Nowhere to hide? Mix-Zones for Private Pseudonym Change using Chaff Vehicles

Christian Vaas[1], Mohammad Khodaei[2], Panos Papadimitratos[2], Ivan Martinovic[1]

University of Oxford[1], KTH, Stockholm[2]

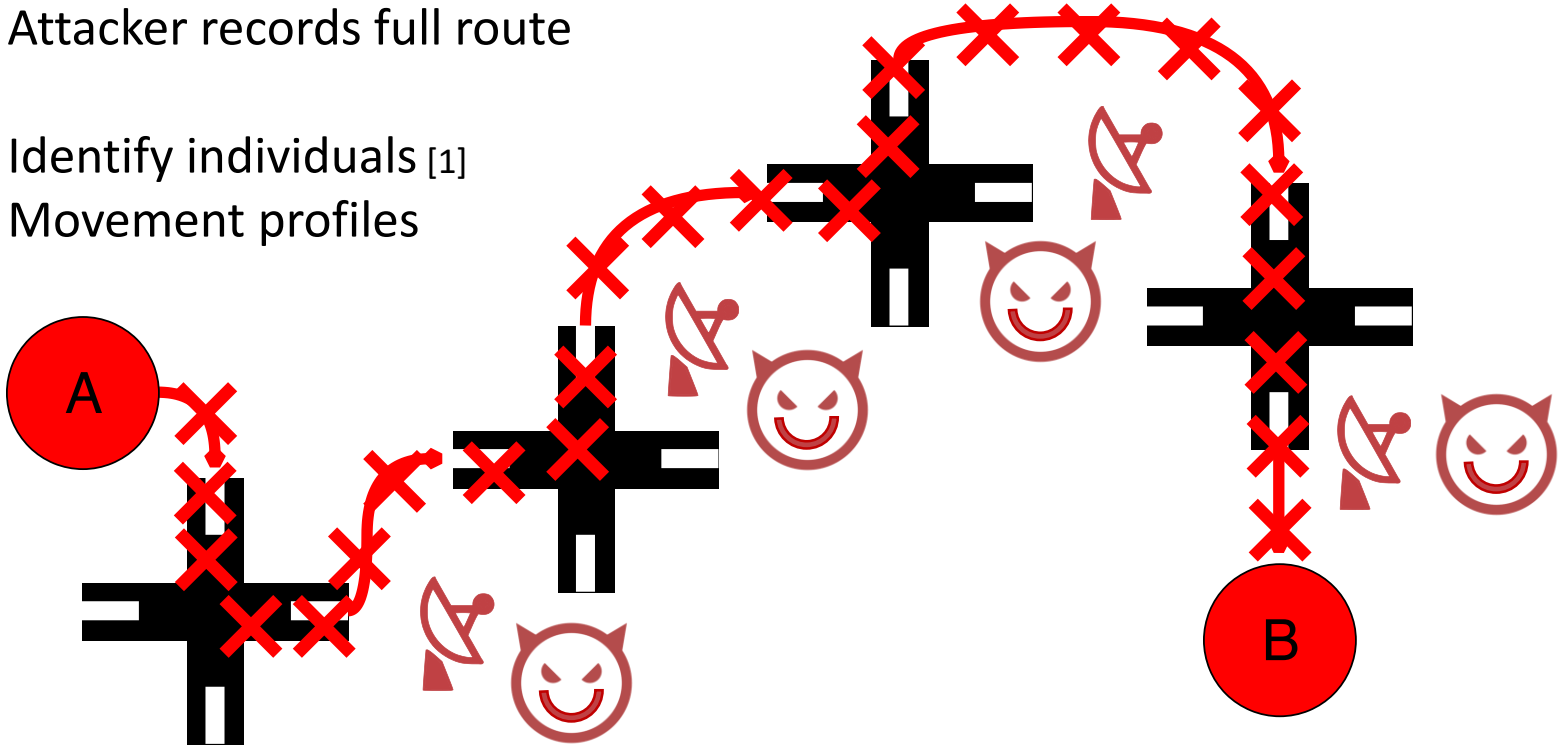
VNC, 6 December 2018

UNIVERSITY OF OXFORD

Motivation: Vehicle Tracking

- Static credentials to sign CAM messages
- Wireless eavesdropper
- Attacker records full route

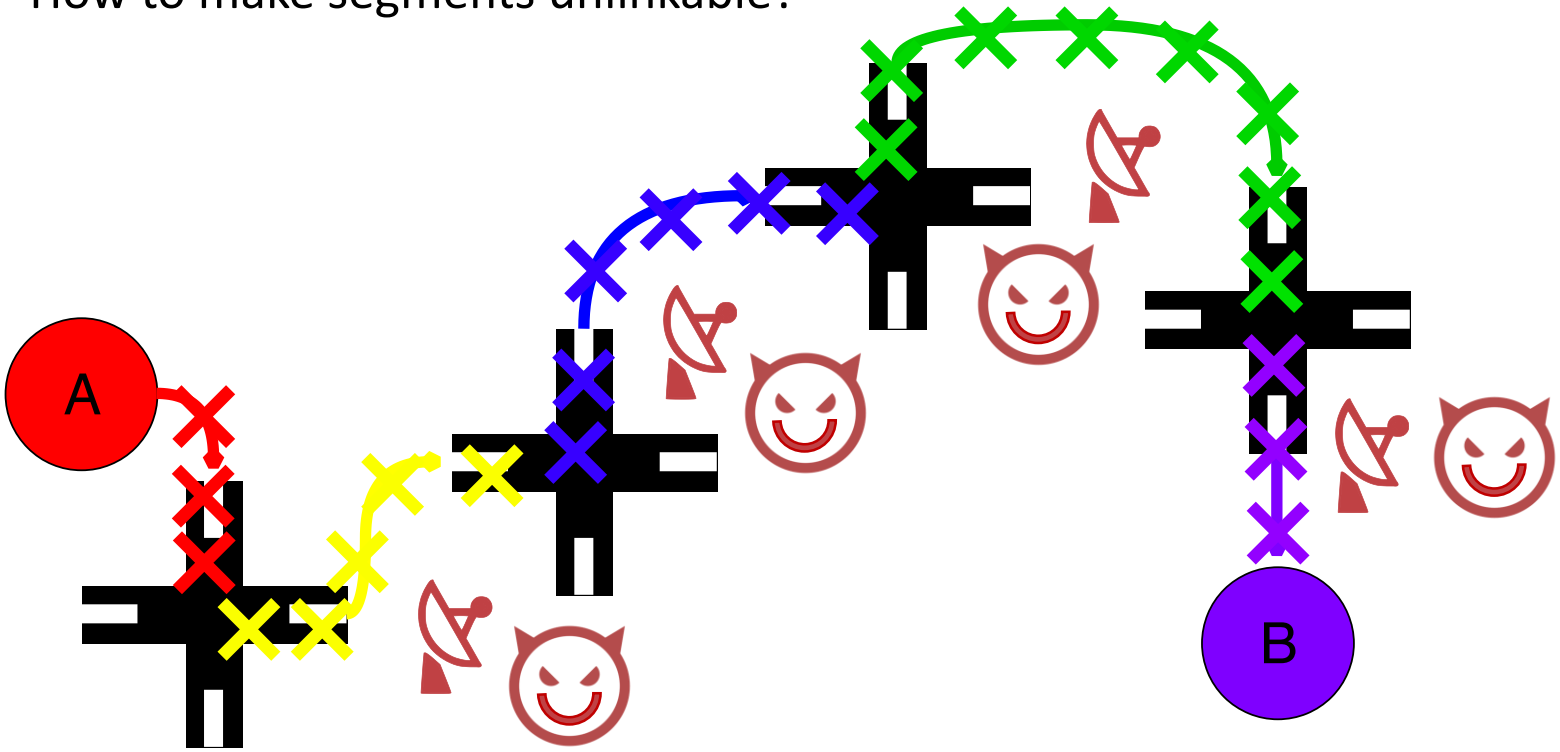
➢ Identify individuals [1]
➢ Movement profiles



Pseudonym Change

- Frequently changing credentials
- Attacker records route segments

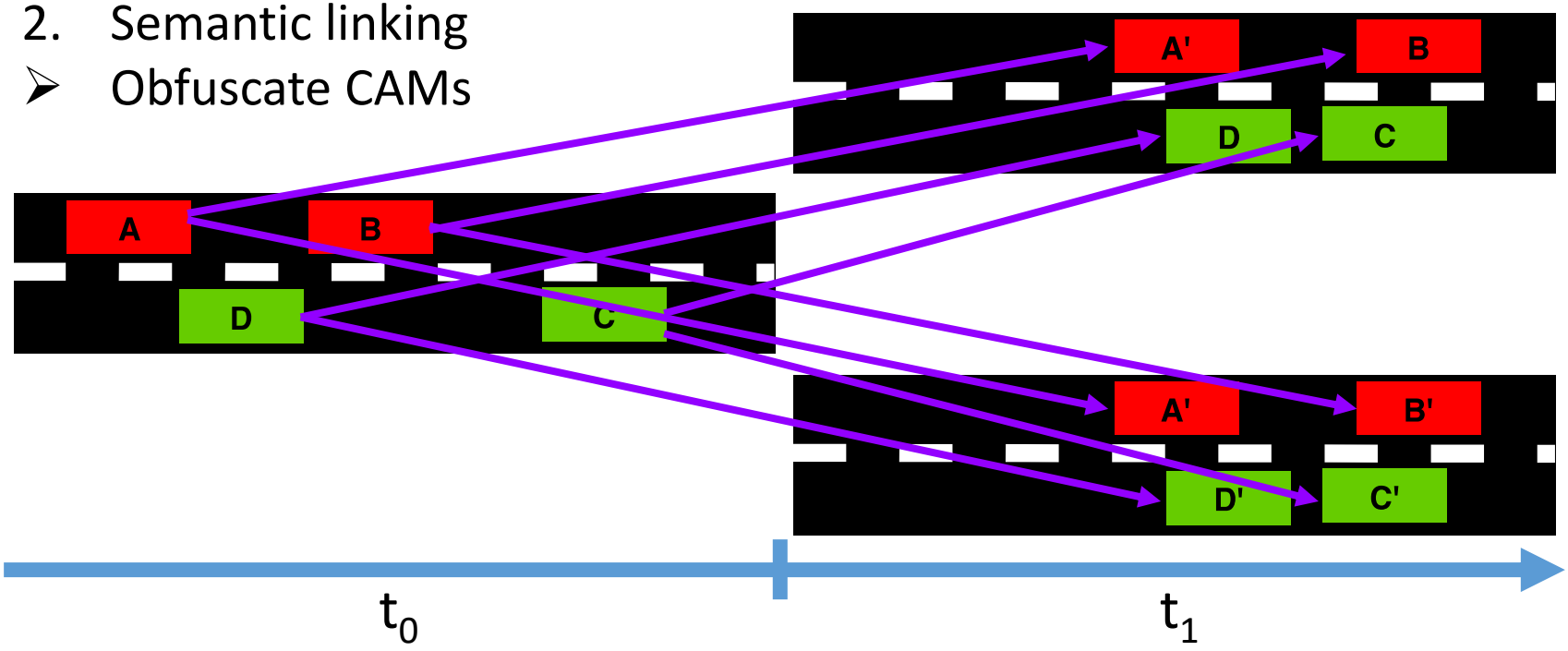
➢ How to make segments unlinkable?



Segment Unlinkability

1. Syntactic linking
   - ➢ Synchronization

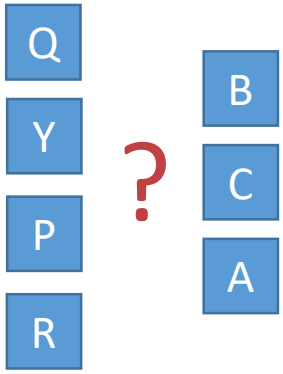
2. Semantic linking
   - ➢ Obfuscate CAMs

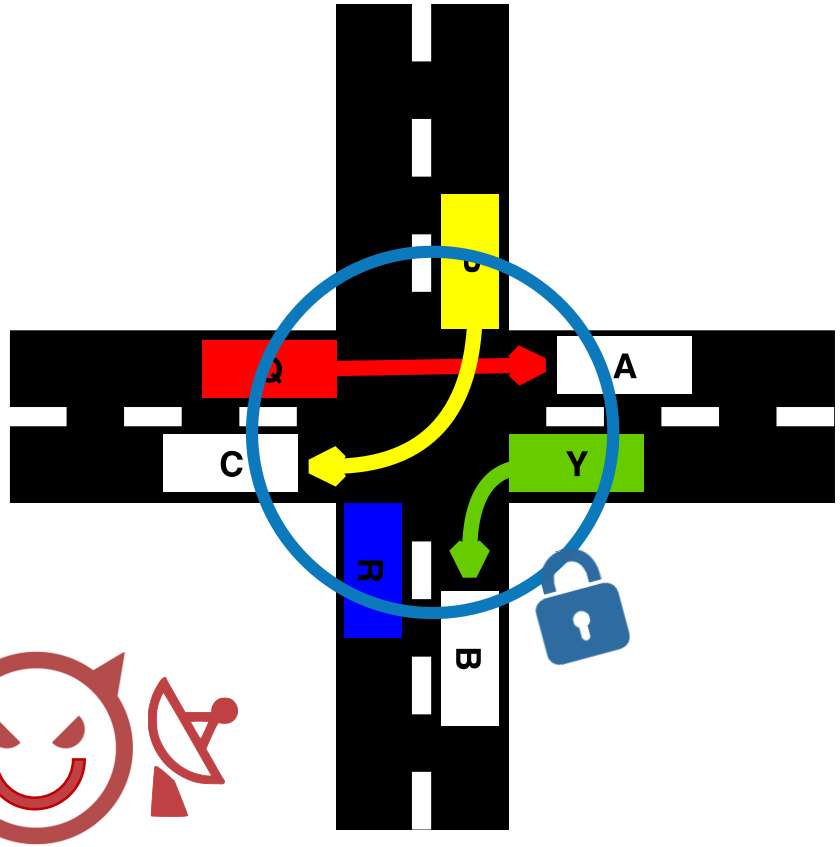


Mix-zones: Principle

- Covers intersections
- Prevent pseudonym linking
- Obfuscate CAMs
- Silent or encrypted periods
- Private change of ECDSA credentials

➢ Recording entry-exit pairs

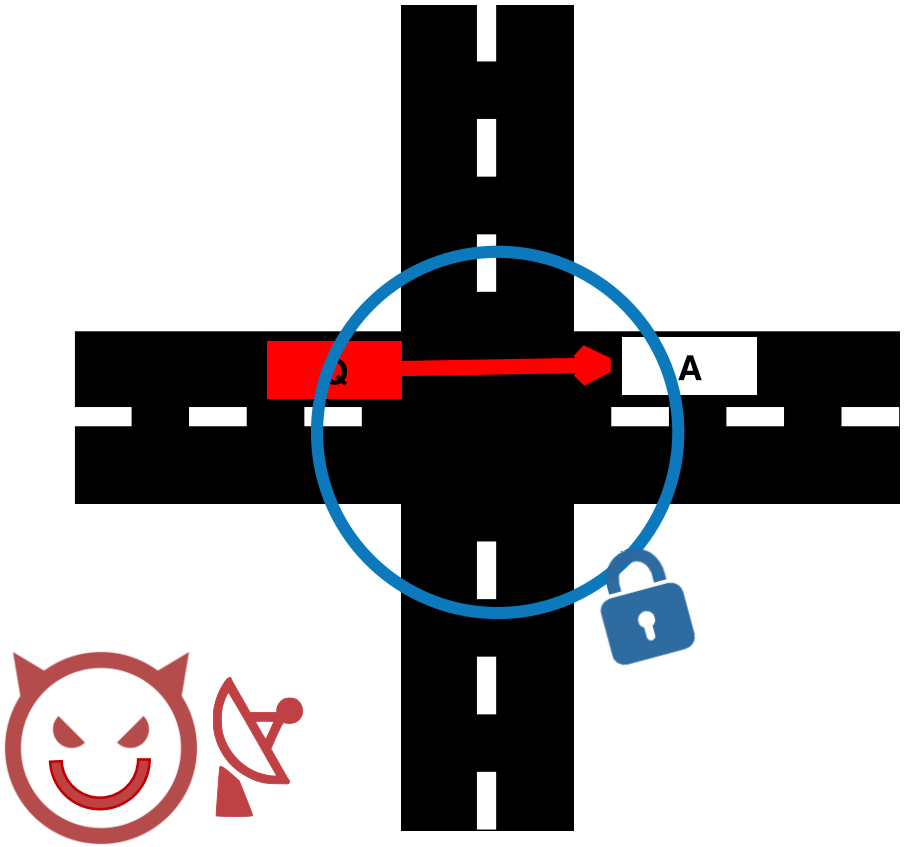




Crypto Mix-zones: Problem

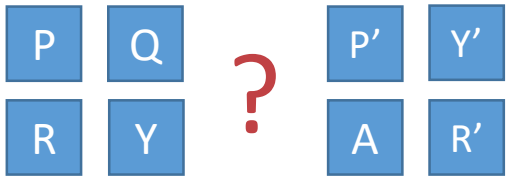
- Dependence on vehicle availability
  - Low traffic regions
  - Low traffic hours
  - Driver population
  - Arrival timings

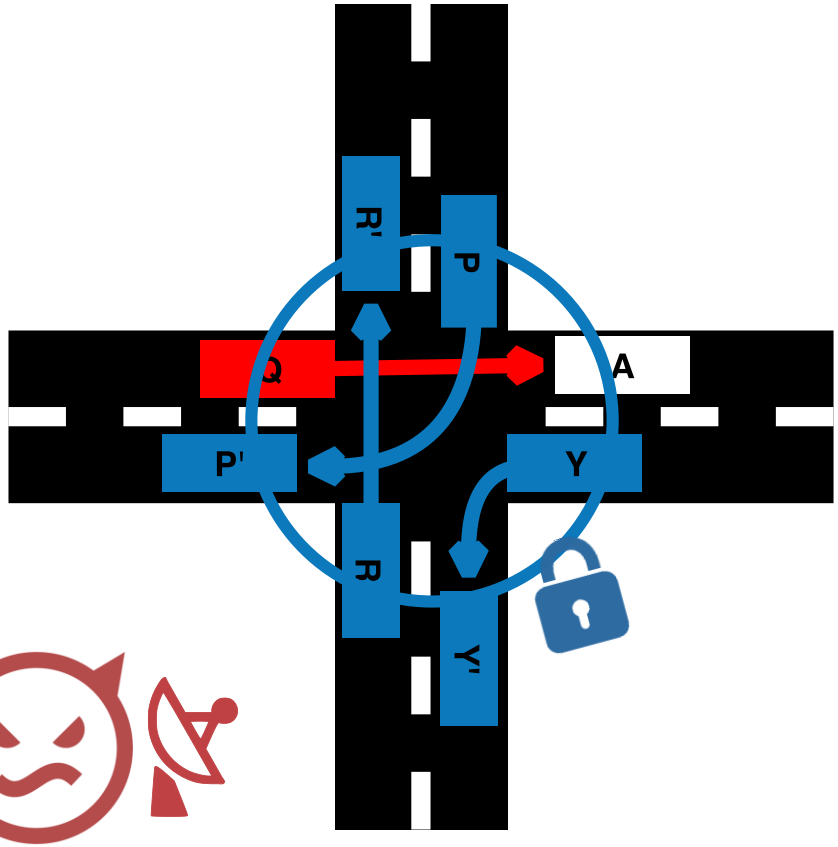
➢ Correlation attack



Our Solution

- Chaff vehicles
- Substitute for real vehicles
- RSUs generate chaff CAMs
- CAMs signed with chaff pseudonyms
- CAMs broadcast by RSUs and OBUs
- Must not impair safety





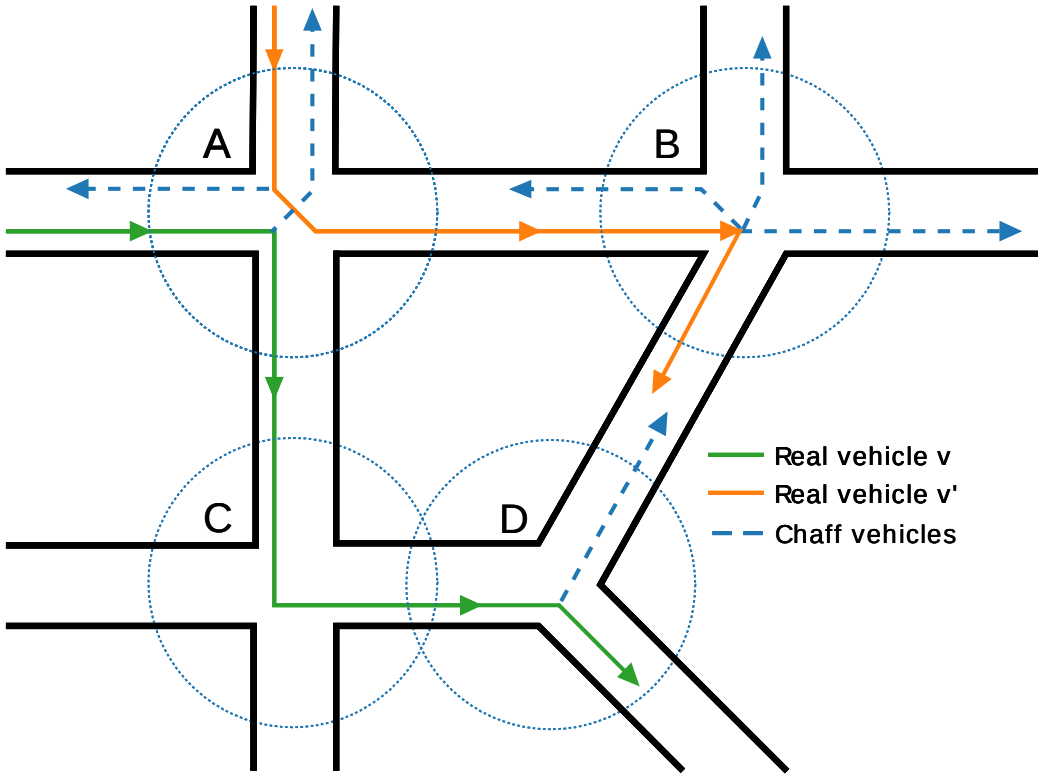
Chaff-based CMIX Scheme

Protocols & Services

1. Key provisioning
2. Chaff-trace generation
3. Chaff notification
   - D to B
4. Filter update

➢ Safety preserving

➢ Maximize mixing



Simulation Environment

LuST

Luxembourg SUMO Traffic Scenario

PREXT

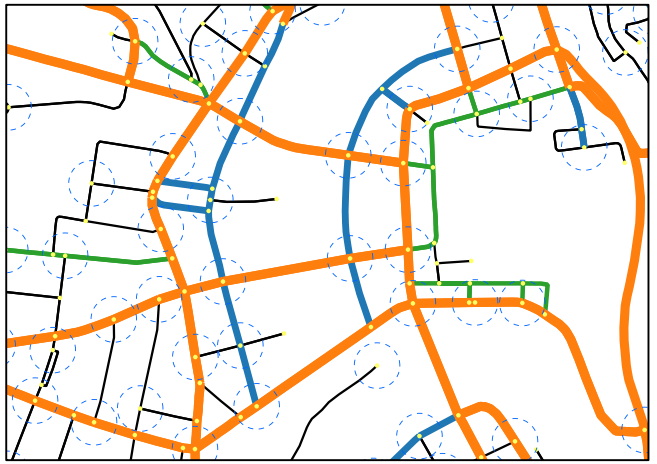
Privacy Extension for Veins VANET Simulator

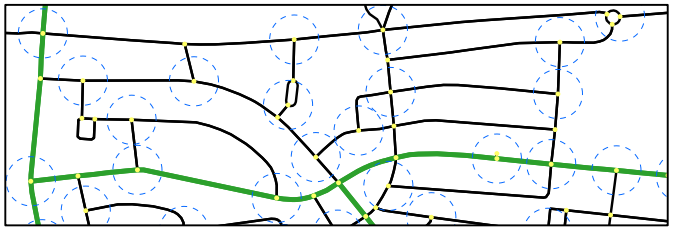
CMIX

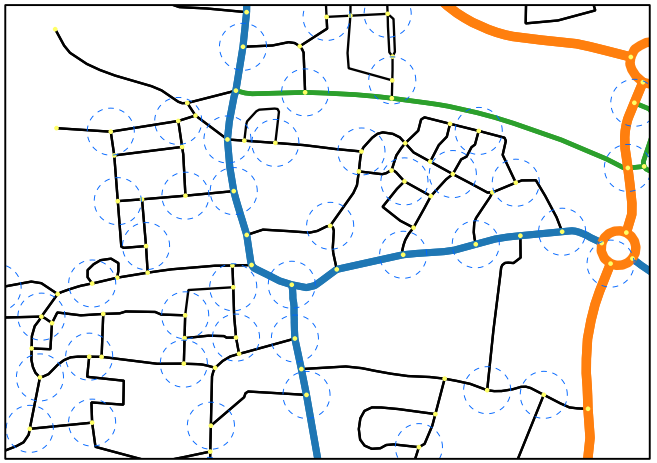
Mix-Zones for Location Privacy in Vehicular Networks

Simulation Scenarios

- Three different areas
  - Suburban – low traffic
  - Residential – medium traffic
  - Central – high traffic
- Encryption radius fixed

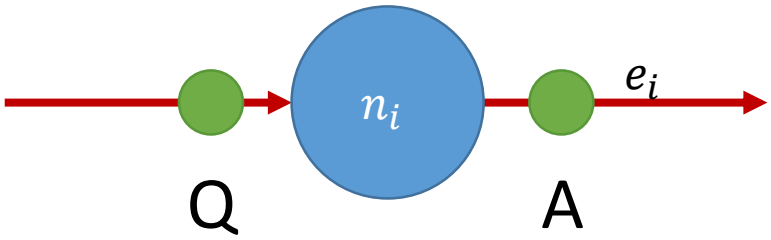






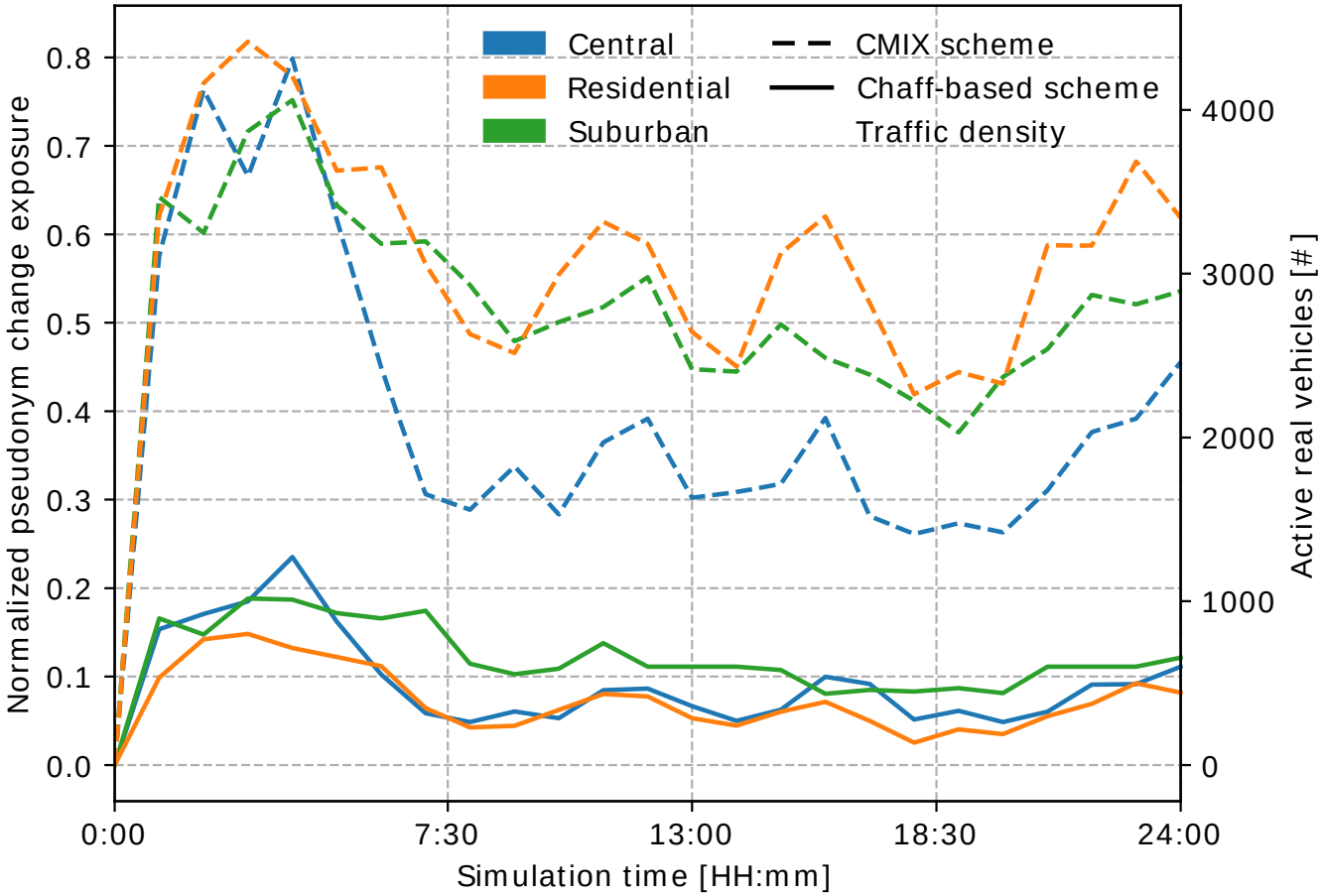
- Tracking probability based metric

$$P(T_v) = \frac{\sum_{i=0}^{m} p_v\,(n_i) * l(e_i)}{|T_v|}$$



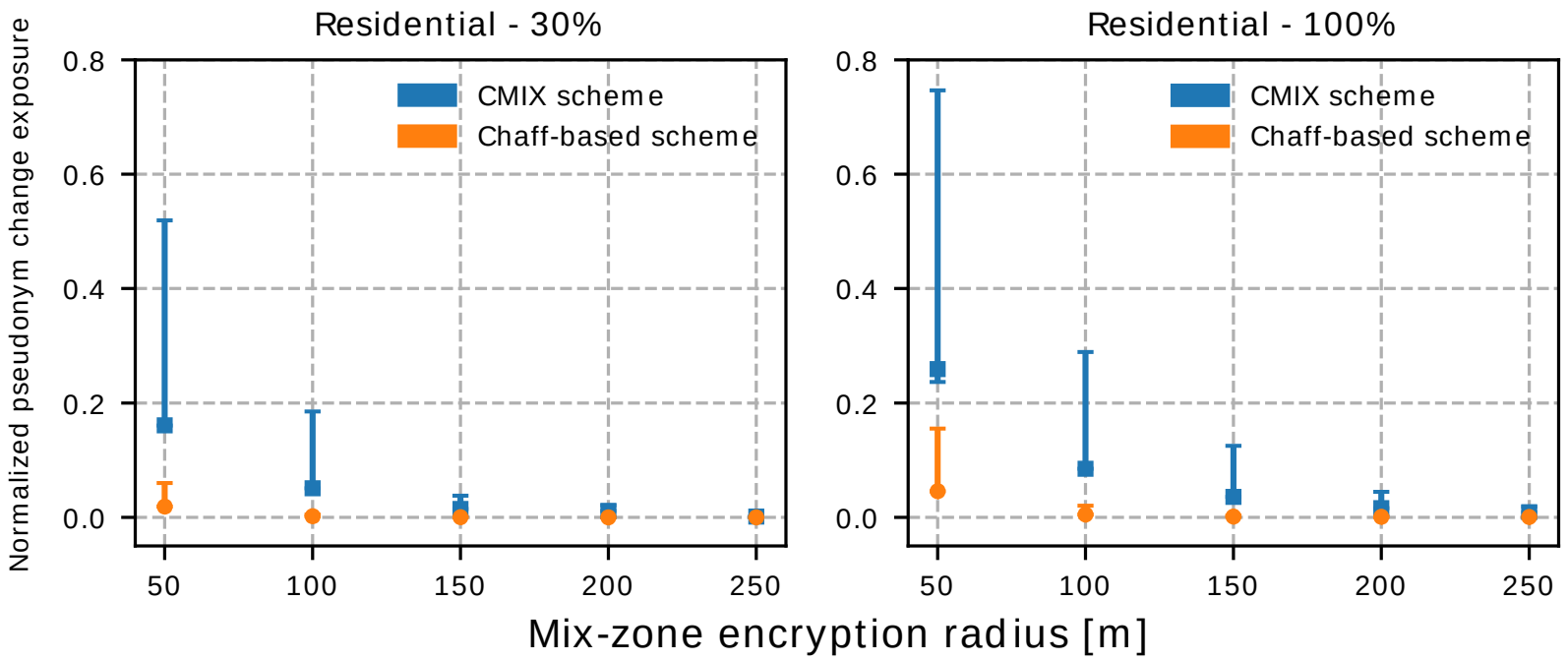
Simulation Results

- Encryption radius 50 m
- Attacker strength 100%



Simulation Results

- Encryption radius 50-250 m
- Attacker strength 30%/100%

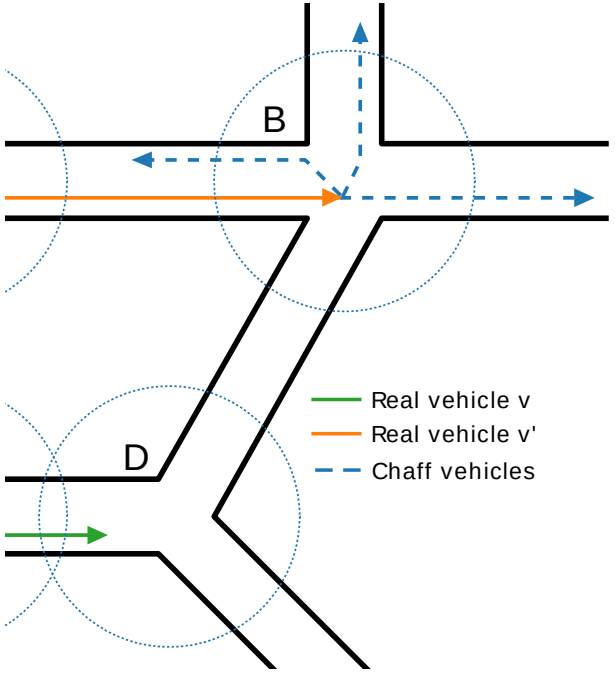


System Feasibility

Mix-zone Encryption Radius [m]	50	100	150	200	250
Max. Active Chaff Pseudonyms [#]	68	176	165	99	66
Max. CAM Generation [msg/s]	240	848	1321	831	634

- 30 * 60 * 176 = 316,800 chaff pseudonyms
- Cuckoo Filter with 3.63 MB
- ✓ Transmission speed 6 Mbit/s in IEEE 802.11p

- Generate 6742 ECDSA signatures per second
- ✓ NEXCOM (Dual-core 1.66 GHz, 1GB memory) with crypto module



Conclusion

- New pseudonym change strategy based on chaff vehicles and chaff messages
- Independent of operation area, mix-zone encryption radius, time of day, and driver population
- System performance: up to 76% improvement over CMIX
- Preserves safety application functionality
- Acceptable resource requirements

Future Work

- Resilience against internal attackers
- Impact of honest-but-curious VPKI entities

Nowhere to hide? Mix-Zones for Private Pseudonym Change using Chaff Vehicles

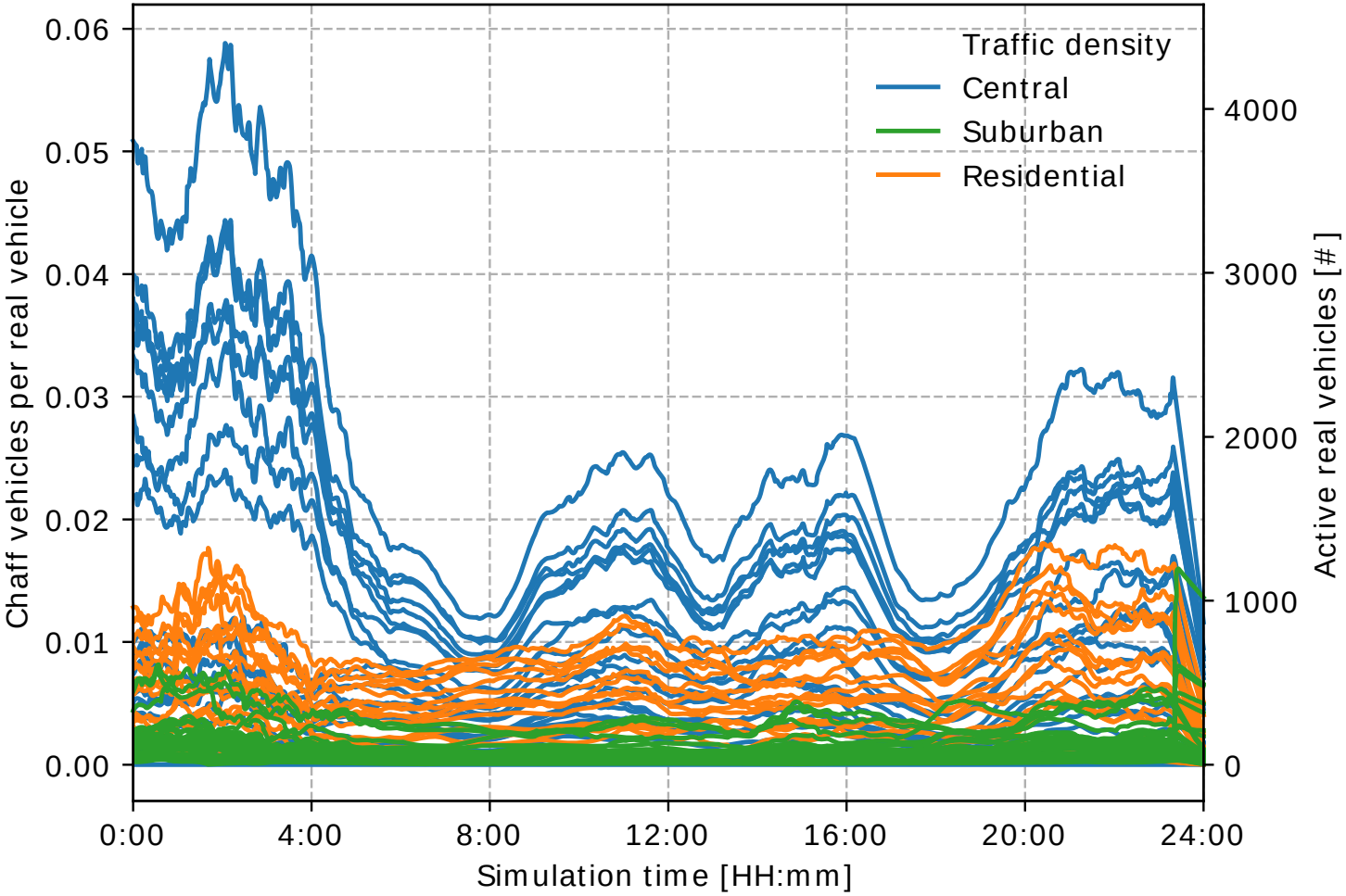
Thank you!

christian.vaas@cs.ox.ac.uk

References

[1] Golle, P., & Partridge, K. (2009, May). On the anonymity of home/work location pairs. In *International Conference on Pervasive Computing* (pp. 390-397). Springer, Berlin, Heidelberg.
[2] L. Codeca, R. Frank, S. Faye and T. Engel, "Luxembourg SUMO Traffic (LuST) Scenario: Traffic Demand Evaluation" in IEEE Intelligent Transportation Systems Magazine, vol. 9, no. 2, pp. 52-63, Summer 2017.
[3] PREXT: Privacy Extension for Veins VANET Simulator", IEEE Vehicular Networking Conference (VNC), Dec. 2016, Columbus, Ohio, USA
[4] Freudiger, J., Raya, M., Félegyházi, M., Papadimitratos, P., & Hubaux, J. P. (2007). Mix-zones for location privacy in vehicular networks. In ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS) (No. LCA-CONF-2007-016).

Simulation Results



Simulation Parameters

Area	1.31 km^2	0.61 km^2	1.38 km^2
Junctions	69	34	61
Mix-zones	31	18	28
Avg. Number of vehicles per zone	1825	4631	6500