



Securing Vehicular Communication Systems: Results and Next Steps

Panos Papadimitratos

<http://people.epfl.ch/panos.papadimitratos>

SE-cure VE-hicle COM-munication

- SEVECOM
 - <http://www.sevecom.org>



	Topic	Scope of work
A1	Key and identity management	Fully addressed
A2	Secure communication protocols	Fully addressed
A3	Tamper proof device	Fully addressed
A4	Intrusion Detection	Investigation work
A5	Data consistency	Investigation work
A6	Privacy	Fully addressed
A7	Secure positioning	Investigation work
A8	Secure user interface	Investigation work

Security Baseline Architecture



- Requirements
 - Authentication, Integrity, Non-repudiation, Access control, Confidentiality
 - Availability
 - Privacy
 - Liability identification

P. P., V. Gligor, J.-P. Hubaux, "Securing Vehicular Communications – Assumptions, Requirements and Principles," ESCAR 2006

F. Kargl, Z. Ma, E. Schoch , "Security Engineering for VANETs ," ESCAR 2006

Security Baseline Architecture (cont'd)

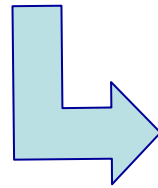


- Objectives
 - Focus on communication
 - Baseline Privacy Enhancing Technology (PET)
 - Future dynamic deployment of stronger PETs
- Baseline solution design approach
 - Standardized cryptographic primitives
 - Easy-to-implement
 - Low overhead
 - Adaptable protection

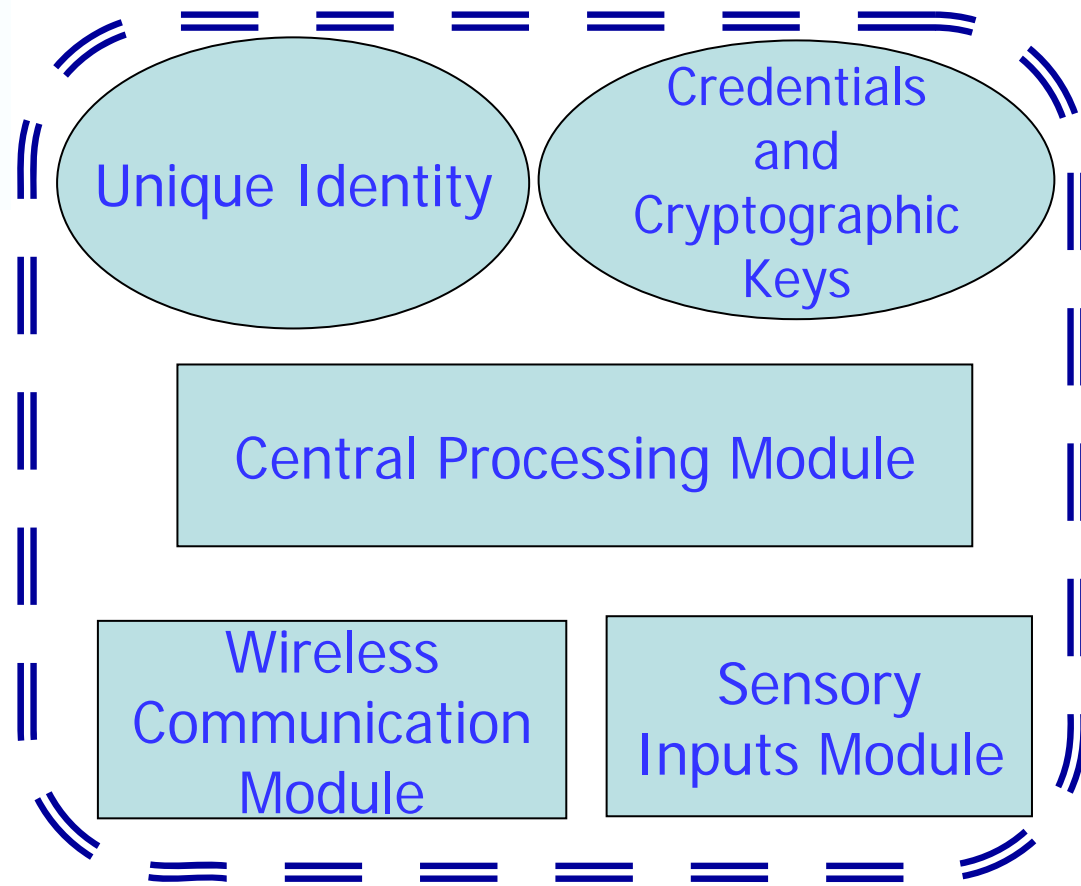
P. P., L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, M. Raya, Architecture for secure and private vehicular communications, ITST 2007

Security Architecture and Mechanisms for V2V / V2I, SEVECOM Deliverable D.2.1

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 $\text{Cert}_{CA}(V, K_V, A_V, T)$
 - A_V : attributes of node V
 - T : lifetime

Secure VC system entities (cont'd)

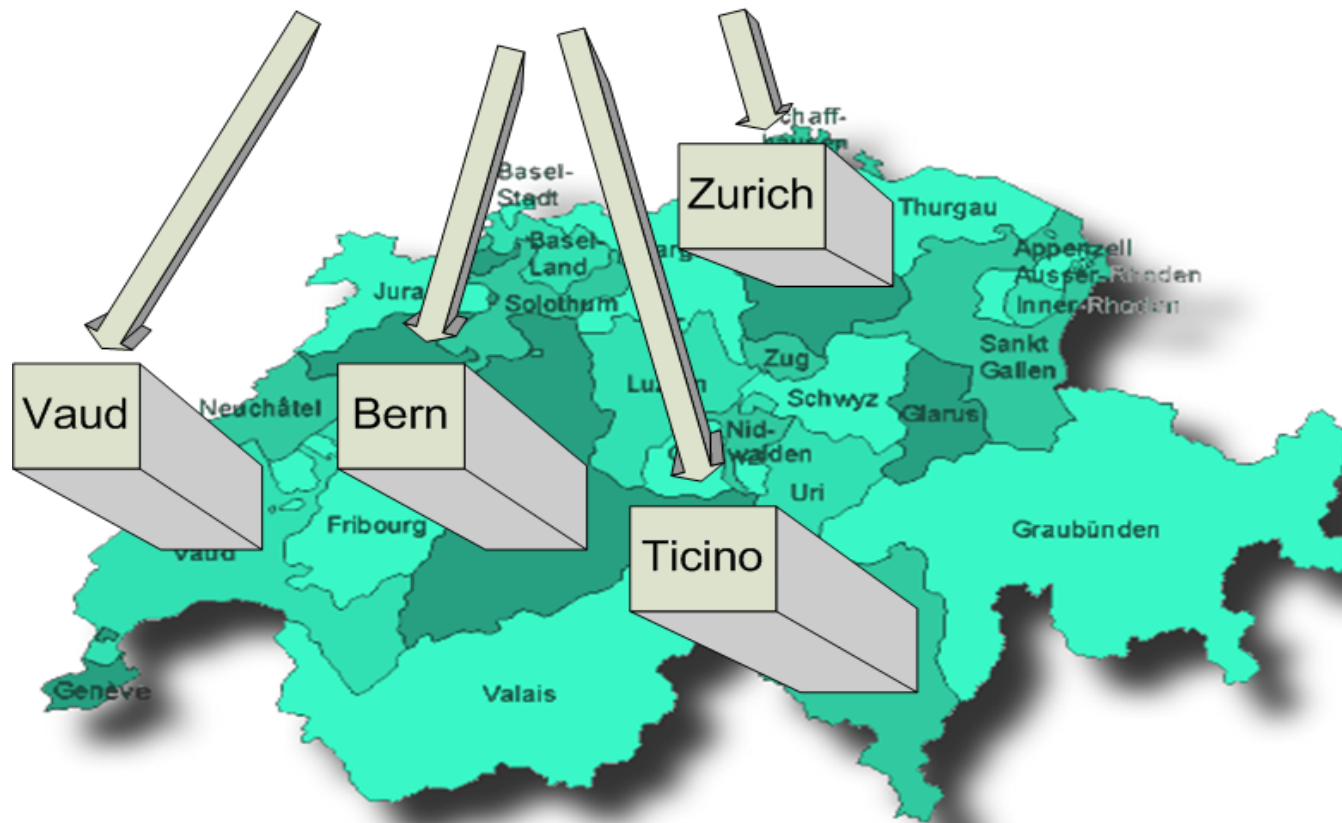
9/28/2006

Higher Level or Other Authority

- Authority

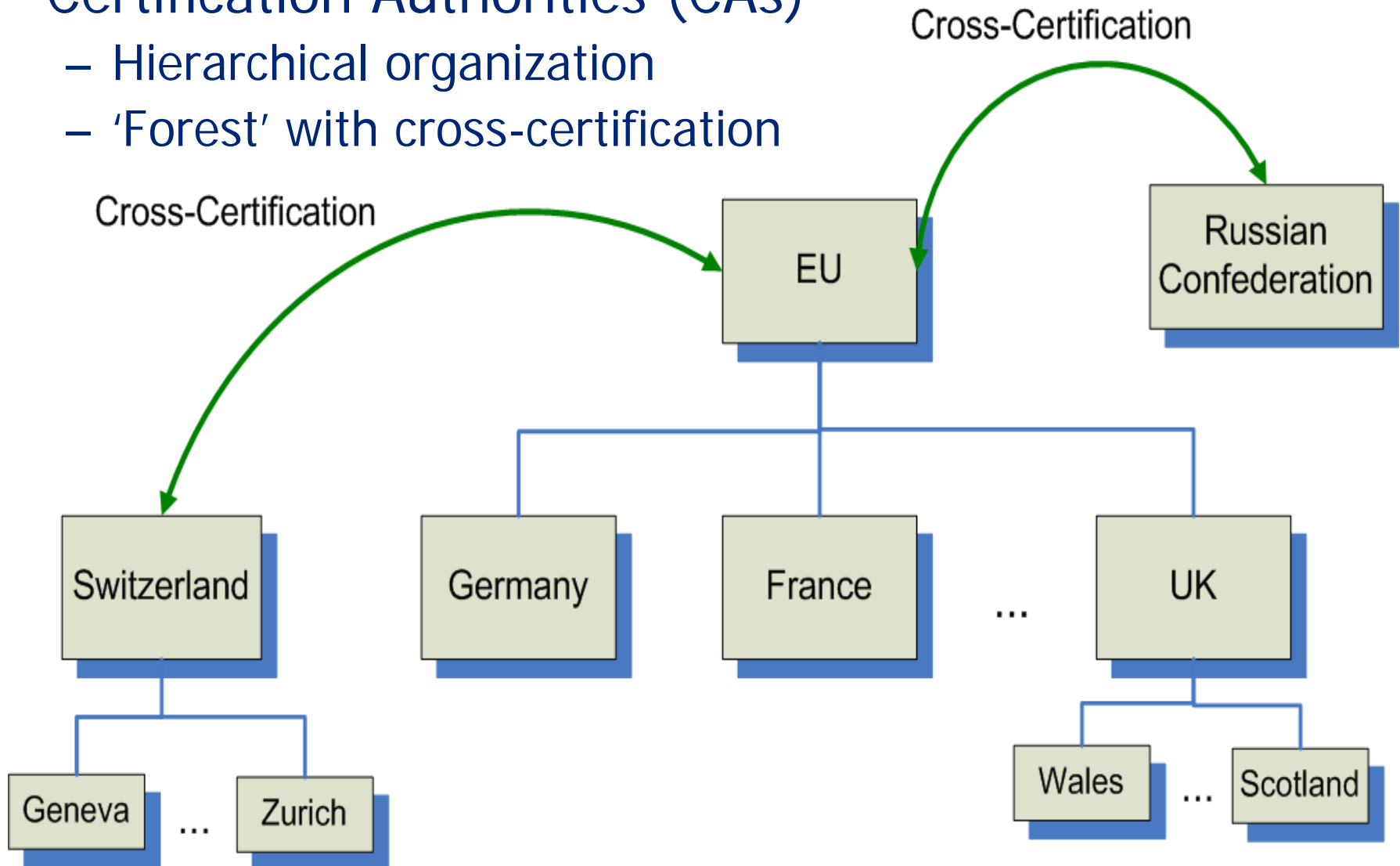
Swiss Automobile Services

9/28/2006

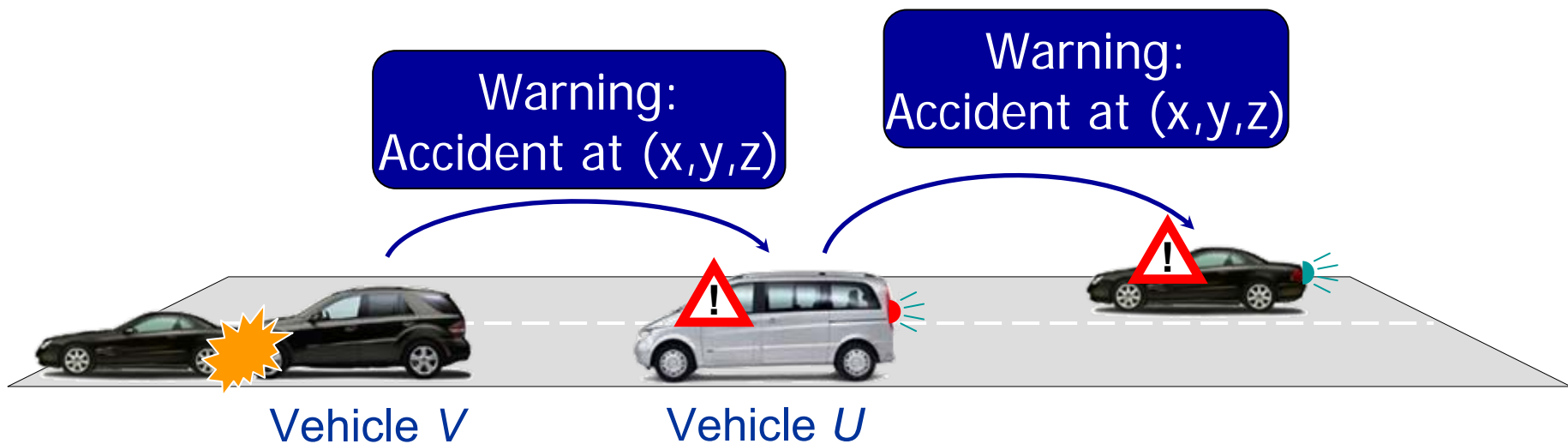
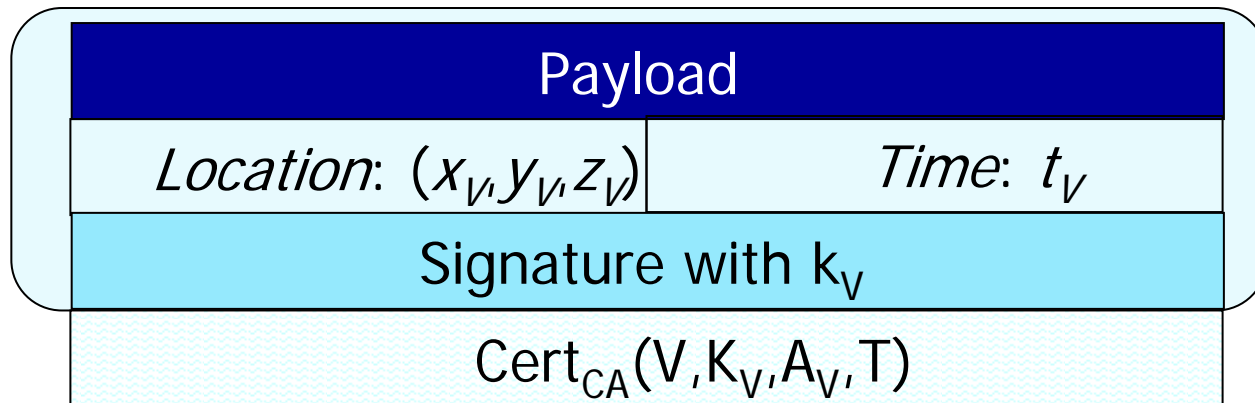


Secure VC system entities (cont'd)

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



Secure communication

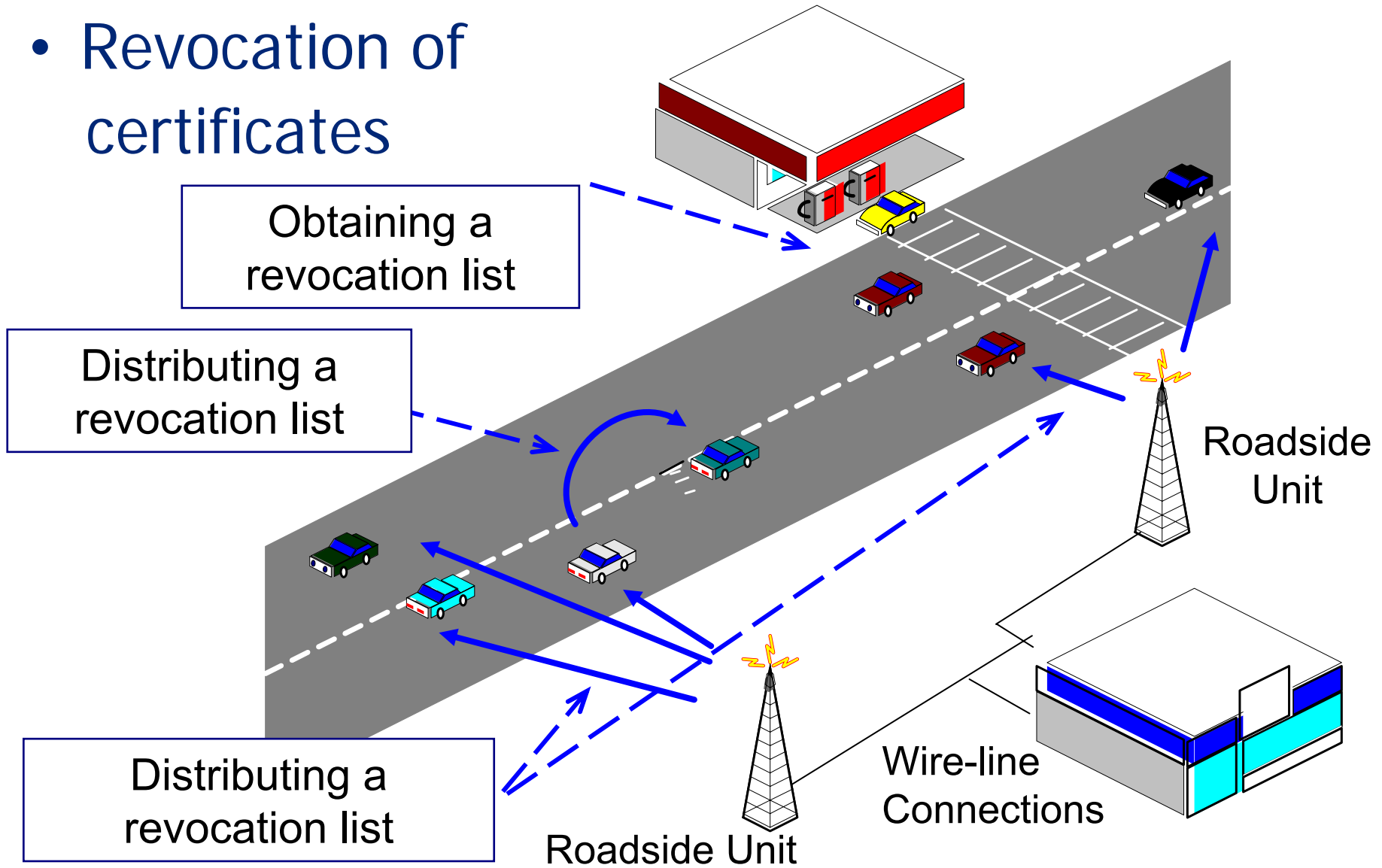


Secure communication (cont'd)

- Single- and multi-hop
- Digital signatures more appropriate tool
 - Any-to-any communication; e.g., broadcast, geo-cast
 - High mobility
 - Signatures hop-by-hop and from the originator
 - C. Harsch, A. Festag, and P. P., "Secure Position-Based Routing for VANETs," IEEE VTC 2007-Fall
- Still, a node with valid credentials can inject false data

Eviction of faulty nodes

- Revocation of certificates



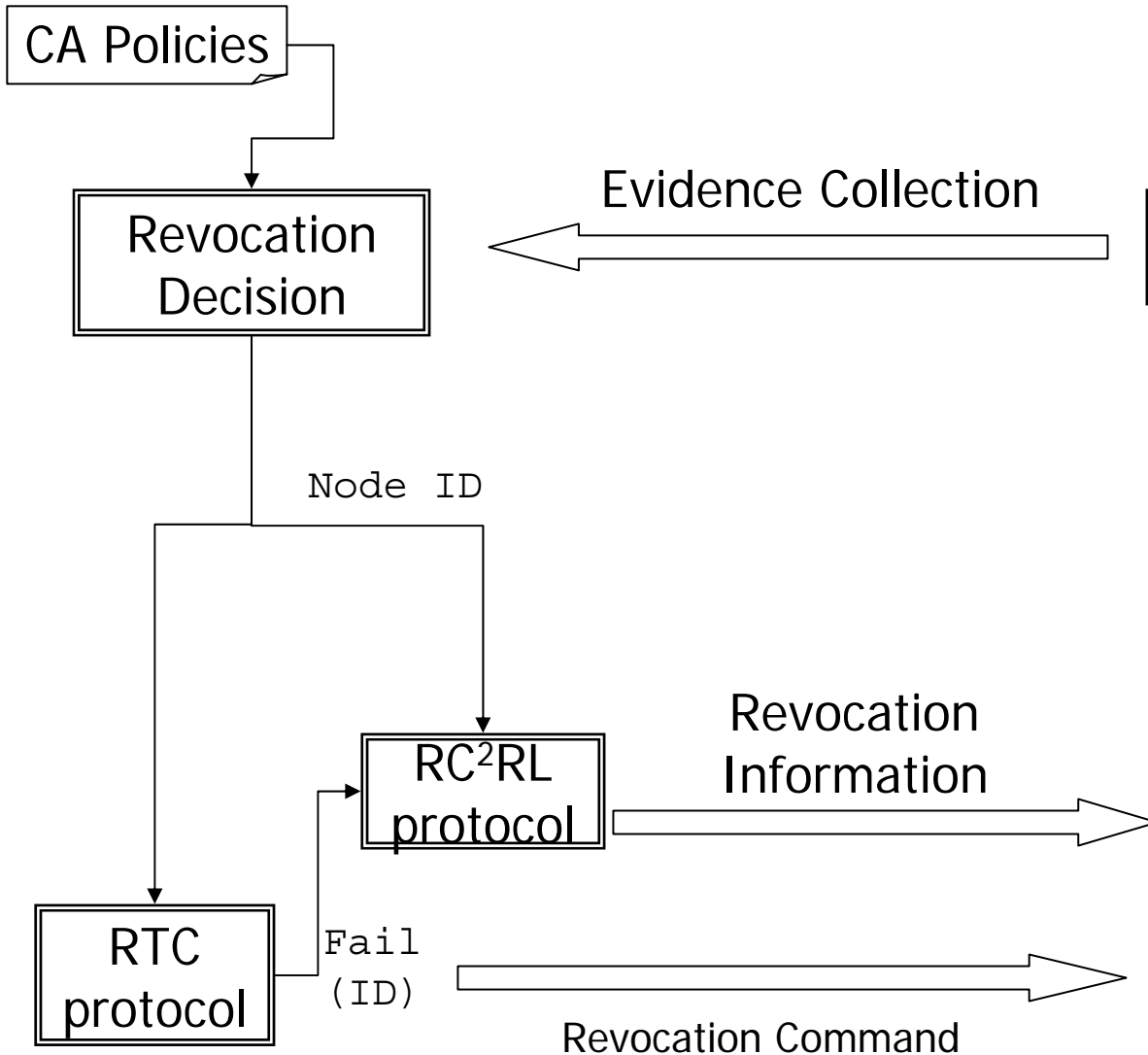
Eviction of faulty nodes (cont'd)

- Challenge
 - Identify faulty nodes and remove them from the network
- Basic ideas
 - Detect misbehaving or faulty nodes in proximity
 - Contribute to the collection of faulty behavior evidence
 - Use locally such detection for self-protection, by ignoring messages originating from nodes suspected to be faulty
 - Only the CA has the power to revoke the credentials of a node

M. Raya, P. P., I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," IEEE JSAC, 2007

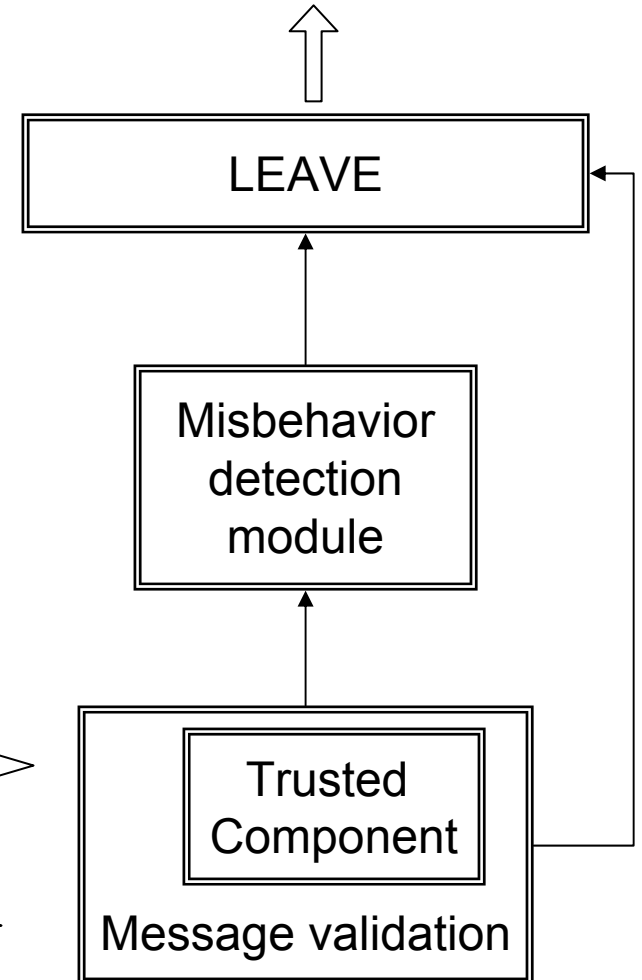
Eviction of faulty nodes (cont'd)

CA and Infrastructure Functionality



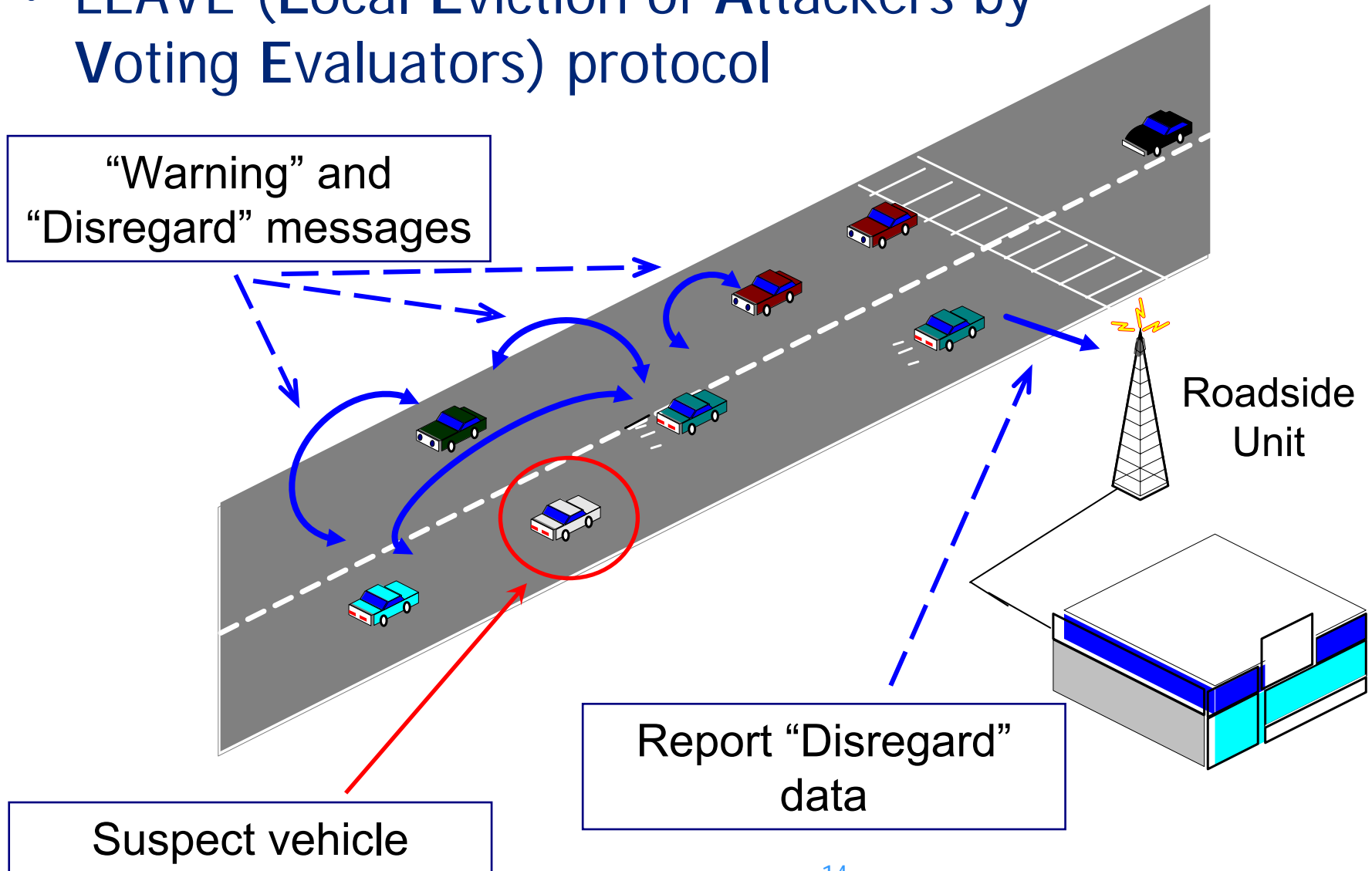
Vehicle Functionality

Local Warning Messages

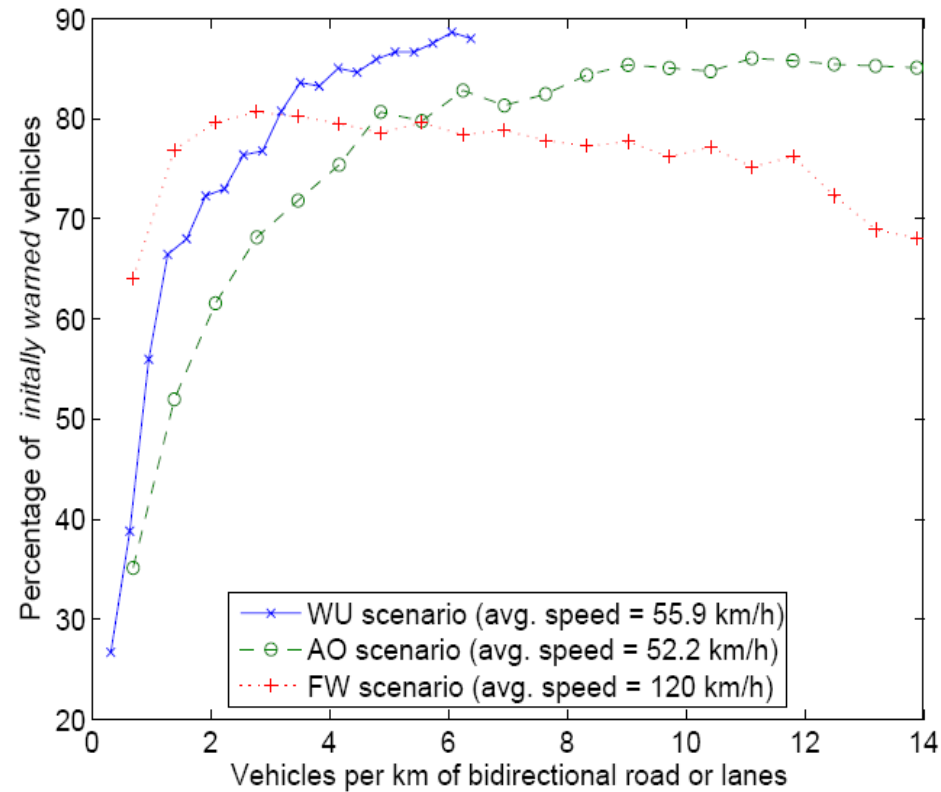
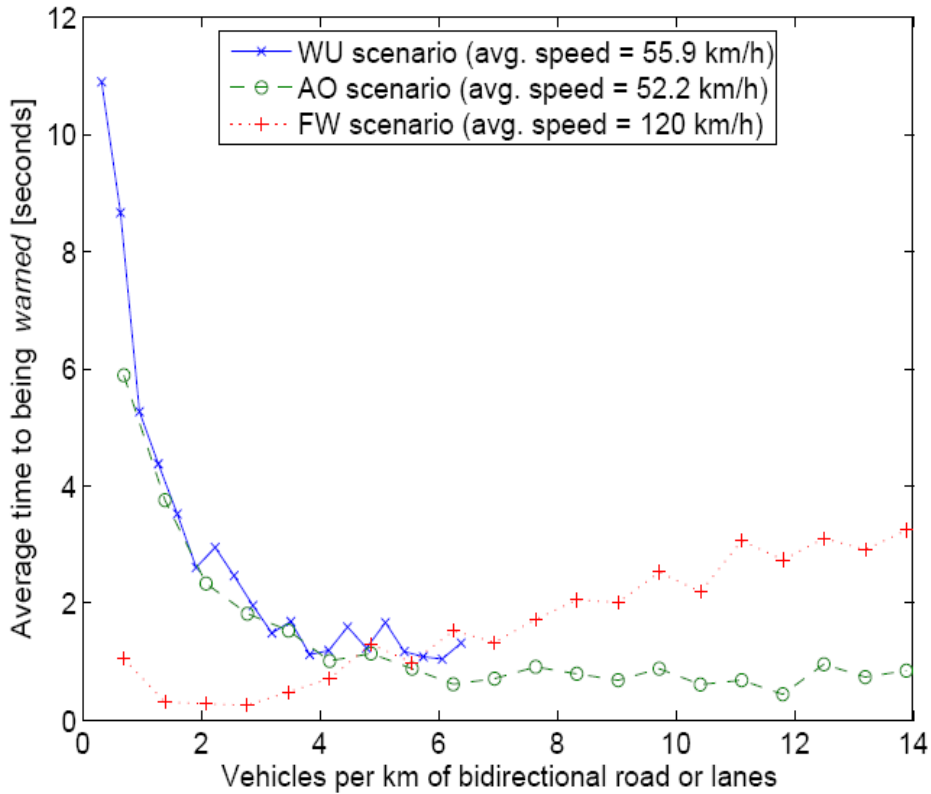


Eviction of faulty nodes (cont'd)

- LEAVE (Local Eviction of Attackers by Voting Evaluators) protocol



Eviction of faulty nodes (cont'd)



Eviction of faulty nodes (cont'd)

- Intention: enhance robustness
- Open issues
 - Distribution of revocation information
 - Design of the CA
- Local defense mechanism
 - Complementary to revocation lists
- Limitations
 - It is often hard to identify misbehaving nodes
 - Cannot rely on lengthy interactions




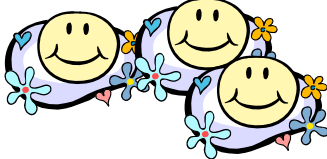


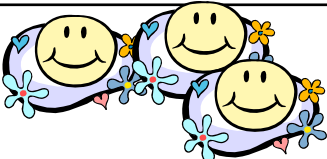
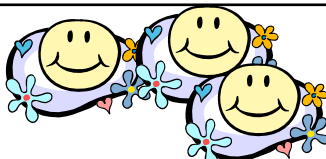

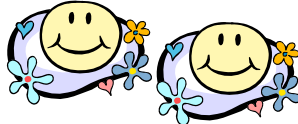













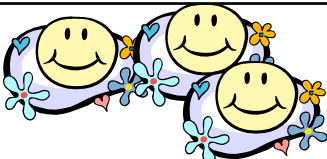

Data-centric trust establishment

- Need to extend the traditional notion *entity-centric* trust
 - Cannot rely or operate exclusively on a priori or largely time-invariant trust relations with network entities
 - What if the identity of the data producing entity is secondary?
 - What if a privacy-enhancing mechanism is used?

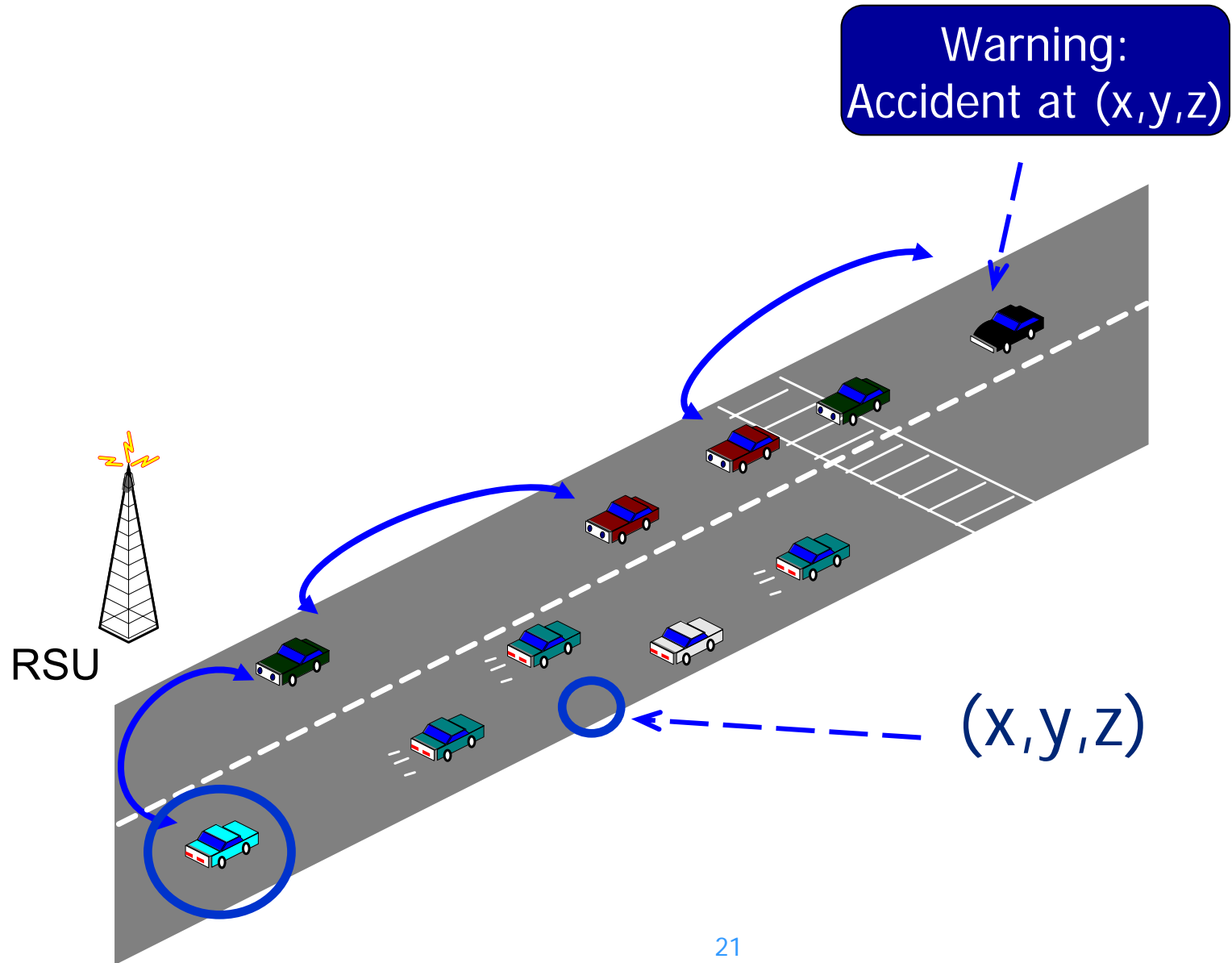
Data-centric trust establishment (cont'd)

- Proposal: *data-centric* trust
 - Trustworthiness attributed to node-reported data per se
- Problem for VC systems
 - Evaluate the trustworthiness of data reported by other vehicle rather than the trustworthiness of the vehicles themselves
 - Contradicting reports
 - Highly volatile network

Data-centric trust establishment (cont'd)

	Traffic Jam	Accident	Junction warning	RL distribution
				
				
				
				
				

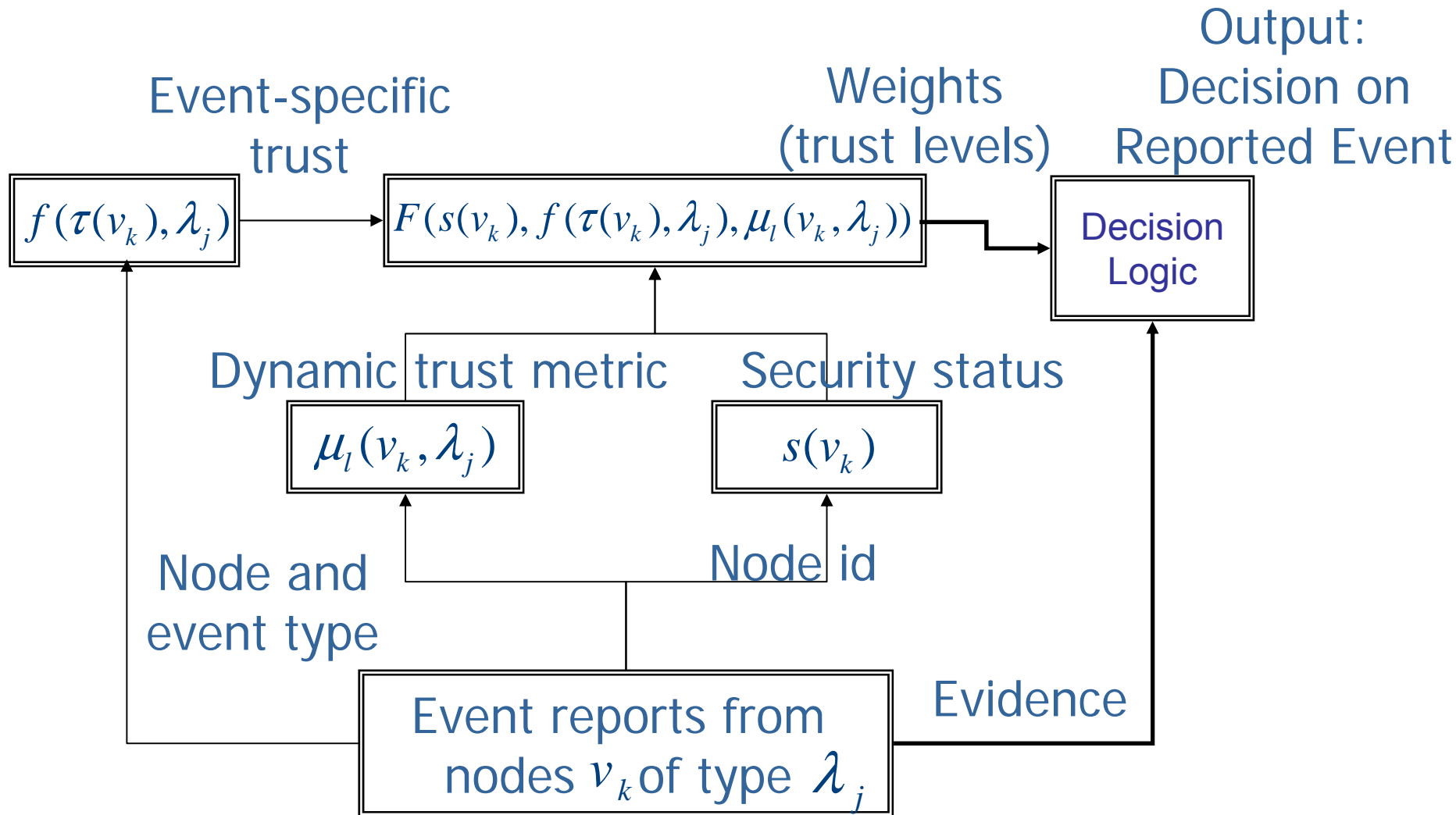
Data-centric trust establishment (cont'd)



Data-centric trust establishment (cont'd)

- Proximity to event can be crucial
 - Geographical
 - Time
- Security status
 - Revoked or not
- Default adaptation
 - Vehicles from a different domain (authority)

Data-centric trust establishment (cont'd)



M. Raya, P. P., V. D. Gligor, and J.-P. Hubaux, " On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," IEEE Infocom 2008

VC and privacy concerns

- Communication cannot be regulated or controlled by the node/user
 - Safety messaging will be essentially an 'always-on' application
- Vehicle-originating wireless transmissions are particularly easy to eavesdrop
 - Data link very similar to a widely adopted technology: IEEE 802.11
 - Very large and increasing numbers of 802.11 access points already deployed
 - Road-side infrastructure deployed for other services could be subverted into acting as an eavesdropper

VC and privacy concerns (cont'd)

- At least the same degree of privacy achieved nowadays, before the advent of 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

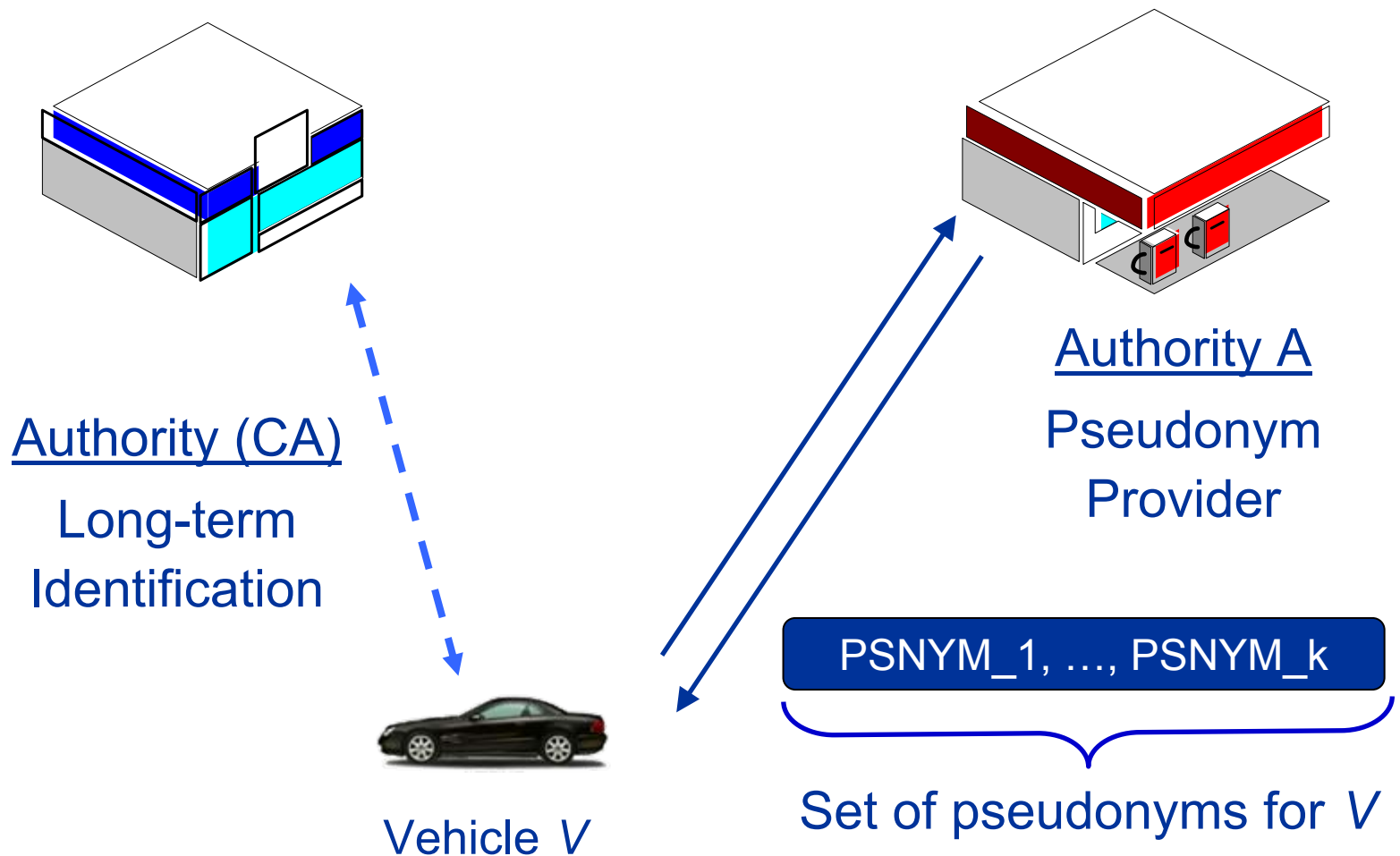
- Pseudonym
 - Remove all identifying information from certificate
- Pseudonym format

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

- Pseudonym provider: a trusted third party

Pseudonymous authentication (cont'd)

- System setup (one option)

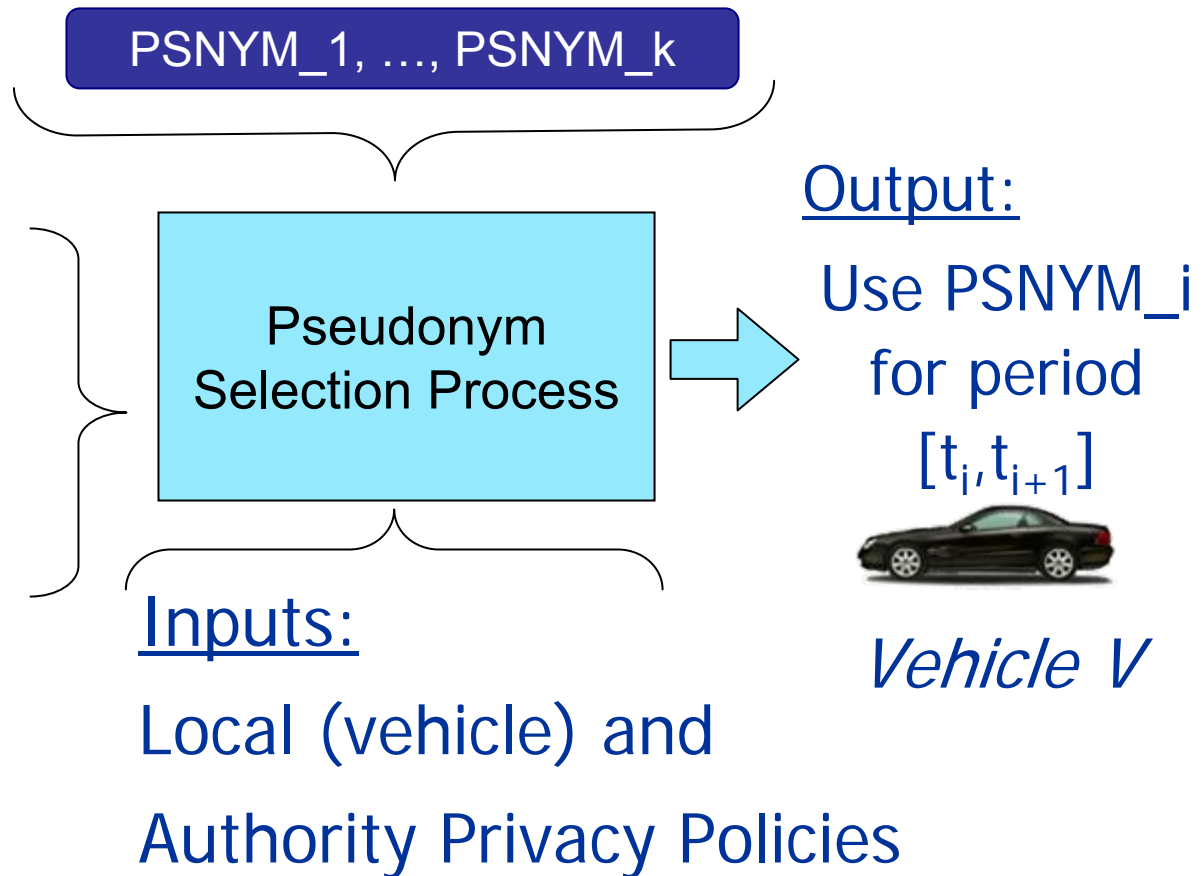


Pseudonymous authentication (cont'd)

- Pseudonym change mechanism

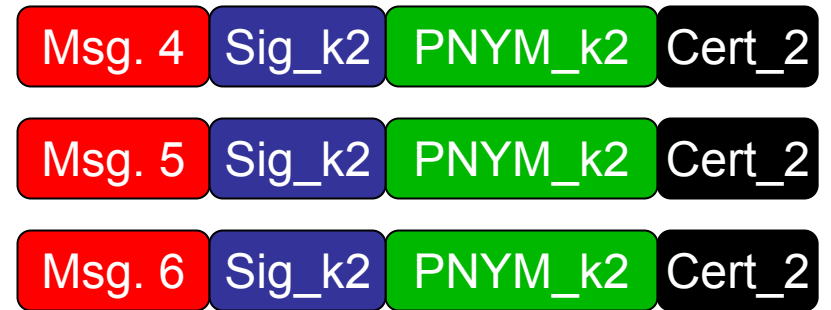
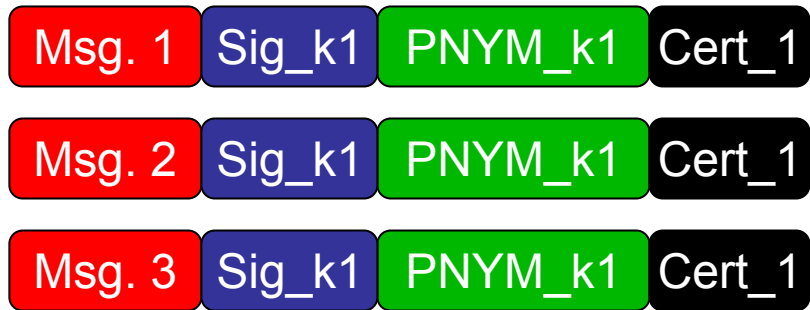
Inputs:

- Vehicle Location
- Vehicle Clock
- Recipient(s) / (Verifier(s))



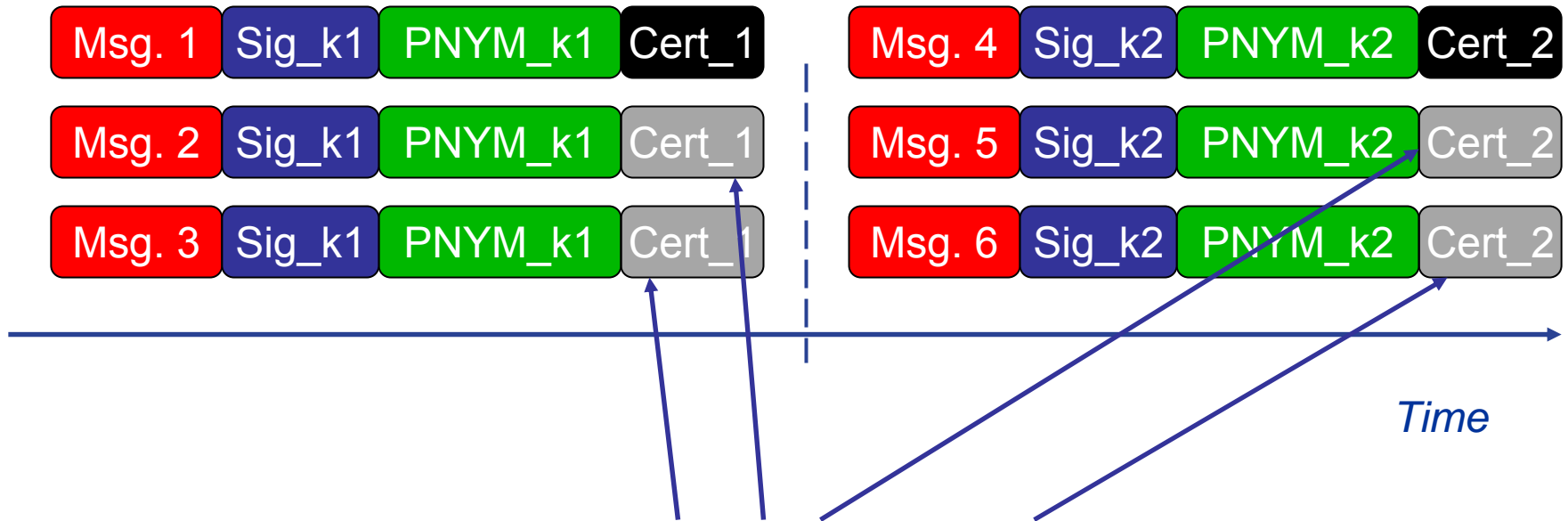
- *One pseudonym per day (?)*
- *One per transaction (?)*

Reducing SVC cost - Optimization (1)



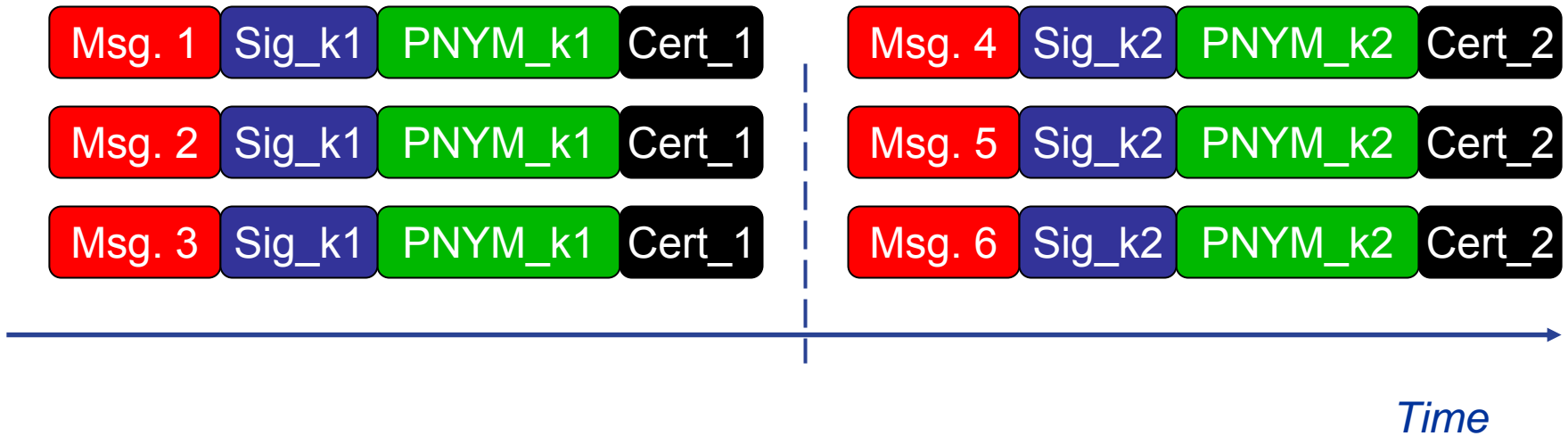
Time

Reducing SVC cost - Optimization (1)

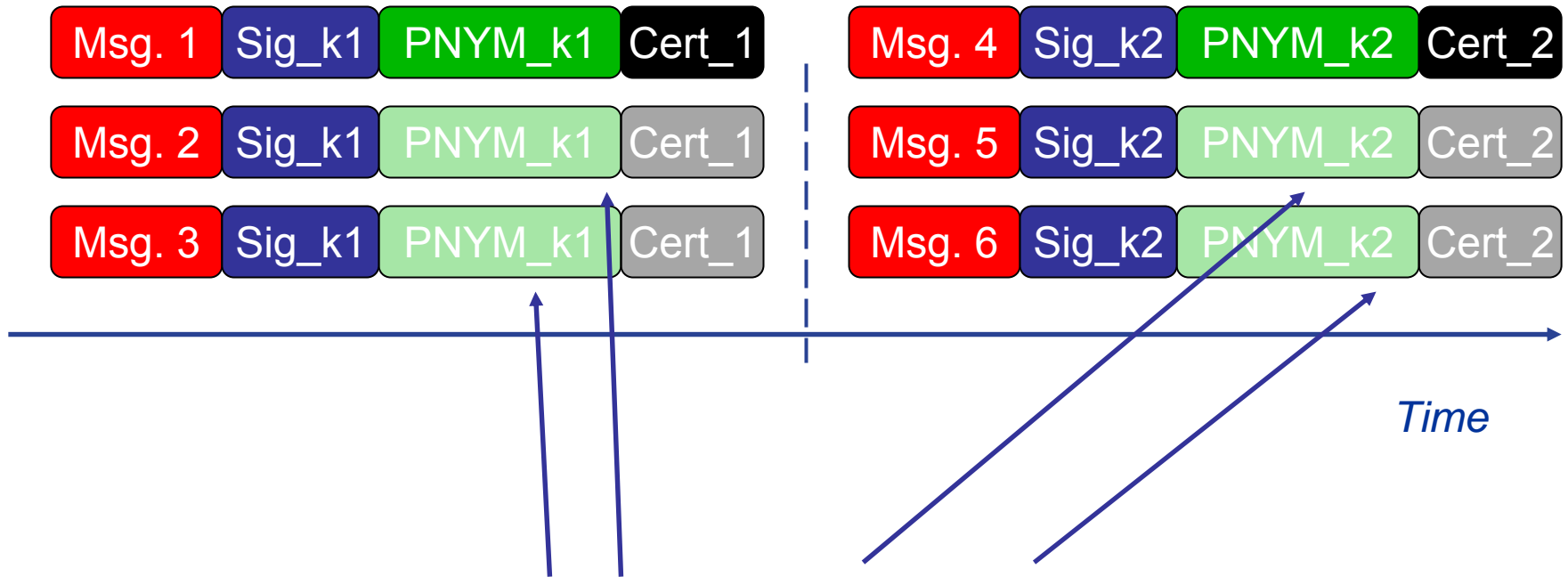


Need to be generated / validated only once per pseudonym lifetime

Reducing SVC cost - Optimization (2)

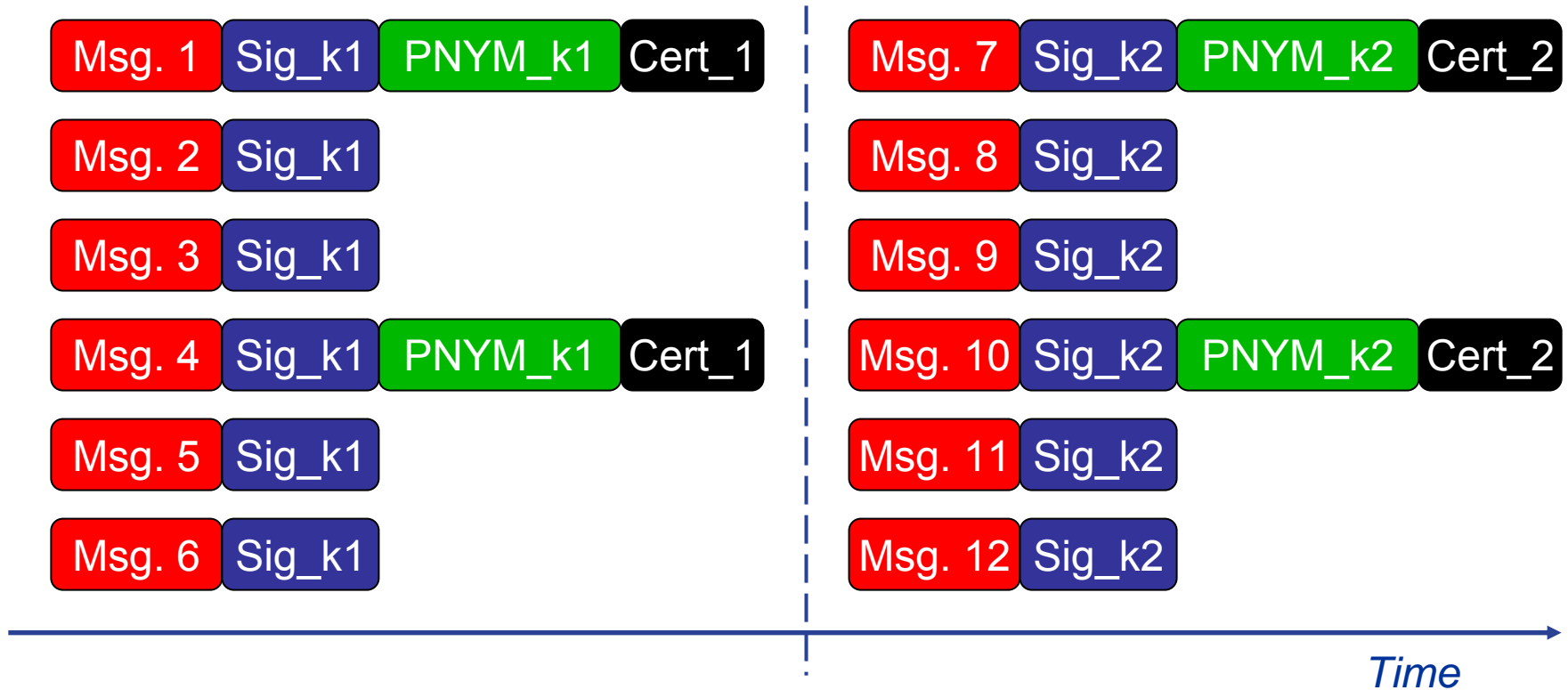


Reducing SVC cost - Optimization (2)

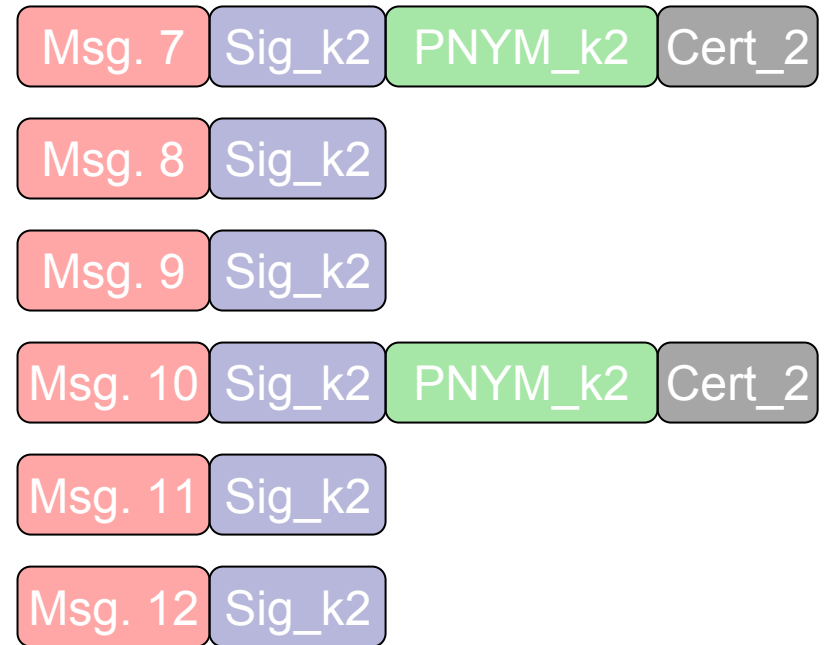
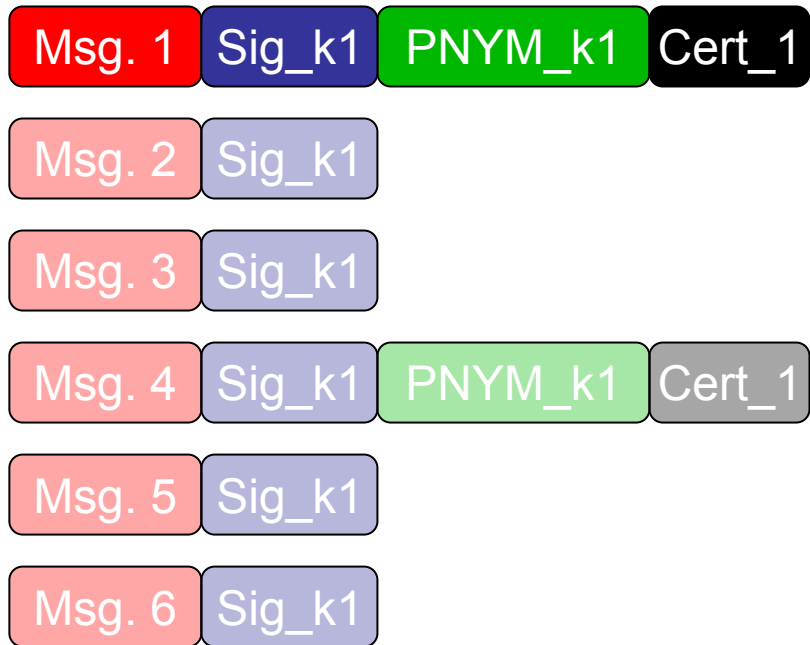
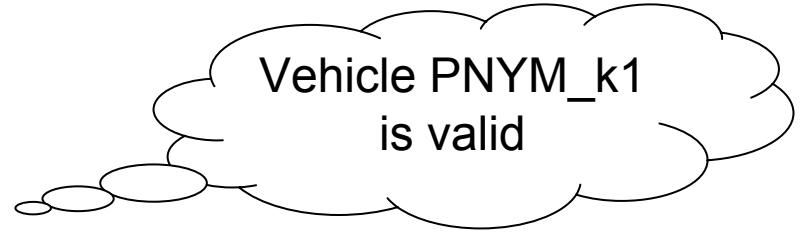
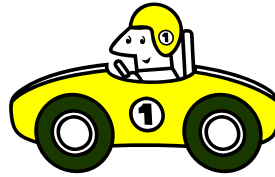


Need to be attached to the message only periodically

Reducing SVC cost - Optimization (2)

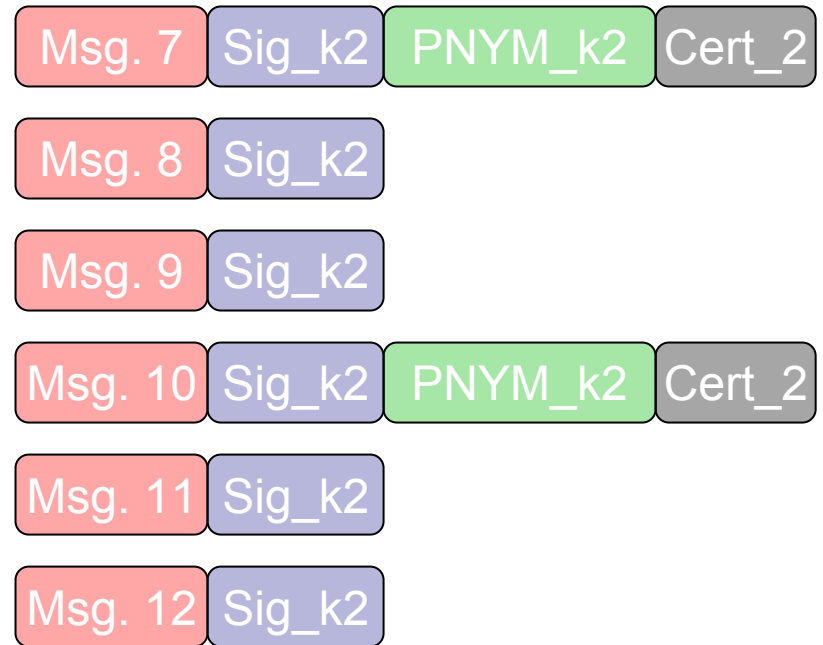
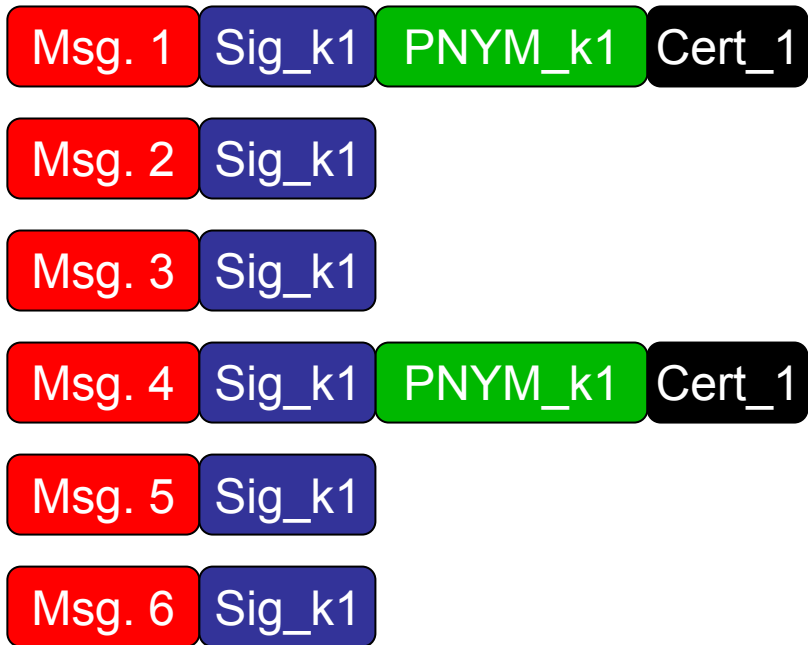
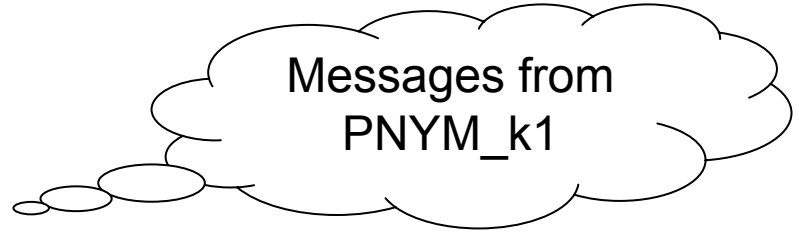
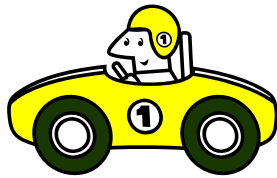


Reducing SVC cost - Optimization (3)

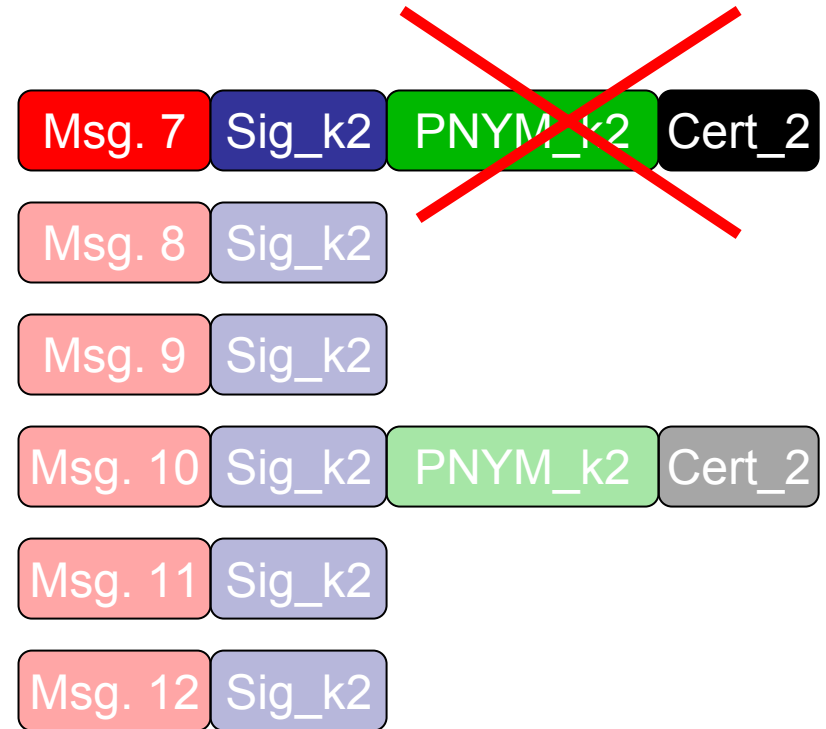
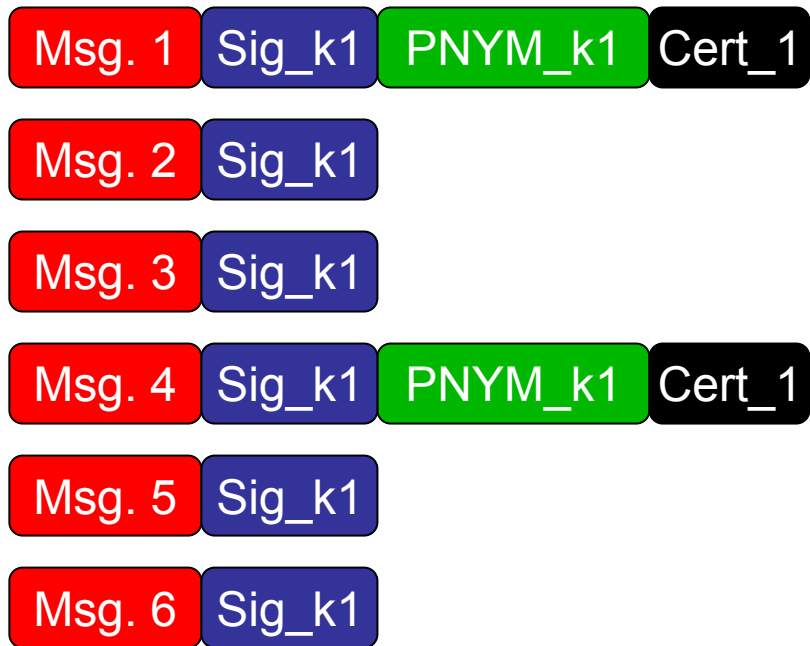


Time

Reducing SVC cost - Optimization (3)

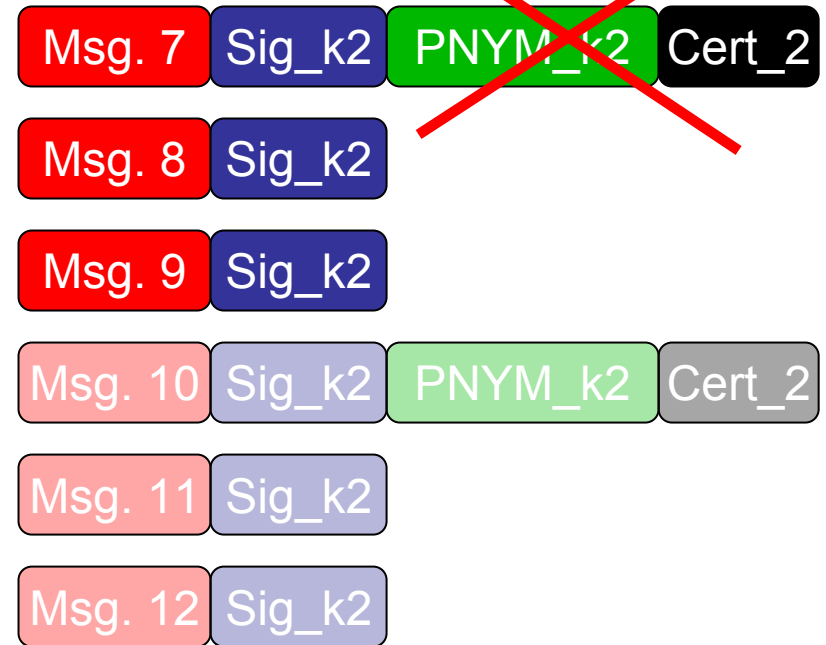
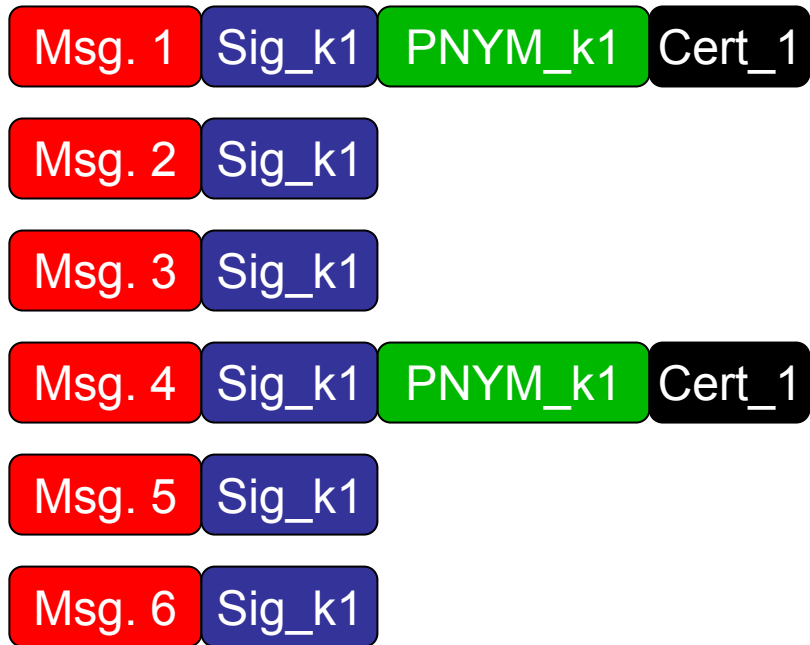


Reducing SVC cost - Optimization (3)



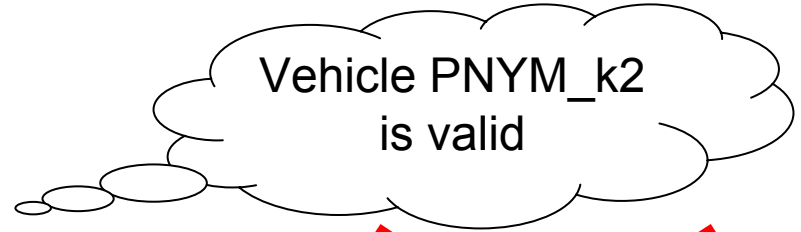
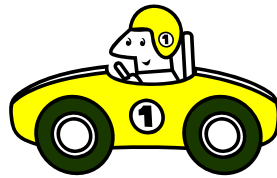
Time

Reducing SVC cost - Optimization (3)



Time

Reducing SVC cost - Optimization (3)



Msg. 1 Sig_k1 PNYM_k1 Cert_1

Msg. 2 Sig_k1

Msg. 3 Sig_k1

Msg. 4 Sig_k1 PNYM_k1 Cert_1

Msg. 5 Sig_k1

Msg. 6 Sig_k1

Msg. 7 Sig_k2 ~~PNYM_k2~~ Cert_2

Msg. 8 Sig_k2

Msg. 9 Sig_k2

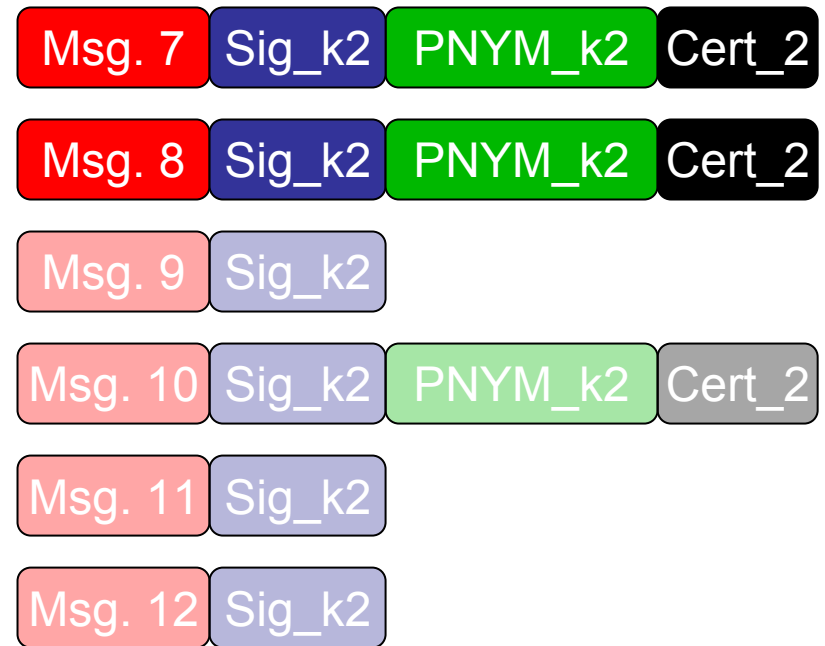
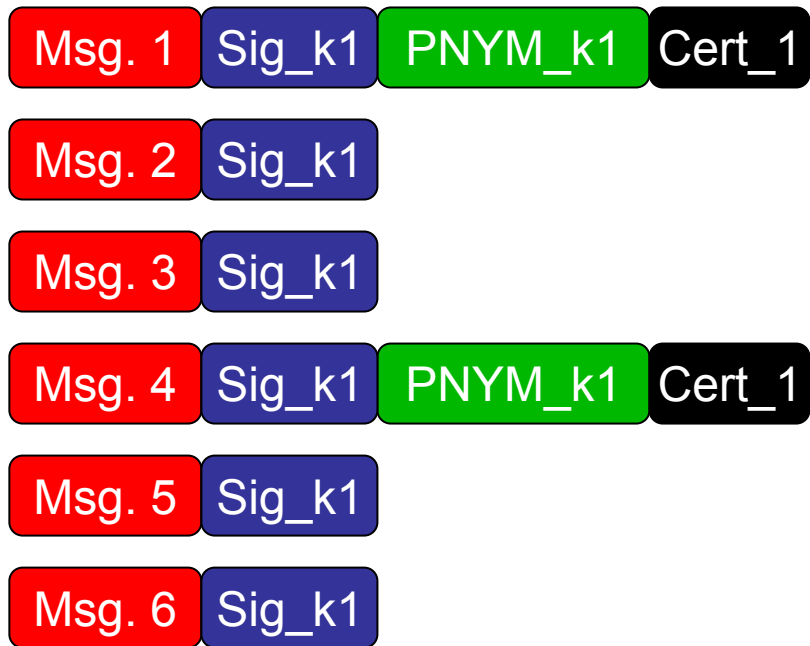
Msg. 10 Sig_k2 PNYM_k2 Cert_2

Msg. 11 Sig_k2

Msg. 12 Sig_k2

Time

Reducing SVC cost - Optimization (3)



Time

Reducing SVC cost - recap

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

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



Valid signature from a
legitimate member of
Group A
??? *Member* ???



gsk_1



gsk_2



gsk_3

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)

m	$\sigma_{k_V^i}(m)$	K_V^i	$Cert_{CA}(K_V^i)$
-----	---------------------	---------	--------------------

Group
Signature (GS)

m	$\Sigma_{CA,V}(m)$
-----	--------------------

Hybrid

m	$\sigma_{k_V^i}(m)$	K_V^i	$\Sigma_{CA}^H(K_V^i)$
-----	---------------------	---------	------------------------

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

Overhead

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

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

Impact of security on safety (cont'd)

- Setting (1):
 - Two vehicles on a single lane starting at a distance d
 - V sends beacons
 - U receives them and approaches V with a fixed relative speed
 - Measure distance at which U validates the first certificate and safety message from V

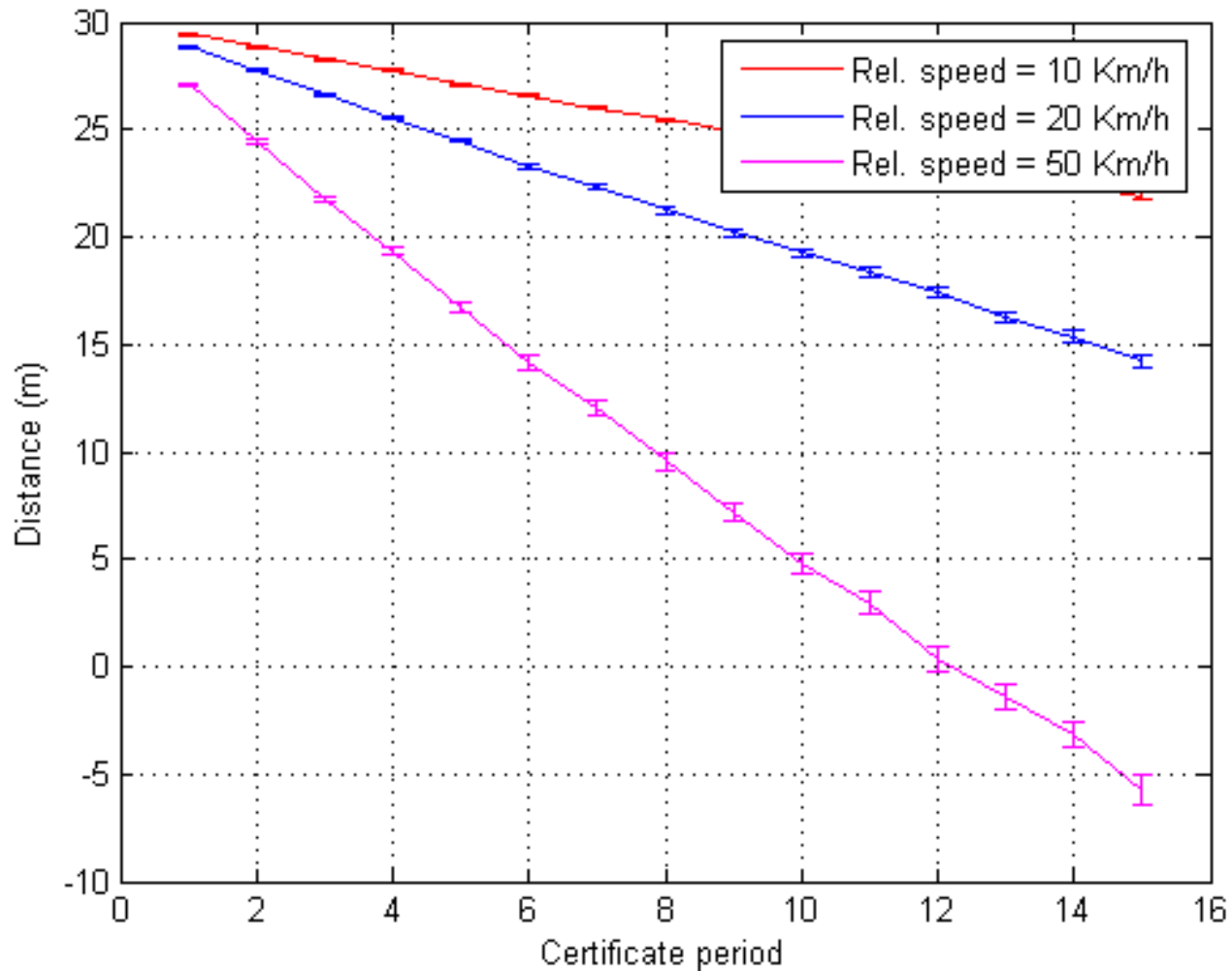
Impact of security on safety (cont'd)

- Setting (2):
 - Platoon of 100 vehicles along one lane
 - Multi-lane highway
 - V_1 , the vehicle at the front of the platoon performs and emergency braking
 - Without VC, ~80% of vehicles collide
 - Measure percentage of vehicles that collide when Secure Vehicular Communications are used

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

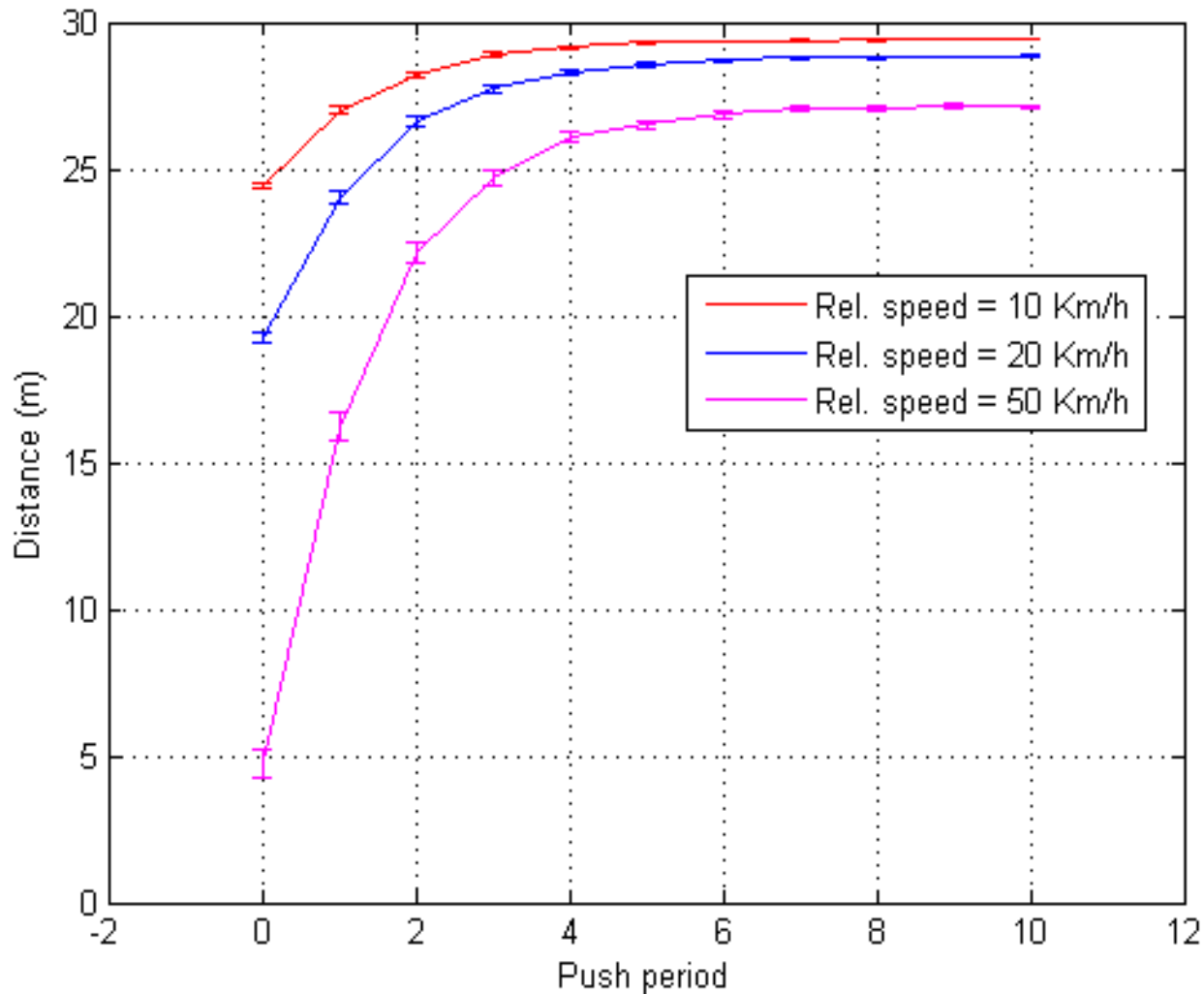
Impact of security on safety (cont'd)

- Setting (1) - Initial distance $d=30\text{m}$



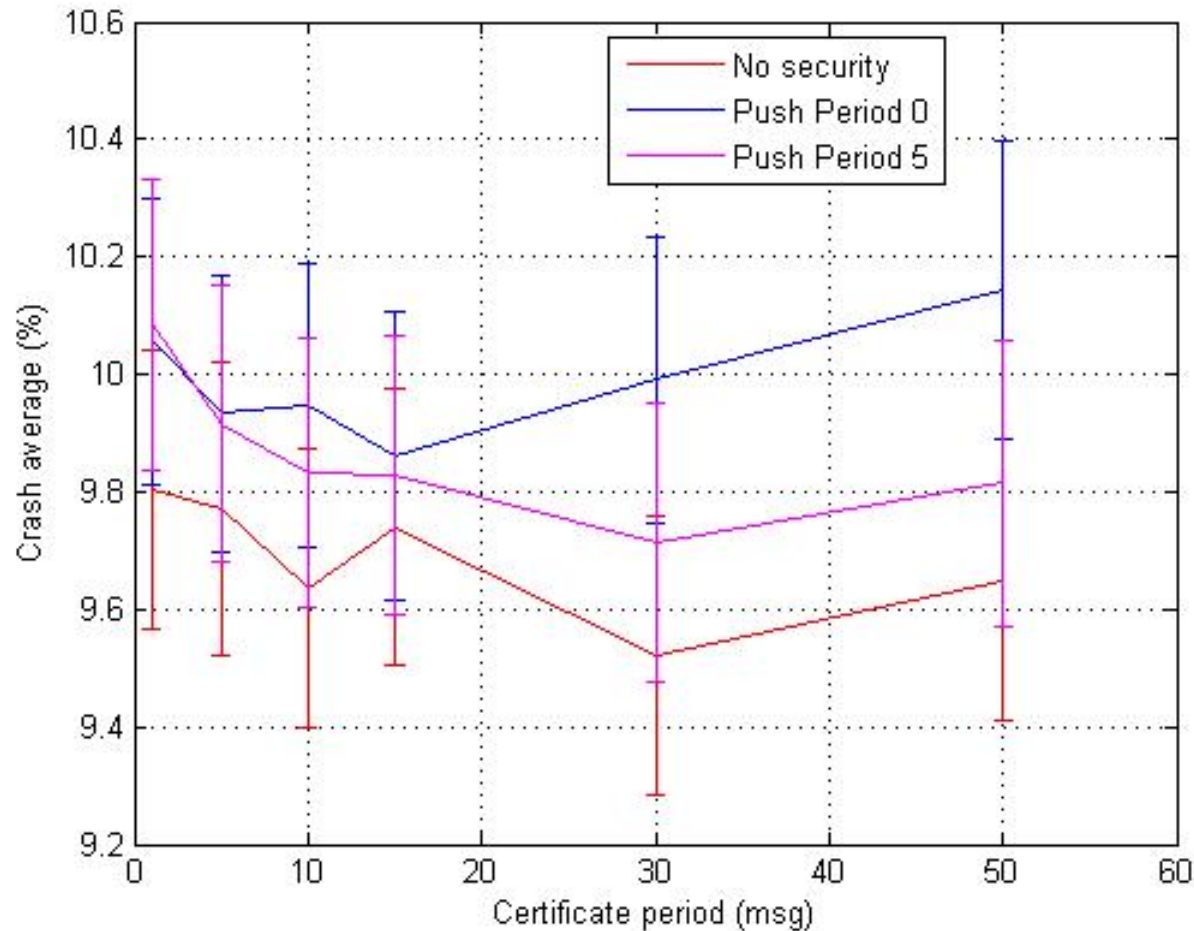
Impact of security on safety (cont'd)

- Setting (1) - $d=30\text{m}$, $\alpha = 10$



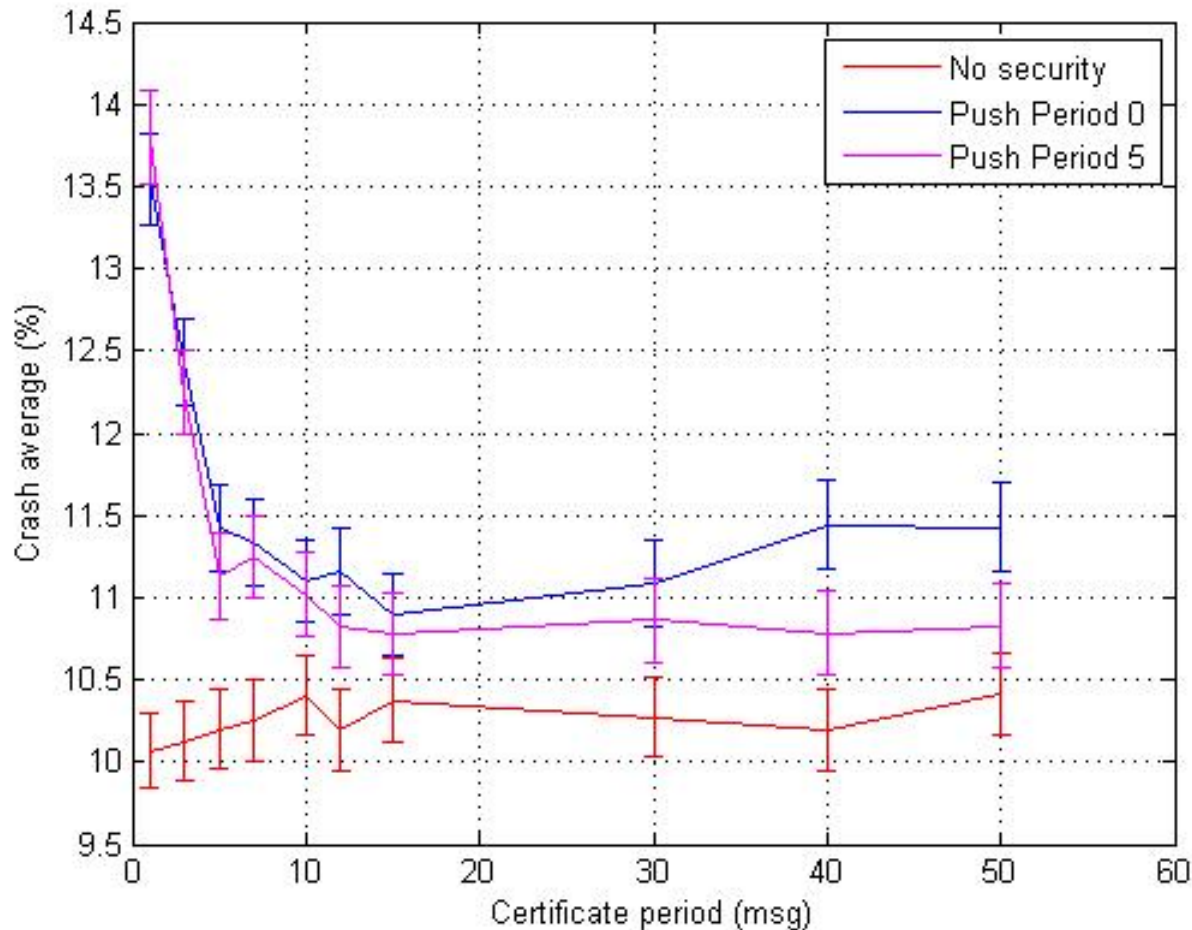
Impact of security on safety (cont'd)

- Setting (2) – eight-lane highway – vehicle collisions



Impact of security on safety (cont'd)

- Setting (2) – eight-lane highway – vehicle collisions



Conclusions

- Addressed problems
 - Identity and key management
 - Secure communication
 - Privacy enhancing technologies (PET)
- Next steps
 - Node eviction
 - CRL distribution
 - Data-centric trust
 - Reducing security and PET overhead and complexity

Conclusions (cont'd)

- Next steps (cont'd)
 - Impact of security and PET on safety
 - New simulation tools
 - Binding traffic and network simulation
- Challenge: New important topics to address
- Response: Encouraging initial results