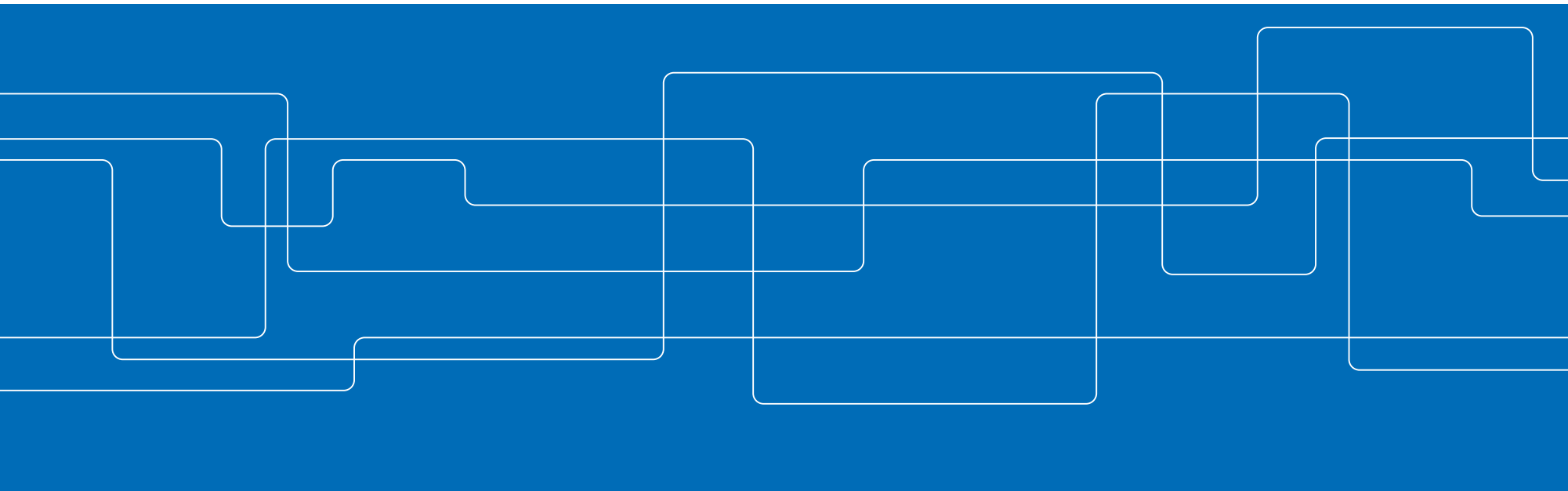
KTH ROYAL INSTITUTE
OF TECHNOLOGY

Security and Privacy in Vehicular Social Networks

Hongyu Jin, Mohammad Khodaei, and
Panos Papadimitratos

Networked Systems Security Group (NSS)

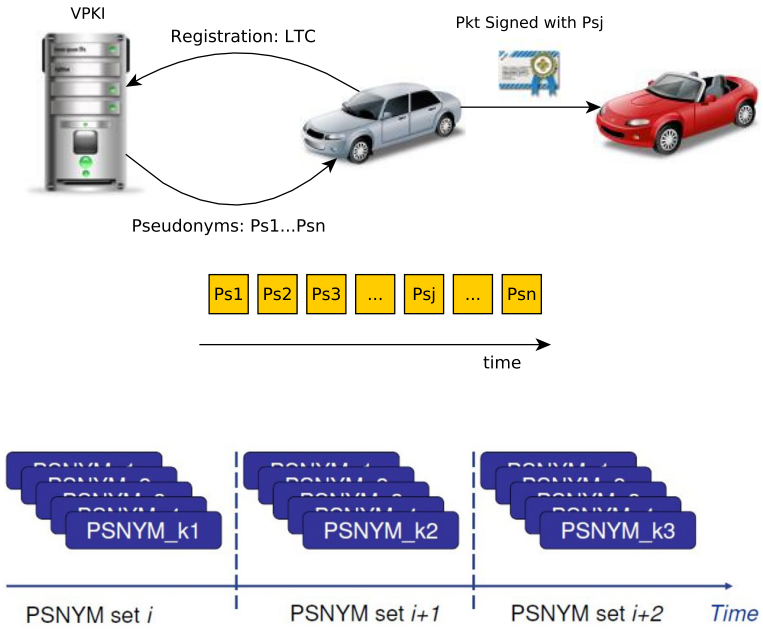
www.eecs.kth.se/nss



Security and Privacy for Vehicular Communication (VC) Systems

Basic Requirements

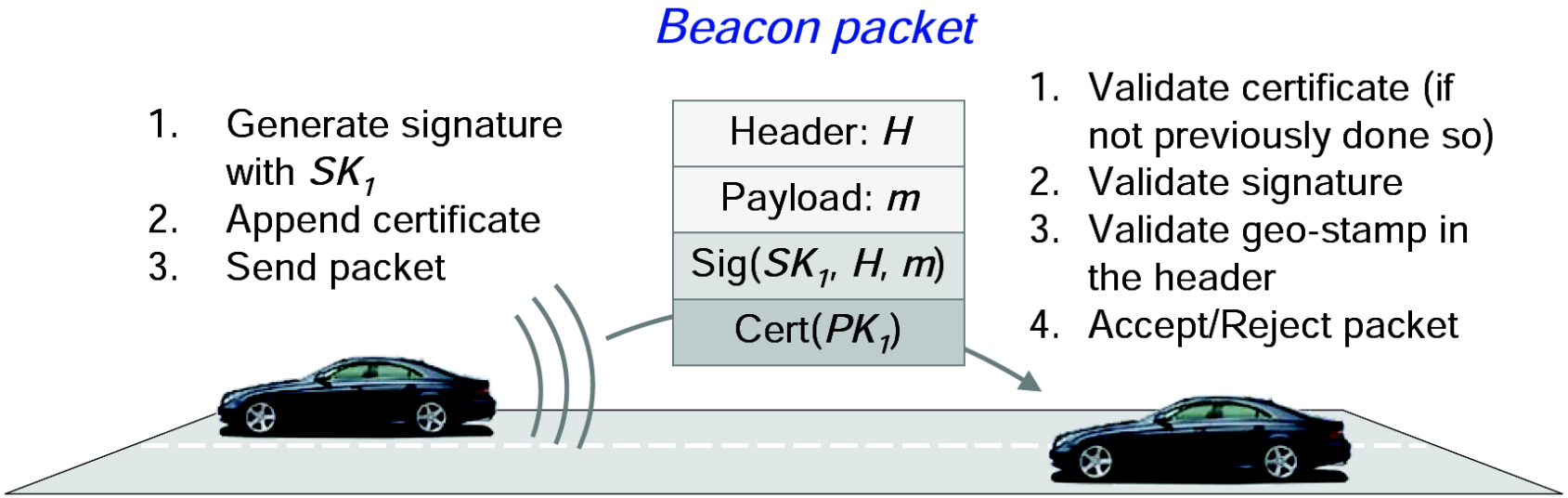
- Authentication & integrity
- Non-repudiation
- Authorization and access control
- Conditional anonymity
- Unlinkability (long-term)



Vehicular Public-Key Infrastructure (VPKI)

- Pseudonymous authentication
- Trusted Third Party (TTP):
  - Certification Authority (CA)
  - Issues credentials & binds users to their pseudonyms

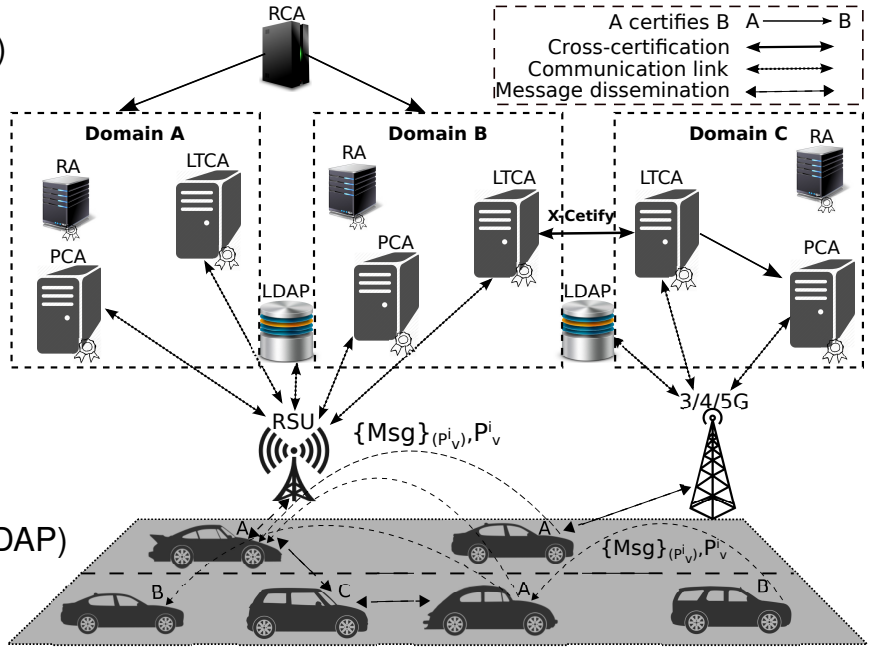
Security and Privacy for VC Systems (cont'd)



- Sign packets with the private key, corresponding to the current valid pseudonym
- Verify packets with the valid pseudonym
- Cryptographic operations in a Hardware Security Module (HSM)

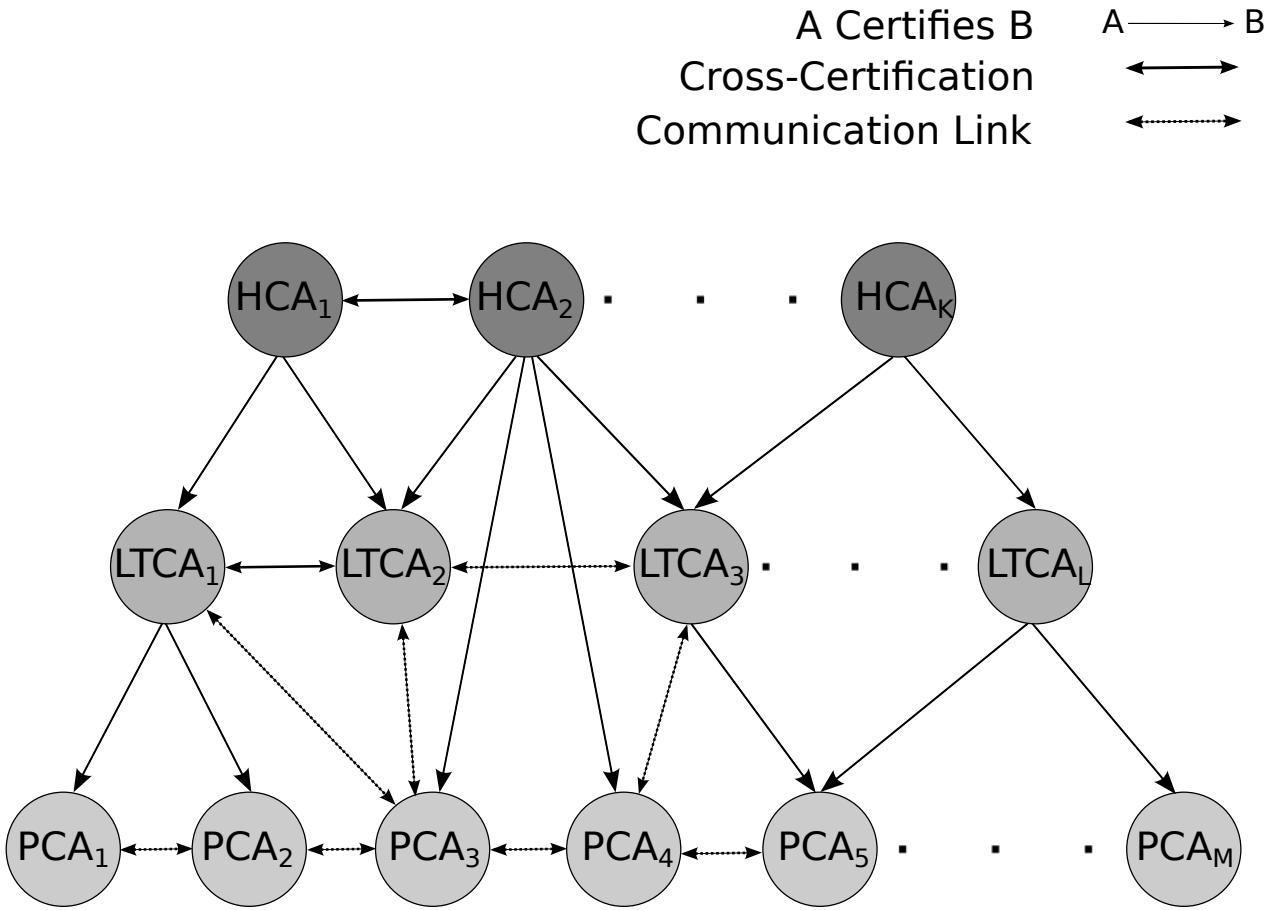
Security and Privacy for VC Systems (cont'd)

- Vehicular Public-Key Infrastructure (VPKI)
- Root CA (RCA)
- Long Term CA (LTCA)
- Pseudonym CA (PCA)
- Resolution Authority (RA)
- Lightweight Directory Access Protocol (LDAP)
- Roadside Unit (RSU)



- Vehicles registered with one LTCA (home domain)
- PCA servers in one or multiple domains
- Vehicles can obtain pseudonyms from any PCA
- Establish trust among entities with a RCA or with cross-certification
- Resolve (de-anonymize) a pseudonym with the help of an RA

Hierarchical Organization of the VC Security Infrastructure



HCA: Higher Level Authority

Security and Privacy Requirements

- Authentication and Integrity
- Confidentiality
- Accountability and Non-repudiation
- Unlinkability and Anonymity
- Access Control
- Availability

Adversarial Model

- Honest-but-Curious Entities
  - Extend our adversarial model from fully-trustworthy to honest-but-curious servers. Honest-but-curious entities never deviate from system security policies or protocols, but they are tempted to infer and exploit user sensitive information, e.g., profile users and push advertisements to users based on their interests.
- Malicious Participants
  - Registered vehicles and users (legitimate insiders) disseminate faulty information
- Selfish Participants
  - Such users could try to achieve higher and optimal awards by sacrificing the minimum resources. These misbehaving internal adversaries utilize the resource of other nodes to achieve a better service without participating in the tasks.

Vehicular Social Network (VSN)

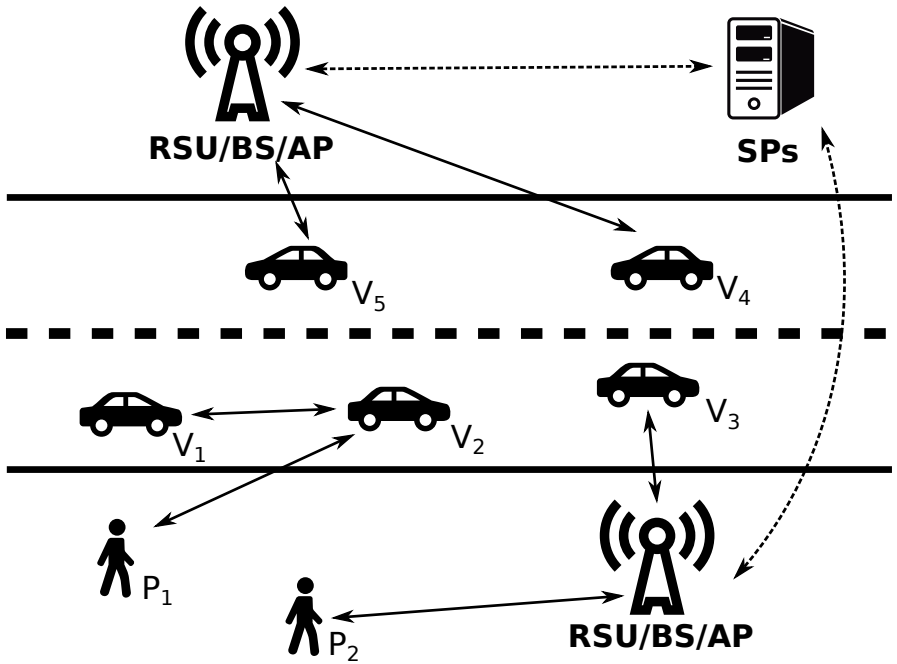


Figure: Illustration of VSNs: (1) Vehicles (with OBUs, e.g., V_3, V_4 and V_5) and users (with smartphones, e.g., P_2) can access various Service Providers (SPs) via Roadside Units (RSUs), Base Stations (BSs) or Access Points (APs); (2) Vehicles (e.g., V_1 and V_2) or users (e.g., P_1) can interact with each other over an ad-hoc network (e.g., share information obtained from SPs).

Pseudonymous Authentication in VSN

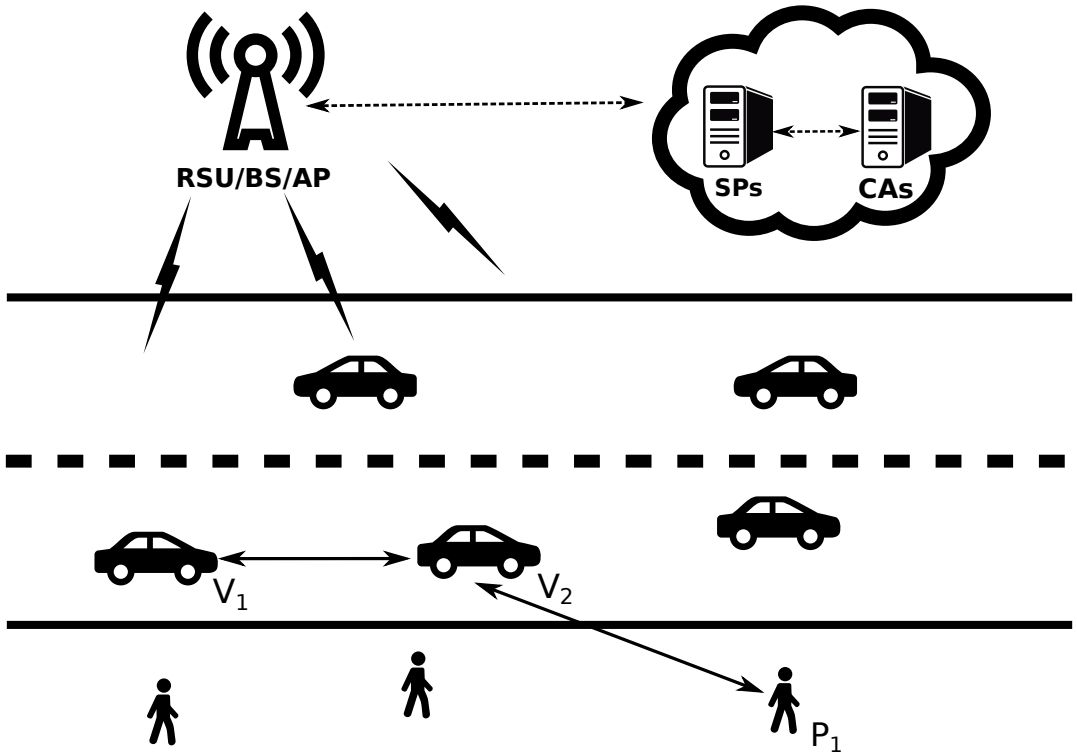


Figure: Vehicles and users can obtain pseudonyms from the Certification Authorities (CAs). The communication in the VSNs is protected with pseudonymous authentication including P2P communication (e.g., V_1-V_2 and V_2-P_1) in the ad-hoc network and vehicle/user-SP communication.

Privacy Challenges

Stronger adversarial model

- User privacy protection against *honest-but-curious* entities
- Inference of service provider or time

LTCA infers relevant information from the requests

- Direct (C2C-CC design) or indirect (ticket-based designs) approaches
- Actual pseudonym acquisition period
- Targeted PCA that the vehicle seeks to obtain credentials from

Trivially linking pseudonyms issued by the PCA

- Fully-trusted proxy-based scheme that shuffles the requests
- Honest-but-curious proxy?

Resilience Considerations

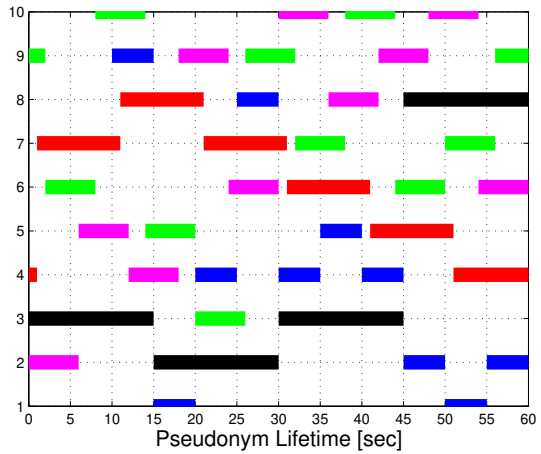
Sybil-based misbehavior

- Acquisition of multiple simultaneously valid credentials
- Allow several pseudonymous valid simultaneously for a specific period of time (C2C-CC or CAMP project)
  - Changing the certificate in a critical traffic situation (e.g., intersection, accident)
  - Safety applications necessitate partial linkability
  - But what if a vehicle gets compromised?
  - Injecting multiple erroneous hazard notification
- VPKI should ensure a compromised vehicle cannot obtain multiple pseudonyms valid simultaneously
  - along with enforcing a policy on the vehicle side
- Standardization bodies and harmonization efforts do not preclude such misbehavior

Pseudonym Lifetime Policy

- Ideally one pseudonym for a single message authentication; but costly, e.g. 10 beacons per sec.
- Safety applications necessitate partial linkability, e.g., collision avoidance: inferring a collision hazard based on unlinkable CAMs is hard; requires precise location information.
- No conclusive view or guideline for pseudonym lifetime policy

- Sybil-based misbehavior → Non-overlapping lifetime
- Flexible access to PCA → undermine unlinkability
- Timing information makes sets of pseudonyms linkable



Certificate Revocation List (CRL)

Revocation

- Eviction of the wrong doers in case of misbehavior
- Not straightforward in the VC systems
  - Multiplicity of pseudonyms
  - Very large number of pseudonyms, thus huge revocation list
  - Efficient distribution of the revocation list among mobile entities
  - Limited memory/bandwidth consumption through usage of CRL

Diminish such vulnerability

- Requiring the vehicles to interact with the VPKI regularly
- Or at least as frequently as dissemination of information by PCA

The remaining challenge:

- No consensus on the need and the method: C2C-CC suggests to preload with 1500 pseudonyms for a year and let them expire (no revocation)
- Timely dissemination of credential validity information
  - Time, cost, bandwidth, network accessibility, etc.

Inference Attacks

- Openness of wireless communication and dissemination of basic safety messages in plaintext (as confidentiality is not needed in VC systems)
- Vehicle Traceability
- **Syntactic Linking:** An adversary might observe an isolated pseudonym change, and associate the old and new pseudonymous identifiers through syntactic linking.
- **Semantic Linking:** An adversary could leverage physical constraints of the road layout, and message payload, e.g., location, velocity, time, acceleration, the length and width 1 of a victim's vehicle, to predict its trajectory towards linking messages semantically.

Other Challenges

- Extending to anonymous authentication primitives
  - Group signature schemes
  - Zero-knowledge proof
- Extensive experimental validation
  - SEROSA
  - SR-VPKI
- Operational challenges:
  - Who is in charge of the identity and credential management
  - How to establish the trust:
    - [Saab, Scania, Volvo] and [Volkswagen, BMW]
    - [EU] and [US]

Security and Privacy in Vehicular Social Networks

Hongyu Jin, Mohammad Khodaei, and
Panos Papadimitratos

Networked Systems Security Group (NSS)

www.eecs.kth.se/nss

In Vehicular Social Networks, A. M. Vegni, V. Loscri, and A. V. Vasilakos, Eds. CRC Press, Taylor & Francis Group, March 2017.