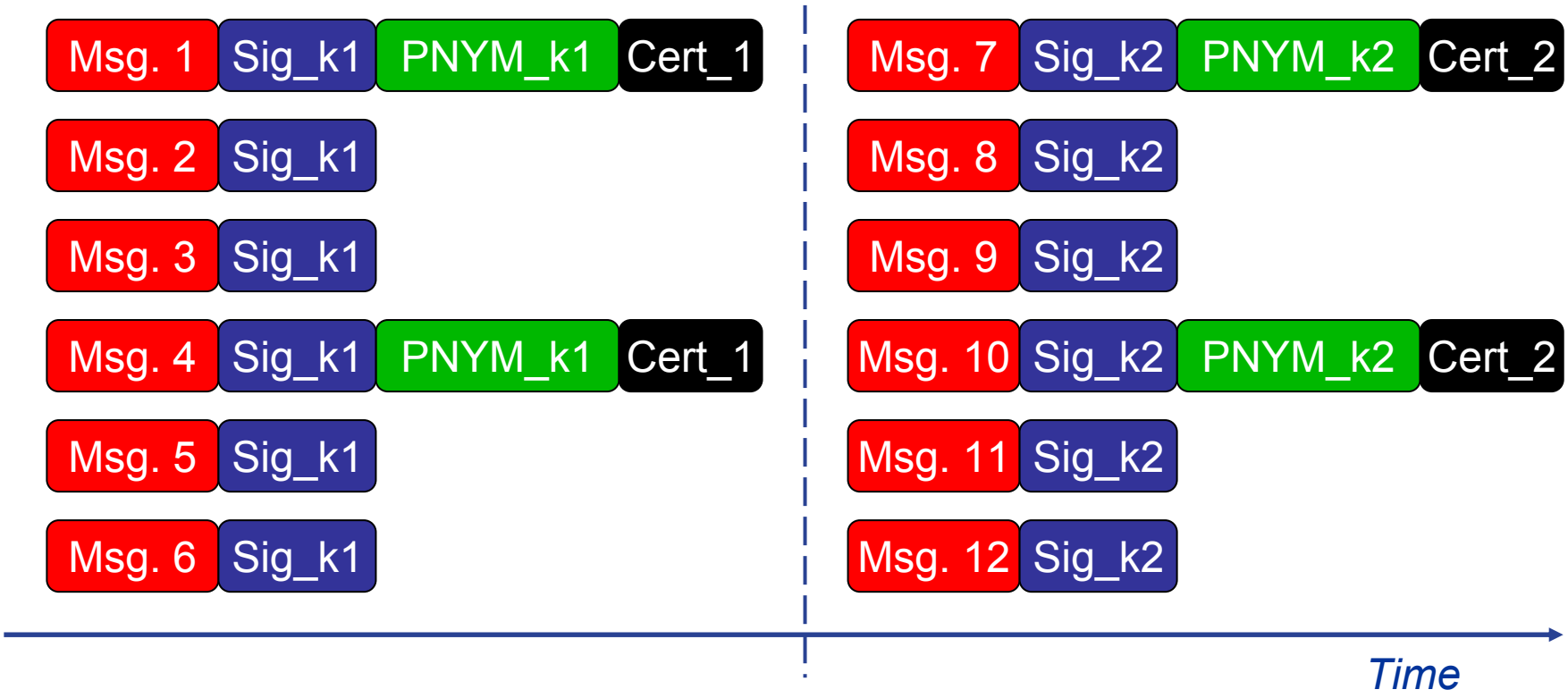


Reducing SVC cost - Optimization (2)

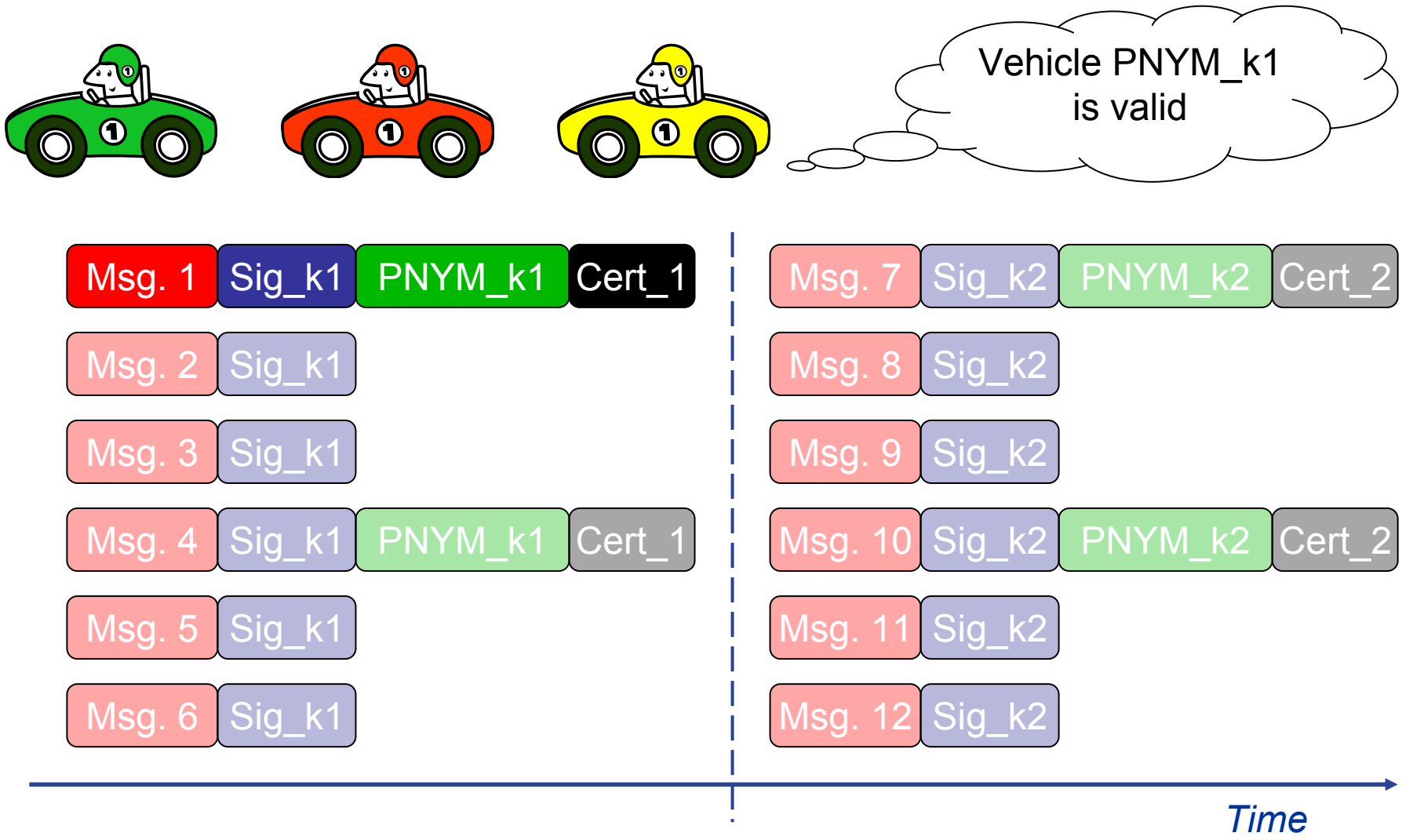


Need to be attached to the message only periodically

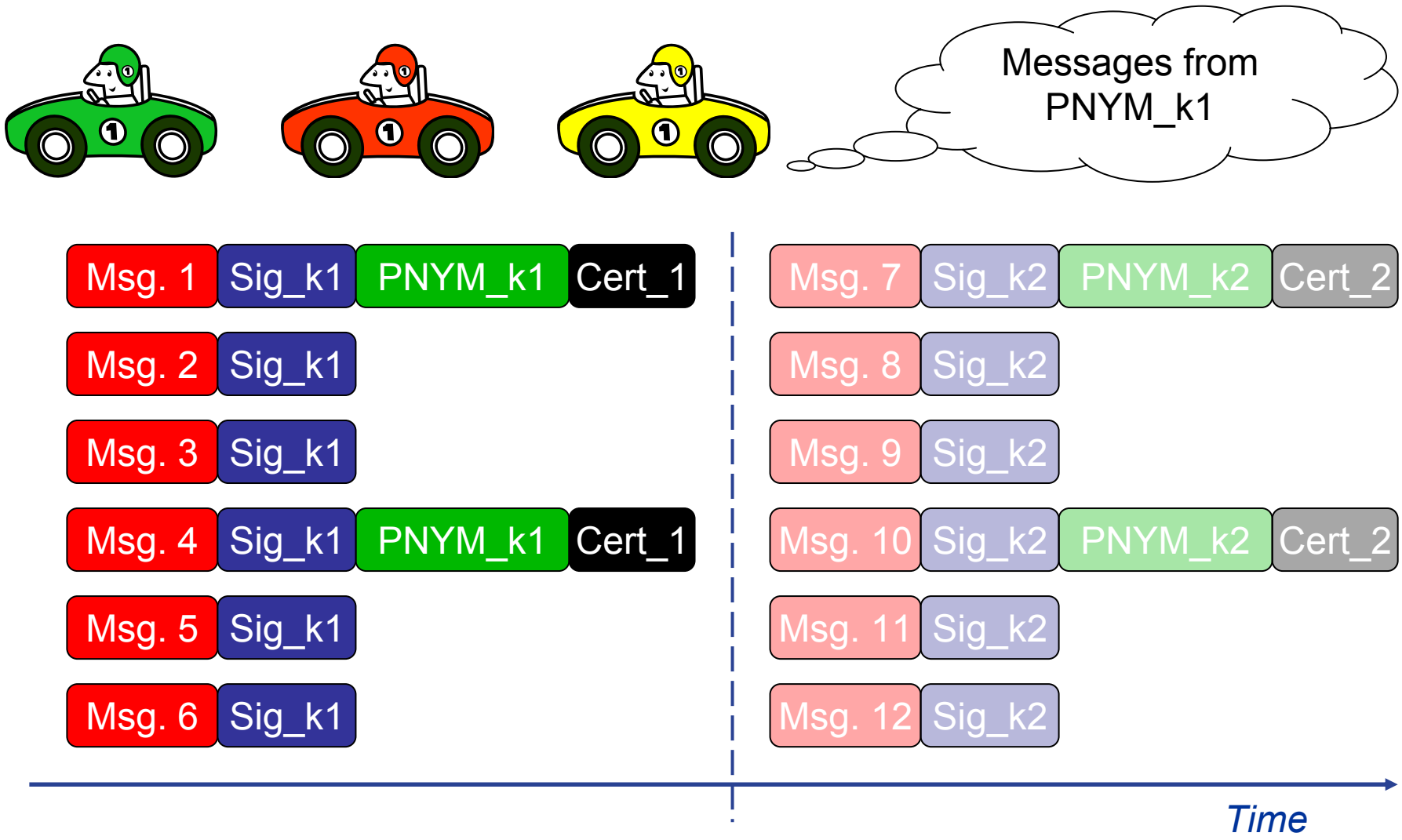
Reducing SVC cost - Optimization (2)



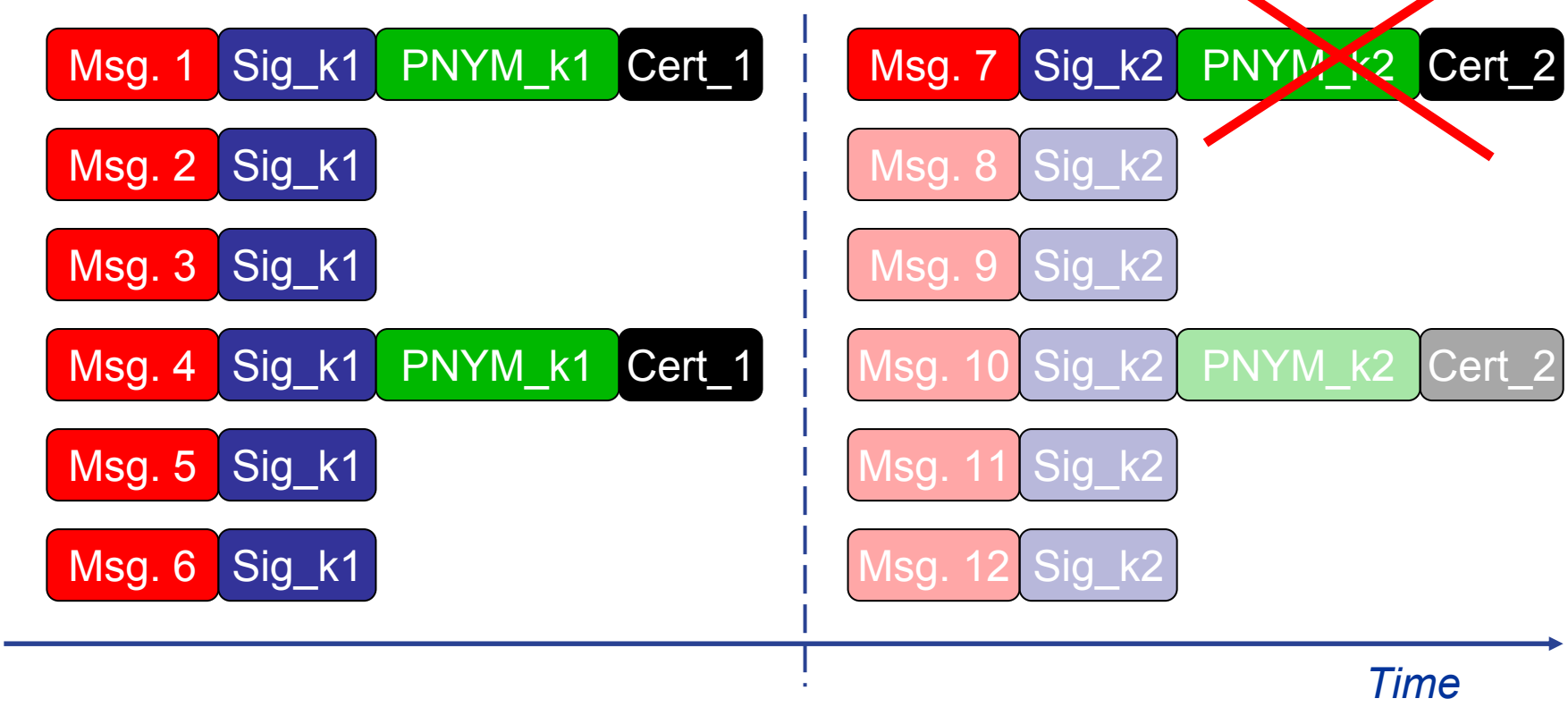
Reducing SVC cost - Optimization (3)



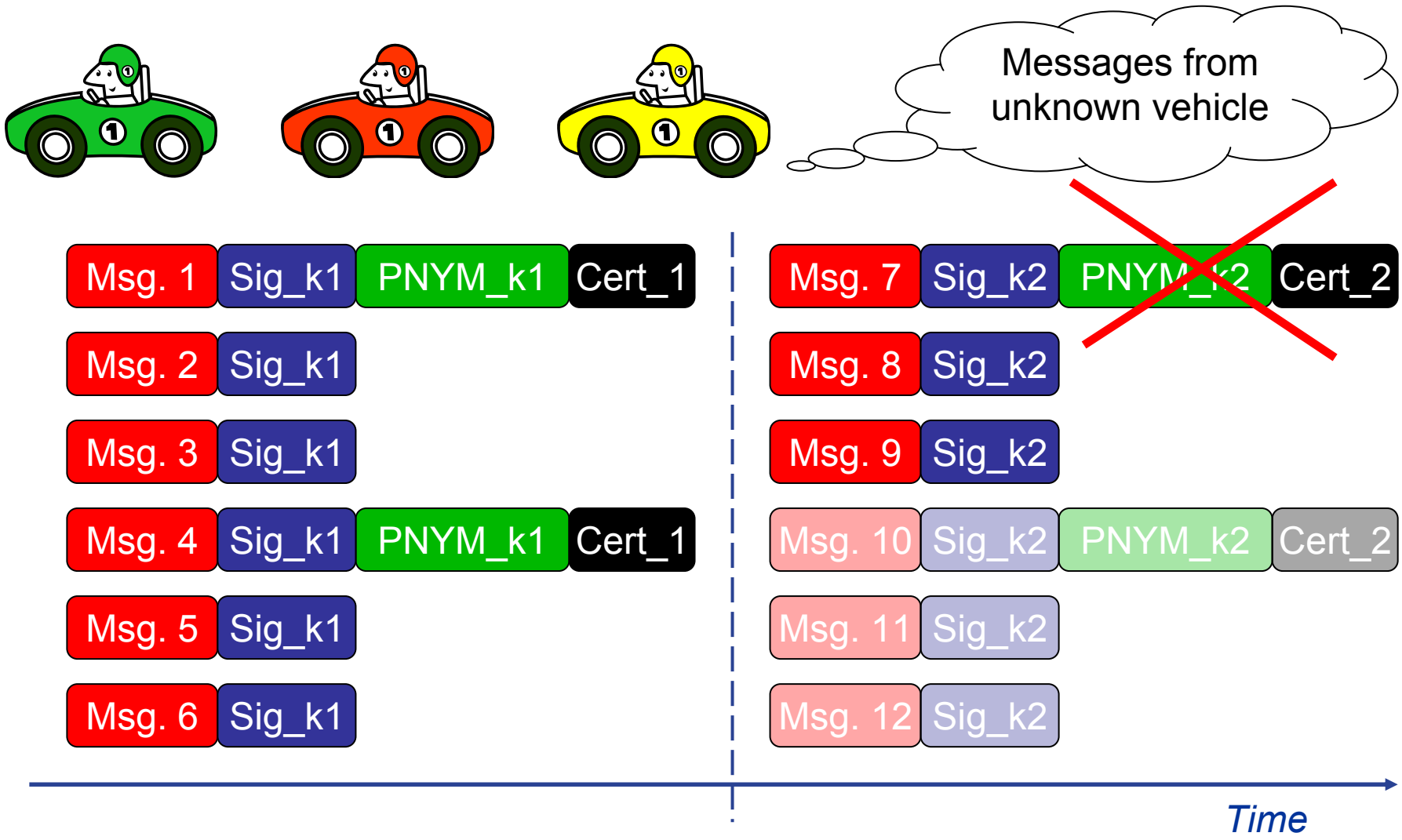
Reducing SVC cost - Optimization (3)



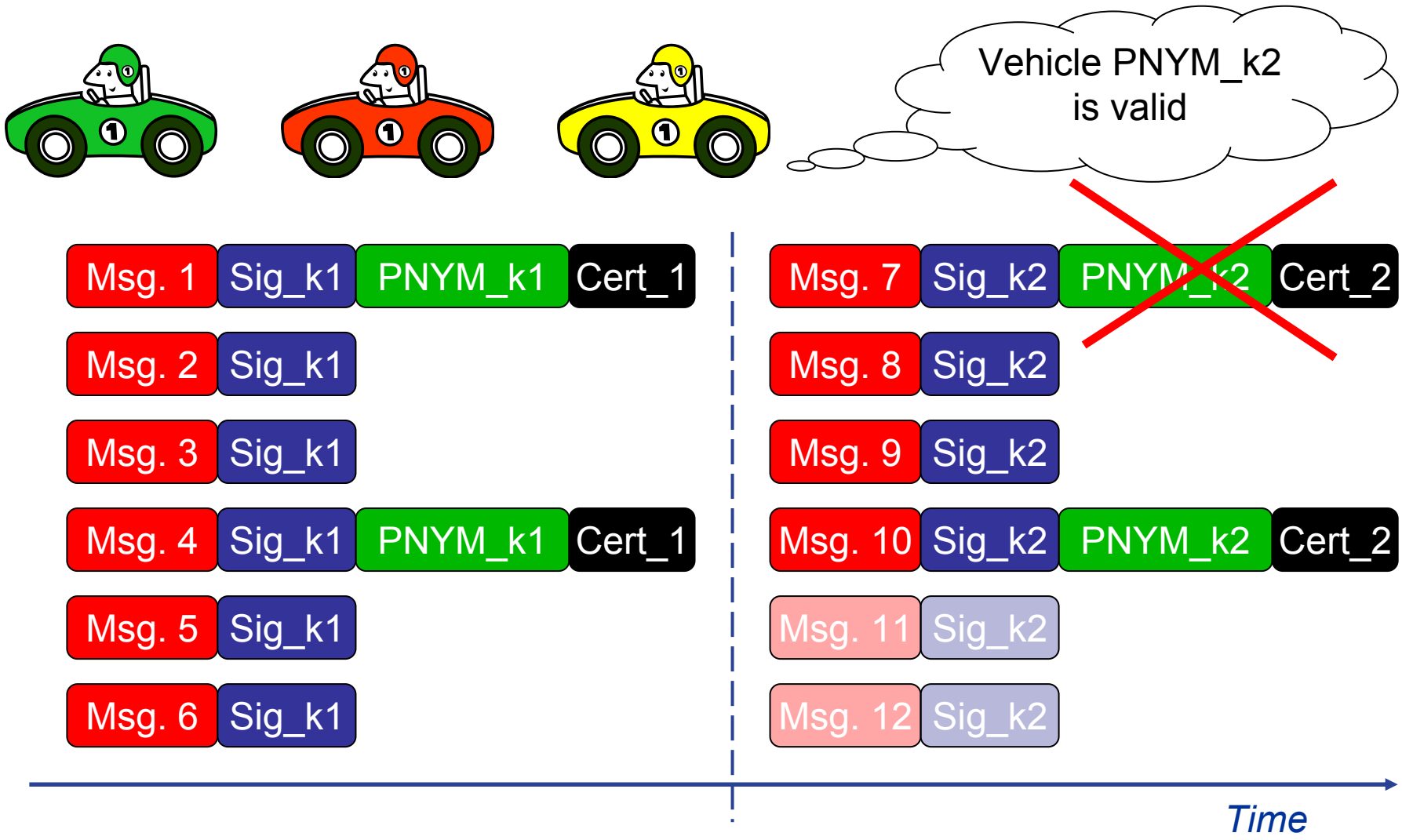
Reducing SVC cost - Optimization (3)



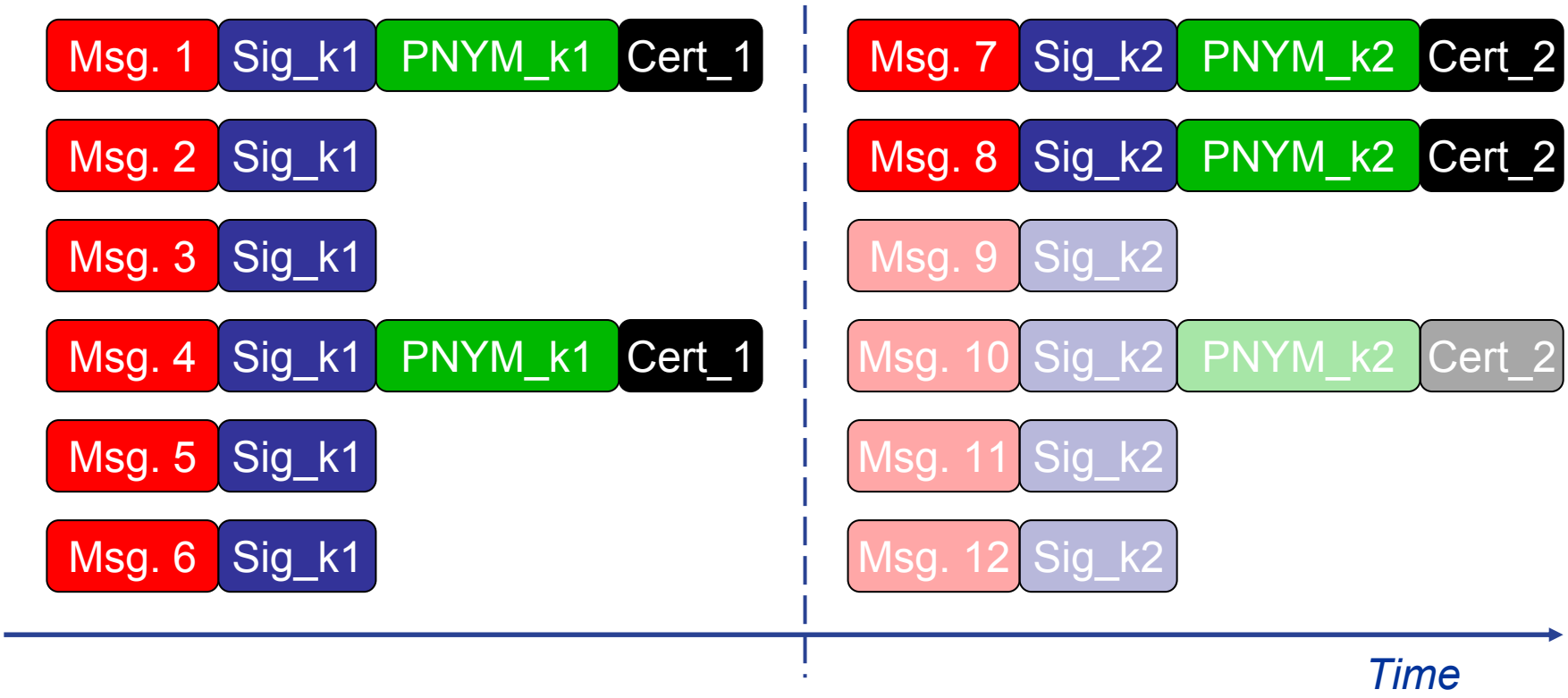
Reducing SVC cost - Optimization (3)



Reducing SVC cost - Optimization (3)



Reducing SVC cost - Optimization (3)



Reducing SVC cost - recap

1. Certify and validate a pseudonym once during its lifetime
2. Append the certificate once every α messages
   - α = *certificate period*
3. When a new pseudonym is issued, transmit the certificate for *p* consecutive messages
   - *β = push period*

Pseudonymous authentication (cont'd)

- Managing a pseudonymous authentication system is cumbersome
  - Preload large numbers of pseudonyms or obtain them on-the-fly
    - Costly computations at the side of the pseudonym provider
    - Costly wireless communication to obtain pseudonyms
  - Need reliable access to the pseudonym provider

- Solution: On-board generation of pseudonyms

Group signatures

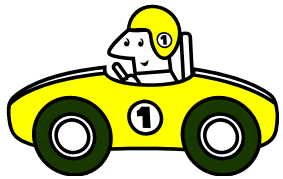
Group A

Group member signing keys

Group A public key

gsk_1

gsk_2



gsk_3

Valid signature from a legitimate member of Group A

??? Member ???

Hybrid scheme

- Combine
  - Pseudonymous authentication (Baseline Pseudonym (BP) approach) and
  - Group Signatures (GS)
- All legitimate vehicles belong to the same group
- Each node is equipped with a secret *group signing key* and the *group public key*

G. Calandriello, **P. P.**, A. Lloy, and J.-P. Hubaux, "Efficient and Robust Pseudonymous Authentication in VANET," ACM VANET 2007

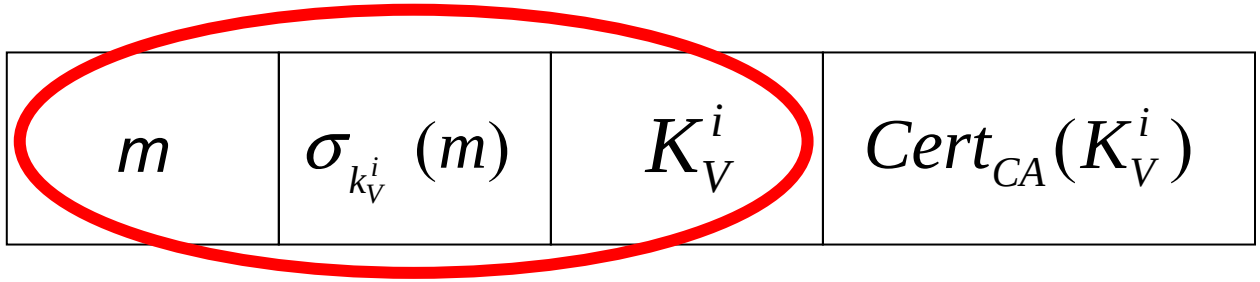
Hybrid scheme (cont'd)

- Each node
  - Generates its own pseudonyms and signs them with a Group Signature
    - GS act as a self-generated certificate
  - Uses the private key corresponding to the pseudonym to sign messages
    - As in the baseline approach
  - Appends the self-generated certificate
    - As in the baseline approach

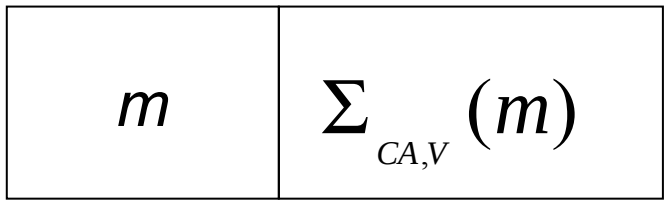
Hybrid scheme (cont'd)

- Message formats

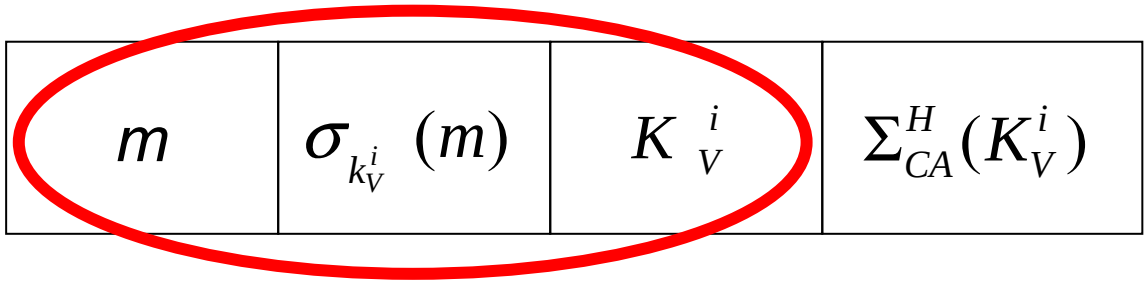
Baseline (BP)



Group Signature (GS)



Hybrid



Evaluation

- Setup
  - EC-DSA as basic signature algorithm
  - Group Signatures as proposed in: D. Boneh and H. Shacham, Group Signatures with verifier-local revocation, ACM CCS 2004
  - Security level of 80 bits for message signatures and 128 bits for certificates
- Benchmarks
  - Reference CPU: 1.5 GHz Centrino
  - OpenSSL for EC-DSA
  - Group Signatures implementation not available
    - Calculated the number of 32-bit word multiplications required for GS and benchmarked the multiplication operation

Cryptographic cost

Signature Scheme	Sign (sec)	Verify (sec)	Sig. size (bytes)	Pub. key (bytes)	Priv. key (bytes)
EC-DSA	8e-4	4.2e-3	64	33	32
GS	5.37e-2	4.93e-2	225	800	64

Computation cost

- Processing delay computed over one pseudonym lifetime $\tau = 60$ sec
- Optimization 1 in place for Hybrid

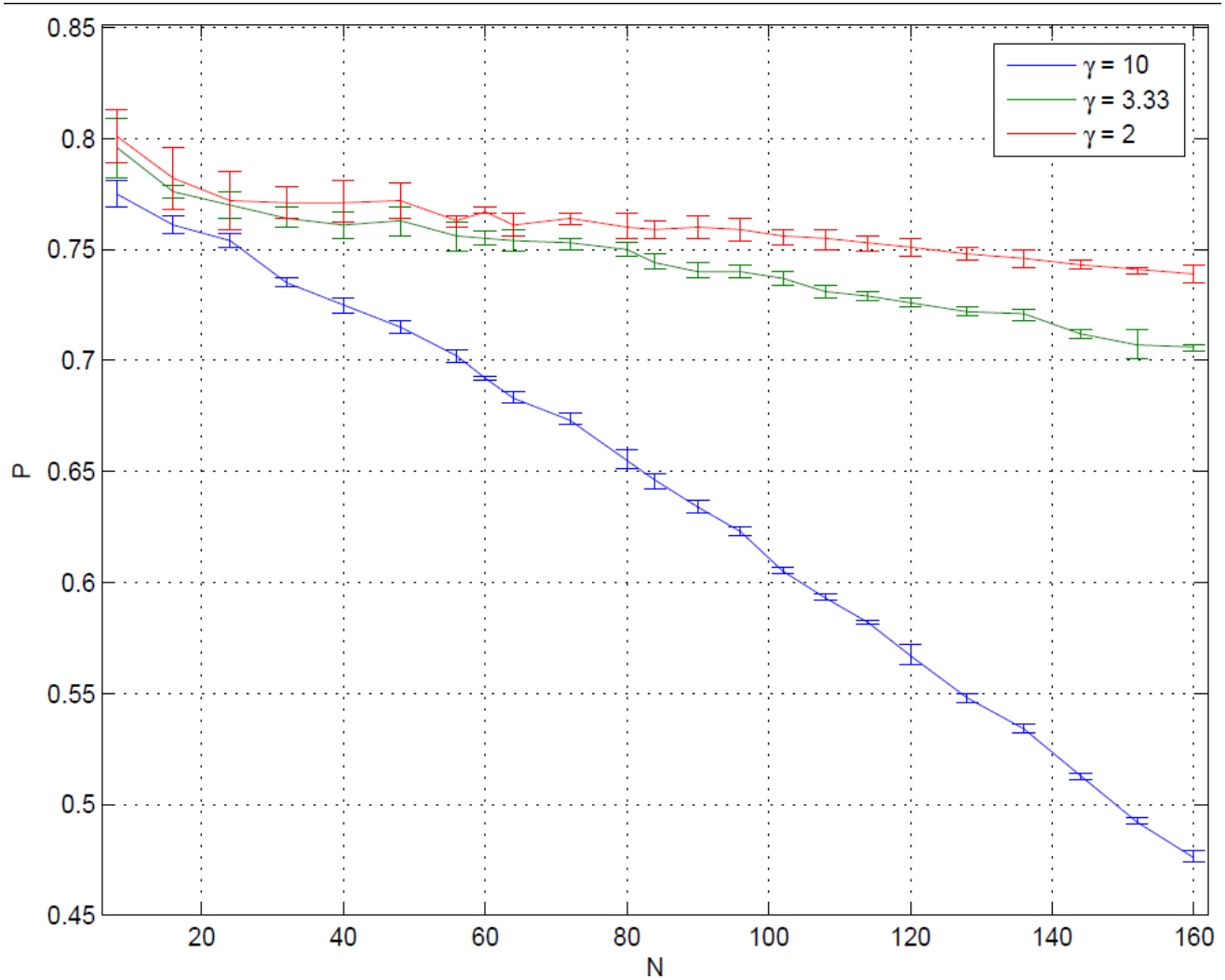
Scheme	Sign (sec)	Verify (sec)	Overhead (bytes)
BP	5e-4	3e-3	137
GS	1.78e-2	1.56e-2	225
Hybrid	5.9e-4	3.1e-3	298

Communication Overhead

- Optimization 2 in place
- GS has a constant overhead of 225 bytes
- Values below in bytes

Scheme \ α (msg)	1	5	10	15
BP	141	70	61	58
Hybrid	302	102	77	69

Communication overhead (cont'd)



Communication reliability (P) as a function of the neighborhood size (N); γ: beaconing rate

Processing power

- Time divided into *slots*
  - 1 slot = 100 ms
- Vehicles generate 1 beacon per slot
- 8 lanes
  - 160 neighbors for a given receiver R
  - 80 of interest
- Hybrid security scheme with optimizations
- How many verifications per slot?

Processing power (cont'd)

	Sign **(ms)**	Verify **(ms)**	Overhead **(bytes)**
BP ***LONG***	1.3	7.2	141
Hybrid ***LONG***	54.2	52.3	302
SHORT	0.5	3	48

G. Calandriello, **P. P.**, J.-P. Hubaux, A. Lioy, Efficient and Robust Pseudonymous Authentication in VANET, VANET 2007

D. Boneh, H. Shacham, Group Signatures with verifier-local Revocation, CCS 2004

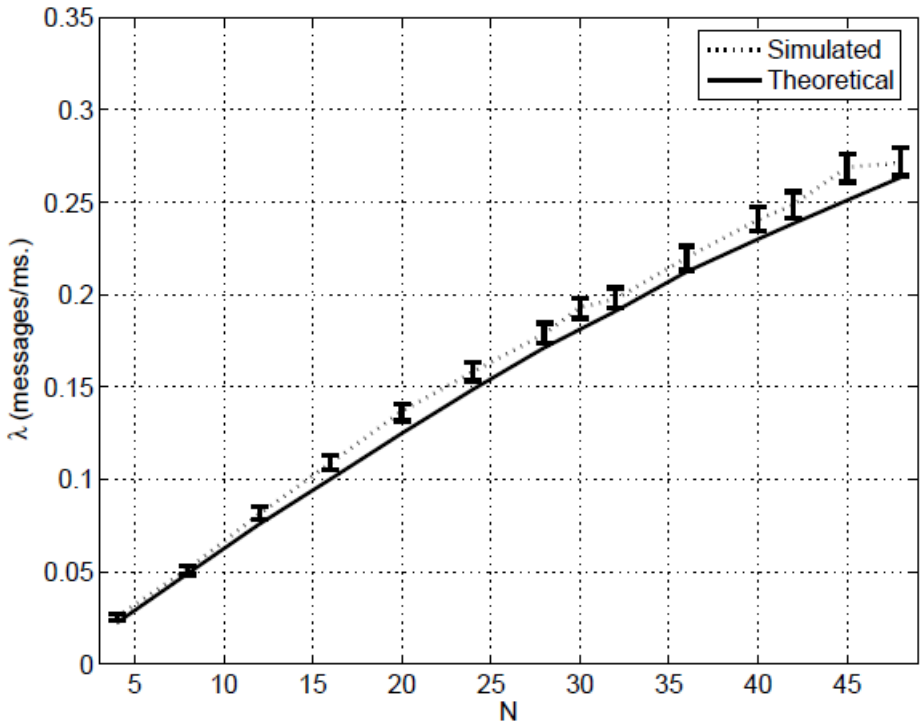
IEEE 1363a – IEEE standard specifications for public-key cryptography, 2004

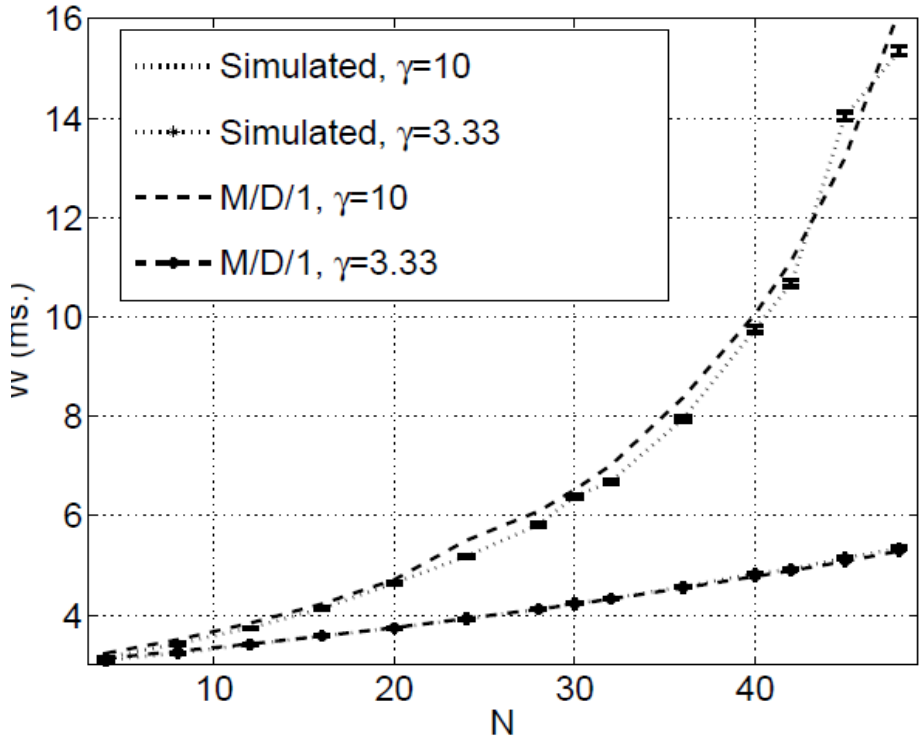
Processing power (cont'd)

	Packets per 100 ms
BP ***LONG***	13.9
Hybrid ***LONG***	1.9
SHORT	33.3

- Use of pure GS is not feasible
- Hybrid scheme
  - One LONG message per vehicle and per pseudonym lifetime
  - SHORT packets are the dominant factor
- System is at the limit of stability

Processing power (cont'd)





2-class M/D/1 queue

$$W_i = t_i + \frac{\sum_{i=1}^{r} \lambda_i t_i^2}{2(1-\rho)} \qquad \rho = \sum_{i=1}^{r} \rho_i \text{ and } \rho_i = \lambda_i t_i$$

Message verification delay, for short packets; α= 10, β= 0, τ= 60; HP scheme; λ for the same setup and for γ=10 beacons/sec

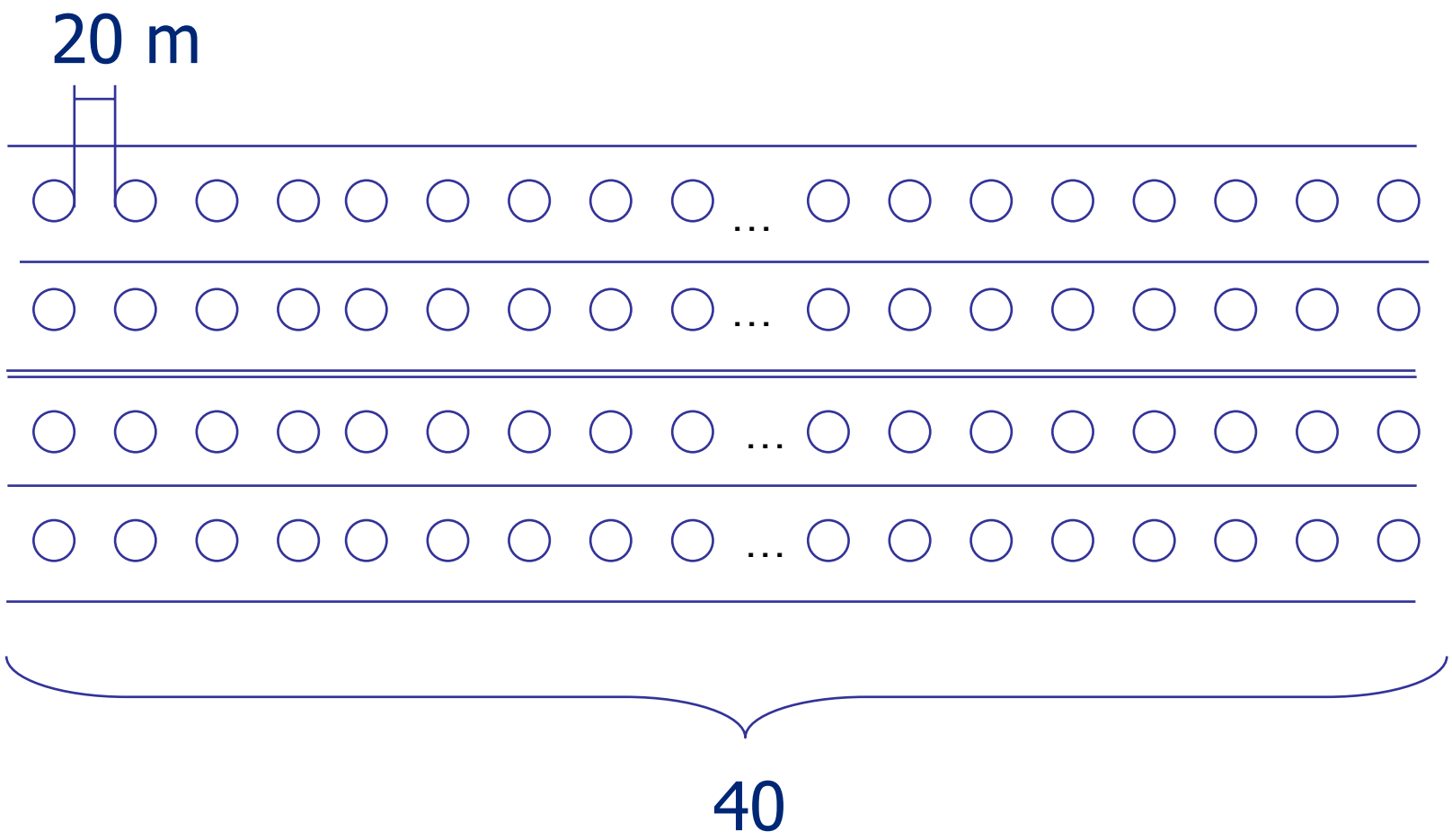
SVC and transportation safety

- Emergency braking
- Platoon on 100 cars on one lane
  - Average spacing: 20 m
  - Average speed: 80 Km/h
  - Wet road
    - Braking capability: 4 m/s^2
  - Driver reaction 0.75 – 1.5 s
  - Pseudonym lifetime 60 s
  - Emergency event at the head after 60 s
  - No lane change

P. P., G. Calandriello, A. Lioy, and J.-P. Hubaux, "Impact of Vehicular Communication Security on Transportation Safety," IEEE INFOCOM MOVE 2008

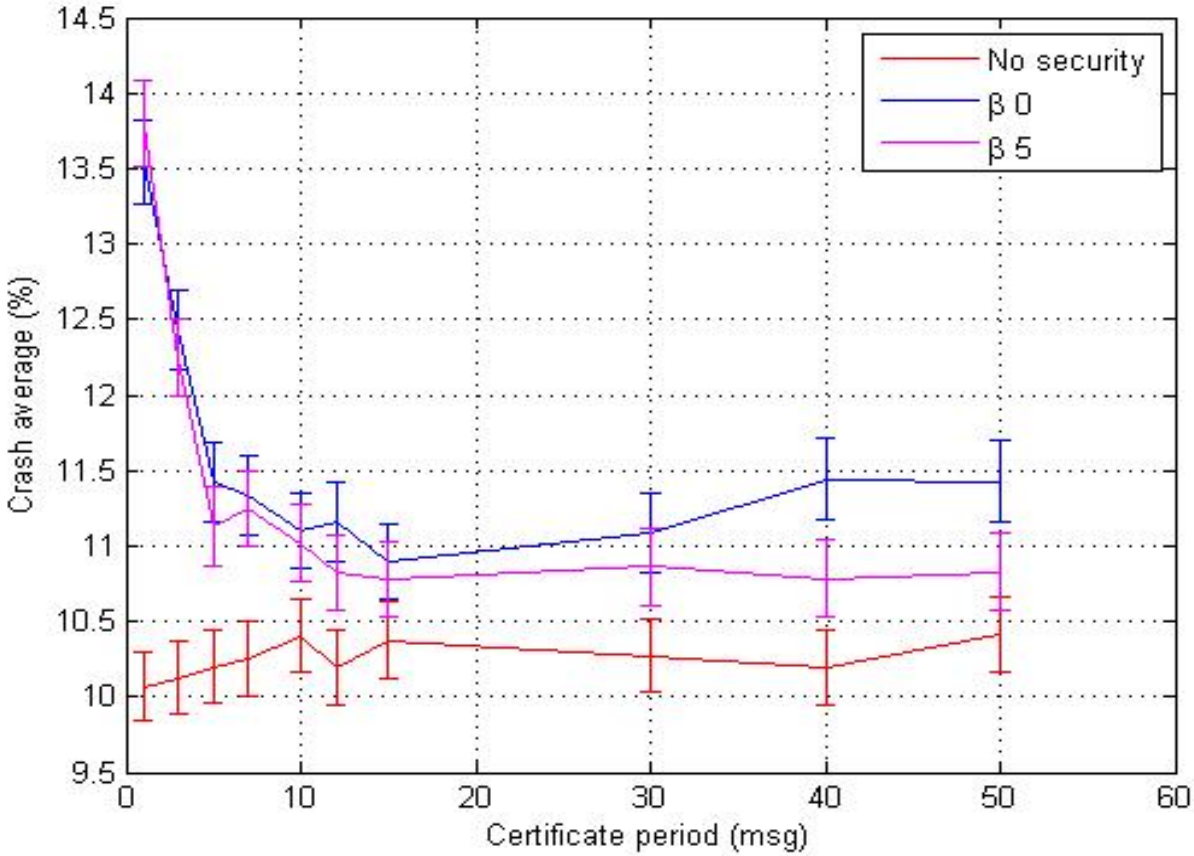
Extended journal version: in submission to IEEE TDSC

SVC and transportation safety (cont'd)



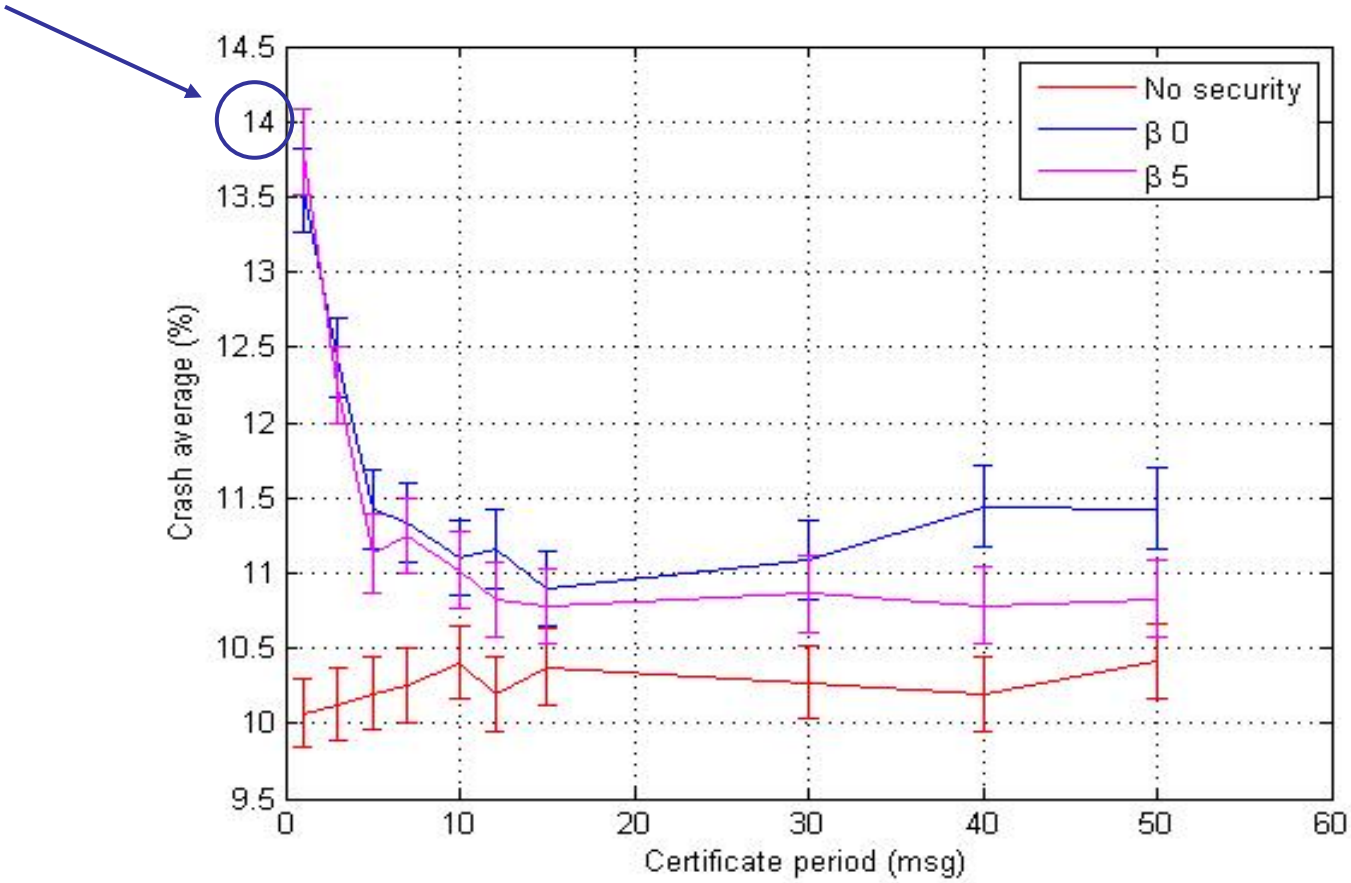
Intended transmission range = 200 m

SVC and transportation safety (cont'd)



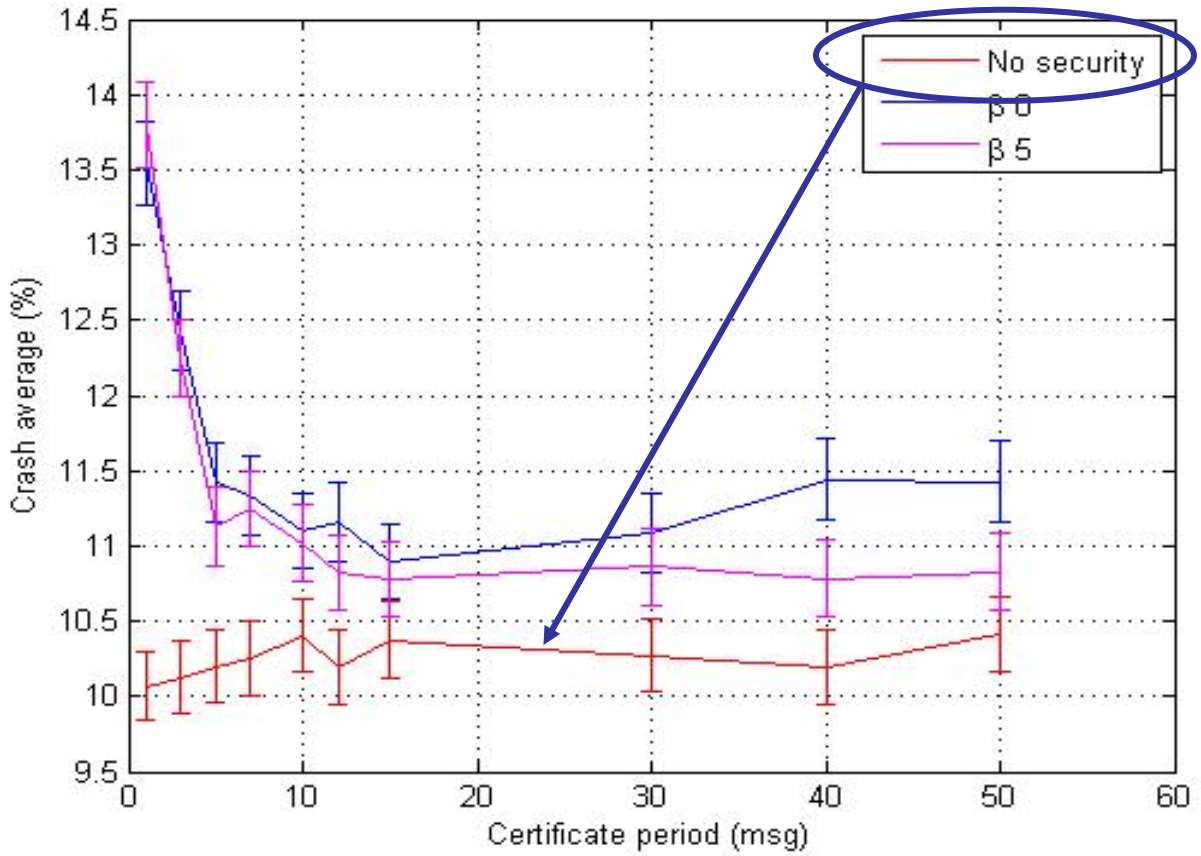
Hybrid scheme, 8 lanes

SVC and transportation safety (cont'd)



Crash average is 80-100% without V2V communications

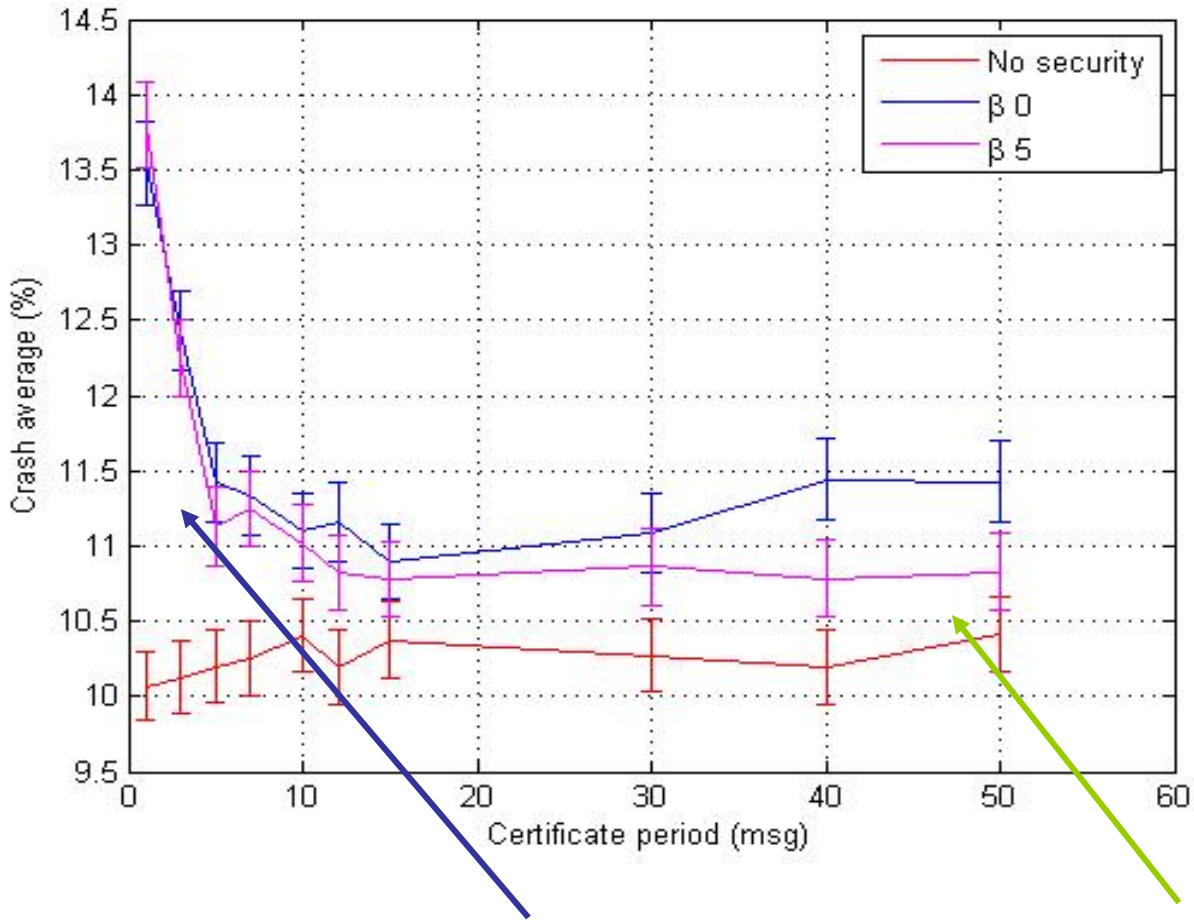
SVC and transportation safety (cont'd)



Lowest network overhead

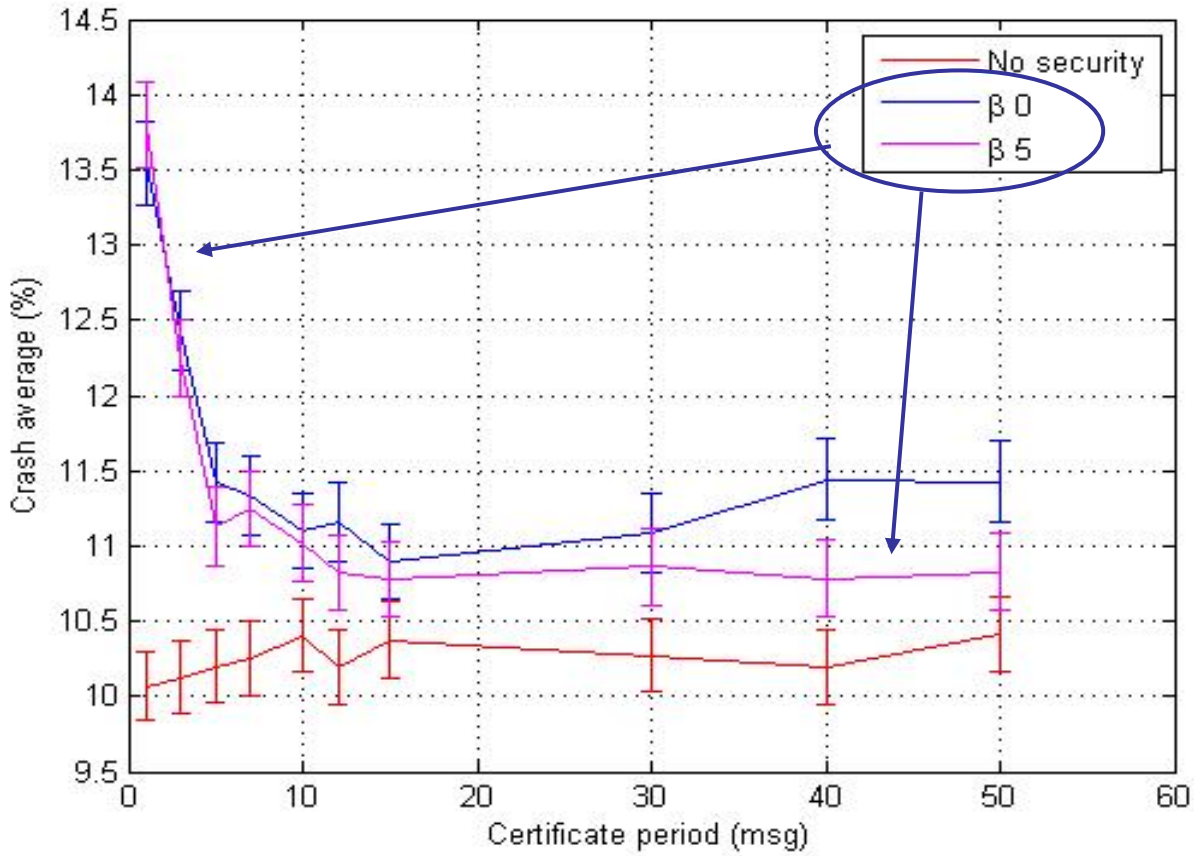
No restrictions on which messages can be validated

SVC and transportation safety (cont'd)



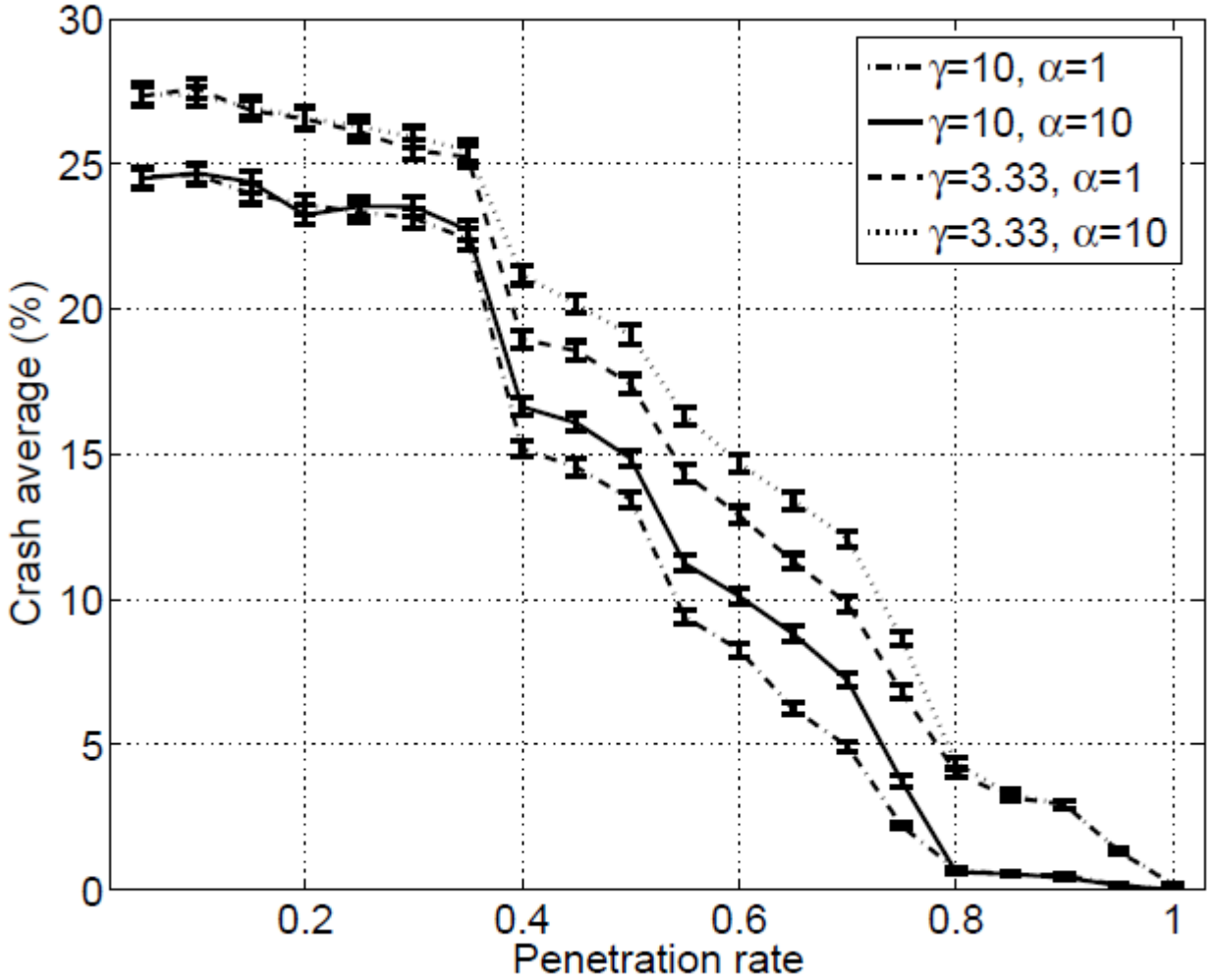
α influences **channel load** and **authentication delay**

SVC and transportation safety (cont'd)



Pushing certificates at PNYM changes reduces authentication delay, especially for high values of α

SVC and transportation safety (cont'd)



Penetration rate and effectiveness

System building: Secure VC

- Field demonstration, Dudenhofen, October 2008, Car to Car Communication Consortium (C2C-CC)
- SeVeCom demonstrator

M. Gerlach, F. Friederici, P. Ardelean, and **P. P.**, “Security Demonstration,” C2C-CC Forum and Demonstration, Dudenhofen, Germany, October 2008

P. Ardelean and **P. P.**, "Secure and Privacy-Enhancing Vehicular Communication," Demo, IEEE WiVeC, Calgary, AL, Canada, September 2008

System building: Secure VC (cont'd)

System building: Secure VC (cont'd)

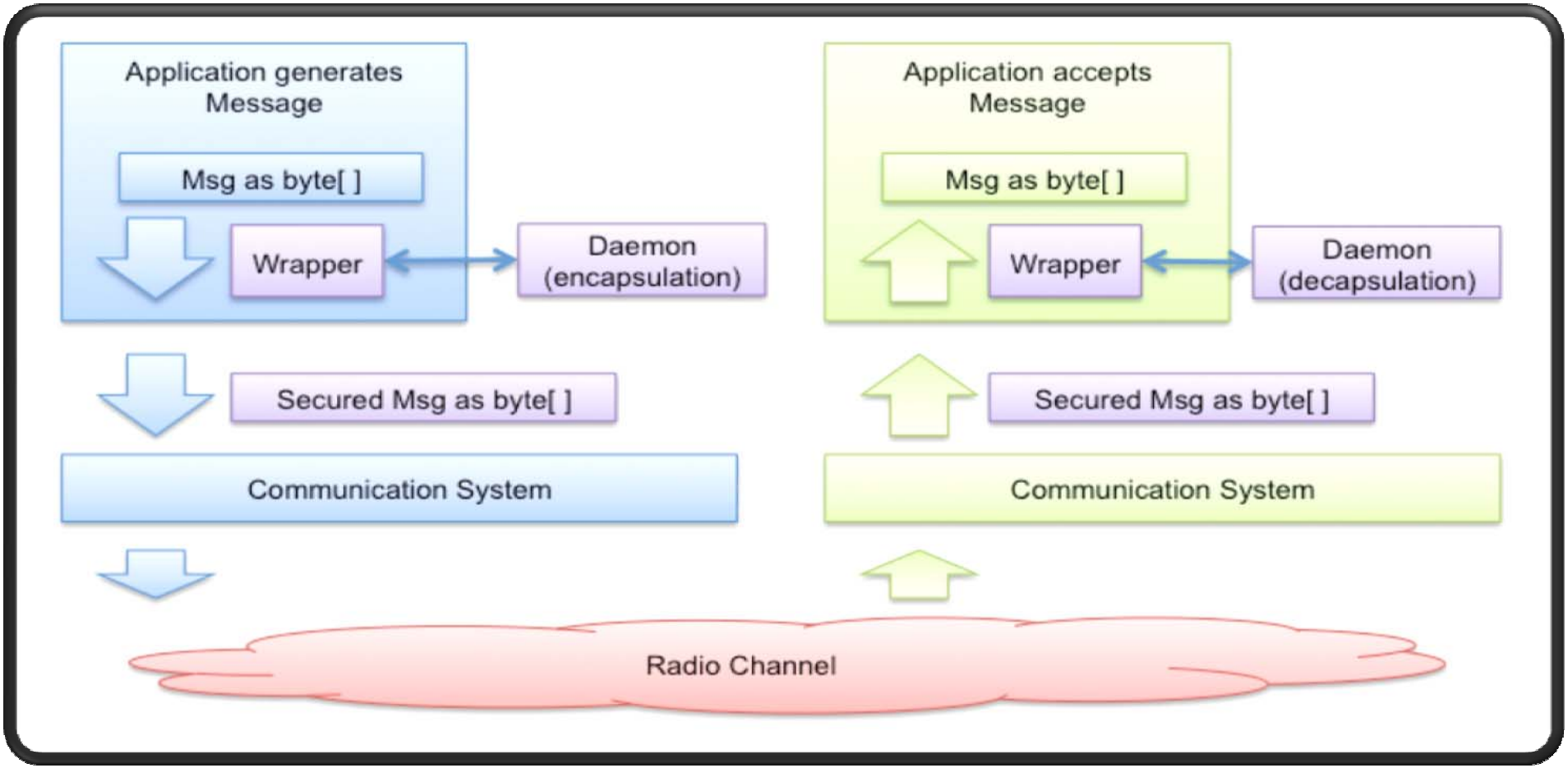
System building: Secure VC (cont'd)

System building: Secure VC (cont'd)

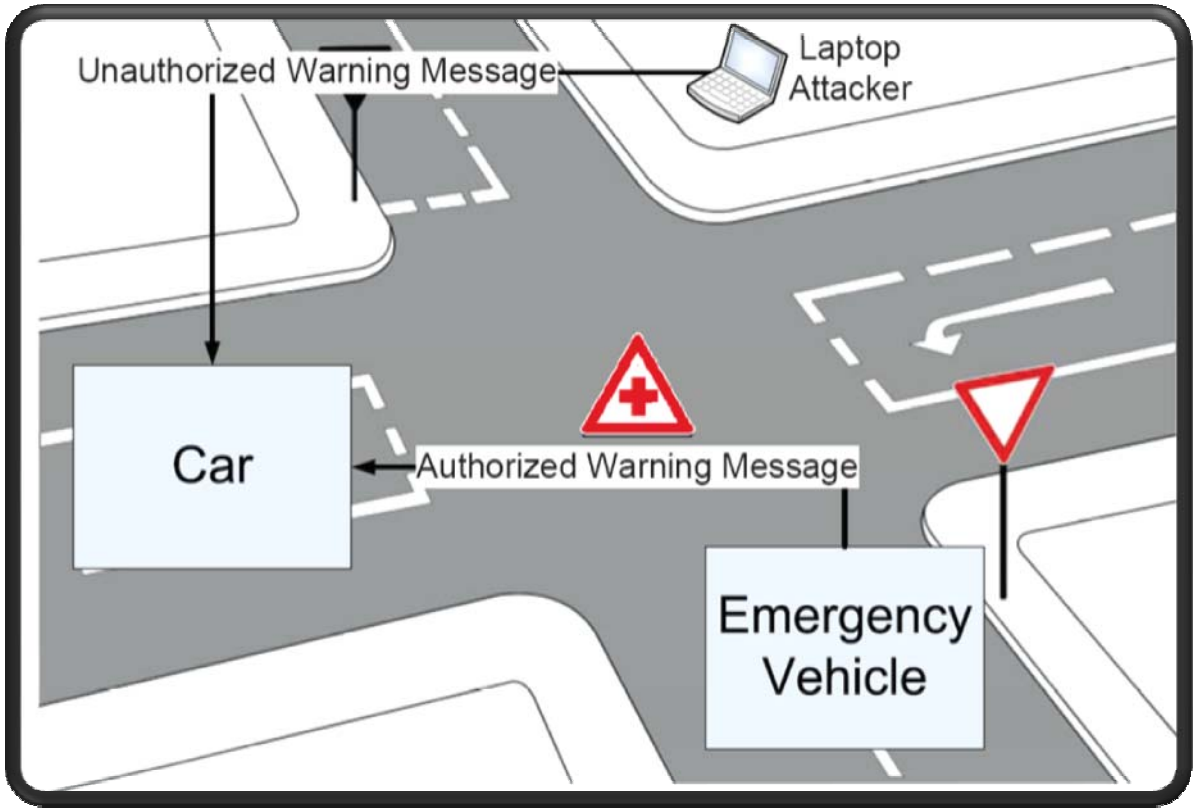
System building: Secure VC (cont'd)

System building: Secure VC (cont'd)

- Security SW for C2C-CC field demo



System building: Secure VC (cont'd)



Laptop attacker

- Security use case: impersonation of an emergency vehicle

Recap

- Addressed problems
  - Identity and key management
  - Secure communication
  - Privacy enhancing technologies
- Challenge: New important topics to address
- Response: Encouraging initial results

P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communications: Design and Architecture," IEEE Communications Magazine, November 2008

F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, B. Wiedersheim, E. Schoch, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communications: Implementation, Performance, and Research Challenges," IEEE Communications Magazine, November 2008

Standardization expectations

- SeVeCom
  - Detailed specification and system architecture
  - Integration of the SeVeCom system into the CVIS system
  - Influence of standardization activities
- IEEE 1609.2 Working Group
  - Part of a broader effort on VC protocols
  - Standardization effort
  - Focus: Vehicle to Infrastructure Communication, Security and Privacy Enhancing mechanisms

Standardization expectations (cont'd)

- Car-to-Car Communication Consortium
  - Security Working Group
  - Security and privacy enhancing mechanisms for VC, in-car security
  - Contributions to and interactions with SeVeCom and ETSI
  - Preparation of architecture document ('white paper') – currently internal

Standardization expectations (cont'd)

- ETSI (European Telecommunications Standards Institute)
  - Efforts of various aspects of VC (e.g., PHY, MAC), ITS WG
  - Recently formed STF on security
- ISO-TC204 WG16, CALM
    - Standardized set of air interface protocols and parameters for medium and long range comm.
- eSafety eSecurity Working Group
  - Coordination
  - Collaboration with Article 29

Conclusions

- Importance of security is broadly understood
- Multiple efforts are on-going
- Interoperability
- Standardization efforts have focused on a basic yet relatively small set of mechanisms
  - This is nonetheless positive, especially because security has come into the broader picture early
  - Most likely, standardization will cover few message formats, a certificate format

Conclusions (cont'd)

- Broadening of the standardization efforts, to cover additional components of a security architecture for secure vehicular communication systems
  - Progressively easier
    - VC systems are getting more mature
    - Security schemes are being developed and evaluated
  - The need is increasingly understood
- Question marks
  - Coordination around the globe
  - Other pressing priorities in the industry