


# Privacy-Enhancing Technologies for Vehicular Communications (VC)

Susan Hohenberger and Panos Papadimitratos

IBM

sus@zurich.ibm.com

EPFL

panos.papadimitratos@epfl.ch

# Pre-VC Transportation Systems

- Administered by public organizations
  - City, County, State Authorities
- Participants
  - Vehicles
  - Drivers
- Rigid identity management processes
- Liability

# Pre-VC Transportation Systems (cont'd)

- Drivers and vehicles already identified in multiple ways
  - Drivers
    - Name
    - License number
    - Mailing address
    - Date of birth
  - Vehicles
    - Vehicle identification number (VIN)
    - Registration number
    - Technical information
      - Type
      - Model
      - Color

# Vehicular Communication Systems

SEVECOM

- System participants
  - Users
  - Network nodes
  - Authorities
- Binding users to vehicles is an important issue
  - Many-to-many relationship
- Focus on network operation and device communication

# Vehicular Communication Systems
(cont'd)

SEVECOM

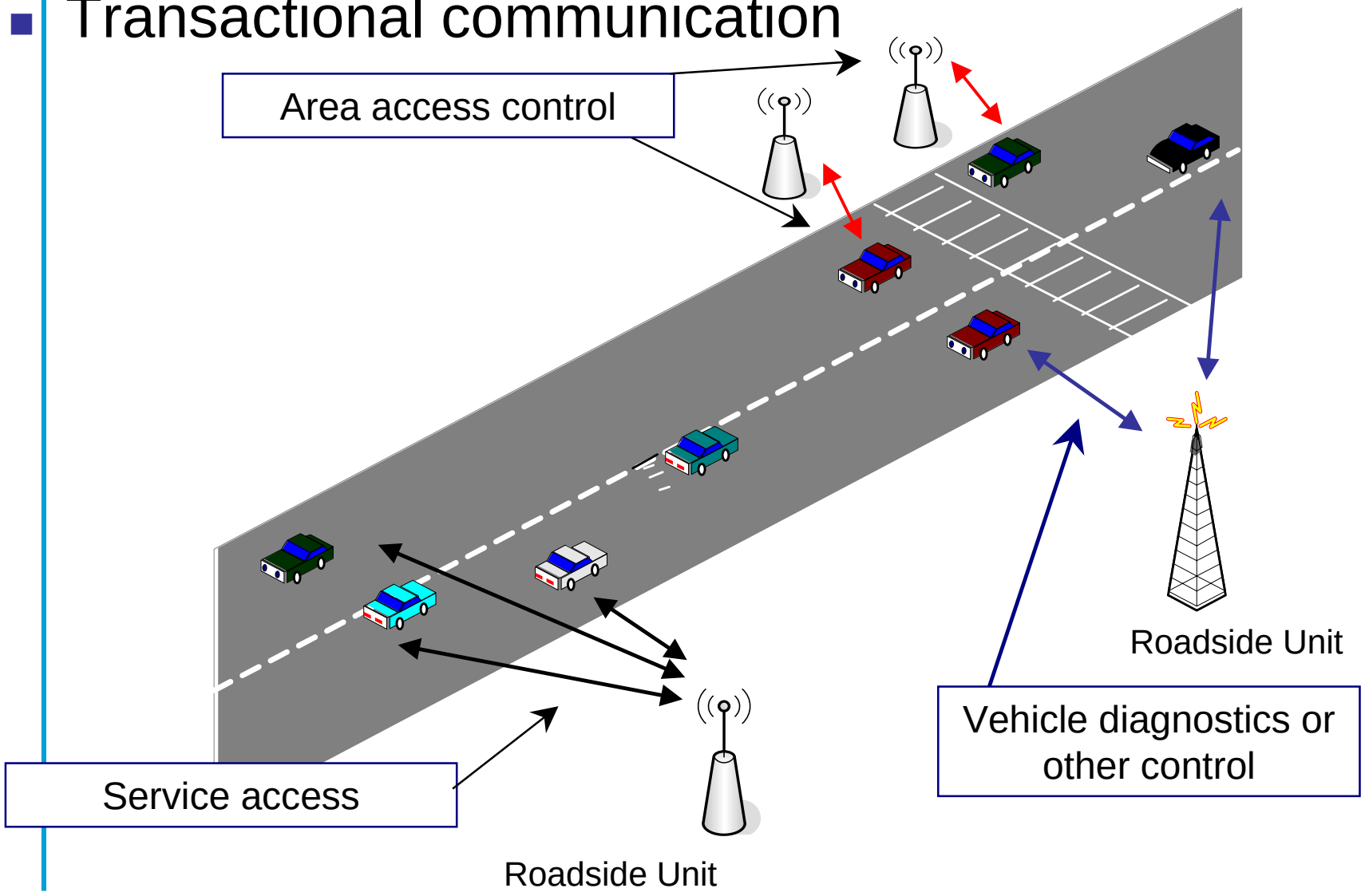
- Relation between "physical" and VC identities
  - Integration - Adaptation
  - Extension
- Vehicular communications identity
  - "Physical world" attributes
  - Network identifiers
    - At different layers of the protocol stack
  - Service identifiers/credentials
  - Cryptographic keys and credentials

# Requirements

- Infrastructure and Public Vehicles
  - No anonymity or privacy enhancement mechanisms
  - Rich description of node attributes
  - Authentication
- Private vehicles
  - Privacy enhancing technologies are necessary
  - Authentication

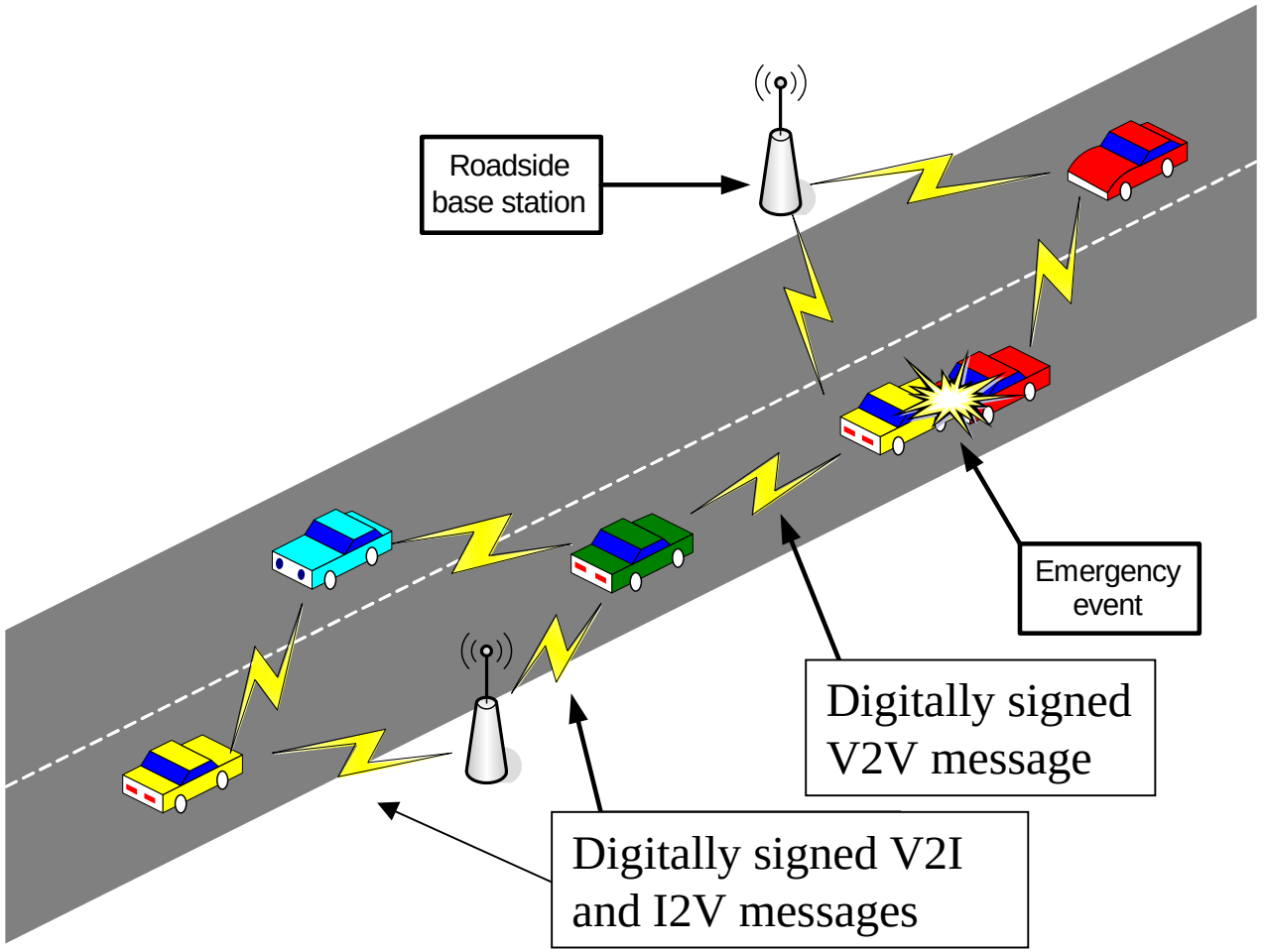
# Scenario 1

- Transactional communication



# Scenario 2

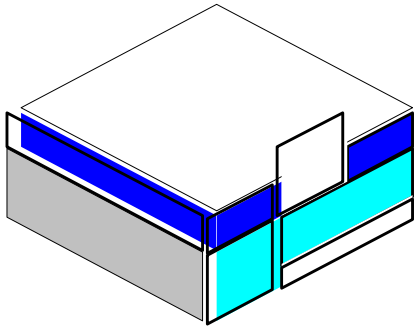
- Safety alerts / messages
  - Periodic, triggered, frequent

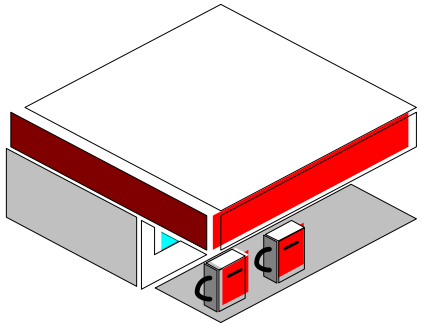


# Requirements (cont'd)

- Full anonymity
  - For an observer, an action could have been performed by any other entity in the system
- In our context, 'system' is $S_X$, the set of nodes registered with an Authority *X*
- Example
  - For each and every safety-related message a vehicle *V* sends, an observer that collects all messages can only guess with probability $1/|S_X|$ that *V* was the sender for each of them

# Anonymity



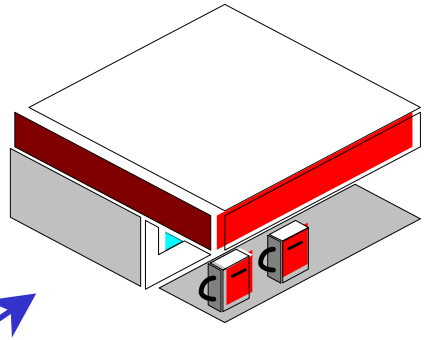


- Authority *X*
  - Provides $Cert_X\{K_V,A_V\}$ to the vehicle *V*
  - $K_X$
- Authority *A*
  - Issues credentials for anonymous authentication
  - $K_A$

- Vehicle *V*
  - $K_V,k_V$
  - $Cert_X\{K_V,A_V\}$
  - $K_X$, $K_A$

# Anonymity (cont'd)

- *Join*
  - Interactive protocol
  - $V$ becomes a member of $G_A$
  - $V$ obtains a secret value $sk_V$ and a membership certificate



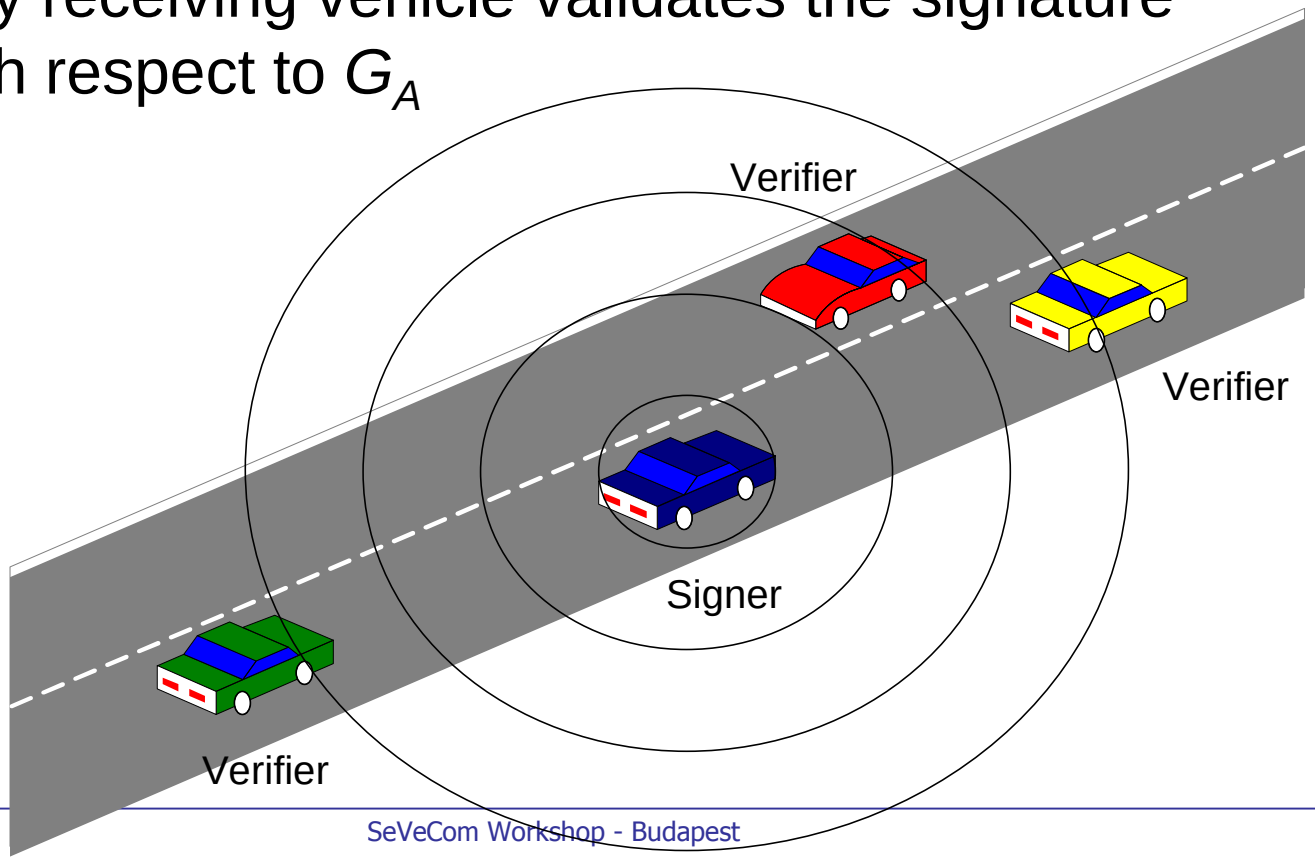
- Authority $A$

- Vehicle $V$

- There is a single public key for $G_A$

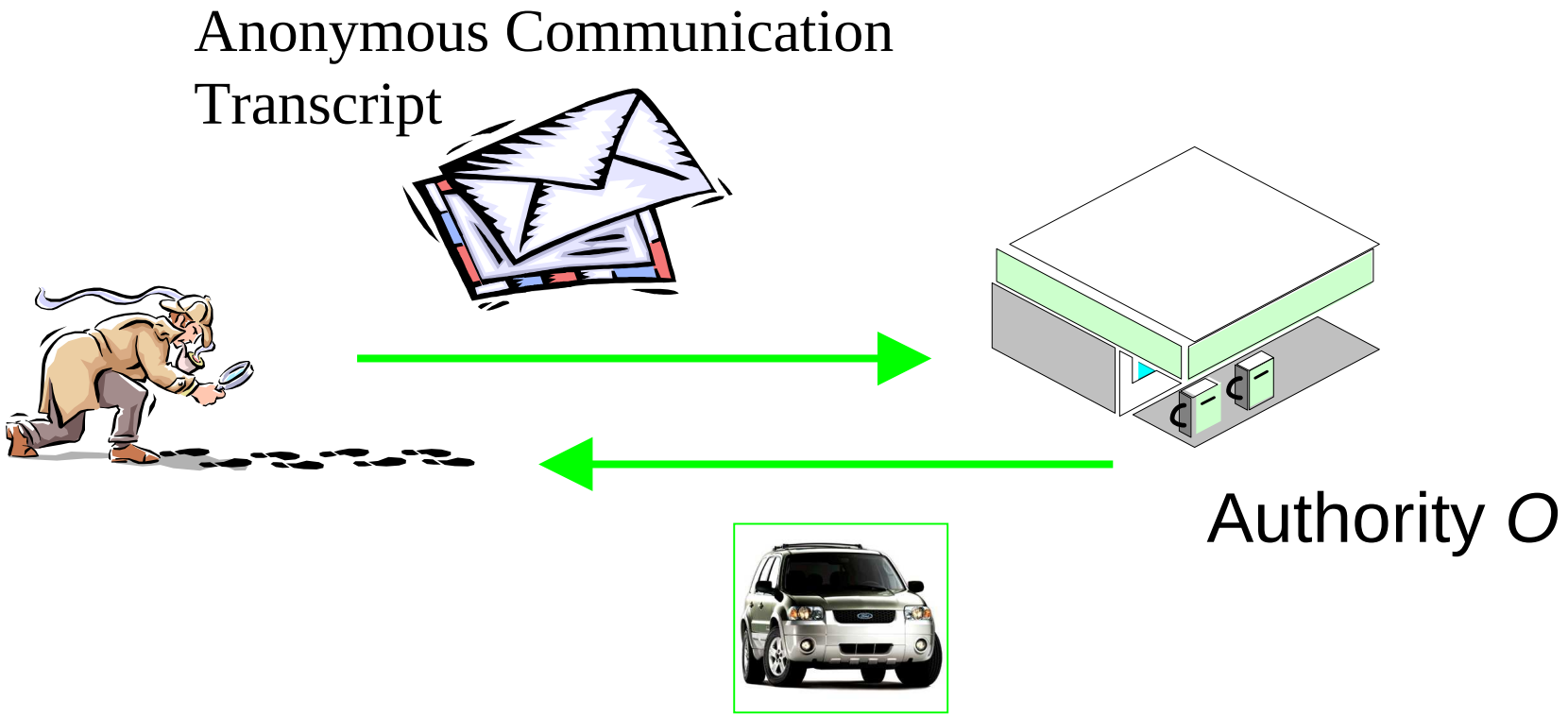
# Anonymity (cont'd)

- *Sign/show*
  - The vehicle uses its secret and membership
- *Verify*
  - Any receiving vehicle validates the signature with respect to $G_A$



# Anonymity (cont'd)

- *Open – Anonymity revocation*



# K-Anonymity

- Limitation of the anonymous system
  - A legitimate member of $G_A$ can generate a large number of unlinkable messages
  - Impact depends on the application
- Solution
  - *K-anonymity*: *K-times per time period* anonymous authentication
  - A legitimate member can use its credentials only up to *K* times within a given time interval

# Recap

- For private vehicles
  - Anonymity
  - K-Anonymity
- ‘Classic’ cryptography cannot provide these features
- New cryptographic primitives are necessary