Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs

Mohammad Khodaei and Panos Papadimitratos

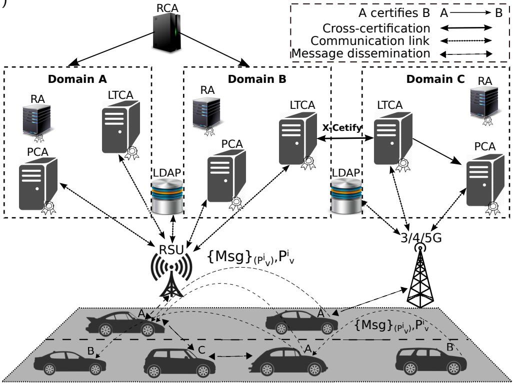
Networked Systems Security Group (NSS)
www.ee.kth.se/nss

Royal Institute of Technology (KTH)
Stockholm, Sweden

June 20, 2018

Secure Vehicular Communication (VC) Systems

- Vehicular Public-Key Infrastructure (VPKI)
- Root CA (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



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 (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

System Model and Assumptions

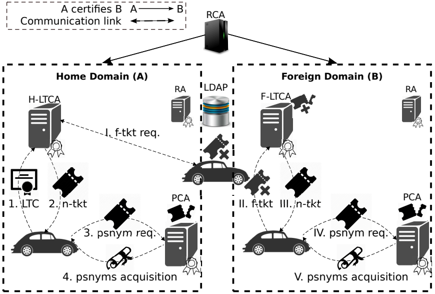


Figure: Pseudonym acquisition overview in the home and foreign domains.

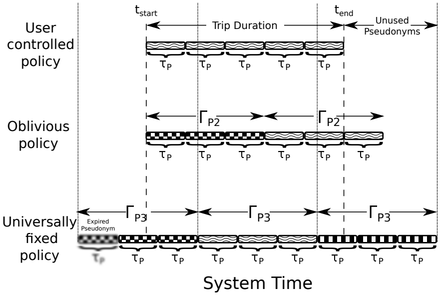


Figure: Pseudonym Acquisition Policies.

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

Vehicle-Centric CRL Distribution

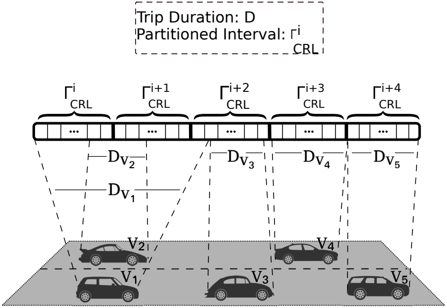


Figure: CRL as a Stream:

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

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

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

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

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

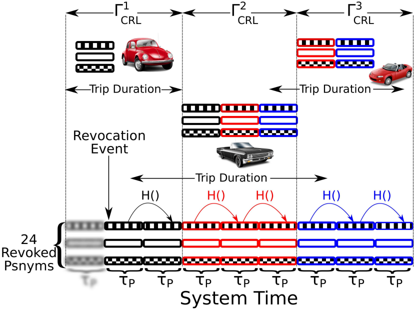


Figure: A vehicle-centric approach: each vehicle only subscribes for pieces of CRLs corresponding to its trip duration.

Vehicle-Centric CRL Distribution (cont'd)

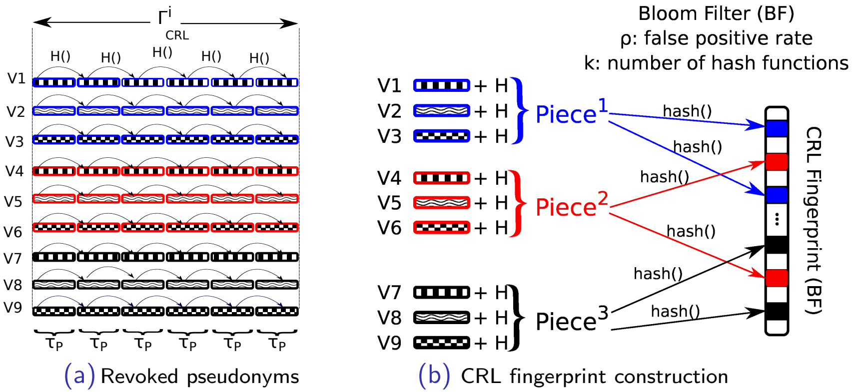
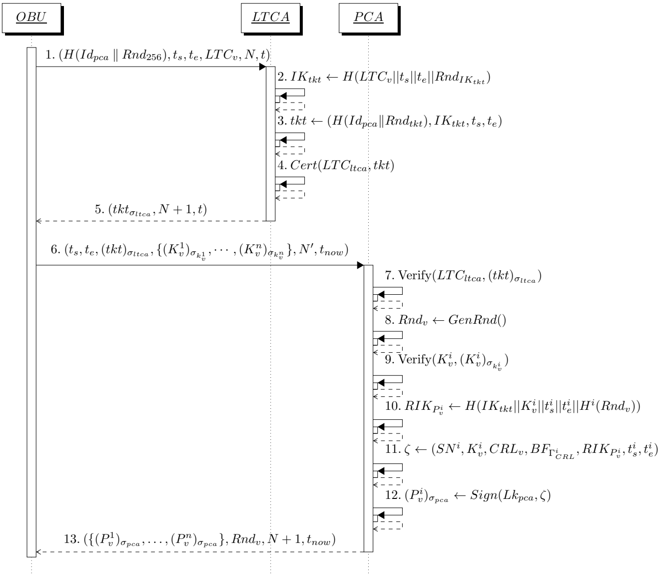


Figure: CRL piece & fingerprint construction by the PCA.

CRL Fingerprint:

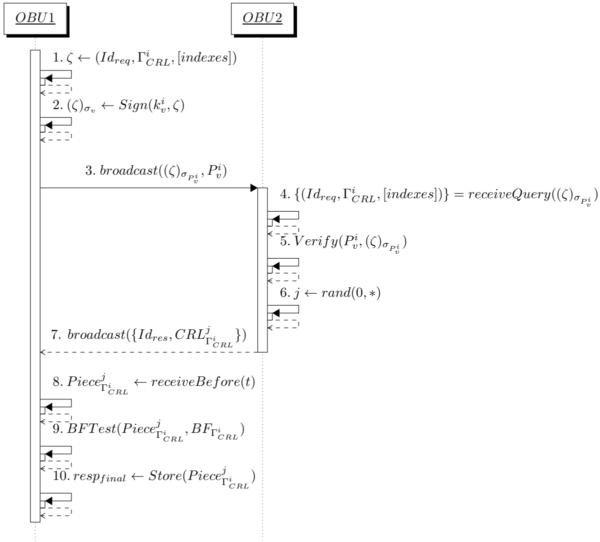
- A signed fingerprint is broadcasted by RSUs
- Also integrated in a subset of recently issued pseudonyms
- A notification about a new CRL-update (revocation) event

Pseudonym Acquisition Process




```
if i = 1 then
    SN^i ← H(RIK_{P_v^i} || H^i(Rnd_v))
else
    SN^i ← H(SN^{i-1} || H^i(Rnd_v))
end if
```

CRL Publish/Subscribe



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

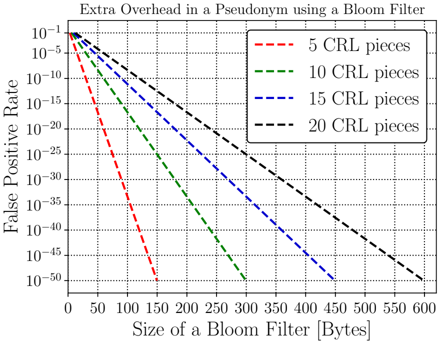


Figure: CRL Fingerprints overhead.

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

An adversary targeting the Bloom Filter (BF) false positive rate:

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

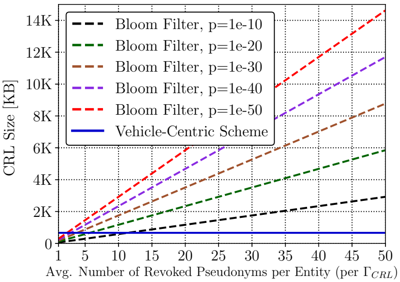
With Antminer-S9 (14TH/s,$3,000), $\Gamma_{CRL} = 1$ hour and $p = 10^{-20}$ ($K = 67$):

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

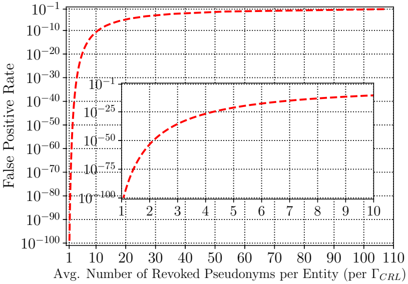
With AntPool ($1,604,608\ TH/s$): 70 minutes to generate a fake piece!

- 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)



(a) CRL size comparison



(b) C^{2}RL [9] 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.

- $m_{BF} = -\dfrac{N \times M \times \ln p}{(\ln 2)^2}$, 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, e.g., 2.6x reduction in CRL size when $M = 10$ and $p = 10^{-30}$.

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 ranges
- Comparison with the *baseline* scheme [8]: under the same assumptions and configuration with the same parameters
- Evaluation of:
    - Efficiency (latency)
    - Resilience (to pollution/DoS attacks)
    - Resource consumption (computation/communication)

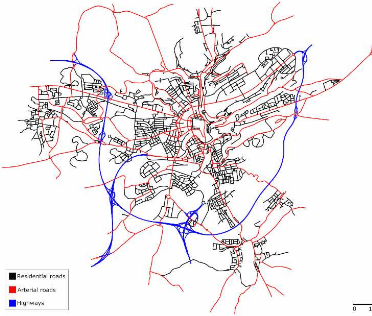
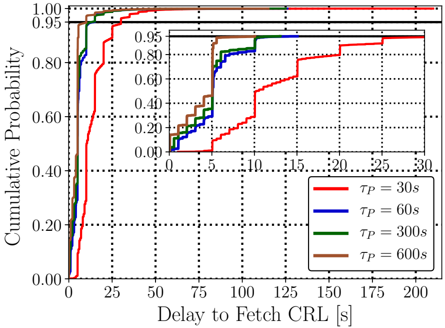
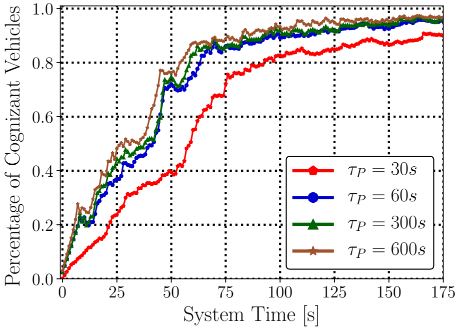


Figure: The LuST dataset, a full-day realistic mobility pattern in the city of Luxembourg (50KM x 50KM) [Codeca et al. (2015)].



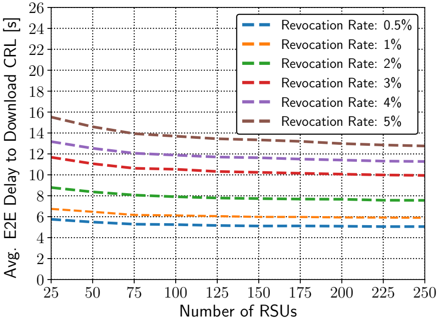
(a) Vehicle-centric scheme ($\mathbb{B}$ =10 KB/s)



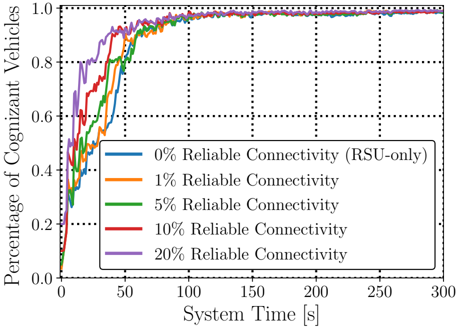
(b) Vehicle-centric scheme ($\mathbb{B}$ =10 KB/s)

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

Quantitative Analysis (cont'd)



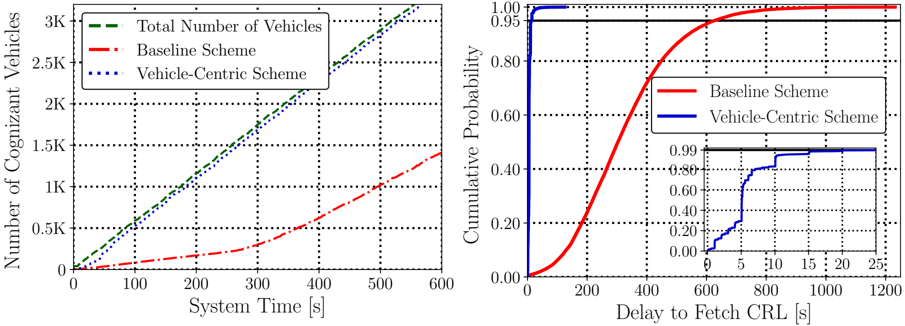
(a) Vehicle-centric scheme ($\mathbb{B}$ =25 KB/s)



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

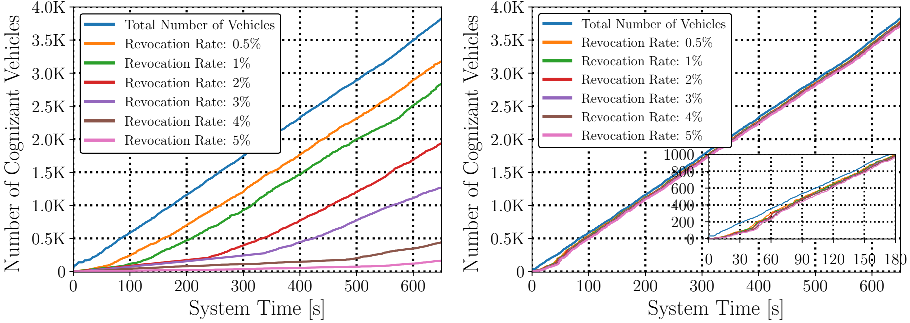


(a) 7:00-7:10 am ($\mathbb{B}$ =25 KB/s) (b) 7-9 am, 5-7 pm ($\mathbb{B}$ =25 KB/s)

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

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

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

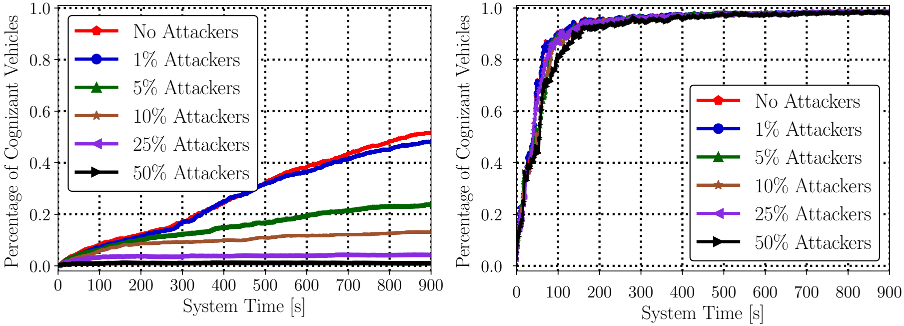


(a) Baseline scheme ($\mathbb{B}$ =50 KB/s)

(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 scheme: $\mathbb{T} \times \mathbb{R}$, linearly increases with $\mathbb{R}$
- Size of an *effective CRL* for vehicle-centric scheme: $\frac{\mathbb{T} \times \mathbb{R}}{|\Gamma_{CRL}|}$, where $|\Gamma_{CRL}|$ is the number of intervals in a day, e.g., $|\Gamma_{CRL}|$ is 24 when $\Gamma_{CRL} = 1$ hour.



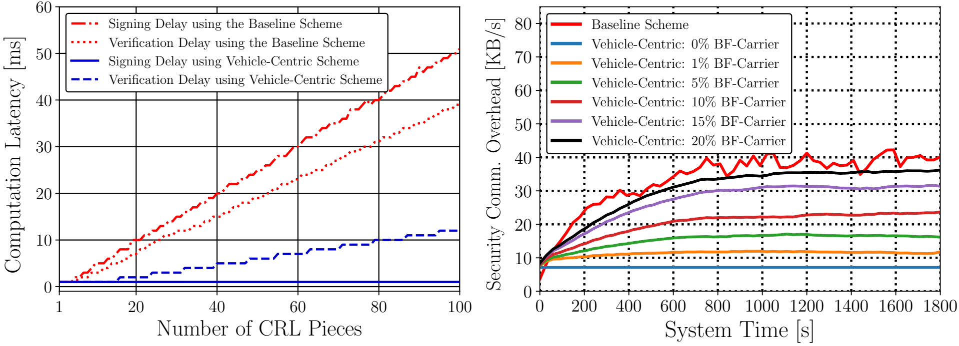
(a) Baseline scheme ($\mathbb{B}$ =25 KB/s)

(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

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 and primitives 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, $p = 10^{-30}$).

Conclusions and Future Work

Conclusions

- 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

Future Work

- Investigating an optimal interval for Γ_{CRL}
- Evaluating with different revocation event models and investigating their impact on CRL distribution

Bibliography I

[1] 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.

[2] 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.

[3] ------, ''Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure,'' in *IEEE VNC*, Paderborn, Germany, Dec. 2014.

[4] M. Khodaei and P. Papadimitratos, ''Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems,'' in *IoV/VoI*, Paderborn, Germany, July 2016.

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

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

[7] P. Papadimitratos and et al, ''Certificate Revocation List Distribution in Vehicular Communication Systems,'' in *ACM VANET*, San Francisco, CA, Sep 2008.

[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.

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

[10] 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.

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

[12] L. Fischer and et al, ''Secure Revocable Anonymous Authenticated Inter-vehicle Communication (SRAAC),'' in *ESCAR*, Berlin, Germany, Nov. 2006.

Bibliography II

[13] F. Stumpf and et al, ''Trust, Security and Privacy in VANETs – a Multilayered Security Architecture for C2C-Communication,'' *Automotive Security*, Nov. 2007.

[14] K.-P. Laberteaux and et al, ''Security Certificate Revocation List Distribution for VANET,'' in *ACM VehiculAr Inter-NETworking*, New York, NY, USA, Sep. 2008.

[15] J.-J. Haas and et al, ''Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET,'' in *ACM Vehicular Internetworking*, NY, USA, Sep. 2009.

[16] M. Raya and et al, ''Eviction of Misbehaving and Faulty Nodes in Vehicular Networks,'' *IEEE JSAC*, pp. 1557--1568, Oct. 2007.

[17] T. Moore and et al, ''Fast Exclusion of Errant Devices from Vehicular Networks,'' in *IEEE SECON*, San Francisco, CA, Jun. 2008.

[18] A. Wasef and X. Shen, ''EDR: Efficient Decentralized Revocation Protocol for Vehicular Ad hoc Networks,'' *IEEE TVT*, vol. 58, no. 9, pp. 5214--5224, 2009.

[19] N. Bißmeyer, ''Misbehavior Detection and Attacker Identification in Vehicular Ad-Hoc Networks,'' Ph.D. dissertation, Technische Universität, Dec. 2014.

Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs

Mohammad Khodaei and Panos Papadimitratos

Networked Systems Security Group (NSS)
www.ee.kth.se/nss

Royal Institute of Technology (KTH)
Stockholm, Sweden

June 20, 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

Prior Work

- CRL distribution via RSUs and car-to-car epidemic communication
- Revoking an ensemble of pseudonyms with a single entry (no *perfect-forward-privacy*)
- Revoking an ensemble of pseudonyms by leveraging a hash chain (*trivially linked by the issuer*)
- Compressing CRLs using a BF (*scalability and efficiency challenges*)
- Validating pseudonym status (revocation) information through Online Certificate Status Protocol (OCSP)
  - *Problematic due to intermittent connectivity, significant usage of the bandwidth by time- and safety-critical operations, and substantial overhead for the VPKI*
- Temporarily "revoking" (isolating) them from further access to the system (*not the "ultimate" decision*)

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

Simulation Parameters Information

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	50 KM $\times$ 50 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 ($\mathbb{R} = 1\%$, $\mathbb{B} = 10KB/s$).

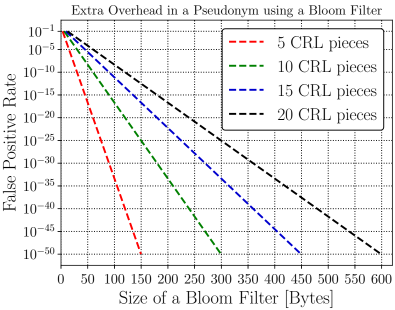
Pseudonym Lifetime	Number of Psnyms	Number of Revoked Psnyms	Average Number per Γ_{CRL}	Number of Pieces
τ_P=30s	3,425,565	34,256	1,428	12
τ_P=60s	1,712,782	17,128	710	6
τ_P=300s	342,556	3,426	143	2
τ_P=600s	171,278	1,713	72	1

Simulation Parameters for LuST Dataset

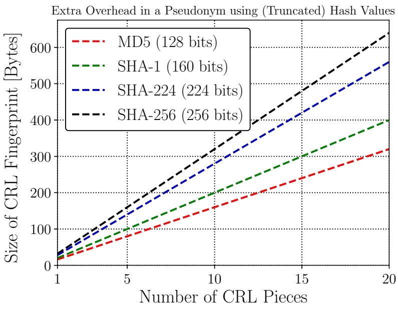
Table: Simulation Parameters for LuST Dataset ($\tau_P = 60s$).

Revocation Rate ($\mathbb{R}$)	**Baseline Scheme**				**Vehicle-Centric Scheme**			
	CRL Entries	**10 KB/s Pieces**	**25 KB/s Pieces**	**50 KB/s Pieces**	**CRL Entries**	**10 KB/s Pieces**	**25 KB/s Pieces**	**50 KB/s Pieces**
0.5%	8,500	70	30	15	355	3	2	1
1%	17,000	140	59	30	710	6	3	2
2%	34,000	279	117	59	1,417	12	5	3
3%	51,000	419	175	89	2,125	18	8	4
4%	68,000	558	233	118	2,834	24	10	5
5%	85,000	697	291	148	3,542	30	13	7

Qualitative Analysis



(a) Vehicle-centric scheme



(b) Precode-and-hash scheme [11]

Figure: Extra overhead for CRL fingerprints.

Issuing Pseudonyms (by the PCA)

Protocol 1 Issuing Pseudonyms (by the PCA)

procedure ISSUEPSNYMS(Req)
$Req \rightarrow (Id_{req}, t_s, t_e, (tkt)_{\sigma_{ltca}}, \{(K_v^1)_{\sigma_{k_v^1}}, \cdots, (K_v^n)_{\sigma_{k_v^n}}\}, nonce, t_{now})$
Verify($\mathrm{LTC}_{ltca}, (tkt)_{\sigma_{ltca}}$)
$Rnd_v \leftarrow GenRnd()$
for i:=1 to **n do**
Begin
Verify($K_v^i, (K_v^i)_{\sigma_{k_v^i}}$)
$RIK_{P_v^i} \leftarrow H(IK_{tkt}||K_v^i||t_s^i||t_e^i||H^i(Rnd_v))$
if $i = 1$ **then**
$SN^i \leftarrow H(RIK_{P_v^i}||H^i(Rnd_v))$
else
$SN^i \leftarrow H(SN^{i-1}||H^i(Rnd_v))$
end if
$\zeta \leftarrow (SN^i, K_v^i, CRL_v, BF_{\Gamma_{CRL}^i}, RIK_{P_v^i}, t_s^i, t_e^i)$
$(P_v^i)_{\sigma_{pca}} \leftarrow Sign(Lk_{pca}, \zeta)$
End
return $(Id_{res}, \{(P_v^1)_{\sigma_{pca}}, \ldots, (P_v^n)_{\sigma_{pca}}\}, Rnd_v, nonce{+}1, t_{now})$
end procedure

CRL Construction (by the PCA)

Protocol 2 CRL Construction (by the PCA)

procedure $\textsc{GenCRL}(\Gamma^{i}_{CRL}, \mathbb{B})$

  $Piece_{\Gamma^{i}_{CRL}} \leftarrow \emptyset$

  repeat

    $\{SN^{k}_{P}, H^{k}_{Rnd_v}, n\} \leftarrow fetchRevokedPsnyms(\Gamma^{i}_{CRL})$ ▷ k: the revoked

    if $SN^{k}_{P} \neq Null$ **then**

      $Piece_{\Gamma^{i}_{CRL}} \leftarrow Append(\{SN^{k}_{P}, H^{k}_{Rnd_v}, n\})$

    end if

  until $SN^{k}_{P} == Null$

  $N \leftarrow \left\lceil \frac{size(Piece_{\Gamma^{i}_{CRL}})}{\mathbb{B}} \right\rceil$ ▷ calculating number of pieces with a given $\mathbb{B}$

  for $j \leftarrow 0, N$ **do** ▷ N: number of pieces in Γ^{i}_{CRL}

    $Piece^{j}_{\Gamma^{i}_{CRL}} \leftarrow Split(Piece_{\Gamma^{i}_{CRL}}, \mathbb{B}, N)$ ▷ splitting into N pieces

  end for

  return $\{(Piece^{1}_{\Gamma^{i}_{CRL}}), \ldots, (Piece^{N}_{\Gamma^{i}_{CRL}})\}$

end procedure

Publishing CRLs (by the OBUs)

Protocol 3 Publishing CRLs (by the OBUs)

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

Subscribing to CRL Pieces (by the OBUs)

Protocol 4 Subscribing to CRL Pieces (by the OBUs)

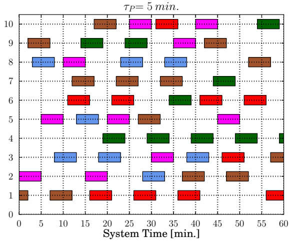
```
procedure SUBSCRIBECRL(Γ^i_CRL, N)
    resp_final ← ∅, j ← 0, t ← t_now + T_timeout
    repeat
        ζ ← (Id_req, Γ^i_CRL, [missing pieces indexes])
        (ζ)_σv ← Sign(k^i_v, ζ)
        broadcast((ζ)_σ_{P^i_v}, P^i_v)
        Piece^j_{Γ^i_CRL} ← receiveBefore(t)
        if BFTest(Piece^j_{Γ^i_CRL}, BF_{Γ^i_CRL}) then
            resp_final ← Store(Piece^j_{Γ^i_CRL})          ▷ storing in local repository
        end if
        j ← j + 1
    until j > N
    return resp_final
end procedure
```

Parsing a CRL Piece (by the OBUs)

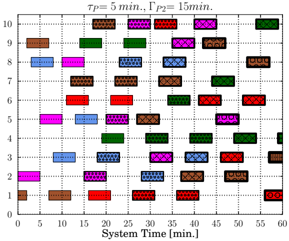
Protocol 5 Parsing a CRL Piece (by the OBUs)

procedure $\textsc{ParseCRL}(Piece^{j}_{\Gamma^{i}_{CRL}})$
  $\{SN^{k}, H^{k}(Rnd_{v}), n\}_{N} \leftarrow Piece^{j}_{\Gamma^{i}_{CRL}}$ ▷ N: Number of Entires
  $CRL_{\Gamma^{i}_{CRL}} \leftarrow \emptyset$
  for $t \leftarrow 0, N$ **do** ▷ N: Total number of CRL pieces
    for $j \leftarrow 0, n$ **do** ▷ n: Number of remaining psnyms in each batch
      $SN^{j+1} \leftarrow H(SN^{j} || H^{j}(Rnd_{v}))$
      $CRL_{\Gamma^{i}_{CRL}} \leftarrow Append(H(SN^{j} || H^{j}(Rnd_{v})))$
    end for
  end for
  return $CRL_{\Gamma^{i}_{CRL}}$
end procedure

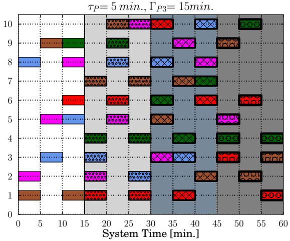
Linkability based on Timing Information of Credentials



User-controlled policy (P1)



Oblivious policy (P2)



Universally fixed policy (P3)

- Non-overlapping pseudonym lifetimes from eavesdroppers' perspective
- Distinct lifetimes per vehicle make linkability easier
- Uniform pseudonym lifetime results in no distinction among obtained pseudonyms set, thus less probable to link pseudonyms