Secure Vehicular Communications – An Architectural View

Panos Papadimitratos
EPFL
panos.papadimitratos@epfl.ch

Problem

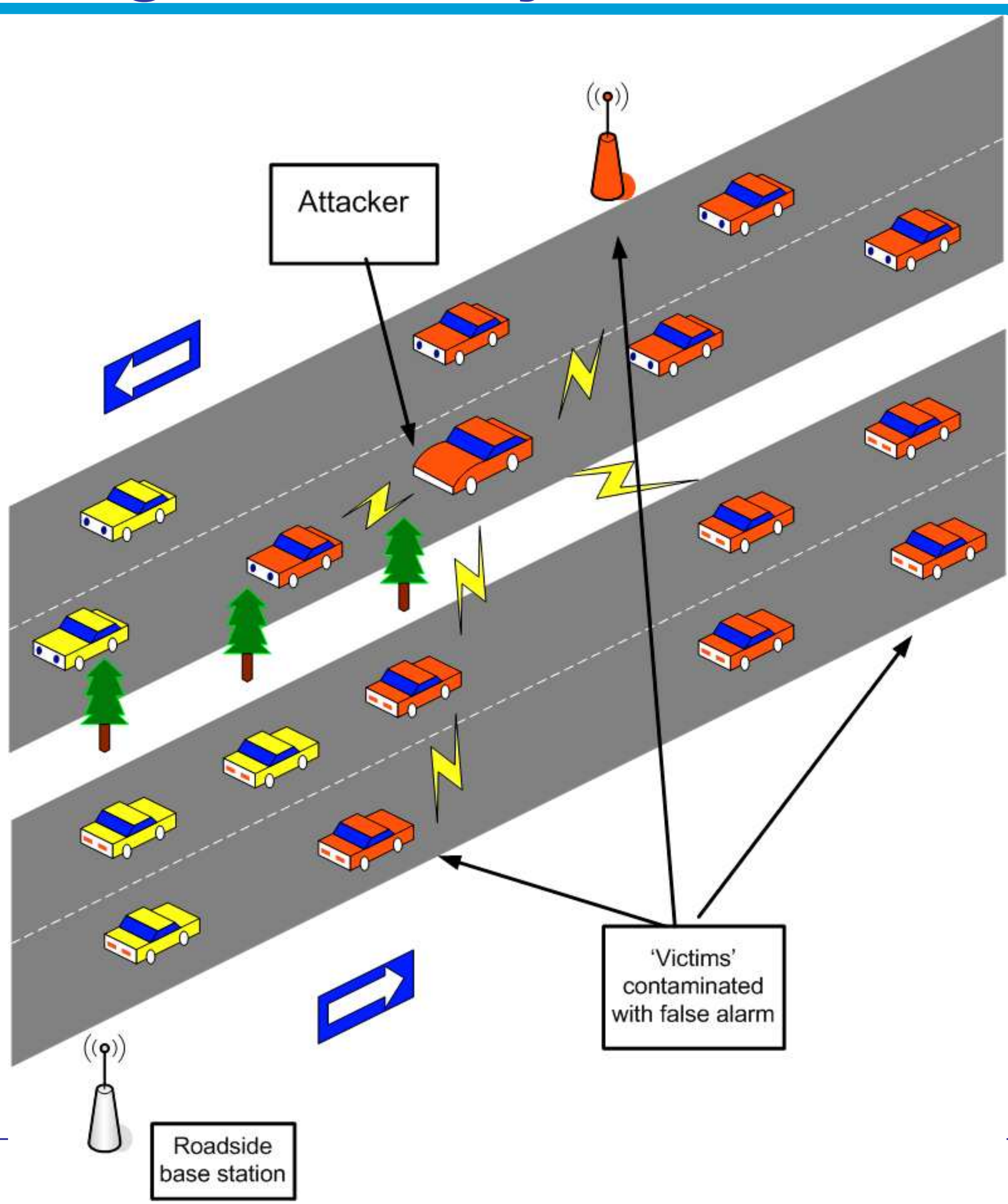
- Vehicular Communications (VC) / Vehicular Ad Hoc Networks (VANET)
  - Technology in the making
  - Wide (eventually) yet gradual deployment
  - Interoperability
  - Standardization
- Security and Privacy
  - Basic requirements/prerequisites
  - No retrofitting

Security and Privacy - Why?

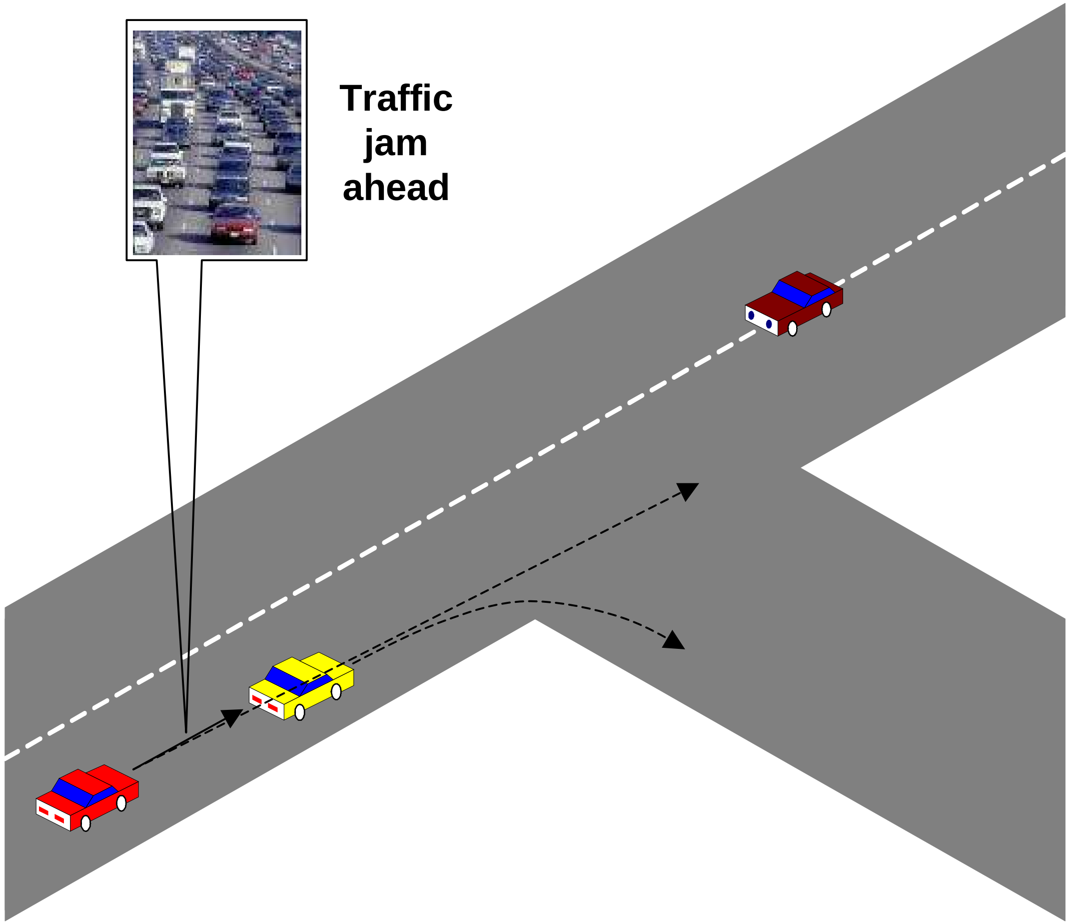
SEVECOM

- Without robust designs, VC systems may facilitate antisocial behavior
- The deployment of vulnerable VC systems may cancel out their envisioned benefits
- Abused, poorly defended VC systems can cause damages and high cost
- Attackers and adversaries will always be present

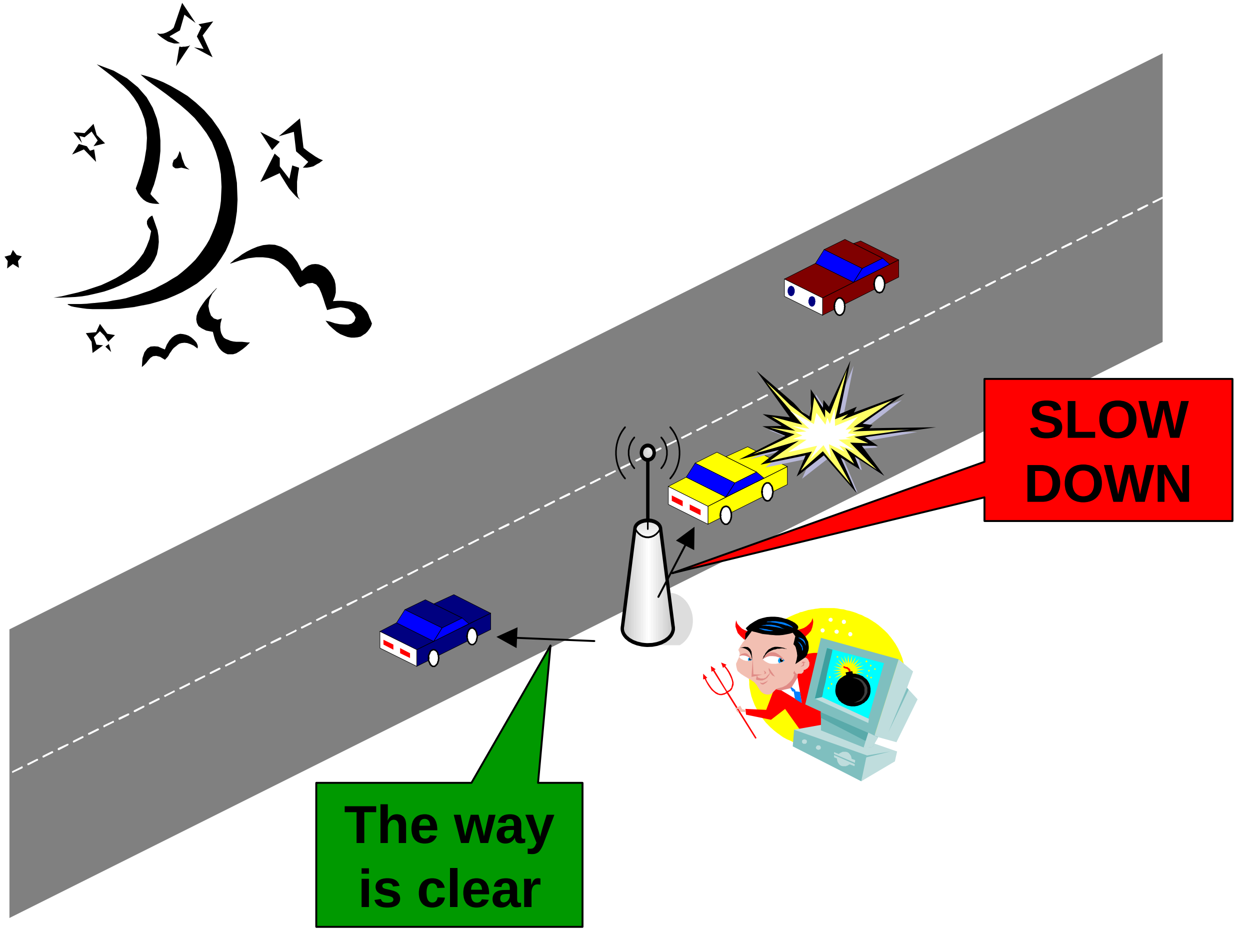
Attacking the VC system



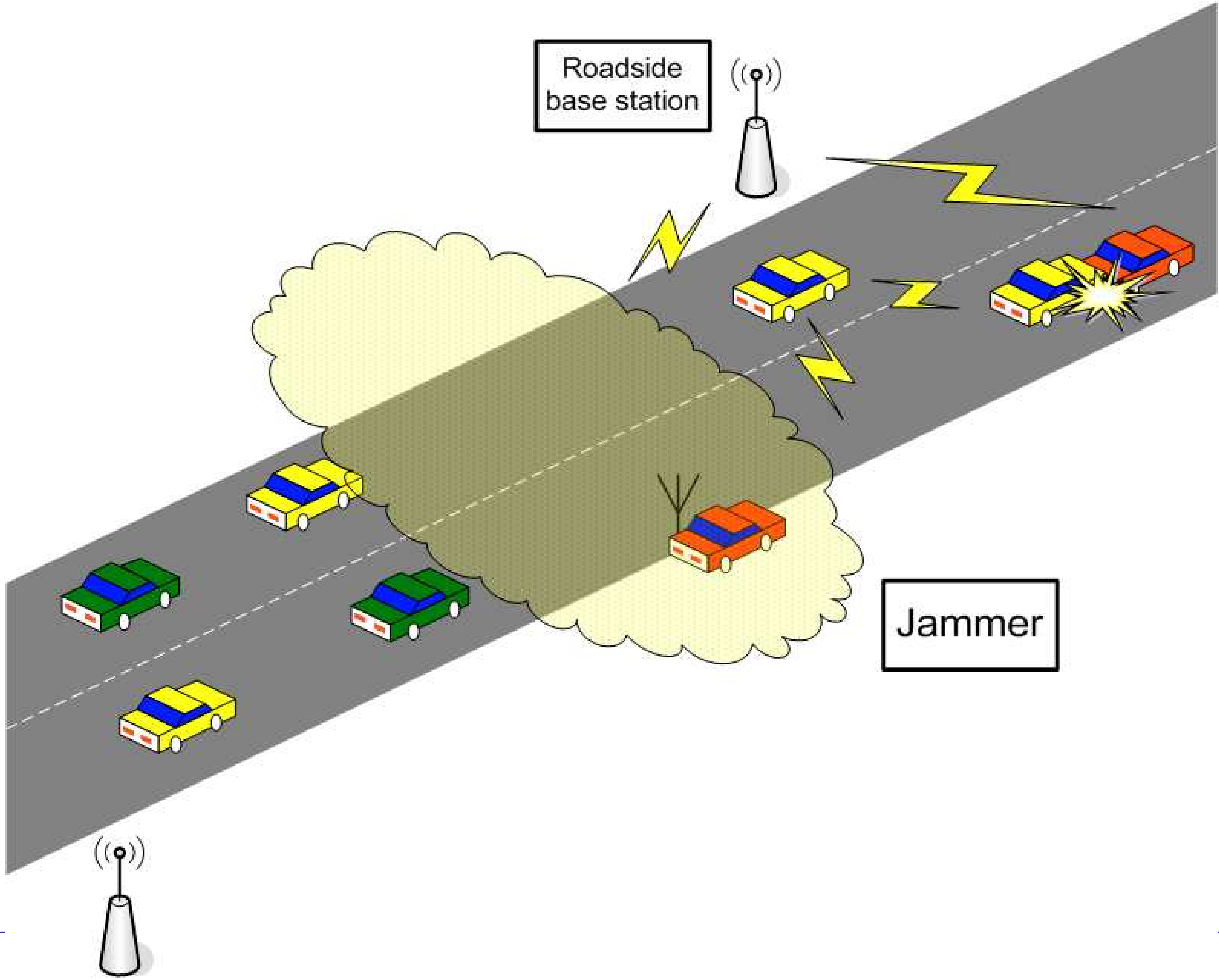
Attacking the VC system (cont'd)



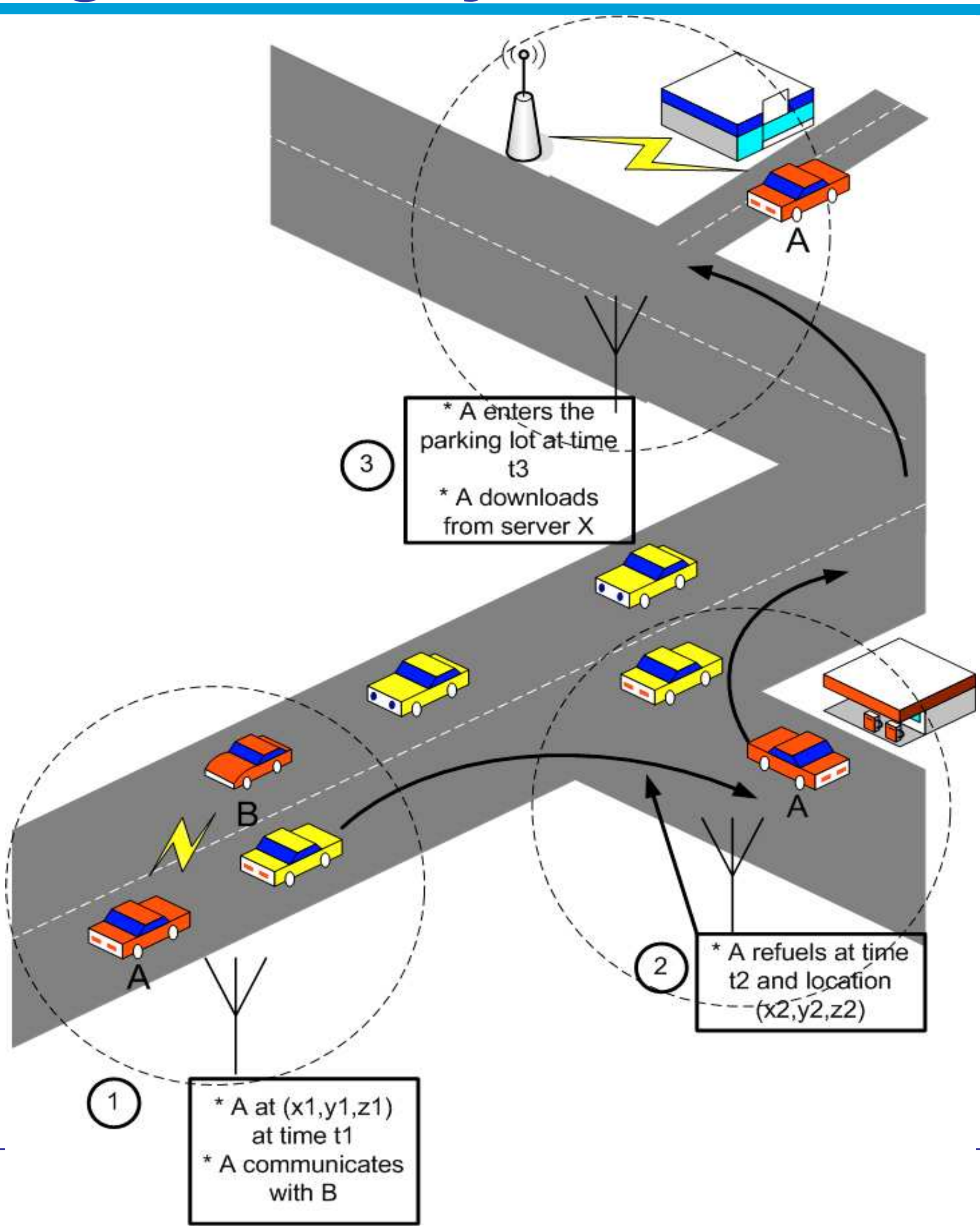
Attacking the VC system (cont'd)



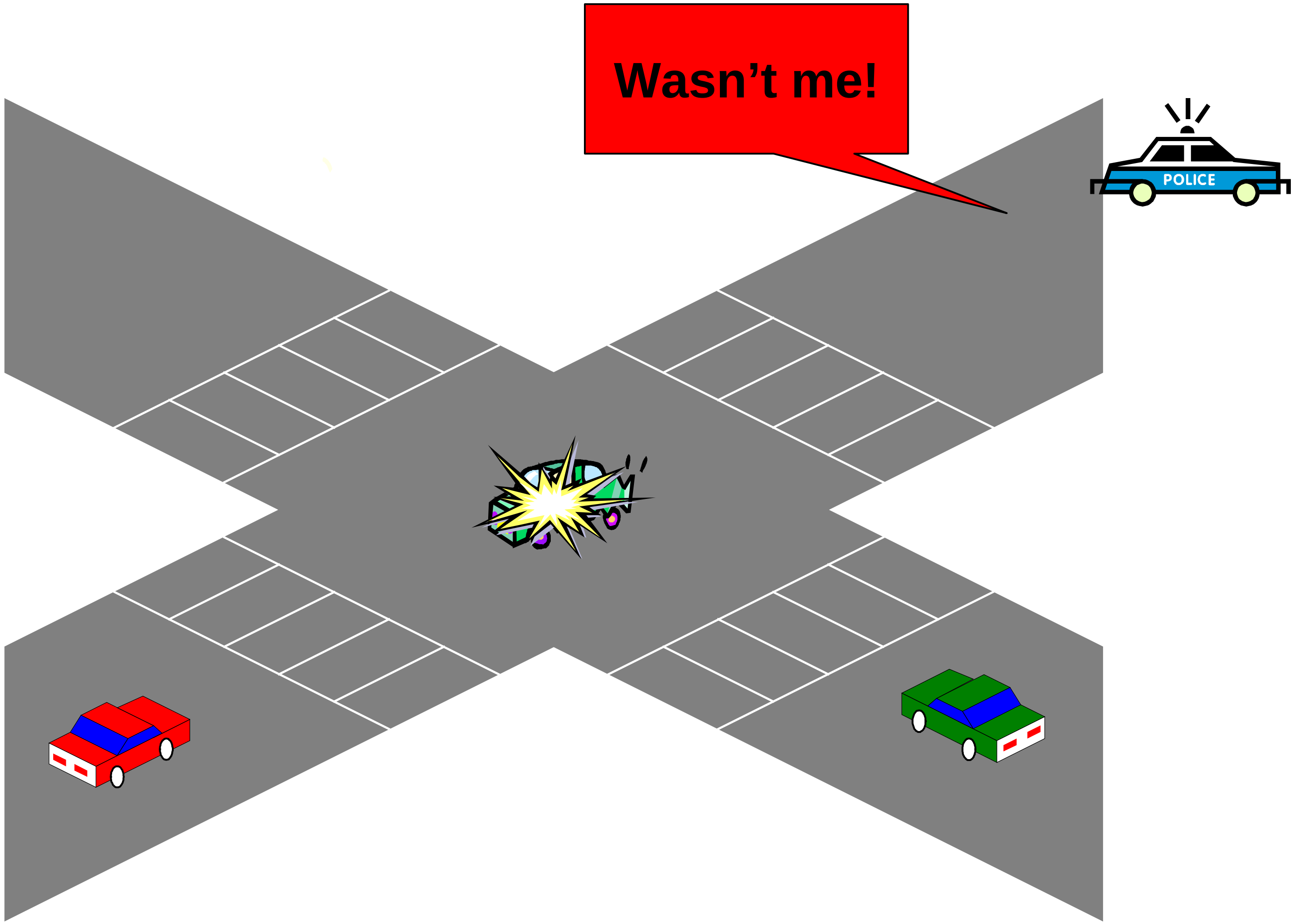
Attacking the VC system (cont'd)



Attacking the VC system (cont'd)



Attacking the VC system (cont'd)



Requirements

- Point of caution
  - Not all requirements listed here are relevant to all applications and scenarios

- (1) Message Authentication and Integrity
  - Messages must be protected from any alteration and the receiver of a message must corroborate the sender of the message

Requirements (cont'd)

- (2) Entity authentication
  - The receiver is ensured that the sender generated a message *recently*
- (3) Message Non-Repudiation
  - The sender of a message cannot deny having sent a message
- (4) Access control
  - Distinct roles for different types of network entities
  - Regulate access to information/services
  - *Authorization:* Establish what each network entity is allowed to do (e.g., protocols to run, messages to send)

Requirements (cont'd)

- (6) Message Confidentiality
  - The content of a message is kept secret from those nodes that are not authorized to access it

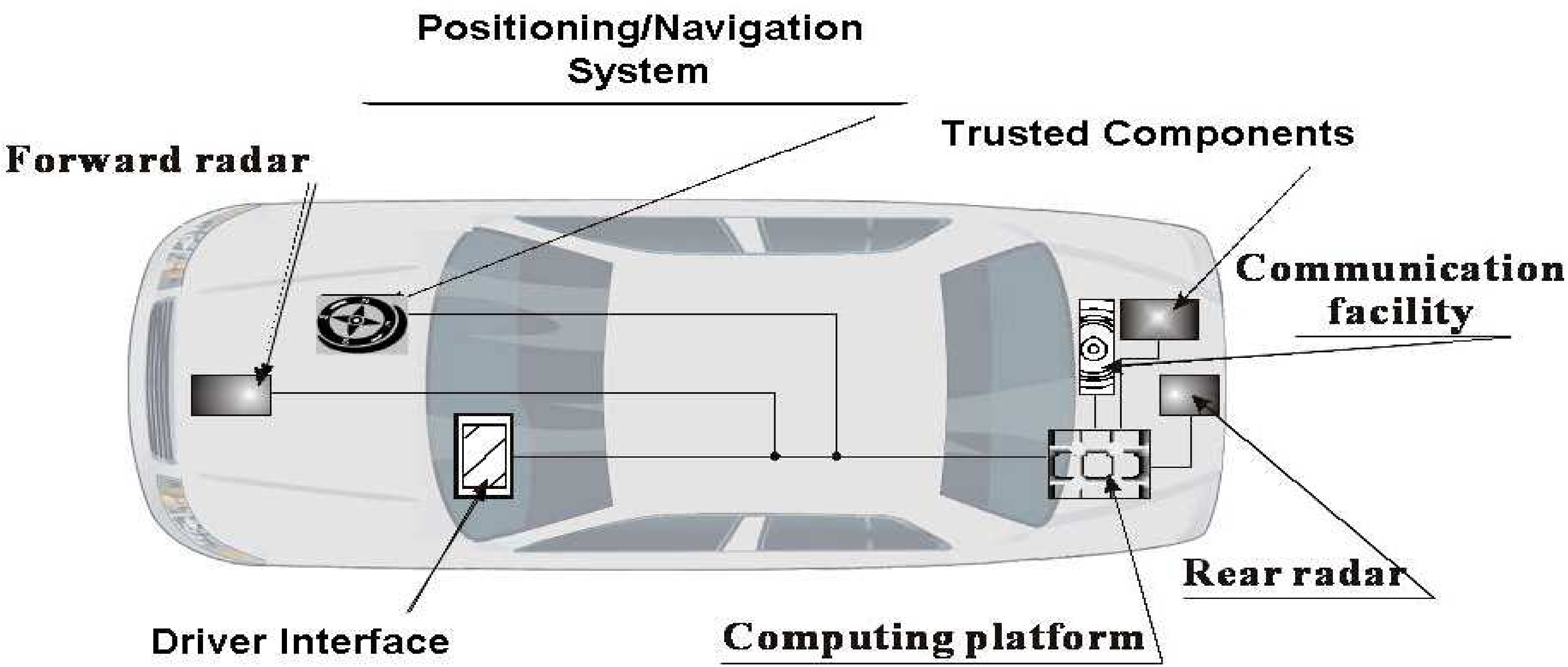
- (7) Privacy - Anonymity
  - *VC* systems should not disclose or allow inferences on the personal and private information of the users
  - At *minimum*, an observer can*not* learn if a node performed, or will perform in the future, a specific action, assuming that the node performs the action

Requirements (cont'd)

- (8) Availability
  - Protocols and services should remain operational even in the presence of faults, malicious or benign
  - Secure and fault-tolerant designs
  - Resilience to resource depletion attacks
  - Self-stable protocols
- (9) Liability
  - Users of vehicles are liable for their deliberate or accidental actions that disrupt the operation of other nodes, or the transportation system
  - The VC system should provide information that assists the attribution of liability
  - Auditing

Security architecture

- Smart vehicle



Security architecture (cont'd)

- Node *V*
  - Unique identity
  - Public / private key pair
    - K_V, k_V
  - Certificate
    - $Cert_X\{K_V,A_V\}$
  - Central processing and communication module
- Additionally (optionally)
  - Set of additional credentials/certificates and cryptographic keys

Security architecture (cont'd)

- Trusted components
  - Tamper-resistant
  - Storage
    - Cryptographic material
    - Data
  - Processing
    - Cryptographic operations
  - Motivation
    - Current state; Event Data Recorders (EDRs)
    - Bind physically cryptographic material to the vehicle

Security architecture (cont'd)

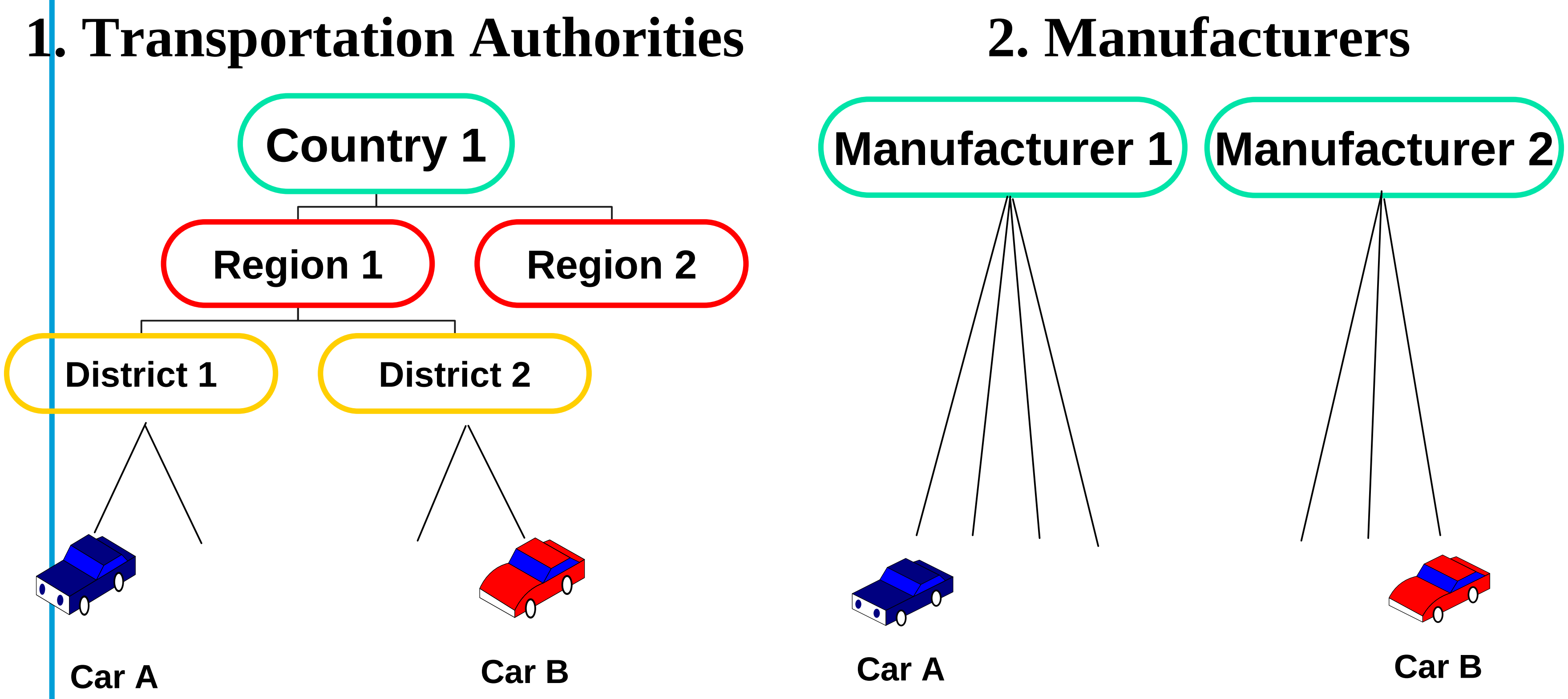
- Public (e.g., emergency, police, buses) vehicles
- Infrastructure (road side units)
- Assigned special roles and attributes
  - Relatively more trustworthy
  - Facilitate security-related operations

Security architecture (cont'd)

- Authorities
  - Trusted entities issuing and managing identities and credentials for all *VC* system entities
  - Multiple and distinct
  - S_X set of *VC* system entities registered with an authority *X*
- Also known as:
  - Certification Authorities (CAs)
  - (Vehicular) Public Key Infrastructure

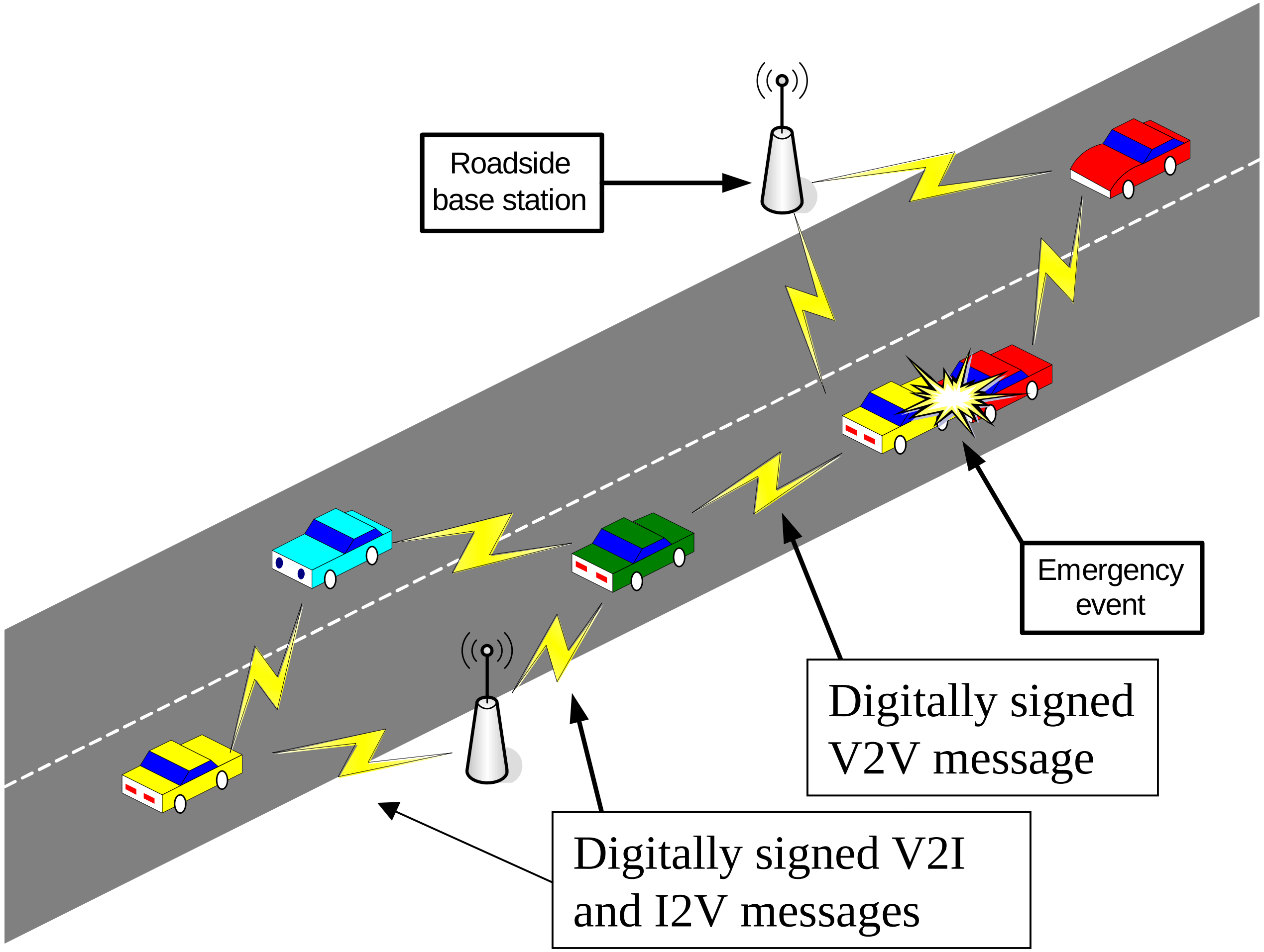
Security architecture (cont'd)

- Options for instantiating an Authority

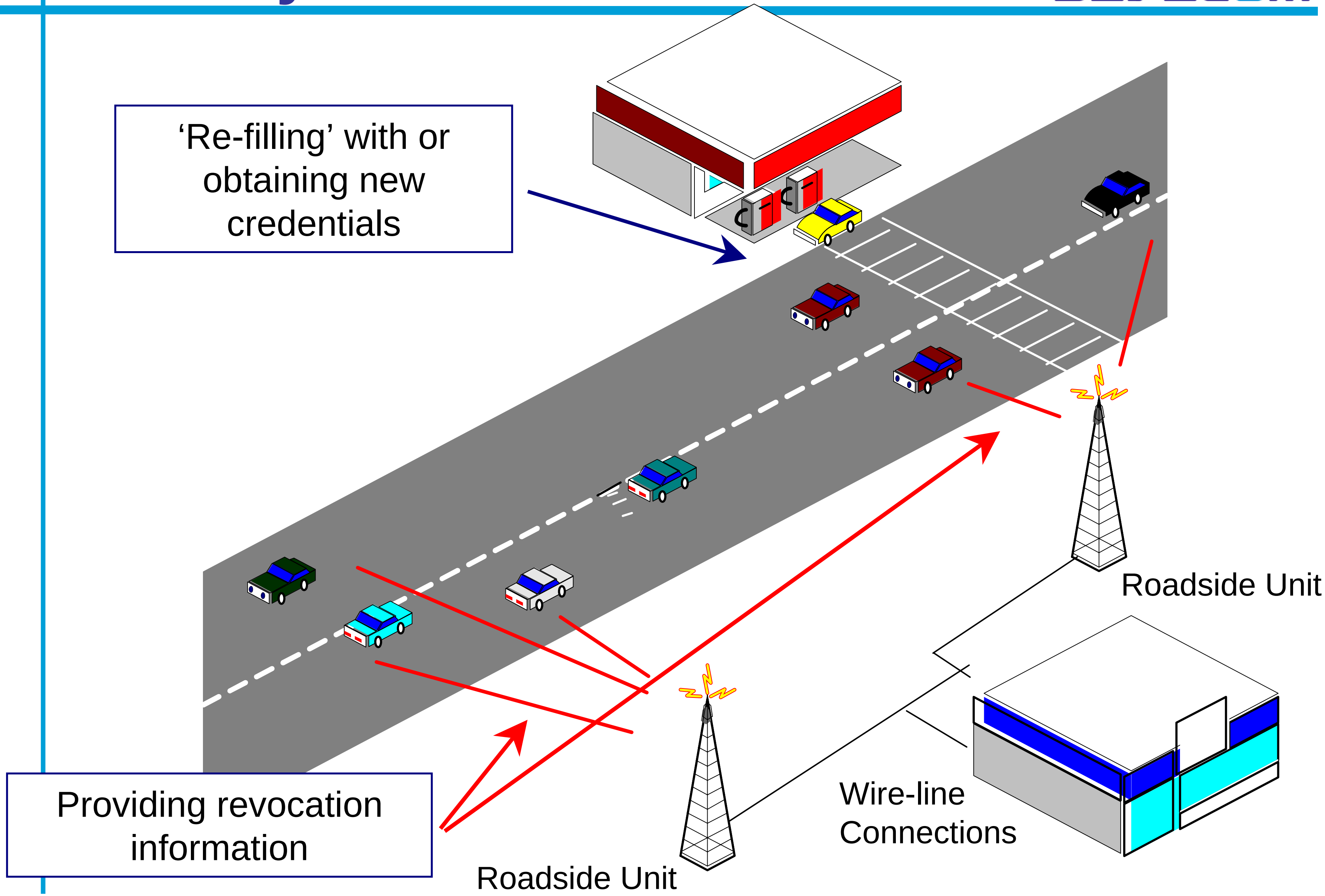


Security architecture (cont'd)

- Vehicle-to-vehicle (V2V) and Vehicle-to-Infrastructure (V2I) secure communication

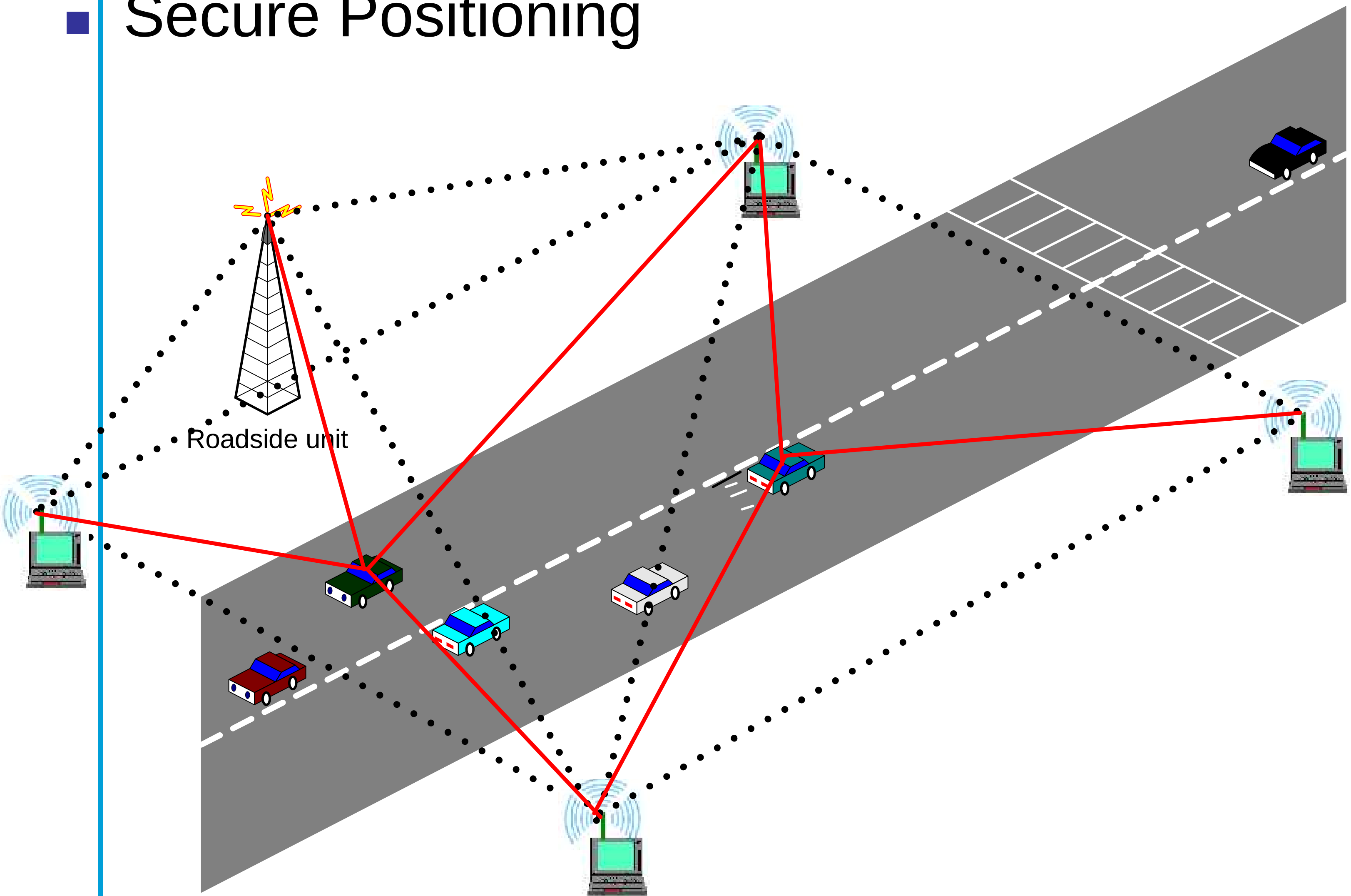


Security architecture (cont'd)



Security architecture (cont'd)

- Secure Positioning

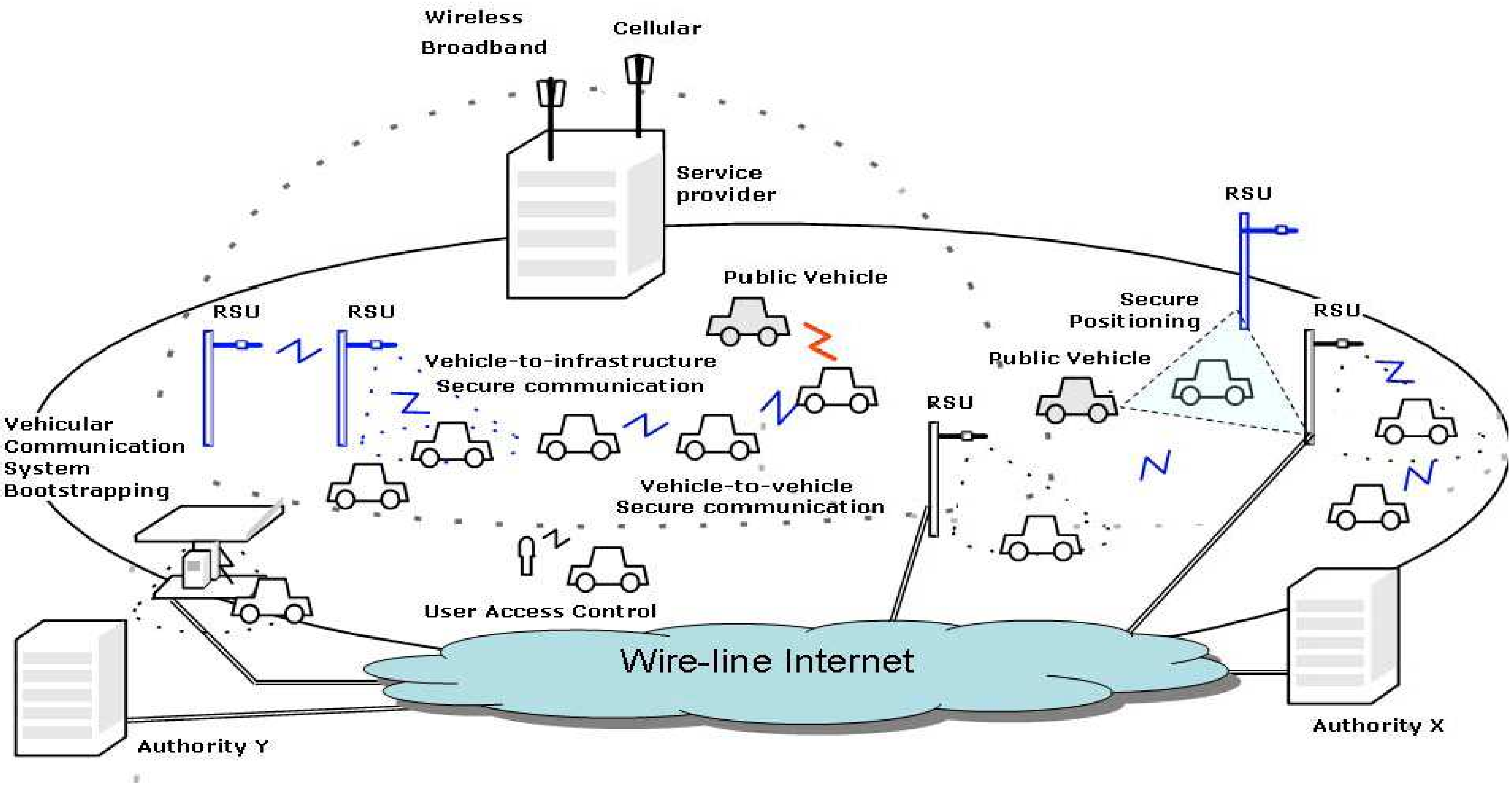


Security architecture (cont'd)

- Other aspects
  - In-car security
  - User identification
  - User-vehicle association
  - Resilience to false measurements/data
  - Resilience to resource-depletion Denial of Service (DoS) attacks
  - …

Security architecture (cont'd)

- Overall System View



Conclusion

- Security and privacy-enhancing mechanisms for vehicular communication systems are a prerequisite for their deployment
- Securing VC systems is a complex problem
- On the positive side
  - Real problem
  - Constrained problem space
- Opportunity
  - Awareness
  - Joint efforts in industry and academia
  - Standardization

Questions?

SEVECOM

http://ivc.epfl.ch

http://www.sevecom.org