Security & Privacy for Vehicular Communication Systems:

The Key to Intelligent Transportation

Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group
KTH Royal Institute of Technology, Sweden
www.ee.kth.se/nss

Vehicular Communication (VC) System

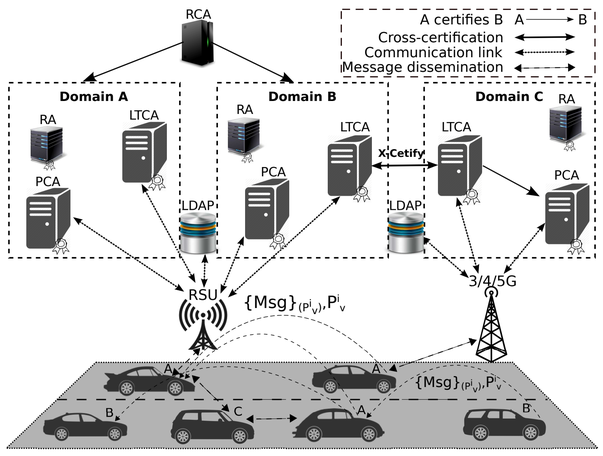

Figure 1: Vehicular Public-Key Infrastructure (VPKI) Architecture [1,3]

Identity and credential management challenges:

- Security and privacy protection, with emphasis on efficiency and scalability
- Multi-domain organization
- Cross-domain operations and service discovery
- Preventing linkability based on timing information
- ***"Honest-but-curious"*** VPKI entities

Security System Entities

- Vehicles registered with one **Long Term Certification Authority (LTCA)** (home domain)
- **Pseudonym Certification Authority (PCA)** servers in one or multiple domains
- Vehicles can obtain pseudonyms from any **PCA** (in home or foreign domains)
- Trust across domains with the help of a **Root CA (RCA)** or cross-certification

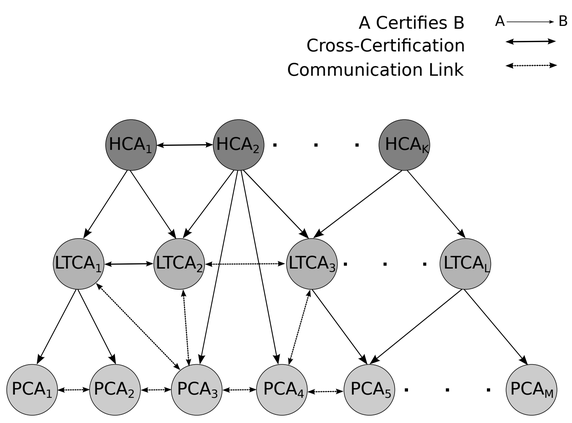

Figure 2: Hierarchical Organization of the VC Security Infrastructure [4]

Security & Privacy Requirements

- Authentication and communication integrity, and confidentiality
- Authorization and access control
- Non-repudiation, accountability and eviction (revocation)
- Anonymity (conditional)
- Unlinkability
- Thwarting Sybil-based attacks
- Availability

SECMACE

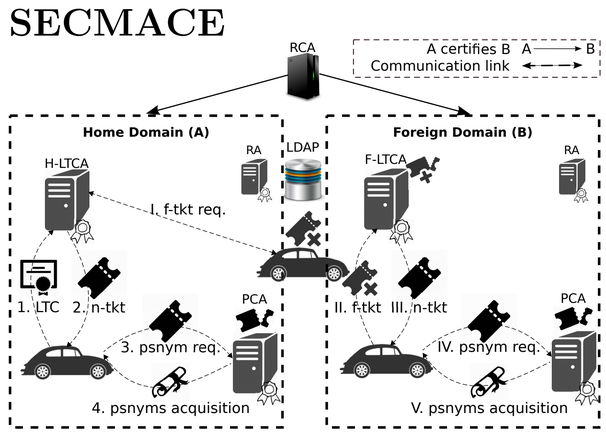

Figure 3: Pseudonym Acquisition Overview in Home and Foreign Domains [1,5]

Pseudonym Acquisition Policy

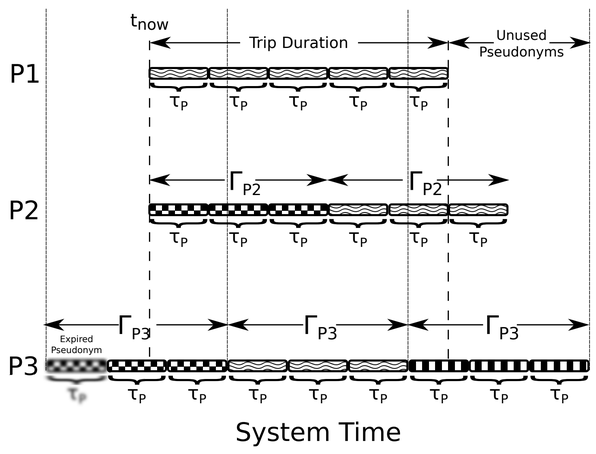

Figure 4: A Schematic Comparison of P1, P2, and P3 [3]

- P1: User-controlled (user-defined) policy
- P2: Oblivious policy
- P3: Universally fixed policy

SECMACE Evaluation

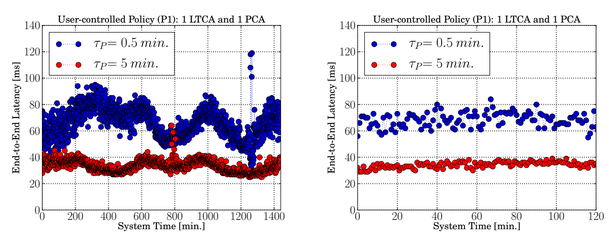

Figure 5: End-to-end Latency for P1 [3]

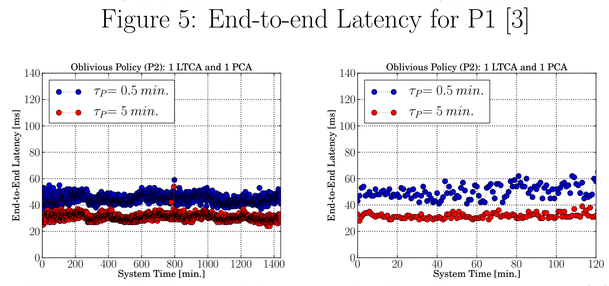

Figure 6: End-to-end Latency for P2, $\Gamma_{P2} = 5$ min. [3]

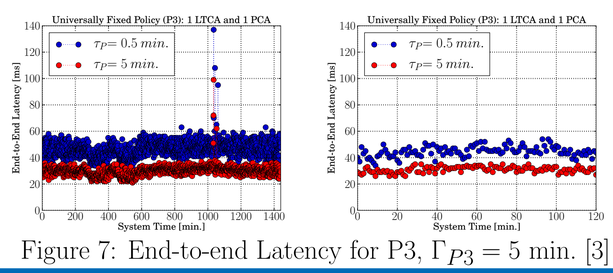

Figure 7: End-to-end Latency for P3, $\Gamma_{P3} = 5$ min. [3]

VPKI Unreachable?

How to ensure vehicle operation without harming user privacy, if the VPKI is unreachable?

- Intermittent coverage (sparsely-deployed Roadside Units (RSUs))
- Highly overloaded cellular infrastructure
- VPKI under an attack, e.g., Distributed Denial of Service (DDoS) [5]

RHyTHM

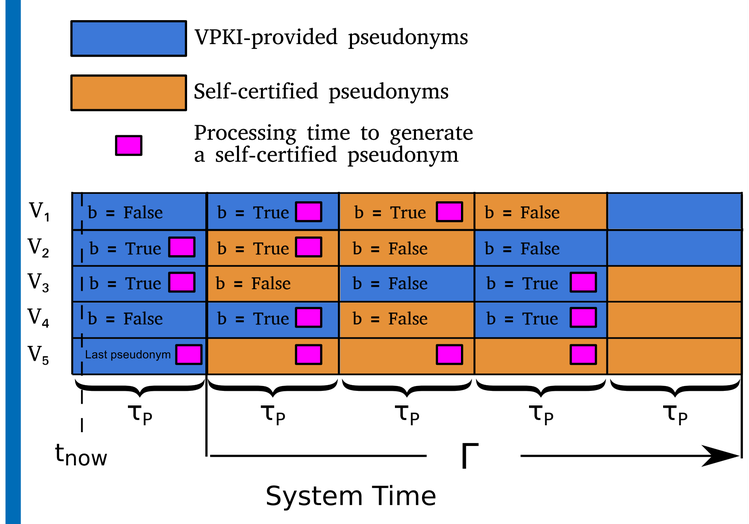

Figure 8: RHyTHM overview: if $b = True$, the vehicle will utilize its self-certified pseudonym; otherwise, it relies on its VPKI-provided pseudonym [2].

RHyTHM Privacy Analysis

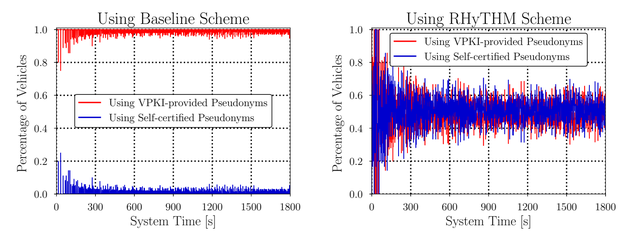

Figure 9: 1% of nodes run out of pseudonyms (pseudonym lifetime: $\tau_P = 60$ sec; probability of switching to self-certified pseudonyms: $r = 0.5$).

RHyTHM Evaluation

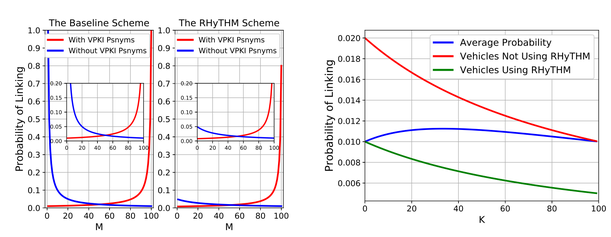

Figure 10: (a) Comparing the probability of linking two pseudonyms using baseline and RHyTHM schemes ($N = 100, r = 0.2$). (b) Probability of linking two VPKI-provided pseudonyms ($N = 100, r = 0.5$).

References

[1] M. Khodaei, H. Jin, and P. Papadimitratos, **"SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,"** IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 5, 1430–1444, May 2018.

[2] M. Khodaei, A. Messing, and P. Papadimitratos. 2017. **"RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd,"** In IEEE Vehicular Networking Conference (VNC), Torino, Italy, Nov. 2017.

[3] M. Khodaei and P. Papadimitratos, **"Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems,"** in Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet, Paderborn, Germany, pp. 7–12, July 2016.

[4] M. Khodaei and P. Papadimitratos, **"The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,"** IEEE VT Magazine, vol. 10, no. 4, pp. 63–69, Dec. 2015.

[5] M. Khodaei, H. Jin, and P. Papadimitratos. **"Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure,"** IEEE VNC, Paderborn, Germany, Dec. 2014.

[6] L. Codeca and et al. 2015. **"Luxembourg SUMO Traffic (LuST) Scenario: 24 Hours of Mobility for Vehicular Networking Research,"** IEEE VNC. Kyoto, Japan.

[7] **"Preparing Secure Vehicle-to-X Communication Systems - PRESERVE."** [Online]. Available: http://www.preserve-project.eu/.