SECMACE: Scalable and Robust Identity and Credential Infrastructure in Vehicular Communication

IEEE Transactions on Intelligent Transportation Systems (IEEE ITS), vol. 19, no. 5, May 2018

Mohammad Khodaei, Hongyu Jin, and **Panos Papadimitratos**

Networked Systems Security Group

www.ee.kth.se/nss

Vehicular communication systems (VCS)

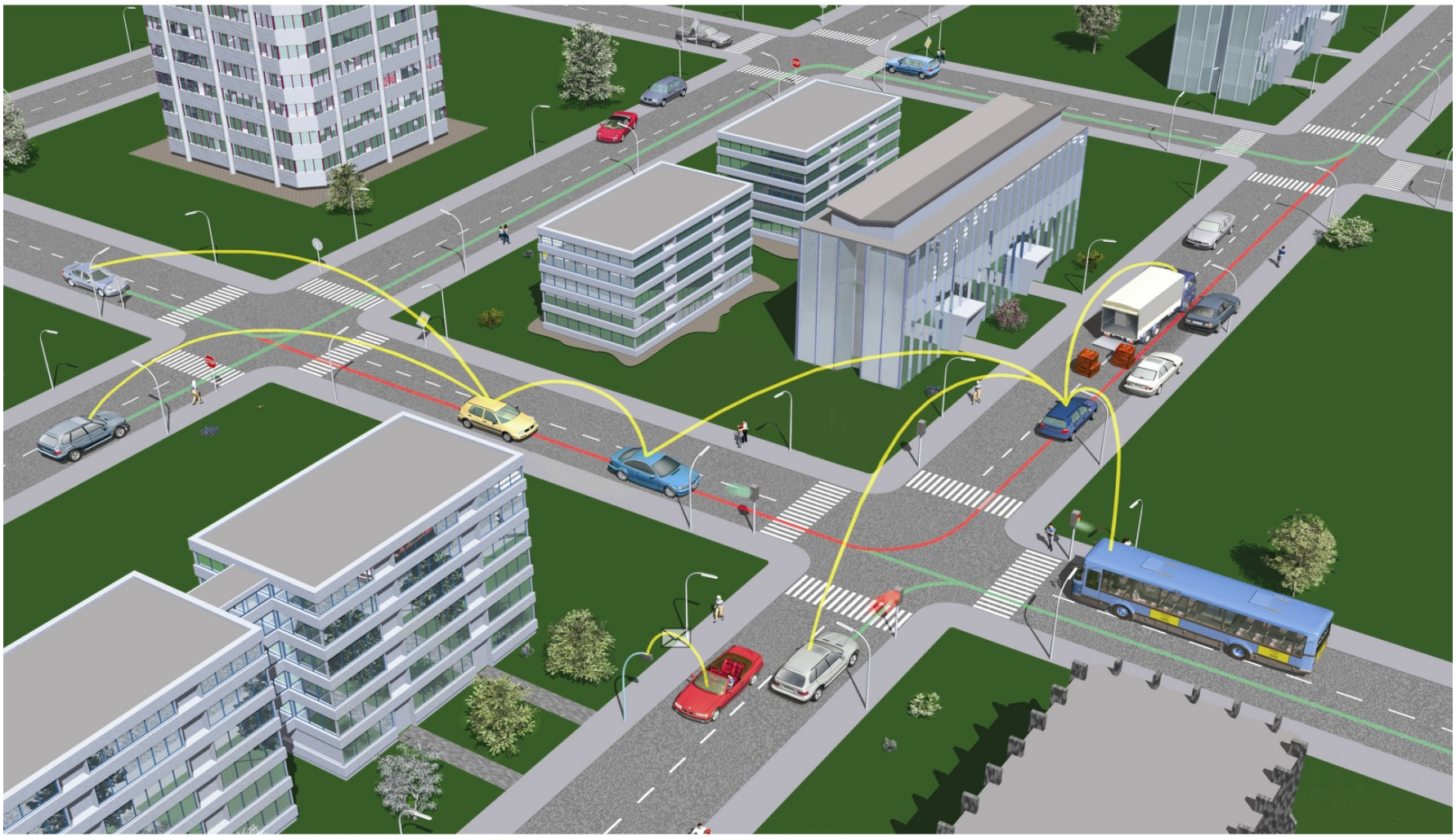
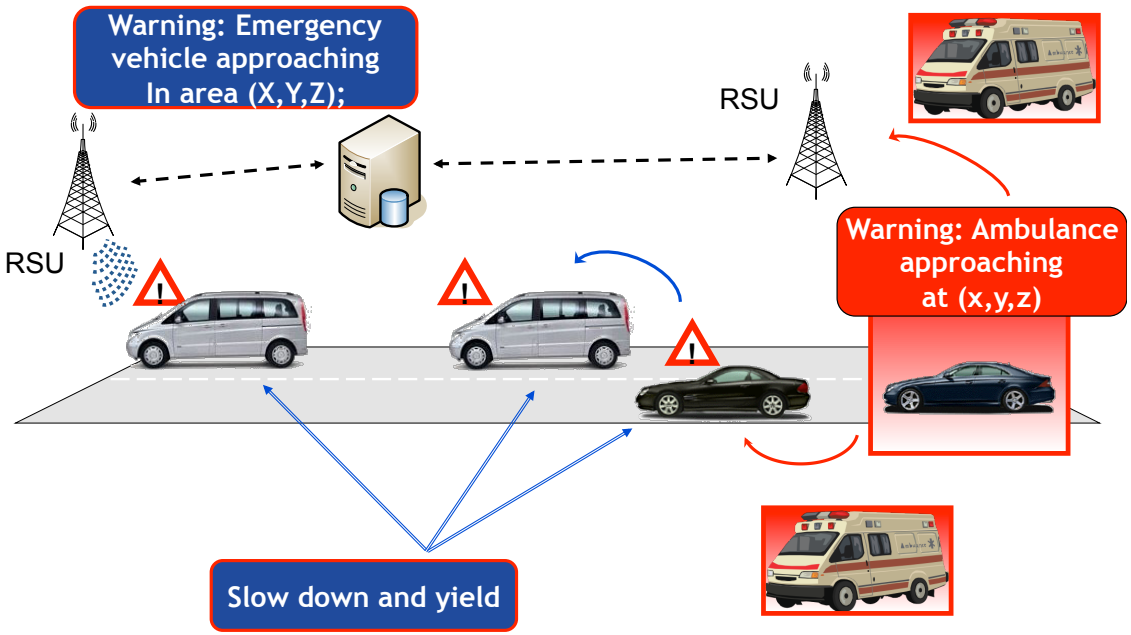


Illustration: C2C-CC

VCS security and privacy requirements*

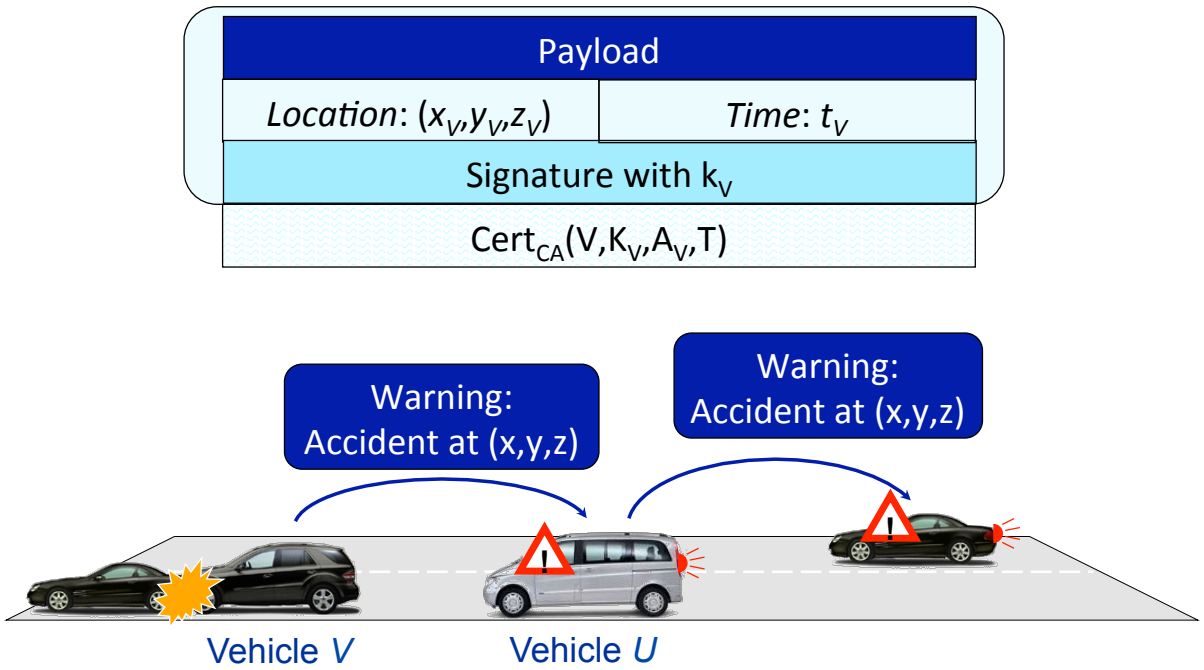


Vehicular communication

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

* *Securing vehicular communications-assumptions, requirements, and principles*, ESCAR 2006

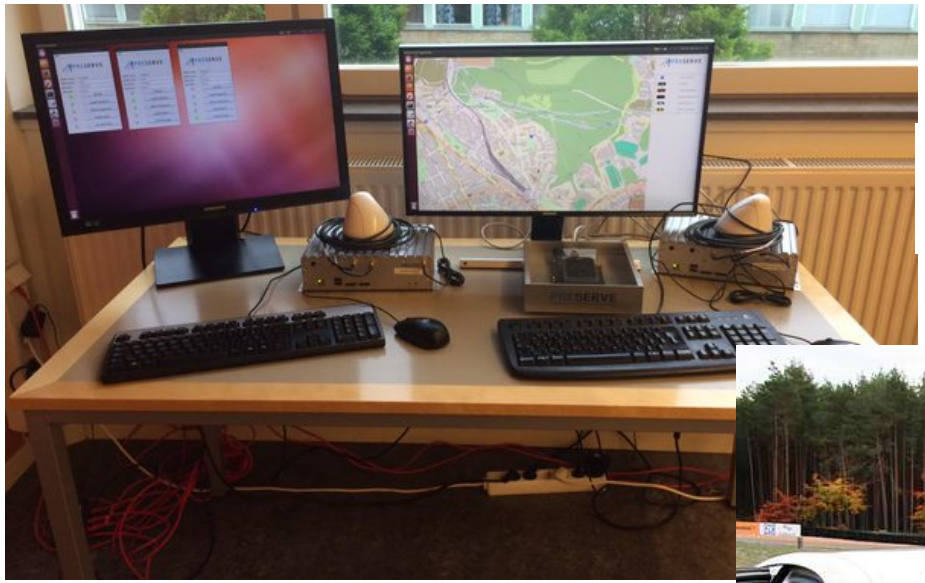
VCS security and privacy: Basic ideas*



- Ephemeral pseudonymous credentials; conditional anonymity
- Digitally signed V2X communications
- Hybrid approach: combination of anonymous and pseudonymous authentication

* *Secure vehicular communication systems: design and architecture*, IEEE CommMag 2008

VCS security and privacy: Basic ideas (cont'd)

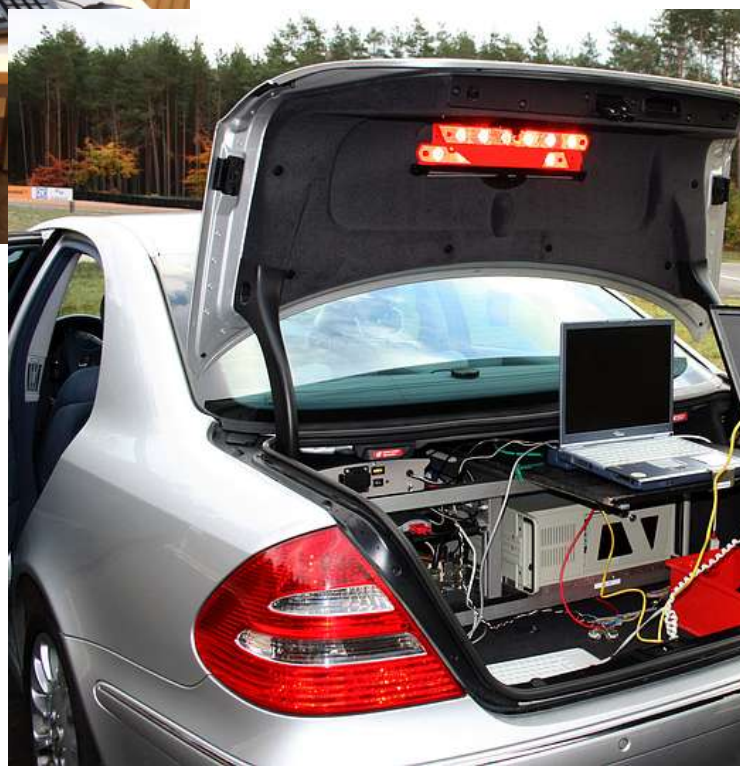


PRESERVE
preparing secure v2x communication systems

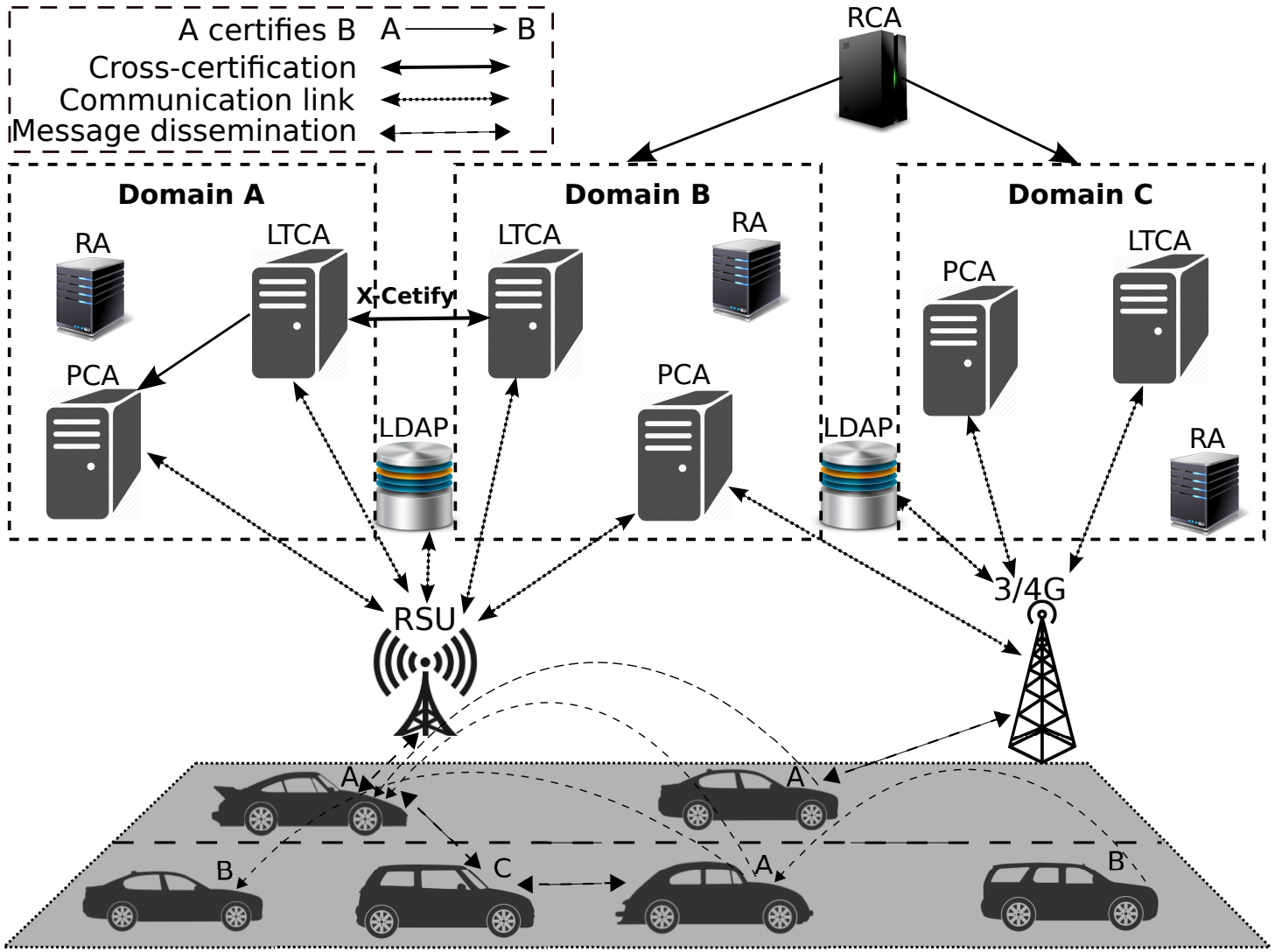
Final event, 2015

CAR 2 CAR
COMMUNICATION CONSORTIUM

First demo, 2008



VCS security and privacy: Basic ideas (cont'd)



VCS security and privacy: Basic ideas (cont'd)

- Vehicles registered with one Long Term CA (LTCA) (home domain)
- Pseudonym CA (PCA) servers in one or multiple domains
- Vehicles can obtain pseudonyms from any PCA (in home or foreign domains)
- Establish trust among entities with a Root CA (RCA) or with cross-certification
- Resolve a pseudonym with the help of a Resolution Authority (RA)

VCS security and privacy: Basic ideas (cont'd)

Adversaries

- Malicious users/vehicles/nodes (On-Board Units (OBUs))
  - Arbitrary behavior
  - "Sybil" users (each posing as multiple users)
  - Collusion
- Selfish users
- Honest-but-curious system infrastructure (security & privacy infrastructure servers)
  - Correct protocol execution
  - Curious to infer private user information

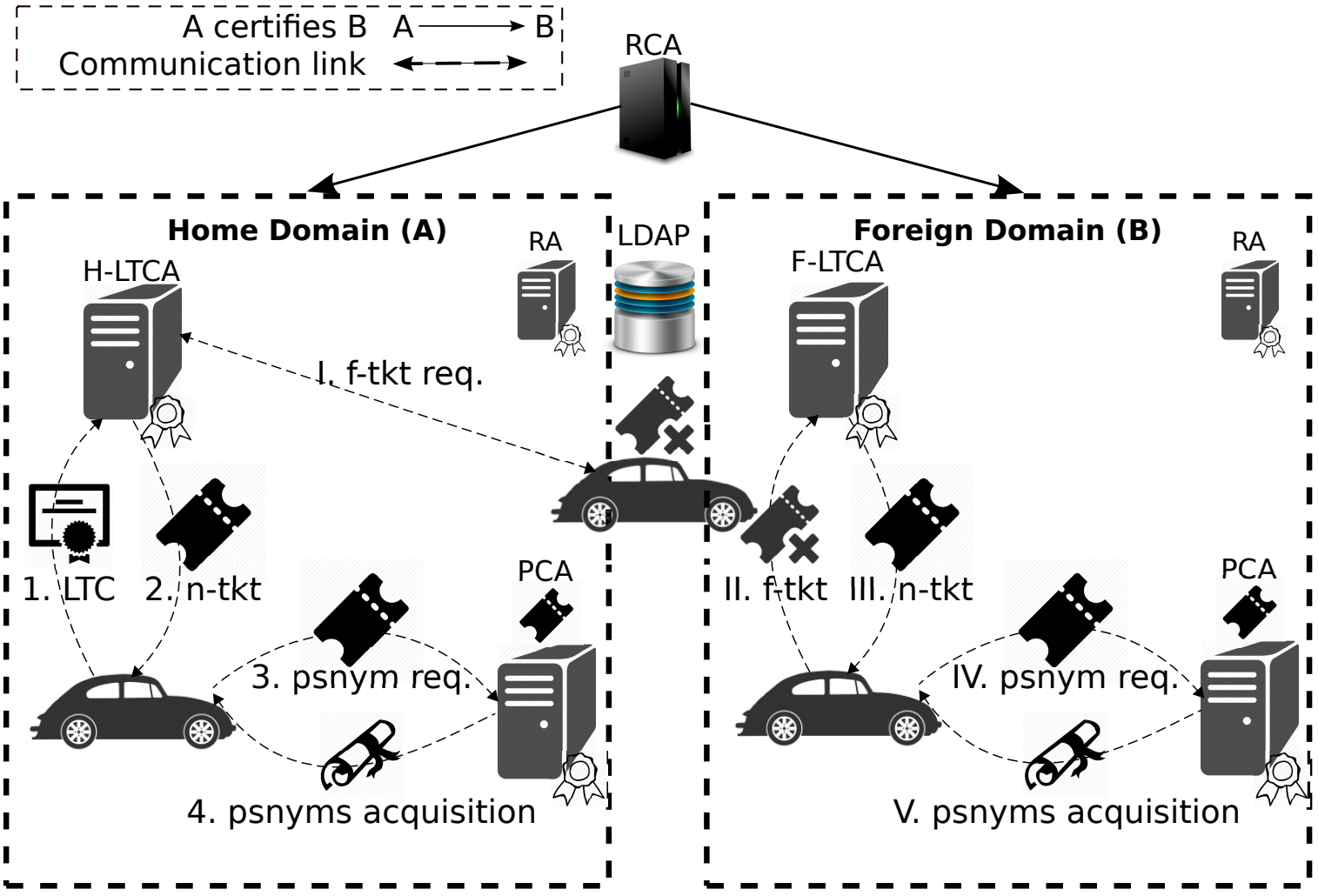
Designing the VCS security infrastructure

- Focus: Vehicular Public-Key Infrastructure (VPKI)
- Design, analyze, implement and evaluate the VPKI
  - Management of credentials: provisioning, revocation, resolution
  - Protocols for all vehicle-to-VPKI and intra-VPKI interactions
- Challenges: complexity and constraints
  - Security **and** privacy
  - Multiple and diverse entities, global deployment, long-lived entities
  - Short-lived credentials, very large numbers
  - Cost-driven platform resource constraints

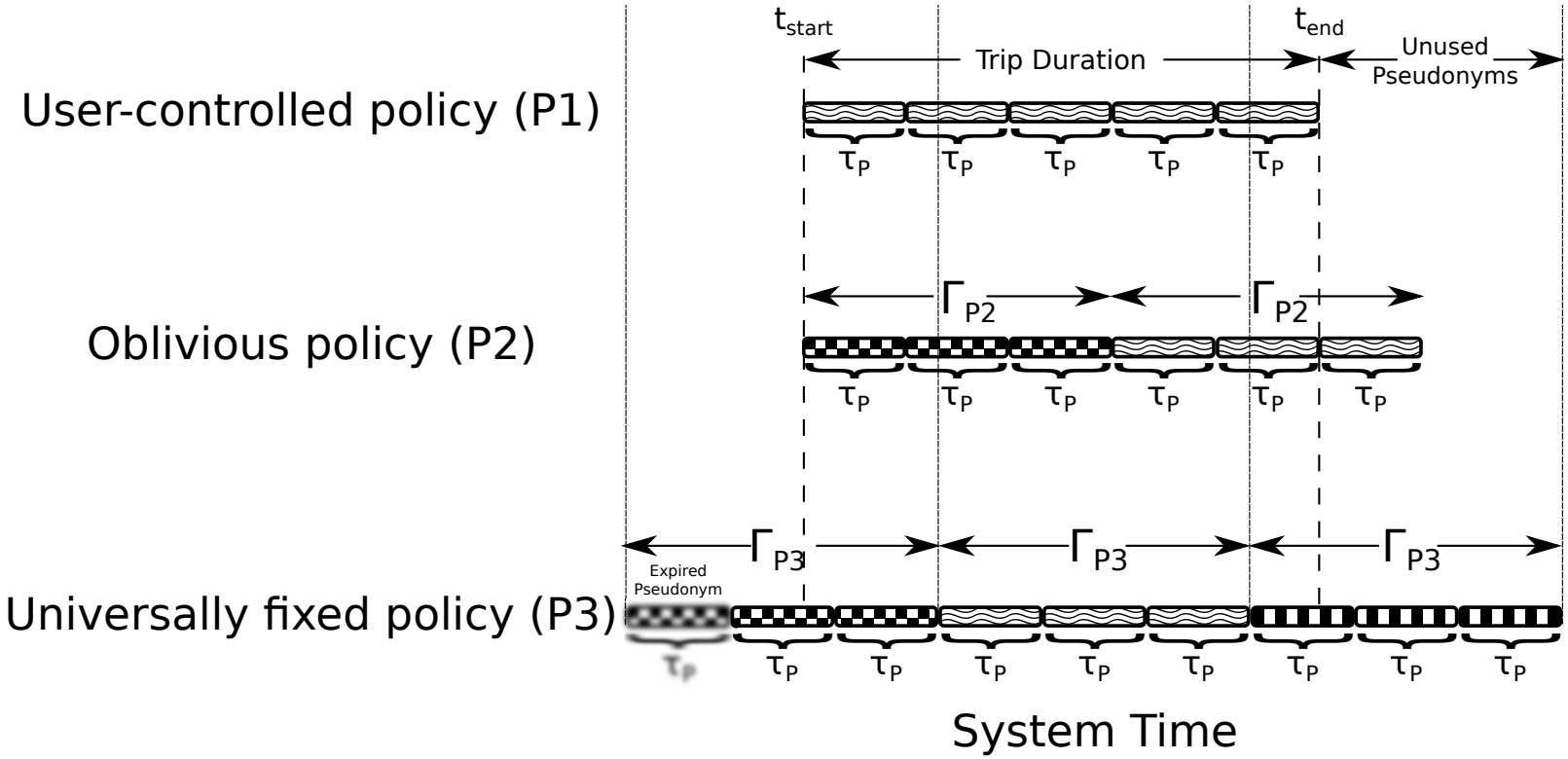
Designing the VCS security infrastructure: goals

- Resilience to *honest-but-curious* VPKI entities
- Eradication of Sybil-based misbehavior
- Standard-compliant implementation
- Scalability
  - Multi-domain operation
  - Efficiency
- Revocation and resolution

Designing the VCS security infrastructure: System instance

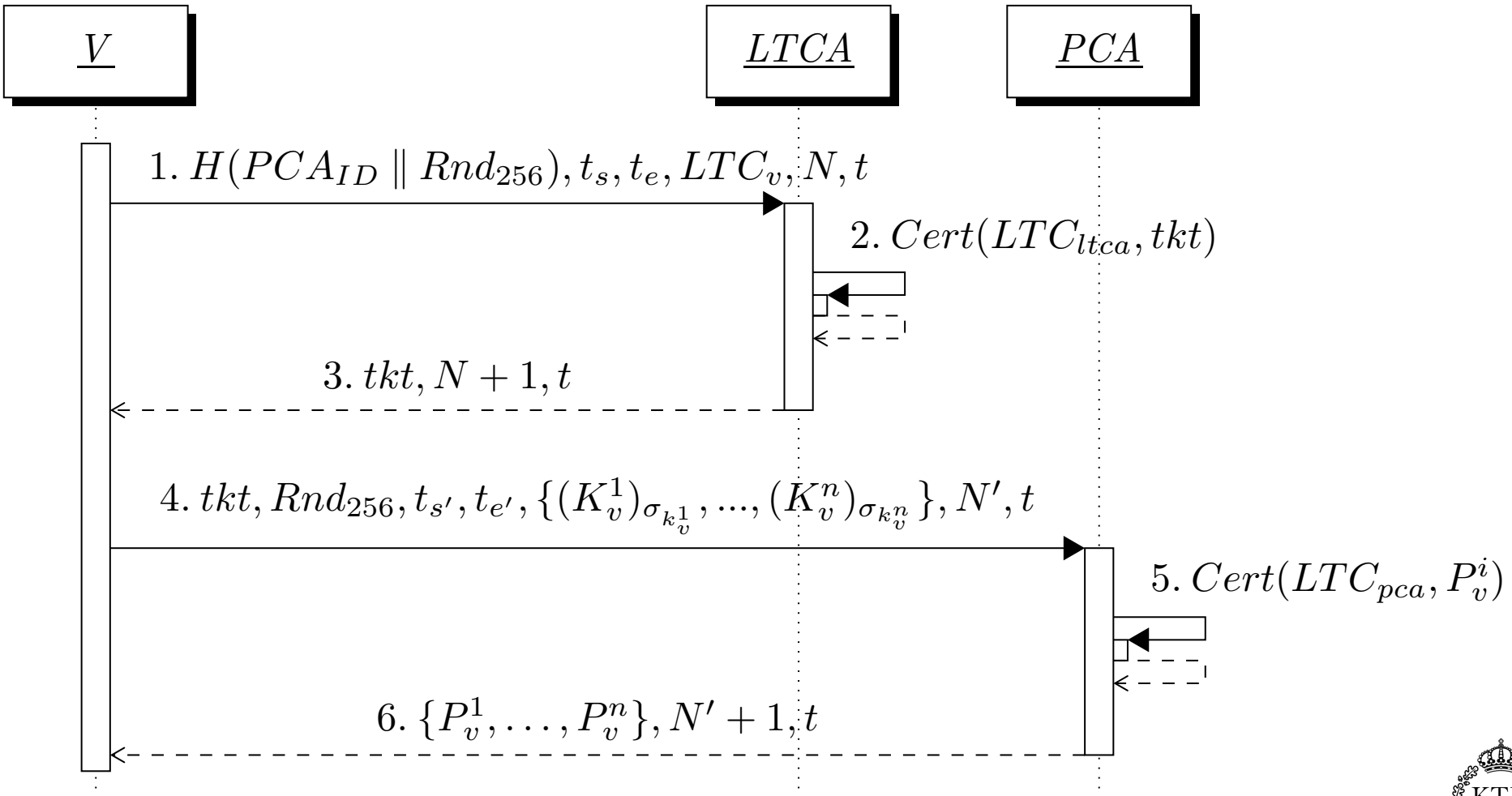


Designing the VCS security infrastructure: Pseudonym acquisition policies



- P1 & P2: Requests could be user *"fingerprints"*: exact times of requests throughout the trip
- P3: Request intervals falling within *"universally"* fixed intervals Γ_{P3}; pseudonym lifetimes aligned with the PCA clock

Ticket and pseudonym acquisition



Ticket acquisition protocols

Protocol 1 Ticket Request (from the LTCA)

1: **procedure** REQTICKET($P_x, \Gamma_{Px}, t_s, t_e, t_{date}$)
2: **if** $P_x = P1$ **then**
3: $(t_s, t_e) \leftarrow (t_s, t_e)$
4: **else if** $P_x = P2$ **then**
5: $(t_s, t_e) \leftarrow (t_s, t_s + \Gamma_{P2})$
6: **else if** $P_x = P3$ **then**
7: $(t_s, t_e) \leftarrow (t_{date} + \Gamma^{i}_{P3}), t_{date} + \Gamma^{i+1}_{P3})$
8: **end if**
9: $\zeta \leftarrow (Id_{tkt\text{-}req}, H(Id_{PCA} \| Rnd_{tkt}), t_s, t_e)$
10: $(\zeta)_{\sigma_v} \leftarrow Sign(Lk_v, \zeta)$
11: **return** $((\zeta)_{\sigma_v}, \text{LTC}_v, N, t_{now})$
12: **end procedure**

- Run over Transport Layer Security (TLS) with mutual authentication

Protocol 2 Issuing a Ticket (by the LTCA)

1: **procedure** ISSUETICKET($(msg)_{\sigma_v}, \text{LTC}_v, N, t_{now}$)
2: Verify($\text{LTC}_v, (msg)_{\sigma_v}$)
3: $IK_{tkt} \leftarrow H(\text{LTC}_v || t_s || t_e || Rnd_{IK_{tkt}})$
4: $\zeta \leftarrow (SN, H(Id_{PCA} \| Rnd_{tkt}), IK_{tkt}, Rnd_{IK_{tkt}}, t_s, t_e, Exp_{tkt})$
5: $(tkt)_{\sigma_{ltca}} \leftarrow Sign(Lk_{ltca}, \zeta)$
6: **return** $((tkt)_{\sigma_{ltca}}, N + 1, t_{now})$
7: **end procedure**

- *"ticket identifiable key"* (IK_{tkt}): it binds a ticket to the corresponding Long Term Certificate (LTC)
- A faulty LTCA cannot resolve an LTC other than the one the ticket was issued for

Pseudonym acquisition protocols

Protocol 3 Pseudonym Request (from the PCA)

1: **procedure** REQPSNYMS($t_s, t_e, (tkt)_{\sigma_{ltca}}$)
2: **for** i:=1 to **n do**
3: **Begin**
4: Generate(K_v^i, k_v^i)
5: $(K_v^i)_{\sigma_{k_v^i}} \leftarrow$ Sign(k_v^i, K_v^i)
6: **End**
7: $psnymReq \leftarrow (Id_{req}, Rnd_{tkt}, t_s, t_e, (tkt)_{\sigma_{ltca}}, \{(K_v^1)_{\sigma_{k_v^1}}, ..., (K_v^n)_{\sigma_{k_v^n}}\}, N, t_{now})$
8: **return** $psnymReq$
9: **end procedure**

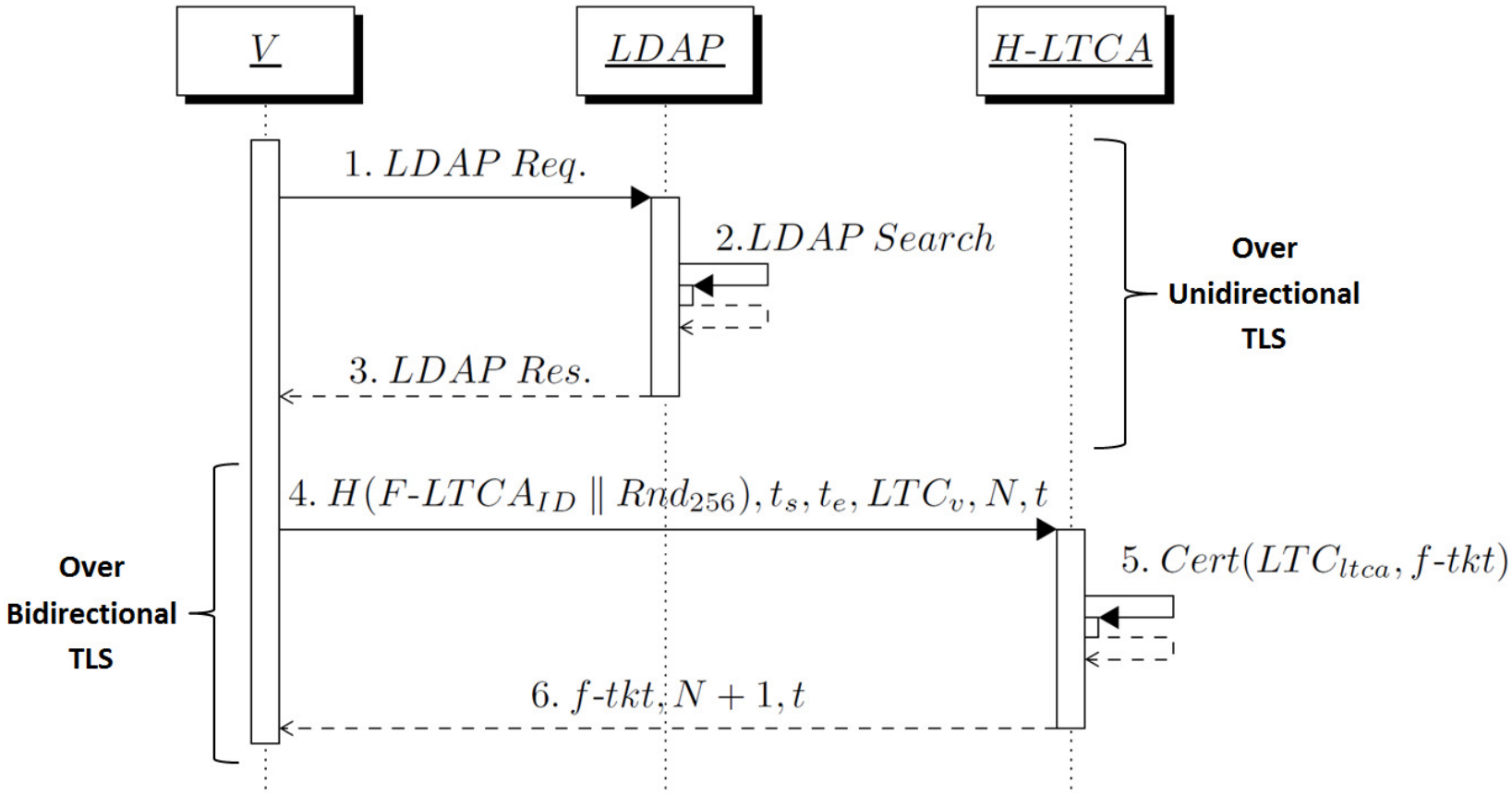
- Run over TLS with unidirectional (server-only) authentication

Protocol 4 Issuing Pseudonyms (by the PCA)

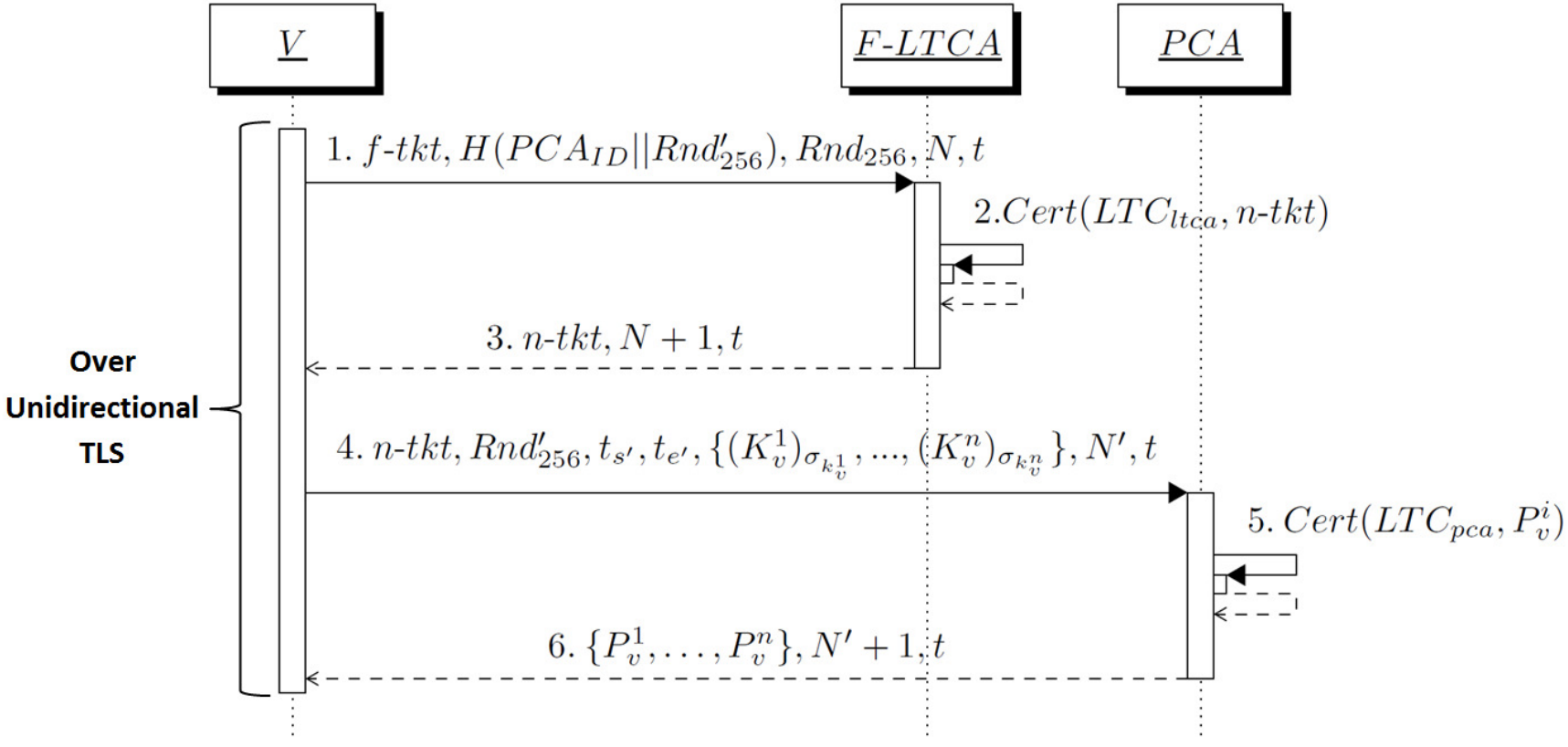
1: **procedure** ISSUEPSNYMS($psnymReq$)
2: $psnymReq \rightarrow (Id_{req}, Rnd_{tkt}, t_s, t_e, (tkt)_{\sigma_{ltca}}, \{(K_v^1)_{\sigma_{k_v^1}}, ..., (K_v^n)_{\sigma_{k_v^n}}\}, N, t_{now})$
3: Verify($LTC_{ltca}, (tkt)_{\sigma_{ltca}}$)
4: $H(Id_{this\text{-}PCA} \| Rnd_{tkt}) \stackrel{?}{=} H(Id_{PCA} \| Rnd_{tkt})$
5: $[t_s,\ t_e] \stackrel{?}{=} ([t_s, t_e])_{tkt}$
6: **for** i:=1 to **n do**
7: **Begin**
8: Verify($K_v^i, (K_v^i)_{\sigma_{k_v^i}}$)
9: $IK_{P^i} \leftarrow H(IK_{tkt} || K_v^i || t_s^i || t_e^i || Rnd_{IK_v^i})$
10: $\zeta \leftarrow (SN^i, K_v^i, IK_{P^i}, Rnd_{IK_v^i}, t_s^i, t_e^i)$
11: $(P_v^i)_{\sigma_{pca}} \leftarrow Sign(Lk_{pca}, \zeta)$
12: **End**
13: **return** $(\{(P_v^1)_{\sigma_{pca}}, \ldots, (P_v^n)_{\sigma_{pca}}\}, N{+}1, t_{now})$
14: **end procedure**

- *"pseudonym identifiable key"* (IK_{Pi}): it binds a pseudonym to the corresponding ticket
- A faulty PCA cannot resolve pseudonyms other than the ones issued for the ticket

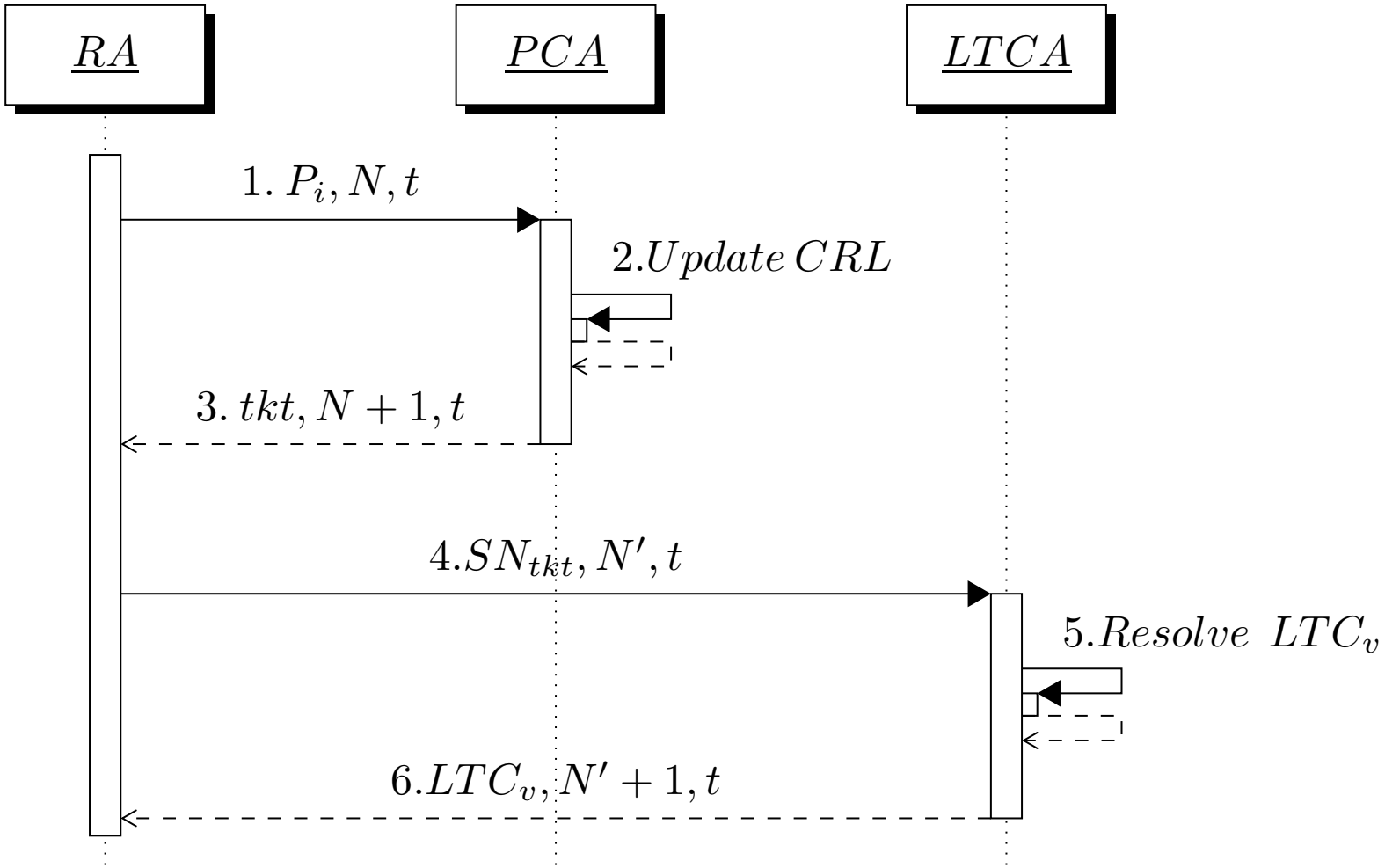
Roaming user: Foreign ticket authentication



Ticket and pseudonym acquisition in a foreign domain



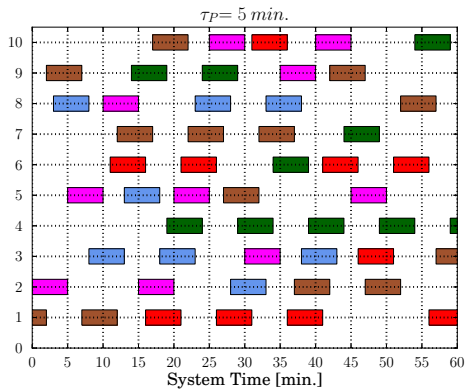
Pseudonym revocation and resolution



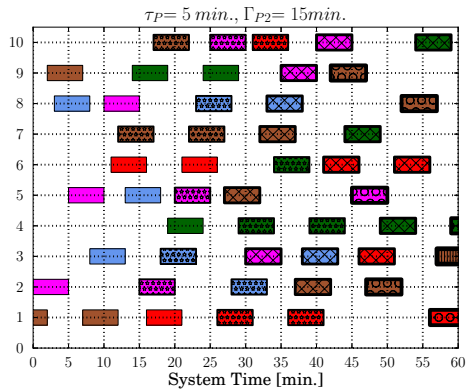
Security analysis

- Communication integrity, confidentiality, and non-repudiation
  - Certificates, TLS and digital signatures
- Authentication, authorization and access control
  - LTCA is the *policy decision and enforcement point*
  - PCA grants the service
  - Discovery of available servers: Lightweight Directory Access Protocol (LDAP)
- Concealing PCAs, F-LTCA, and actual pseudonym acquisition times
  - Sending $H(PCA_{id} \| Rnd_{256})$, t_s, t_e, LTC_v to the H-LTCA
  - A PCA verifies whether $[t'_s,\ t'_e] \subseteq [t_s,\ t_e]$
- Thwarting Sybil-based misbehavior
  - An LTCA never issues valid tickets with overlapping lifetimes (for a given domain)
  - A ticket is bound to a specific PCA
  - A PCA keeps records of used tickets

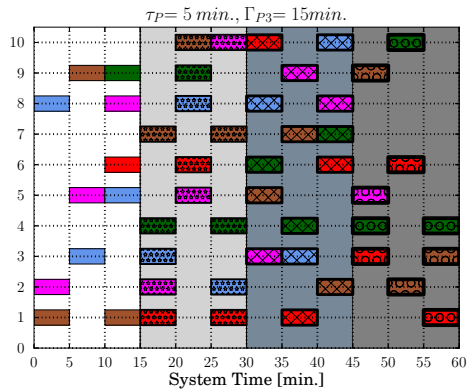
Pseudonym linkability based on timing information



(a) P1: User-controlled policy



(b) P2: Oblivious policy



(c) P3: Universally fixed policy

- P1 & P2: Distinct lifetimes per vehicle make linkability easier (requests/pseudonyms could act as user *'fingerprints'*)
- P3: Uniform pseudonym lifetimes eliminate the timing fingerprints

Experimental setup

- VPKI testbed
  - Implementation in C++
  - OpenSSL: TLS and Elliptic Curve Digital Signature Algorithm (ECDSA)-256 according to the standard [1]

	LTCA	PCA	RA	Clients
VM Number	2	5	1	25
Dual-core CPU (Ghz)	2.0	2.0	2.0	2.0
BogoMips	4000	4000	4000	4000
Memory	2GB	2GB	1GB	1GB
Database	MySQL	MySQL	MySQL	MySQL
Web Server	Apache	Apache	Apache	-
Emulated Threads	-	-	-	400

Experimental setup (cont'd)

	TAPAS Cologne	LuST [2]
Number of vehicles	75,576	138,259
Number of trips	75,576	287,939
Duration of snapshot (hours)	24	24
Available duration of snapshot (hours)	2 (6-8 AM)	24
Average trip duration (seconds)	590.49	692.81
Total trip duration (seconds)	44,655,579	102,766,924

- Main metric: Pseudonym acquisition latency (note: termed *end-to-end)*
  - *From the initialization of the ticket acquisition protocol till the successful completion of pseudonym acquisition protocol*
- *Note: PRESERVE Nexcom boxes: dual-core 1.66 GHz, 2GB Memory*

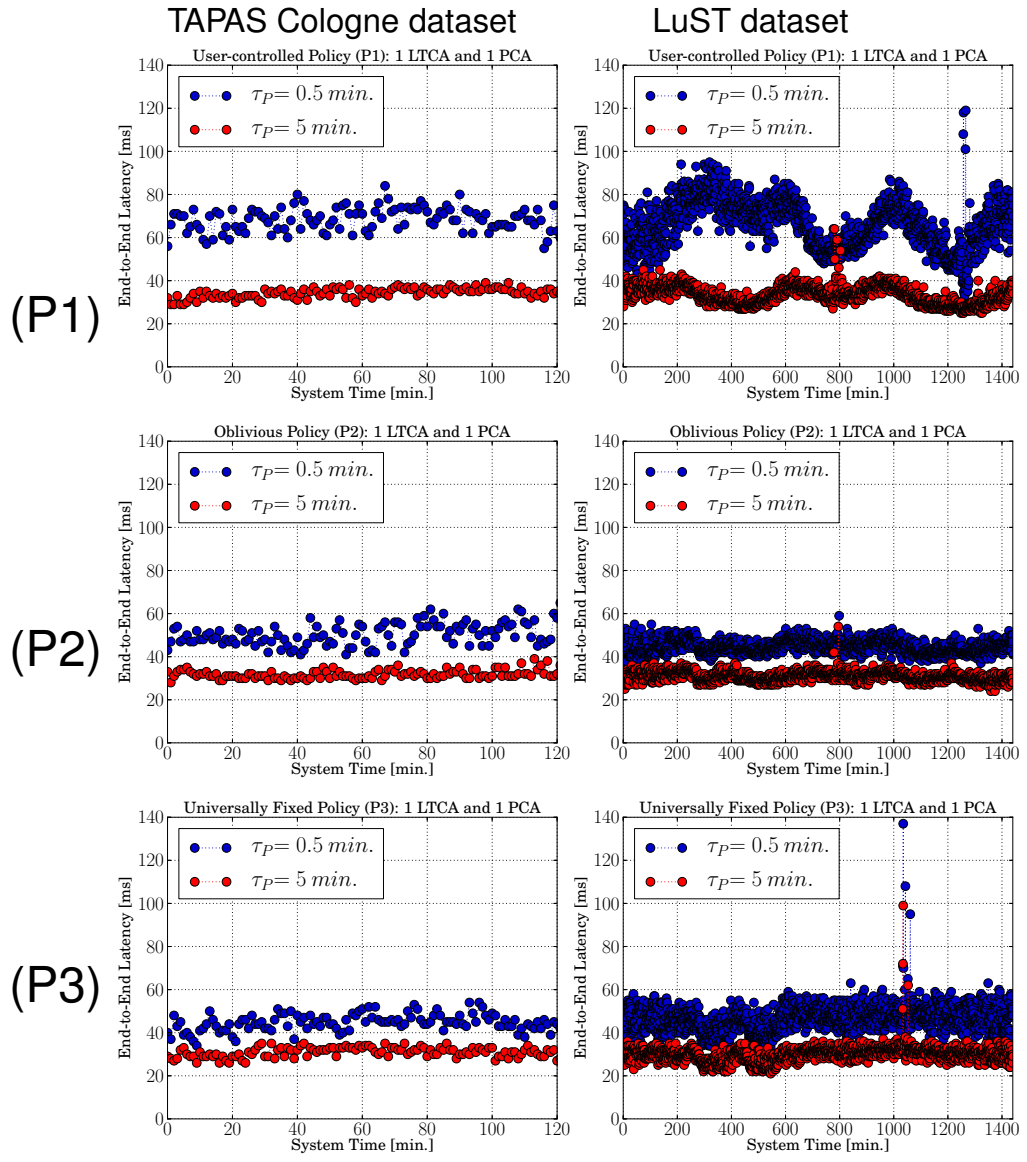
Latency for P1, P2, and P3

Parameters:

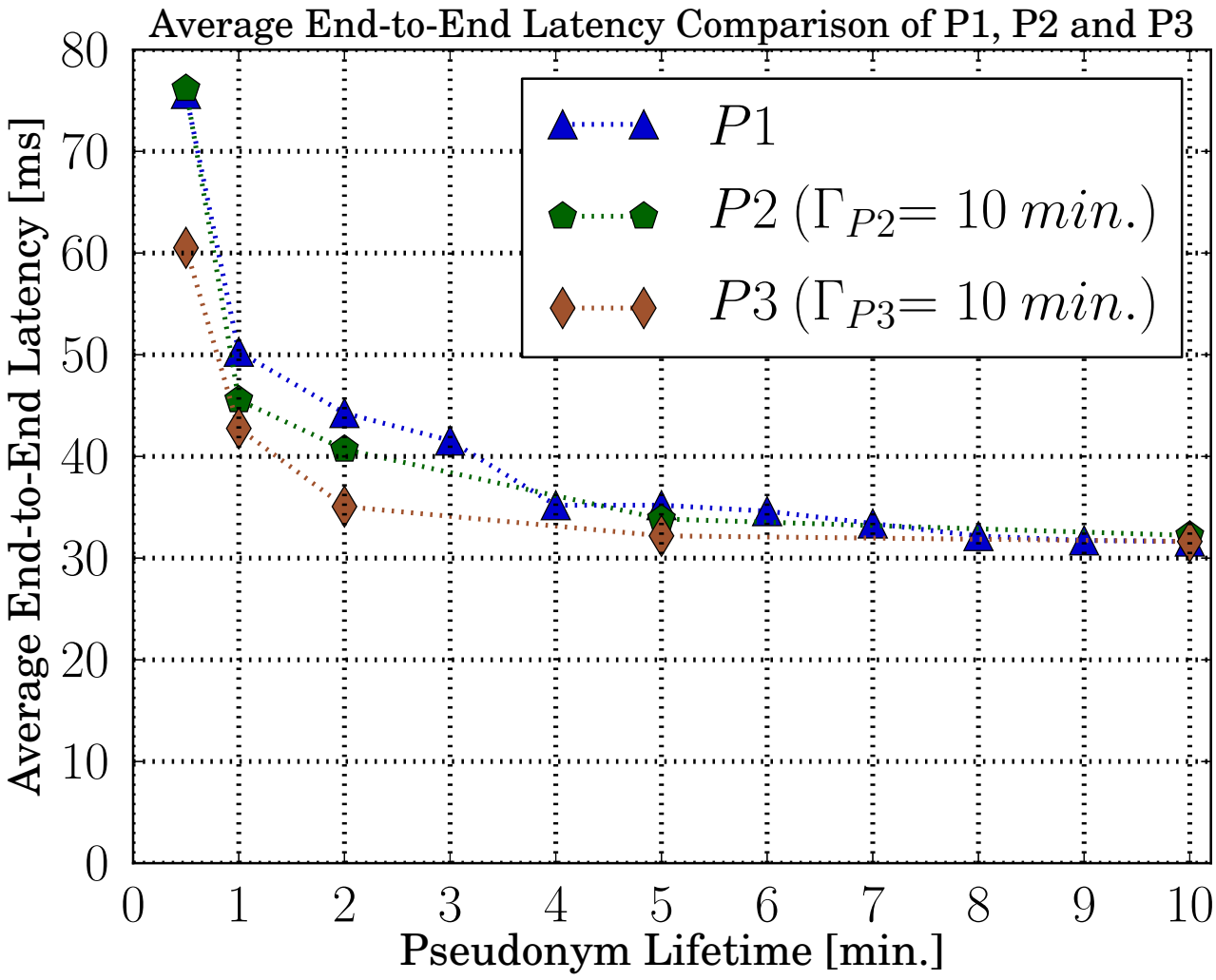
- Improved privacy, thus short-lived pseudonyms, and frequent interactions with/high workload for the PCA
- Γ=5 min, τ_P=0.5 min, 5 min

LuST dataset ($\tau_P = 0.5\ min$):

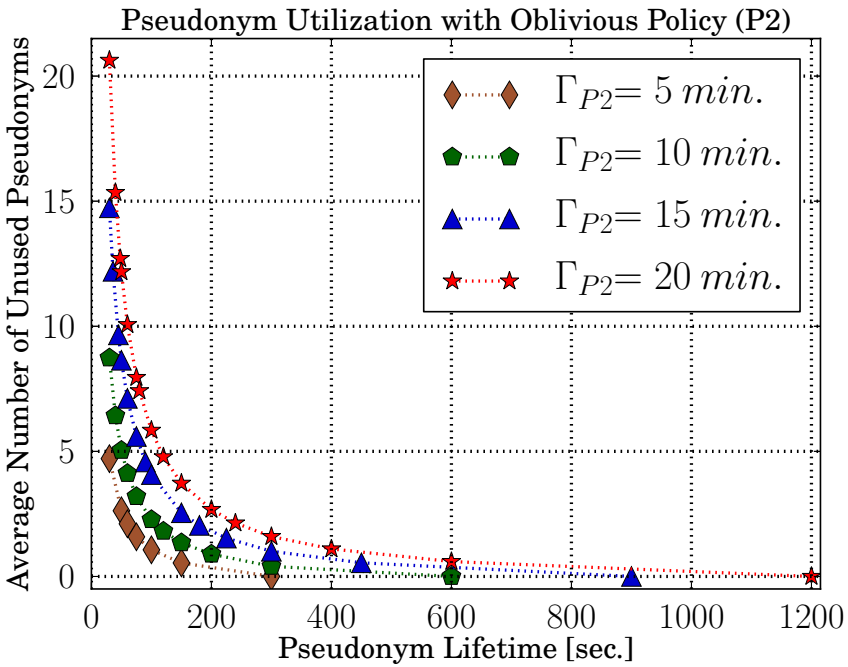
- P1: $F_x(t = 167\ ms) = 0.99$
- P2: $F_x(t = 80\ ms) = 0.99$
- P3: $F_x(t = 74\ ms) = 0.99$



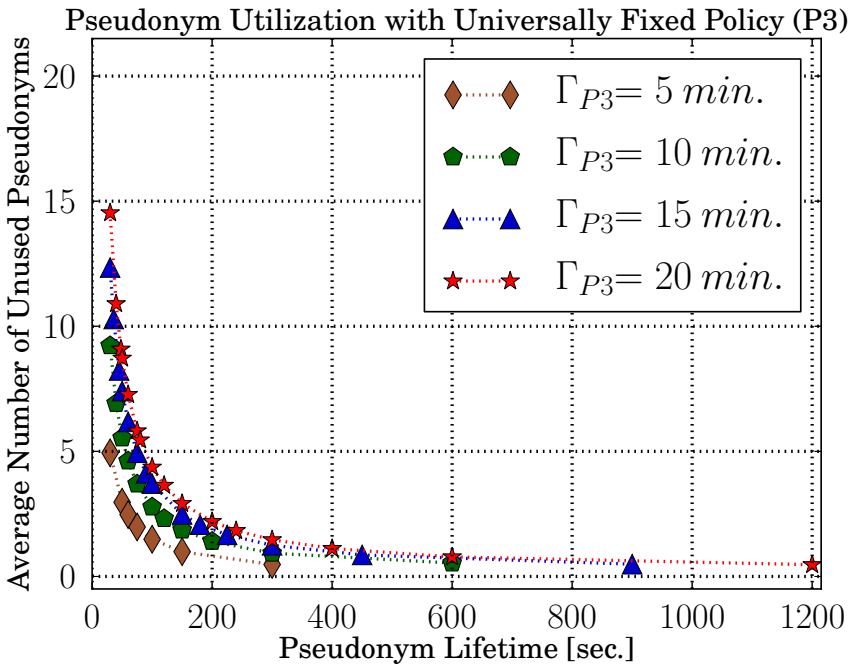
Latency for P1, P2, and P3 (cont'd)



Pseudonym utilization



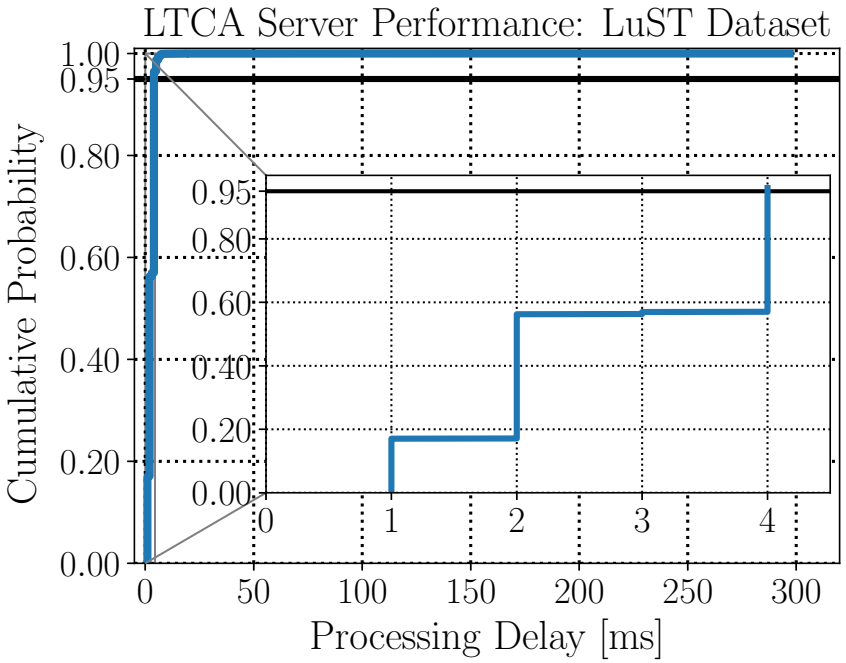
P2: Oblivious Policy



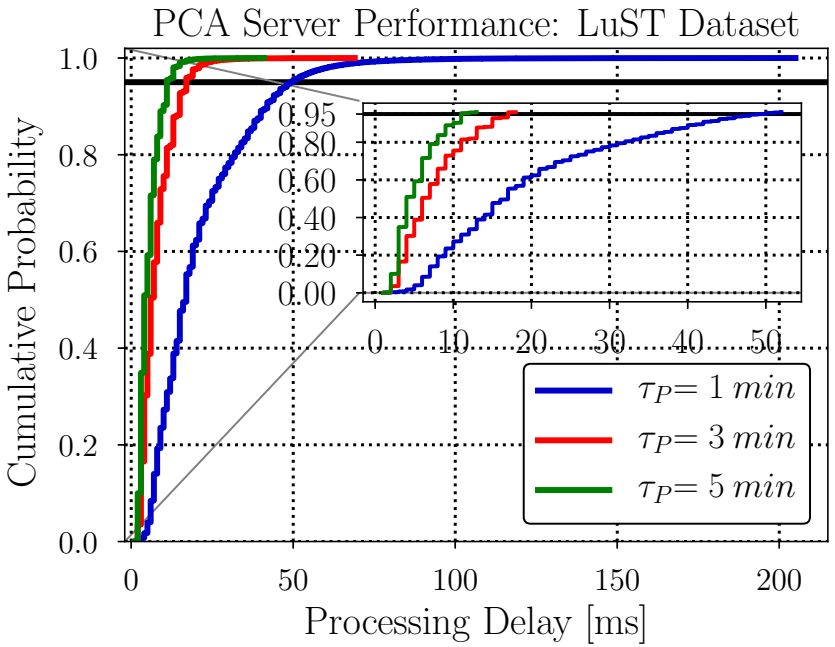
P3: Universally Fixed Policy

LuST dataset for P2 & P3

Ticket and pseudonym acquisition



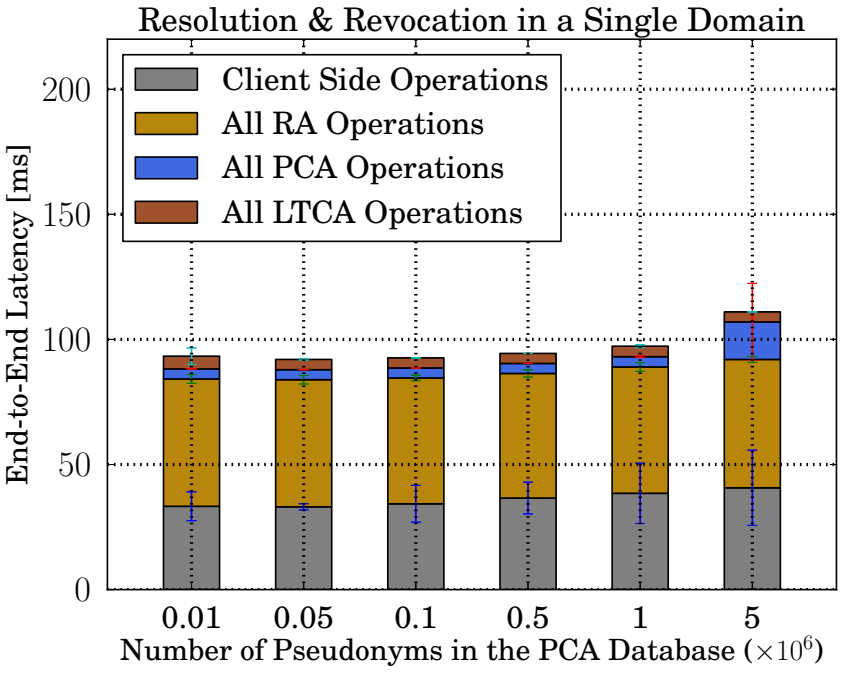
LTCA delay



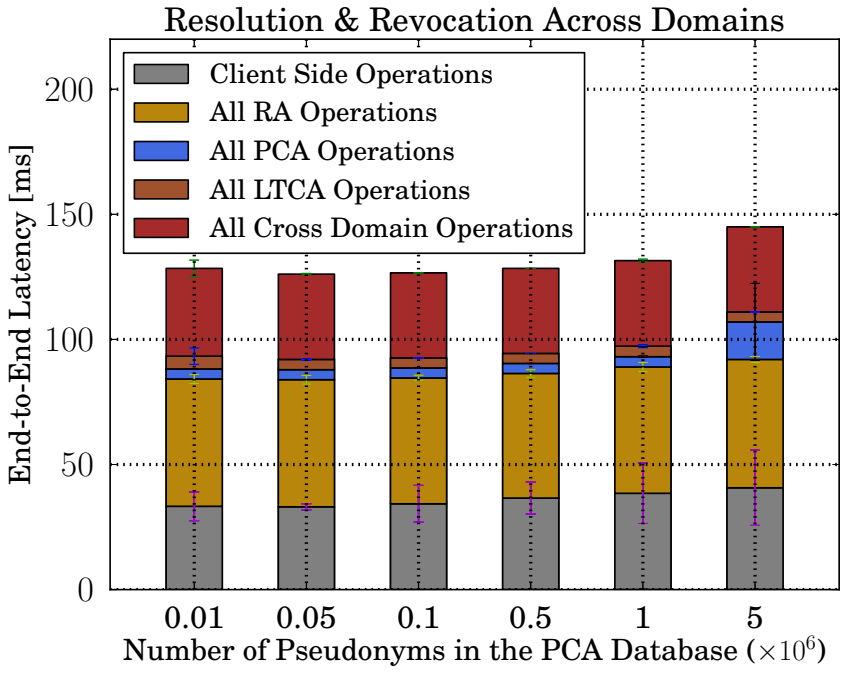
PCA delay

- Ticket Acquisition: F_x(t=4ms)=0.95
- Pseudonym Acquisition: F_x(t=52ms)=0.95

Pseudonym resolution and revocation



Single domain



Across domains

- On average 100 ms to resolve & revoke a pseudonym

Comparison with other implementations

- Latency for 100 pseudonyms (without communication delay)

	$Delay_{\text{PCA}}$	CPU_{PCA}
VeSPA [3]	817 ms	3.4 GHz
SEROSA [4]	650 ms	2.0 GHz
PUCA [5]	1000 ms	2.53 GHz
PRESERVE PKI (Fraunhofer SIT) [6]	$\approx$ 4000 ms	N/A
C2C-CC PKI (ESCRYPT) [7]	393 ms	N/A
SECMACE	260 ms	2.0 GHz

Wrap-up

- Solution for a challenging problem at hand
  - Security & privacy
  - Complexity
  - Cost and deployment constraints
  - VC system constraints and scale
- Modest workstations running the PCA and LTCA servers can handle tens of thousands of vehicles
- More work
  - Revocation: distribution of revocation information
  - Misbehaviour/fault detection
  - Dynamic scaling of the servers
- System can be used in different contexts
  - Security and privacy for Location Based Services (LBSs)
- Common ideas with other large-scale mobile systems
  - Security and privacy for Participatory Sensing systems

CRL distribution in VCS: Challenges and motivation

Traditional PKI vs. Vehicular PKI

- Dimensions (5 orders of magnitude more credentials)
- Balancing act: security, privacy, and efficiency
  - *Honest-but-curious* VPKI entities
  - Performance constraints: safety- and time-critical operations
- “Mechanics” of revocation:
  - *Highly dynamic environment with intermittent connectivity*
  - *Short-lived pseudonyms, multiple per entity*
  - *Resource constraints*

CRL distribution in VCS: Challenges and motivation

(cont'd)

- Efficient and timely distribution of Certificate Revocation Lists (CRLs) to every legitimate vehicle in the system
- Strong privacy for vehicles prior to revocation events
- Computation and communication constraints for On-Board Units (OBUs), intermittent connectivity to the infrastructure
- Peer-to-peer distribution is a double-edged sword: abusive peers could "pollute" the process, thus degrading the timeliness of the CRL distribution

Vehicle-Centric CRL Distribution*

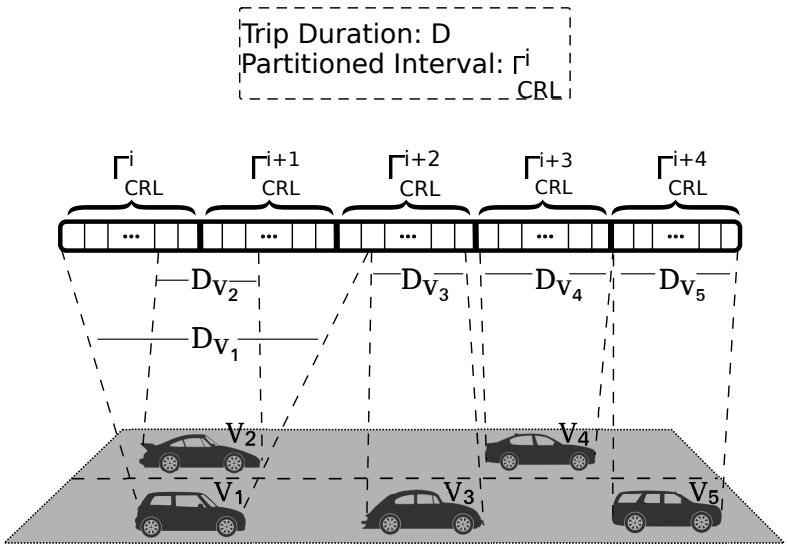


Figure: CRL as a Stream:

V_1 subscribes to $\{\Gamma^i_{CRL}, \Gamma^{i+1}_{CRL}, \Gamma^{i+2}_{CRL}\}$;
$V_2 : \{\Gamma^i_{CRL}, \Gamma^{i+1}_{CRL}\}$;
$V_3 : \{\Gamma^{i+2}_{CRL}\}$;
$V_4 : \{\Gamma^{i+3}_{CRL}\}$;
$V_5 : \{\Gamma^{i+4}_{CRL}\}$.

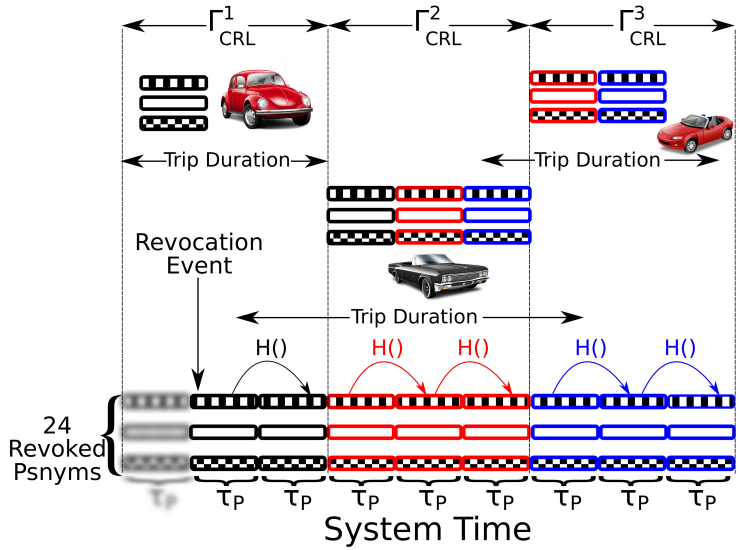
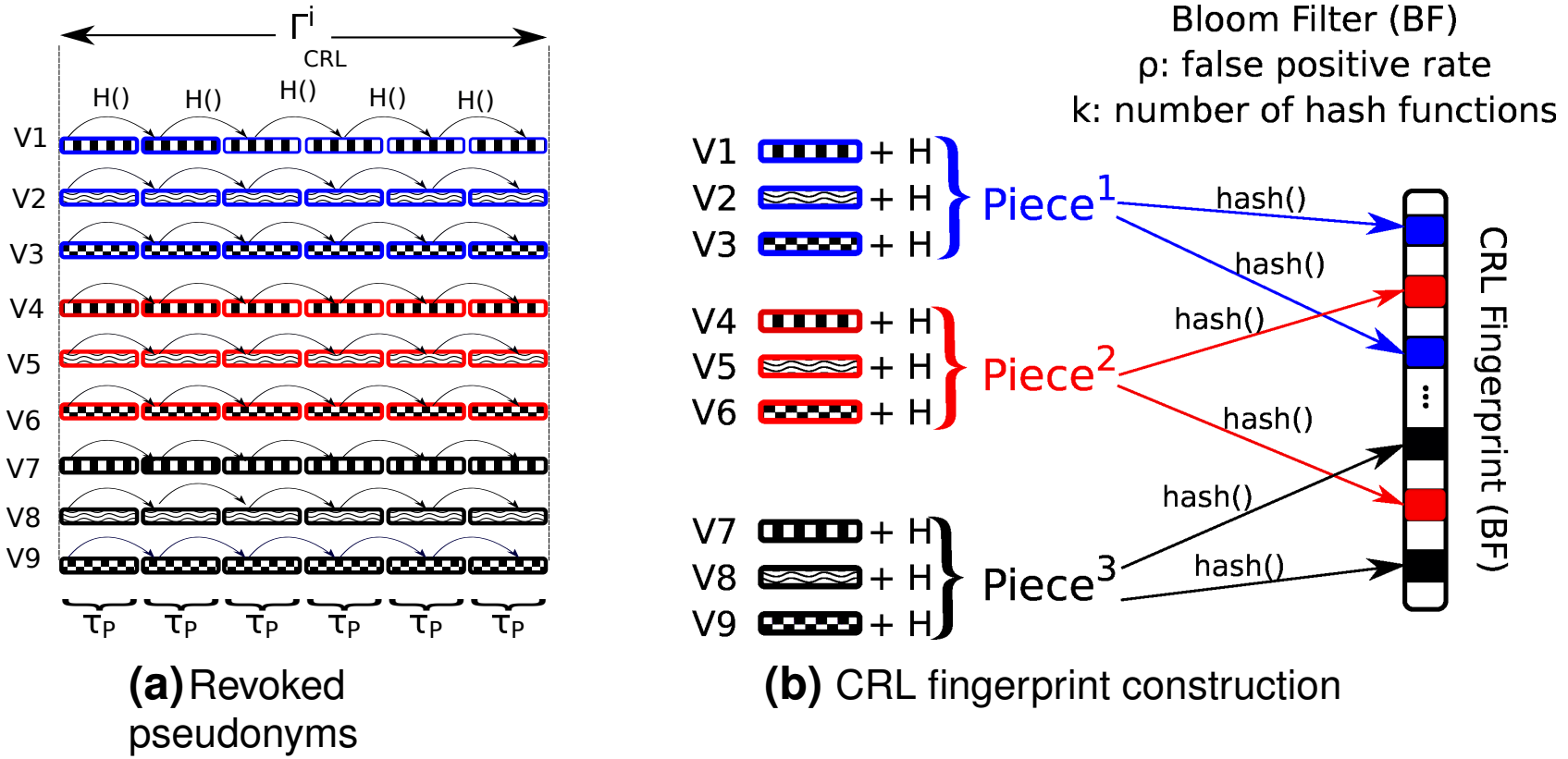


Figure: A vehicle-centric approach: each vehicle only subscribes for pieces of CRLs corresponding to its trip duration.

* *Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs*, ACM WiSec 2018

Vehicle-Centric CRL Distribution (cont'd)



(a) Revoked pseudonyms

(b) CRL fingerprint construction

Figure: CRL piece & fingerprint construction by the PCA.

CRL Fingerprint

- Signed, broadcast by Roadside Units (RSUs)
- Integrated in (a subset of) recently issued pseudonyms
- Notification about a new CRL-update (revocation event)

Quantitative Analysis

- OMNET++ & Veins framework using SUMO
- Cryptographic protocols and primitives (OpenSSL): ECDSA-256 and SHA-256 as per IEEE 1609.2 and ETSI standards
- V2X communication over IEEE 802.11p
- Placement of the RSUs: “highly-visited” intersections with non-overlapping radio ranges
- Comparison with the *baseline* scheme [8]: under the same assumptions and configuration with the same parameters
- Evaluation
  - Efficiency (latency)
  - Resilience (to pollution/DoS attacks)
  - Resource consumption (computation/communication)

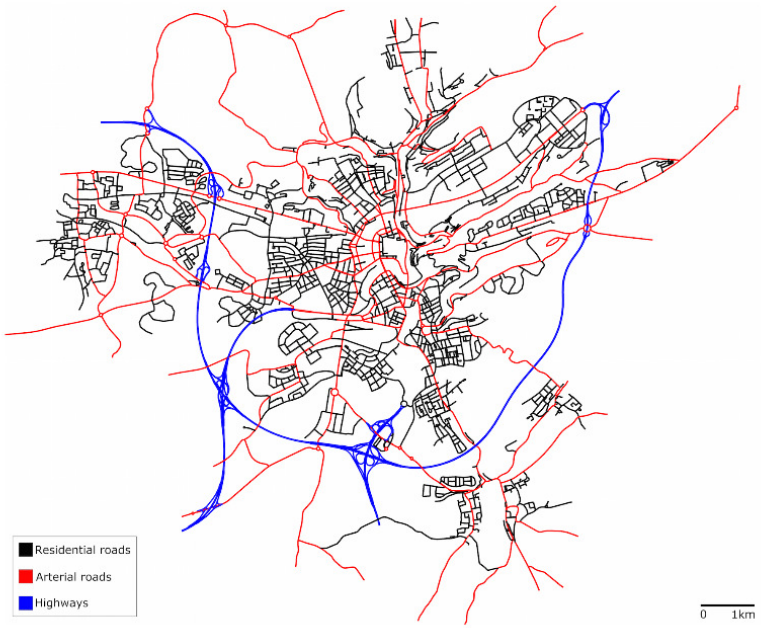
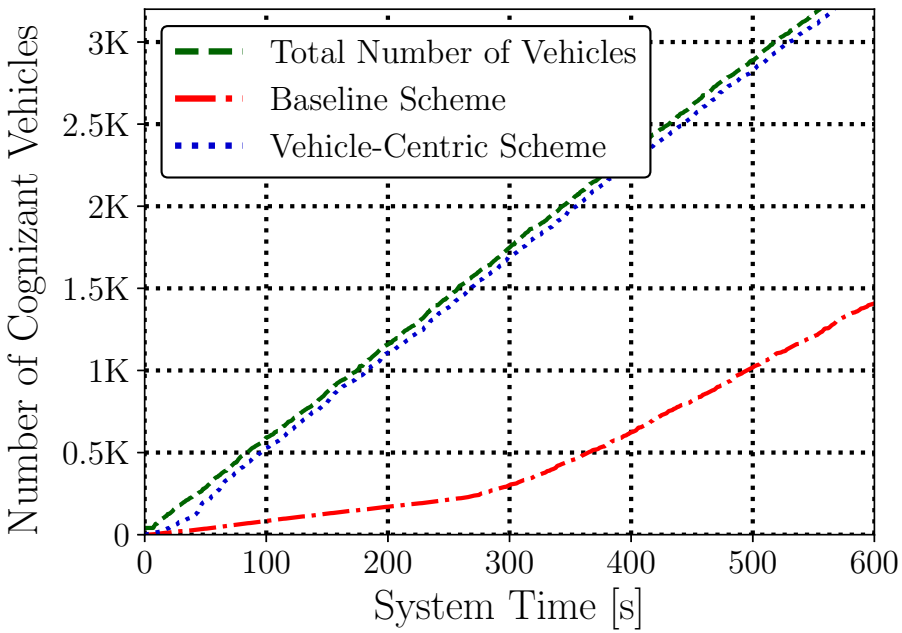
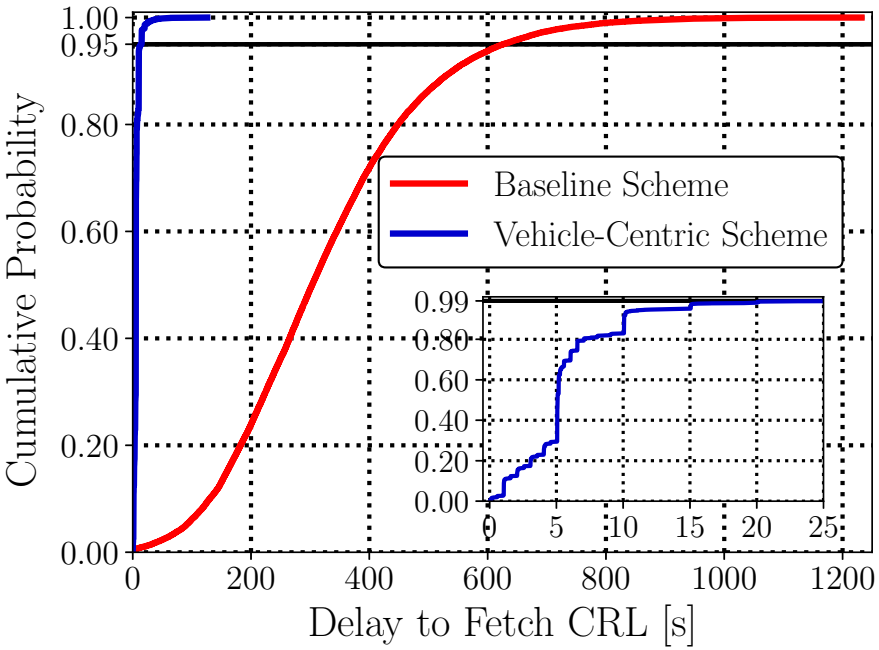


Figure: The LuST dataset, a full-day realistic mobility pattern in the city of Luxembourg (50KM x 50KM) [Codeca et al. (2015)].

Quantitative Analysis (cont'd)



(a) 7:00-7:10 am ($\mathbb{B}$ =25 KB/s)



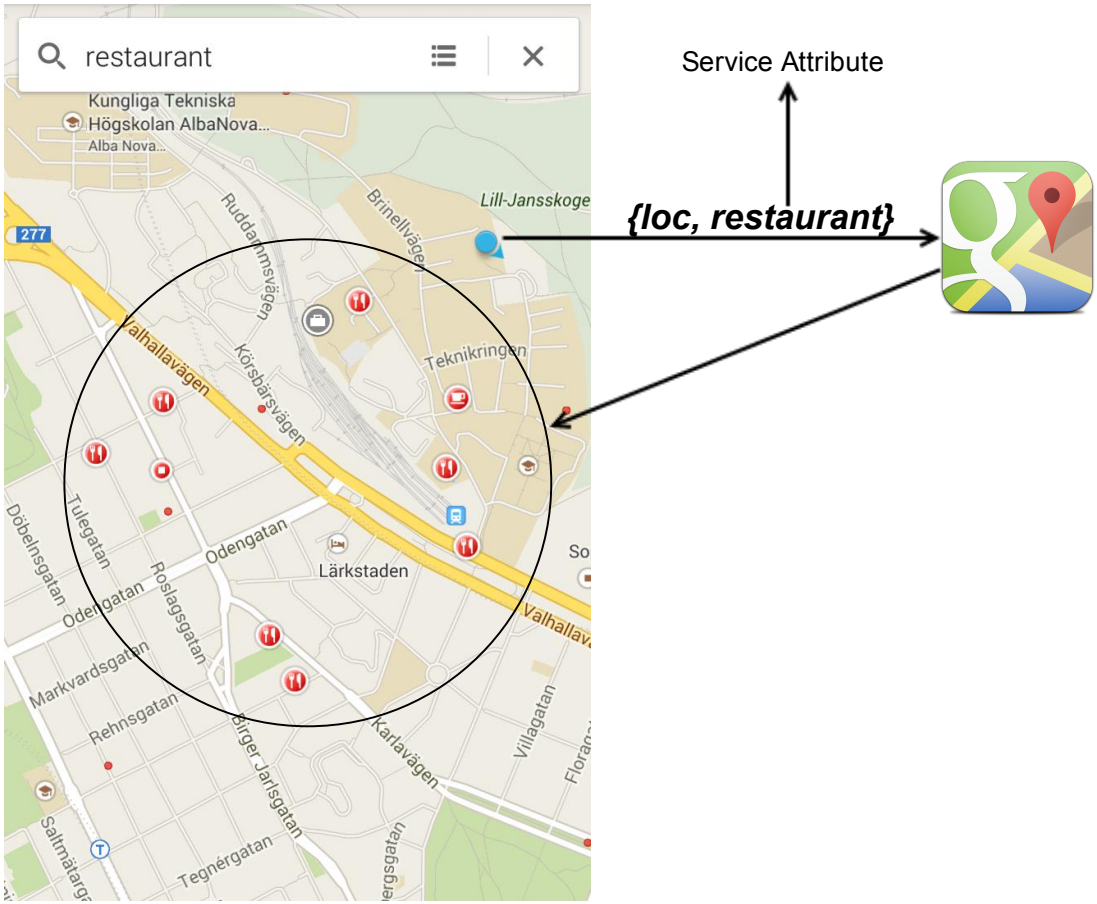
(b) 7-9 am, 5-7 pm ($\mathbb{B}$ =25 KB/s)

Figure: End-to-end delay to fetch CRLs ($\mathbb{R}$ = 1%, τ_P = 60s).

Converging more than 40 times faster than the state-of-the-art

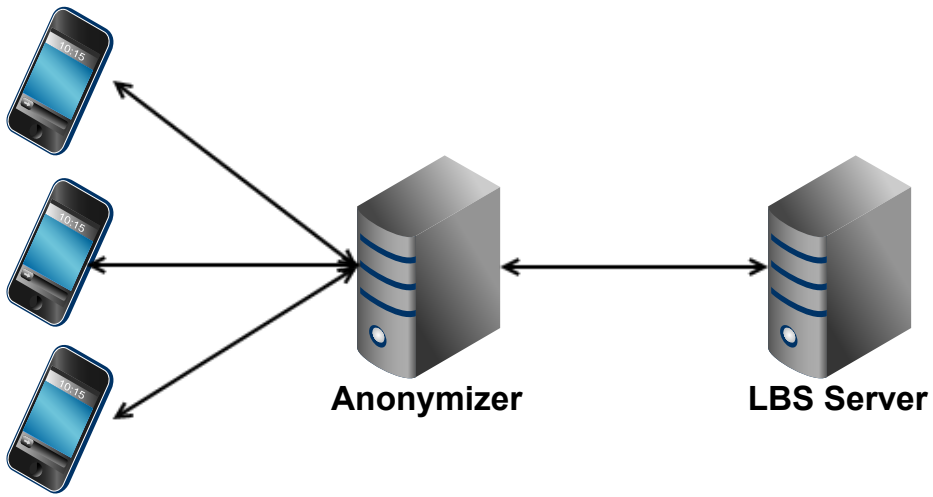
- Baseline scheme: $F_x(t = 626s) = 0.95$
- Vehicle-centric scheme: $F_x(t = 15s) = 0.95$

LBS Privacy



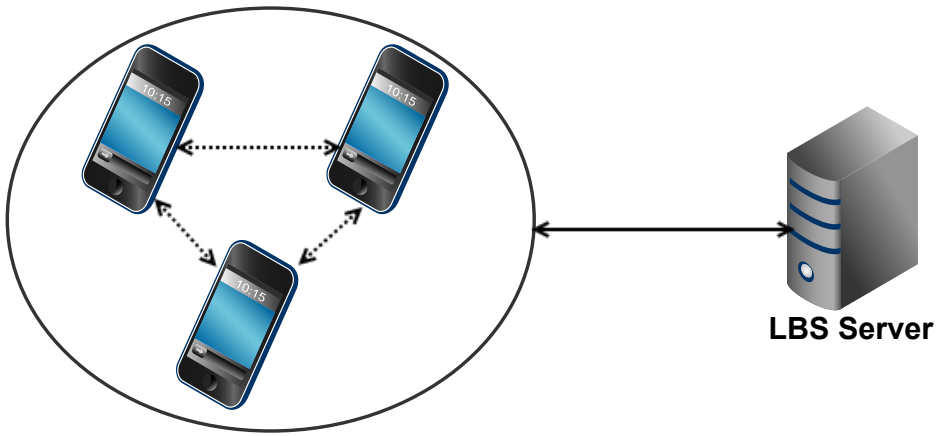
- **Adversary**: *honest-but-curious* LBS server

LBS Privacy (cont'd)



- Advantages: Transparency for clients, effectiveness
- Why do we trust the (possibly honest-but-curious) anonymizer?

Decentralized LBS Privacy*



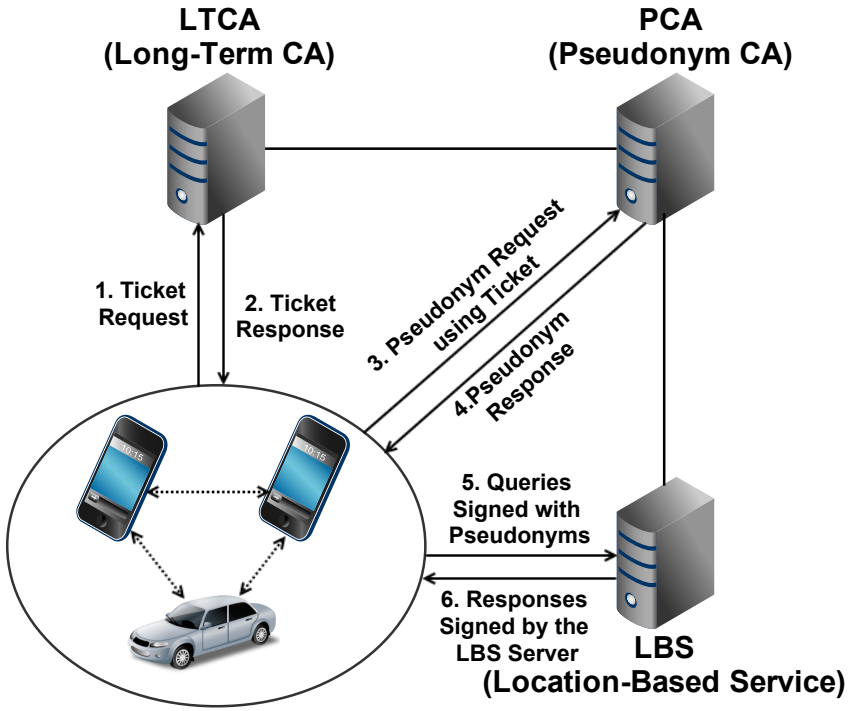
- No need for an anonymizer: reliance on peers
- Cache responses, contact the LBS server only when absolutely necessary

* *Hiding in the Mobile Crowd: Location Privacy through Collaboration*, IEEE TDSC, 2014

Decentralized LBS Privacy **and Security**

- *Misbehaving peers?*
  - *Active*: Masquerading, tampering, DoS...
  - *Passive*: Eavesdrop queries and responses
- Accountability
- Privacy protection

Decentralized LBS Privacy **and Security** (cont'd)*



- Leverage a VPKI-like solution for pseudonymous authentication of peer interactions
  - Peer functionality resilient to misbehavior
- Run this scheme in parallel to the LBS, without shifting trust; motivation for privacy-cautious users

* *Resilient Privacy Protection for Location-Based Services Through Decentralization*, ACM WiSec 2017

Decentralized LBS Privacy and Security (cont'd)

- The PCA randomly assigns a small fraction of system nodes as serving nodes
- The serving period can be coincide with pseudonym request interval
- Serving nodes proactive request Point of Interest (PoI) data for the whole region and announce their presence and available data
- Any interested node listens to beacons and requests PoI data
- Can request responses from $N > 1$ serving nodes for cross-checking

Security and Privacy Analysis - Quantitative

$$ExpoDeg(Id_{LTC}, C) = \sum_{Id_i \in ID(Id_{LTC}, C)} \frac{T(Id_i)}{T(Id_{LTC})} * \frac{R_H(Id_i)}{R(Id_{LTC})} \quad (1)$$

- $ID(Id_{LTC}, C)$: set of identities corresponding to Id_{LTC} exposed to honest-but-curious (possibly colluding) entities
- $T(Id)$: trip duration of a node under identity Id
- $R(Id)$: number of regions the node visits as Id
- $R_H(Id)$: number of visited regions exposed
- $ExpoDeg$: accuracy of reconstructed node trajectories based on recorded node queries, taking into account pseudonymous authentication

Security and Privacy Analysis - Quantitative (cont'd)

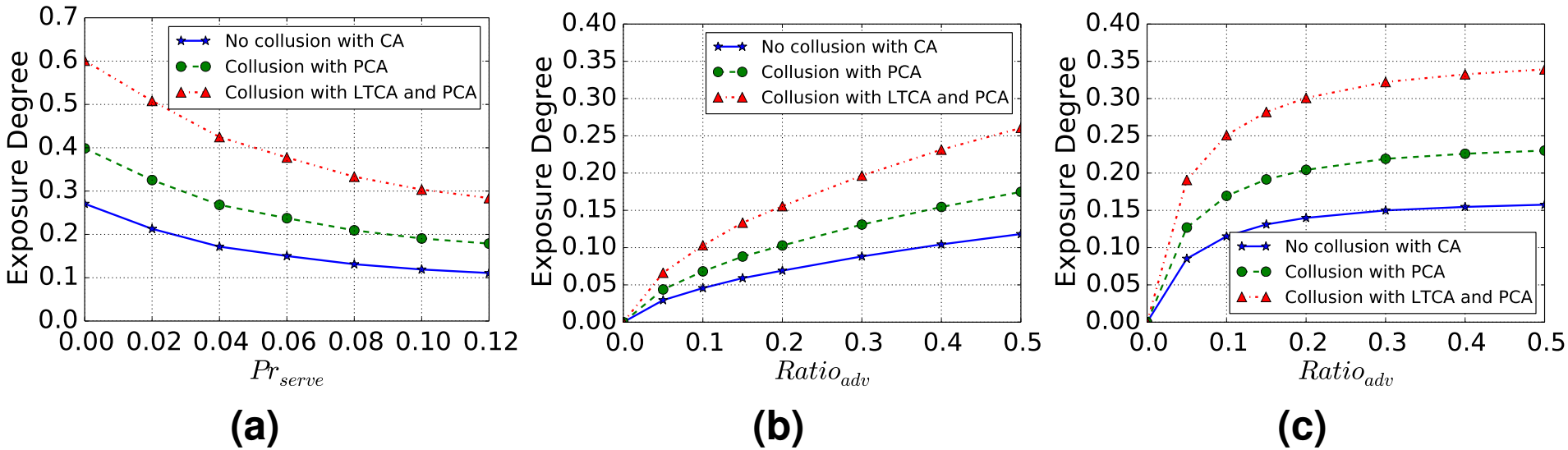


Figure: (a) Exposure degree to the LBS server as a function of Pr_{serve}. Exposure degree to colluding passive adversaries as a function of $Ratio_{adv}$ (b) with and (c) without encryption for P2P communication.

Security and Privacy Analysis - Quantitative (cont'd)

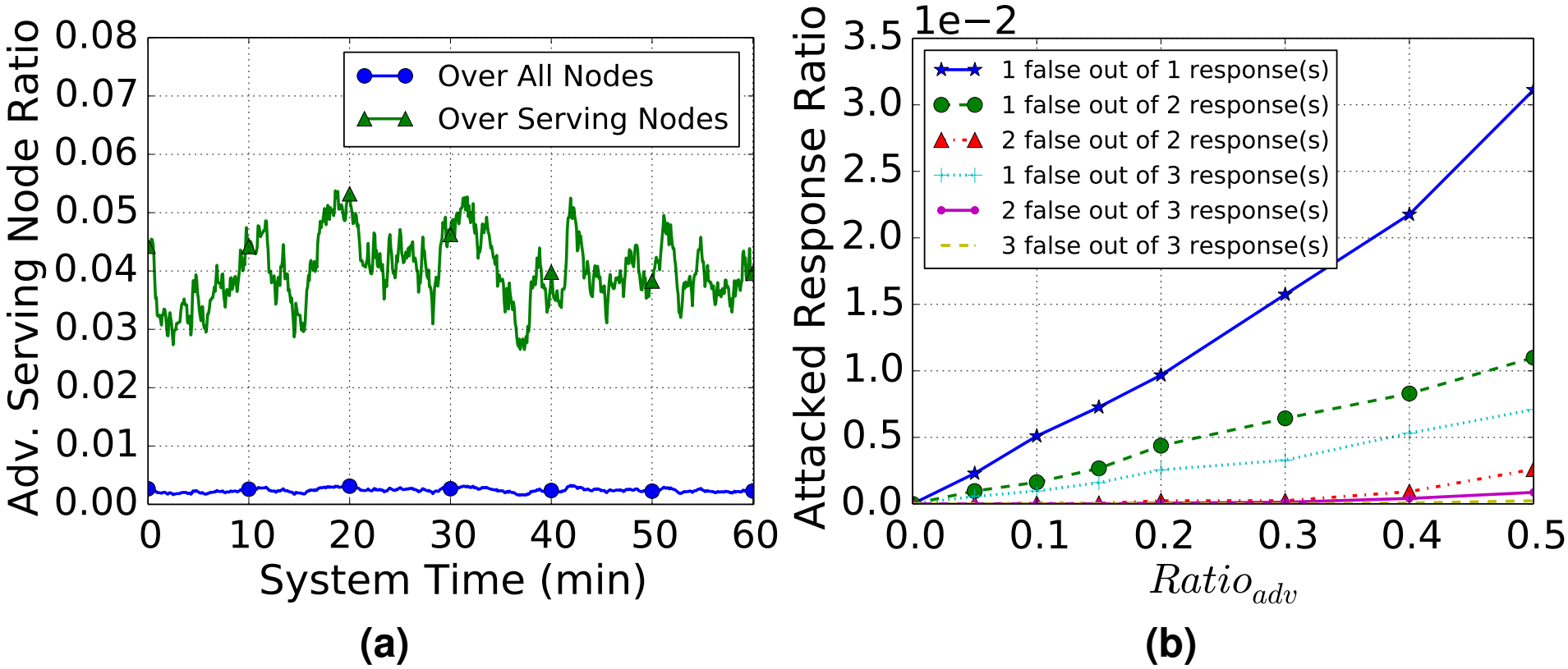
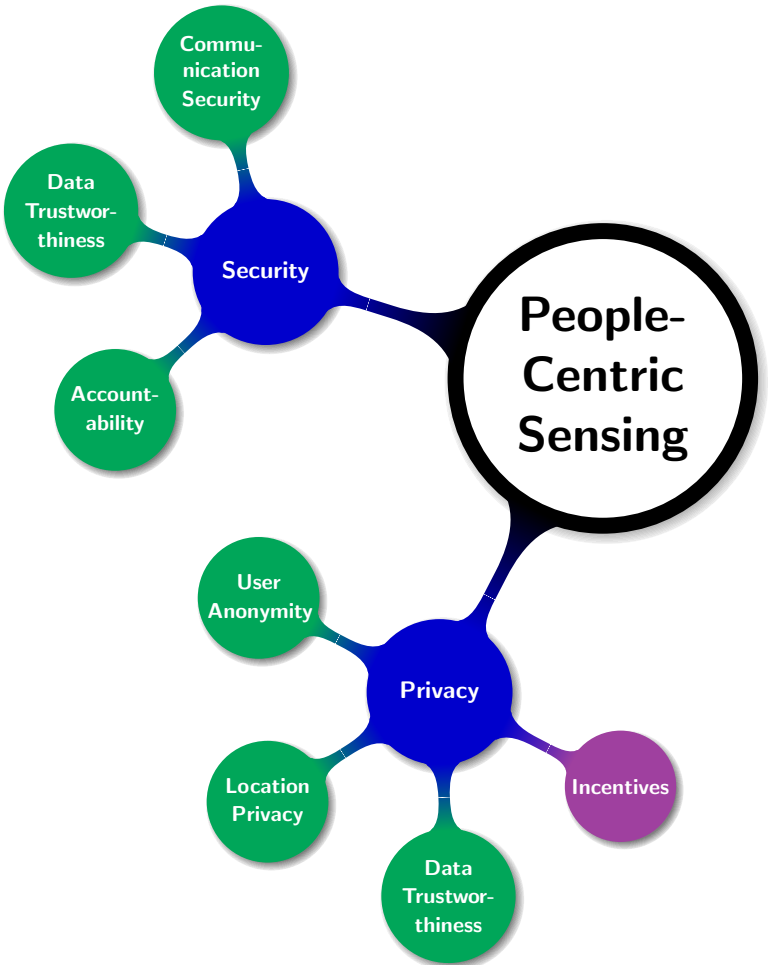


Figure: (a) Malicious serving node ratio during simulation (1 p.m. - 2 p.m.) with default settings. (b) Attacked LBS query ratio as a function of $Ratio_{adv}$.

Urban Sensing Systems

Illustration: complexitys.com

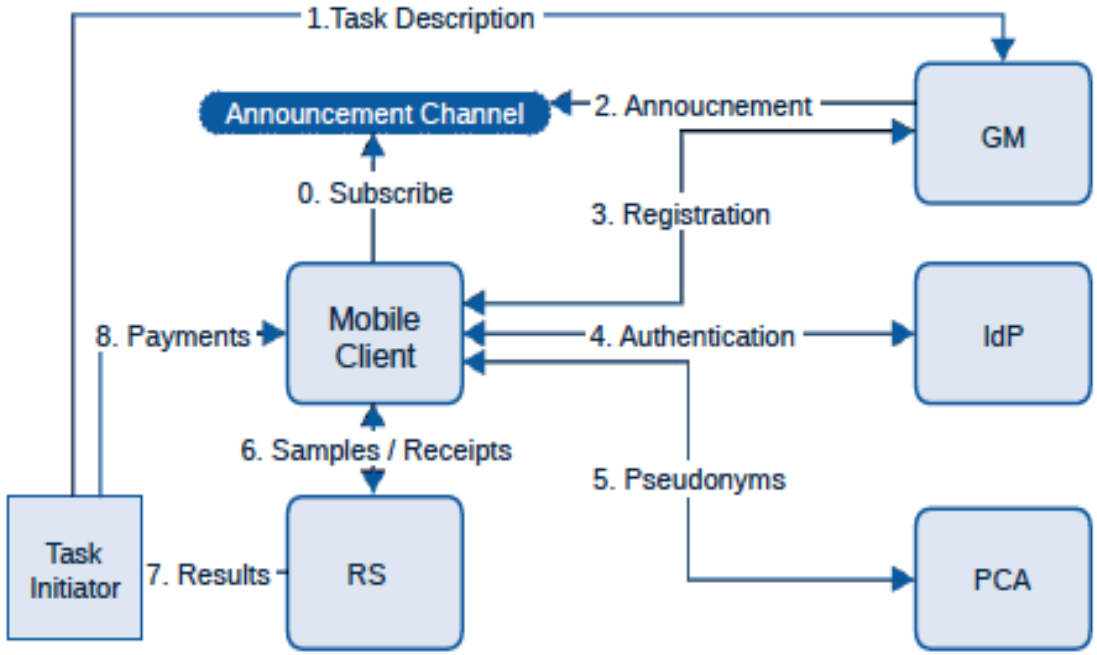
Security & Privacy Requirements*



- Protect the users from the system (privacy)
  - ✓ Anonymity (conditional)
  - ✓ Unlinkability
- Protect the system from the users (security)
  - ✓ Authentication & Authorization
  - ✓ Accountability
  - ✓ Misbehavior detection
- ✓ User incentives

* *Trustworthy People-Centric Sensing: Privacy, Security and User Incentives Road-Map*, IEEE/IFIP MedHocNet 2014

SPPEAR Overview*



Seperation of Duty

* *SPPEAR: security & privacy-preserving architecture for participatory-sensing applications*, ACM WiSec 2014

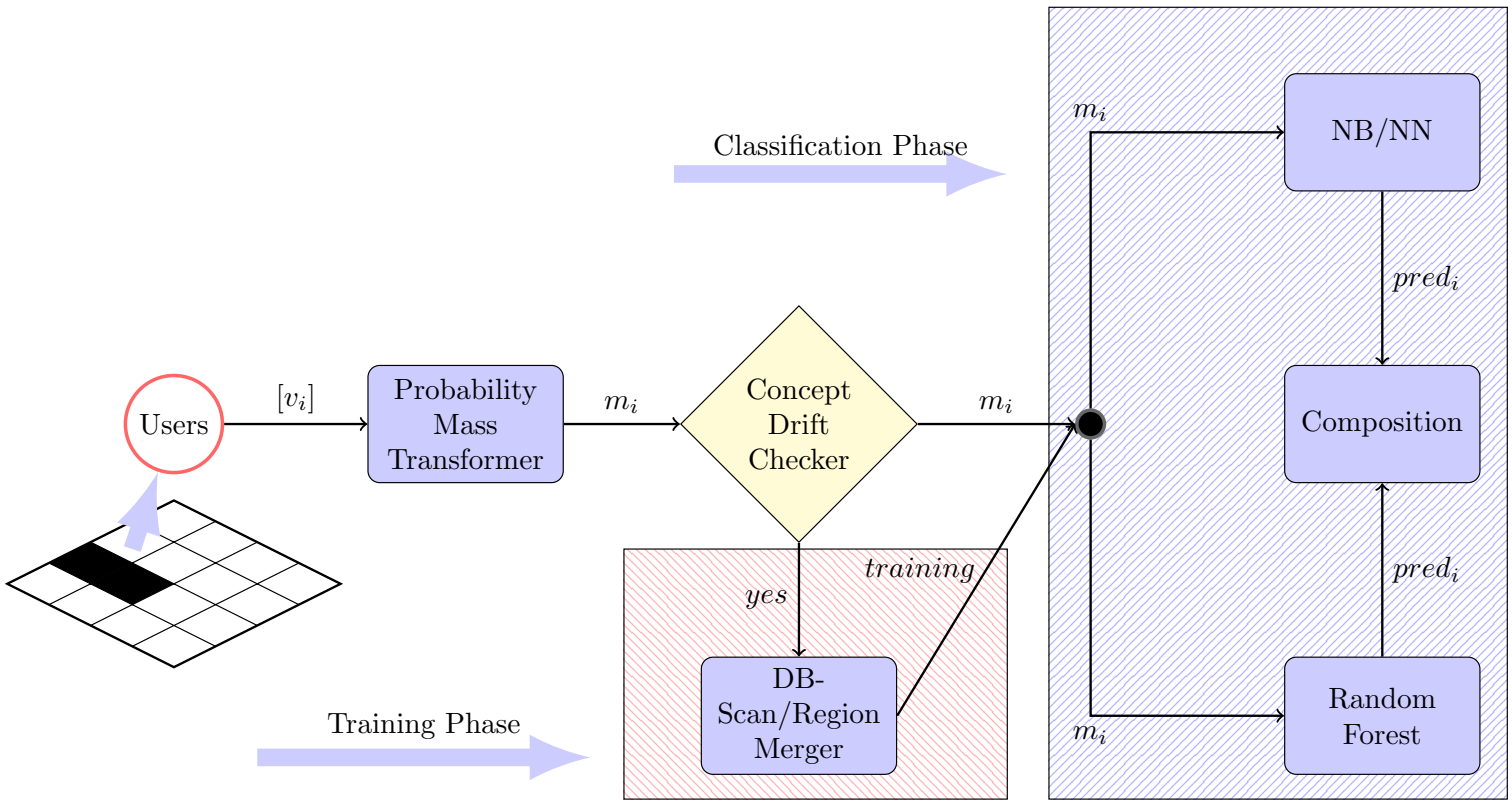
Analysis

- ✓ Confidentiality, integrity (TLS and digital signatures)
- ✓ Access control, authorization (GM = PDP and IdP = PEP)
- ✓ Sybil-proof (non-overlapping pseudonyms)
- ✓ GM does not know the user task(s) (OT for token retrieval)
- ✓ Unlinkable and unobservable interactions (TOR)
- ✓ Accountability, exculpability (Revocation protocol + interactive mode for BBS)

Analysis (cont'd)

- ProVerif protocol checker
- Model with π-Calculus
- Entities (infrastructure components and users) described as processes
- Protocol modelled as a parallel composition of multiple copies of the processes
- Basic cryptographic primitives modelled as symbolic operations over bit-strings representing messages, encoded with *constructors* and *destructors*
- Dolev-Yao adversaries (eavesdrop, modify, craft and inject messages based on the keys they possess)
- We can prove **secrecy** (i.e., values are secret) and **strong-secrecy** (the adversary cannot infer changes over secret values) properties

Secure and Privacy-preserving Participatory Sensing*



* *Security, Privacy and Incentive Provision for Mobile Crowd Sensing Systems*, IEEE IoT Journal, 2016

Bibliography I

[1] "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," Mar. 2016.

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

[3] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos, "VeSPA: Vehicular Security and Privacy-preserving Architecture," in *ACM HotWiSec*, Budapest, Hungary, Apr. 2013.

[4] S. Gisdakis, M. Laganà, T. Giannetsos, and P. Papadimitratos, "SEROSA: SERvice Oriented Security Architecture for Vehicular Communications," Boston, MA, USA, Dec. 2013, pp. 111–118.

[5] D. Förster, F. Kargl, and H. Löhr, "PUCA: A Pseudonym Scheme with User-Controlled Anonymity for Vehicular Ad-Hoc Networks," in *IEEE VNC*, Paderborn, Germany, Dec. 2014.

[6] "PRESERVE Project," www.preserve-project.eu/, Jun. 2015.

[7] "PKI Memo C2C-CC," http://www.car-2-car.org/, Feb. 2011.

[8] J.-J. Haas, Y.-C. Hu, and K.-P. Laberteaux, "Efficient Certificate Revocation List Organization and Distribution," *IEEE JSAC*, vol. 29, no. 3, pp. 595–604, 2011.

Other publications

- S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, and **P. P.**, *Secure and Privacy-Preserving Smartphone-based Traffic Information Systems,* IEEE Trans. on ITS, Vol. 16, No. 3, pp. 1428-1436, June 2015
- M. Khodaei, H. Jin, and **P. P.**, *Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure,* IEEE VNC, Paderborn, Germany, Dec. 2014
- H Jin and **P. P.** *Proactive Certificate Validation for VANETs*, IEEE Vehicular Networking Conference (IEEE VNC), Columbus, OH, USA, December 2016
- M. Khodaei and **P. P.**, *Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems,* ACM MobiHoc Workshop on Internet of Vehicles and Vehicles of Internet (ACM MobiHoc IoV-VoI), Paderborn, Germany, July 2016
- H. Jin and **P. P.**, *Scaling VANET Security Through Cooperative Message Verification,* IEEE Vehicular Networks Conference (IEEE VNC), Kyoto, Japan, December 2015
- K. Zhang, R. A. Tuhin, and **P. P.**, *Detection and Exclusion RAIM Algorithm against Spoofing/Replaying Attacks,* International Symposium on GNSS, Kyoto, Japan, November 2015
- K. Zhang and **P. P.**, *GNSS Receiver Tracking Performance Analysis under Distance-Decreasing Attacks,* International Conference on Localization and GNSS (ICL-GNSS), Gothenburg, Sweden, June 2015
- H. Jin, M. Khodaei, and **P. P.**, *Security and Privacy for Vehicular Social Networks,* Vehicular Social Networks, A. M. Vegni, V. Loscri, A. V. Vasilakos, Eds., CRC Taylor & Francis Group, 2016
- P. Ardelean and **P. P.**, *Secure and Privacy-Enhancing Vehicular Communication,* IEEE Symposium on Wireless Vehicular Communications (IEEE WiVec), Calgary, AL, Canada, September 2008

Other publications (cont'd)

- **P. P.** and A. Jovanovic, *Method to secure GNSS based locations in a device having GNSS receiver,* US Patent 8,159,391, April 2012
- M. Khodaei and **P. P.**, *The Key To Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,* IEEE Vehicular Technology Magazine, Vol. 10, No. 4, pp. 63-69, December 2015
- S. Gisdakis, M. Lagana, T. Giannetsos, and **P. P.**, *SEROSA: Service Oriented Security Architecture for Vehicular Communications,* IEEE VNC, Boston, MA, USA, Dec. 2013
- N. Alexiou, S. Gisdakis, M. Laganà, and **P. P.**, *Towards a Secure and Privacy-preserving Multi-service Vehicular Architecture,* IEEE D-SPAN, Madrid, June 2013
- N. Alexiou, M. Laganà, S. Gisdakis, and **P. P.**, *VeSPA: Vehicular Security and Privacy-preserving Architecture,* ACM HotWiSec, Budapest, April 2013
- V. Manolopoulos, S. Tao, A. Rusu, and **P. P.**, *HotMobile Demo: Smartphone-based Traffic Information System for Sustainable Cities,* ACM MC2R, vol. 16, no. 4, pp. 30-31, Oct. 2012
- M. Poturalski, **P. P.**, and J.-P. Hubaux, *Formal Analysis of Secure Neighbor Discovery in Wireless Networks,* IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), Vol. 10, No. 6, pp. 355 - 367, Nov.-Dec. 2013
- M. Fiore, C. Casetti, C.-F. Chiasserini, and **P. P.**, *Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks,* IEEE Transactions on Mobile Computing (IEEE TMC), Vol. 12, No. 2, pp. 289?303, February 2013
- M. Poturalski, M. Flury, **P. P.**, J.-P. Hubaux, and J.-Y. Le Boudec, *On Secure and Precise IR-UWB Ranging,* IEEE Transactions on Wireless Communications (IEEE TWC), Vol.11, No.3, pp. 1087?1099, March 2012
- G. Calandriello, **P. P.**, A. Lioy, and J.-P. Hubaux, *On the Performance of Secure Vehicular Communication Systems,* IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), Vol. 8, No. 6, pp. 898?912, Nov.-Dec. 2011
- **P. P.**, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, *Secure Vehicular Communication Systems: Design and Architecture,* IEEE Communications Magazine, Vol. 46, No. 11, pp. 100-109, November 2008

SECMACE: Scalable and Robust Identity and Credential Infrastructure in Vehicular Communication

IEEE Transactions on Intelligent Transportation Systems (IEEE ITS), vol. 19, no. 5, May 2018

Mohammad Khodaei, Hongyu Jin, and **Panos Papadimitratos**

Networked Systems Security Group

www.ee.kth.se/nss