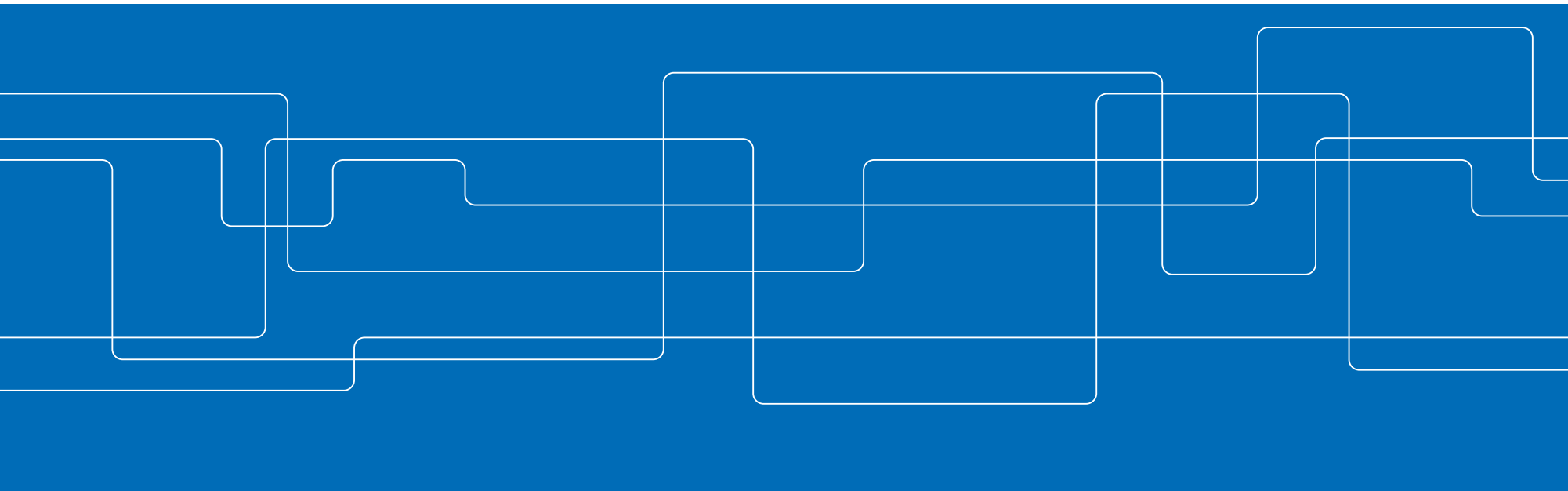
KTH ROYAL INSTITUTE
OF TECHNOLOGY

The Key to Intelligent Transportation Systems: Identity and Credential Management for Secure and Privacy-Preserving Vehicular Communication Systems

Mohammad Khodaei
Networked Systems Security Group

June 15, 2020



Outline

Vehicular Communication (VC) Systems

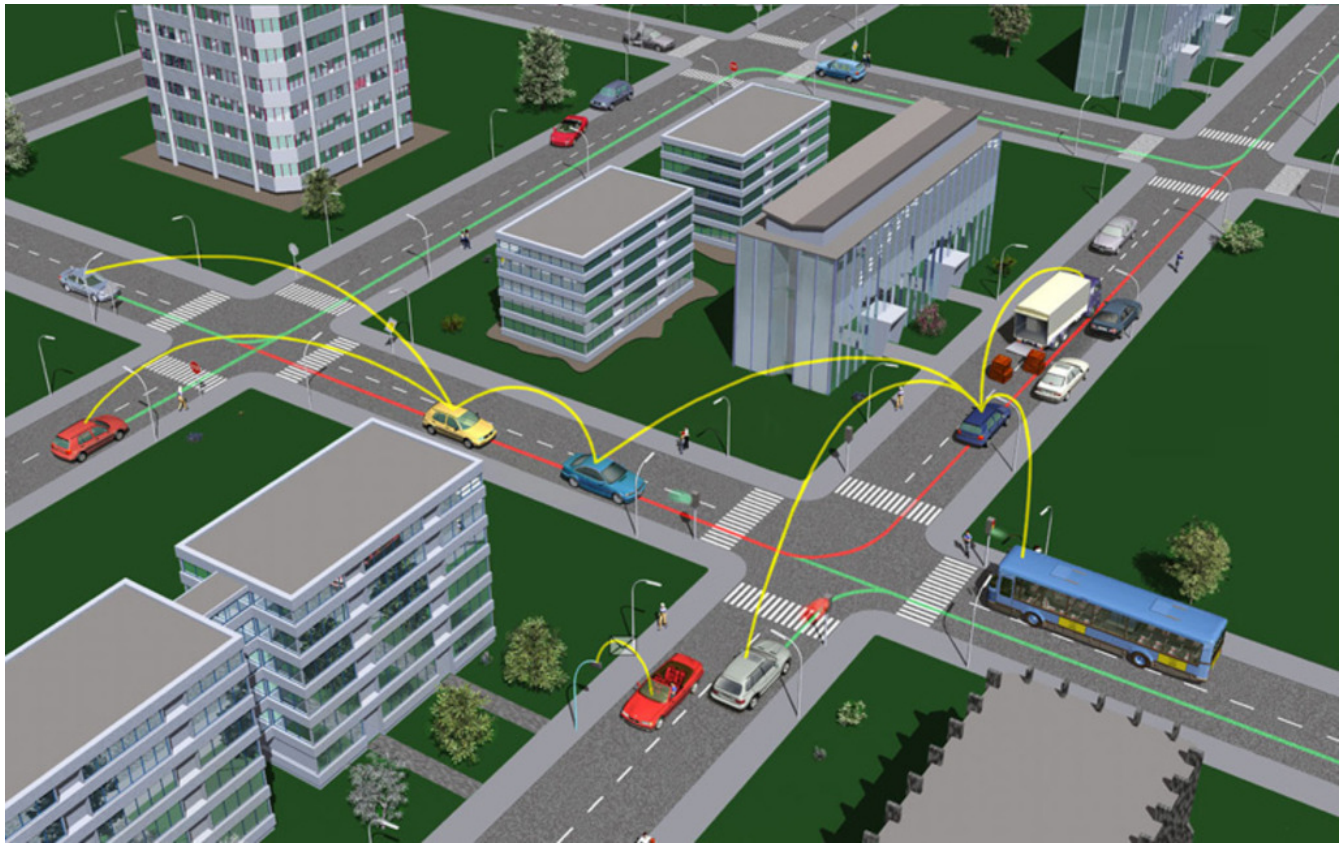
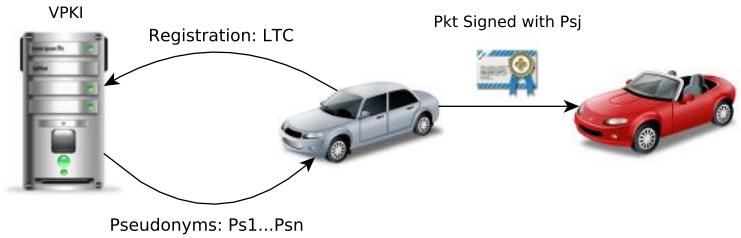


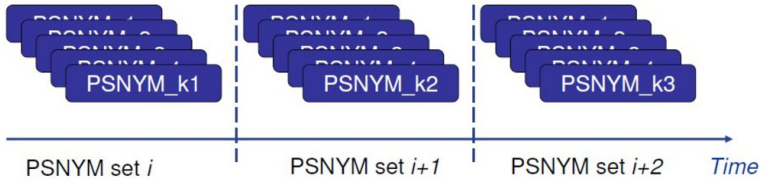
Figure: Photo Courtesy of the Car2Car Communication Consortium (C2C-CC)

Security and Privacy for VC Systems

Basic Requirements

- Message authentication & integrity
- Message non-repudiation
- Authorization & access control
- Entity authentication
- Accountability
- Anonymity (conditional)
- Unlinkability (long-term)

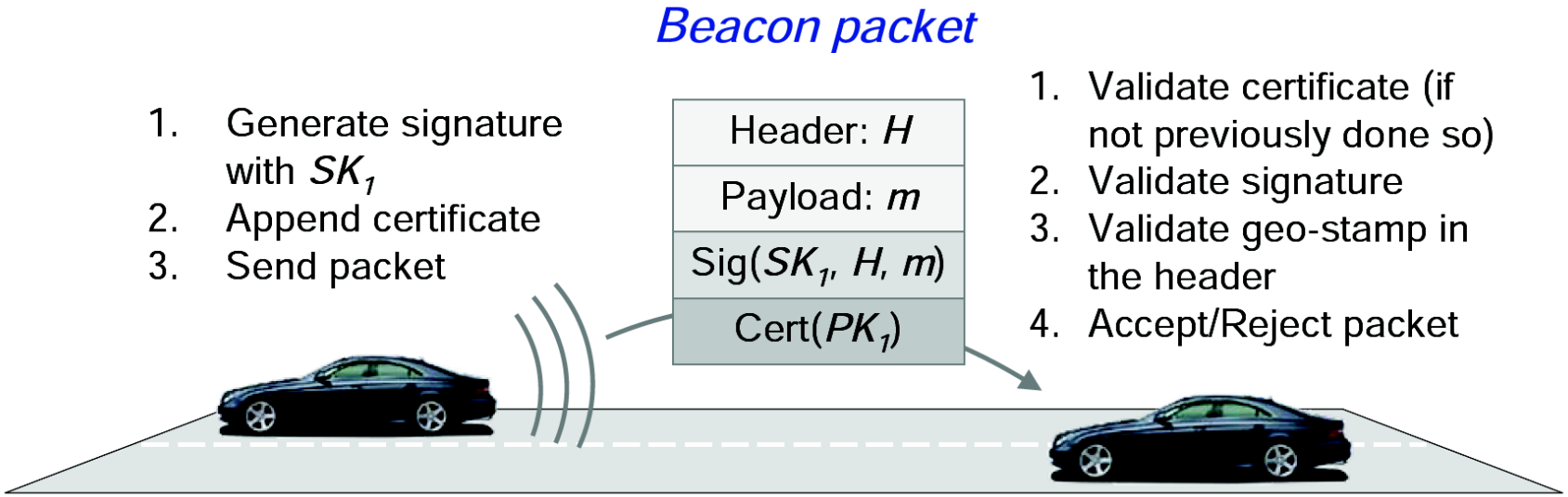




Vehicular Public-Key Infrastructure (VPKI)

- Pseudonymous authentication
- Trusted Third Party (TTP):
  - Certification Authority (CA)
  - Issues credentials & binds users to their pseudonyms

Security and Privacy for VC Systems (cont'd)



- Sign packets with the private key, corresponding to the current valid pseudonym
- Verify packets with the valid pseudonym
- Cryptographic operations in a Hardware Security Module (HSM)

Challenges and Motivation
Traditional PKI vs. Vehicular PKI

- Dimensions (5 orders of magnitude more credentials)
- Complexity and constraints
  - Balancing act: security, privacy, and efficiency
    - *Honest-but-curious* VPKI entities
    - Performance constraints: safety- and time-critical operations (rates of 10 safety beacons per second)
  - Multiple and diverse entities, global deployment, long-lived entities
  - Cost-driven platform resource constraints
- Mechanics of revocation
  - Highly dynamic environment
  - Short-lived pseudonyms, multiple per entity
  - Need for efficient and timely distribution of Certificate Revocation Lists (CRLs)

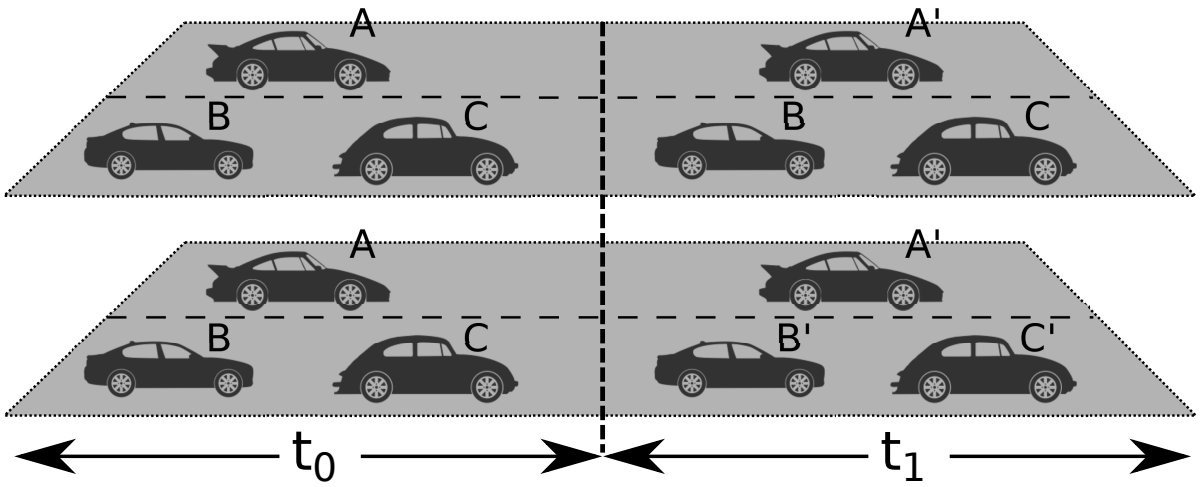
Challenges and Motivation (cont'd)

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

Challenges and Motivation (cont'd)

Attacks on location privacy (traceability): Openness of wireless communication and dissemination of basic safety messages in plaintext

- *Syntactic linking:* "joining the dots" between two Cooperative Awareness Messages (CAMs) by looking at the pseudo-identifier attributes, i.e., time of changing pseudonyms.
- *Semantic linking:* constructing a trajectory through a consistent series of (position, velocity, etc.) pairs.



Thesis Contribution

- Identity and Credential Management
  - Paper A (ACM HotWiSec'13)
  - Paper B (IEEE VNC'14)
  - Paper C (IEEE VT-Mag'15)
  - Paper D (ACM IoV-VoI'16)
  - Paper E (IEEE VNC'17)
  - Paper F (IEEE TITS'18)
  - Paper H (ACM WiSec'19)
- Certificate Revocation List Distribution
  - Paper G (ACM WiSec'18)
  - Paper I (IEEE TMC'20)
- Location Privacy Protection
  - Paper J (submitted to IEEE IoT Journal)

Outline

Secure VC System

- Root Certification Authority (RCA)
- Long Term CA (LTCA)
- Pseudonym CA (PCA)
- Resolution Authority (RA)
- Lightweight Directory Access Protocol (LDAP)
- Roadside Unit (RSU)
- Trust established with RCA, or through cross certification

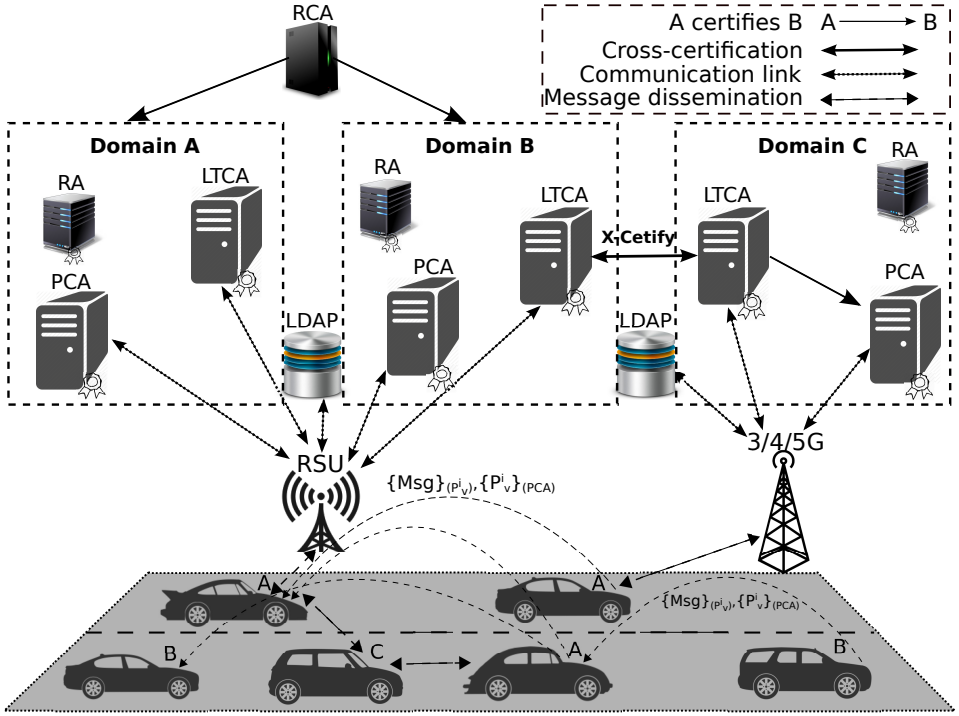


Figure: VPKI Overview

Adversarial Model

- *Honest-but-curious* service providers, i.e., they can attempt to gain advantages towards its goal, e.g., profiling users
- In addition, malicious PCAs could try to:
  - issue multiple sets of (simultaneously valid) pseudonyms for a legitimate vehicle
  - issue a set of pseudonyms for a non-existing vehicle
  - fraudulently accuse different vehicles (users) during a pseudonym resolution process
- A deviant LTCA could attempt to:
  - map a different Long Term Certificate (LTC) during the resolution process
  - issue fake authorization tickets, to be used during pseudonym acquisition process

Adversarial Model (cont'd)

- Malicious (compromised) entities:
  - Internal adversaries, i.e., OBUs, could try to:
    - repeatedly request multiple simultaneously valid pseudonyms, thus misbehaving each as multiple registered legitimate-looking vehicles
    - degrade the operations of the system by mounting a clogging Denial of Service (DoS) attack against the VPKI servers
  - External adversaries, i.e., unauthorized entities, could try to:
    - harm the system operations by launching a DoS attack, thus degrading the availability of the system

Objectives

- Design, analyze, implement and evaluate the VPKI
  - Management of credentials: provisioning, revocation, resolution
  - Standard-compliant implementation
- Resilience to *honest-but-curious* and *malicious* VPKI entities
- Eradication of Sybil-based misbehavior (without degrading performance)
- Handling unexpected demanding loads while being cost-effective
- Scalability
- Efficient revocation and resolution

System Model

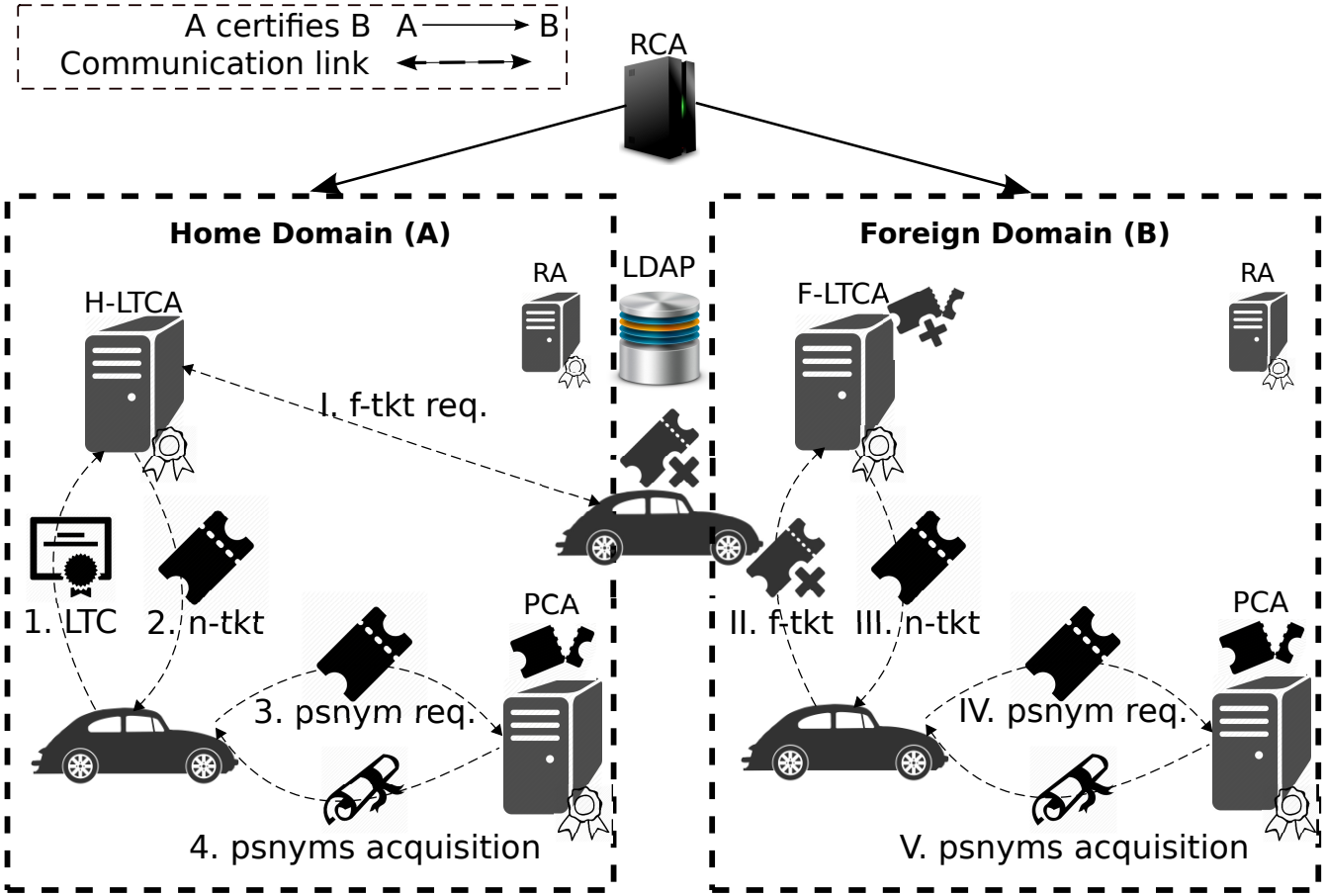
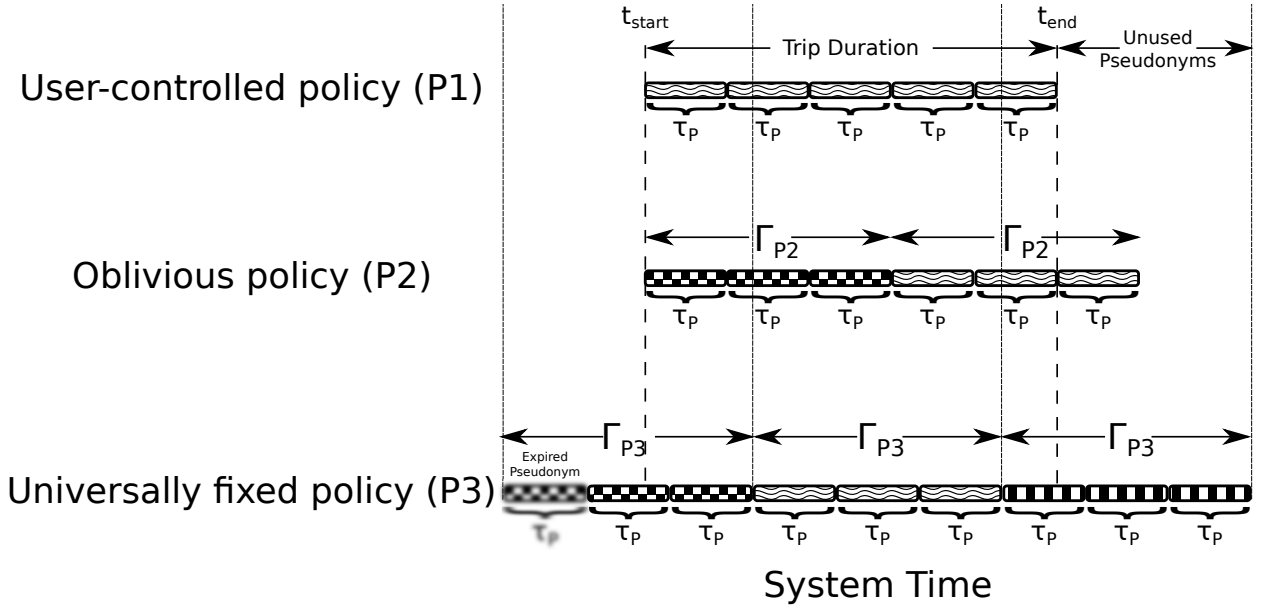


Figure: VPKI Architecture

Pseudonym Acquisition Policies



- P1 & P2: Requests could act as user *"fingerprints"*; the exact time of requests and all subsequent requests until the end of trip could be unique, or one of few
- P3: Requesting intervals fall within *"universally"* fixed interval Γ_{P3}, and pseudonym lifetimes are aligned with PCA clock

VPKI as a Service (VPKIaaS)

- Refactoring a state-of-the-art VPKI source code
- Fully automated all procedures of deployment
- Migrating VPKI to the cloud, e.g., Google Cloud Platform (GCP), Amazon Web Service (AWS), Microsoft Azure
- Enhancing its functionalities towards a highly-available, dynamically-scalable, and fault-tolerant design
- Providing health and load metric publishing feature to be used by an orchestration service to scale in/out accordingly
- Eradicating Sybil-based misbehavior when deploying such a system on the cloud with multiple replicas of a microservice without diminishing the efficiency of the pseudonym acquisition process

VPKI as a Service (VPKIaaS) Architecture

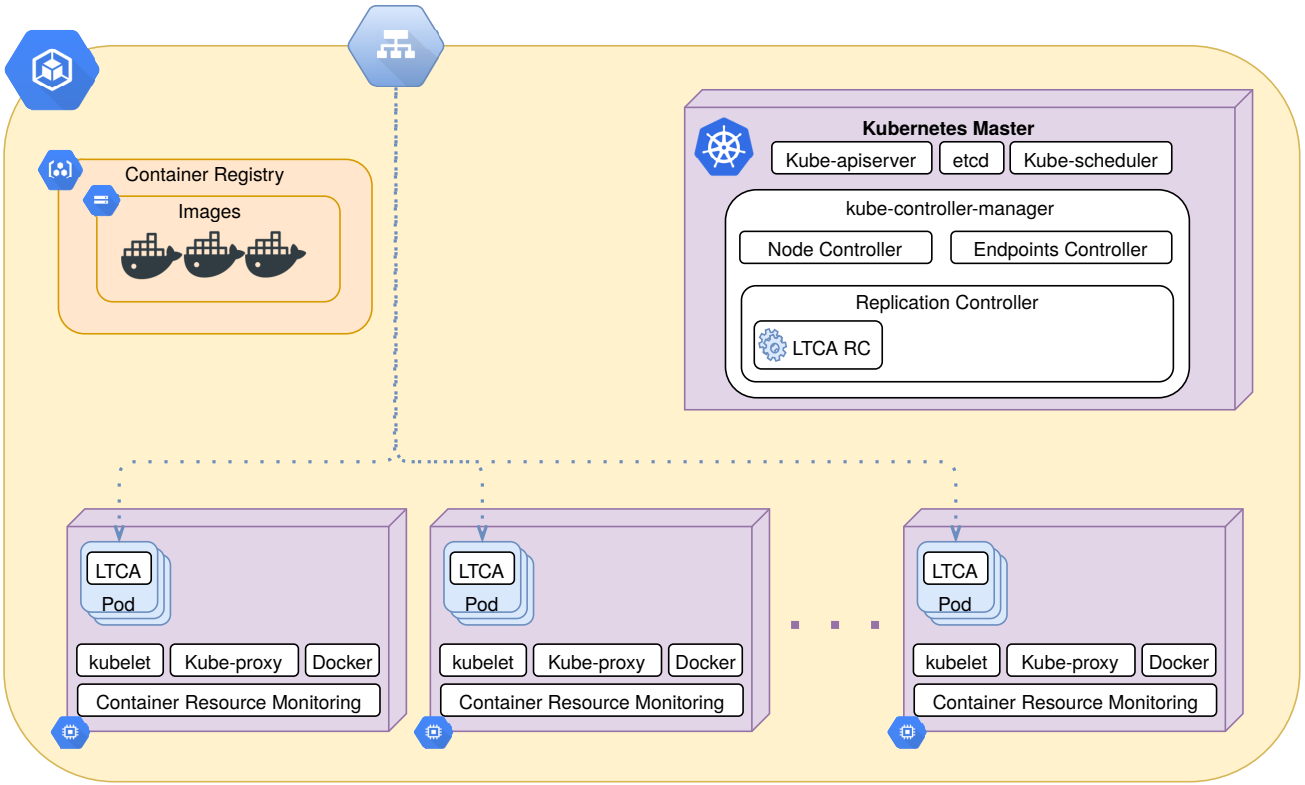


Figure: A High-level Overview of VPKIaaS Architecture on the Cloud

VPKI as a Service (VPKIaaS) Architecture

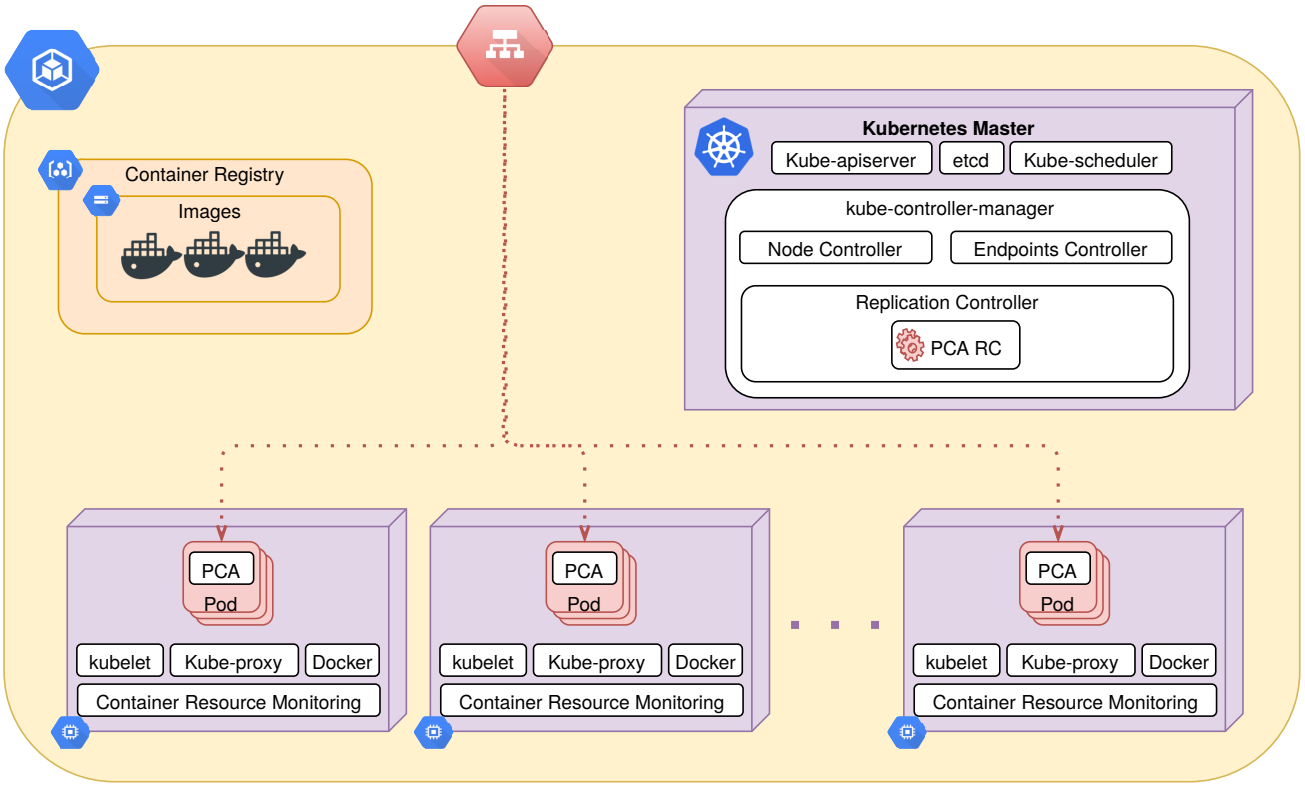


Figure: A High-level Overview of VPKIaaS Architecture on the Cloud

VPKI as a Service (VPKIaaS) Architecture

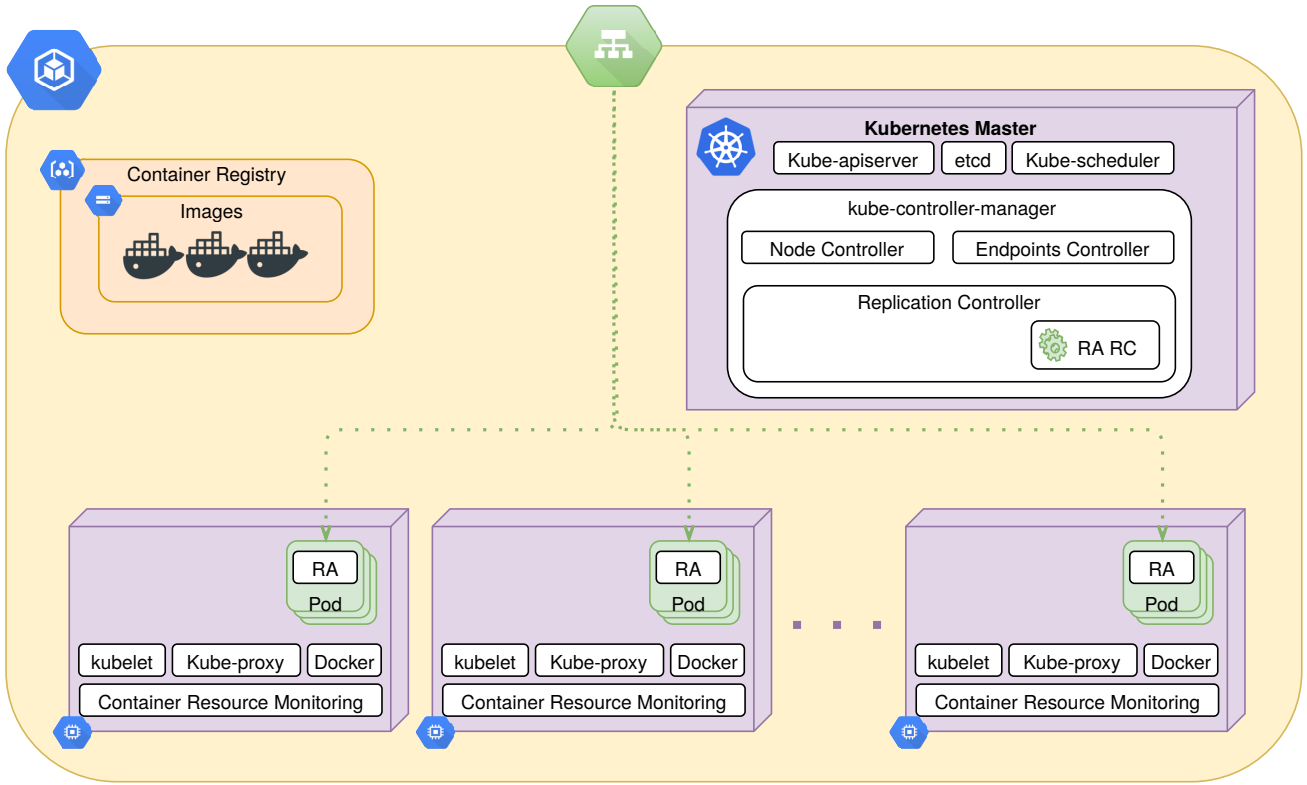


Figure: A High-level Overview of VPKIaaS Architecture on the Cloud

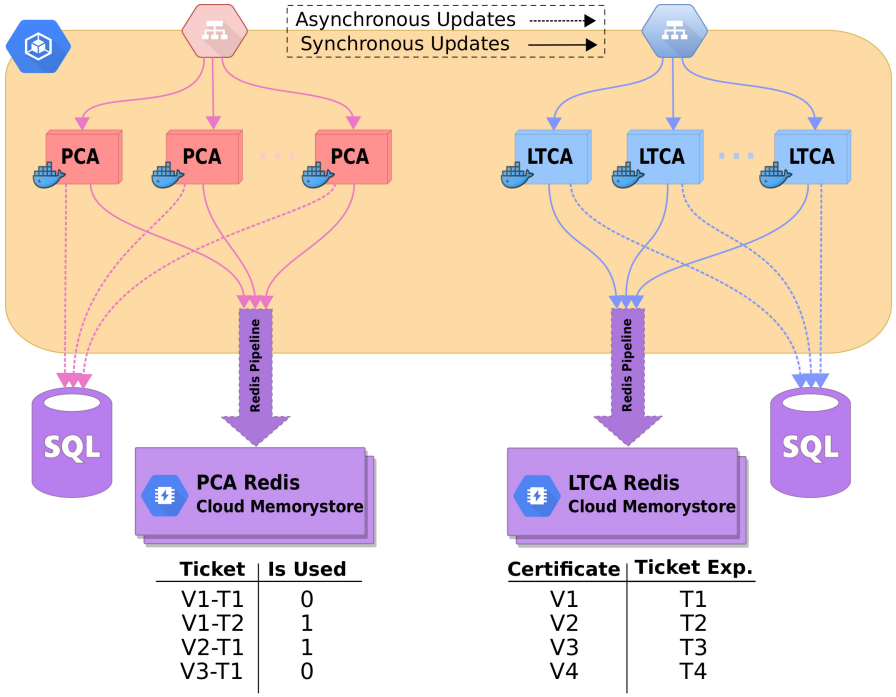
VPKIaaS Memorystore with Redis and MySQL

LTCA Sybil Attack Mitigation:

- Checking if a ticket was issued to the requester during that period
- Storing the serial number of the vehicle's LTC (as the key) and the expiration time of its current ticket (as the value) on the Redis database
- Invoking ticket issuance procedure

PCA Sybil Attack Mitigation:

- Checking if pseudonyms were issued to the requester of a given ticket
- Updating the Redis database with the value of true (i.e., used)
- Invoking pseudonym issuance procedure



VPKIaaS Memorystore with Redis & MySQL

Experimental Setup

- **VPKI testbed**
  - Implementation in C++, OpenSSL for cryptographic protocols & primitives, TLS and Elliptic Curve Digital Signature Algorithm (ECDSA)-256.
  - FastCGI to interface Apache web-server; we use XML-RPC & Google Protocol Buffers
- **VPKIaaS system**
  - Built and pushed Docker images for LTCA, PCA, RA, MySQL, and Locust, *an open source load testing tool*, to the Google Container Registry
  - Google Kubernetes Engine (GKE) v1.10.11
  - Configured a cluster of five Virtual Machines (VMs) (n1-highcpu-32), each with 32 vCPUs and 28.8GB of memory
- **VPKIaaS Memorystore**
  - Redis, in-memory key-value data store, and MySQL

Table: Experiment Parameters

Parameters	Config-1	Config-2
total number of vehicles	1000	100, 50,000
hatch rate	1	1, 100
interval between requests	1000-5000 ms	1000-5000 ms
pseudonyms per request	100, 200, 300, 400, 500	100, 200, 500
LTCA memory request	128 MiB	128 MiB
LTCA memory limit	256 MiB	256 MiB
LTCA CPU request	500 m	500 m
LTCA CPU limit	1000 m	1000 m
LTCA HPA	1-40; CPU 60%	1-40; CPU 60%
PCA memory request	128 MiB	128 MiB
PCA memory limit	256 MiB	256 MiB
PCA CPU request	700 m	700 m
PCA CPU limit	1000 m	1000 m
PCA HPA	1-120; CPU 60%	1-120; CPU 60%

- Config-1: normal vehicle arrival rate; every 1-5 sec, a new vehicle joins the system, requesting 100-500 pseudonyms
- Config-2: for a flash crowd scenario; beyond having vehicles joining the system based on Config-1, 100 new vehicles join the system every 1-5 sec, requesting 100-200

Experimental Setup (cont'd)

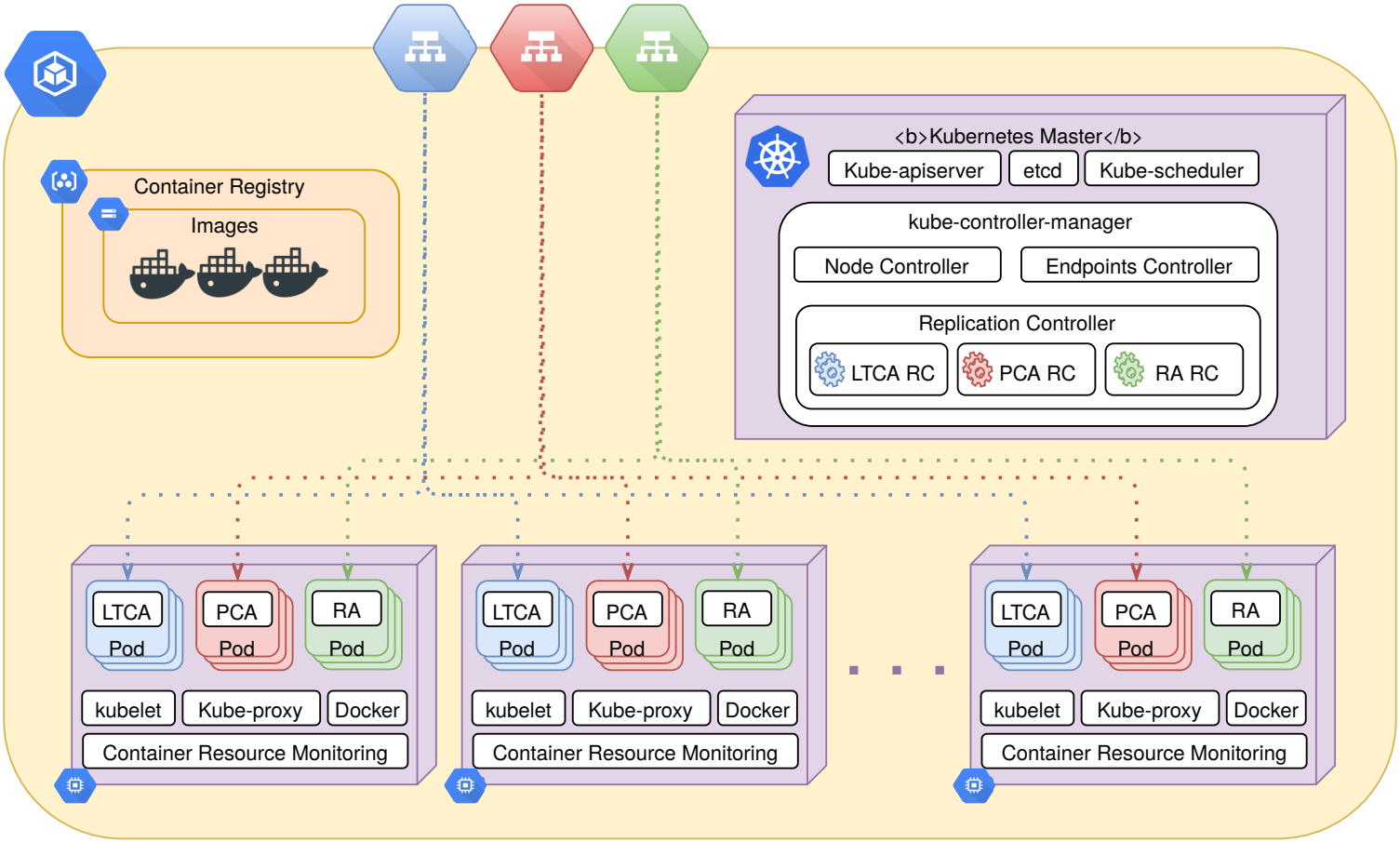
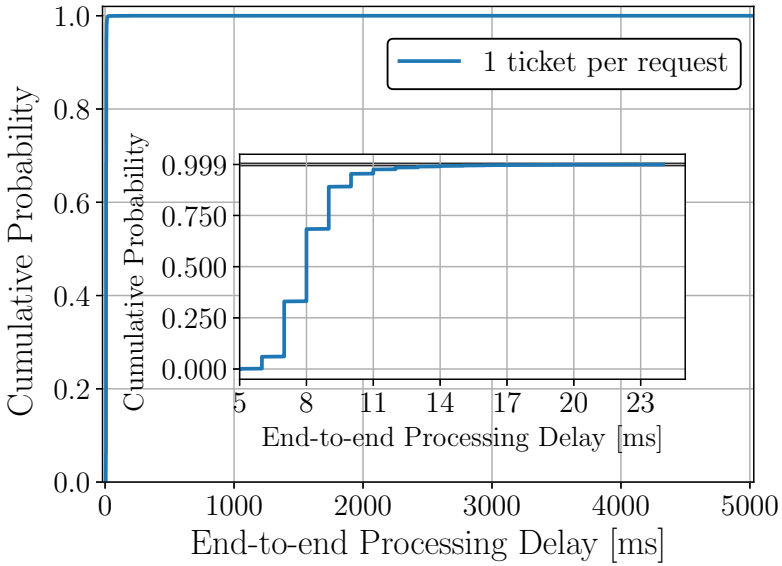


Figure: A High-level Overview of VPKIaaS Architecture on the Cloud

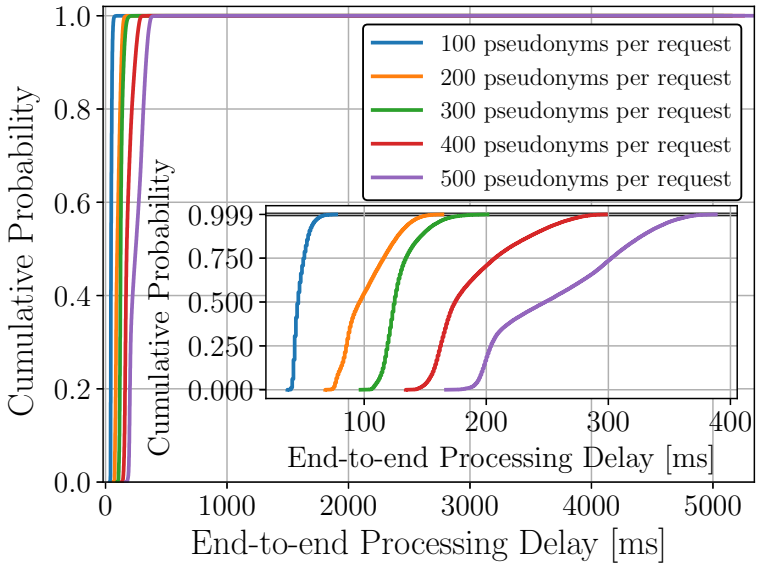
Experimental Setup (cont'd)

- **Network connectivity**
  - Varies depending on the actual OBU-VPKI connectivity
  - Reliable connectivity to the VPKI (e.g., RSU, Cellular, opportunistic WiFi)
- **Metrics**
  - **End-to-end processing delay to issue tickets and pseudonyms**
  - **High-availability and dynamic-scalability**
- **Use cases**
  - Large-scale pseudonym provision
  - VPKIaaS with flash crowd load pattern
  - Dynamic-scalability of the VPKIaaS
- **Remark**
  - Pseudonyms are issued with non-over-lapping intervals, to mitigate Sybil-based misbehavior
  - **Average daily commute time is 10-30 min. (actual urban vehicular mobility dataset), or 1 hour (according to the US DoT)**
  - **Obtaining 100 and 500 pseudonyms per day implies pseudonyms lifetimes of 14.4 min. ($\tau_P = 14.4$ min.) or 3 min. (τ_P =172.8 sec), respectively, covering 24 hours trip duration**
  - **Requesting pseudonyms based on Config-2, i.e., VPKIaaS system would serve 720,000 vehicles joining the system within an hour**

Performance Evaluation



(a) E2E latency to issue a ticket

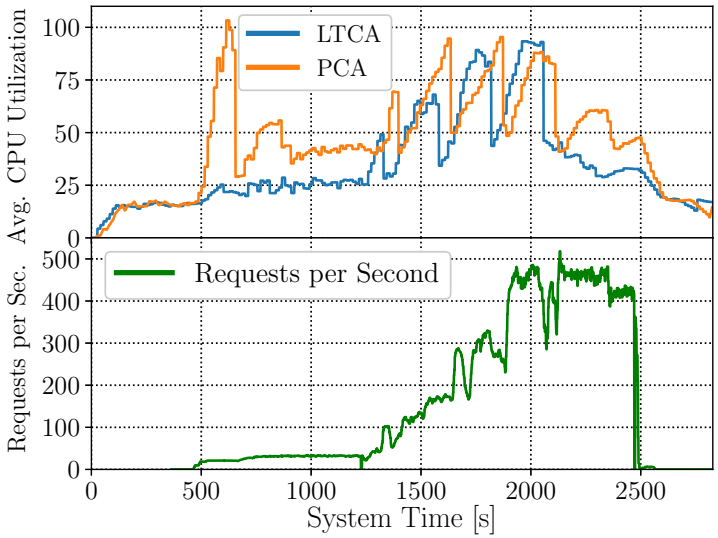


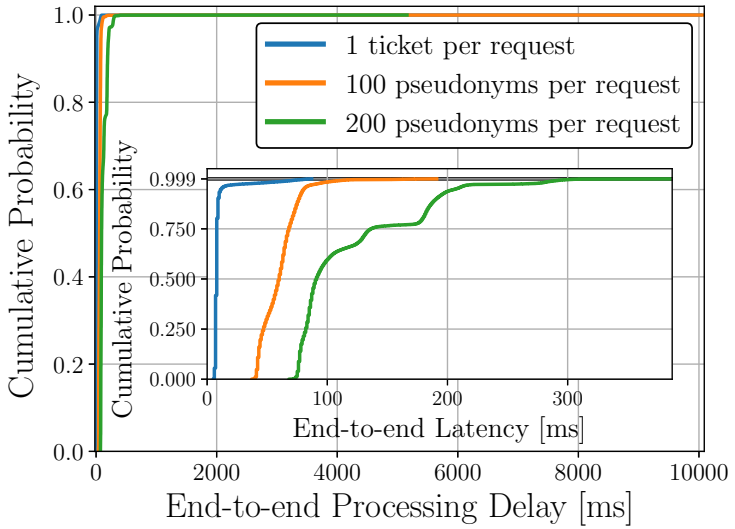
(b) E2E processing delay to issue psnyms

Large-scale pseudonym acquisition (based on Config-1):

- End-to-end Latency for ticket: $F_x(t = 24\ ms) = 0.999$
- With a batch of 100 pseudonyms per request, 99.9% of the vehicles are served within less than 77 ms ($F_x(t = 77\ ms) = 0.999$)
- With a batch of 500 pseudonyms per request, the VPKIaaS system efficiently issues pseudonyms: $F_x(t = 388\ ms) = 0.999$

Performance Evaluation (cont'd)





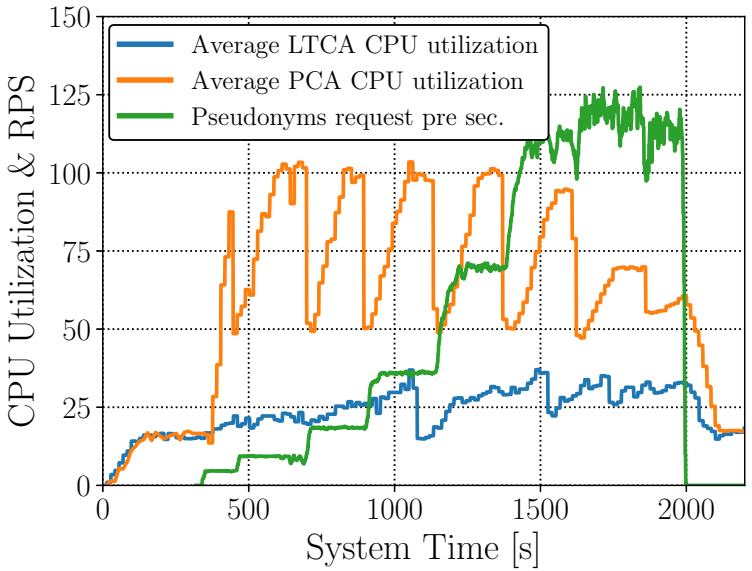
(a) CPU utilization and the number of requests per second (100 psnyms/req)

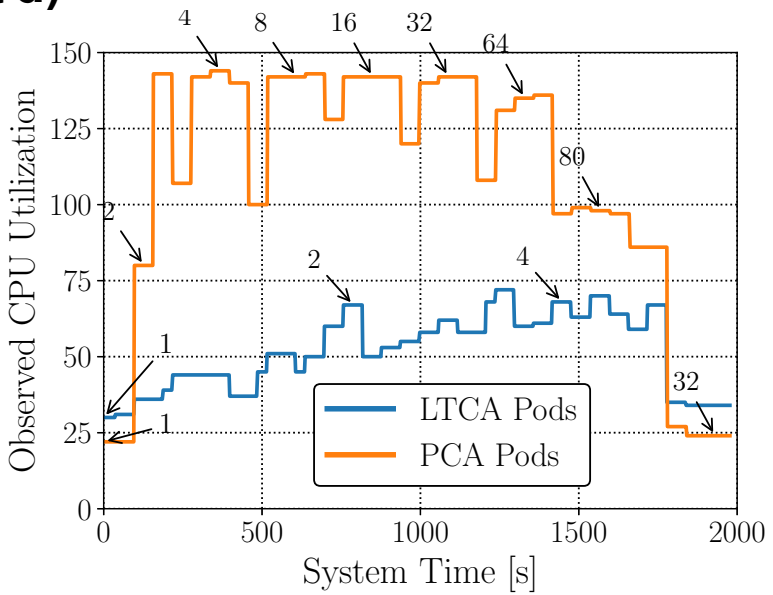
(b) CDF of processing latency to issue tickets and pseudonyms

VPKIaaS system in a flash crowd load situation (based on Config-2):

- CPU utilization hits 60% threshold, services scale out, CPU utilization drops
- The processing latency to issue a single ticket is: $F_x(t = 87\ ms) = 0.999$
- Issuing a batch of 100 pseudonyms per request: $F_x(t = 192\ ms) = 0.999$
- 'normal' conditions vs. flash crowd: processing latency of issuing a single ticket increases from 24 ms to 87ms; the processing latency to issue a batch of 100 psnyms increased from 77ms to 192ms

Performance Evaluation (cont'd)





(a) Number of active vehicles and CPU utilization **(b)** Dynamic scalability of VPKIaaS system

Reliability and dynamic scalability of the VPKIaaS system (with flash crowd load pattern, based on Config-2):

- Each vehicle requests 500 pseudonyms (CPU utilization observed by HPA)
- Synthetic workload generated using 30 containers, each with 1 vCPU and 1GB of memory (based on Config-2)

Outline

Vehicle-Centric CRL Distribution

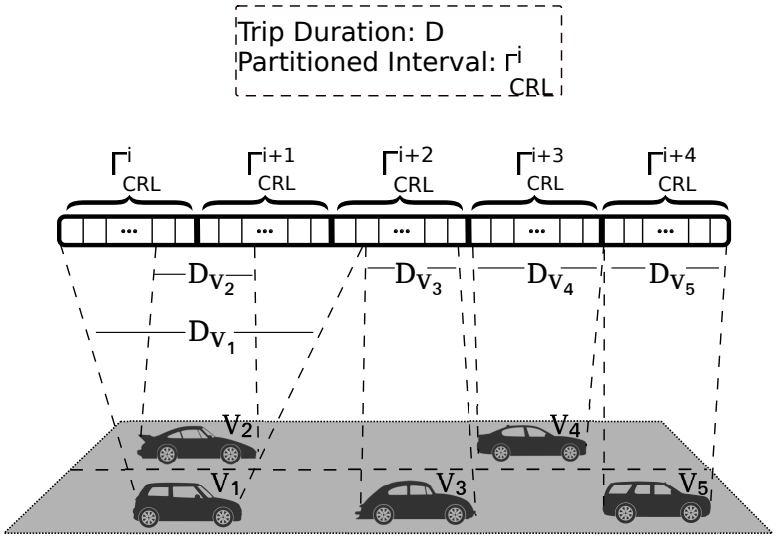


Figure: CRL as a Stream:

V_1 subscribes to $\{\Gamma^{i}_{CRL}, \Gamma^{i+1}_{CRL}, \Gamma^{i+2}_{CRL}\}$;

$V_2 : \{\Gamma^{i}_{CRL}, \Gamma^{i+1}_{CRL}\}$;

$V_3 : \{\Gamma^{i+2}_{CRL}\}$; $V_4 : \{\Gamma^{i+3}_{CRL}\}$; $V_5 : \{\Gamma^{i+4}_{CRL}\}$.

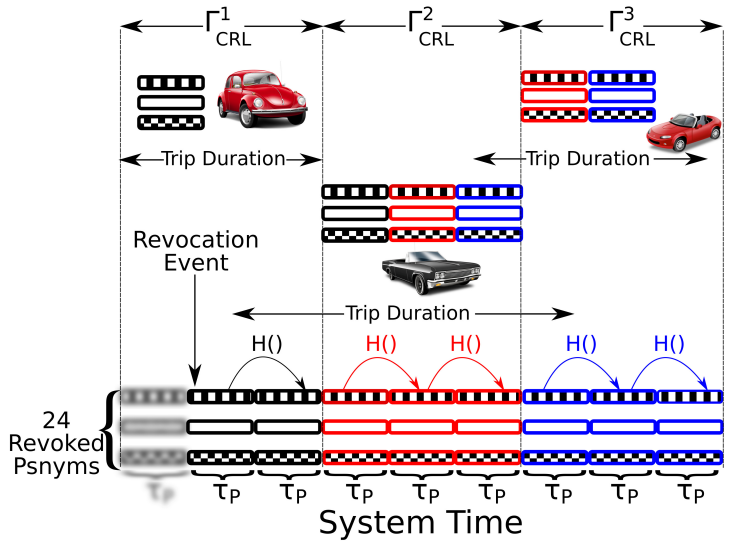
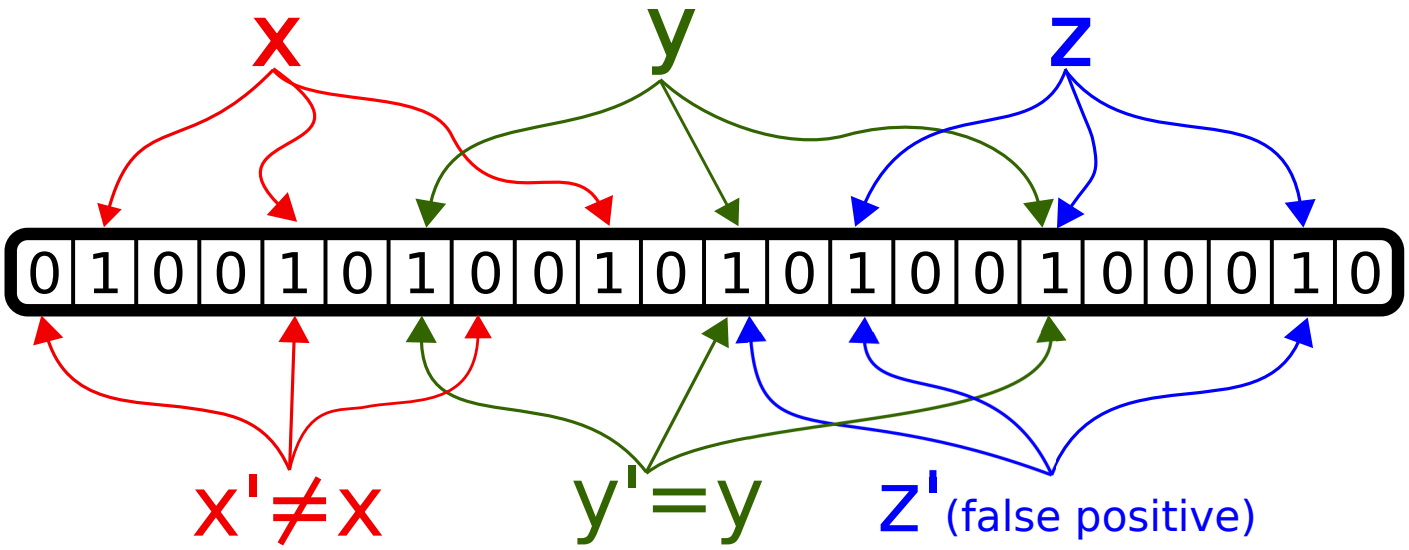


Figure: A vehicle-centric approach: each vehicle only subscribes for pieces of CRLs corresponding to its trip duration.

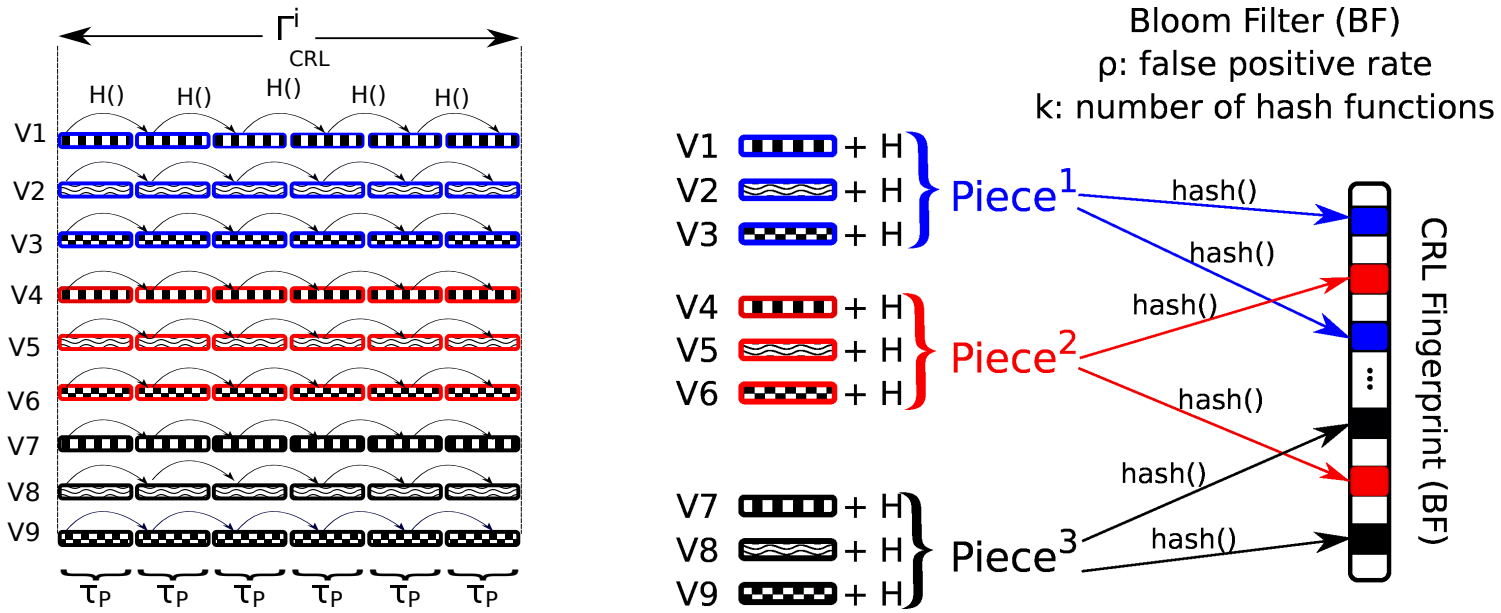
Bloom Filter (BF) and Cuckoo Filter (CF): Construction & Membership Checks



Bloom Filter (BF) (and Cuckoo Filter (CF)) features:

- A space-efficient probabilistic data structure
- Fast membership checking
- No false negatives, but false positive matches are possible
- A query returns either *"possibly in set"* or *"definitely not in set"*
- No deletion is allowed in a BF; but CF supports deletion.

Vehicle-Centric CRL Fingerprint Construction



(a) Revoked pseudonyms

(b) CRL fingerprint construction

Figure: CRL piece & fingerprint construction by the PCA.

CRL Fingerprint:

- A signed fingerprint is broadcasted by RSUs
- Also integrated in a subset of recently issued pseudonyms
- A notification about a new CRL-update (revocation) event

Qualitative Analysis

- BF trades off communication overhead for false positive rate
- BF size increases linearly as the false positive rate decreases

An adversary targeting the BF false positive rate:

- Excluding revoked pseudonym serial numbers from a CRL
- Adding valid pseudonyms by forging a fake CRL (piece)

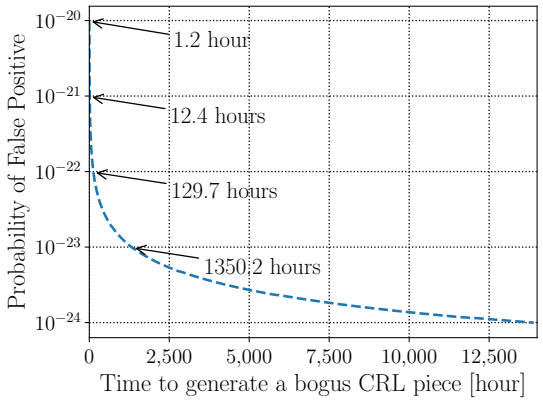


Figure: Query-only attack on the CRL fingerprints; adversary's computational power is $1.6 \times 10^{18}\, TH/sec$.

With Antminer-S9 (14TH/s,\$3,000), $\Gamma_{CRL} = 1$ hour and $p = 10^{-20}$ ($K = 67$):

- 132,936 Antminer-S9 (\$400M) to generate a bogus piece in 1 hour ($\frac{10^{20} \times 67}{14 \times 10^{12}}$)

With AntPool ($1,604,608\ TH/s$): 70 minutes to generate a fake piece!

- With $p = 10^{-22}$ ($K = 73$): 5 days ($\frac{10^{22} \times 73}{1.6 \times 10^{18}} = 126h$)
- With $p = 10^{-23}$ ($K = 76$): 55 days ($\frac{10^{23} \times 76}{1.6 \times 10^{18}} = 1,319h$)

Experimental Setup

- 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 : under the same assumptions and configuration with the same parameters
- Evaluation of:
  - **Efficiency (latency)**
  - **Resilience (to pollution/DoS attacks)**
  - Resource consumption (computation/communication)

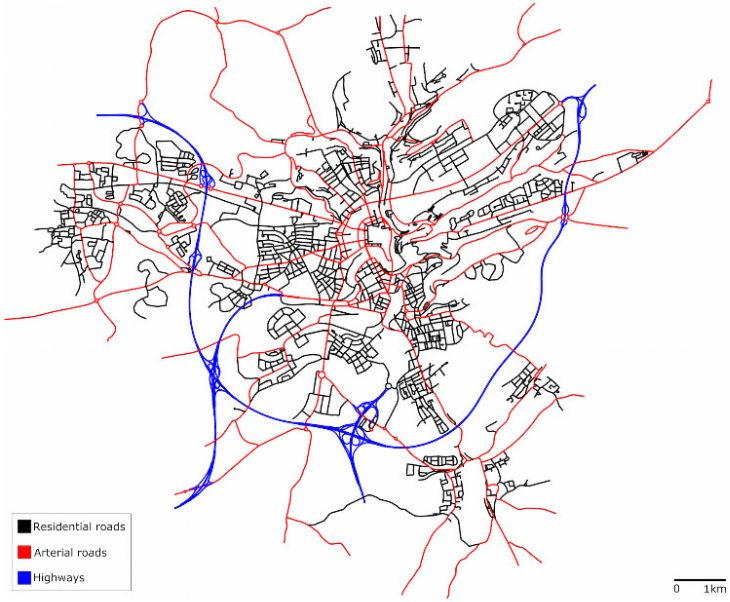
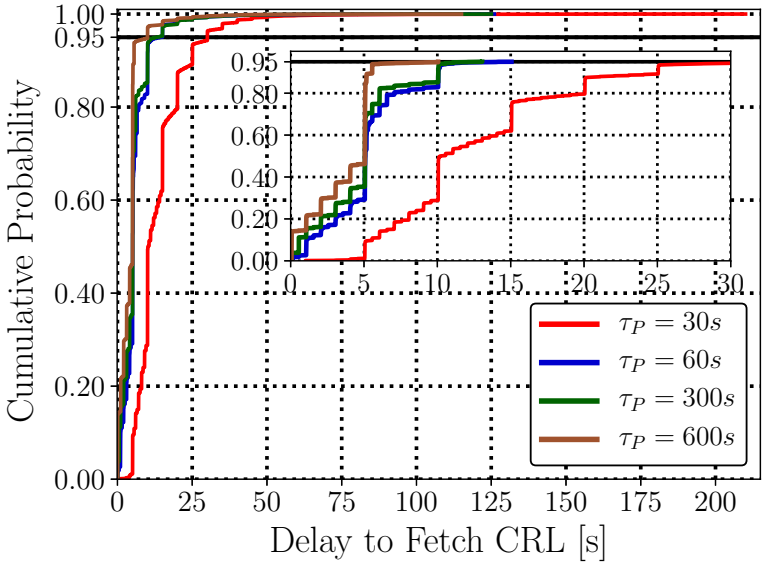
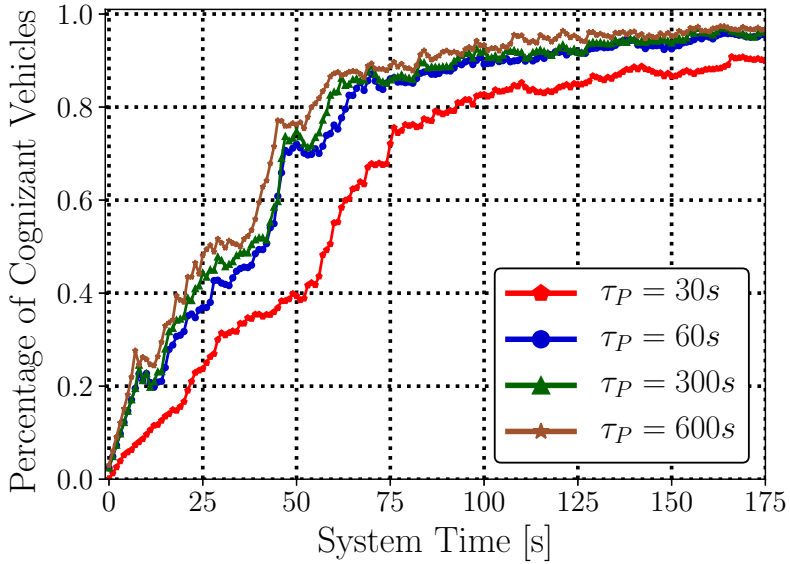


Figure: The LuST dataset, a full-day realistic mobility pattern in the city of Luxembourg (15KM x 15KM) [Codeca et al. (2015)].

Quantitative Analysis



(a) Vehicle-centric scheme ($\mathbb{B}$ =10 KB/s)

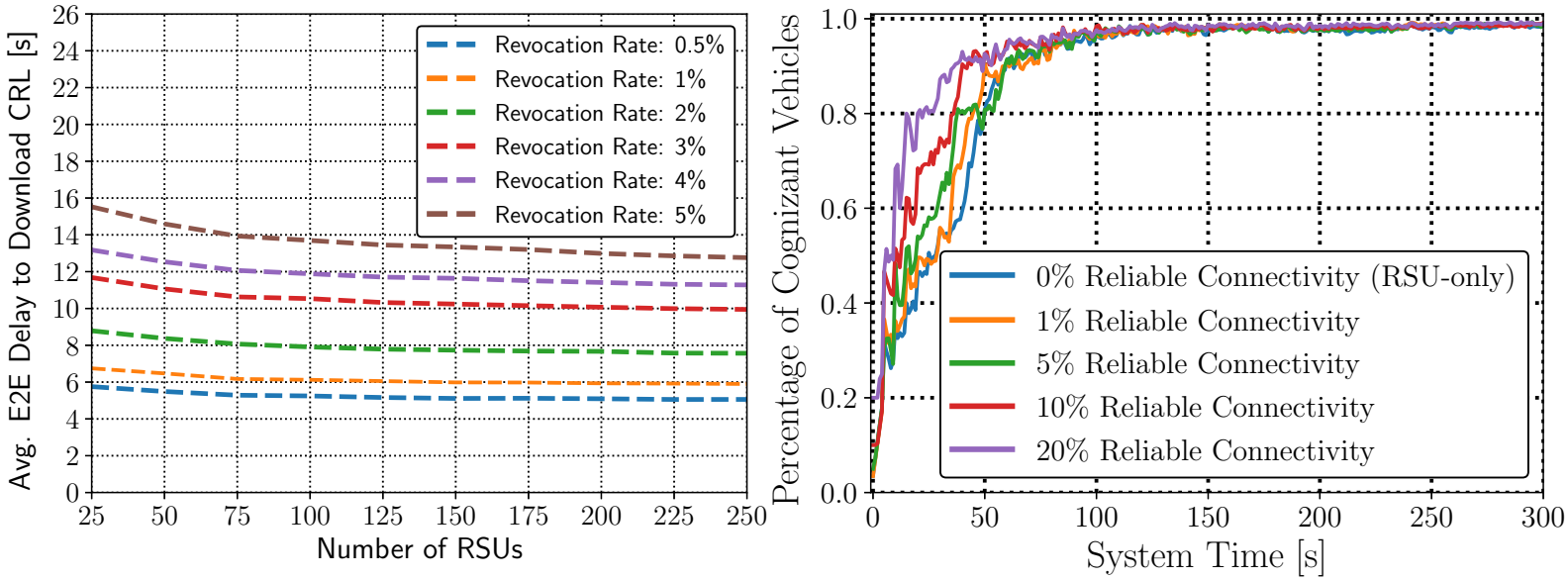


(b) Vehicle-centric scheme ($\mathbb{B}$ =10 KB/s)

Figure: (a) End-to-end latency to fetch CRL pieces. (b) Percentage of cognizant vehicles over time.

- The majority of the vehicles received the effective CRL pieces in the 15s when $\tau = 60s$
- The longer the τ is, the shorter the CRL size is, thus the faster the convergence time becomes.

Quantitative Analysis (cont'd)

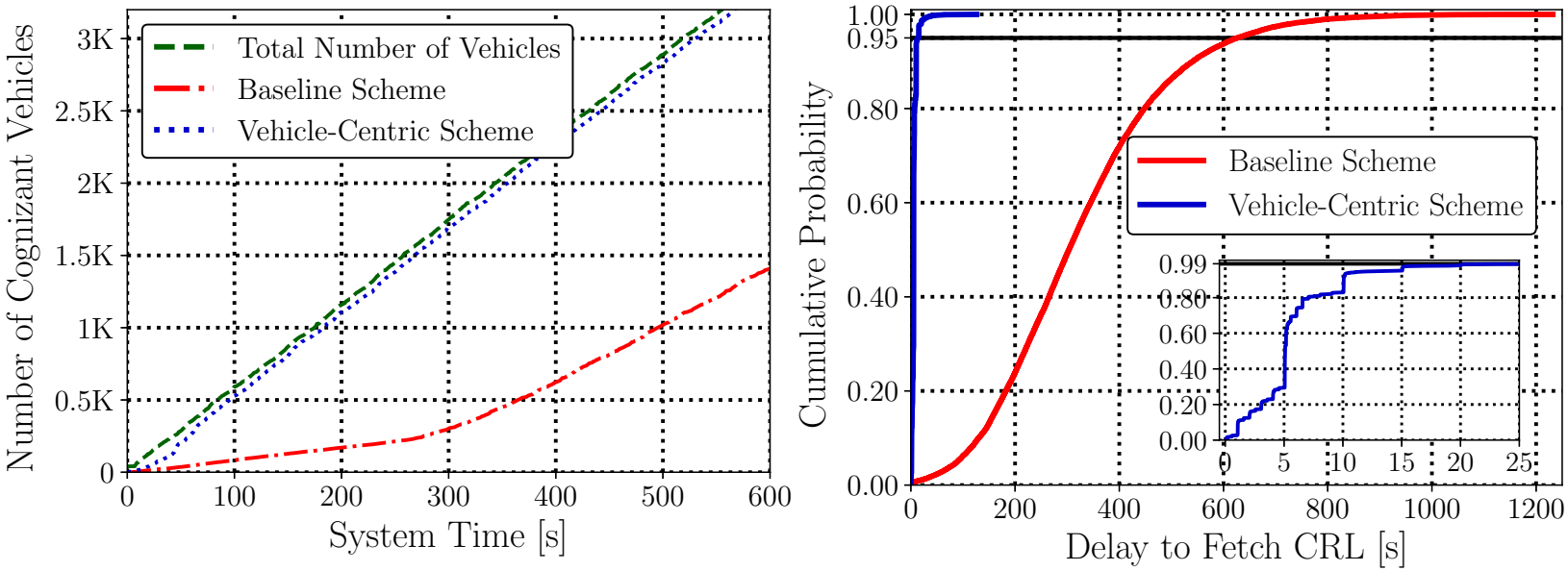


(a) Vehicle-centric scheme ($\mathbb{B}$ =25 KB/s) **(b)** Vehicle-centric scheme (TX =5s)

Figure: (a) Average end-to-end delay to download CRLs. (b) Dissemination of CRL fingerprints.

- Total number of pseudonyms is 1.7M ($\tau_P = 60s$).
- Signed fingerprint of CRL pieces periodically broadcasted only by RSUs, or broadcasted by RSUs (365 bytes with $TX = 5s$) and integrated into a subset of pseudonyms with 36 bytes of extra overhead ($p = 10^{-30}$, $\mathbb{R} = 0.5\%$).

Quantitative Analysis (cont'd)



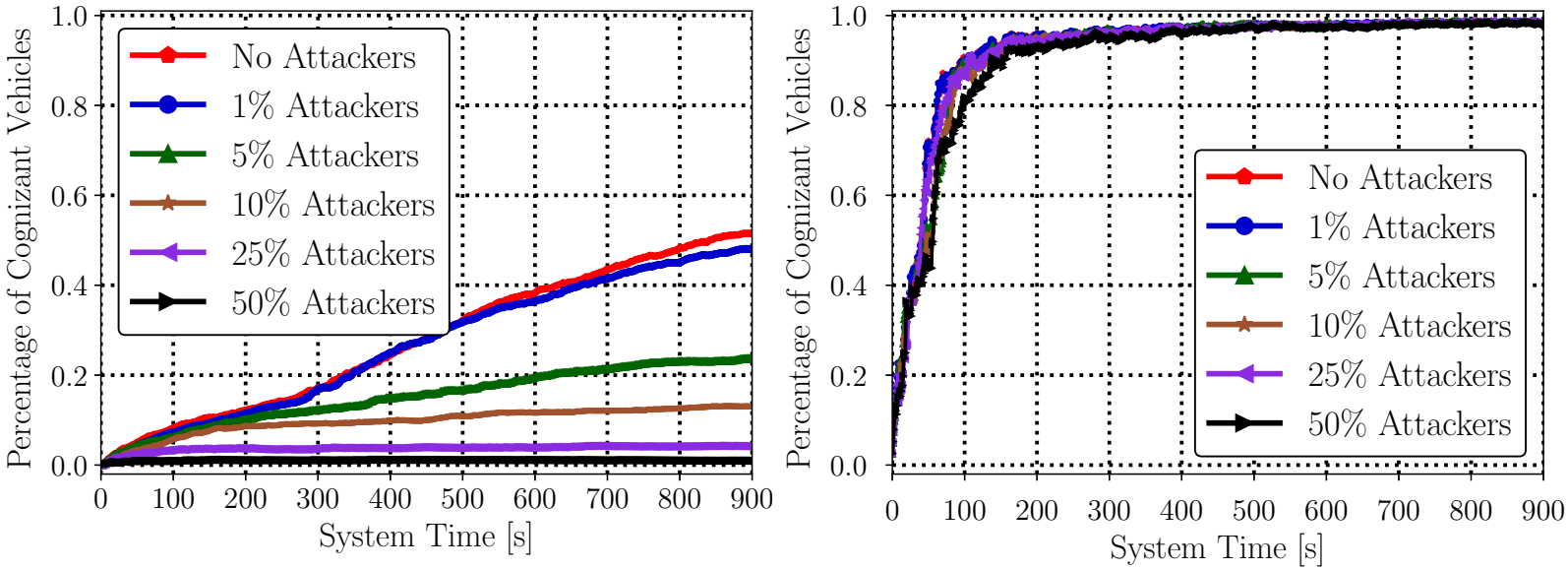
(a) 7:00-7:10 am ($\mathbb{B}$ =25 KB/s) **(b)** 7-9 am, 5-7 pm ($\mathbb{B}$ =25 KB/s)

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: $F_x(t = 15s) = 0.95$

Quantitative Analysis (cont'd)



(a) Baseline scheme ($\mathbb{B}$ =25 KB/s) **(b)** Vehicle-centric scheme ($\mathbb{B}$ =25 KB/s)

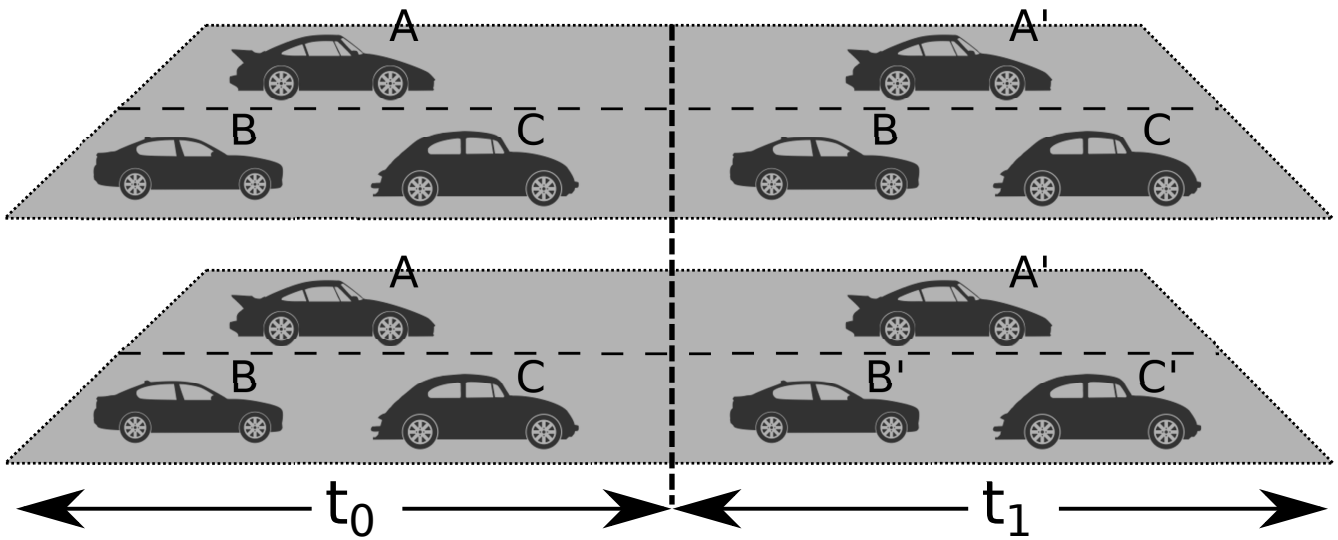
Figure: Resilience comparison against pollution and DDoS attacks.

- Attackers periodically broadcast fake CRL pieces once every 0.5 second.
- The resilience to pollution and DDoS attacks stems from three factors:
  - A huge reduction of the CRL size
  - Efficient verification of CRL pieces
  - Integrating the fingerprint of CRL pieces in a subset of pseudonyms

Outline

Vehicle Traceability (Syntactic & Semantic Linking Attacks)

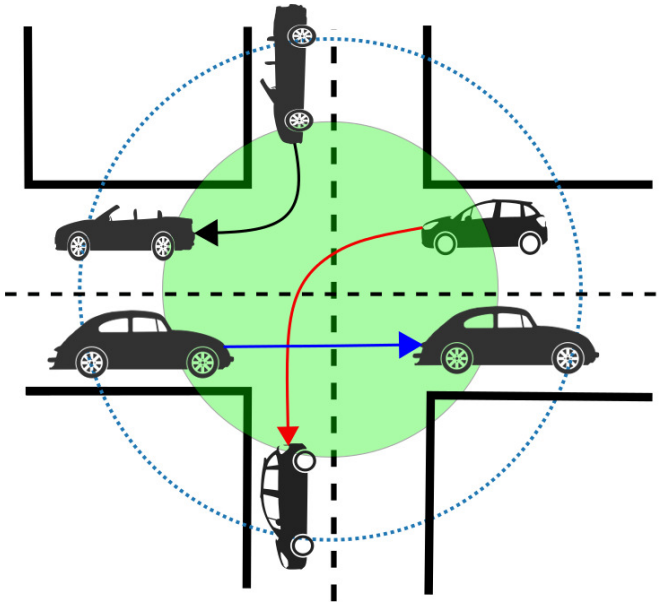
- Leveraging *K-anonymity*, obfuscating CAMs, or silent period
  - Diminishing situational awareness, thus, affecting operation of safety applications
- Leveraging group signature schemes
  - Computation overhead; only mitigating syntactic linking attack
- Synchronous pseudonym updates
  - Only mitigating syntactic linking attack



Vehicle Traceability (Syntactic & Semantic Linking Attacks) (cont'd)

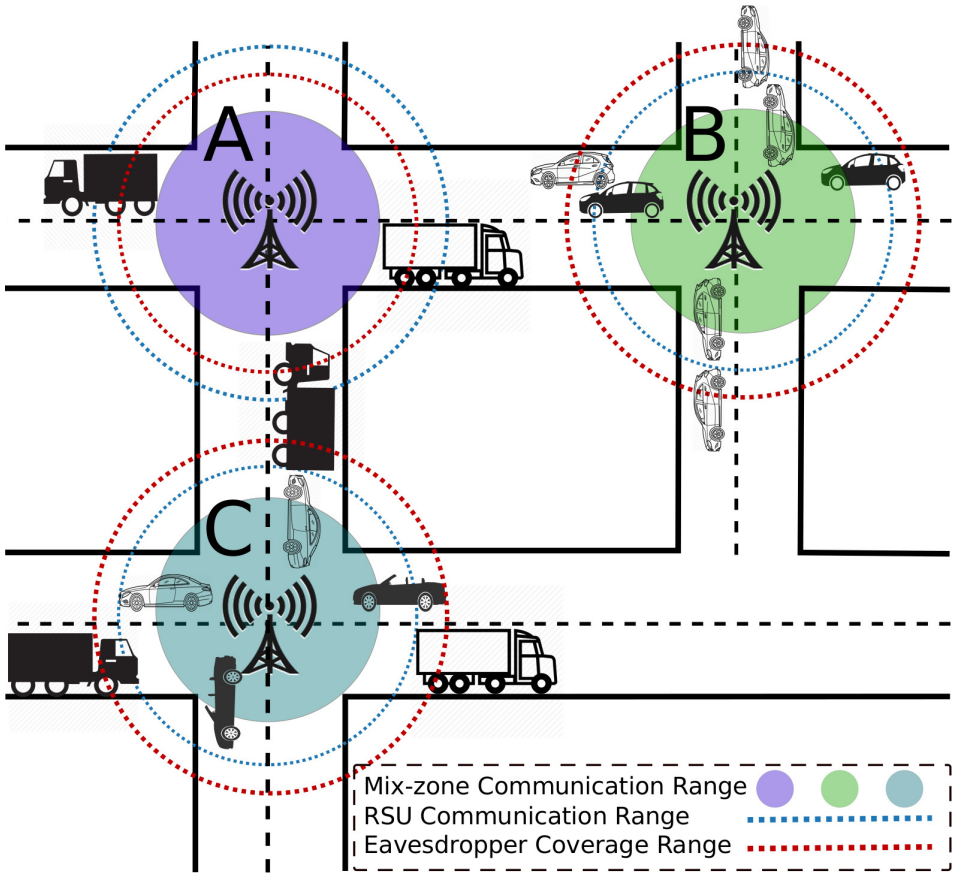
Cryptographic Mix-Zone (CMIX):

- Mitigating syntactic and semantic linking attacks
- Without affecting the operation of safety applications



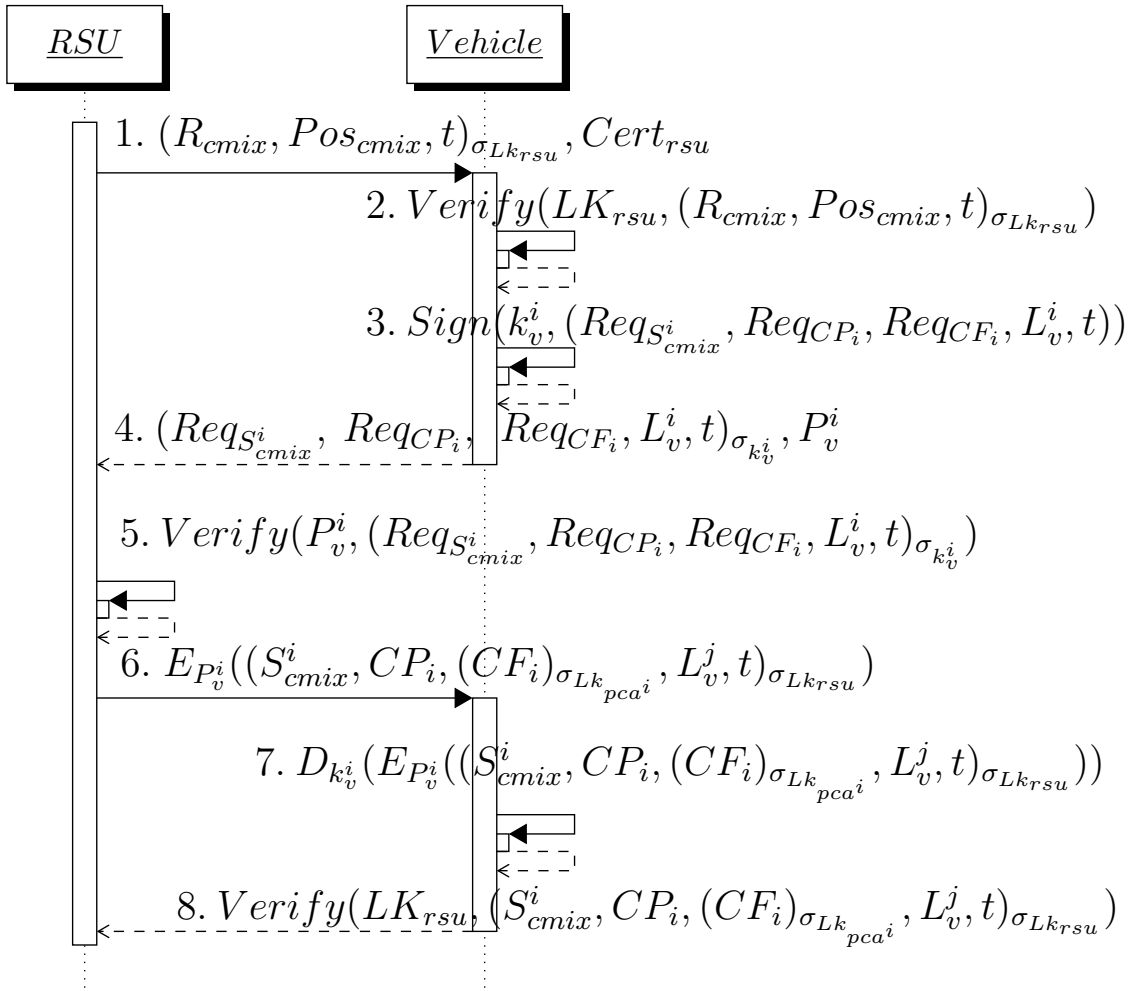
- Arrival rates
- Mix-zone geometries
- Physical constraints of the road layout
- Mobility patterns (e.g., velocity, acceleration)
- Vehicle density (e.g., sparse traffic conditions)

Mix-zones Construction with Decoy Traffic



- What about safety applications?
  - Dissemination of a signed Cuckoo Filter (CF)

Mix-zones Advertisement and Chaff Pseudonym Acquisition Protocols



Protocol 1 Syntactic and Semantic Linking Algorithm

procedure LINKINGSUCCESSIVEPSEUDONYMSALGORITHM( )
    Fetch eavesdropped beacon and road layout information
    Classify eavesdropped beacons based on vehicle length
    Create a list with the first & last seen beacons for each identifier
    Filter out trivially linked pseudonyms (not changing psnyms)
    $MaxTravTime \leftarrow$ Maximum time to traverse a mix-zone
    $MinTravTime \leftarrow$ Minimum time to traverse a mix-zone
    for Each B_i in BEACON_SET **do**
        B_i^f is the first seen message for beacon B_i
        B_i^l is the last seen message for beacon B_i
        for Each B_{i+1}^f in BEACON_SET **do**
            B_i^l and B_{i+1}^f are not correlated
            diff $\leftarrow$ time difference between B_i^l and B_{i+1}^f
            if diff $\geq$ *MinTravTime* && diff $\leq$ *MaxTravTime* **then**
                if pseudo-id for B_i^l and B_{i+1}^f not seen together **then**
                    if exists a road path from B_i^l to B_{i+1}^f **then**
                        if B_{i+1}^f direction is from an exit point **then**
                            B_i^l and B_{i+1}^f are correlated
                            break
                        end if
                    end if
                end if
            end if
        end for
    end for
end procedure

Syntactic and Semantic Linking Algorithm

In order to link two pseudonyms:

- An adversary places wireless receivers near each mix-zone (entry and exit points)
- An adversary tries to link one of the last seen beacon before entering a mix-zone to one of the first-seen beacon exiting the mix-zone
- Filtering out trivially linked pseudonyms
- Estimated time to traverse a mix-zone
- The two pseudonyms have not been seen together
- Considering the physical road layout (exists a path between the two)
- The second beacon (direction) is from an exit points of the mix-zone

Experimental Setup

- OMNET++ & Veins framework using SUMO with the LuST dataset
- Placement of the mix-zones: “highly-visited” intersections
- One PCA for CF dissemination
- RSUs randomly assign a percentage of vehicles to be relaying ones
- **Metrics:**
  - **Average successful tracking through syntactic and semantic linking attacks**
  - **Resilience (non-cooperative vehicles)**
  - Efficiency (latency)
  - Resource consumption (computation/communication)

Table: Simulation parameters.

Parameters	Value	Parameters	Value
Beacon TX interval (γ_v)	0.2s, 0.5s, 1s	Number of RSUs	100
Carrier frequency	5.89 GHz	RSUs transmission range	600 meter
TX power	20mW	Number of Mix-zones	25
Physical layer bit-rate	18Mbps	Mix-zone advertisement TX interval (γ_{mz})	0.5s, 1s
Sensitivity	-89dBm	Mix-zone transmission range	100 meter
Thermal noise	-110dBm	Number of eavesdropper	25
Area size	15 KM $\times$ 15 KM	Eavesdropping range	250 meter
Average trip duration	692.81s	Percentage of internal adversaries	10%-50%
Number of trips	287,939	CF distribution bandwidth ($\mathbb{B}$)	50 KB/sec
Number of vehicles	138,259	CF TX interval	1s

Comparison:

- **Cryptographic Mix-Zone (CMIX) [Win-ITS’07]**
- Chaff-based CMIX [VNC’18]

Quantitative Analysis

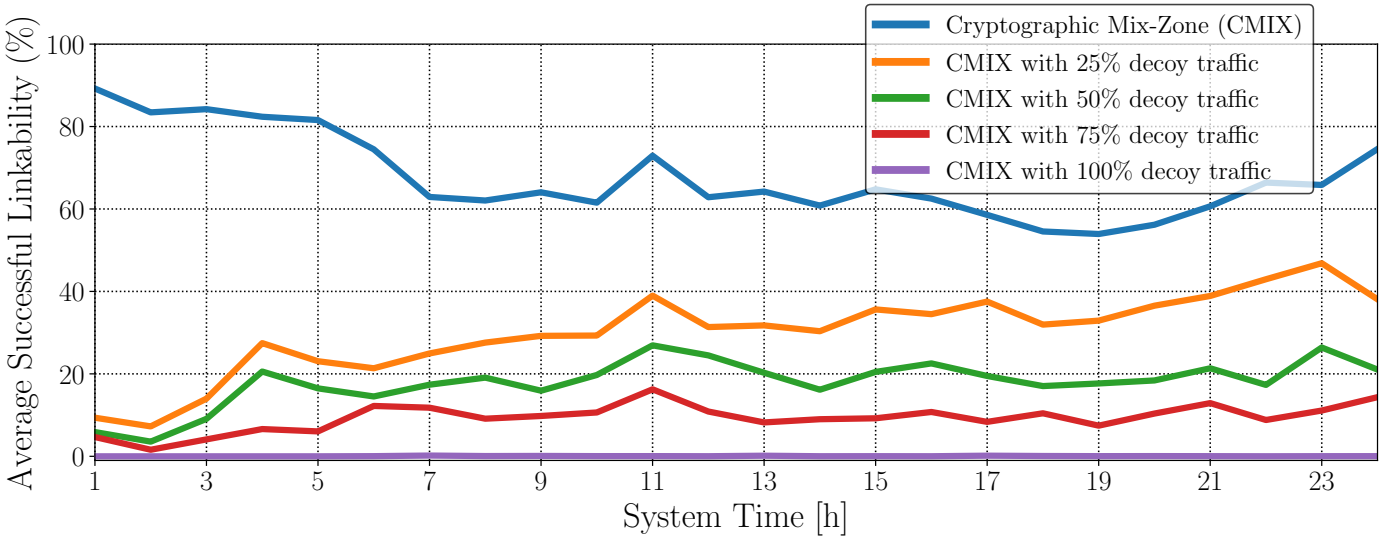
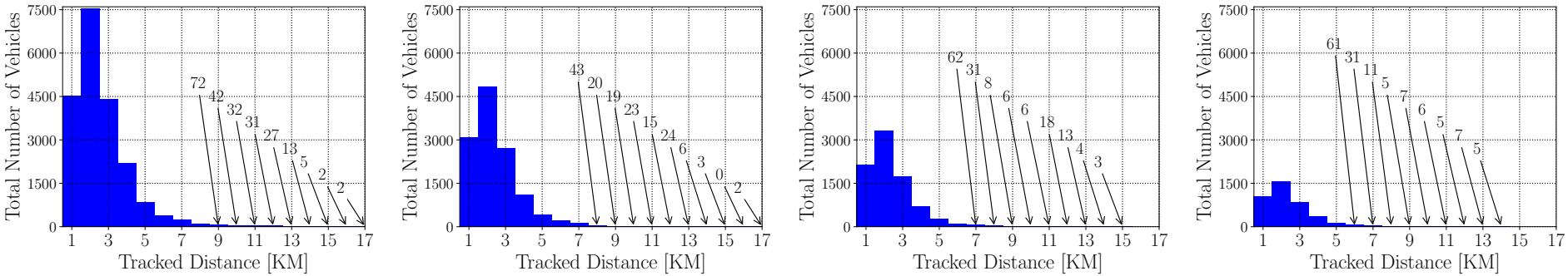


Figure: Average successful linkability comparison with the CMIX baseline scheme through conducting syntactic and semantic linking attacks.

- The probability of linking decreases when the traffic density increases.
- For the baseline scheme, one could link pseudonyms with high probability success rate.
- By introducing decoy traffic for 50% of vehicles, the probability of linking drops from 63% to 17% at system time 7.

Quantitative Analysis (cont'd)

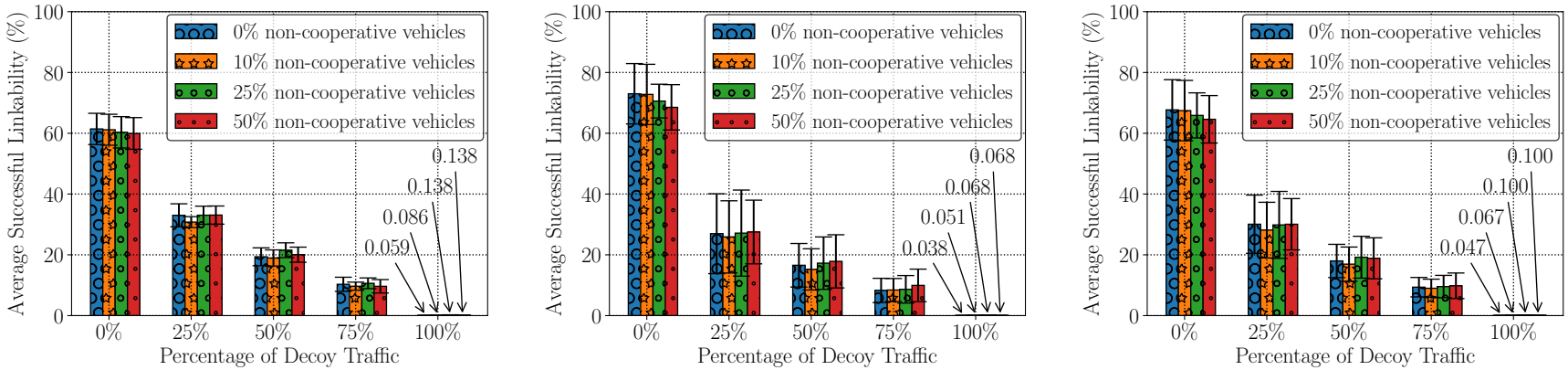


(a) CMIX **(b)** CMIX: 25% decoy traffic **(c)** CMIX: 50% decoy traffic **(d)** CMIX: 75% decoy traffic

Figure: Histogram of tracked distances by eavesdroppers based on the linked pseudonyms sets for the baseline scheme (CMIX) and our scheme.

- By introducing decoy traffic for vehicles exiting the mix-zones, the total number of vehicles, tracked by the eavesdroppers, drastically decreases.

Quantitative Analysis (cont'd)



(a) During Rush Hours **(b)** During Non-rush Hours **(c)** During 24 Hours

Figure: Average successful linkability in the presence of non-cooperative vehicles, not changing their pseudonyms while crossing the mix-zones.

- Non-cooperative vehicles exit the mix-zone without changing pseudonyms; also, if chosen to be relaying vehicles, do not disseminate decoy traffic.
- Selection of such vehicles is independent of selection of relaying vehicles; in each scenario, different sets are selected to be non-cooperative.
- The average successful tracking is not considerably affected in the presence of non-cooperative vehicles.

Original Work

- 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.
- M. Khodaei, H. Jin, and P. Papadimitratos, *"Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure,"* in IEEE VNC, Paderborn, Germany, Dec. 2014.
- 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.
- M. Khodaei and P. Papadimitratos, *"Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems,"* in ACM MobiHoc, Workshop on Internet of Vehicles and Vehicles of Internet (IoV-VoI), Paderborn, Germany, July 2016.
- M. Khodaei, A. Messing, and P. Papadimitratos, *"RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd,"* in Proceedings of the IEEE Vehicular Networking Conference (VNC), Torino, Italy, Nov. 2017.

Original Work (cont'd)

- 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 (T-ITS), vol. 19, no. 5, pp. 1430–1444, May 2018.
- M. Khodaei and P. Papadimitratos, *"Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs,"* in Proceedings of the ACM Conference on Security and Privacy in Wireless & Mobile Networks (WiSec), Stockholm, Sweden, June 2018.
- M. Khodaei, H. Noroozi, and P. Papadimitratos, *"Scaling Pseudonymous Authentication for Large Mobile Systems,"* in Proceedings of the ACM Conference on Security and Privacy in Wireless & Mobile Networks (WiSec), Miami, FL, USA, May 2019.
- M. Khodaei and P. Papadimitratos, *"Scalable & Resilient Vehicle-Centric Certificate Revocation List Distribution in Vehicular Communication Systems,"* to appear in IEEE Transactions on Mobile Computing (TMC).
- M. Khodaei and P. Papadimitratos, *"Cooperative Location Privacy in Vehicular Networks: Why Simple Mix-zones are not Enough,"* submitted to IEEE Internet Of Things (IoT) Journal.

The Key to Intelligent Transportation Systems: Identity and Credential Management for Secure and Privacy-Preserving Vehicular Communication Systems

PhD Defense

Mohammad Khodaei
Networked Systems Security Group

June 15, 2020