RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd

Mohammad Khodaei, Andreas Messing, and Panos Papadimitratos

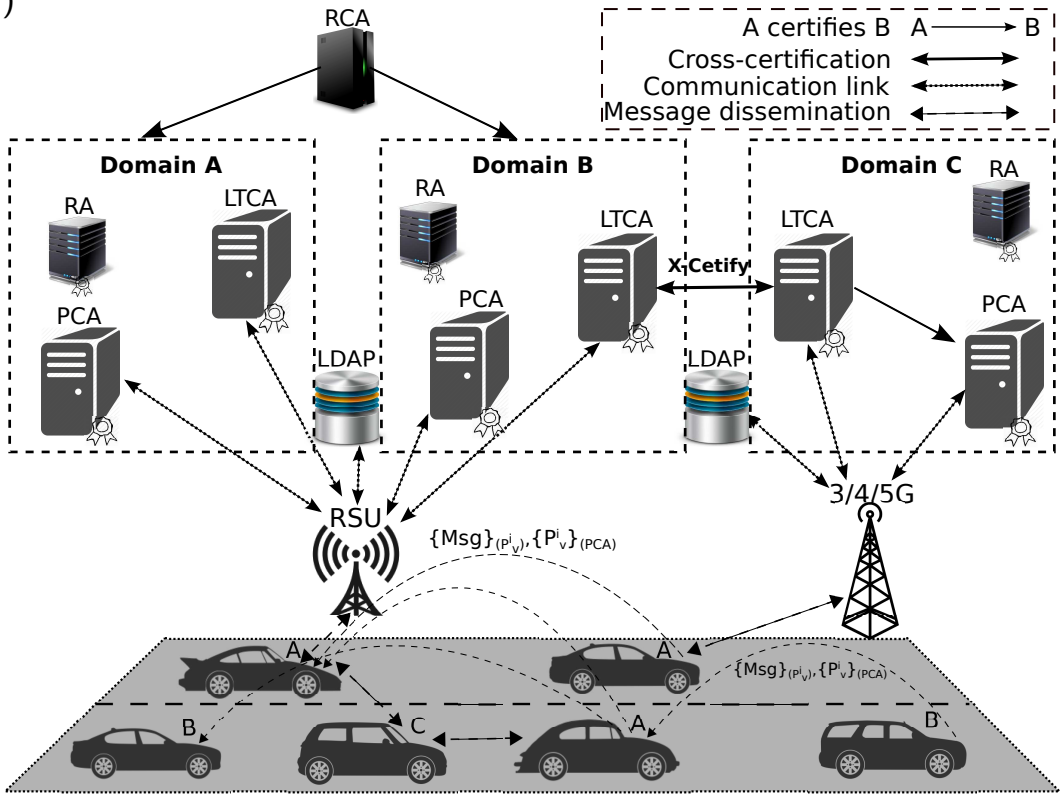
Networked Systems Security Group (NSS)
www.ee.kth.se/nss

Royal Institute of Technology (KTH)
Stockholm, Sweden

Nov. 28, 2017

Secure Vehicular Communication (VC) Systems

- Vehicular Public Key Infrastructure (VPKI)
- 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



Pseudonym Refilling Strategies

Preloading schemes

- Computationally costly, inefficient utilization, cumbersome revocation

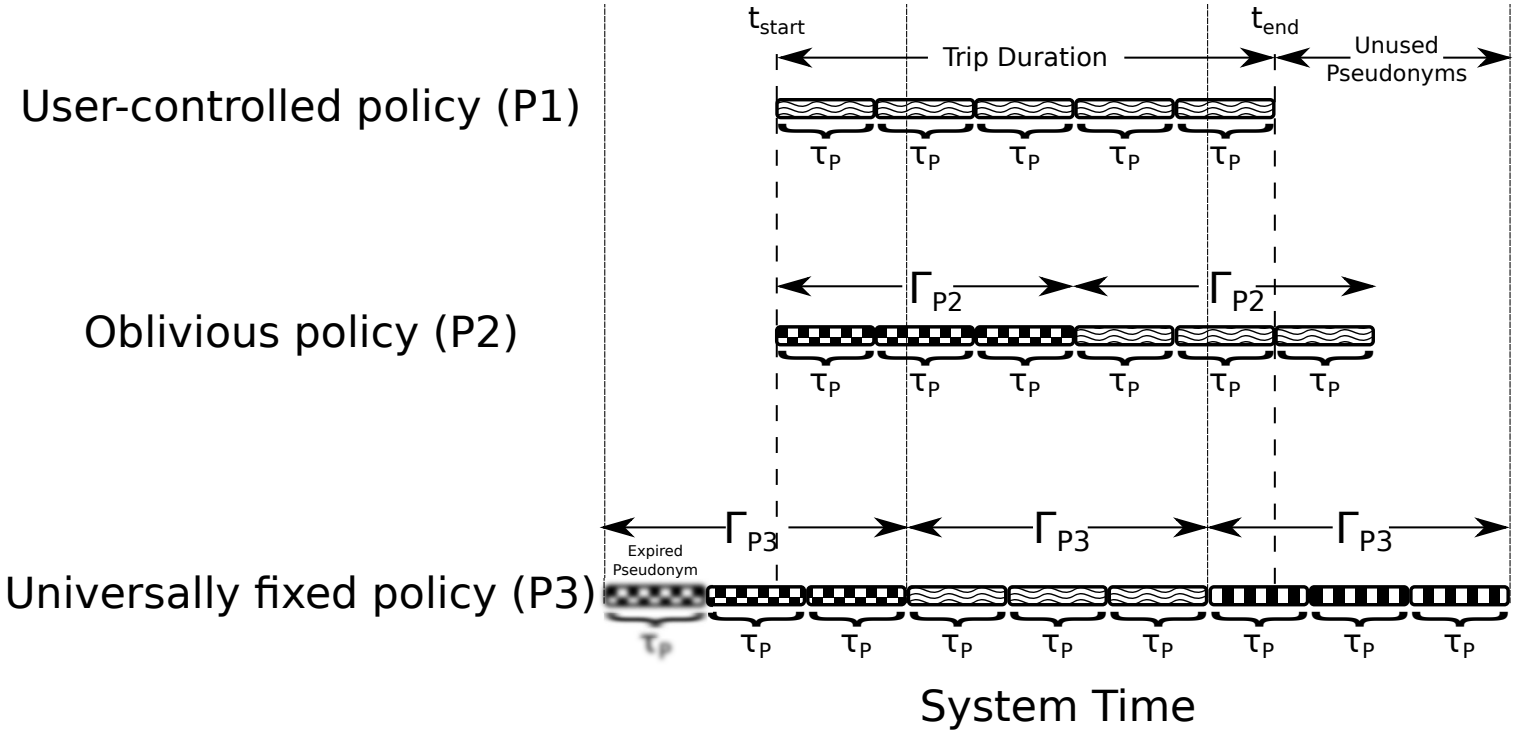
On-demand schemes

- Efficient in utilization & revocation; effective in fending off misbehavior
- The more frequent interactions, the more dependent on connectivity

Strategies / Metrics	Preloading & Overlapping	Preloading & Nonoverlapping	On-demand & Overlapping	On-demand & Nonoverlapping
Storage size	large	large	small	small
Pseudonym quantity	fixed & low volume	fixed & high volume	varying	varying
Pseudonym lifetime	long	short	varying	varying
V-VPKI communication frequency	**low**	**low**	**high**	**high**
Communication overhead	**low**	**low**	**high**	**high**
Efficient pseudonym utilization	**very low**	**very low**	**high**	**high**
Pseudonym revocation	**difficult & challenging**	**difficult & challenging**	**no need (lower risk)**	**no need (lower risk)**
Pseudonym vulnerability window	**wide**	**wide**	**narrow**	**narrow**
Resilience to Sybil-based misbehavior	×	✓	×	✓
User privacy protection (probability of linking sets of pseudonyms based on timing information)	**privacy protection: high (probability of linking: low)**	**privacy protection: low (probability of linking: high)**	**privacy protection: high (probability of linking: low)**	**privacy protection: low (probability of linking: high)**
User privacy protection (duration for which a pseudonym provider can trivially link sets of pseudonyms for the same vehicle; the longer the duration, the higher the chance to link sets of pseudonyms)	**privacy protection: low (long duration)**	**privacy protection: low (long duration)**	**privacy protection: high (short duration)**	**privacy protection: high (short duration)**
Effect on safety application operations	low	low	high	high
Deployment cost (e.g. RSU)	low	low	high	high
Proposals & schemes	**C2C-CC [1], PRESERVE [2], CAMP VSC3 [3, 4]**	**SeVeCom [5], Safety Pilot**	**SRAAC [6], V-tokens [7], CoPRA [8]**	**VeSPA, SEROSA, SECMACE [9, 10], PUCA [11]**

M. Khodaei et al., "Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems," in Proceedings of the IoV/VoI, Paderborn, Germany, July 2016.

On-demand 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 [12]
- P3: Requesting intervals fall within *"universally"* fixed interval Γ_{P3}, and pseudonyms are aligned with VPKI clock [12]

M. Khodaei et al., "Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems," in Proceedings of the IoV/VoI, Paderborn, Germany, July 2016.

Problem Statement

Challenges

- *How to ensure vehicle operation without harming user privacy, if the VPKI is unreachable?*
- Intermittent coverage (sparsely-deployed RSUs), highly overloaded cellular infrastructure, VPKI under an attack, e.g., DDoS [9]
- **Baseline hybrid scheme:** issuing *on-the-fly self-certified* pseudonyms [13]
- Vehicles without VPKI-provided pseudonyms would *"stand out in a crowd":* different certificate format (Group Signatures (GS)-based) and timing information

Contributions

- RHyTHM: A cooperative & adaptive scheme
- Improving privacy for VPKI-disconnected vehicles without deteriorate the privacy of others
- At the expense of a reasonable computational overhead

Strong adversarial model

Increased protection against *honest-but-curious* VPKI entities [9]

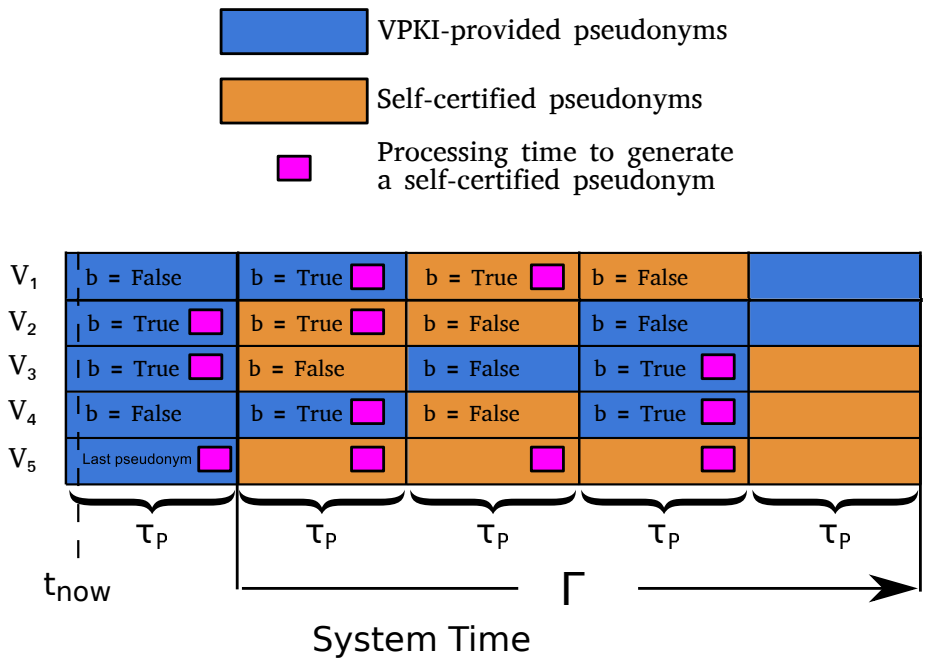
- Correct execution of protocols but motivated to profile users
- Compromising RHyTHM by performing Sybil-based misbehavior or DoS attacks

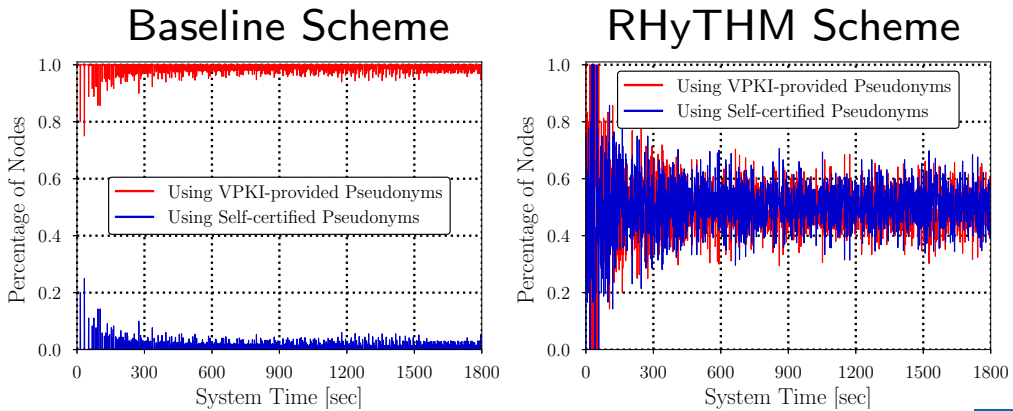
Our Solution: RHyTHM

Protocol 1 RHyTHM Initiation Protocol

1: **procedure** RHyTHMInit(t_s, t_e)
2: **for** i:=1 to **n do**
3: **Begin**
4: Generate(K_v^i, k_v^i)
5: $\zeta \leftarrow (K_v^i, t_s^i, t_e^i)$
6: $(K_v^i)_{\Sigma_{k_v^i}} \leftarrow \text{Sign}(gsk_v, \zeta)$
7: **End**
8: $Flag_{rhythm} \leftarrow True$
9: $CAM \leftarrow \{Fields, Flag_{rhythm}, t_{now}\}$
10: $(CAM)_{\sigma_{k_v^i}} \leftarrow \text{Sign}(CAM, K_v^i)$
11: **end procedure**

- Registration phase: LTCA and Group Manager (GM)
- A universally fixed interval, Γ, to refill pseudonyms pool
- Aligning pseudonyms lifetimes
- Elliptic Curve Digital Signature Algorithm (ECDSA) key pairs
- If $b = True$, the vehicle will utilize its self-certified pseudonym; otherwise, it relies on its VPKI-provided pseudonym.





1% of nodes run out of pseudonyms ($\tau_P = 60\ sec, r = 0.5$)

Security & Privacy Analysis

- **Non-repudiation, authentication and integrity**
  - Pseudonyms, group signing key, and digital signatures
- **Thwarting Sybil-based misbehavior**
  - Hardware Security Module (HSM) ensures signatures under one private key of a single valid pseudonym
  - Employing *"n-times anonymous authentication"* scheme [14, 13]
- **Revocation**
  - Interacting RA with the PCA, GM, and LTCA, to resolve and possibly revoke a misbehaving vehicle
  - Distributing Certificate Revocation Lists (CRLs)
- **Thwarting clogging Denial of Service (DoS) attack**
  - Ignoring RHyTHM initiation query if VPKI is reachable
  - RHyTHM only lasts while the VPKI is out of reach

Security & Privacy Analysis (cont'd)

N: Vehicles with VPKI-provided pseudonyms, joining RHyTHM

M: Vehicles without VPKI-provided pseudonyms, joining RHyTHM

r: The probability of switching to self-certified pseudonyms

Privacy metric: Probability of linking two pseudonyms belonging to the same vehicle

If all vehicles join RHyTHM:

- Baseline scheme: $Pr_{vpki\text{-}2\text{-}vpki} = \frac{1}{N}$
- RHyTHM scheme:
  $Pr_{vpki\text{-}2\text{-}vpki} = \frac{(1-r)}{N-(r\times N)} = \frac{1}{N}$
- RHyTHM scheme
  - $Pr_{vpki\text{-}2\text{-}selfcertifed} = \frac{r}{M+(r\times N)} = \frac{1}{N+\frac{M}{r}}$
    $(\frac{1}{N+\frac{M}{r}} < \frac{1}{N}$, if $M > 0)$

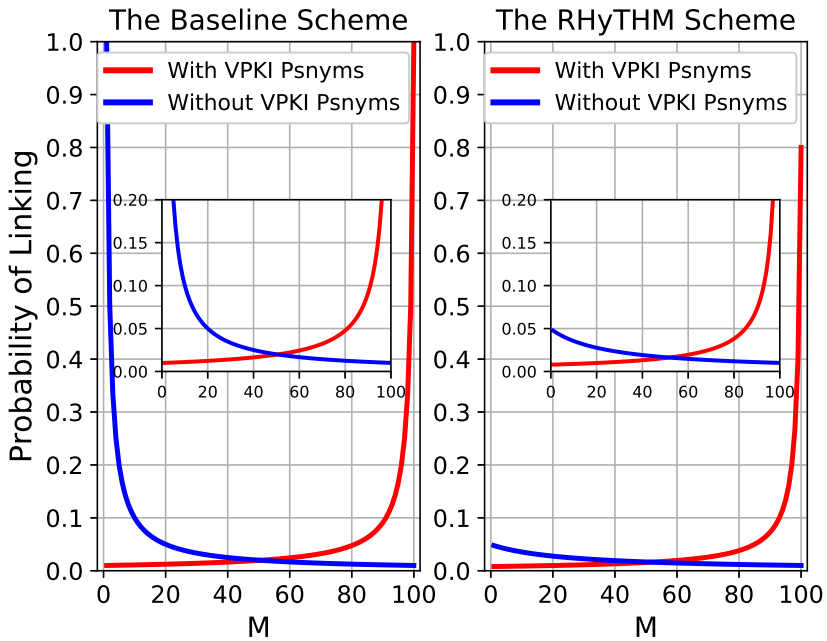


Figure : Comparing the probability of linking two successive pseudonyms using baseline and RHyTHM schemes $(N = 100, r = 0.2)$.

Security & Privacy Analysis (cont'd)

- **A fraction of vehicles never join RHyTHM**
- **K:** Vehicles with VPKI-provided pseudonyms, never joining RHyTHM
  - $Pr = \frac{K}{[K+(N-K)\times(1-r)]^2} + \frac{N-r\times(N-K)-K}{[K+(N-K)\times(1-r)]^2} \times (1-r)$
- If K=0 or K=N, the probability of linking on average becomes $\frac{1}{N}$.
- The probability of linking two successive VPKI-provided pseudonyms, if participating in RHyTHM, is always less than the one if not joining RHyTHM.

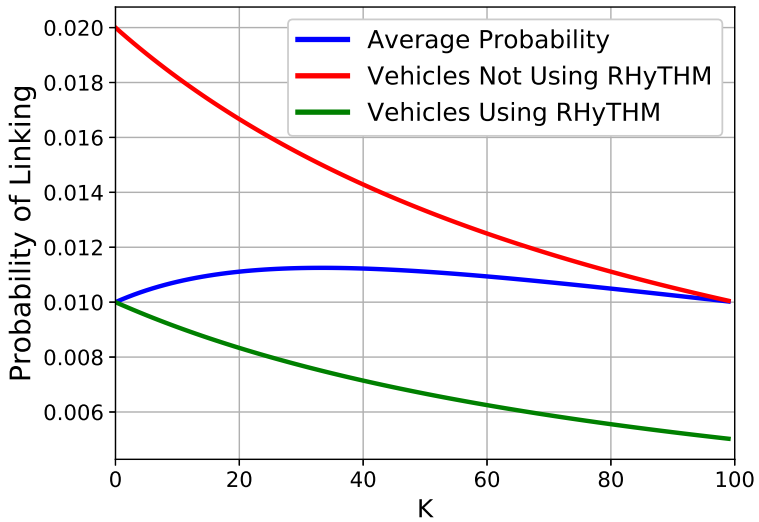
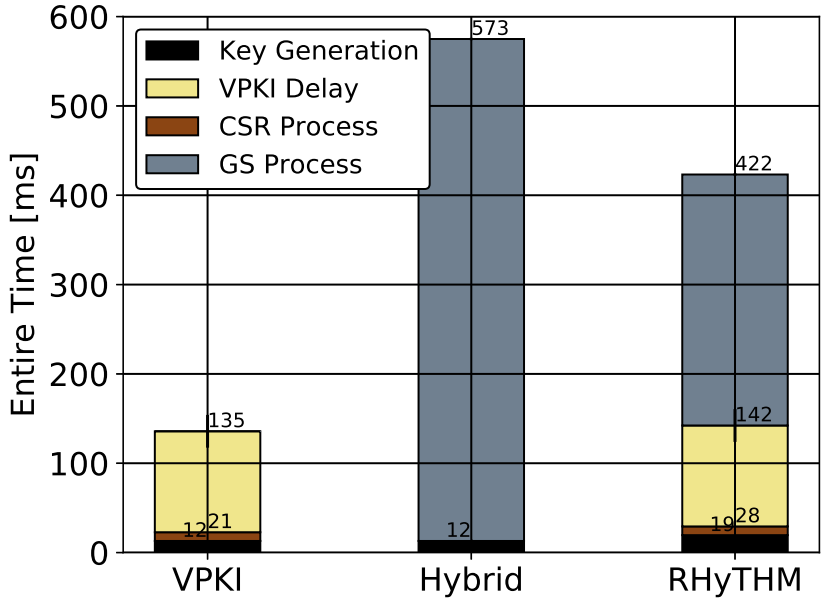
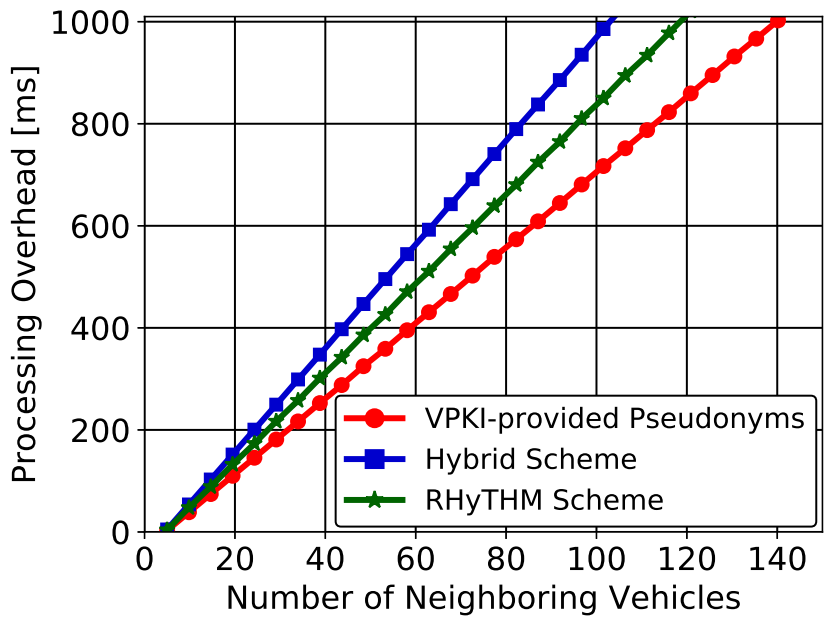


Figure : Probability of linking two VPKI-provided pseudonyms, belonging to a given vehicle ($N = 100, r = 0.5$).

Performance Evaluation



(a) End-to-end latency



(b) Cryptographic overhead

Figure : (a) End-to-end latency to acquire 10 pseudonyms, averaged over 500 runs. (b) Processing overhead as a function of the neighborhood size ($\tau_P = 30$ sec, ratio of received messages: up to 60 beacon/sec, $r = 0.5$).

- Emulating a large neighborhood with 7 PRESERVE Nexcom boxes: dual-core 1.66 GHz, 2GB Memory
- C, OpenSSL, an implementation of short group signature [15]: Pairings in C (`https://github.com/IAIK/pairings_in_c`)

Conclusions and Future Work

Conclusions

- RHyTHM enhances the privacy of disconnected users with a reasonable computation overhead
- Vehicles with VPKI-provided pseudonyms: if using RHyTHM, gaining higher privacy protection; if not, their privacy slightly decreases

Future Work

- Investigating the provision of incentives to participate in RHyTHM
- Optimal probability of switching to utilizing self-certified pseudonyms
- Degree of propagating RHyTHM initiation query in actual scenarios
- Rigorous analysis of the security and privacy protocols

Bibliography

[1] **Car-to-Car Communication Consortium (C2C-CC)**, http://www.car-2-car.org/.

[2] "**Preparing Secure Vehicle-to-X Communication Systems - PRESERVE**," http://www.preserve-project.eu/.

[3] W. Whyte *et al.*, "**A Security Credential Management System for V2V Communications**," in *VNC*, Boston, Dec. 2013.

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

[5] P. Papadimitratos *et al.*, "**Secure Vehicular Communication Systems: Design and Architecture**," *IEEE CommMag*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

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

[7] F. Schaub *et al.*, "**V-tokens for Conditional Pseudonymity in VANETs**," in *IEEE WCNC*, NJ, USA, Apr. 2010.

[8] N. Bißmeyer *et al.*, "**CoPRA: Conditional Pseudonym Resolution Algorithm in VANETs**," in *WONS*, Canada, Mar. 2013.

[9] M. Khodaei *et al.*, "**Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure**," in *IEEE VNC*, Paderborn, Germany, Dec. 2014.

[10] M. Khodaei, *et al.*, "**SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems**," *in the IEEE TITS*, Mar. 2018. Online: https://arxiv.org/abs/1707.05518.

[11] D. Förster *et al.*, "**PUCA: A Pseudonym Scheme with User-Controlled Anonymity for Vehicular Ad-Hoc Networks (VANET)**," in *IEEE VNC*, Paderborn, Germany, Dec. 2014.

[12] M. Khodaei *et al.*, "**Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems**," in *Proceedings of the IoV-VoI*, Paderborn, Germany, pp. 7–12, July 2016.

[13] G. Calandriello *et al.*, "**On the Performance of Secure Vehicular Communication Systems**," *IEEE TDSC*, vol. 8, no. 6, pp. 898–912, Nov. 2011.

[14] J. Camenisch *et al.*, "**How to Win the Clonewars: Efficient Periodic n-Times Anonymous Authentication**," in *ACM CCS*, NY, USA, Oct. 2006, pp. 201–210, Oct. 2006.

RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd

Mohammad Khodaei, Andreas Messing, and Panos Papadimitratos

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

Royal Institute of Technology (KTH)
Stockholm, Sweden

Nov. 28, 2017

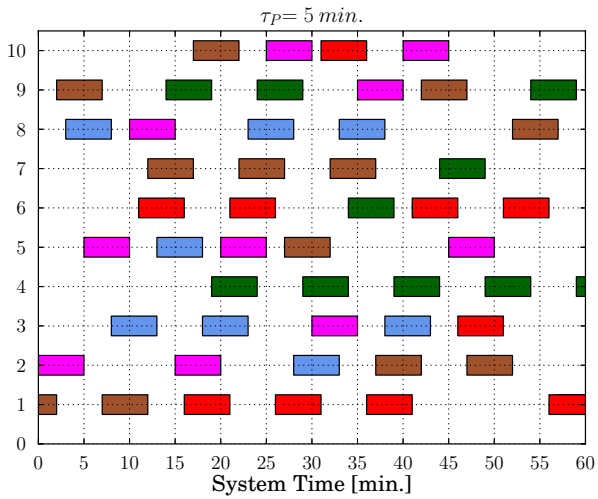
Probability of Linking Pseudonyms with RHyTHM

- $Pr = \frac{K}{[K+(N-K)\times(1-r)]^2} + \frac{N-r\times(N-K)-K}{[K+(N-K)\times(1-r)]^2} \times (1-r)$

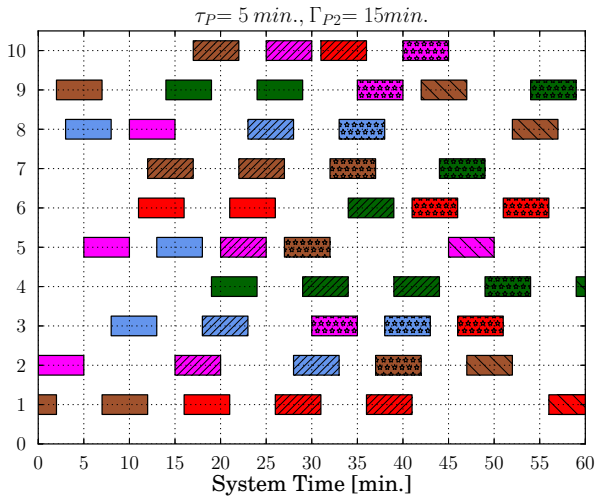
- **The first term:**
  - $\frac{K}{[K+(N-K)\times(1-r)]}$: the probability of the pseudonym being in K set.
  - $\frac{1}{[K+(N-K)\times(1-r)]}$: the probability of linking it to its successive pseudonym.
  - The denominator is the size of the entire VPKI-provided pseudonym set.

- **The second term:**
  - $\frac{N-(r)\times(N-K)-K}{[K+(N-K)\times(1-r)]}$: the probability of a pseudonym belonging to a vehicle using RHyTHM.
  - $\frac{(1-r)}{[K+(N-K)\times(1-r)]}$: the probability of linking it to its successive pseudonym.

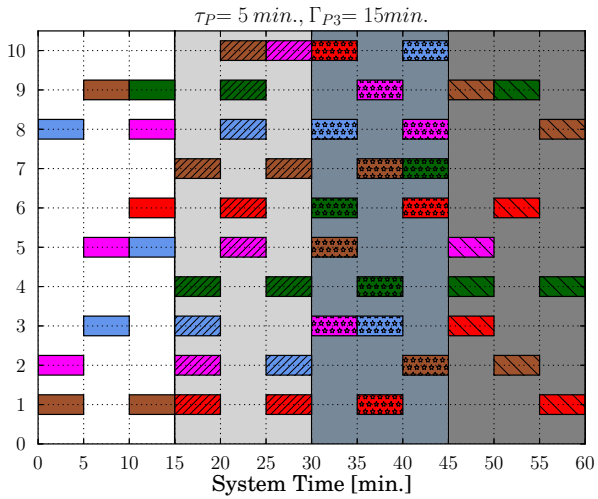
Linkability based on Timing Information of Credentials



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