THE FULLY NETWORKED CAR

Panos Papadimitratos

Senior Researcher, EPFL

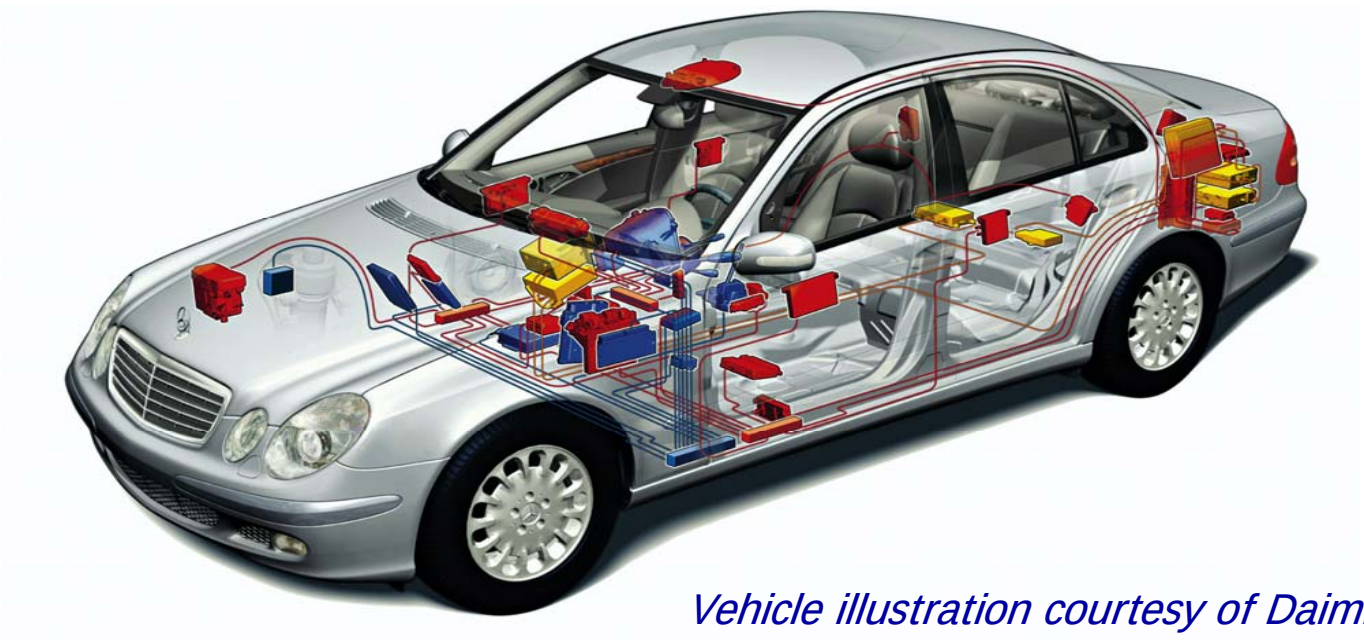
Geneva, 5-7 March 2008

ISO IEC ITU International Telecommunication Union

Towards Trustworthy Information and Communication Technologies in Vehicular Systems

Vehicular Communication Systems

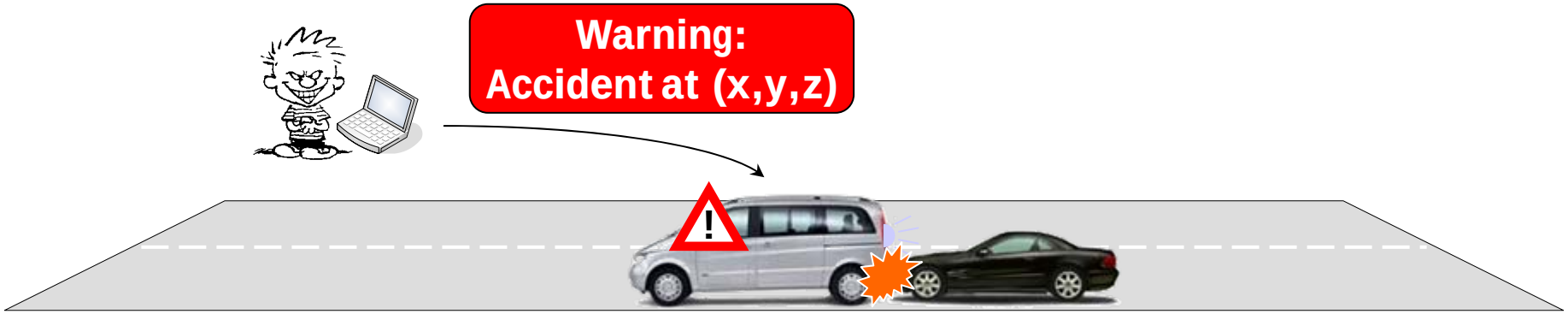
- Vehicles equipped with
  - Computers
  - Sensors
  - Wireless transceivers



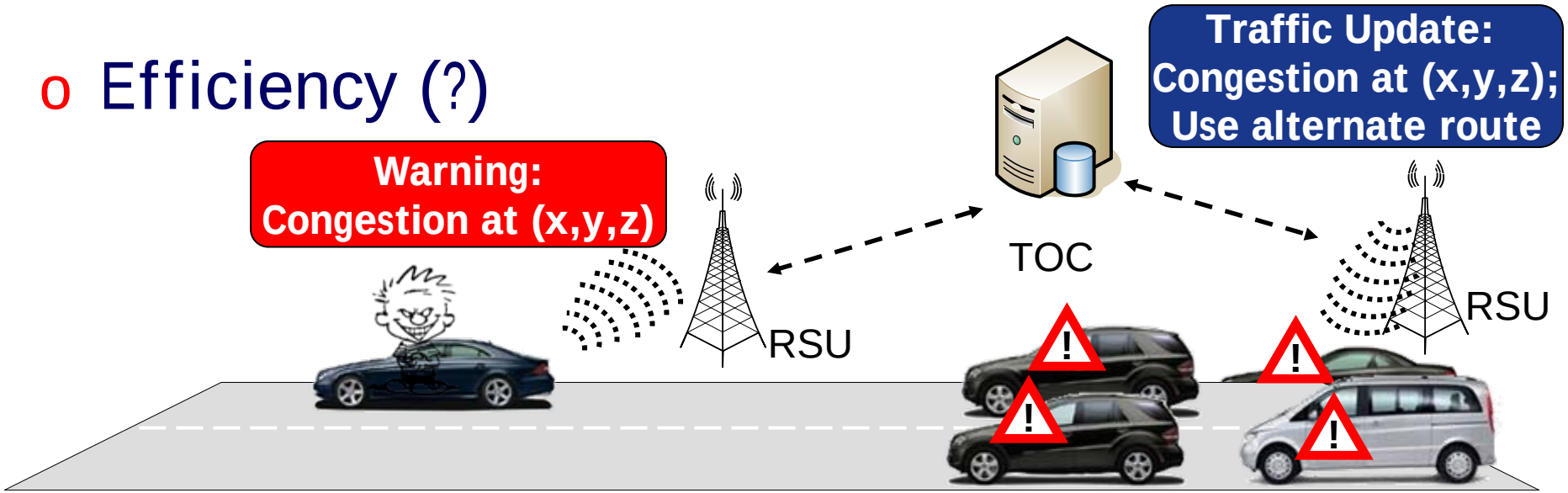
Vehicle illustration courtesy of Daimler

Security – Why?

- Safety (?)

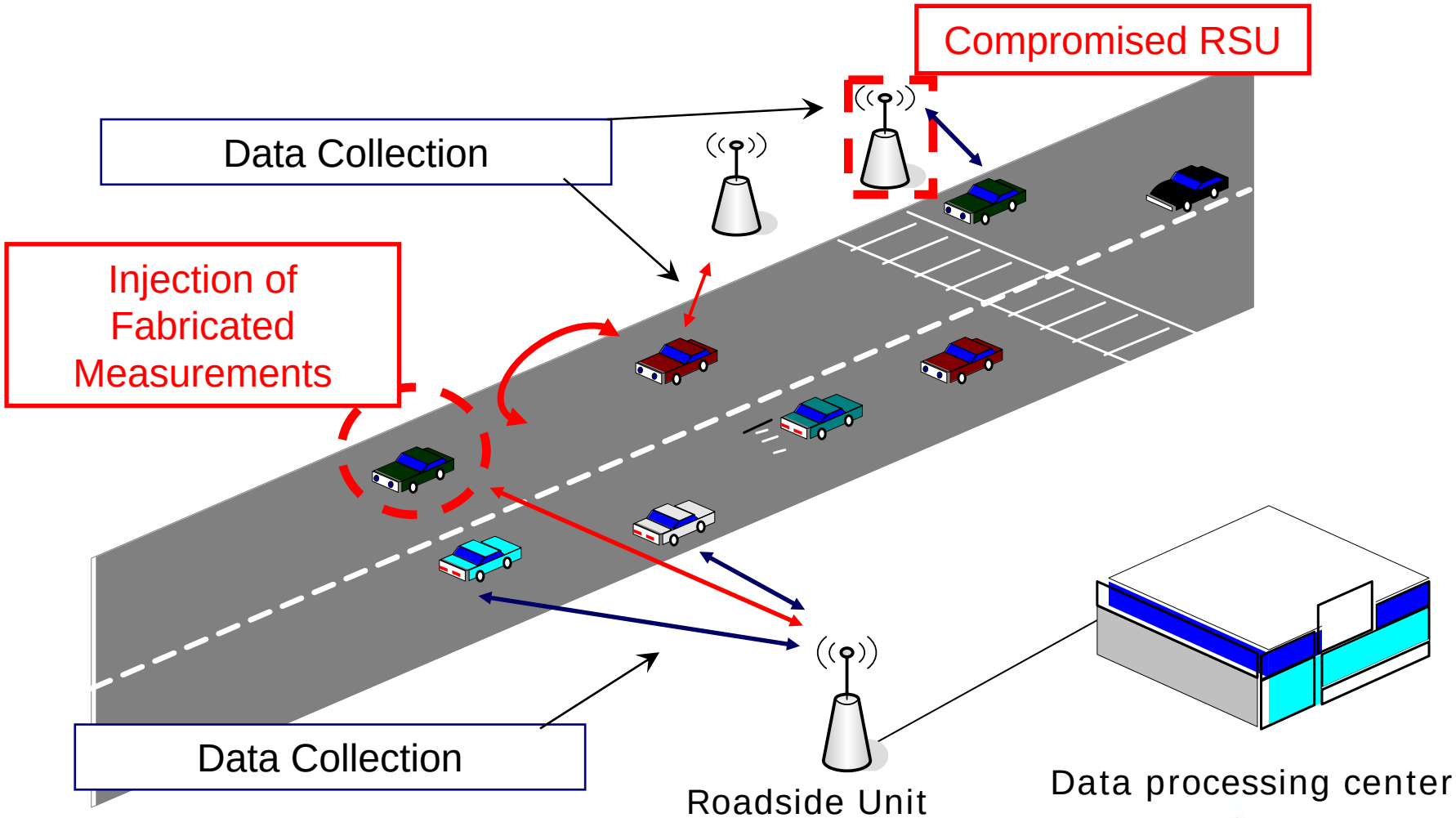


- Efficiency (?)



Security – Why?

- Accurate environmental monitoring (?)



- 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)

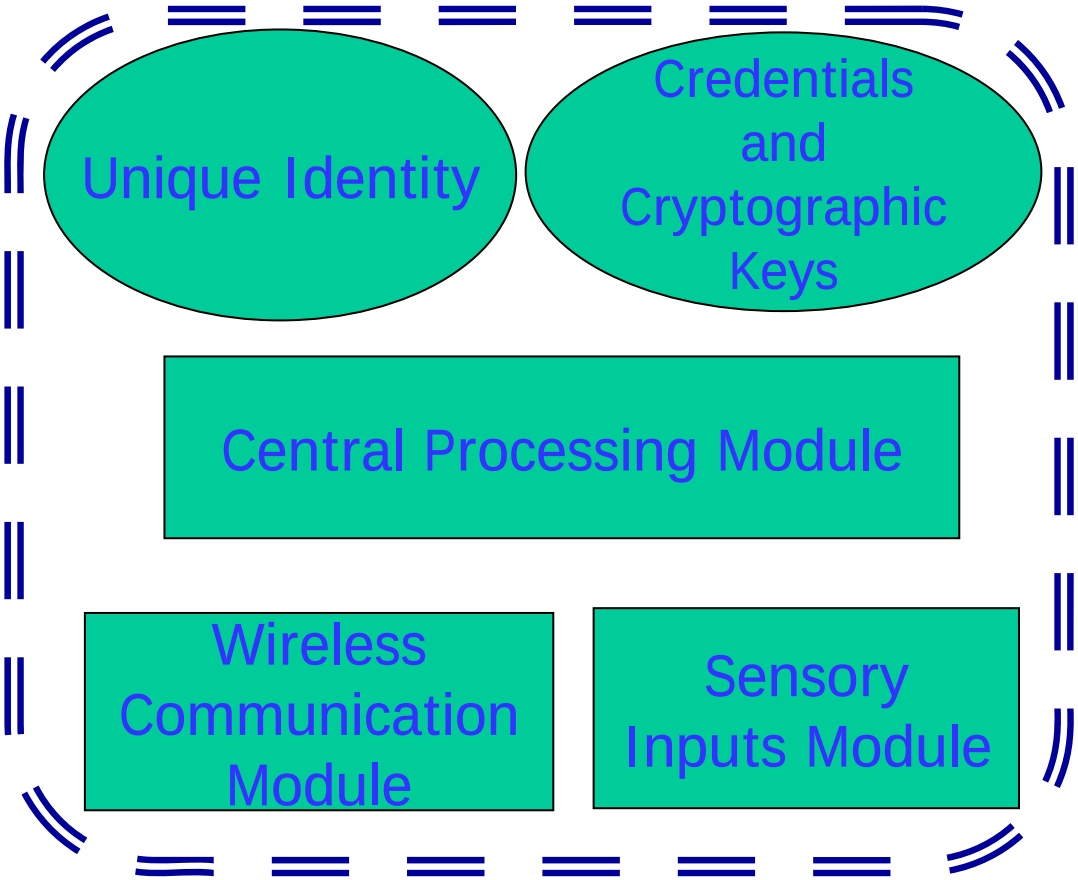
- Objectives
  - Focus on communication
  - Baseline Privacy Enhancing Technology (PET)
- Baseline solution design approach
  - Standardized cryptographic primitives
  - Easy-to-implement
  - Low overhead
  - Adaptable protection

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

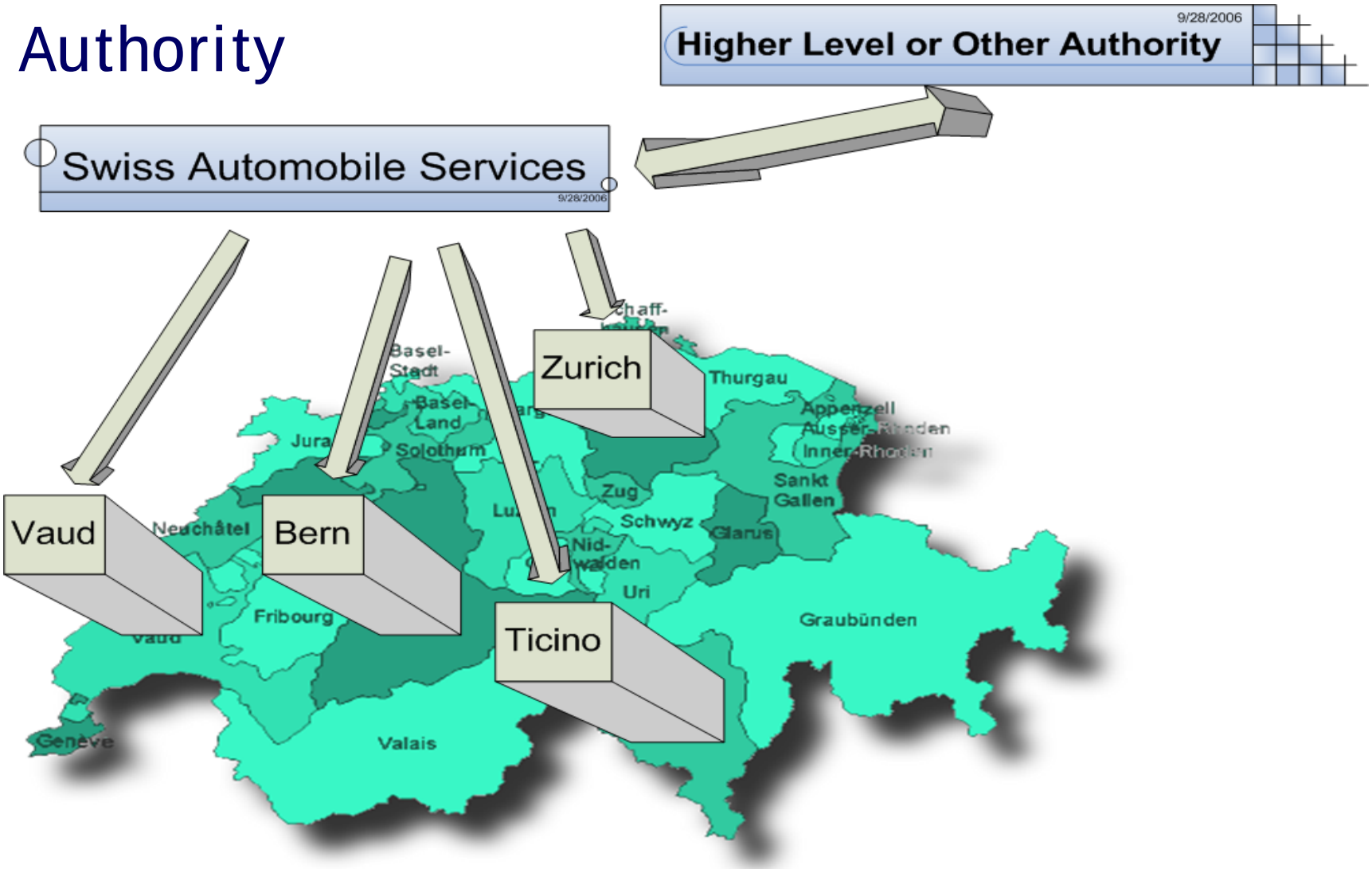


Secure VC system entities (cont'd)

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

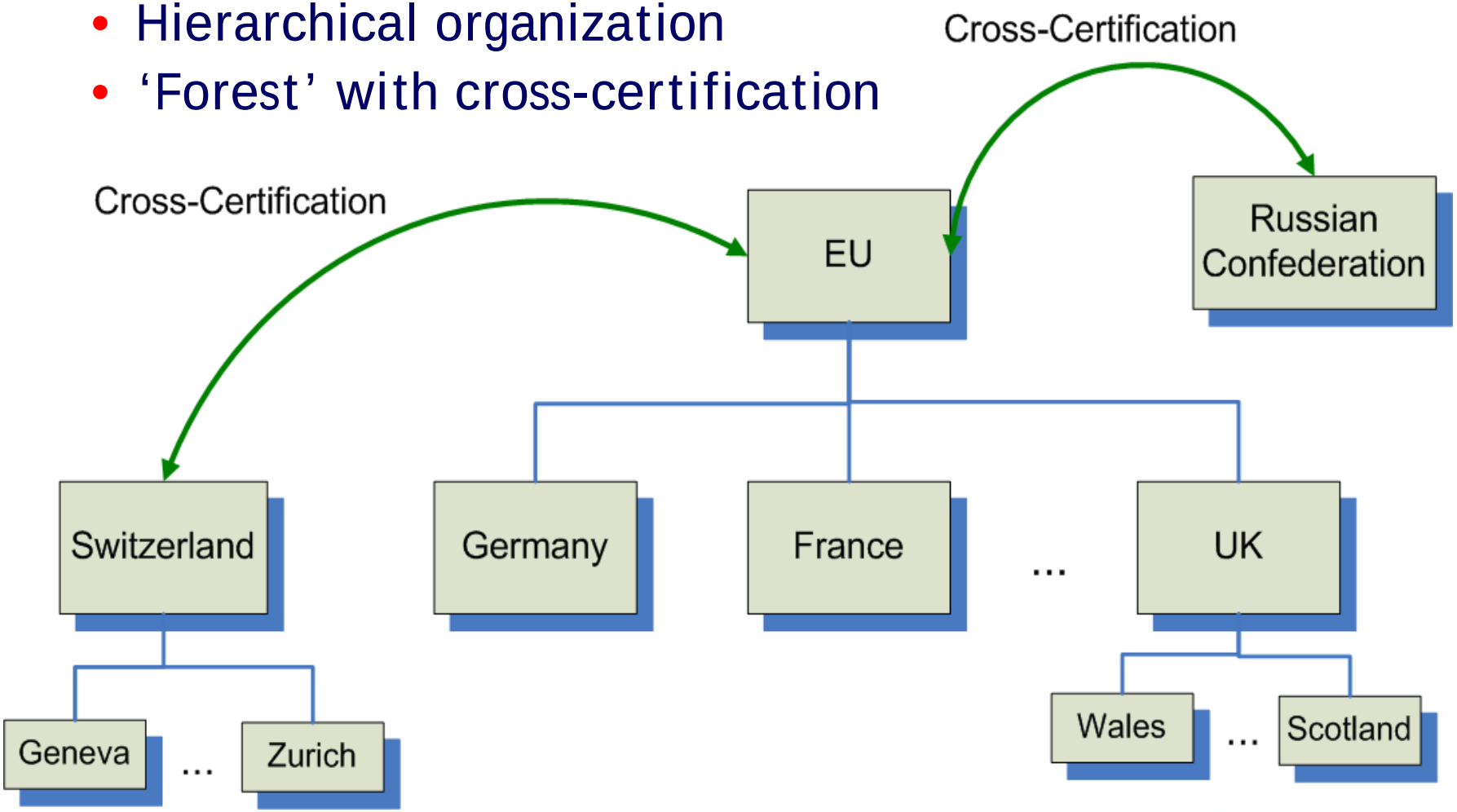
Secure VC system entities (cont'd)

- Authority



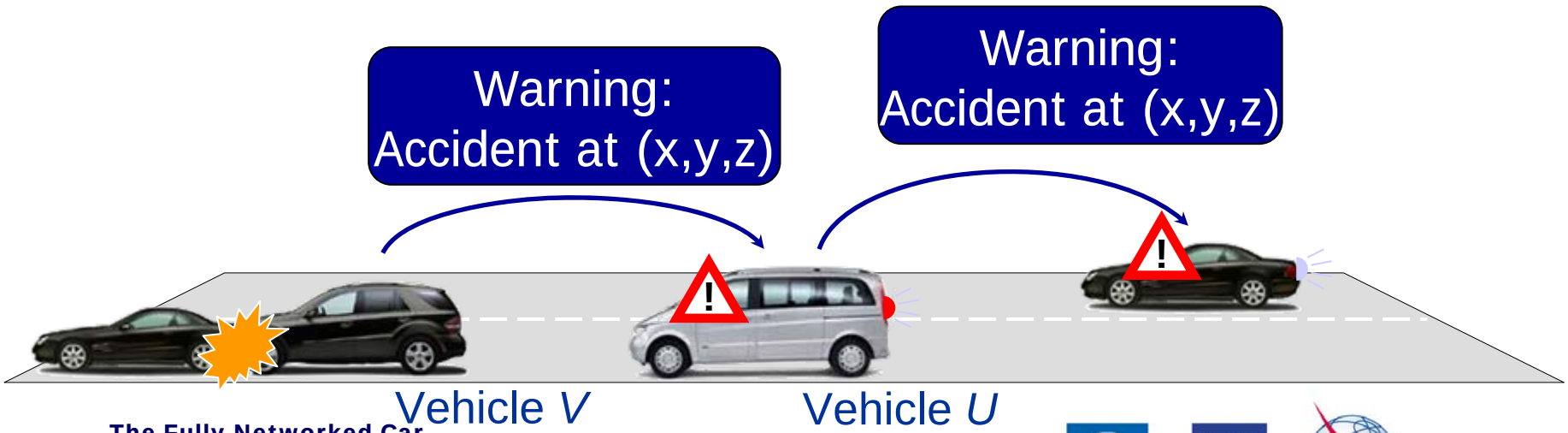
Secure VC system entities (cont'd)

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



Secure communication

Payload	
Location: (x_V, y_V, z_V)	*Time*: t_V
Signature with k_V	
$Cert_{CA}(V, K_V, A_V, T)$	

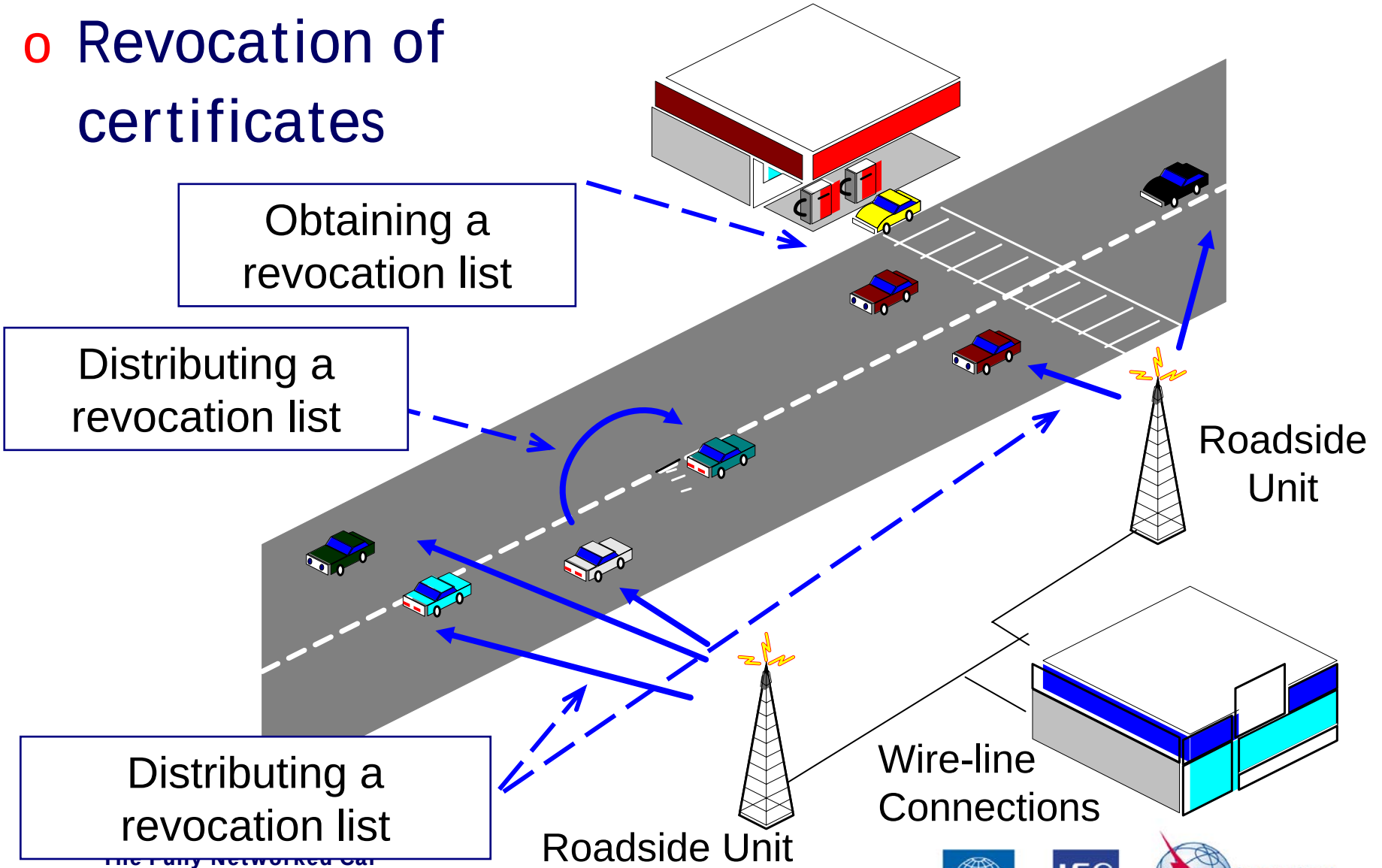


Secure communication (cont'd)

- 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
- **Still, a node with valid credentials can inject false data**

Eviction of faulty nodes

- Revocation of certificates

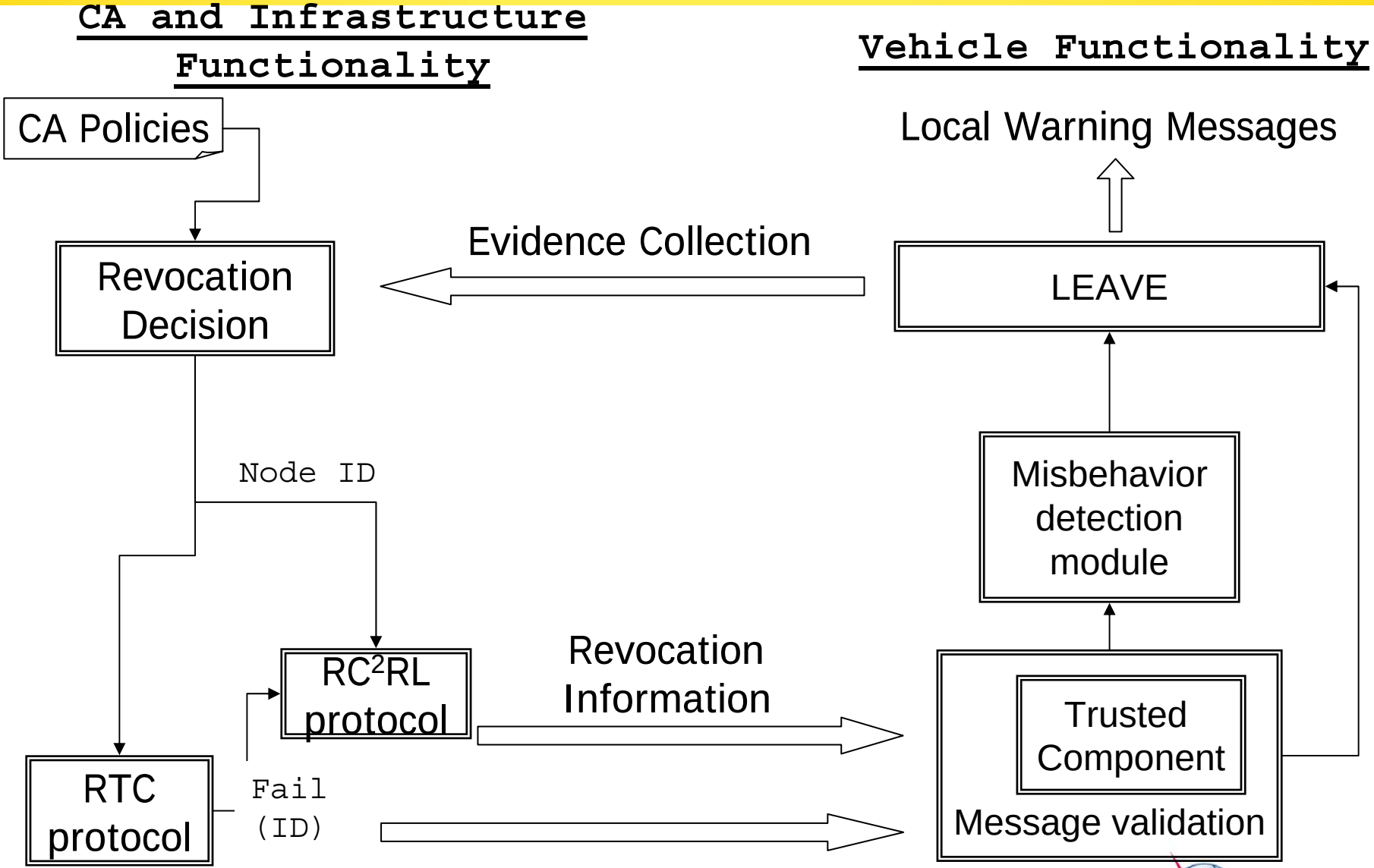


Eviction of faulty nodes (cont'd)

- 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

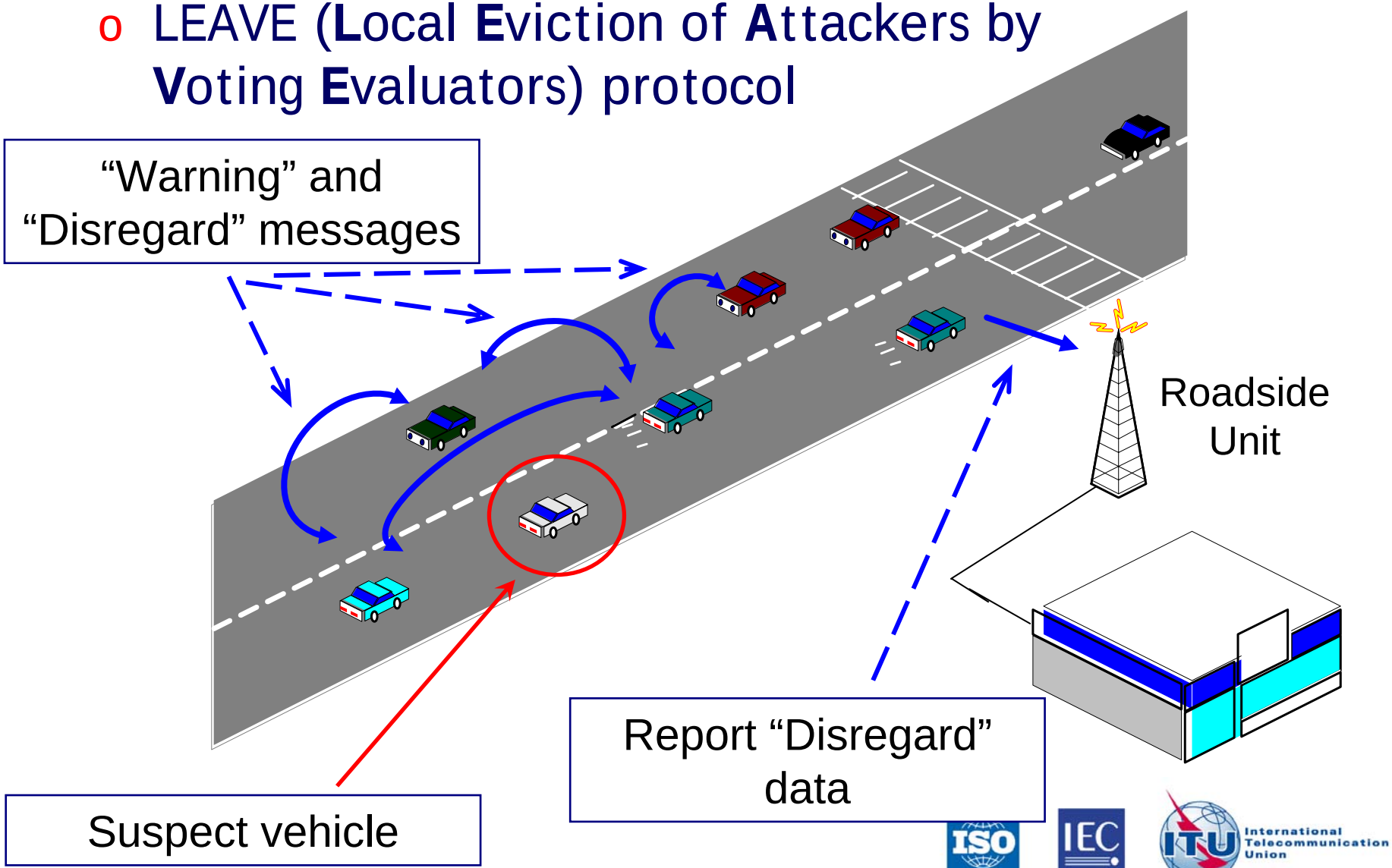
M. Raya, P. P., I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," IEEE JSAC, 2007

Eviction of faulty nodes (cont'd)



Eviction of faulty nodes (cont'd)

- LEAVE (**L**ocal **E**viction of **A**ttackers by **V**oting **E**valuators) protocol



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

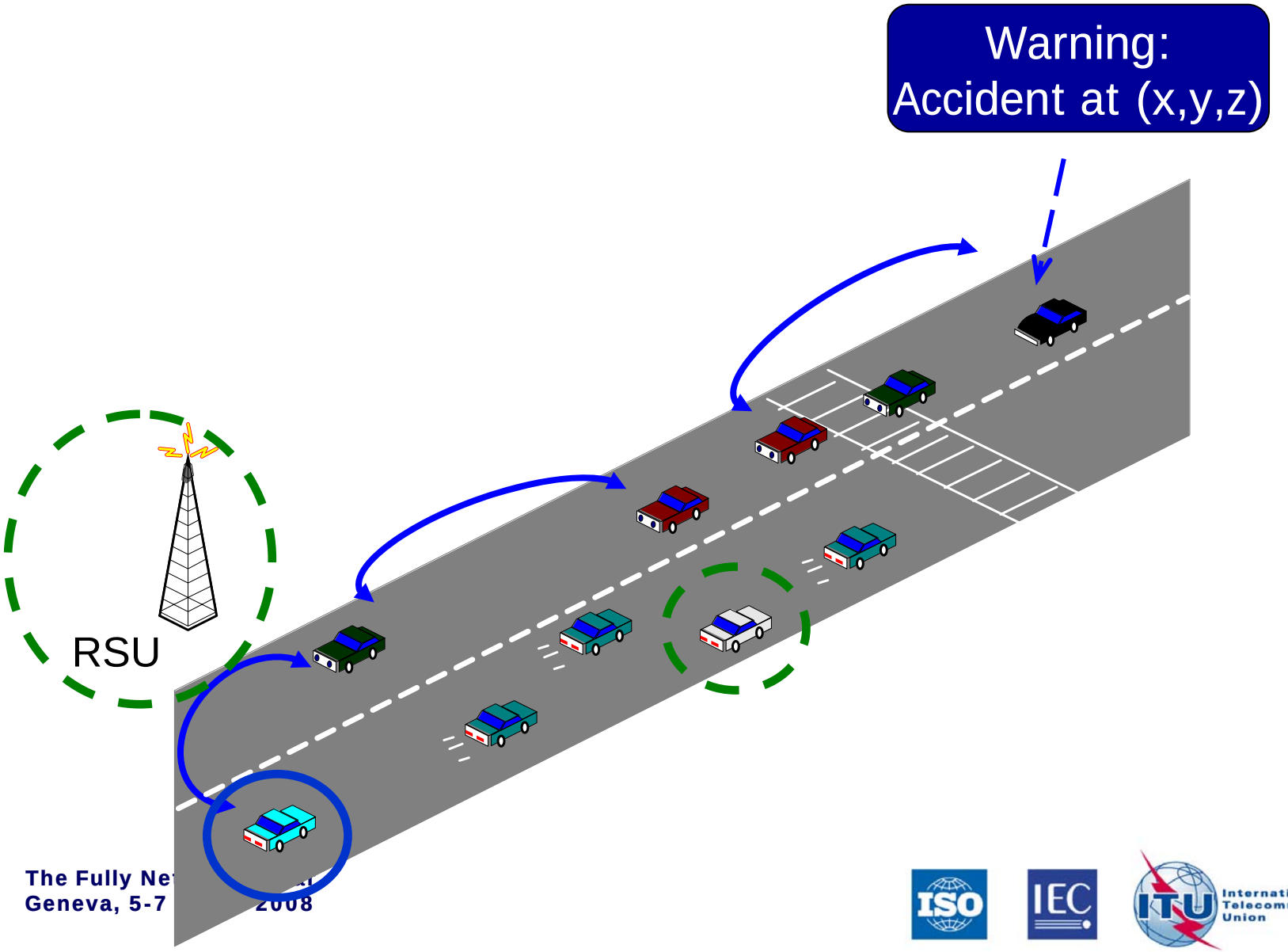
- Need to extend the traditional notion *entity-centric* trust
  - Cannot rely or operate exclusively on a priori or largely time-invariant trust relations with network entities
  - What if the identity of the data producing entity is secondary?
  - What if a privacy-enhancing mechanism is used?

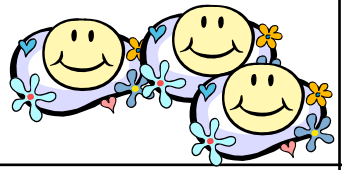
Data-centric trust establishment (cont'd)

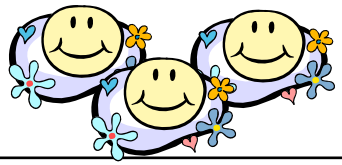
- Proposal: *data-centric* trust
  - Trustworthiness attributed to node-reported data per se

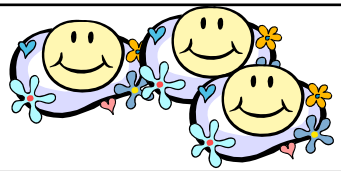
- Problem for VC systems
  - Evaluate the trustworthiness of data reported by other vehicle rather than the trustworthiness of the vehicles themselves
  - Contradicting reports
  - Highly volatile network

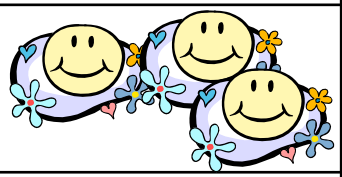
Data-centric trust establishment (cont'd)

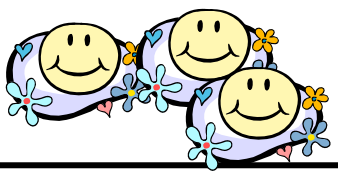


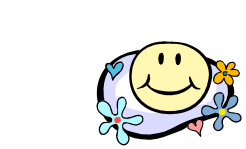


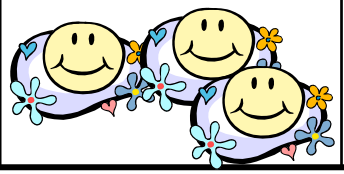








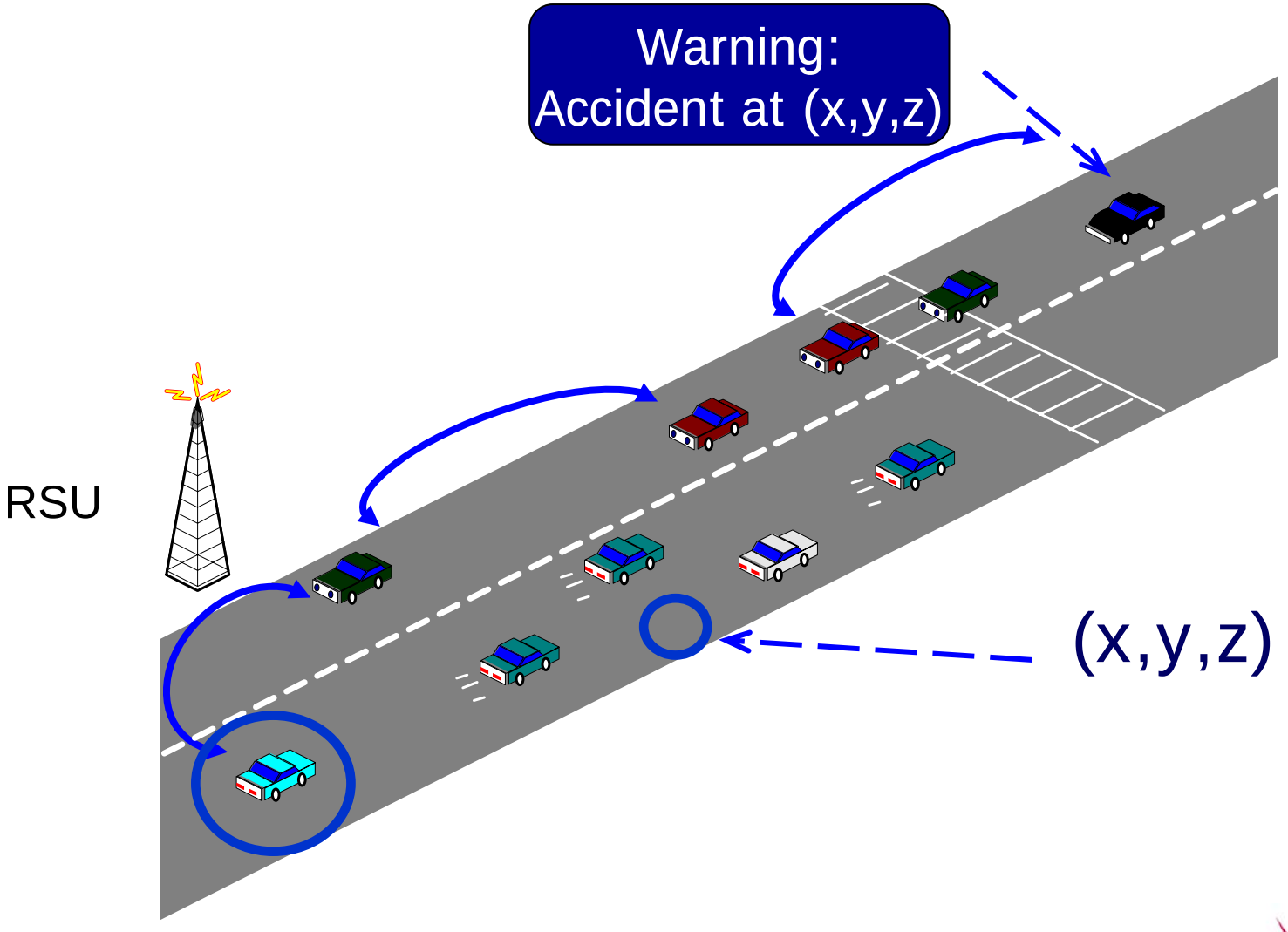




Data-centric trust establishment (cont'd)

	Traffic Jam	Accident	Junction warning	RL distribution
	☺	☺☺	☺☺☺	☺☺☺
	☺☺☺	☺☺☺	☺☺	☺☺
	☺☺	☺☺	☺	☺
	☺	☺	☺	☺
	☺☺☺	☺	☺☺☺	☺

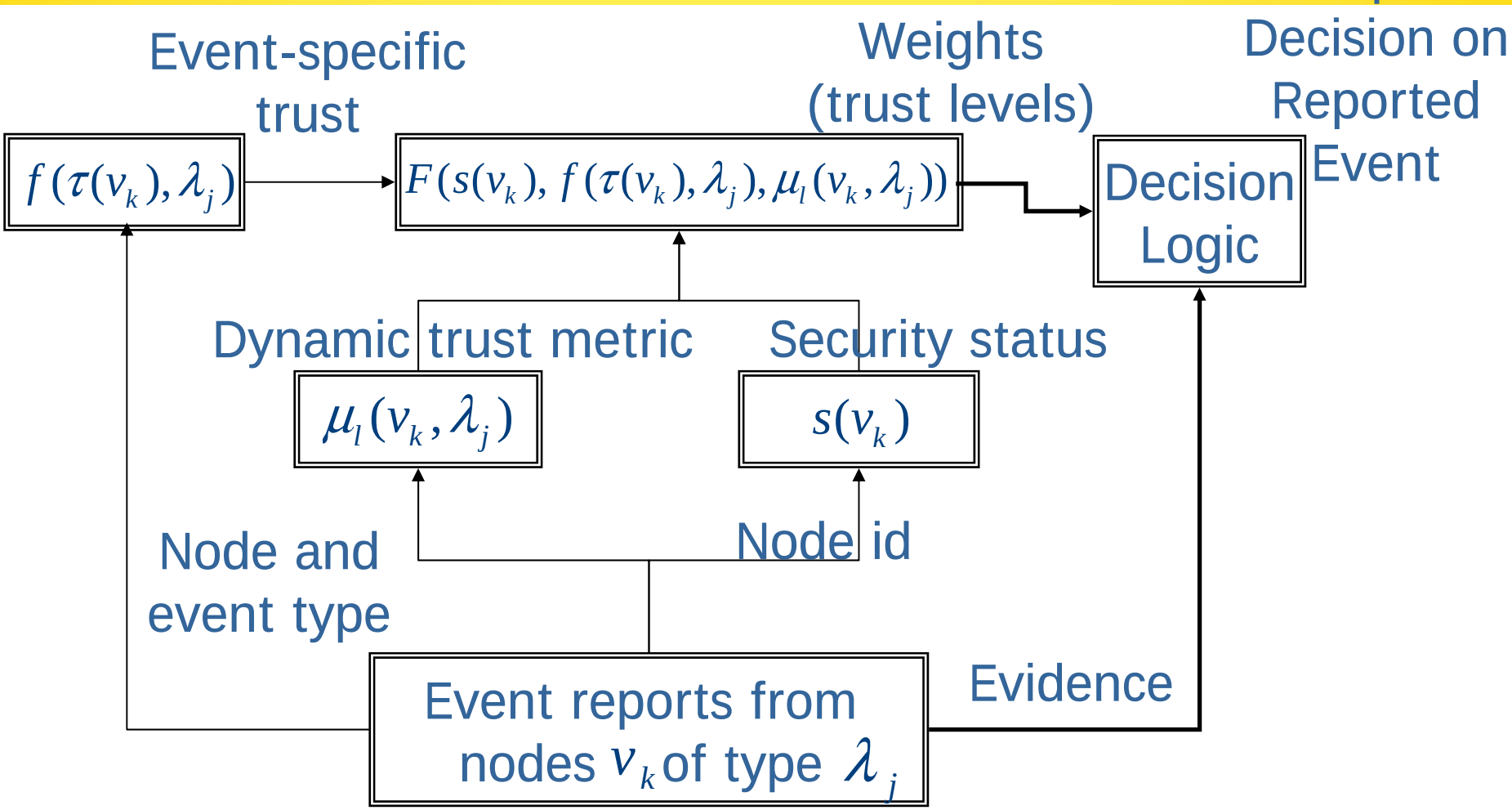
Data-centric trust establishment (cont'd)



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

Conclusions

- Secure vehicular communication architecture
- Trustworthy data are critical
  - Vehicular communication applications (safety, efficiency)
  - Monitoring applications that leverage on vehicular communication systems
- Challenging problem
- Awareness and encouraging results
- Latest developments:
  - Workshop on "Secure Vehicular Communications: Results and Challenges Ahead," Feb. 20-21, 2008
  - http://lcawww.epfl.ch/papadimitratos/SVCWCR/index.html