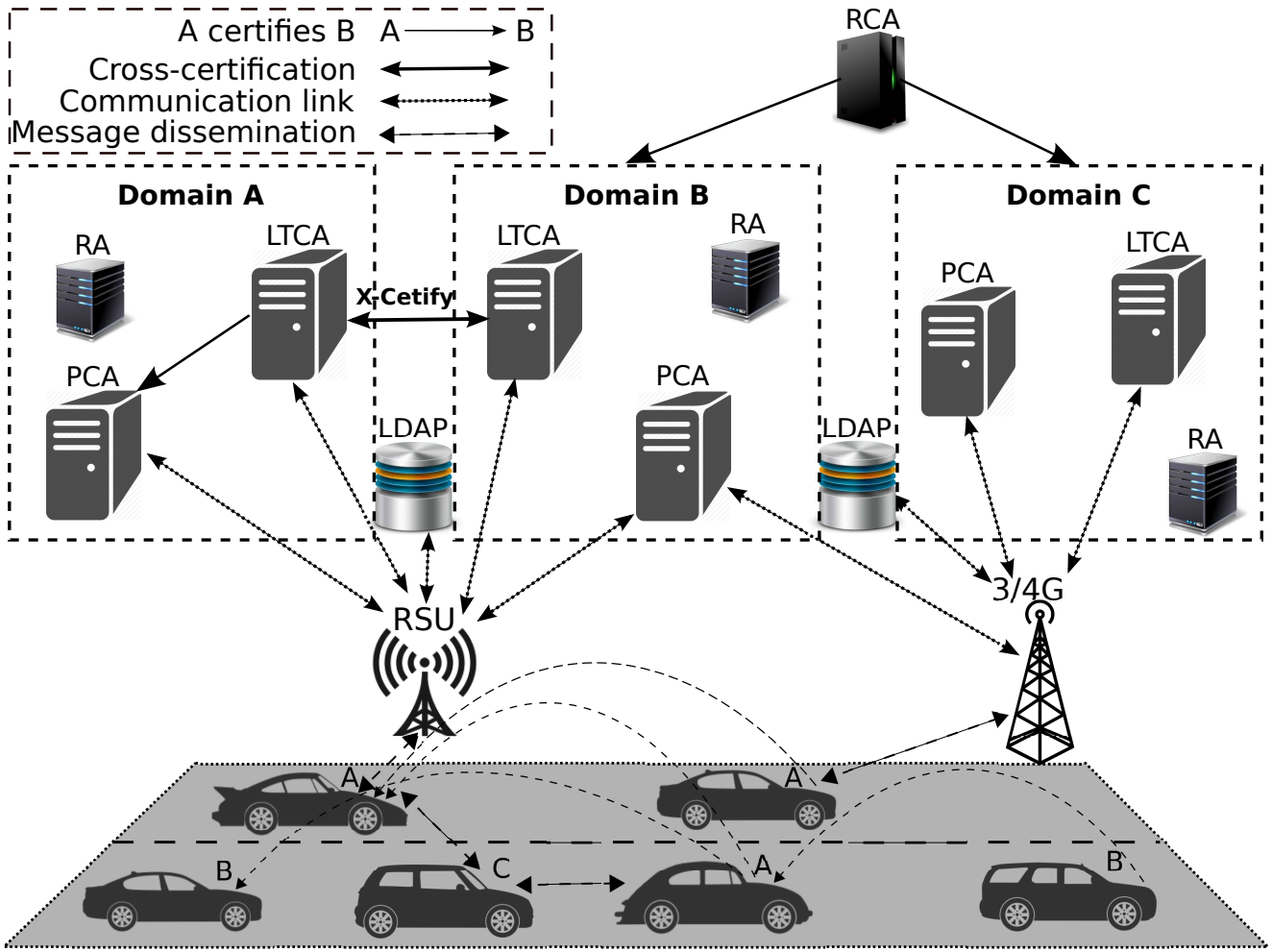
The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems

Mohammad Khodaei and Panos Papadimitratos

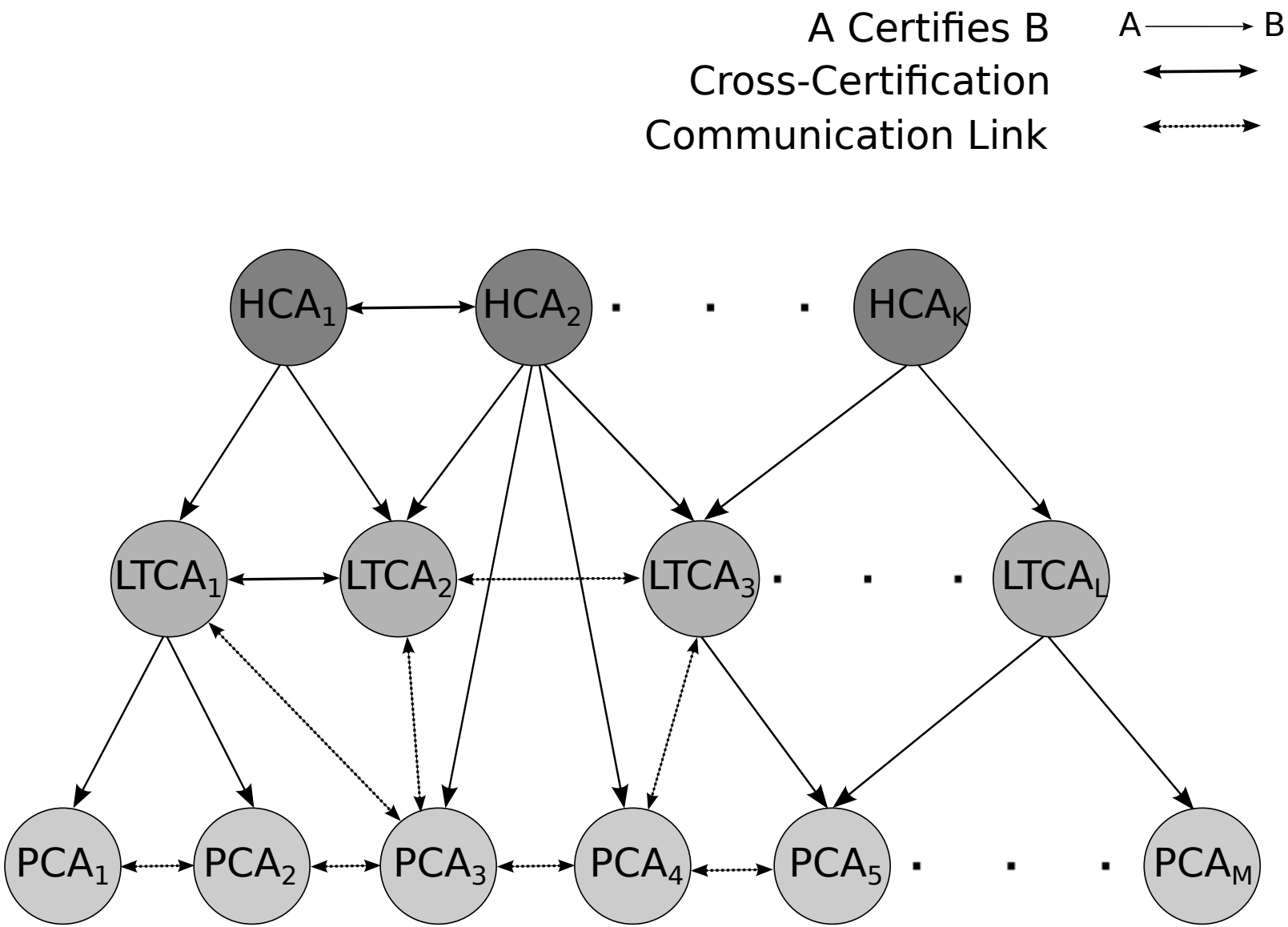
Networked Systems Security Group

Dec, 2015

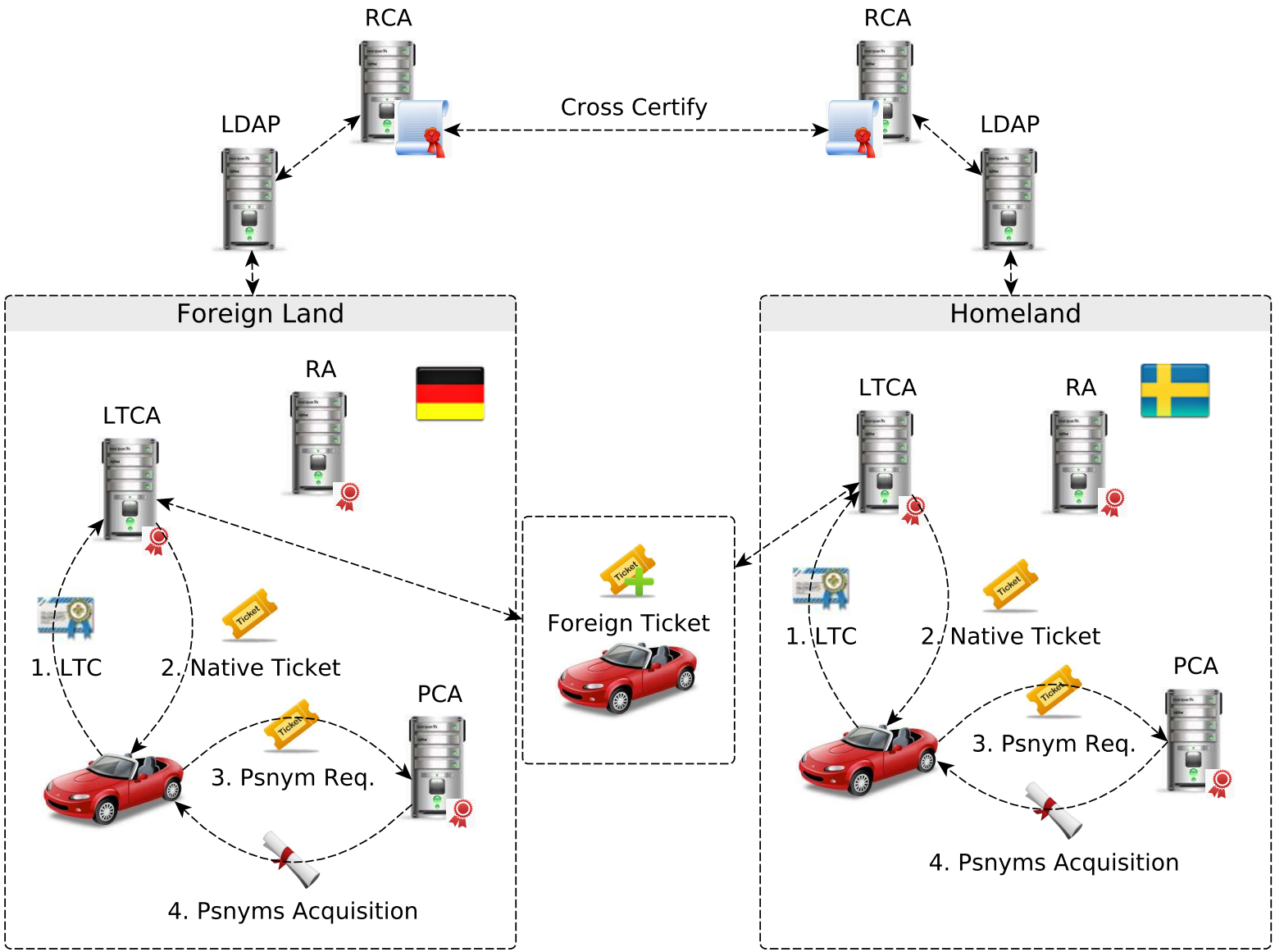
Secure Vehicular Communication (VC) System



Hierarchical Organization of the VC Security Infrastructure



VPKI Architecture



State-of-the-art

Projects

SEVECOM, EVITA, PRECIOSA, OVERSEE, DRIVE-C2X, PRESERVE, CAMP-VSC3

Standarization and Harmonization

IEEE 1609.2, ETSI and C2C-CC: VC related specifications for privacy-preserving architectures

Vehicular Public Key Infrastructure (VPKI)

- *Do we indeed have a corner-stone to build upon secure and privacy-protecting VC systems?*
- More precisely, *do we have all answers needed to deploy an identity and credential management infrastructure for VC?*

Privacy Challenges

Stronger adversarial model[1]

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

LTCA infers relevant information from the requests[2]

- 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 (CAMP)[3] that shuffles the requests
- Honest-but-curious proxy?

[1] Gisdakis et al., 2013 and Khodaei et al., 2014.
[2] Khodaei et al., 2014.
[3] Whyte et al. 2013

Resilience Considerations

Sybil-based misbehavior

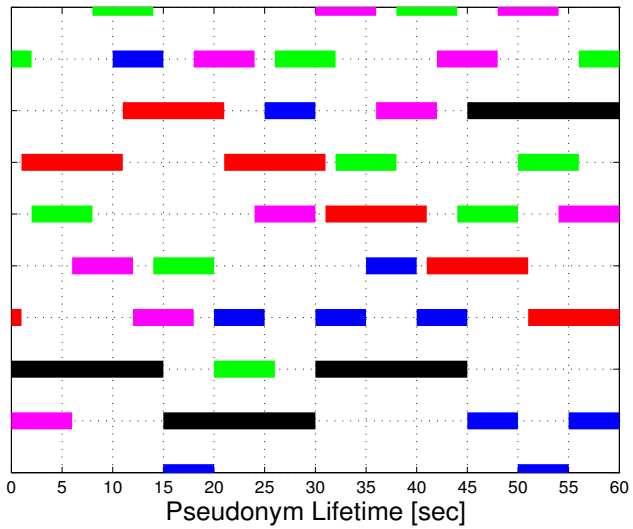
- Acquisition of multiple simultaneously valid credentials
- Allow several pseudonymous valid simultaneously for a specific period of time (C2C-CC or CAMP project)
  - Changing the certificate in a critical traffic situation (e.g., intersection, accident)
  - Safety applications necessitate partial linkability
  - But what if a vehicle gets compromised?
  - Injecting multiple erroneous hazard notification
- VPKI should ensure a compromised vehicle cannot obtain multiple pseudonyms valid simultaneously[4]
  - along with enforcing a policy on the vehicle side
- Standardization bodies and harmonization efforts do not preclude such misbehavior

[4] Khodaei et al., 2014.

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



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 and bandwidth consumption for OBU 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 recommendation 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.

Other Challenges

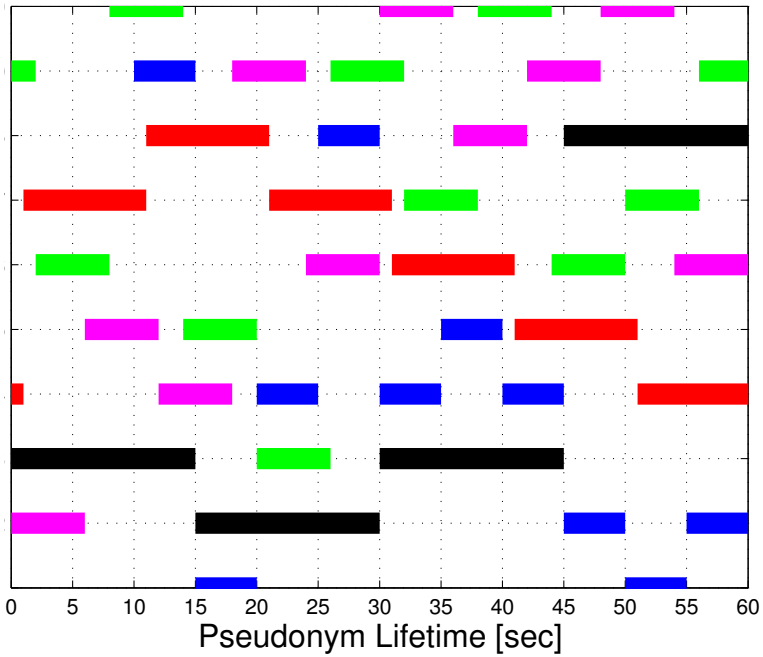
- Extending to anonymous authentication primitives
  - Group signature schemes[5]
  - Zero-knowledge proof[6]
- Extensive experimental validation
  - SEROSA[7]
  - SR-VPKI[8]
- Operational challenges:
  - Who is in charge of the identity and credential management
  - How to establish the trust:
    - [Saab, Scania, Volvo] and [Volkswagen, BMW]
    - [EU] and [US]

[5] Papadimitratos et al., 2007 & Perrig et al., 2009
[6] Förster et al., 2014
[7] Gisdakis et al., 2013
[8] Khodaei et al., 2014

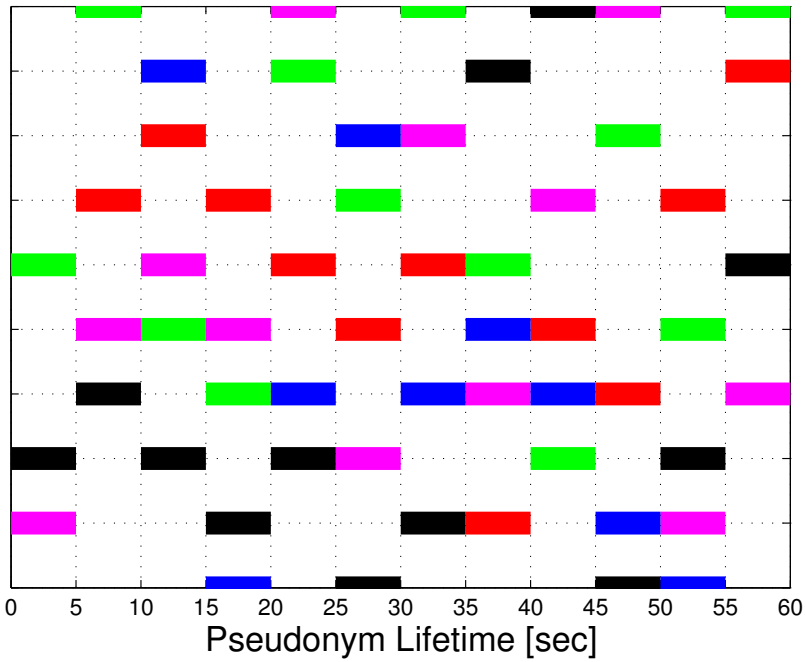
Identity and Credential Management in Vehicular Communication Systems

Questions and Discussion

Pseudonym Lifetime Policy



Flexible lifetimes



Fixed lifetimes

- Non-overlapping pseudonym lifetimes from eavesdroppers' perspective
- Distinct lifetimes per vehicle make linkability easier
- Uniform pseudonym lifetime in a domain
- No distinction among obtained pseudonyms set, thus less probable to link pseudonyms