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

Trust establishment

A certifies B
Cross-certification
Communication link
Message dissemination
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.

Vehicle-Centric CRL Distribution

Partitioned Interval: $CRL^i$

Trip Duration: $D$

Figure: CRL as a Stream:
- $V_1$ subscribes to $\{CRL^i, CRL^{i+1}, CRL^{i+2}\}$;
- $V_2$: $\{CRL^i, CRL^{i+1}\}$;
- $V_3$: $\{CRL^{i+2}\}$;
- $V_4$: $\{CRL^{i+3}\}$;
- $V_5$: $\{CRL^{i+4}\}$.

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

Bloom Filter (BF)

ρ: false positive rate
k: number of hash functions
Pseudonym Acquisition Process

1. \( H(Id_{pca} \| Rnd_{256}), t_s, t_e, LTC_v, N, t \) → \( IKTkt \leftarrow H(LTC_v \| t_s \| t_e \| Rnd_{IKtkt}) \) → \( tkt \leftarrow (H(Id_{pca} \| Rnd_{tkt}), IKTkt, t_s, t_e) \) → \( Cert(LTC_{ltca}, tkt) \)

5. \( (tkt_{\sigma_{ltca}}, N + 1, t) \) → \( 7. \text{Verify}(LTC_{ltca}, (tkt)_{\sigma_{ltca}}) \)

6. \( (t_s, t_e, (tkt)_{\sigma_{ltca}}, \{(K^1_v)_{\sigma_{h_v}}, \ldots, (K^u_v)_{\sigma_{h_v}}\}, N', t_{\text{now}}) \) → \( 8. Rnd_v \leftarrow \text{GenRnd}() \) → \( 9. \text{Verify}(K^i_v, (K^i_v)_{\sigma_{h_v}}) \) → \( 10. RIK_{P_v} \leftarrow H(IKTkt \| K^i_v \| t_s^i \| t_e^i \| H'(Rnd_v)) \) → \( 11. \zeta \leftarrow (SN^i, K^i_v, CRL_v, BF_{CRL}, RIK_{P_v}, t_s^i, t_e^i) \) → \( 12. (P^i_v)_{\sigma_{pca}} \leftarrow \text{Sign}(Lk_{pca}, \zeta) \) → \( 13. \{((P^1_v)_{\sigma_{pca}}, \ldots, (P^u_v)_{\sigma_{pca}}), Rnd_v, N + 1, t_{\text{now}}) \)
1. $\zeta \leftarrow (Id_{req}, \Gamma_{CRL}^i, [indexes])$

2. $(\zeta)_{\sigma_v} \leftarrow \text{Sign}(k_v^i, \zeta)$

3. broadcast($(\zeta)_{\sigma_P^i}, P_v^i)$

4. $\{(Id_{req}, \Gamma_{CRL}^i, [indexes])\} = \text{receiveQuery}((\zeta)_{\sigma_P^i})$

5. $\text{Verify}(P_v^i, (\zeta)_{\sigma_P^i})$

6. $j \leftarrow \text{rand}(0, *)$

7. broadcast($\{Id_{res}, CRL_{\Gamma_{CRL}^i}^j\}$)

8. $\text{Piece}_{\Gamma_{CRL}^i}^j \leftarrow \text{receiveBefore}(t)$

9. $\text{BFTest}($\text{Piece}_{\Gamma_{CRL}^i}^j, BF_{\Gamma_{CRL}^i}$)$

10. $\text{resp}_{\text{final}} \leftarrow \text{Store}($\text{Piece}_{\Gamma_{CRL}^i}^j$)
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)

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)

Figure: CRL Fingerprints overhead.

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.

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

$m_{BF}$
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)].
Quantitative Analysis (cont’d)

Figure: (a) End-to-end latency to fetch CRL pieces. (b) Percentage of cognizant vehicles.
Quantitative Analysis (cont’d)

(a) Vehicle-centric scheme ($B = 25$ 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 ($p = 10^{-30}, \mathbb{R} = 0.5\%$).
Converging more than 40 times faster than the state-of-the-art:

- Baseline scheme: \( F_x(t = 626) = 0.95 \)
- Vehicle-centric scheme: \( F_x(t = 15) = 0.95 \)
Quantitative Analysis (cont’d)

Figure: Cognizant vehicles with different revocation rates.

- $T$: the total number of pseudonyms; $R$: the revocation rate.
- Size of CRLs for the Baseline scheme: $T \times R$, linearly increases with $R$.
- Size of an effective CRL for vehicle-centric scheme: $\frac{T \times R}{|\Gamma_{CRL}|}$, where $|\Gamma_{CRL}|$ is the number of intervals in a day, e.g., $|\Gamma_{CRL}|$ is 24 when $\Gamma_{CRL} = 1$ hour.
Quantitative Analysis (cont’d)

(a) Baseline scheme (B = 25 KB/s)

(b) Vehicle-centric scheme (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)

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

- 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 $\Gamma_{CRL}$
- Evaluating with different revocation event models and investigating their impact on CRL distribution


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)
Table: Notation Used in the Protocols.

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

*Table: Simulation Parameters (LuST dataset).*

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRL/Fingerprint TX interval</td>
<td>0.5s/5s</td>
<td>Pseudonym lifetime</td>
<td>30s-600s</td>
</tr>
<tr>
<td>Carrier frequency</td>
<td>5.89 GHz</td>
<td>Area size</td>
<td>50 KM × 50 KM</td>
</tr>
<tr>
<td>TX power</td>
<td>20mW</td>
<td>Number of vehicles</td>
<td>138,259</td>
</tr>
<tr>
<td>Physical layer bit-rate</td>
<td>18Mbps</td>
<td>Number of trips</td>
<td>287,939</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>-89dBm</td>
<td>Average trip duration</td>
<td>692.81s</td>
</tr>
<tr>
<td>Thermal noise</td>
<td>-110dBm</td>
<td>Duration of simulation</td>
<td>4 hour (7-9, 17-19)</td>
</tr>
<tr>
<td>CRL dist. Bandwidth (B)</td>
<td>10, 25, 50 KB/s</td>
<td>Π</td>
<td></td>
</tr>
<tr>
<td>Number of RSUs</td>
<td>100</td>
<td>Π&lt;sub&gt;CRL&lt;/sub&gt;</td>
<td>60 min</td>
</tr>
</tbody>
</table>

*Table: LuST Revocation Information (R = 1%, B = 10KB/s).*

<table>
<thead>
<tr>
<th>Pseudonym Lifetime</th>
<th>Number of Psnyms</th>
<th>Number of Revoked Psnyms</th>
<th>Average Number per Γ&lt;sub&gt;CRL&lt;/sub&gt;</th>
<th>Number of Pieces</th>
</tr>
</thead>
<tbody>
<tr>
<td>τ&lt;sub&gt;P&lt;/sub&gt;=30s</td>
<td>3,425,565</td>
<td>34,256</td>
<td>1,428</td>
<td>12</td>
</tr>
<tr>
<td>τ&lt;sub&gt;P&lt;/sub&gt;=60s</td>
<td>1,712,782</td>
<td>17,128</td>
<td>710</td>
<td>6</td>
</tr>
<tr>
<td>τ&lt;sub&gt;P&lt;/sub&gt;=300s</td>
<td>342,556</td>
<td>3,426</td>
<td>143</td>
<td>2</td>
</tr>
<tr>
<td>τ&lt;sub&gt;P&lt;/sub&gt;=600s</td>
<td>171,278</td>
<td>1,713</td>
<td>72</td>
<td>1</td>
</tr>
</tbody>
</table>
Table: Simulation Parameters for LuST Dataset ($\tau_p = 60s$).

| Revocation Rate (R) | Baseline Scheme | | | | Vehicle-Centric Scheme | | | |
|---------------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
|                     | CRL Entries     | 10 KB/s         | 25 KB/s         | 50 KB/s         | CRL Entries     | 10 KB/s         | 25 KB/s         | 50 KB/s         |
|                     | Pieces          | Pieces          | Pieces          | Pieces          | Pieces          | Pieces          | Pieces          | 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               |
(a) Vehicle-centric scheme

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

Figure: Extra overhead for CRL fingerprints.
Protocol 1 Issuing Pseudonyms (by the PCA)

1: procedure ISSUE_PSNYMS(Req)
2: \hspace{1em} Req \rightarrow (Id_{req}, t_s, t_e, (tkt)_{\sigma_{ltca}}, \{(K^1_v)_{\sigma_{k^1_v}}, \ldots, (K^n_v)_{\sigma_{k^n_v}}\}, nonce, t_{now})
3: \hspace{1em} Verify(LTC_{ltca}, (tkt)_{\sigma_{ltca}})
4: \hspace{1em} Rnd_v \leftarrow \text{GenRnd}()$
5: \hspace{1em} \text{for } i := 1 \text{ to } n \text{ do}
6: \hspace{2em} \text{Begin}
7: \hspace{3em} \text{Verify}(K^i_v, (K^i_v)_{\sigma_{k^i_v}})
8: \hspace{3em} RIK_{p_i^v} \leftarrow H(\Pi_K_{tkt} || K^i_v || t^i_s || t^i_e || H^i(Rnd_v))$
9: \hspace{3em} \text{if } i = 1 \text{ then}
10: \hspace{4em} SN^i \leftarrow H(RIK_{p_i^v} || H^i(Rnd_v))$
11: \hspace{3em} \text{else}
12: \hspace{4em} SN^i \leftarrow H(SN^{i-1} || H^i(Rnd_v))$
13: \hspace{3em} \text{end if}
14: \hspace{3em} \zeta \leftarrow (SN^i, K^i_v, CRL_v, BF_{CRL}^i, RIK_{p_i^v}, t^i_s, t^i_e)$
15: \hspace{3em} (P^i_v)_{\sigma_{pca}} \leftarrow \text{Sign}(Lk_{pca}, \zeta)$
16: \hspace{2em} \text{End}
17: \hspace{1em} \text{return } (Id_{res}, \{(P^1_v)_{\sigma_{pca}}, \ldots, (P^n_v)_{\sigma_{pca}}\}, Rnd_v, nonce+1, t_{now})$
18: \hspace{1em} \text{end procedure}
Protocol 2 CRL Construction (by the PCA)

1: procedure GENCRL($\Gamma_{CRL}^i, B$)  
2: \hspace{1em} $Piece_{CRL}^i \leftarrow \emptyset$  
3: repeat  
4: \hspace{2em} $\{SN_k^P, H_{Rnd_v}^k, n\} \leftarrow \text{fetchRevokedPsnyms}(\Gamma_{CRL}^i)$  
5: \hspace{2em} if $SN_k^P \neq \text{Null}$ then  
6: \hspace{3em} $Piece_{CRL}^i \leftarrow \text{Append}(\{SN_k^P, H_{Rnd_v}^k, n\})$  
7: \hspace{2em} end if  
8: until $SN_k^P == \text{Null}$  
9: $N \leftarrow \left\lceil \frac{\text{size}(Piece_{CRL}^i)}{B} \right\rceil$  
10: for $j \leftarrow 0, N$ do  
11: \hspace{2em} $Piece_{CRL}^i \leftarrow \text{Split}(Piece_{CRL}^i, B, N)$  
12: end for  
13: return $\{(Piece_{CRL}^1), \ldots, (Piece_{CRL}^N)\}$  
14: end procedure
**Protocol 3** Publishing CRLs (by the OBUs)

1: procedure PublishCRL()
2: \{\{Id_{req}, \Gamma_i^{CRL}, [indexes]\}\} = receiveQuery((\zeta)_{P_i^v})
3: Verify(P_i^v, (\zeta)_{P_i^v})
4: $CRL_i^{\ast}_{\Gamma_{CRL}} = search_{local}(\Gamma_i^{CRL})$
5: $j \leftarrow rand(0, \ast)$
6: if $CRL_j^{\Gamma_{CRL}} \neq \emptyset$ then
7: broadcast\{\{Id_{res}, CRL_j^{\Gamma_{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 \text{SubscribeCRL}(\Gamma_i^{CRL}, N)
2: \hspace{1em} res_{final} \leftarrow \emptyset, j \leftarrow 0, t \leftarrow t_{now} + T_{timeout}
3: \hspace{1em} repeat
4: \hspace{2em} \zeta \leftarrow (Id_{req}, \Gamma_i^{CRL}, \text{[missing pieces indexes]})
5: \hspace{2em} (\zeta)_{\sigma_v} \leftarrow \text{Sign}(k_i^v, \zeta)
6: \hspace{2em} \text{broadcast}((\zeta)_{\sigma_{P_i^v}}, P_i^v)
7: \hspace{2em} Piece_{\Gamma_i^{CRL}}^j \leftarrow \text{receiveBefore}(t)
8: \hspace{2em} \text{if BFTest(Piece}_{\Gamma_i^{CRL}}^j, BF_{\Gamma_i^{CRL}}) \text{ then}
9: \hspace{3em} res_{final} \leftarrow \text{Store(Piece}_{\Gamma_i^{CRL}}^j)
10: \hspace{2em} \text{end if}
11: \hspace{2em} j \leftarrow j + 1
12: \hspace{2em} until \hspace{1em} j > N
13: \hspace{1em} return \hspace{1em} res_{final}
14: \hspace{1em} end procedure
Protocol 5 Parsing a CRL Piece (by the OBUs)

1: procedure PARSESCRL(Piece\(_i^{\Gamma_{CRL}}\))
2: \{SN^k, H^k(Rvd), n\}_N \leftarrow Piece\(_i^{\Gamma_{CRL}}\)
3: \(CRL^{\Gamma_{CRL}} \leftarrow \emptyset\)
4: for \(t \leftarrow 0, N\) do
5: \(CRL^{\Gamma_{CRL}} \leftarrow \emptyset\)
6: \(SN^{i+1} \leftarrow H(SN^i || H^i(Rvd))\)
7: \(CRL^{\Gamma_{CRL}} \leftarrow Append(H(SN^i || H^i(Rvd)))\)
8: end for
9: end for
10: return \(CRL^{\Gamma_{CRL}}\)
11: end procedure
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