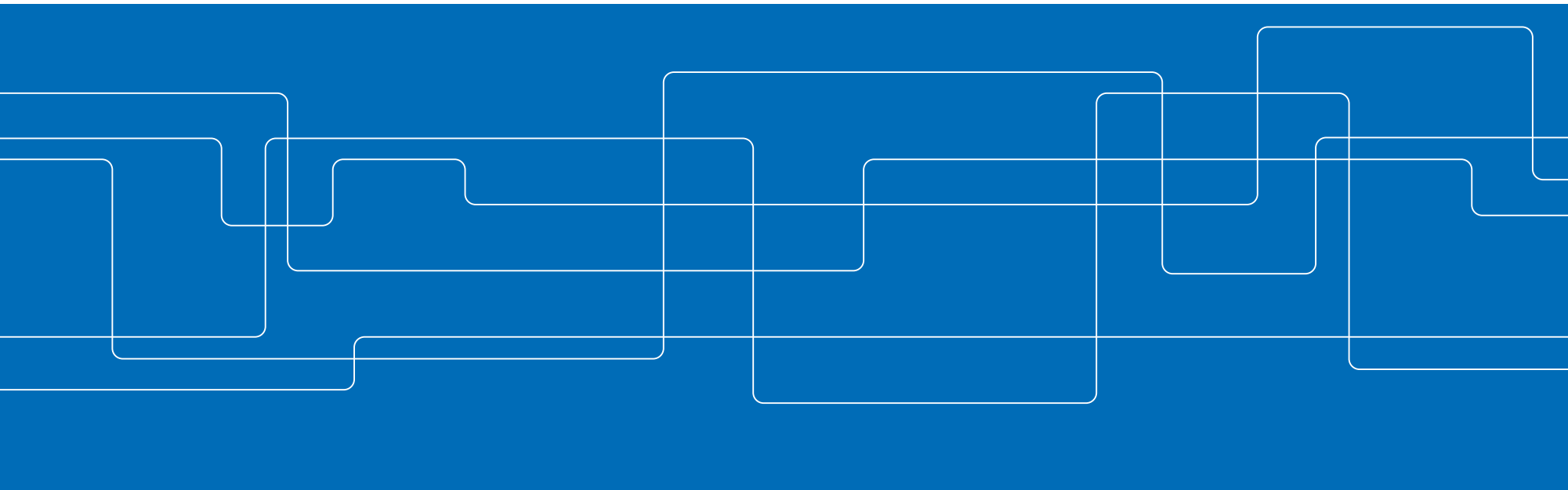
KTH ROYAL INSTITUTE
OF TECHNOLOGY

Scalable & Resilient Vehicle-Centric Certificate Revocation List Distribution in Vehicular Communication Systems

Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group (NSS)
www.eecs.kth.se/nss



Outline

Vehicular Communication (VC) Systems

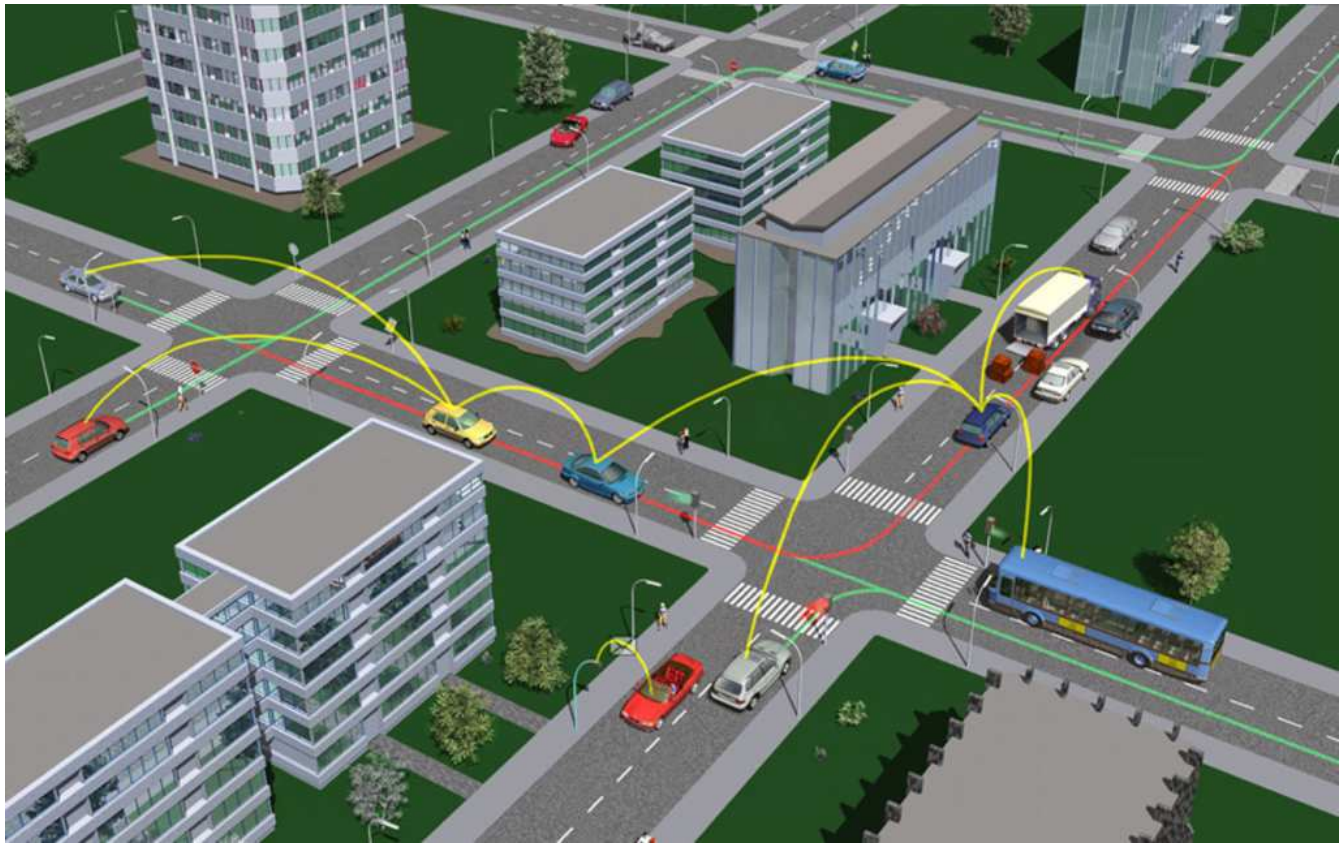
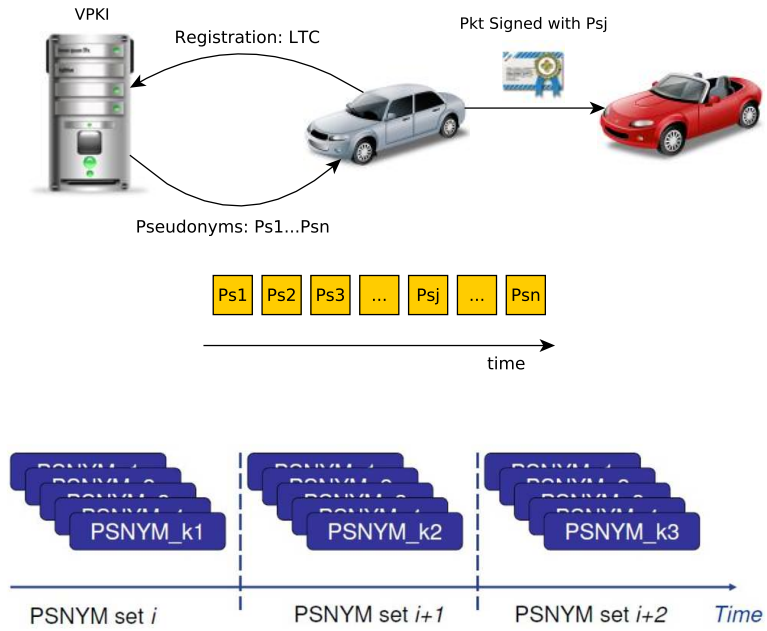


Figure: Photo Courtesy of the Car2Car Communication Consortium (C2C-CC)

Security and Privacy for VC Systems[1]

Basic Requirements [1, 2]

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

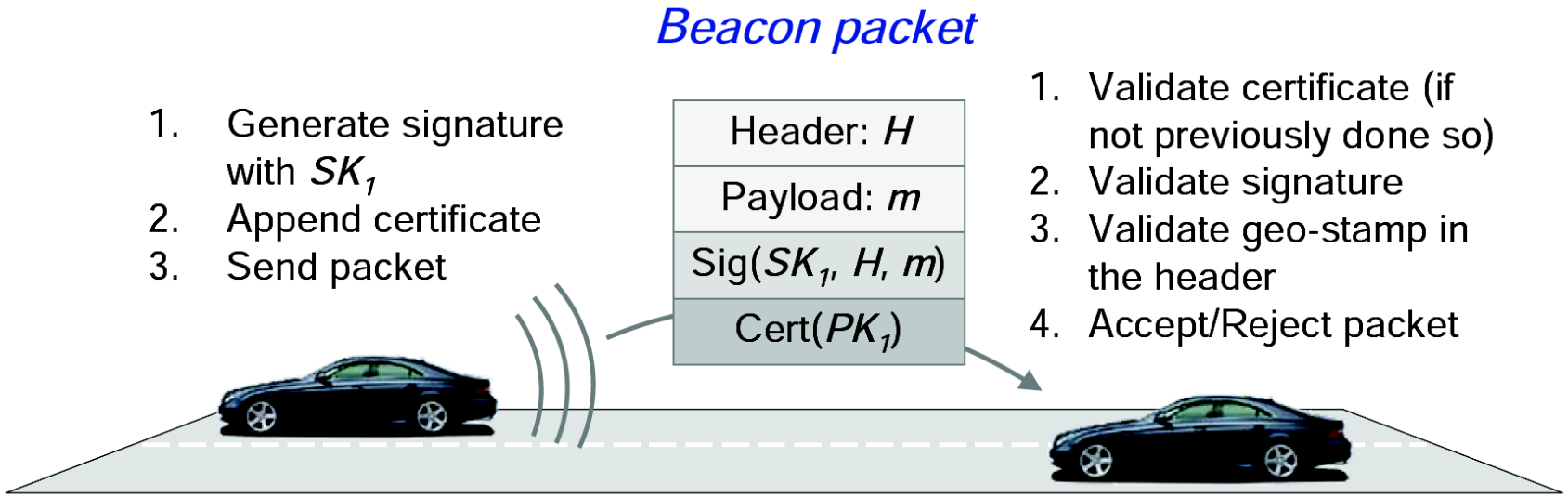


Vehicular Public-Key Infrastructure (VPKI)

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

[1] P. Papadimitratos, et al. "Securing Vehicular Communications - Assumptions, Requirements, and Principles," in ESCAR, Berlin, Germany, pp. 5-14, Nov. 2006.
P. Papadimitratos, et al. "Secure Vehicular Communication Systems: Design and Architecture," in IEEE Communications Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.

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)

Secure & Privacy-preserving VC Systems

- 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

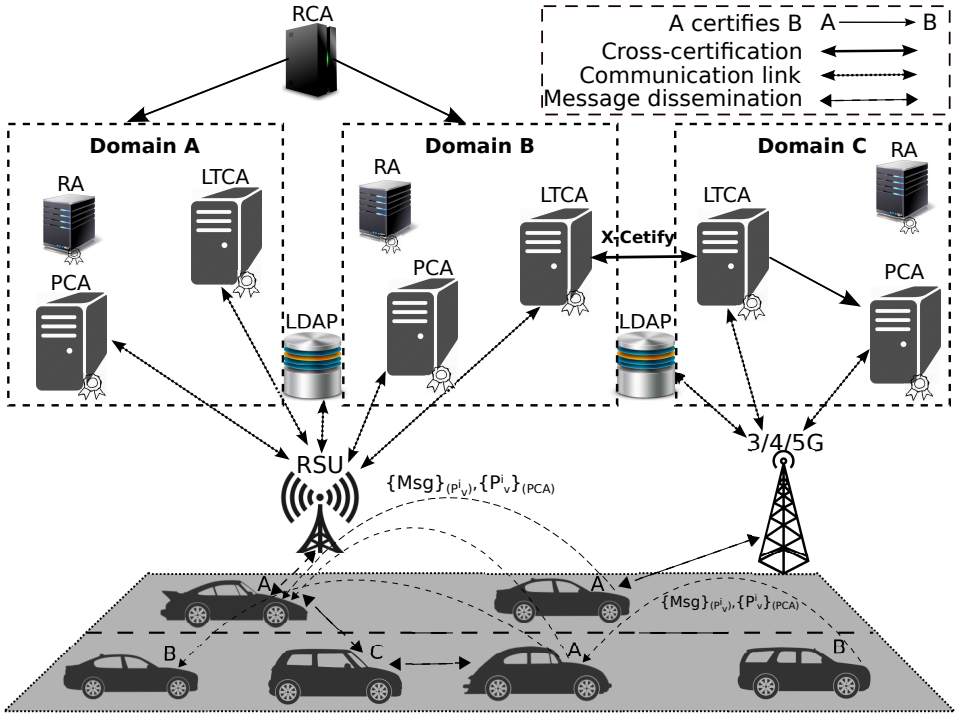


Figure: VPKI Overview

Challenges & 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
    (rates of 10 safety beacons per second)
- Mechanics of revocation:
  - *Highly dynamic environment with intermittent connectivity*
  - *Short-lived pseudonyms, multiple per entity*
  - *Resource constraints*

Challenges and Motivation (cont'd)
Revocation challenges:

- Efficient and timely distribution of Certificate Revocation Lists (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

Outline

System Model and Assumptions

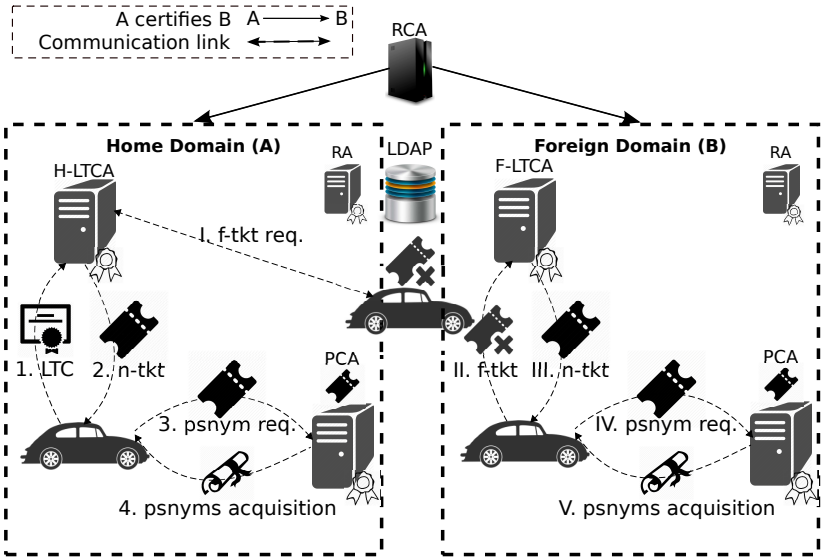


Figure: Pseudonym acquisition overview in the home and foreign domains.

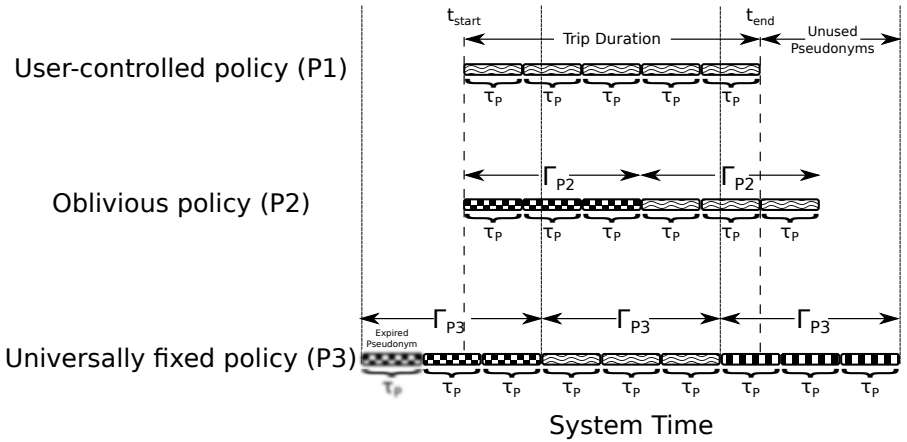


Figure: Pseudonym Acquisition Policies.

M. Khodaei, H. Jin, and P. Papadimitratos. IEEE T-ITS, vol. 19, no. 5, pp. 1430-1444, May 2018.

System Model and Requirements

Adversarial Model:

- Excluding revoked pseudonym serial numbers from a CRL
- Adding valid pseudonyms by forging a fake CRL (piece)
- Preventing legitimate vehicles from obtaining genuine and the most up-to-date CRL (pieces) or delaying the distribution
- Harming user privacy by the VPKI entities

Requirements:

- Fine-grained authentication, integrity, and non-repudiation
- Unlinkability (perfect-forward-privacy)
- Availability
- Efficiency
- Explicit and/or implicit notification on revocation events

Vehicle-Centric CRL Distribution

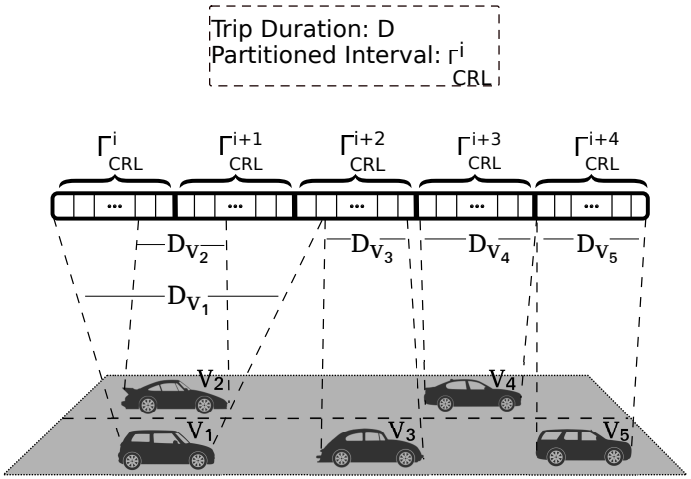


Figure: CRL as a Stream:

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

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

$V_3 : \{\Gamma^{i+2}_{CRL}\}$;

$V_4 : \{\Gamma^{i+3}_{CRL}\}$;

$V_5 : \{\Gamma^{i+4}_{CRL}\}$.

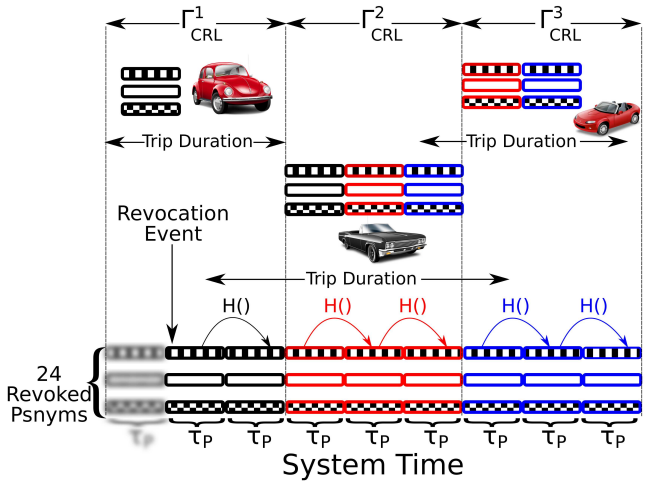
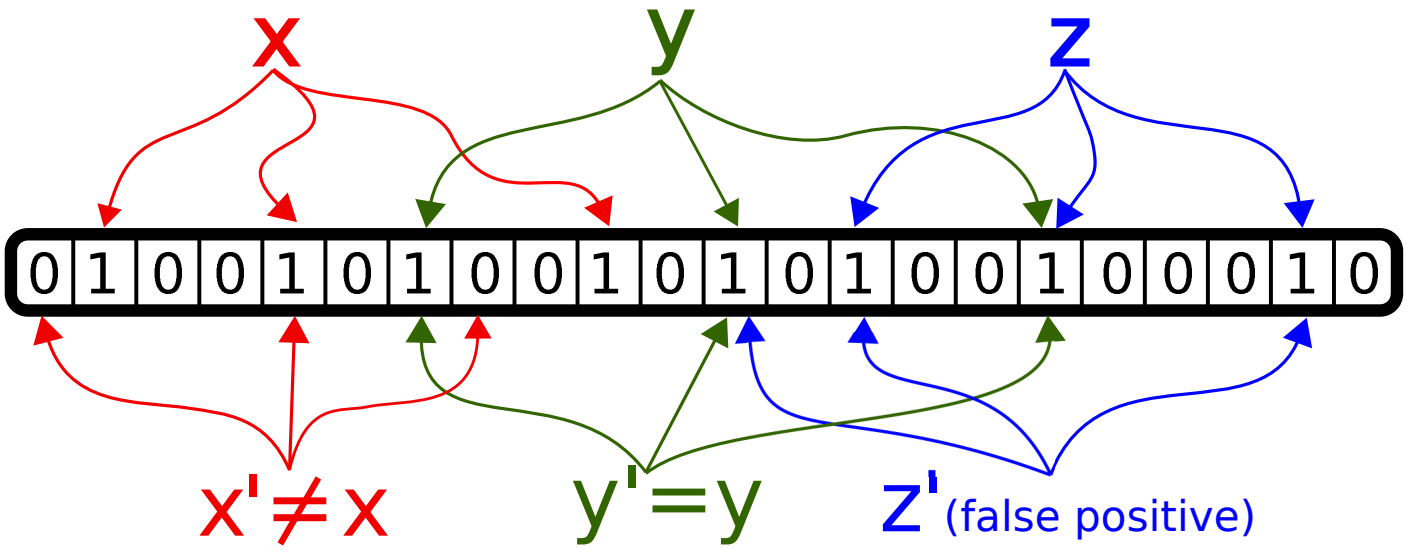


Figure: A vehicle-centric approach: each vehicle only subscribes for pieces of CRLs corresponding to its trip duration.

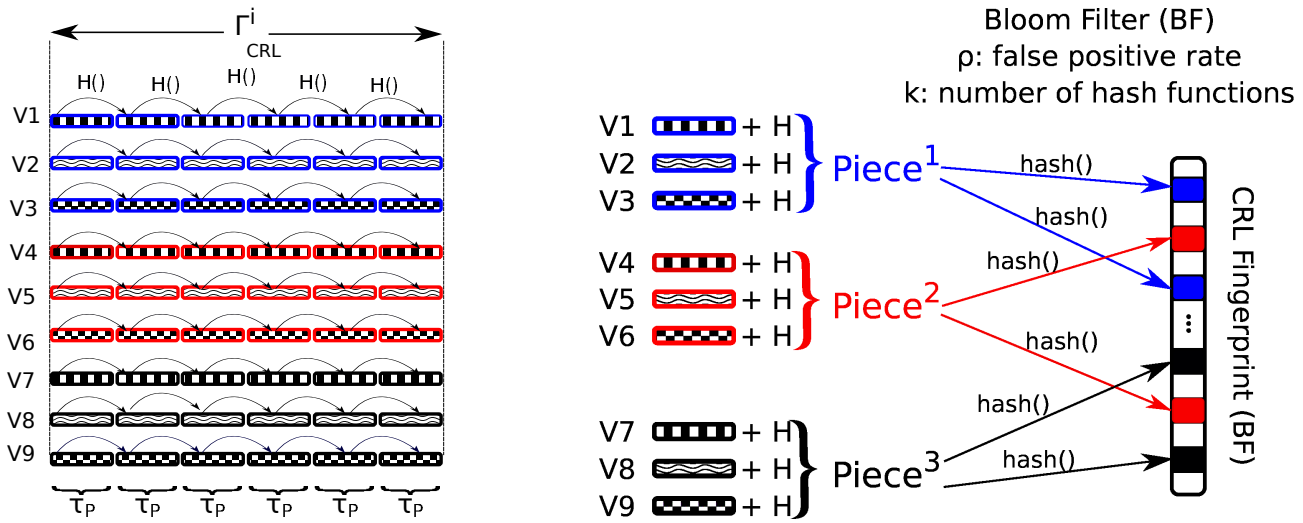
Bloom Filter Construction & Membership Checks



Bloom Filter (BF) 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; (Cuckoo Filter (CF) supports deletion)

Vehicle-Centric CRL Distribution (cont'd)



(a) Revoked pseudonyms

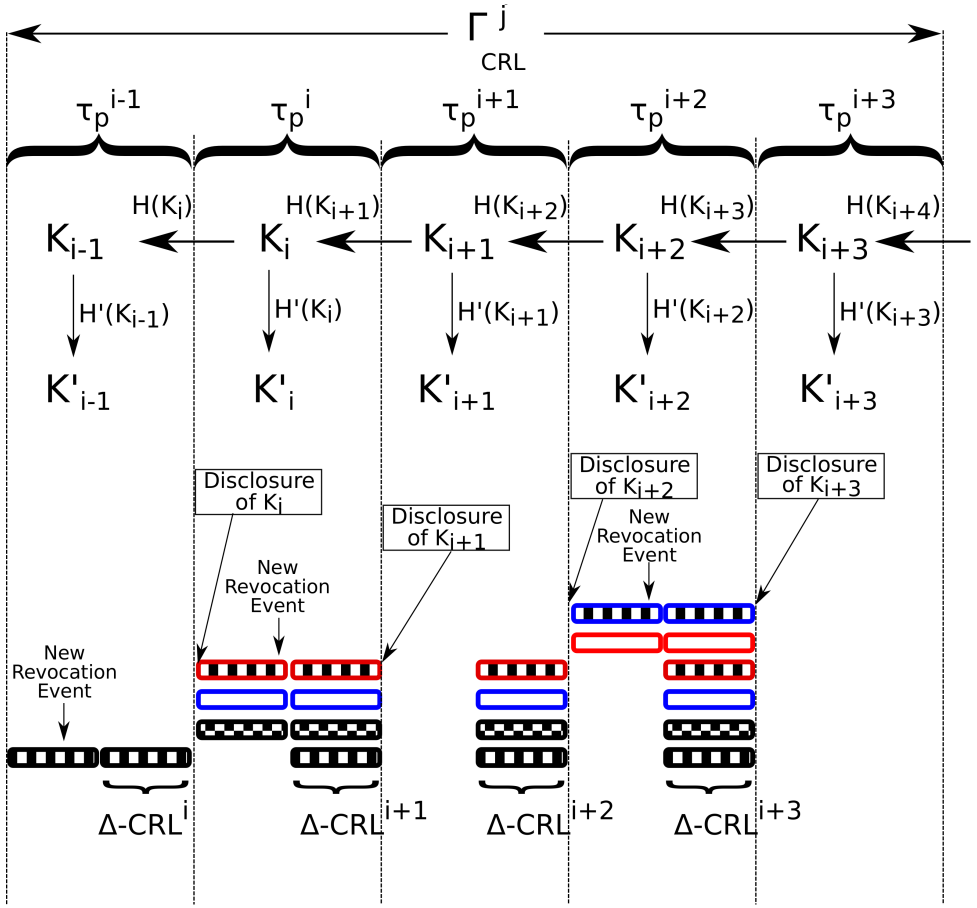
(b) CRL fingerprint construction

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

Vehicle-centric Δ-CRL distribution



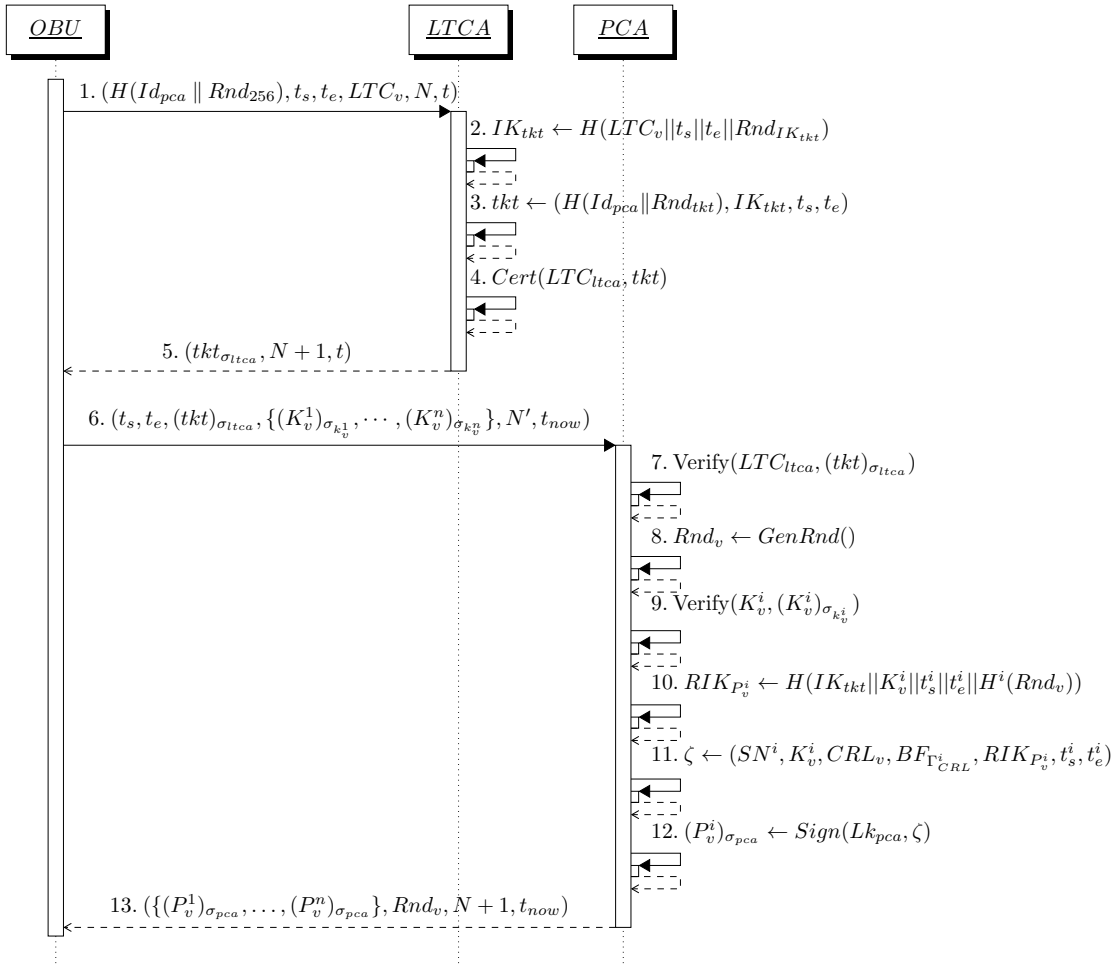
Outline

Notation Used in the Protocols

Table: Notation Used in the Protocols.

Notation	Description	Notation	Description
$(P_v^i)_{pca}$, P_v^i	a valid psnym signed by the PCA	$Append()$	appending a revoked psnym SN to CRLs
(K_v^i, k_v^i)	psnym pub./priv. key pairs	BFTest()	BF membership test
$(K_{pca}; Lk_{pca})$	long-term pub./priv. key pairs	p, K	false positive rate, optimal hash functions
$(msg)_{\sigma_v}$	signed msg with vehicle's priv. key	Γ	interval to issue time-aligned psnyms
LTC	Long Term Certificate	Γ_{CRL}	interval to release CRLs
t_{now}, t_s, t_e	a fresh, starting, ending timestamp	RIK	revocation identifiable key
$T_{timeout}$	response reception timeout	$\mathbb{B}$	max. bandwidth for CRL distribution
$n\text{-}tkt$, $(n\text{-}tkt)_{ltca}$	a native ticket	$\mathbb{R}$	revocation rate
Id_{req}, Id_{res}	request/response identifiers	N	total number of CRL pieces in each Γ_{CRL}
SN	psnym serial number	n	number of remaining psnyms in each batch
$Sign(Lk_{ca}, msg)$	signing a msg with CA's priv. key	k	index of the first revoked psnym
$Verify(LTC_{ca}, msg)$	verifying with the CA's pub. key	CRL_v	CRL version
$GenRnd(), rand(0, *)$	GEN. a random number, or in range	$\emptyset$	Null or empty vector
$H^k(), H$	hash function (k times), hash value	k, j, m, ζ	temporary variables

Pseudonym Acquisition Process



1: **if** $i = 1$ **then**
2: $SN^i \leftarrow H(RIK_{P_v^i}||H^i(Rnd_v))$
3: **else**
4: $SN^i \leftarrow H(SN^{i-1}||H^i(Rnd_v))$
5: **end if**

Issuing Pseudonyms (by the PCA)

Protocol 1 Issuing Pseudonyms (by the PCA)

1: **procedure** IssuePsnyms(Req)
2: $Req \rightarrow (Id_{req}, t_s, t_e, (tkt)_{\sigma_{ltca}}, \{(K_v^1)_{\sigma_{k_v^1}}, \cdots, (K_v^n)_{\sigma_{k_v^n}}\}, nonce, t_{now})$
3: Verify($\mathrm{LTC}_{ltca}, (tkt)_{\sigma_{ltca}}$)
4: $Rnd_v \leftarrow GenRnd()$
5: **for** i:=1 to **n do**
6: **Begin**
7: Verify($K_v^i, (K_v^i)_{\sigma_{k_v^i}}$)
8: $RIK_{P_v^i} \leftarrow H(IK_{tkt}||K_v^i||t_s^i||t_e^i||H^i(Rnd_v))$
9: **if** $i = 1$ **then**
10: $SN^i \leftarrow H(RIK_{P_v^i}||H^i(Rnd_v))$
11: **else**
12: $SN^i \leftarrow H(SN^{i-1}||H^i(Rnd_v))$
13: **end if**
14: $\zeta \leftarrow (SN^i, K_v^i, CRL_v, BF_{\Gamma^i_{CRL}}, RIK_{P_v^i}, t_s^i, t_e^i)$
15: $(P_v^i)_{\sigma_{pca}} \leftarrow Sign(Lk_{pca}, \zeta)$
16: **End**
17: **return** $(Id_{res}, \{(P_v^1)_{\sigma_{pca}}, \ldots, (P_v^n)_{\sigma_{pca}}\}, Rnd_v, nonce{+}1, t_{now})$
18: **end procedure**

CRL Construction (by the PCA)

Protocol 2 CRL Construction (by the PCA)

1: **procedure** GENCRL($\Gamma^{i}_{CRL}, \mathbb{B}$)
2: $Piece_{\Gamma^{i}_{CRL}} \leftarrow \emptyset$
3: **repeat**
4: $\{SN^{k}_{P}, H^{k}_{Rnd_v}, n\} \leftarrow fetchRevokedPsnyms(\Gamma^{i}_{CRL})$ ▷ k: the revoked
5: **if** $SN^{k}_{P} \neq Null$ **then**
6: $Piece_{\Gamma^{i}_{CRL}} \leftarrow Append(\{SN^{k}_{P}, H^{k}_{Rnd_v}, n\})$
7: **end if**
8: **until** $SN^{k}_{P} == Null$
9: $N \leftarrow \left\lceil \frac{size(Piece_{\Gamma^{i}_{CRL}})}{\mathbb{B}} \right\rceil$ ▷ calculating number of pieces with a given $\mathbb{B}$
10: **for** $j \leftarrow 0, N$ **do** ▷ N: number of pieces in Γ^{i}_{CRL}
11: $Piece^{j}_{\Gamma^{i}_{CRL}} \leftarrow Split(Piece_{\Gamma^{i}_{CRL}}, \mathbb{B}, N)$ ▷ splitting into N pieces
12: **end for**
13: **return** $\{(Piece^{1}_{\Gamma^{i}_{CRL}}), \ldots, (Piece^{N}_{\Gamma^{i}_{CRL}})\}$
14: **end procedure**

Publishing CRLs (by the OBUs)

Protocol 3 Publishing CRLs (by the OBUs)

1: **procedure** PUBLISHCRL() ▷ The g.c.d. of a and b
2: $\{(Id_{req}, \Gamma^{i}_{CRL}, [indexes])\} = receiveQuery((\zeta)_{\sigma_{P^{i}_{v}}})$
3: $Verify(P^{i}_{v}, (\zeta)_{\sigma_{P^{i}_{v}}})$
4: $CRL^{*}_{\Gamma^{i}_{CRL}} = search_{local}(\Gamma^{i}_{CRL})$ ▷ search local repository
5: $j \leftarrow rand(0, *)$ ▷ randomly select one of the available pieces
6: **if** $CRL^{j}_{\Gamma^{i}_{CRL}} \neq \emptyset$ **then**
7: $broadcast(\{Id_{res}, CRL^{j}_{\Gamma^{i}_{CRL}}\})$
8: **end if**
9: **end procedure**

Subscribing to CRL Pieces (by the OBUs)

Protocol 4 Subscribing to CRL Pieces (by the OBUs)

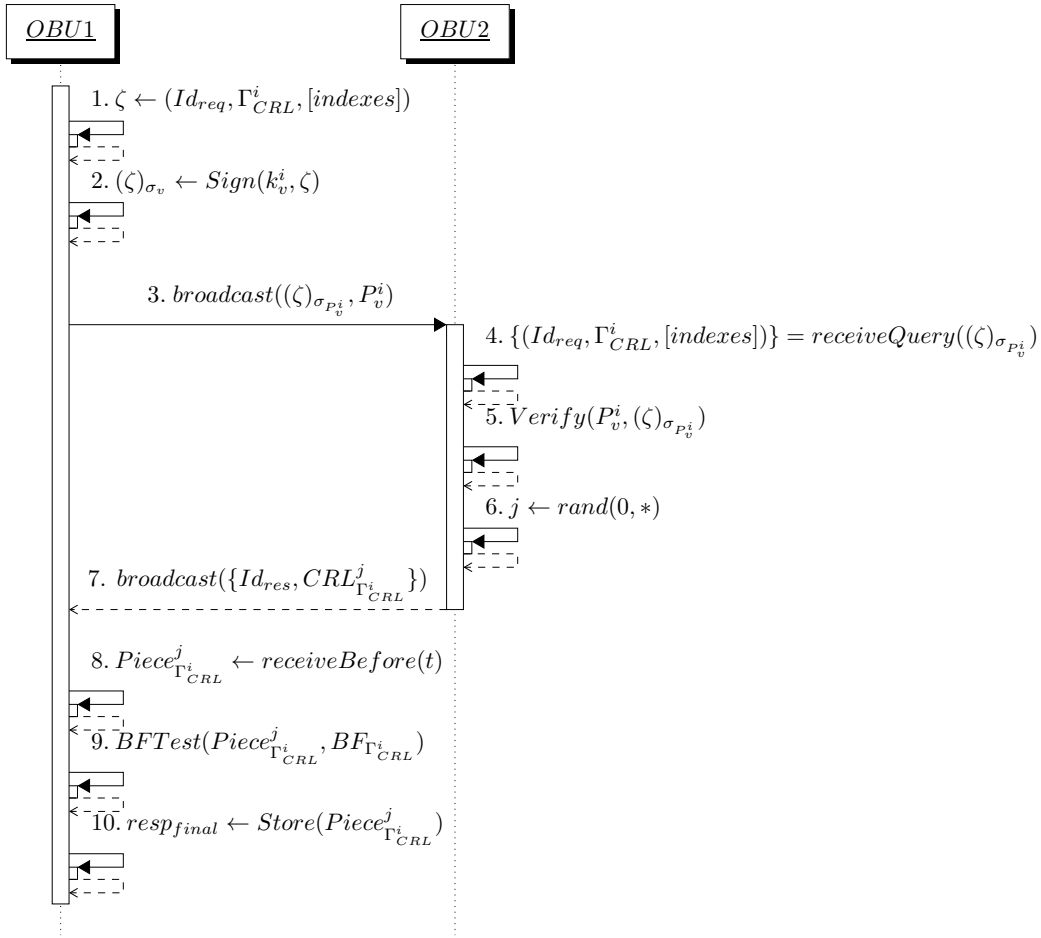
1: **procedure** SUBSCRIBECRL(Γ^i_{CRL}, N)
2: $resp_{final} \leftarrow \emptyset, j \leftarrow 0, t \leftarrow t_{now} + T_{timeout}$
3: **repeat**
4: $\zeta \leftarrow (Id_{req}, \Gamma^i_{CRL}, [missing\ pieces\ indexes])$
5: $(\zeta)_{\sigma_v} \leftarrow Sign(k^i_v, \zeta)$
6: $broadcast((\zeta)_{\sigma_{P^i_v}}, P^i_v)$
7: $Piece^j_{\Gamma^i_{CRL}} \leftarrow receiveBefore(t)$
8: **if** $BFTest(Piece^j_{\Gamma^i_{CRL}}, BF_{\Gamma^i_{CRL}})$ **then**
9: $resp_{final} \leftarrow Store(Piece^j_{\Gamma^i_{CRL}})$ ▷ storing in local repository
10: **end if**
11: $j \leftarrow j + 1$
12: **until** $j > N$
13: **return** $resp_{final}$
14: **end procedure**

Parsing a CRL Piece (by the OBUs)

Protocol 5 Parsing a CRL Piece (by the OBUs)

1: **procedure** PARSECRL($Piece^{j}_{\Gamma^{i}_{CRL}}$)
2: $\{SN^{k}, H^{k}(Rnd_{v}), n\}_{N} \leftarrow Piece^{j}_{\Gamma^{i}_{CRL}}$ ▷ N: Number of Entires
3: $CRL_{\Gamma^{i}_{CRL}} \leftarrow \emptyset$
4: **for** $t \leftarrow 0, N$ **do** ▷ N: Total number of CRL pieces
5: **for** $j \leftarrow 0, n$ **do** ▷ n: Number of remaining psnyms in each batch
6: $SN^{j+1} \leftarrow H(SN^{j}||H^{j}(Rnd_{v}))$
7: $CRL_{\Gamma^{i}_{CRL}} \leftarrow Append(H(SN^{j}||H^{j}(Rnd_{v})))$
8: **end for**
9: **end for**
10: **return** $CRL_{\Gamma^{i}_{CRL}}$
11: **end procedure**

CRL Publish/Subscribe



Δ-CRL Construction (by the PCA)

1: **procedure** GENDELTACRL($\Gamma^{j}_{CRL}, i, K_i, \mathbb{B}, t_{now}$)
2: $Piece^{\Delta_i}_{\Gamma^{j}_{CRL}} \leftarrow \emptyset$
3: **repeat** ▷ Fetching revoked pseudonym, not included in base-CRL
4: $SN_P \leftarrow fetchRevokedPsnyms(\Gamma^{j}_{CRL}, i, t_{now})$
5: **if** $SN_P \neq Null$ **then**
6: $Piece^{\Delta_i}_{\Gamma^{j}_{CRL}} \leftarrow Append(SN_P)$
7: **end if**
8: **until** $SN_P == Null$
9: $K_{i-1} \leftarrow H(K_i)$ ▷ Calculating the key for interval $i-1$
10: $K'_i \leftarrow H'(K_i)$ ▷ Calculating the key for interval i
11: $N \leftarrow \left\lceil \frac{size(Piece^{\Delta_i}_{\Gamma^{j}_{CRL}})}{\mathbb{B}} \right\rceil$ ▷ Calculating number of pieces
12: **for** $w \leftarrow 0, N$ **do** ▷ N: number of pieces
13: $\zeta \leftarrow Split(Piece^{\Delta_i}_{\Gamma^{j}_{CRL}}, \mathbb{B}, N)$
14: $Piece^{\Delta^{w}_i}_{\Gamma^{j}_{CRL}} \leftarrow \{\zeta || MAC(K'_i, \zeta) || K_{i-1}\}$
15: **end for**
16: **return** $\{(Piece^{\Delta^{1}_i}_{\Gamma^{j}_{CRL}}), \ldots, (Piece^{\Delta^{N}_i}_{\Gamma^{j}_{CRL}})\}$
17: **end procedure**

Parsing a CRL Piece (by the OBUs)

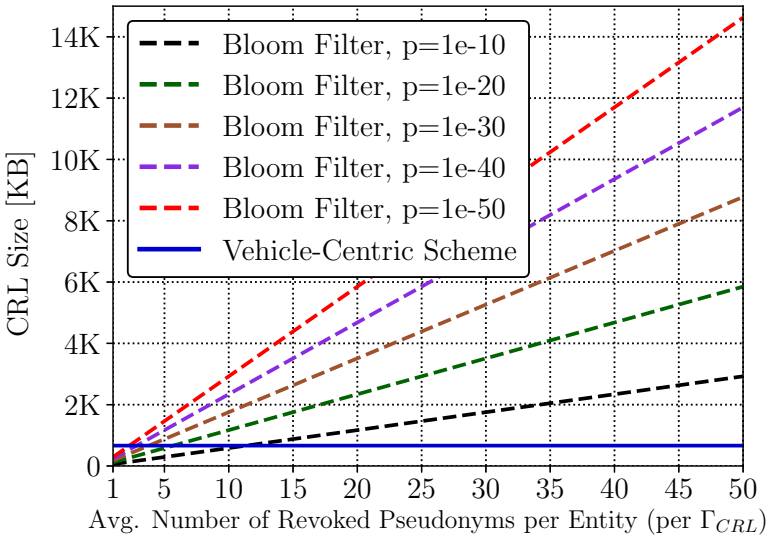
1: **procedure** PARSECRL($Piece^{j}_{\Gamma^{i}_{CRL}}, N$)
2: $\quad \{SN_z, Rnd_z, n_z\}_N \leftarrow Piece^{j}_{\Gamma^{i}_{CRL}}$
3: $\quad CRL_{\Gamma^{i}_{CRL}} \leftarrow \emptyset$
4: $\quad$ **for** $z \leftarrow 1, N$ **do** ▷ N: Number of entries in this piece
5: $\quad\quad$ **for** $w \leftarrow 1, n_z$ **do** ▷ n: Number of remaining pseudonyms
6: $\quad\quad\quad CRL_{\Gamma^{i}_{CRL}} \leftarrow Append(H(SN_z || H^{w}_{z}(Rnd_z)))$
7: $\quad\quad\quad SN_z \leftarrow H(SN_z || H^{w}_{z}(Rnd_z))$
8: $\quad\quad$ **end for**
9: $\quad$ **end for**
10: $\quad$ **return** $CRL_{\Gamma^{i}_{CRL}}$
11: **end procedure**

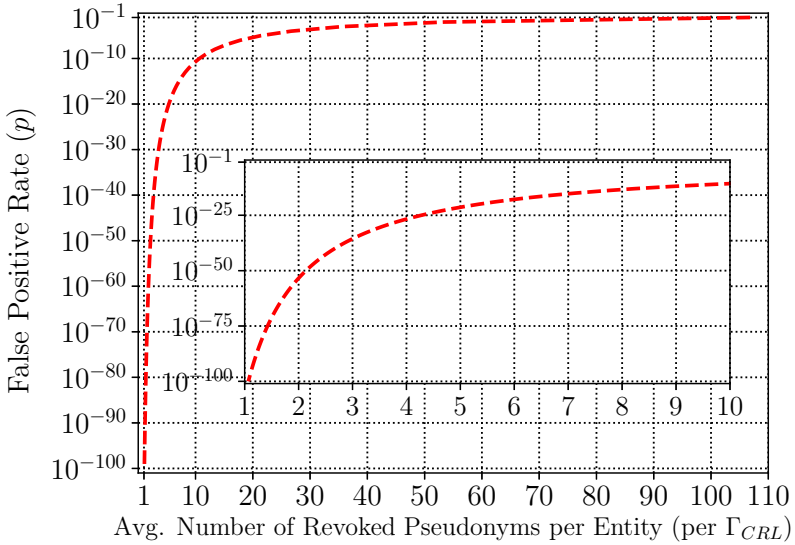
Outline

Qualitative Analysis

- ✓ *Fine-grained authentication, integrity, and non-repudiation:* signed fingerprints
- ✓ *Unlinkability (perfect-forward-privacy):* multi-session pseudonym requests, timely-aligned pseudonym lifetime, utilization of hash chains
- ✓ *Availability:* leveraging RSUs and car-to-car epidemic distribution
- ✓ *Efficiency:* Efficient construction of fingerprints, fast validation per piece, and implicitly binding of a batch
- ✓ *Explicit and/or implicit notification on revocation events:* Broadcasting signed fingerprints, also integrated into a subset of recently issued pseudonyms

Qualitative Analysis (cont'd)



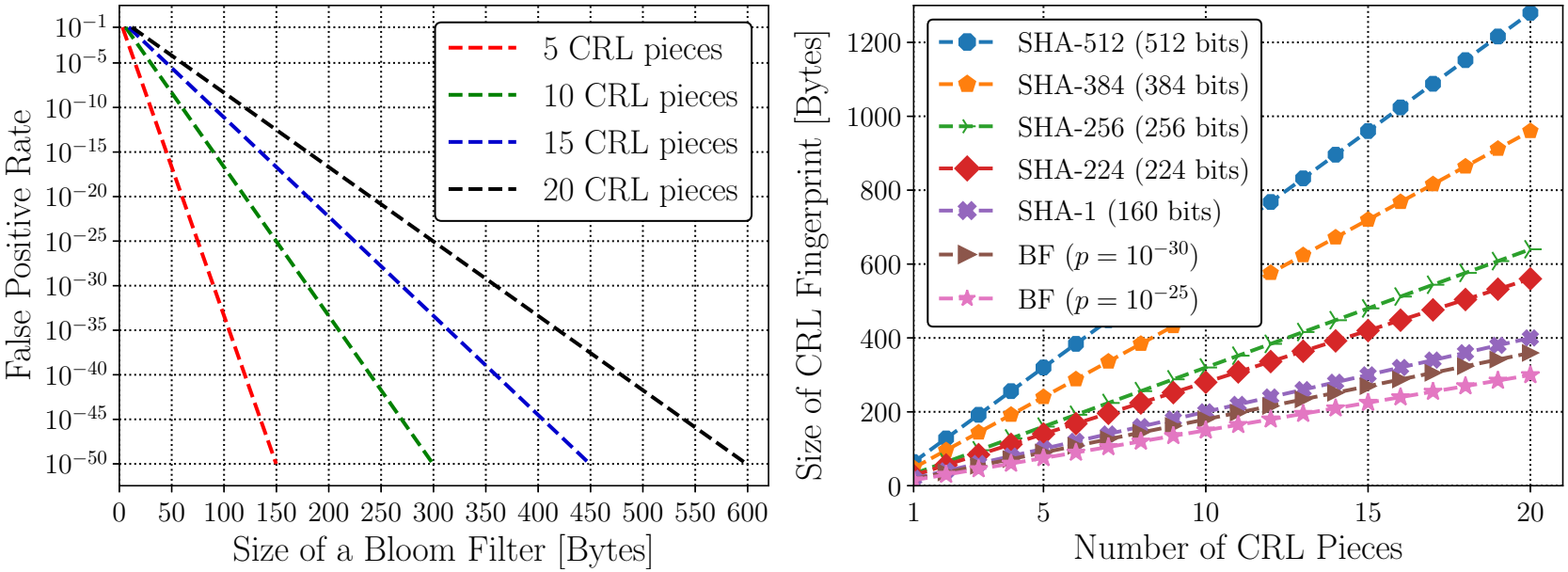


(a) CRL size comparison **(b)** C^{2}RL [6] as a factor of false positive rate

Figure: (a) CRL size comparison for C^{2}RL and vehicle-centric scheme (10,000 revoked vehicles). (b) Achieving vehicle-centric comparable CRL size for the C^{2}RL scheme.

- $m_{BF} = -\frac{N \times M \times ln\, p}{(ln2)^2}$, N is the total number of compromised vehicles, M is the average number of revoked pseudonyms per vehicle per Γ_{CRL}.
- Significant improvement over C^{2}RL: 2.6x reduction in CRL size when $M = 10$ and $p = 10^{-30}$.

Qualitative Analysis (cont'd)



(a) Vehicle-centric scheme **(b)** Precode-and-hash scheme [8]

Figure: Extra overhead for CRL fingerprints.

Qualitative Analysis (cont'd)

- 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)

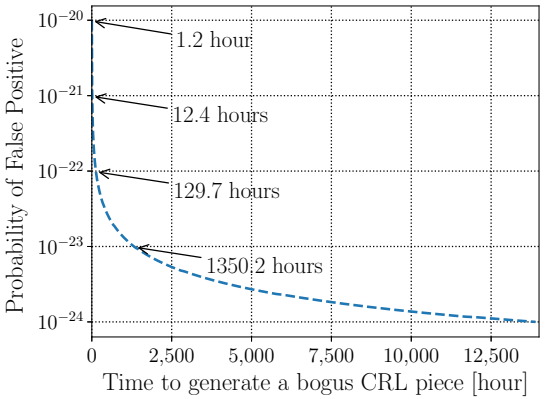


Figure: Query-only attack on the CRL fingerprints; adversary's computational power is $1.6 \times 10^{18} TH/sec$.

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 ($\frac{10^{23} \times 76}{1.6 \times 10^{18}} = 1,319h$)

Qualitative Analysis (cont'd)

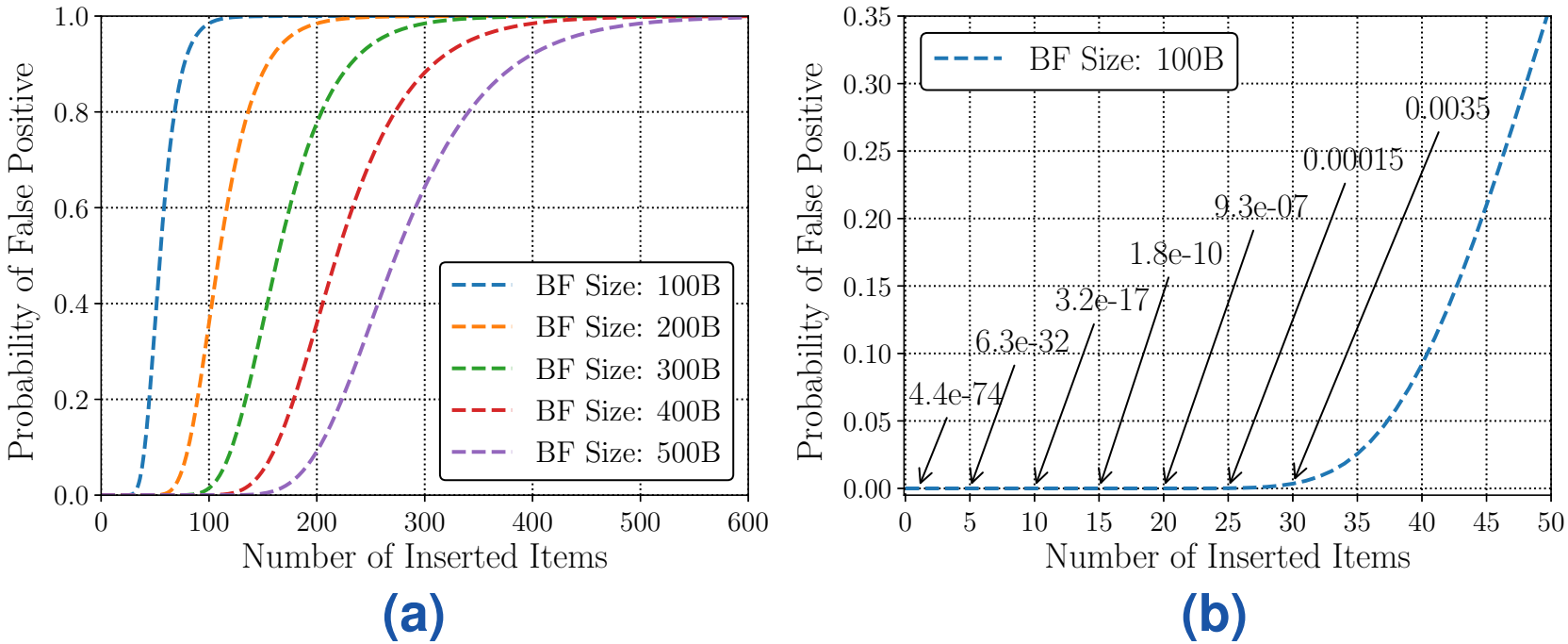


Figure: Chosen-insertion attack on the CRL fingerprint.

Outline

Quantitative Analysis

- OMNET++ & Veins framework using SUMO
- Cryptographic protocols and primitives (OpenSSL): Elliptic Curve Digital Signature Algorithm (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 range
- Comparison with the *baseline* scheme [9]: under the same assumptions and configuration with the same parameters
- Evaluation of: efficiency (latency), resilience (to pollution/DoS attacks), resource consumption (computation/communication)

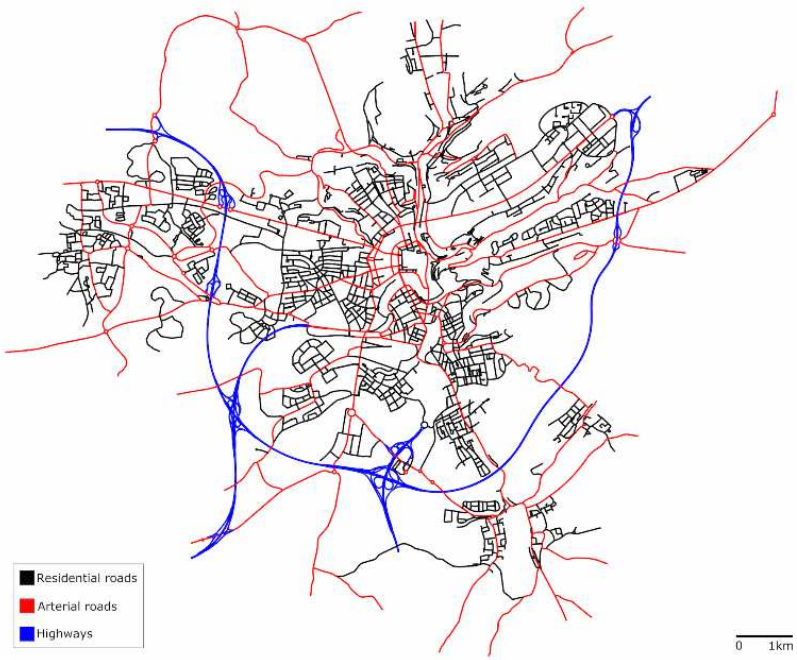


Figure: The LuST dataset, a full-day realistic mobility pattern in the city of Luxembourg (15KM x 15KM) [Codeca et al. (2015)].

Quantitative Analysis (cont'd)

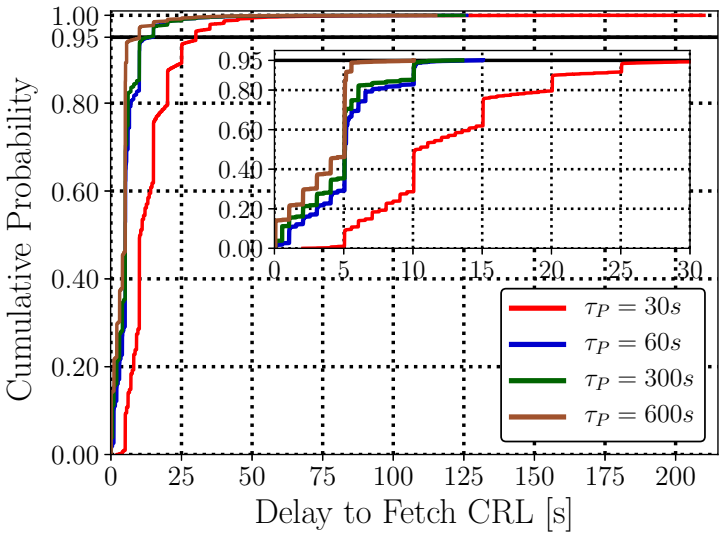
Table: Simulation Parameters (LuST dataset).

Parameters	Value	Parameters	Value
CRL/Fingerprint TX interval	0.5s/5s	Pseudonym lifetime	30s-600s
Carrier frequency	5.89 GHz	Area size	15 KM $\times$ 15 KM
TX power	20mW	Number of vehicles	138,259
Physical layer bit-rate	18Mbps	Number of trips	287,939
Sensitivity	-89dBm	Average trip duration	692.81s
Thermal noise	-110dBm	Duration of simulation	4 hour (7-9, 17-19)
CRL dist. Bandwidth ($\mathbb{B}$)	10, 25, 50 KB/s	Γ	1-60 min
Number of RSUs	100	Γ_{CRL}	60 min

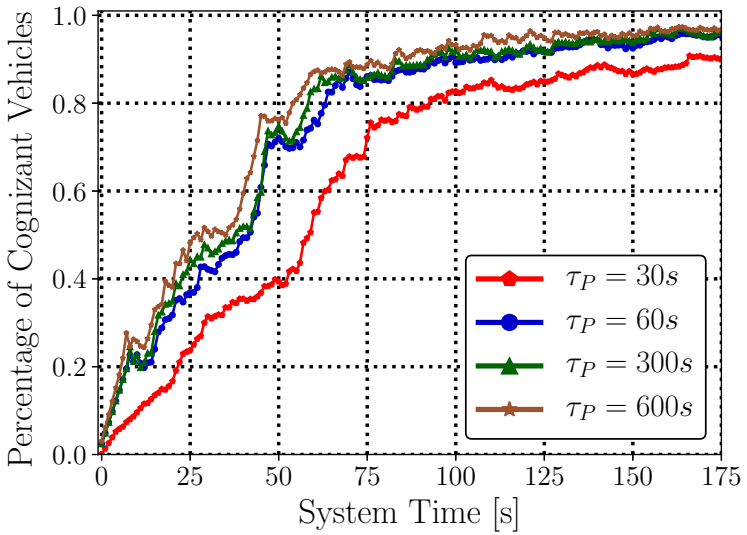
Table: LuST Revocation Information ($\mathbb{R} = 1\%$, $\mathbb{B} = 10KB/s$).

Pseudonym Lifetime	Number of Psnyms	Number of Revoked Psnyms	Average Number per Γ_{CRL}	Number of Pieces
τ_P=30s	3,425,565	34,256	1,428	12
τ_P=60s	1,712,782	17,128	710	6
τ_P=300s	342,556	3,426	143	2
τ_P=600s	171,278	1,713	72	1

Quantitative Analysis (cont'd)



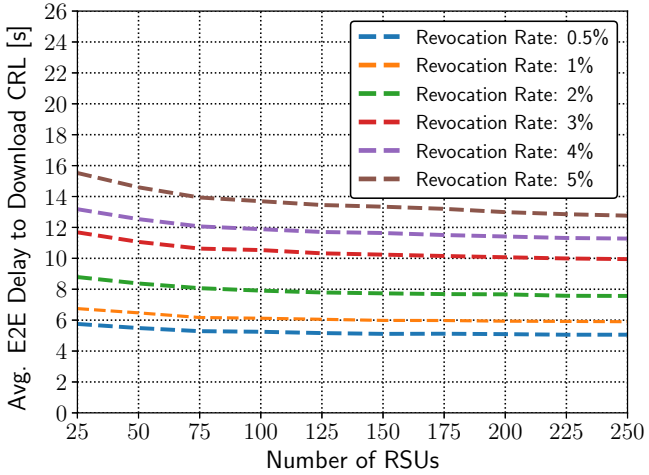
(a) Vehicle-centric scheme ($\mathbb{B}$ =10 KB/s)



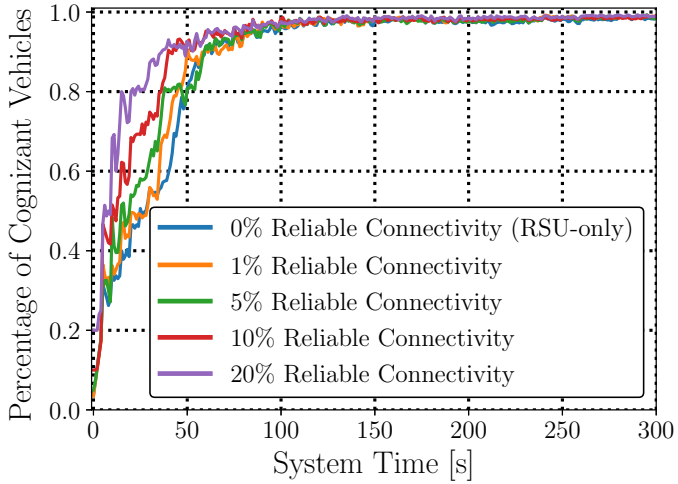
(b) Vehicle-centric scheme ($\mathbb{B}$ =10 KB/s)

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

Quantitative Analysis (cont'd)



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

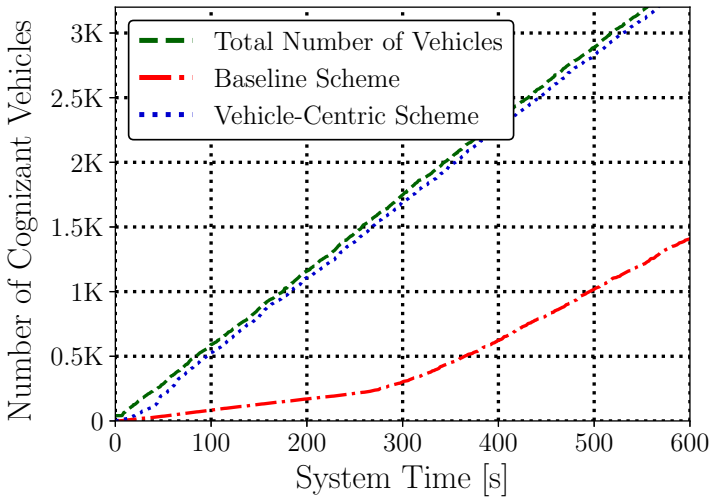


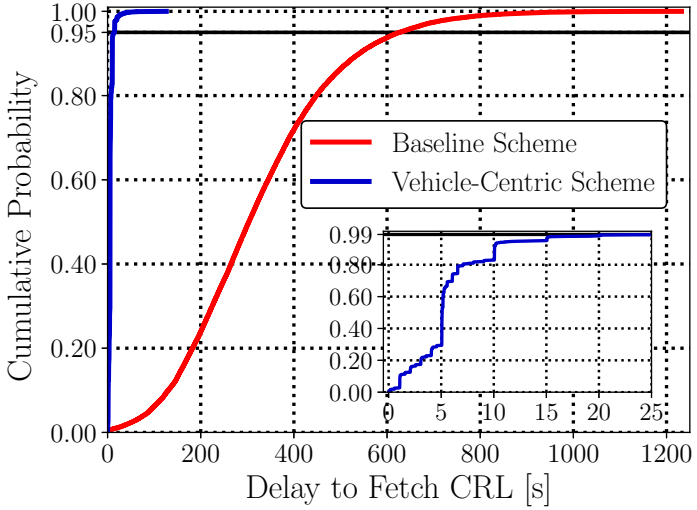
(b) Vehicle-centric scheme (TX =5s)

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 [8], or broadcasted by RSUs (365 bytes with $TX = 5s$) and, in addition, integrated into a subset of pseudonyms with 36 bytes of extra overhead ($p = 10^{-30}$, $\mathbb{R} = 0.5\%$).

Quantitative Analysis (cont'd)





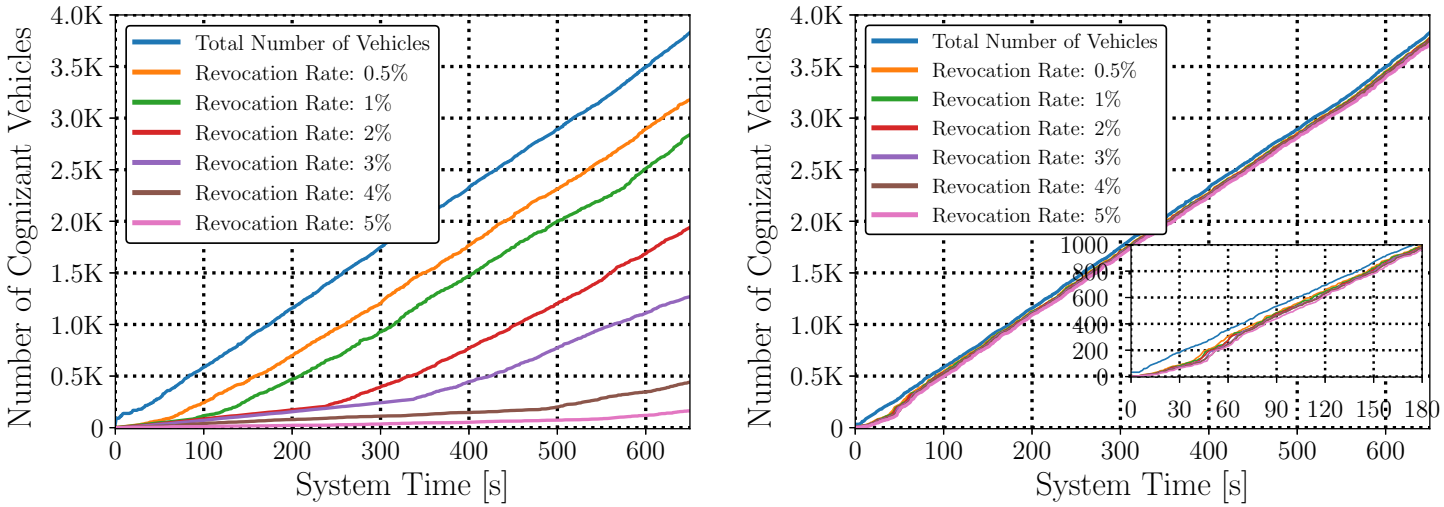
(a) 7:00-7:10 am ($\mathbb{B}$ =25 KB/s) **(b)** 7-9 am, 5-7 pm ($\mathbb{B}$ =25 KB/s)

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)

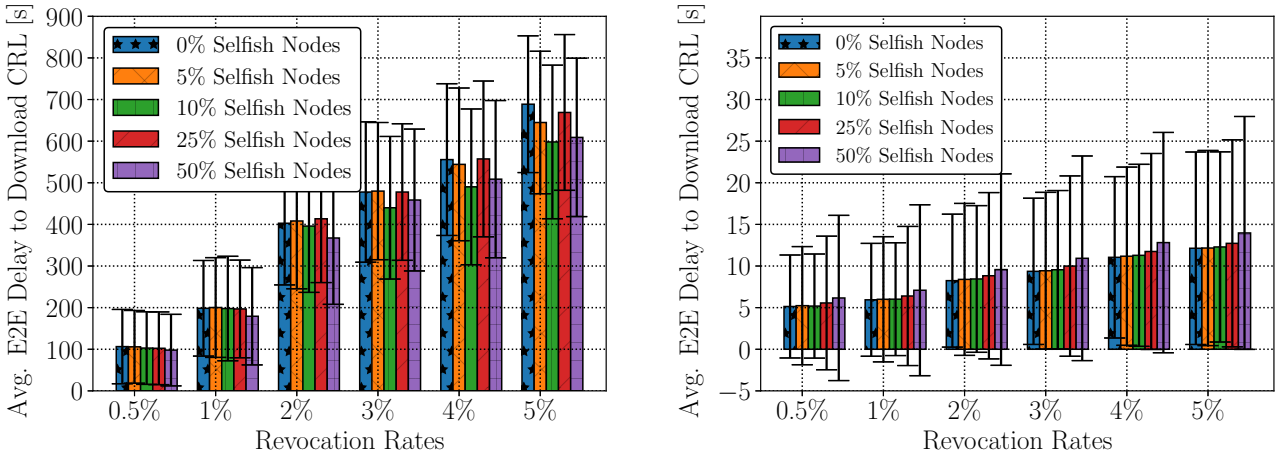


(a) Baseline scheme ($\mathbb{B}$ =50 KB/s) **(b)** Vehicle-centric scheme ($\mathbb{B}$ =50 KB/s)

Figure: Cognizant vehicles with different revocation rates.

- $\mathbb{T}$: the total number of pseudonyms; $\mathbb{R}$: the revocation rate.
- Size of CRLs for the Baseline: $\mathbb{T} \times \mathbb{R}$, linearly increases with $\mathbb{R}$
- Size of an *effective CRL* for vehicle-centric: $\frac{\mathbb{T} \times \mathbb{R}}{|\Gamma_{CRL}|}$, where $|\Gamma_{CRL}|$ is the number of intervals in a day, e.g., $|\Gamma_{CRL}|$ is 24 when $\Gamma_{CRL} = 1$h.

Quantitative Analysis (cont'd)

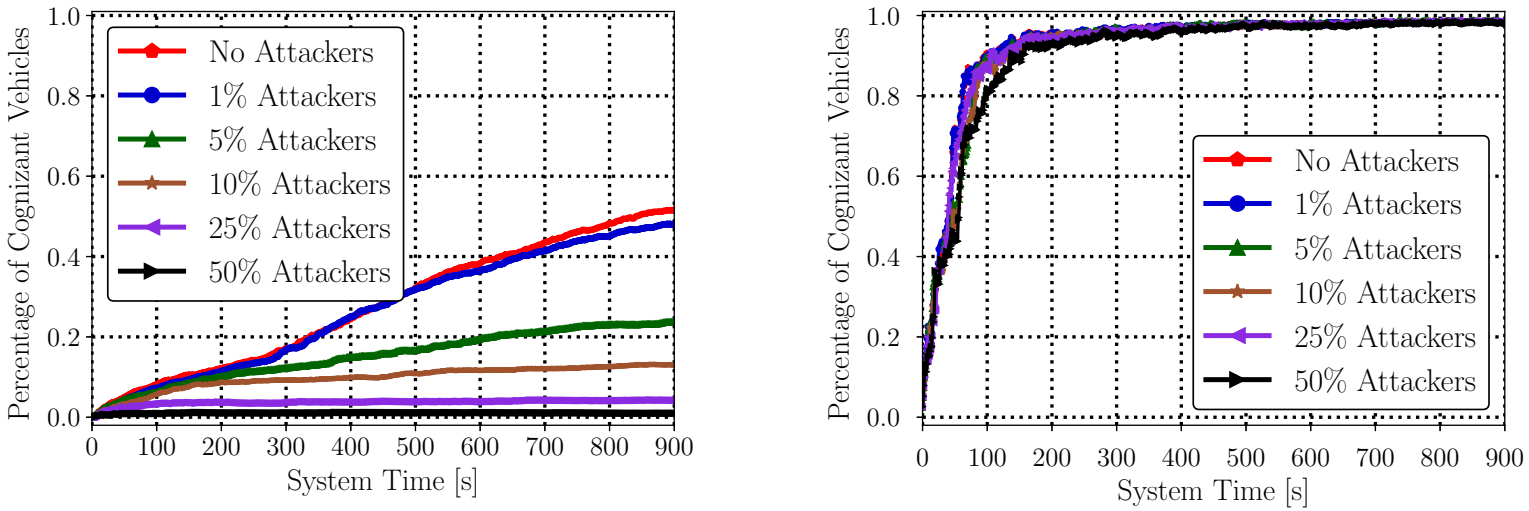


(a) Baseline scheme **(b)** Vehicle-centric scheme

Figure: Resilience comparison against selfish nodes with different revocation rates (7:00-7:30, $\tau_p = 30s$, $\mathbb{B} = 50KB/s$).

- Selfish nodes do not perform any ‘‘active’’ attacks; rather, they become silent and they never respond to a CRL piece request.

Quantitative Analysis (cont'd)

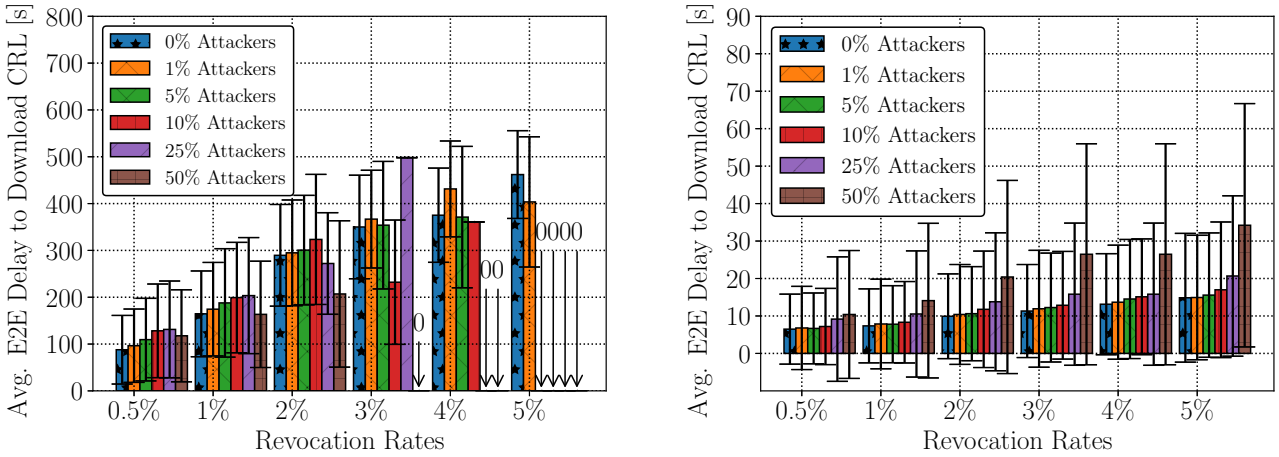


(a) Baseline scheme ($\mathbb{B}$ =25 KB/s) **(b)** Vehicle-centric scheme ($\mathbb{B}$ =25 KB/s)

Figure: Resilience comparison against DoS attacks.

- Attackers periodically broadcast fake CRL pieces once every 0.5 second.
- The resilience to pollution and DoS 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

Quantitative Analysis (cont'd)

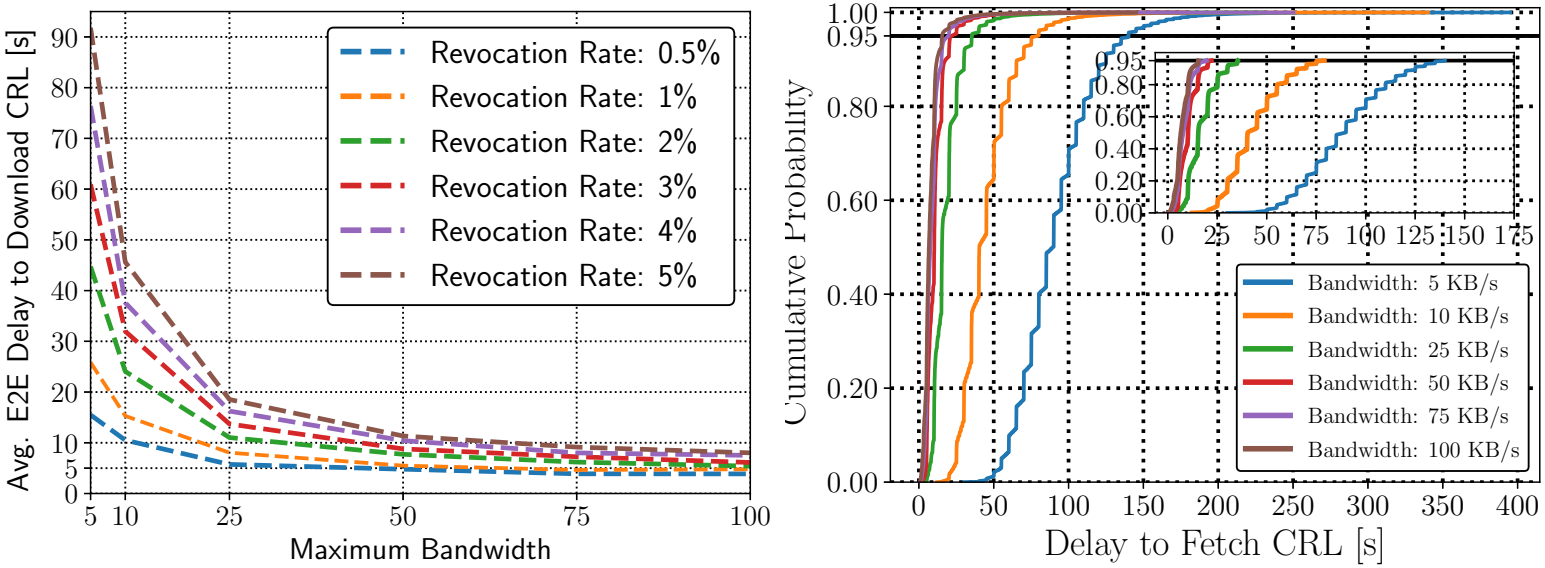


(a) Baseline scheme **(b)** Vehicle-centric scheme

Figure: Resilience comparison against pollution and DoS attacks with different revocation rates (7:00-7:10, $\tau_p = 30s$, $\mathbb{B} = 50KB/s$).

- Attackers periodically broadcast fake CRL pieces once every 0.5 second.
- The resilience to pollution and DoS 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

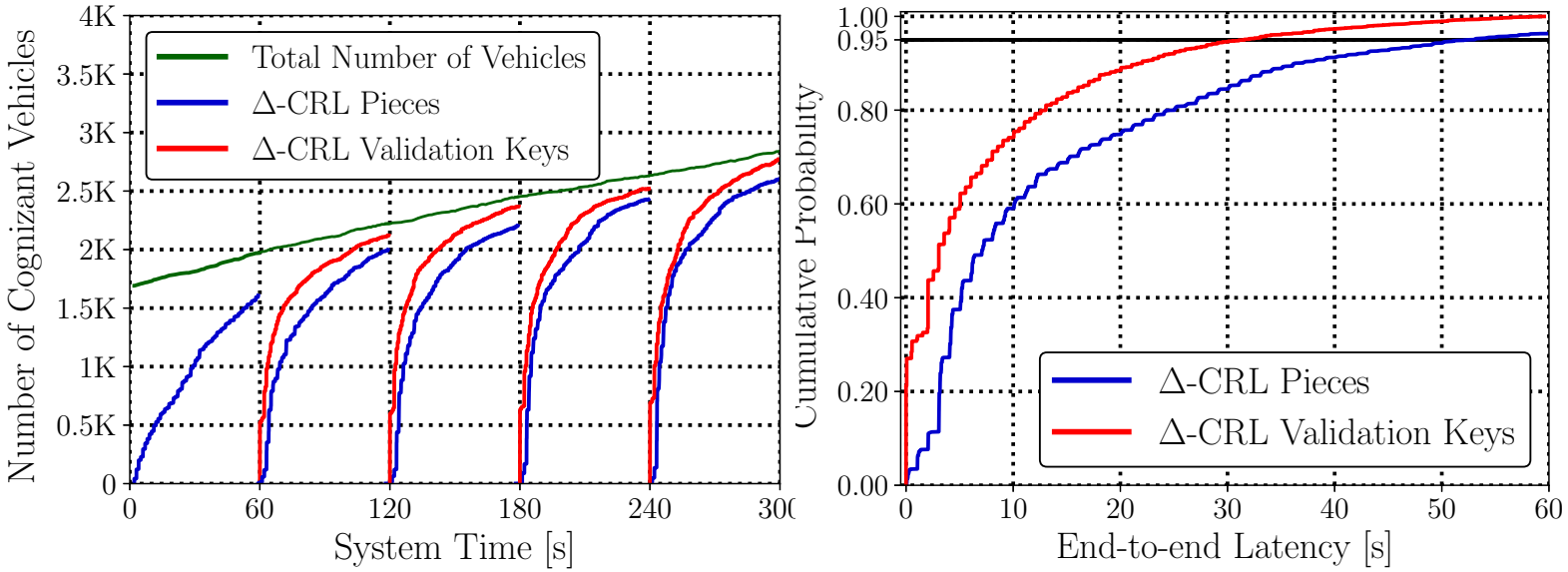
Quantitative Analysis (cont'd)



(a) Vehicle-centric scheme **(b)** Vehicle-centric scheme

Figure: (a) Bandwidth-delay trade off ($\tau_P = 60s$). (b) CDF of end-to-end delay with different bandwidth ($\tau_P = 30s$, $\mathbb{R} = 5\%$).

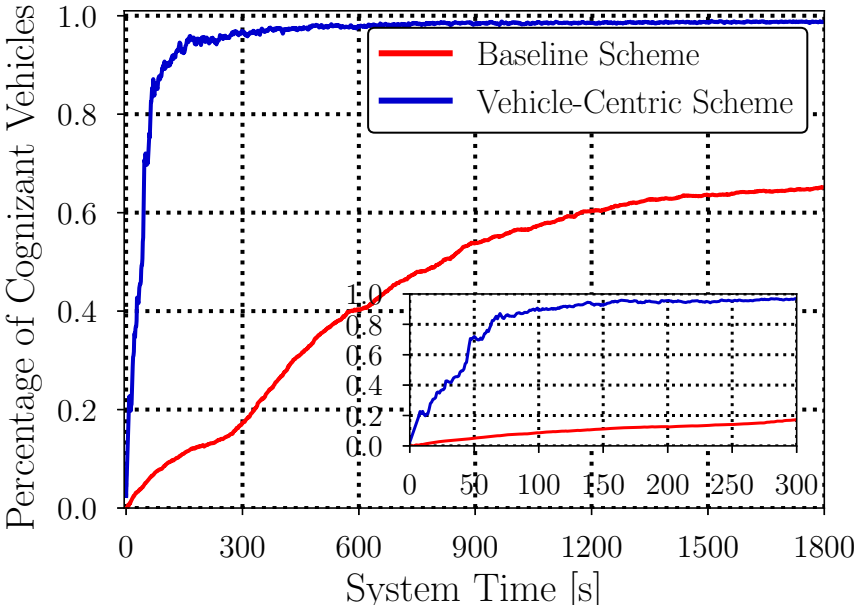
Quantitative Analysis (cont'd)



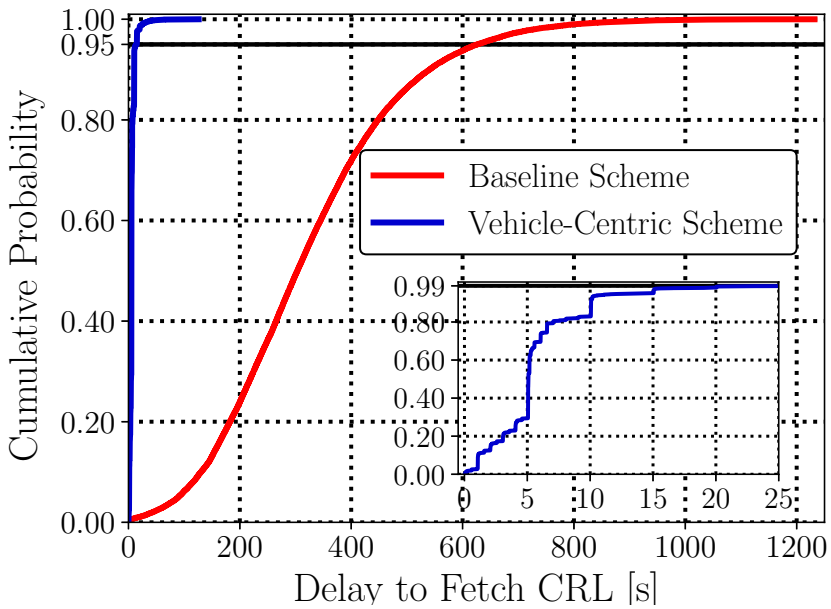
(a) 7:05-7:10 am ($\mathbb{B}$ =10 KB/s) **(b)** 7:05-7:10 am ($\mathbb{B}$ =10 KB/s)

Figure: End-to-end delay to fetch Δ-CRL pieces and validation keys for vehicle-centric scheme ($\tau_P = 60$ sec., $\mathbb{R} = 5\%$, $\gamma_{key} = 0.5$, $\gamma_{piece} = 2$).

Quantitative Analysis (cont'd)



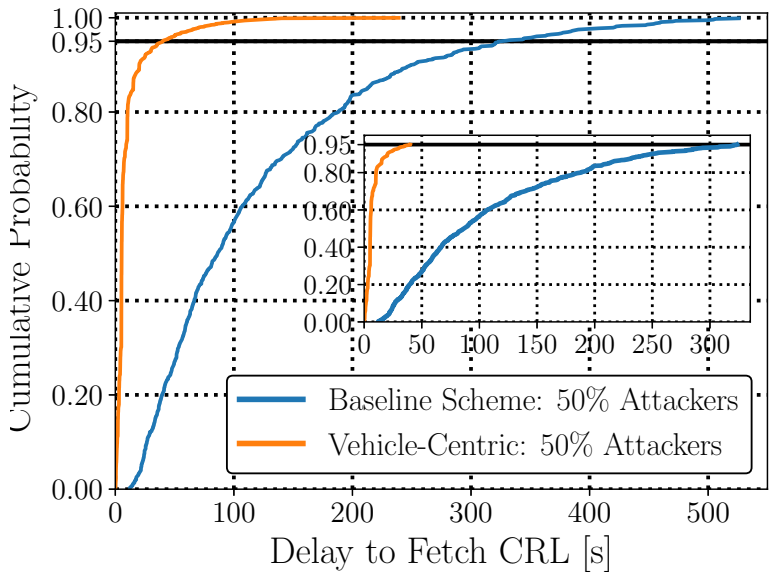
(a) 7:00-7:10 am ($\mathbb{B}$ =25 KB/s)



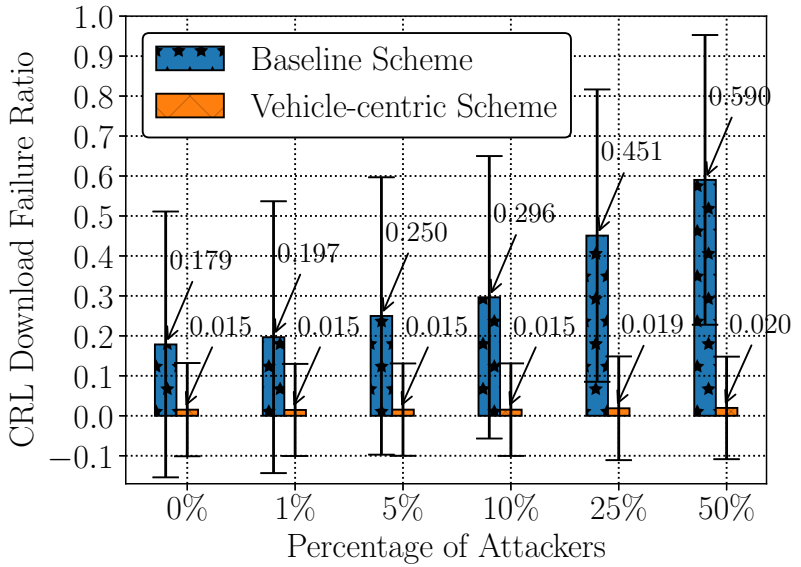
(b) 7-9 am, 5-7 pm ($\mathbb{B}$ =25 KB/s)

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

Quantitative Analysis (cont'd)



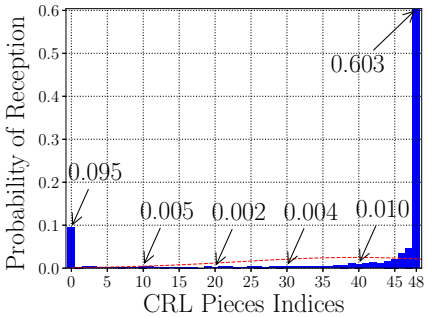
(a) CDF of delays under a DoS attack



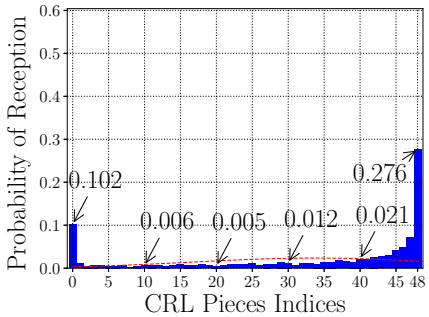
(b) Probability of failure

Figure: (a) CDF of latency to successfully obtain CRL pieces (50% attackers). (b) CRL download failure ratio as a function of DoS attackers ($\tau_P = 30s$, $\mathbb{B} = 50KB/s$).

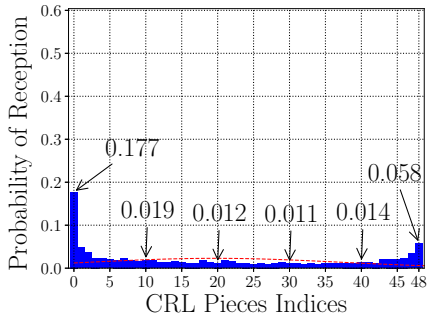
Quantitative Analysis (cont'd)



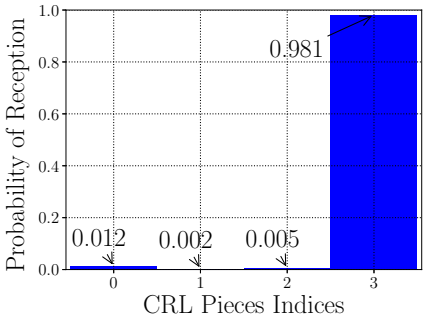
(a) Baseline: no attackers



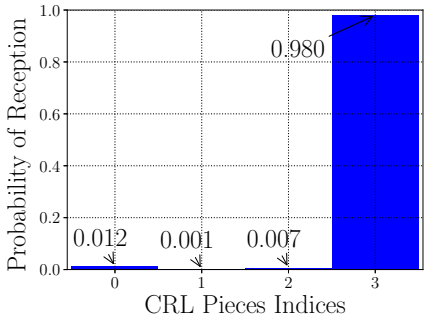
(b) Baseline: 10% attackers



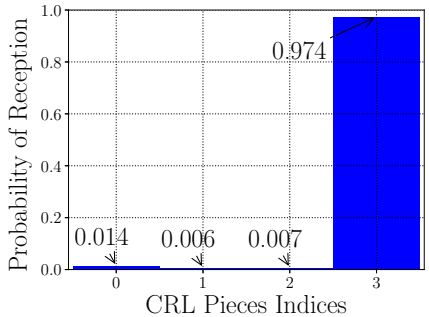
(c) Baseline: 50% attackers



(d) Vehicle-centric: no attackers



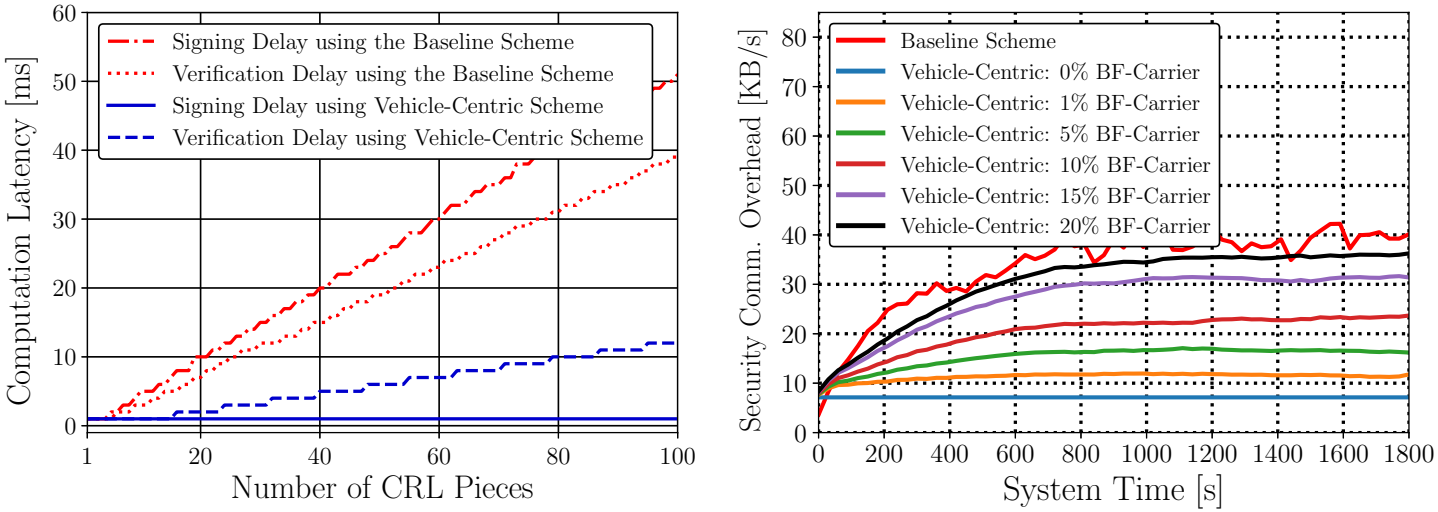
(e) Vehicle-centric: 10% attackers



(f) Vehicle-centric: 50% attackers

Figure: Probability of successful CRL pieces reception ($\tau_P = 30s$, $\mathbb{B} = 50KB/s$). (a) and (d): no attacks. (b), (c), (e), (f): under a DoS attack.

Quantitative Analysis (cont'd)



(a) End-to-end latency **(b)** Cryptographic overhead

Figure: (a) Computation latency comparison. (b) Security overhead comparison, averaged every 30s ($\mathbb{R}$=1%, $\mathbb{B}$ = 50KB/s).

- Cryptographic protocols were executed on a VM (dual-core 2.0 GHz).
- Signed fingerprint broadcasted every 5s via RSUs (365 bytes long), also integrated into a subset of pseudonyms (36 bytes extra overhead, $p = 10^{-30}$).

Outline

Conclusion

- A practical framework to effectively distribute CRLs in VC systems
- Highly efficient, scalable, and resilient design
- Viable solution towards catalyzing the deployment of the secure and privacy-protecting VC systems

Bibliography

[1] P. Papadimitratos and et al, ‘‘Securing Vehicular Communications-Assumptions, Requirements, and Principles,’’ in *ESCAR*, Berlin, Germany, Nov. 2006.

[2] ------, ‘‘Secure Vehicular Communication Systems: Design and Architecture,’’ *IEEE Comm. Mag.*, vol. 46, no. 11, pp. 100--109, Nov. 2008.

[3] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, ‘‘A Security Credential Management System for V2V Communications,’’ in *IEEE VNC*, Boston, MA, Dec. 2013.

[4] V. Kumar and et al, ‘‘Binary Hash Tree based Certificate Access Management for Connected Vehicles,’’ in *ACM WiSec*, Boston, USA, July 2017.

[5] M. Khodaei, H. Jin, and P. Papadimitratos, ‘‘SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,’’ *IEEE T-ITS*, vol. 19, no. 5, pp. 1430--1444, May 2018.

[6] M. Raya and et al, ‘‘Certificate Revocation in Vehicular Networks,’’ *Technical Report, EPFL, Switzerland*, 2006.

[7] S. Tarkoma and et al, ‘‘Theory and Practice of Bloom Filters for Distributed Systems,’’ *IEEE Communications Surveys & Tutorials*, vol. 14, no. 1, pp. 131--155, Apr. 2011.

[8] V.-T. Nguyen and et al, ‘‘Secure Content Distribution in Vehicular Networks,’’ *arXiv preprint arXiv:1601.06181*, Jan. 2016, Accessed Date: 30-July-2017.

[9] 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.

[10] M. Khodaei and P. Papadimitratos, ‘‘Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs,’’ in *ACM WiSec*, Stockholm, Sweden, June 2018.

Scalable & Resilient Vehicle-Centric Certificate Revocation List Distribution in Vehicular Communication Systems

Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group (NSS)
www.eecs.kth.se/nss

In IEEE Transactions on Mobile Computing (TMC), 2020.