A Cooperative Location Privacy Protection Scheme for Vehicular Ad-hoc Networks

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

Vehicular Communication (VC) Systems

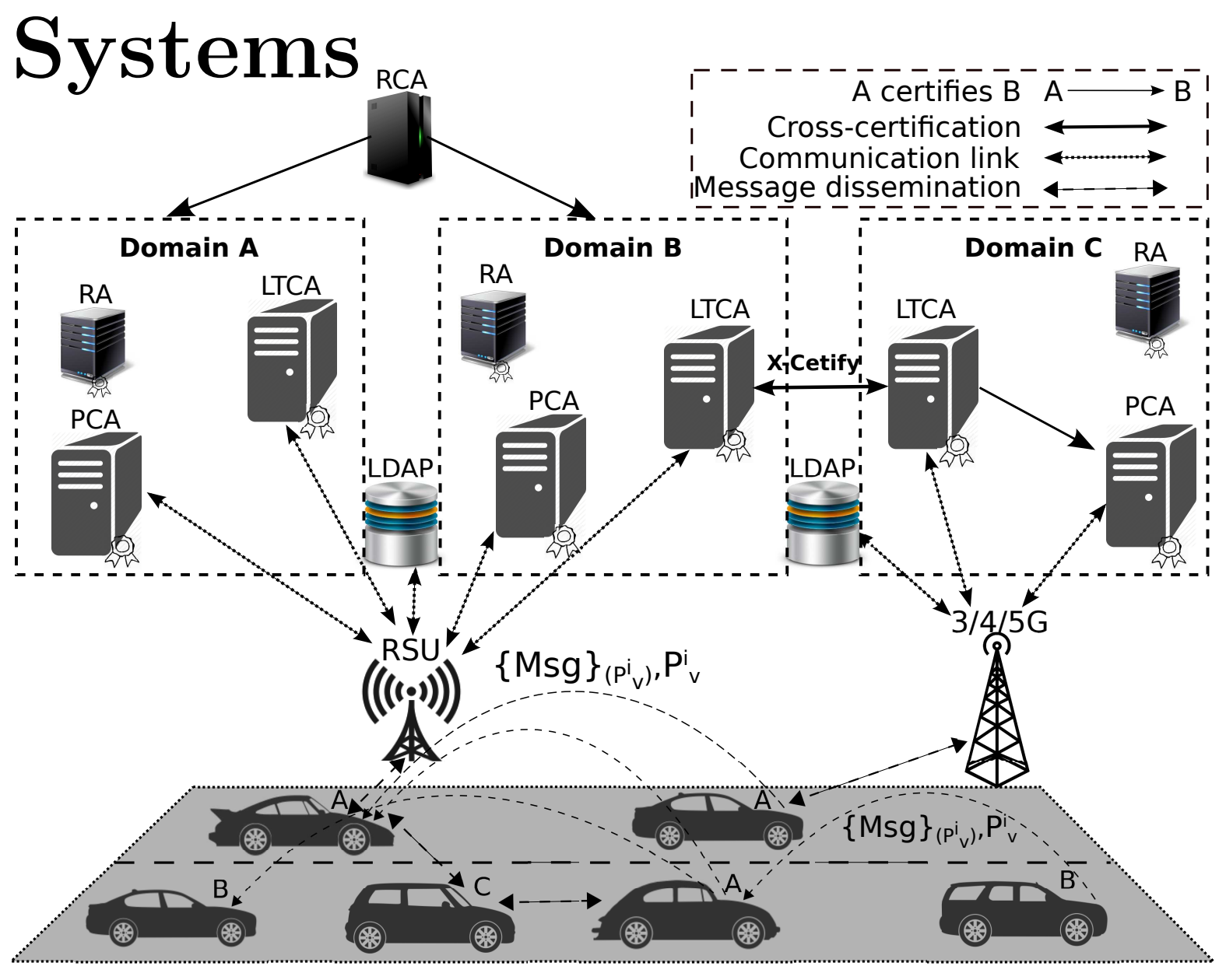

Figure 1: Vehicular Public-Key Infrastructure (VPKI) Architecture [7, 9].

Security System Entities

- Vehicles registered with one (home) **Long Term Certification Authority (LTCA)**
- **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

Security & Privacy Requirements

- Authentication and communication integrity
- Authorization and access control
- Non-repudiation, accountability and eviction
- **Conditional anonymity & unlinkability**

Adversarial Model

- *Honest-but-curious* VPKI entities
- Adversaries could eavesdrop VC systems to infer user-sensitive information, derived from Cooperative Awareness Messages (CAMs), e.g., timing, velocity, heading, and location, to harm user privacy

Pseudonym Acquisition Policy

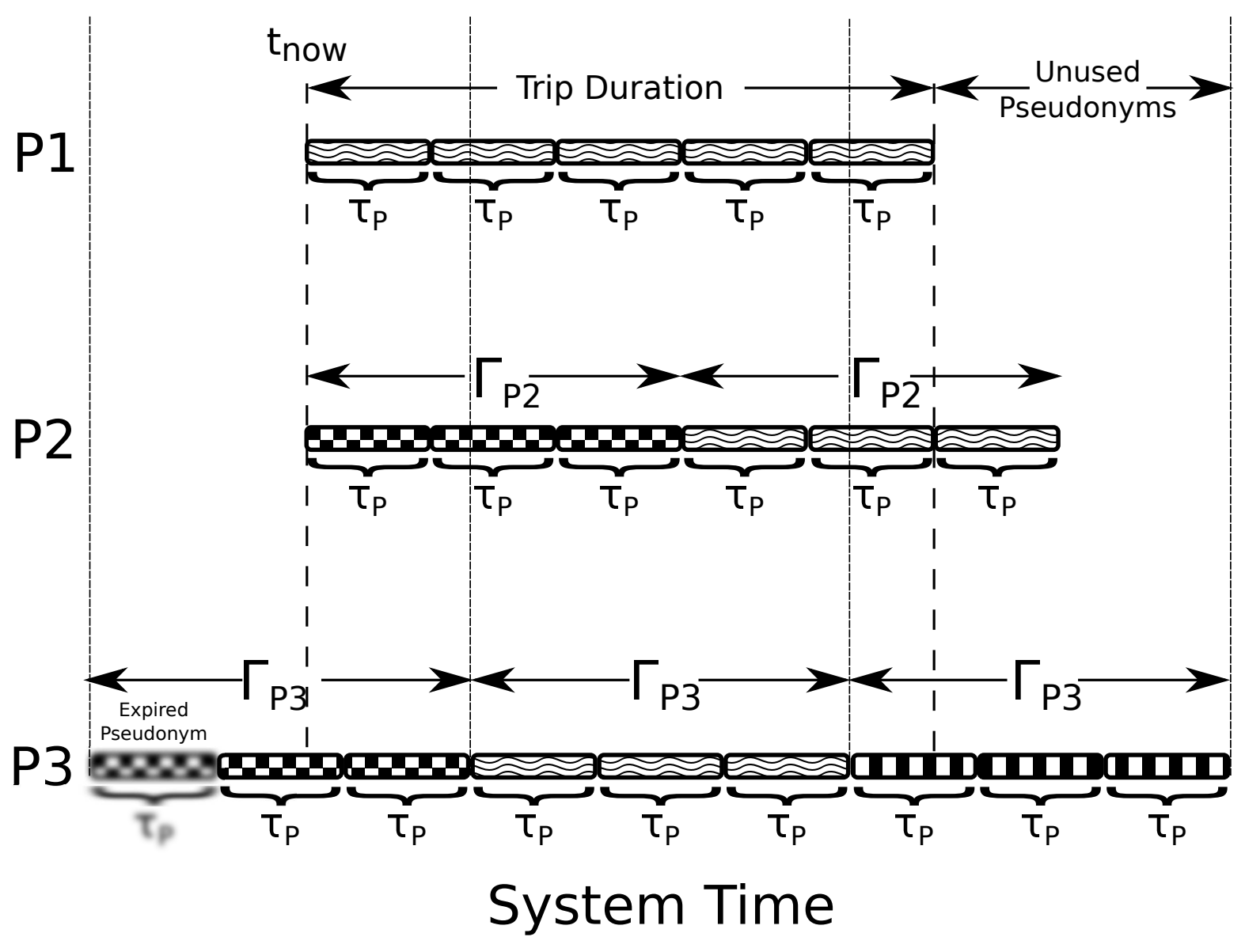

Figure 2: A Schematic Comparison of P1, P2, and P3 [9].

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

Inferring User-sensitive Information

- **Syntactically and semantically (i.e., time and velocity) linking messages**
- **Linking based on times of pseudonym changes (cannot be obfuscated)**

SECMACE Overview

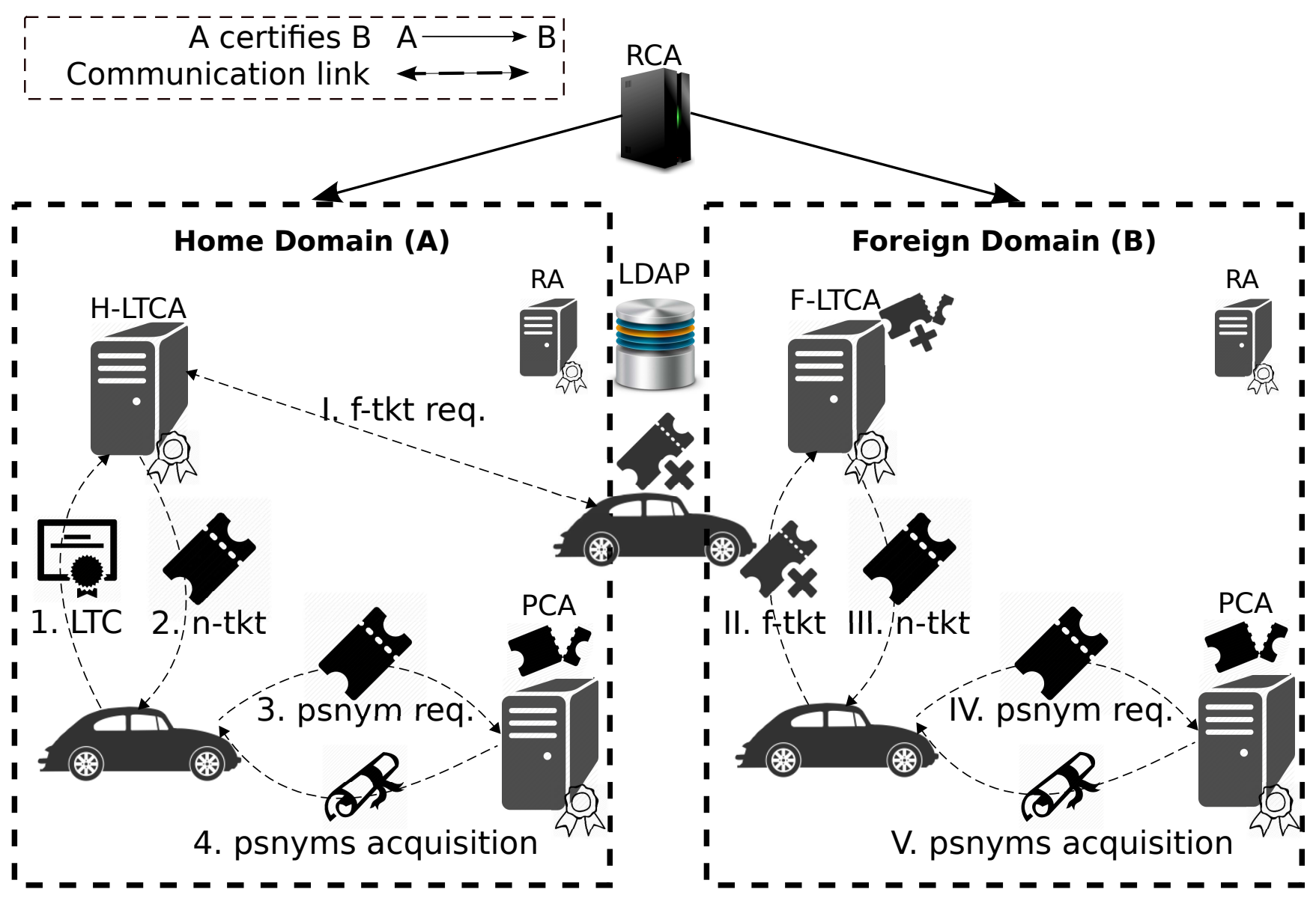

Figure 3: Pseudonym Acquisition Overview in Home and Foreign Domains [7, 12].

Mitigating Timing-based Inferences

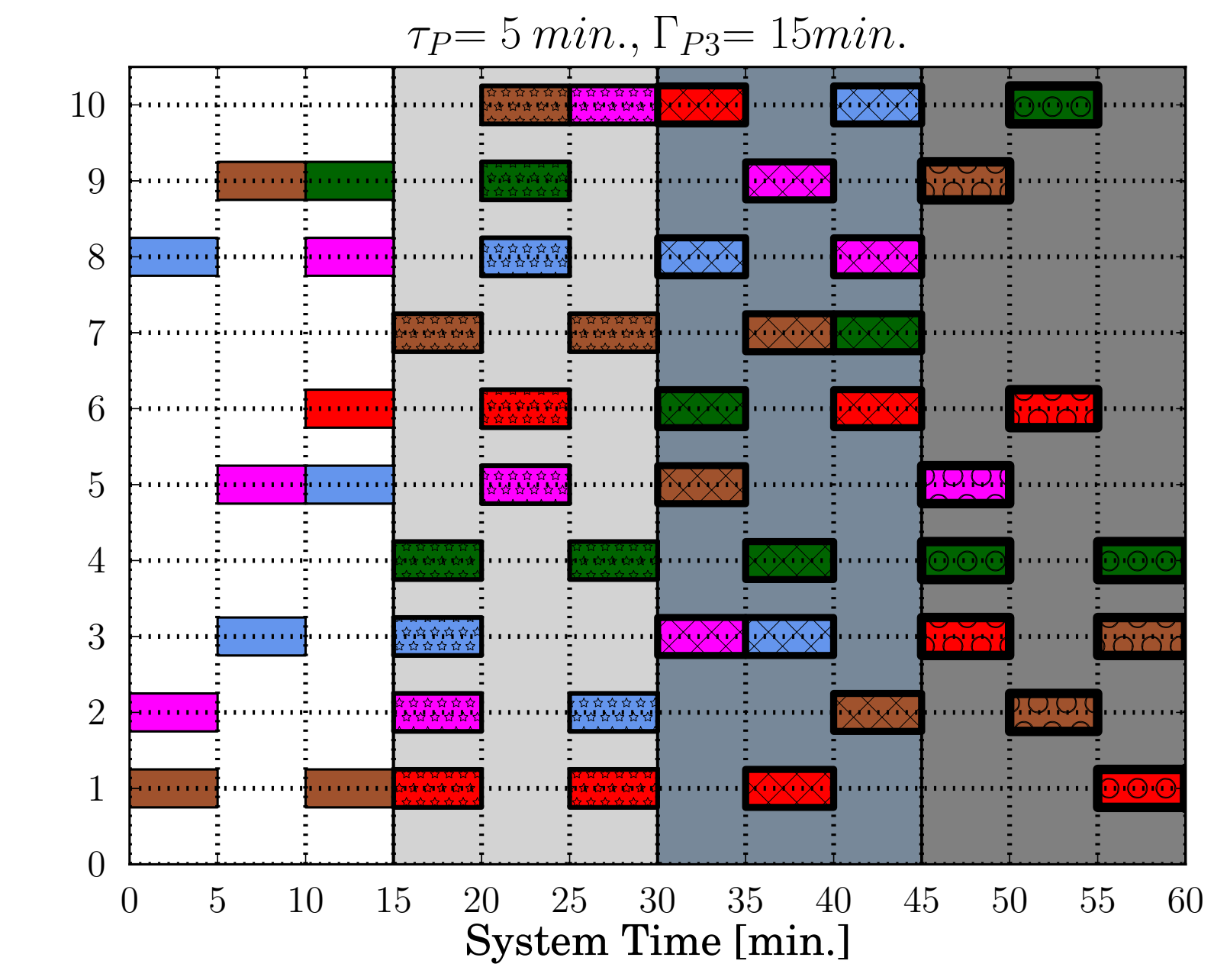

Figure 4: Universally Fixed Policy [7, 9, 12]

- Achieving highest level of privacy: anonymity set equals to the number of active vehicles
- Preventing a single *honest-but-curious* VPKI entity from linking pseudonyms

Solution 1: Mix-zones Everywhere

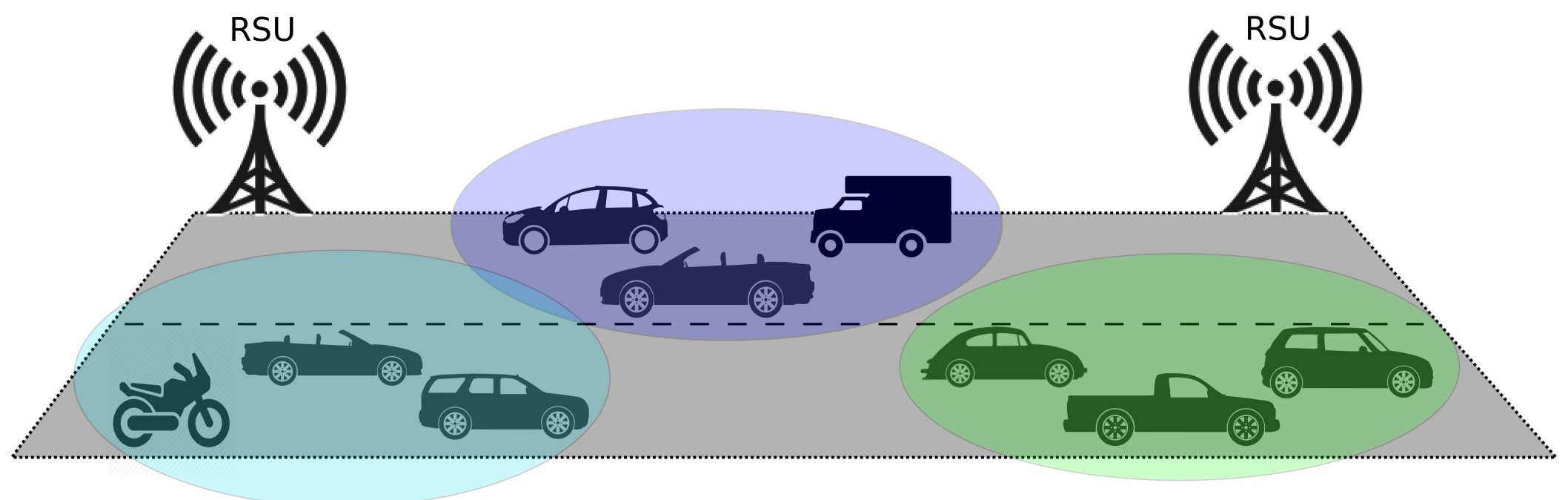

Figure 5: Dynamic construction of Mix-zones.

- Upon reaching a pseudonym transition process, a dynamic mix-zone formation is initiated
- All CAMs within each mix-zone are encrypted using a distinct symmetric session key
- Dynamic formation of mix-zones combined with the fully-unlinkable pseudonyms issuance process hinder harming user privacy by colluding entities, e.g., a VPKI entity

Mix-Zone Initiation Protocol

Protocol 1: Mix-Zone Initiation Protocol

```
procedure INITIATE-MIXZONE()
    $Flag_{INIT\text{-}MIX} \leftarrow True$                          ▷ Initializing Mix-zone flag to true
    $CAM \leftarrow \{Fields, Flag_{INIT\text{-}MIX}, t_{now}\}$       ▷ Encapsulating a CAM
    $(CAM)_{\sigma_{k_v}} \leftarrow$ Sign$(CAM, K_v)$                 ▷ Signing the CAM
    $broadcast((CAM)_{\sigma_{k_v}})$                                  ▷ Broadcasting a CAM with Mix-zone initiation
    Generate$(SK)$                                                     ▷ Generating a symmetric key SK
    for i:=1 to n do                                                   ▷ n: number of neighboring vehicles
        Begin
            $SK_{\sigma_{K_v^i}} \leftarrow$ Encrypt$(K_v^i, SK)$       ▷ Encrypting SK with a neighbor's public key
            $\zeta \leftarrow (INIT\text{-}MIX, SK_{\sigma_{K_v^i}}, K_v, K_v^i, t_{now})$   ▷ Encapsulating the msg
            $\zeta_{\sigma_{k_v}} \leftarrow Sign(k_v, \zeta)$          ▷ Signing the message with it's private key
            $broadcast(\zeta_{\sigma_{k_v}})$                           ▷ Broadcasting Mix-zone SK
        End
end procedure
```

Solution 2: A Vehicle-centric & Cooperative Mix-zone Scheme

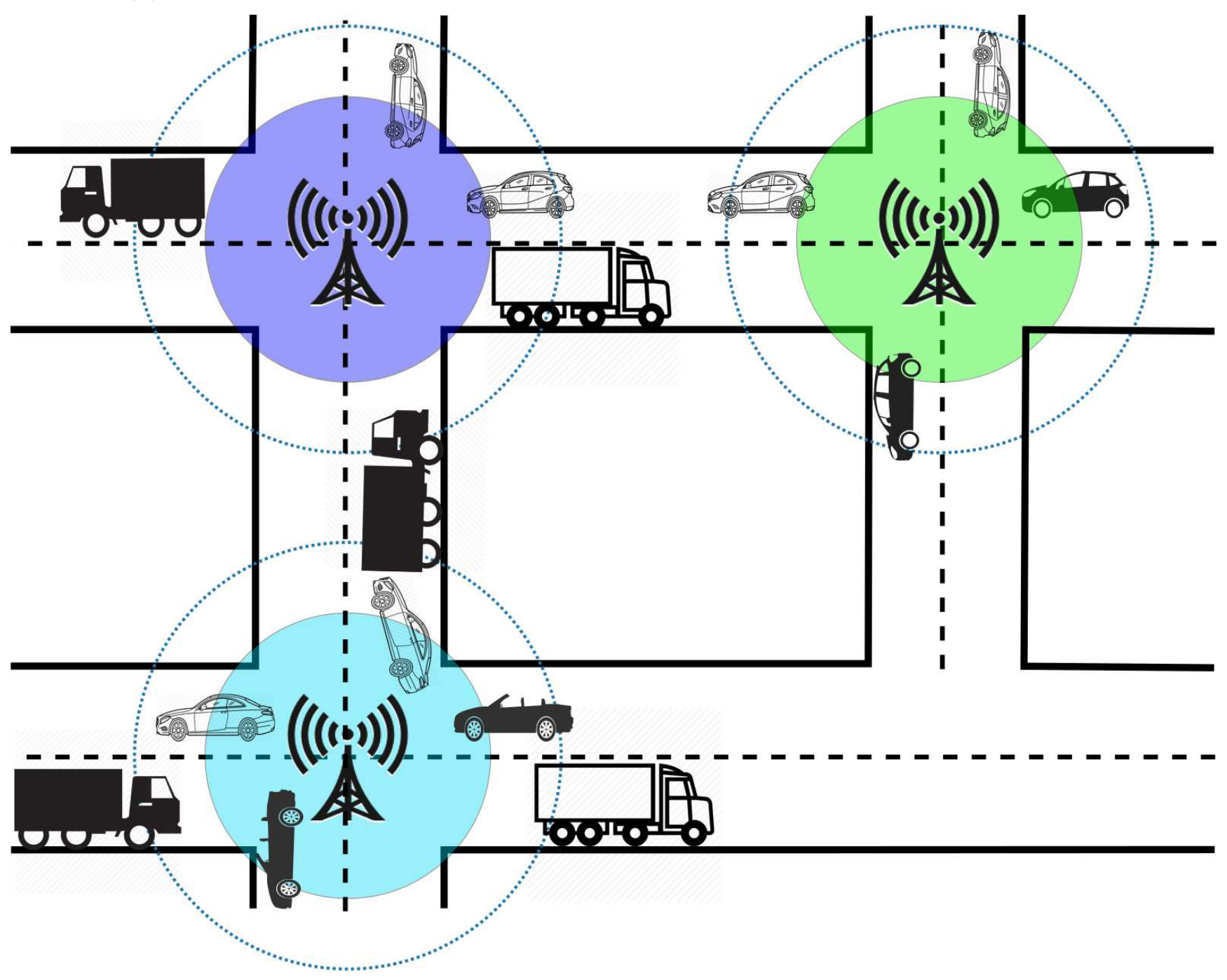

Figure 6: Mix-zones construction with *decoy traffic.*

- Mitigating syntactic & semantic linking attacks
- Requires having vehicles provided with pseudonyms with overlapping lifetimes
- Preventing malicious internal vehicles from degrading the anonymity set
- Strongly protecting user privacy in the presence of *honest-but-curious* VPKI entities

Remaining Challenges

- Efficient, scalable, and resilient group authentication scheme to initiate dynamic formation of mix-zones
- Evaluating the performance of the two solutions in simulation and gauging the achieved privacy protection

References

[1] M. Khodaei, H. Noroozi, and P. Papadimitratos, **"Scaling Pseudonymous Authentication for Large Mobile Systems,"** in ACM WiSec, Miami, FL, USA, May 2019.

[2] M. Khodaei and P. Papadimitratos, **"Poster: Mix-Zones Everywhere: A Dynamic Cooperative Location Privacy Protection Scheme,"** in IEEE Vehicular Networking Conference (VNC), Taipei, Taiwan, Dec. 2018.

[3] C. Vaas, M. Khodaei, P. Papadimitratos, and M. Ivan, **"Nowhere to hide? Mix-Zones for Private Pseudonym Change using Chaff Vehicles,"** in IEEE Vehicular Networking Conference (VNC), Taipei, Taiwan, Dec. 2018.

[4] M. Khodaei and P. Papadimitratos, **"Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs,"** in ACM WiSec, Stockholm, Sweden, June 2018, pp. 172–183.

[5] H. Noroozi, M. Khodaei, and P. Papadimitratos, **"DEMO: VPKIaaS: A Highly-Available and Dynamically-Scalable Vehicular Public-Key Infrastructure,"** in ACM WiSec, Stockholm, Sweden, June 2018, pp. 302–304.

[6] M. Khodaei, H. Noroozi, and P. Papadimitratos, **"POSTER: Privacy Preservation through Uniformity,"** in ACM WiSec, Stockholm, Sweden, June 2018, pp. 279–280.

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

[8] 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.

[9] 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.

[10] H. Jin, M. Khodaei, and P. Papadimitratos, **"Security and Privacy in Vehicular Social Networks,"** in Vehicular Social Networks. Taylor & Francis Group, 2016.

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

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