Oregon State University

Thresholding Vehicular Public Key Infrastructure for Resiliency and Improved Performance Benefits

Opeyemi Ajibuwa

12/02/2022

COLLEGE OF ENGINEERING

School of Electrical Engineering and Computer Science

V2V Communication

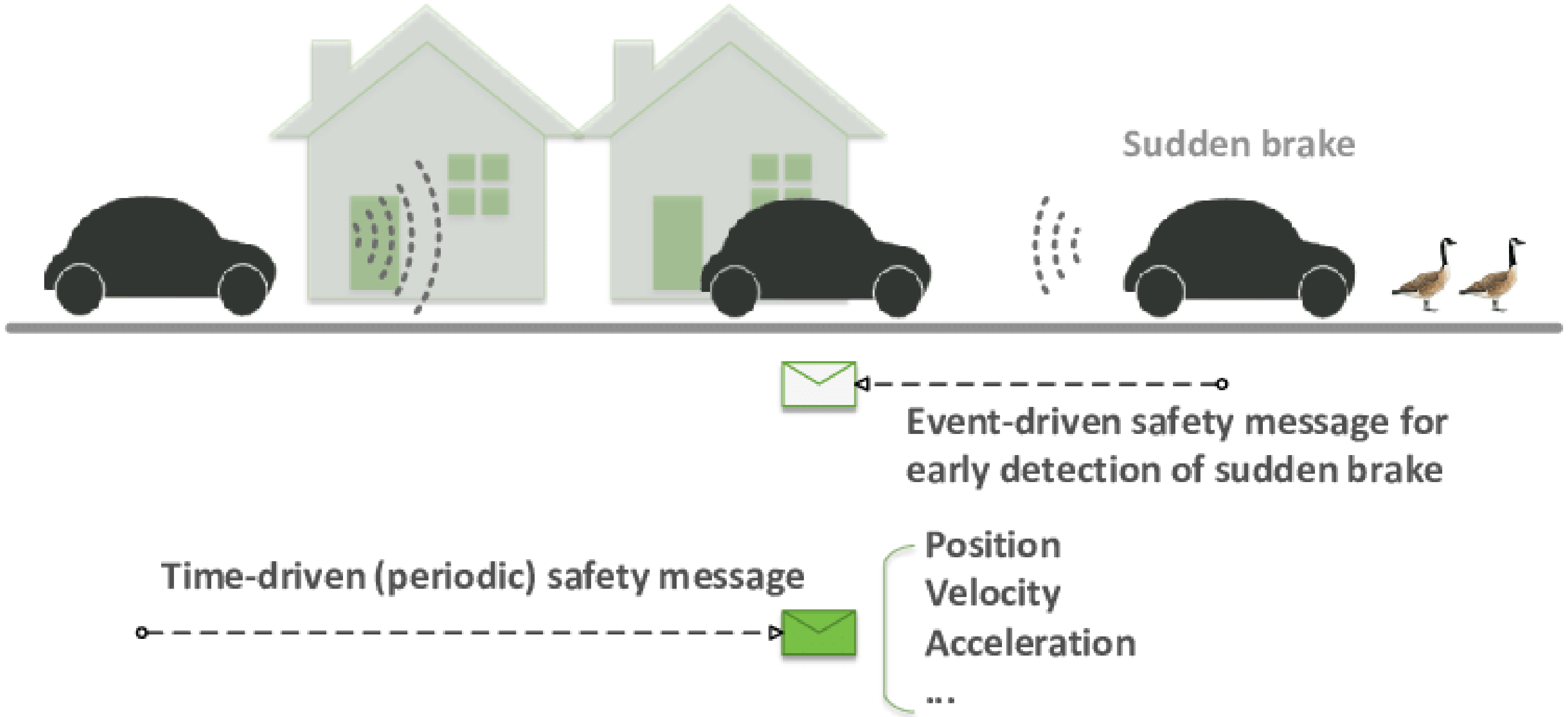
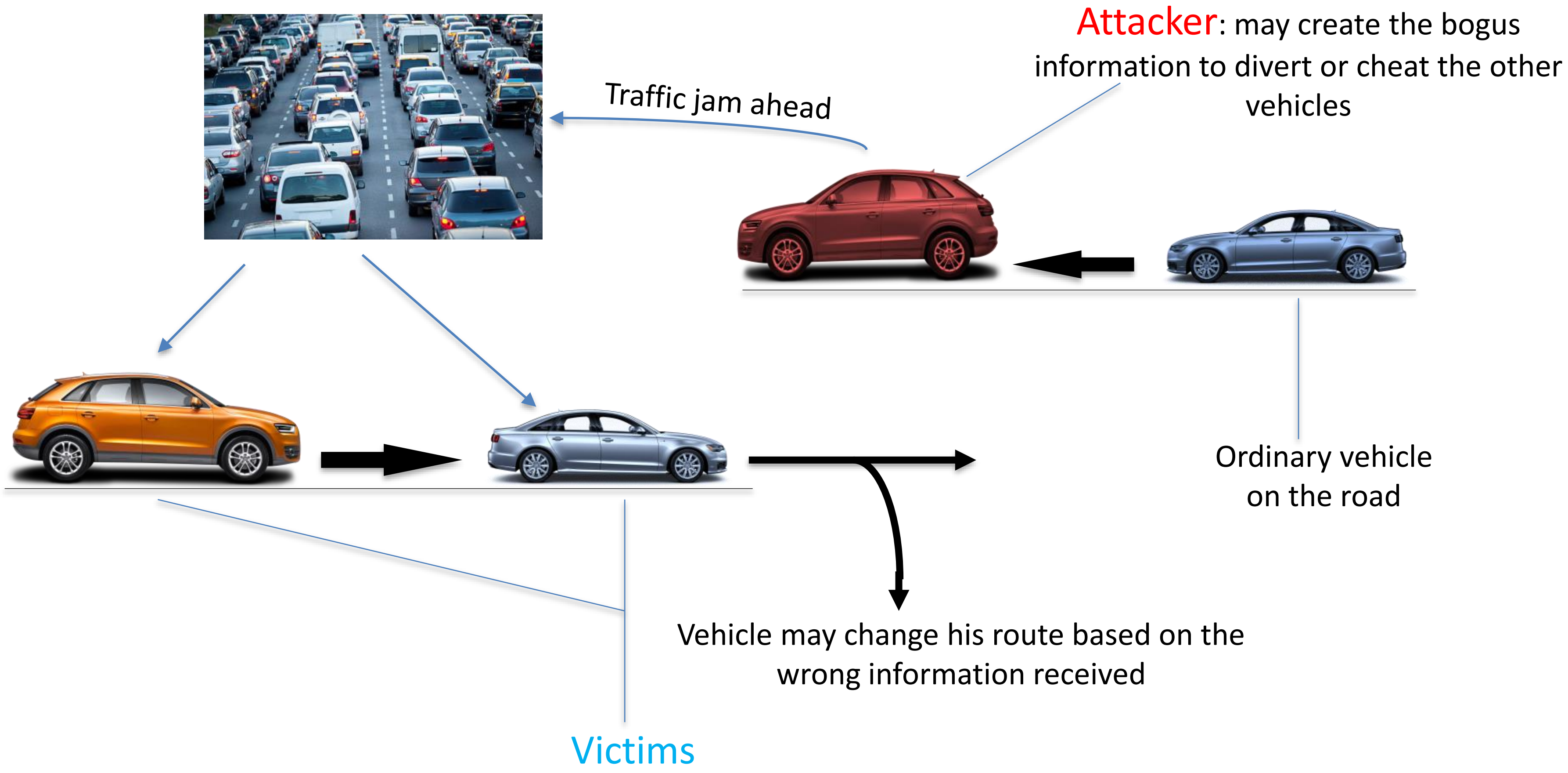


Image credit: Lu, Ning, et al. "Connected vehicles: Solutions and challenges." *IEEE internet of things journal* 1.4 (2014): 289-299.

Attacking V2V Communications

Oregon State University
College of Engineering

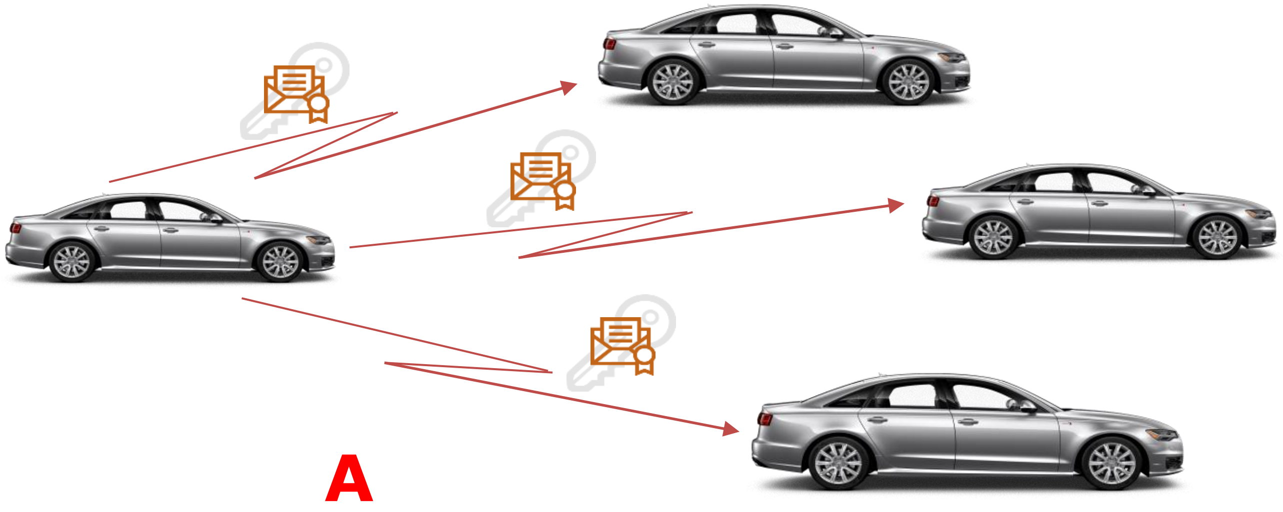


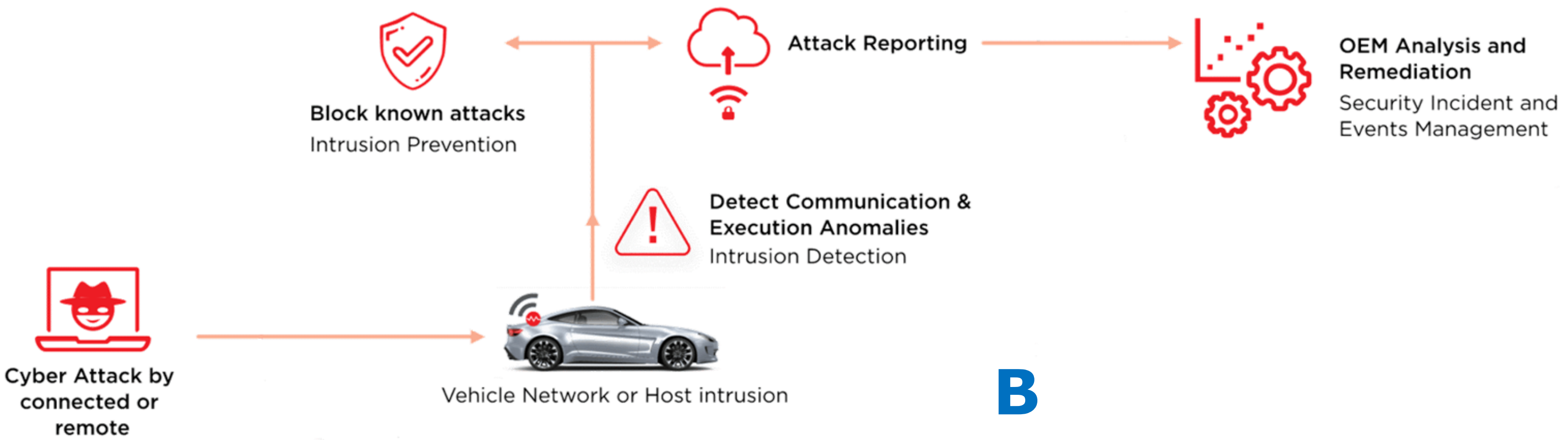
Challenges

- Safety risks
- Security issues
- Privacy violations

Securing V2V Communications

Oregon State University College of Engineering



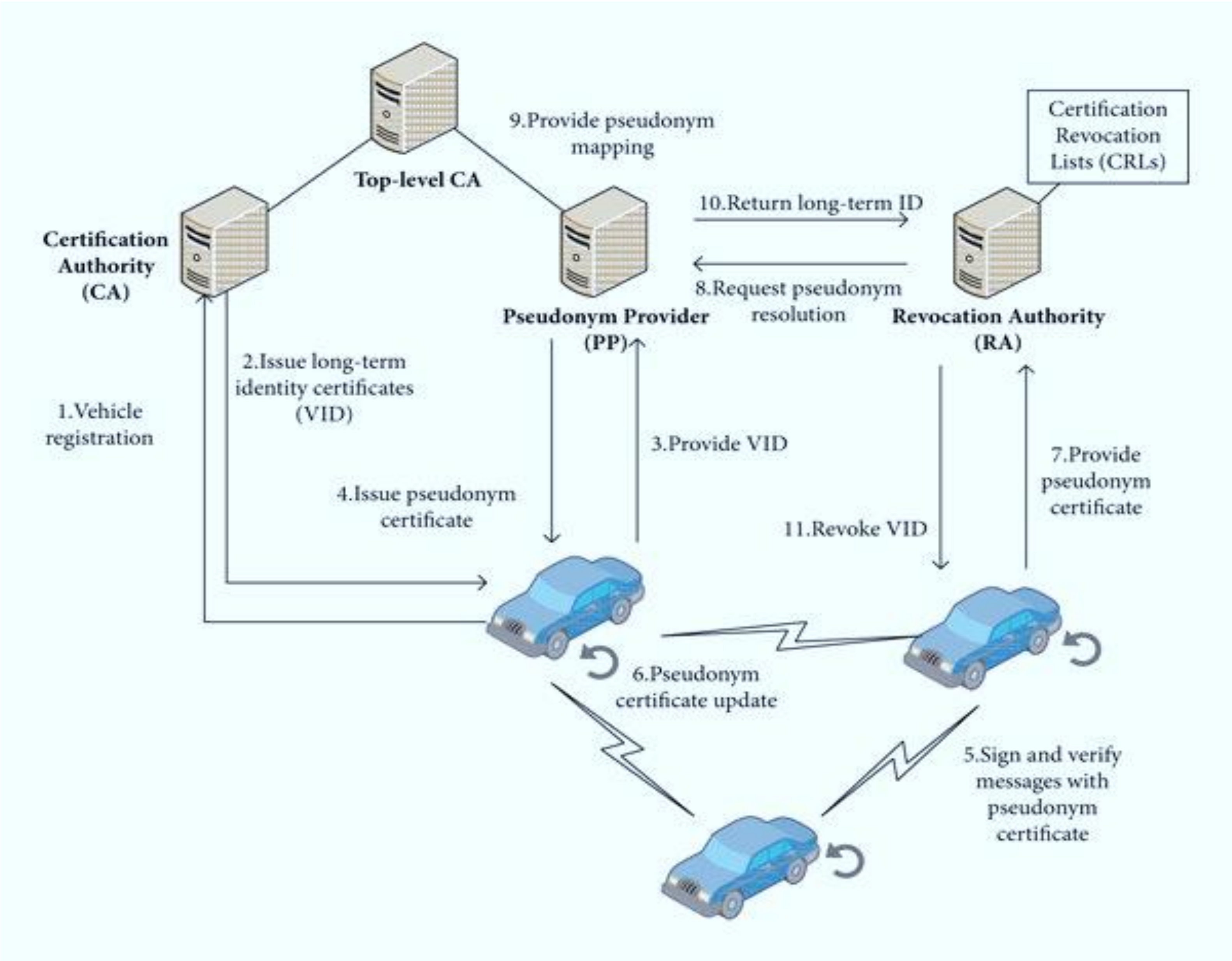


Layers of security

A. Identity and/or message authentication

B. Intrusion and/or misbehavior detection

Vehicular Public Key Infrastructure



Functions of VPKI

1. Registration Authority: Long-term identity certificate issuance (enrollment certificate)

2. Pseudonym CA: Short-term authentication certificate issuance (pseudonyms)

3. Misbehavior & Revocation Authority: Certificate revocation of misbehaving vehicles

Image credit: Chen, Liquan, et al. "V-LDAA: A New Lattice-Based Direct Anonymous Attestation Scheme for VANETs System." *Security and Communication Networks* 2021 (2021).

VPKI Design Goals and Challenges

Oregon State University
College of Engineering

Design Goals:

1. Device Authenticity
2. Data Authenticity
3. Data integrity
4. Privacy-preservation of devices and data

Challenges to VPKI:

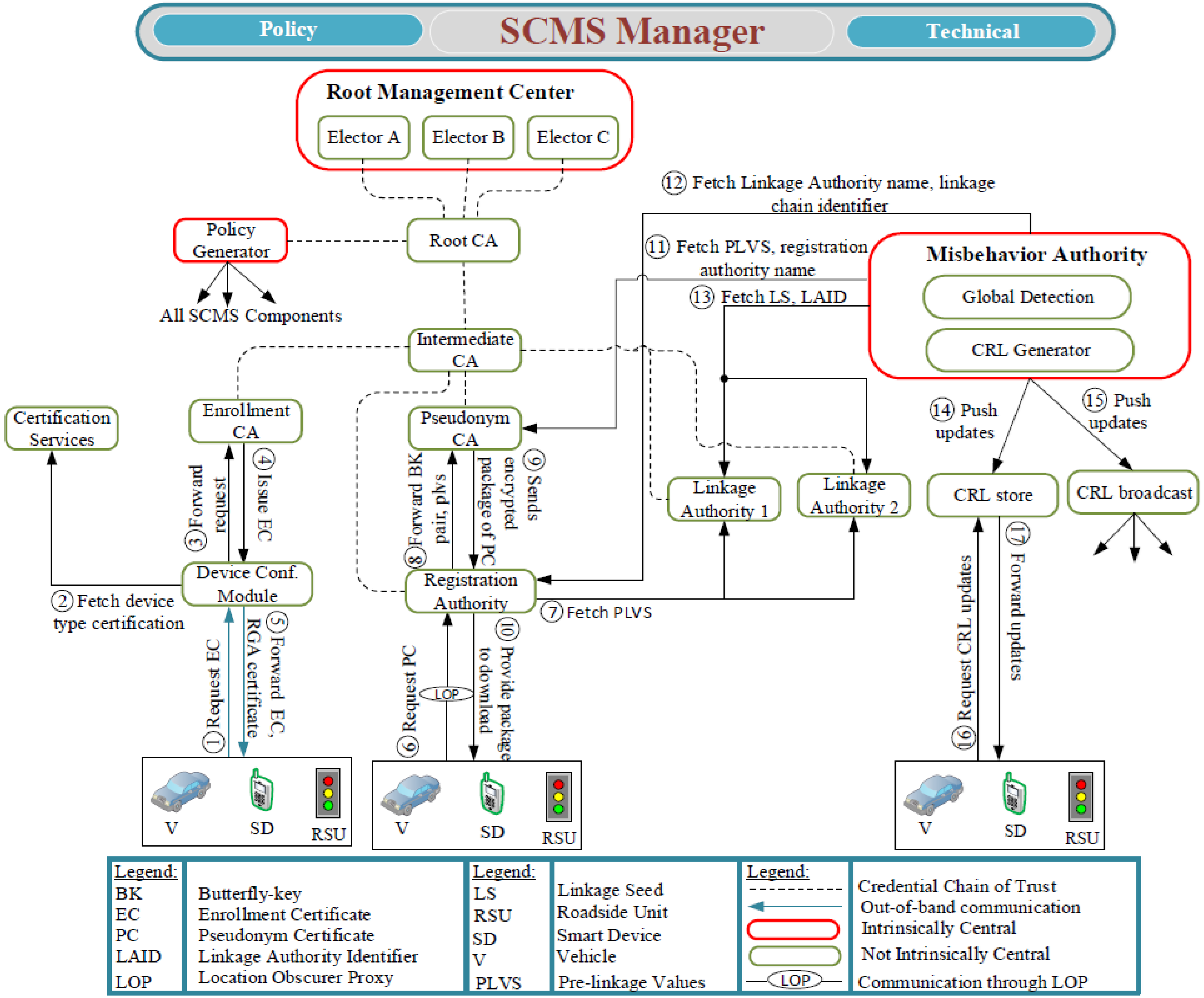
1. Strict time requirements of vehicular communications (100 ~ 300ms)
2. Limited computational capability of vehicles
3. High dynamics of network topology and limited range of V2V communication
4. Conflicting security and privacy goals

Existing VPKI Standards and Architectures

Oregon State University
College of Engineering

- *Standards*
  - *US Standard for VPKI: CRL-based architecture*
    - Security Credential Management System (SCMS)
  - *ETSI ITS European Standard: Activation code/token-based approaches*
    - Issue First Activate Later (IFAL)
- *Other VPKI Proposals:*
  - *Trusted Platform Computing Module (TPM) architectures*
    - Group signatures
    - Direct Anonymous Attestation (DAA-based) methods
  - Decentralized VPKI architectures
    - Blockchain-based schemes

Baseline SCMS and its Limitations



SCMS Features

1. Multiple pseudonyms issuance – Buttery key expansion
2. Anonymous pseudonyms issuance – Separation of roles
3. Linked pseudonyms – Through linkage values/linkage authorities

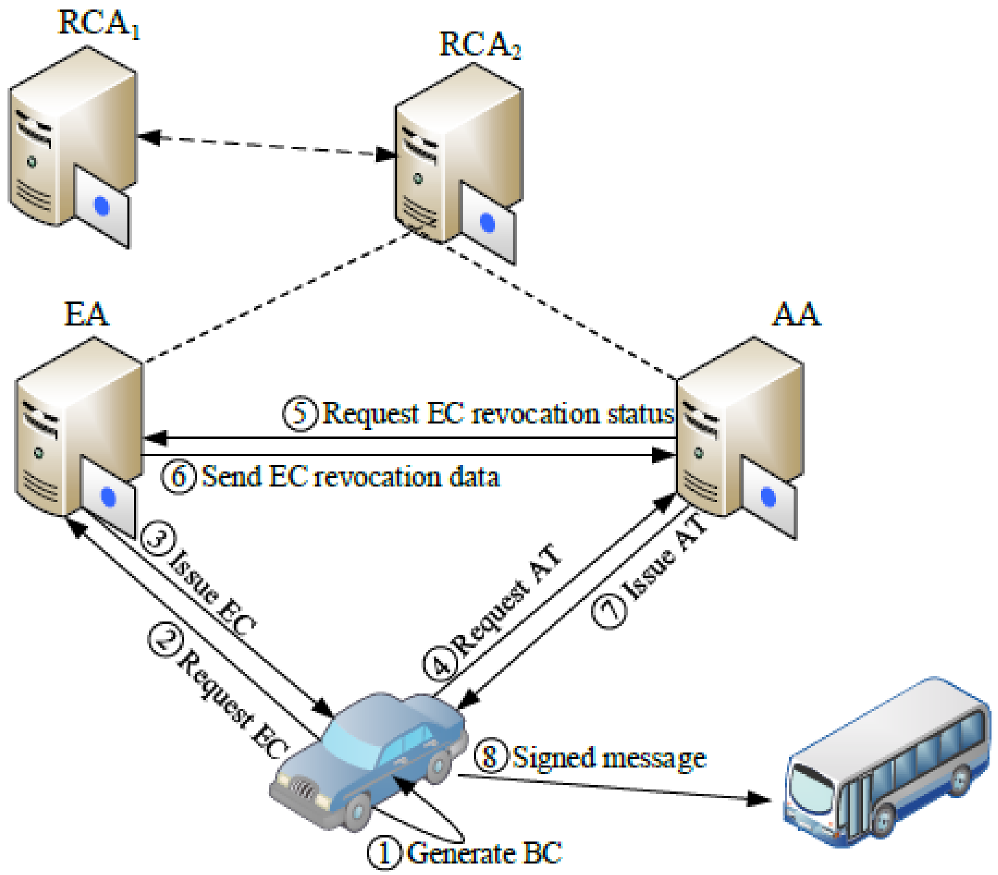
SCMS Weaknesses

1. Real-time CRL update and distribution issues
2. Scalability issues due to CRL size
3. Lack of resistance against compromise of individual entities
4. Sybil attacks

Image credit: Brecht, Benedikt, and Thorsten Hehn. "A security credential management system for V2X communications." *Connected Vehicles*. Springer, Cham, 2019. 83-115.

IFAL (ETSI-Standard) and its Limitation

Oregon State University
College of Engineering



Legend:		Legend:	
AA	Authorization Authority	EC	Enrollment Certificate
AT	Authorization Tickets	RCA	Root Certification Authority
BC	Bootstrap certificate	--------	Trust path
EA	Enrollment Authority	←- - -→	Trust Relationship

IFAL Features

1. Pseudonym issuance and revocation does not rely on CRL

2. Large pool of P-certs are preloaded at manufacture to last a lifetime

3. The pre-loaded p-certs are activated in batches with an SMS activation code from the CAs

4. In the event of misbehavior, vehicle simply does not receive activation code again for future P-certs.

IFAL Weaknesses

1. Continuous usage of P-certs activated before revocation

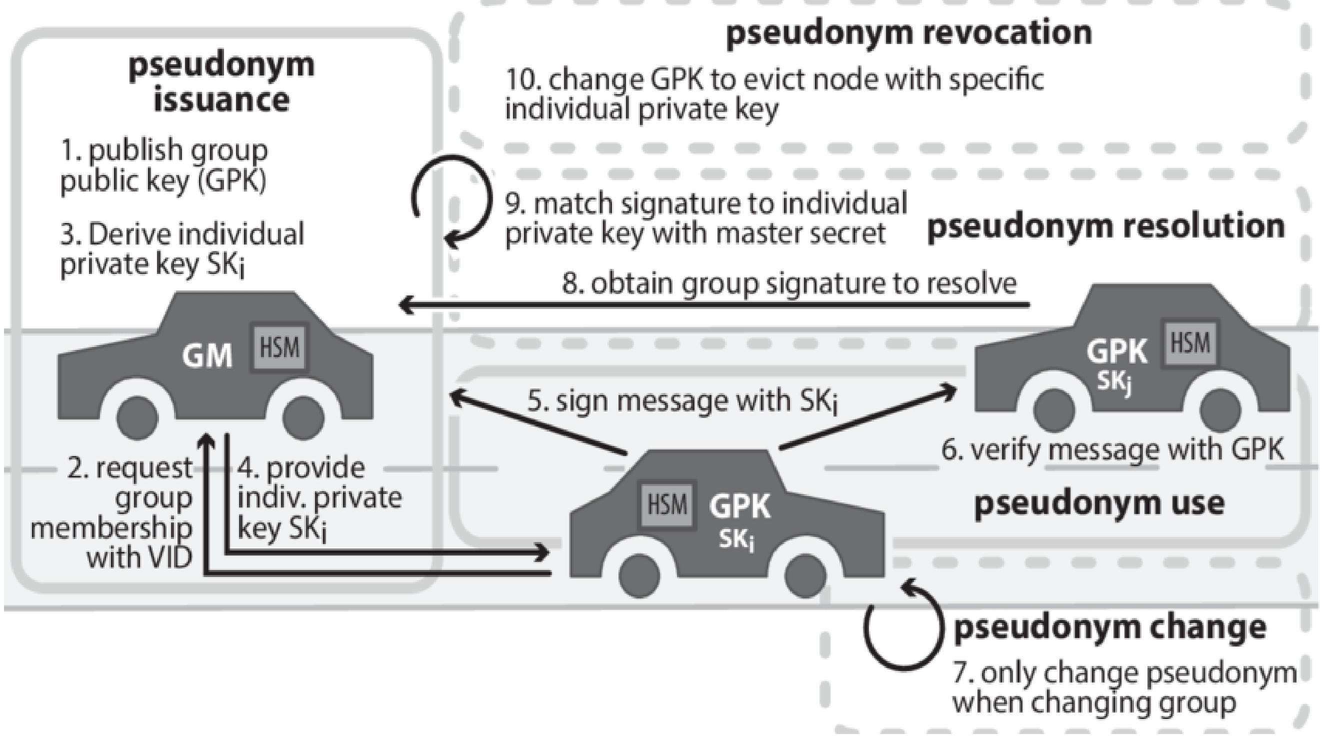
2. Scalability issues with transmission of the activation codes

3. Corrupt PCA can still issue P-certs to revoked vehicles even without any detection

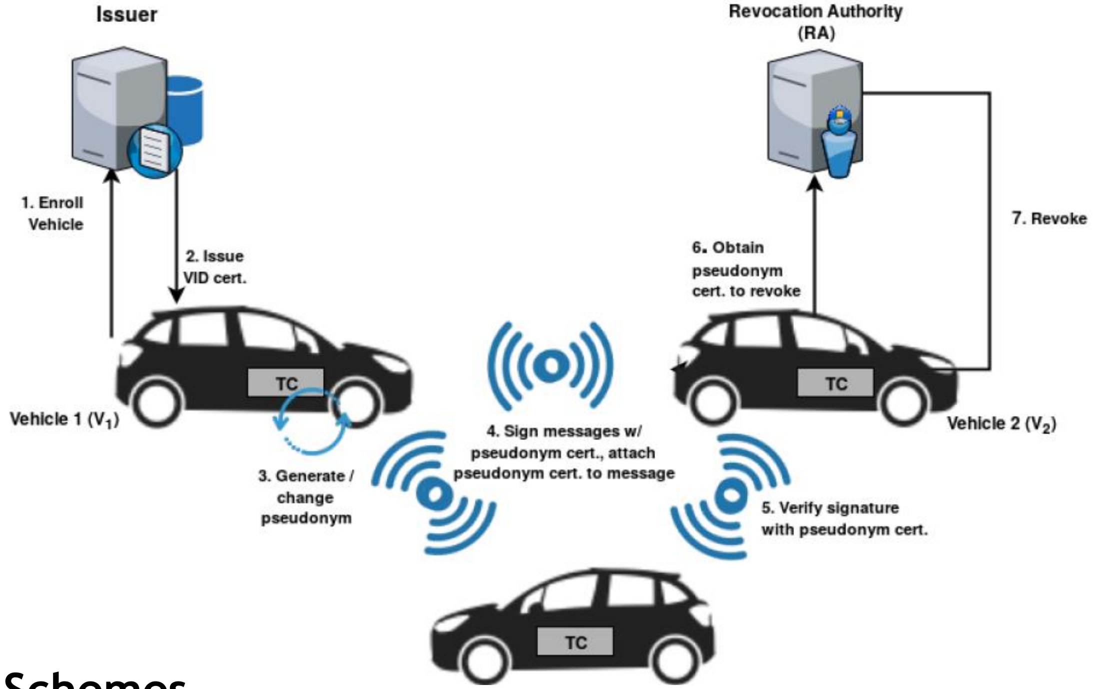
Image credit: ETSI, TS. "102 940: Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management." *Technical specification, European Telecommunications Standards Institute* (2012): 29.

Other VPKI Proposals and their Limitations

Group Signature (GS) based schemes[1]



DAA with Trusted Computing[2]



<u>Limitations of both Schemes</u>

1. Size of group signature in GS-schemes is prohibitive in real-world deployment
2. Not scalable due to heavy computational requirements associated with the underlying group-membership signature
3. DAA relies on strong hardware trust assumptions that are unrealistic in the real world

Image credit: Petit, Jonathan, et al. "Pseudonym schemes in vehicular networks: A survey." IEEE communications surveys & tutorials 17.1 (2014): 228–255.[1]
Image credit: Whitefield, Jorden, et al. "Privacy–enhanced capabilities for VANETs using direct anonymous attestation." *2017 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2017.[2]

Threshold Signatures

Oregon State University
College of Engineering

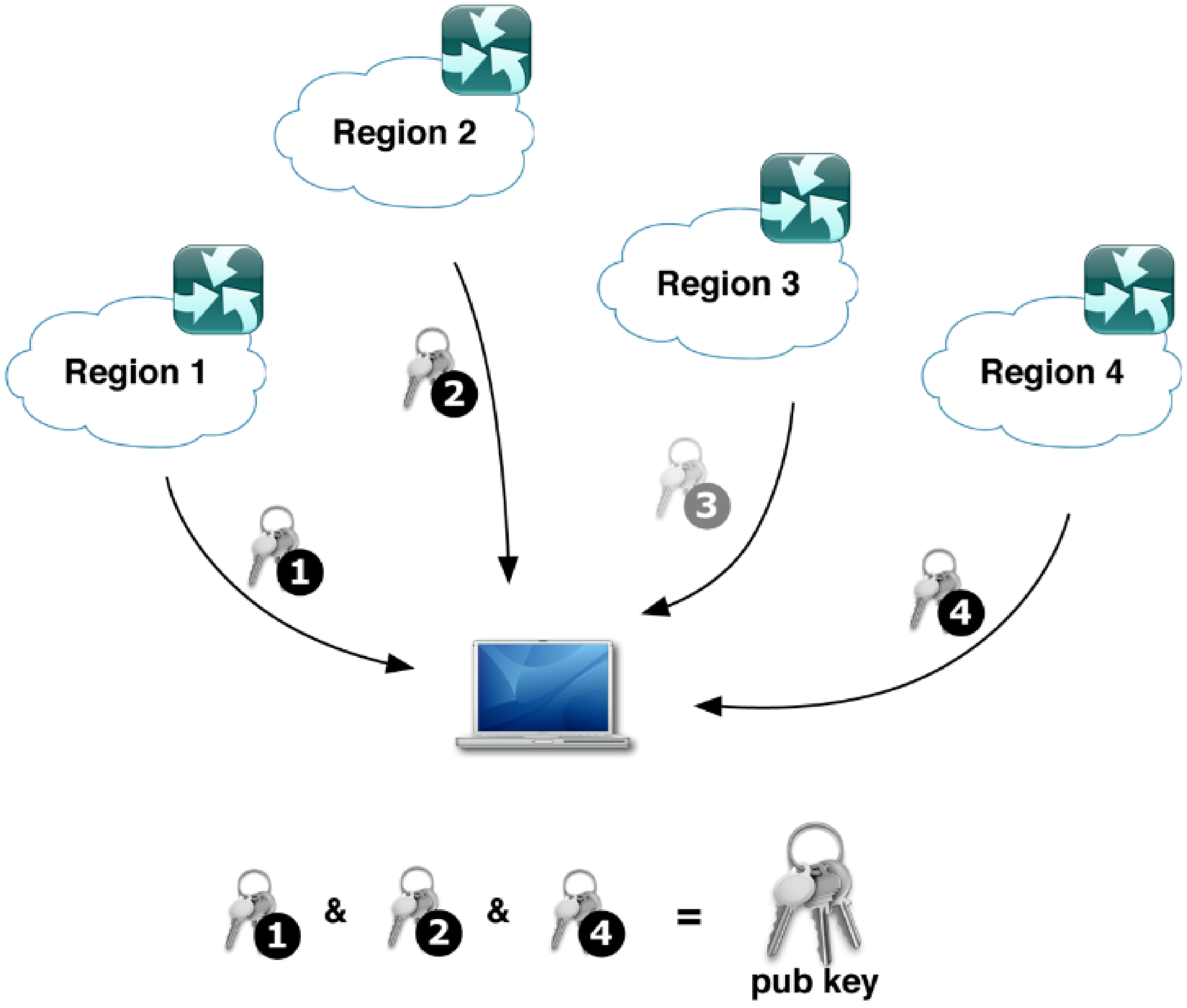
- Joint Public Key, Secret-Shared Private Key

- Threshold signature schemes (TSS) are underpinned by the notion of (t, n) secret sharing scheme

- n represents the total number of allowed participants; t the threshold

- Partitions a secret among a set of participants, such that recovering/using the secret requires cooperation among a threshold number of participants

- Secret sharing schemes were introduced independently by Shamir and Blakley (1979)



Elliptic Curve Cryptography and TSS

Oregon State University
College of Engineering

- ECC relies on the hardness problem of discovering the discrete logarithm of a random elliptic curve
- Schnorr signatures, ECDSA and EdDSA are digital signatures based on Elliptic Curve Cryptography (ECC)
- Generally, generating signatures in a threshold setting imposes overhead due to network rounds among signers, proving costly on network-limited devices or over unreliable networks [1]
- Despite ECDSA wide adoption, its non-linearity algebraic structure doesn't make it a particularly good choice for threshold signing and especially for VPKI
- ECDSA relies on complex MPC techniques and need many communication rounds and strong honest majority assumptions as well as assumptions on the reliability of the network [2]

Ref: Komlo, Chelsea, and Ian Goldberg. "FROST: flexible round–optimized Schnorr threshold signatures." International Conference on Selected Areas in Cryptography. Springer, Cham, 2020.[1]
Ref: Ruffing, Tim, et al. "ROAST: Robust asynchronous Schnorr threshold signatures." Cryptology ePrint Archive (2022).[2]

FROST: Flexible Round-Optimized Schnorr Threshold Signatures

Oregon State University
College of Engineering

- Two-round threshold signing protocol, or single-round protocol with preprocessing
- Signing operations are secure when performed concurrently, improving upon prior similar schemes
- Signing can be performed with a threshold t number of signers where t can be less than the number of possible signers n
- Secure against an adversary that controls up to t – 1 signers
- FROST derives its efficiency improvements in part by allowing the protocol to abort in the presence of a misbehaving participant
- Frost tradeoffs robustness for improved round efficiency

FROST Protocol Building Blocks

Oregon State University
College of Engineering

Single-Party Schnorr Signing and Verification

Signer		**Verifier**
$(x, Y) \leftarrow KeyGen()$		
	$\xleftarrow{(m, Y)}$	
$k \xleftarrow{\$} \mathbb{Z}_q$ $R = g^k \in \mathbb{G}$ $c = H(R, Y, m)$ $z = k + c \cdot x$		
	$\xrightarrow{(m, \sigma = (R, z))}$	
		$c = H(R, Y, m)$ $R' = g^z \cdot Y^{-c}$ Output $R \stackrel{?}{=} R'$

Image credit: Chelsea Komlo Presentation Slides, UCL Information Security Research Seminar (2020)

FROST Protocol Building Blocks

Oregon State University
College of Engineering

FROST Keygen

- Can be performed by either a trusted dealer or a Distributed Key Generation (DKG) Protocol
- The DKG is an *n*-wise Shamir Secret Sharing protocol, with each participant acting as a dealer
- After KeyGen, each participant holds secret share s_i and public key Y_i (used for verification during signing) with joint public key Y.

Image credit: Chelsea Komlo Presentation Slides, UCL Information Security Research Seminar (2020)

FROST Protocol Building Blocks

FROST Sign

- Can be performed in two rounds, or optimized to single round with preprocessing
- We show here with a signature aggregator, but can be performed without centralized roles

Image credit: Chelsea Komlo Presentation Slides, UCL Information Security Research Seminar (2020)

FROST Protocol Building Blocks

Oregon State University
College of Engineering

FROST Preprocess

Participant i | **Commitment Server**

$((d_{ij}, e_{ij}), \ldots) \xleftarrow{\$} \mathbb{Z}_q^* \times \mathbb{Z}_q^*$

$(D_{ij}, E_{ij}) = (g^{d_{ij}}, g^{e_{ij}})$

Store $((d_{ij}, D_{ij}), (e_{ij}, E_{ij}), \ldots)$

$$\xrightarrow{((D_{ij}, E_{ij}), \ldots)}$$

Store $((D_{ij}, E_{ij}), \ldots)$

Image credit: Chelsea Komlo Presentation Slides, UCL Information Security Research Seminar (2020)

FROST Protocol Building Blocks

Oregon State University
College of Engineering

FROST Sign

Signer i

Signature Aggregator

$B = ((1, D_1, E_1), \ldots, (t, D_t, E_t))$

$$\xleftarrow{(m, B)}$$

$\rho_\ell = H_1(\ell, m, B), \ell \in S$

$R = \prod_{\ell \in S} D_\ell \cdot (E_\ell)^{\rho_\ell}$

$c = H_2(R, Y, m)$

$z_i = d_i + (e_i \cdot \rho_i) + \lambda_i \cdot s_i \cdot c$

$$\xrightarrow{z_i}$$

Publish $\sigma = (R, z = \sum z_i)$

Image credit: Chelsea Komlo Presentation Slides, UCL Information Security Research Seminar (2020)

Proposed VPKI Architecture

Oregon State University College of Engineering

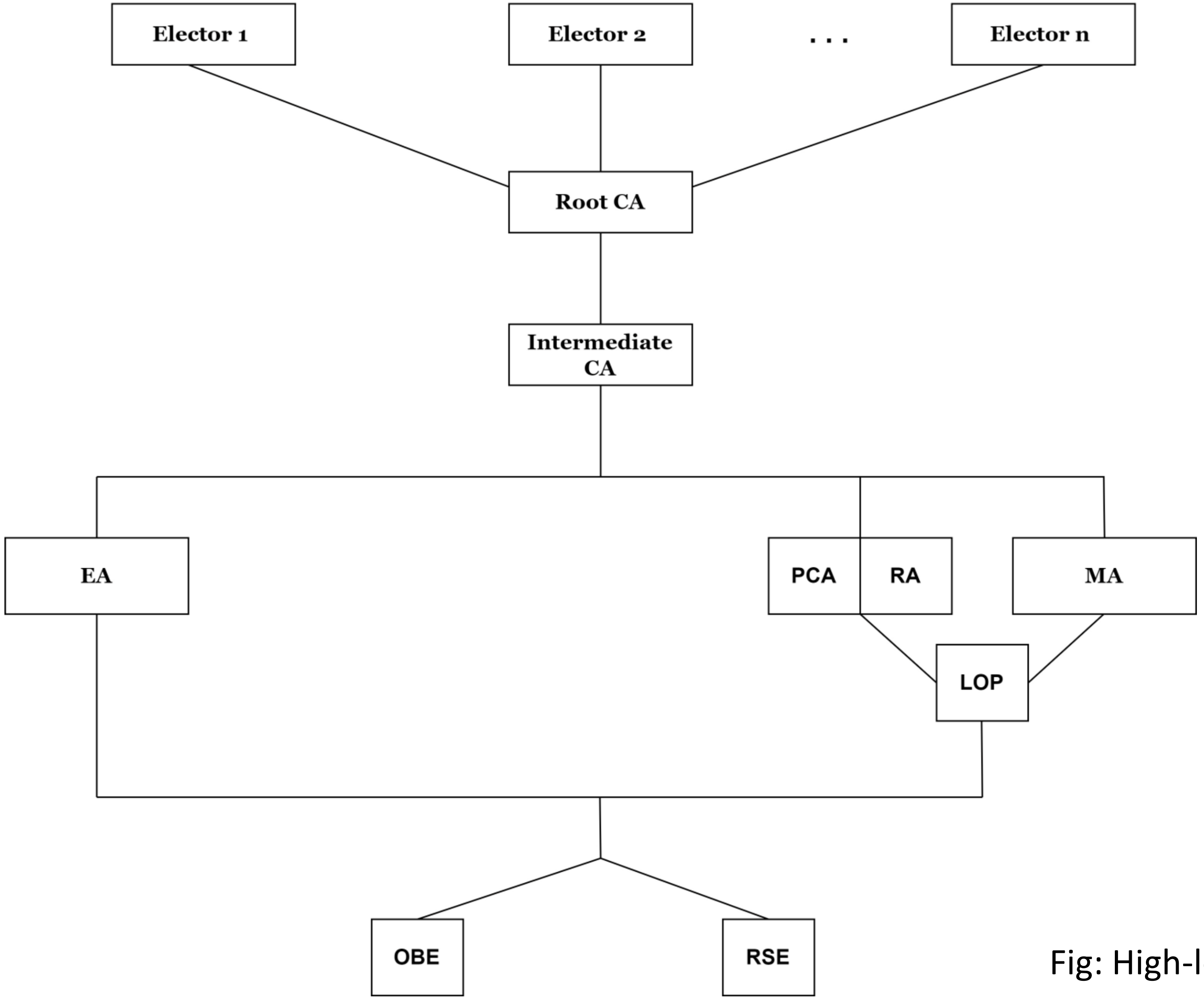
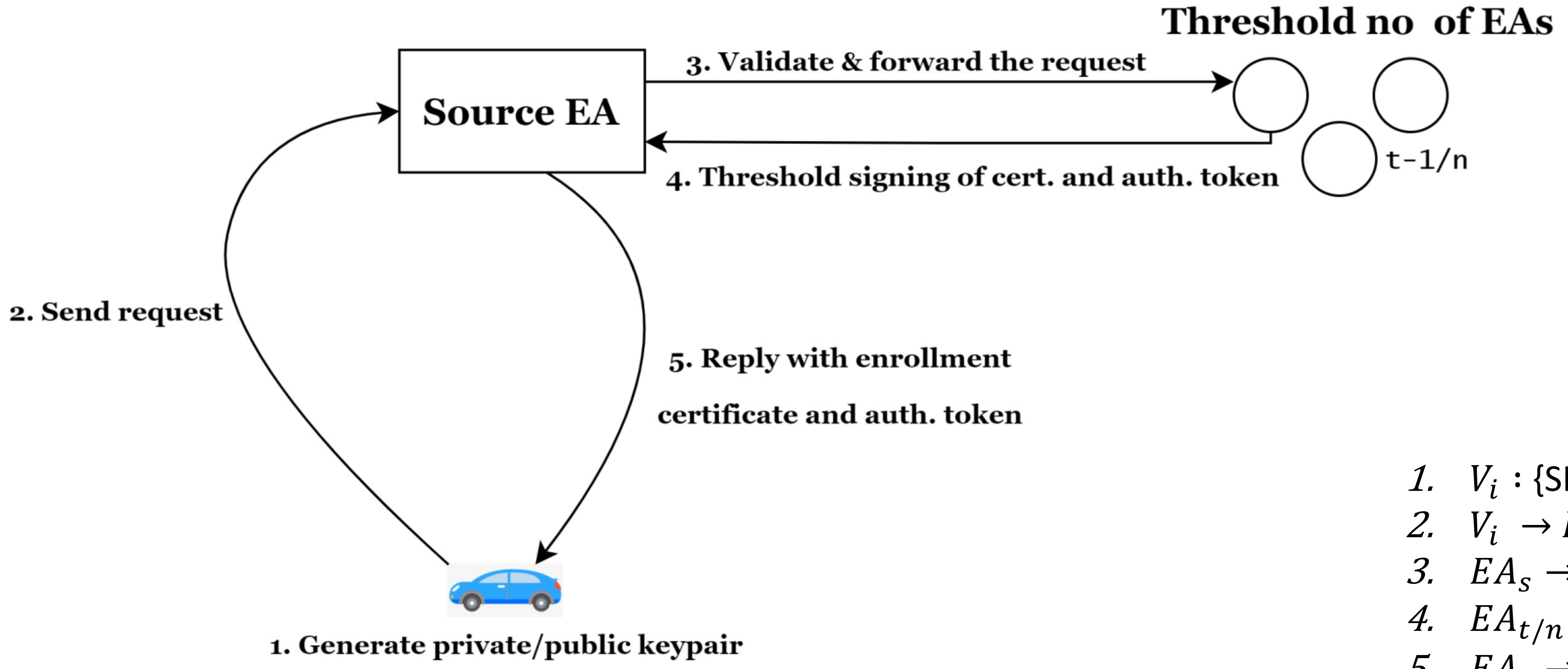


Fig: High-level overview of proposed architecture

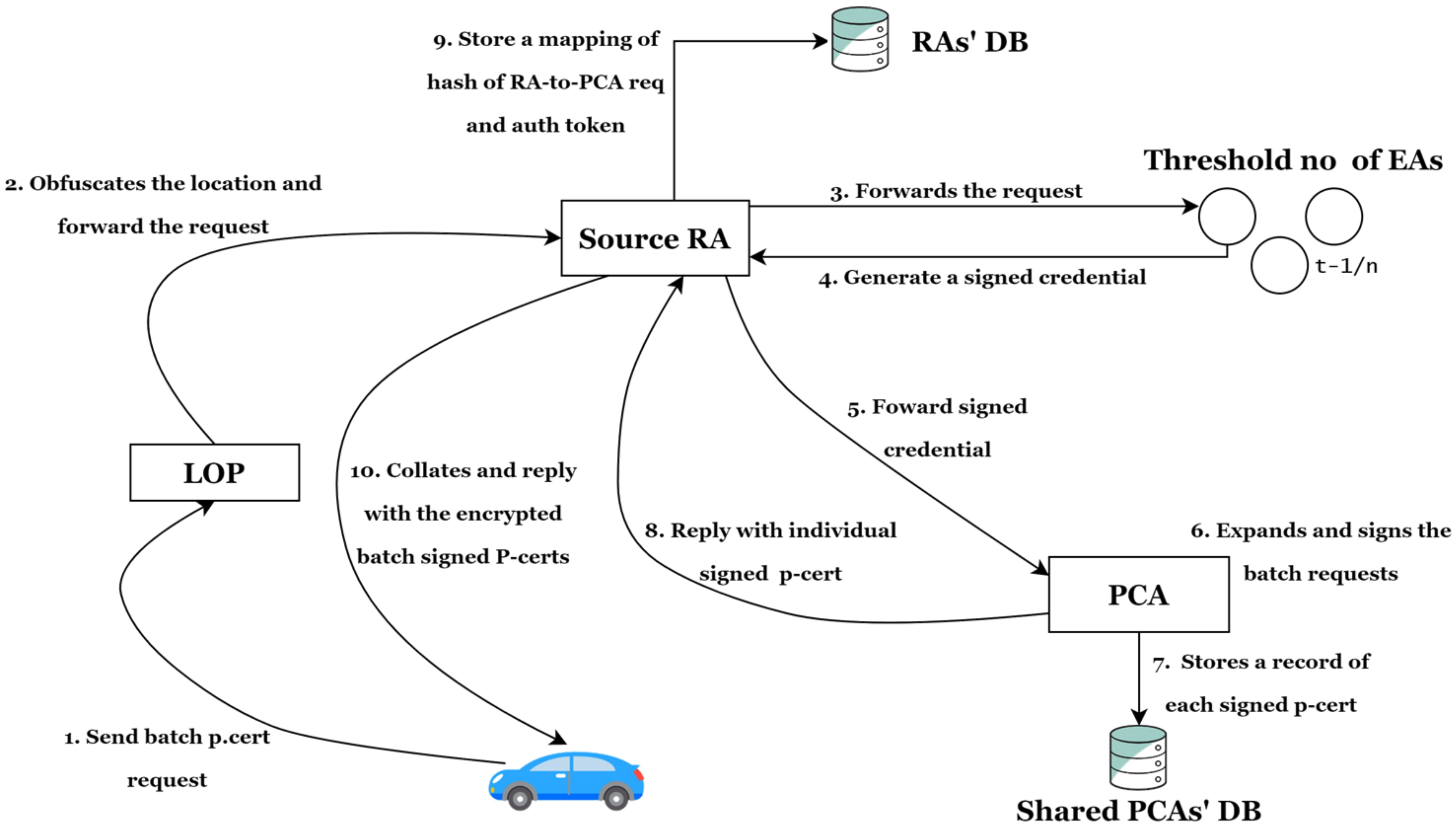
Device Enrollment in the Proposed Architecture



1. V_i : {SK, PK}
2. $V_i \rightarrow EA_s$: {VIN ‖ PK_i}
3. $EA_s \rightarrow EA_{n-1}$: {VIN ‖ PK_i}
4. $EA_{t/n}$: $Cert(PK_i$ ‖ VIN ‖ $Auth\ token)$
5. $EA_s \rightarrow V_i$: $Cert(PK_i$ ‖ VIN ‖ $Auth\ token)$

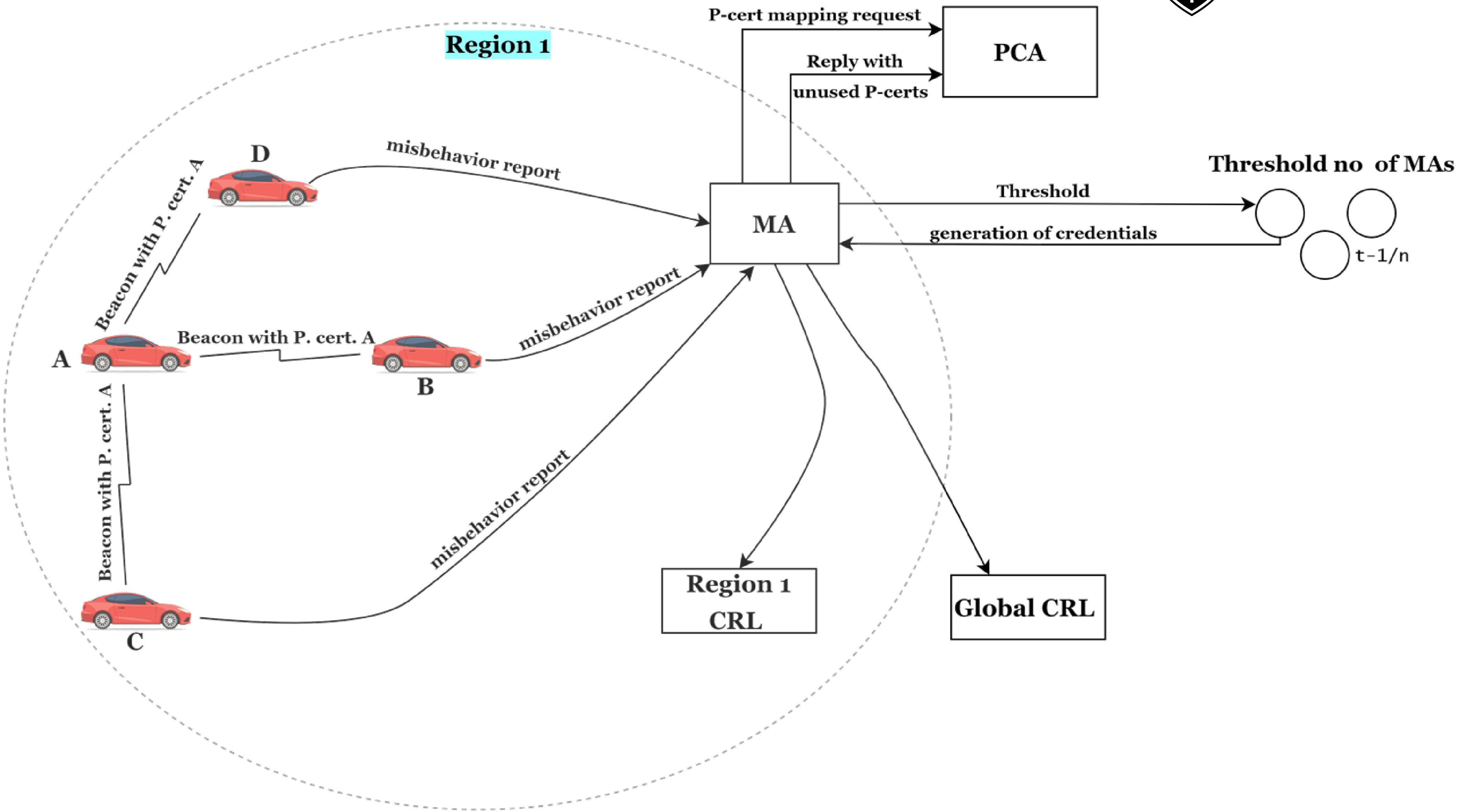
Pseudonym Provisioning in the Proposed Architecture

Oregon State University
College of Engineering



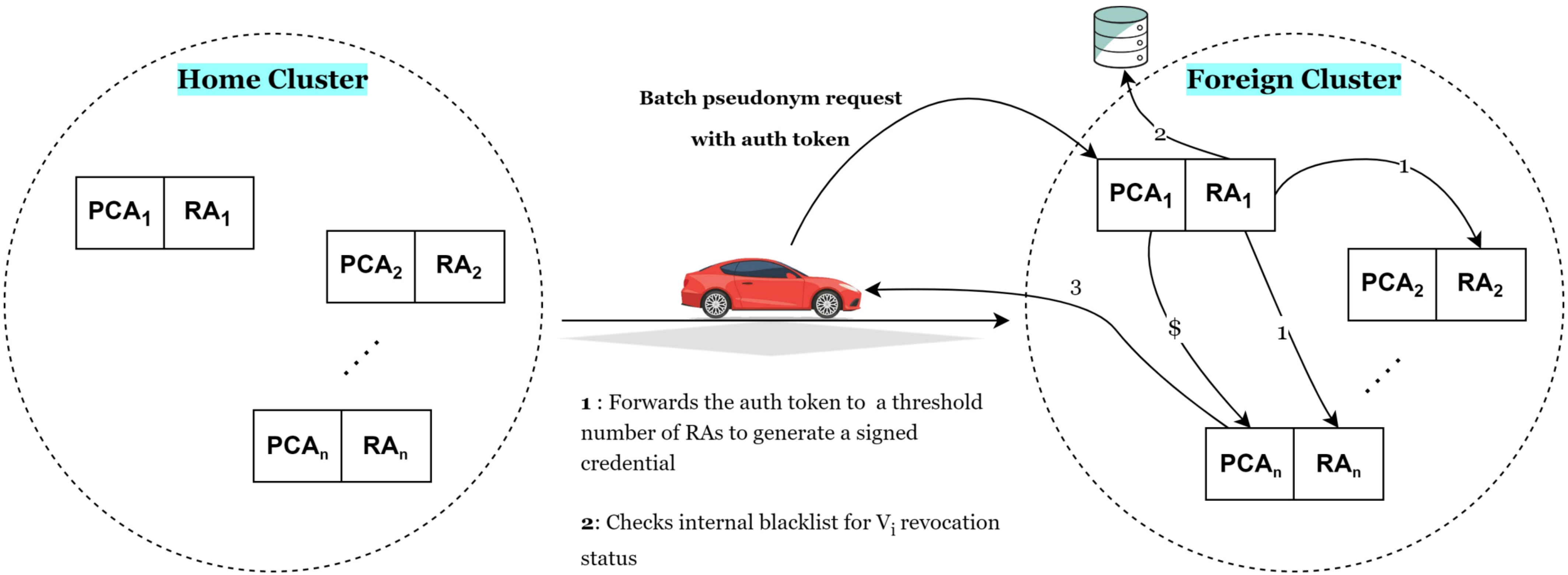
Revocation in the Proposed Architecture

Oregon State University
College of Engineering



Handover between CAs in the Proposed Architecture

Oregon State University
College of Engineering



1 : Forwards the auth token to a threshold number of RAs to generate a signed credential

2: Checks internal blacklist for V_i revocation status

3: Transmits the signed batch p-certs back to the vehicle

$: Forward signed credential and batch p-cert issuance request to a randomly selected PCA

Proposed Architecture vs Others

Oregon State University
College of Engineering

	Requirements	Description	Proposed Architecture	SCMS(2018)	IFAL(2019)	SECMACE(2018)
1	**Revocation Scalability**	To handle increasing revocation. To ensure efficient checking and distribution in case of a heavy workload. Low, Medium and High are used to measure revocation scalability.	High. Proposed architecture reduces size and latency through region-specific CRL along with the expiry of P-certs. The smaller regional CRL reduces the distribution cost and the size.	Medium. The use of a global CRL could still limit the revocation latency in the face of increasing network size even with the SCMS design of publishing a single entry for each revoked entities.	High. IFAL eliminates the use of a CRL. It stops sending activation codes for the unused p-certs of a revoked vehicle. However, the downside is that the misbehaving vehicle will continue to misbehave for as long as the activation codes for future epochs are known.	Low. All valid, unexpired p-certs of a misbehaving vehicle are added to the CRL.
2	**Real-time Revocation Validation**	It specifies the proposal's capacity to offer real-time revocation status validation services to the devices. This is a binary measure.	Yes. The proposed architecture adopts use of region-specific CRL which drastically reduce the checking and distribution time	No. SCMS proposed the use of CRL distribution.	Not applicable	No. The global size of the CRL limits its real-time revocation validation.
3	**Identity Privacy**	Device privacy says that a malicious entity should not be able to learn device's real-identities	Yes	Yes	Yes	Yes
4	**P-cert set linkage**	This says that the issuing PCA should not be able to link the set of P-certs nor link real-identities of devices during the credential provision	Yes	Yes	Not applicable	No. Issuing a bundle of P-certificates per ticket by PCA enables the issuing PCA to track the set of P-certificates.

Proposed Architecture vs Others

Oregon State University
College of Engineering

	Requirements	Description	Proposed Architecture	SCMS(2018)	IFAL(2019)	SECMACE(2018)
5	**Location Privacy**	Ensures that the verification and validation process does not know about device connection	Yes	Yes	Not applicable	No. This is not considered in the architecture.
6	**Backwards Privacy**	Revoked p-certs should not reveal further information about the P-certs used before revocation	Yes	Yes	Not applicable	Yes.
7	**Conditional Anonymity**	Anonymity is conditional in the sense that the corresponding long-term identity can be retrieved by the VPKI entities and accordingly revoked, if a vehicle deviates from system policies, e.g., submitting faulty information	Yes	Yes	Yes	Yes.
8	**Thwarting Sybil-based attacks**	VPKI should not issue multiple simultaneously valid pseudonyms for a vehicle. Binary measure	Yes. Eliminates Sybil-attack vulnerability by designing pseudonym certificates valid for specific time periods	No. Vulnerable to Sybil-attacks as SCMS allows multiple p-certs to be valid for a specific period of time.	No. With the ETSI-based architecture of IFAL, the proposed pseudonym change of every 5minutes means the scheme is vulnerable to sybil attacks.	No. Multiple p-certs are simultaneously valid in the proposed architecture.
9	**Resiliency & Reliability**	The VPKI should remain operational in the presence of benign failures (system faults or crashes) and be resilient to resource depletion attacks, e.g., DDOS attack	Yes. The threshold cryptography backbone of the proposed architecture is resilient to attacks against individual authority entities in the network.	No. SCMS architecture is not resilient to individual entities compromise	No. IFAL is not resilient to individual entities compromise.	No. SECMACE is not resilient to individual entities compromise.

Proposed Architecture vs Others

Oregon State University
College of Engineering

	Requirements	Description	Proposed Architecture	SCMS(2018)	IFAL(2019)	SECMACE(2018)
10	Unlinkability	1. Real identity of the vehicle should not be linked to its corresponding pseudonyms	Yes	Yes	Yes	Yes
		2. LTCA should know neither the targeted PCA nor the actual pseudonym acquisition periods, nor the credentials themselves	Yes	Yes	Not applicable	Not clear
		3. Successive pseudonym requests should not be linked to the same requester and to each other.	Yes	Yes	Not applicable	Not clear
		4. PCA should not be able to retrieve the long-term identity of any requester, nor link multiple pseudonym requests (of the same requester).	Yes	Yes	Not applicable	No.
		5. An external observer should not be able to link pseudonym of a specific vehicle based on information they carry, notably their timing information.	Yes	Yes	Yes	Yes
		6. To achieve full unlinkability, which results in perfect privacy, no single entity (even the PCAs) should be able to link a set of pesudoynms issued for a vehicle as a response to a single request.	Yes	Yes	Not applicable	No.
11	Short-term Linkability	For Privacy, an eavesdropper should not be able to link messages from the same OBE in the long term. However, some VANET applications require that in the short-term, a recipient be able to link two messages sent out by the same OBE.	Yes	Yes	Yes	Yes

Analytical Evaluations

Oregon State University College of Engineering

Threshold Scheme Computational Costs for Pseudonym Provisioning

	Entity	Operations	Costs
1	Vehicle Computation Overheads	i. AES decryption of batch pseudonyms ii. Batch pseudonym certificate verification	T_{dec} $(T_H + T_{SM} + T_{SA}) \times d \times B$
2	RA Computation Overheads	i. Auth token validation	$(T_H + T_{SM} + T_{SA}) \times d$
		ii. Threshold credential signing	$(\propto^2 + 2\propto + 1) \times T_H$ $(\propto^2 + 3\propto) \times T_{SM}$ $(\propto^2 + 3\propto) \times T_{SA}$ $(2\propto) \times T_{BM}$
3	PCA Computation Overheads	i. RA credential verification	$(T_H + T_{SM} + T_{SA}) \times d - 1$
		ii. Batch request expansion and individual pseudonym signing	$(T_H + T_{SM} + T_{BM}) \times B$
		iii. Encryption of batch pseudonym certs.	T_{enc}

T_H : Time for SHA-256 one-way hashing = 0.006ms
T_{SM}: Time for ECC scalar multiplication = 0.4400ms
T_{SA} : Time for ECC scalar addition = 0.0018ms
d = depth of trust = 3
B = Batch pseudonym size = 30
$\propto$ = Actual number of signing participants (for t/n)
T_{BM}: Time for Big integer multiplication = 0.005ms
T_{enc} : Time for AES symmetric encryption = 0.041ms
T_{dec} : Time for AES symmetric decryption

Ref: Hakeem, Shimaa A. Abdel, Mohamed A. Abd El−Gawad, and HyungWon Kim. "A decentralized lightweight authentication and privacy protocol for vehicular networks." IEEE Access 7 (2019): 119689−119705..[1]
Ref: Othman, Wajdy, et al. "Physically secure lightweight and privacy−preserving message authentication protocol for VANET in smart city." IEEE Transactions on Vehicular Technology 70.12 (2021): 12902−12917.[2]

Analytical Evaluations

Oregon State University College of Engineering

Conventional Scheme Computational Costs for Pseudonym Provisioning

	Entity	Operations	Costs
1	Vehicle Computation Overheads	i. AES decryption of batch pseudonyms	T_{dec}
		ii. Batch pseudonym certificate verification	$(T_H + T_{SM} + T_{SA}) \times d \times \mathrm{B}$
2	RA Computation Overheads	i. Auth token validation	$(T_H + T_{SM} + T_{SA}) \times d$
		ii. Credential signing	$T_H + T_{SM} + T_{BM}$
3	PCA Computation Overheads	i. RA credential verification	$(T_H + T_{SM} + T_{SA}) \times d - 1$
		ii. Batch request expansion and individual pseudonym signing	$(T_H + T_{SM} + T_{BM}) \times \mathrm{B}$
		iii. Encryption of batch pseudonym certs.	T_{enc}

T_H : Time for SHA-256 one-way hashing = 0.006ms
T_{SM}: Time for ECC scalar multiplication = 0.4400ms
T_{SA} : Time for ECC scalar addition = 0.0018ms
d : depth of trust = 3
B : Batch pseudonym size = 30
T_{BM}: Time for Big integer multiplication = 0.005ms
T_{enc} : Time for AES symmetric encryption = 0.041ms
T_{dec} : Time for AES symmetric decryption

Ref: Hakeem, Shimaa A. Abdel, Mohamed A. Abd El-Gawad, and HyungWon Kim. "A decentralized lightweight authentication and privacy protocol for vehicular networks." IEEE Access 7 (2019): 119689-119705..[1]
Ref: Othman, Wajdy, et al. "Physically secure lightweight and privacy-preserving message authentication protocol for VANET in smart city." IEEE Transactions on Vehicular Technology 70.12 (2021): 12902-12917.[2]

Handover Requests for Threshold vs. Conventional

Conventional: Number of handover requests = Number of regions traversed

Threshold: Number of handover requests = $\frac{\text{Network size (n)}}{\text{Cluster size (k)}}$

Network size ≡ Number of regions in the network

Analytical Evaluations

Oregon State University
College of Engineering

Threshold Scheme Message Communication Costs for Pseudonym Provisioning

	Entity	Operations	Costs	
1	Vehicle Communication Overheads	Batch pseudonym request and auth token transmission	$(PK_i)B \parallel Auth.token \parallel T$	1032 bytes
2	RA Communication Overheads	i. Auth token broadcast to ∝ RAs	$(Auth.token) \propto$	68∝ bytes
		ii. Signed credential and batch request transmission to PCA	$Cred \parallel (PK_i)B \parallel T$	1032 bytes
		iii. Signed batch pseudonym transmission to vehicle	$(Cert)B \parallel K_{enc}$	2192 bytes
		iv. Transmission of the hash of RA-to-PCA request to PCA	$\mathrm{H}(Cred \parallel PK_i \parallel (B \propto))$	32 bytes
3	PCA Communication Overheads	Signed batch pseudonym transmission to RA	$(Cert)B \parallel K_{enc}$	2192 bytes

Public key (PK_i) = 32 bytes
Time period (T) = 4 bytes
AES Encryption Key (K_{enc}) = 32 bytes
Batch size (B) = 30

Auth token = Schnorr signature (64bytes) + Anonymous Identifying information (4bytes)
Cred size = Schnorr signature (64bytes) + prefix information (4bytes)
Pseudonym certificate = Schnorr signature (64bytes) + metadata (8bytes)
Hash of RA-to-PCA request size = 32 bytes

Analytical Evaluations

Oregon State University College of Engineering

Conventional Scheme Communication Costs for Pseudonym Provisioning

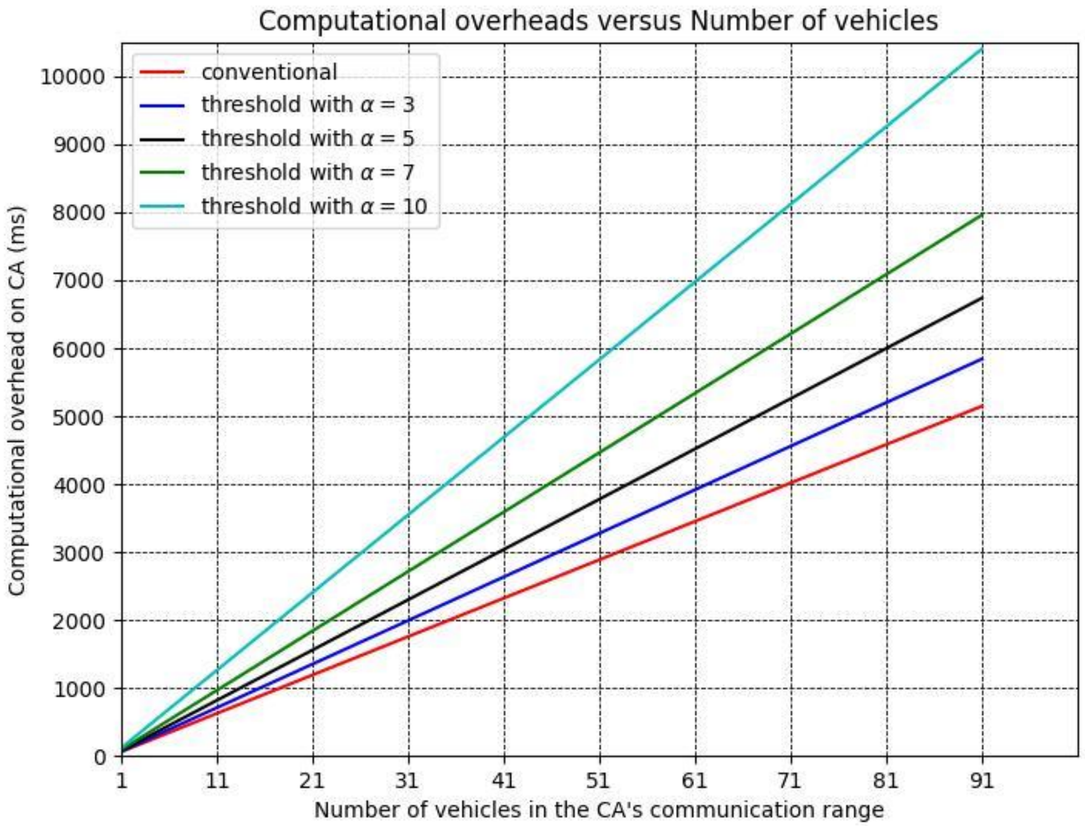
	Entity	Operations	Costs	
1	Vehicle Communication Overheads	Batch pseudonym request and auth token transmission	$(PK_i)B \parallel Auth.token \parallel T$	1032 bytes
	RA Communication Overheads	ii. Signed credential and batch request transmission to PCA	$Cred \parallel (PK_i)B \parallel T$	1032 bytes
		iii. Signed batch pseudonym transmission to vehicle	$(Cert)B \parallel K_{enc}$	2192 bytes
		iv. Transmission of the hash of RA-to-PCA request to PCA	$\mathrm{H}(Cred \parallel PK_i \parallel (B))$	32 bytes
3	PCA Communication Overheads	Signed batch pseudonym transmission to RA	$(Cert)B \parallel K_{enc}$	2192 bytes

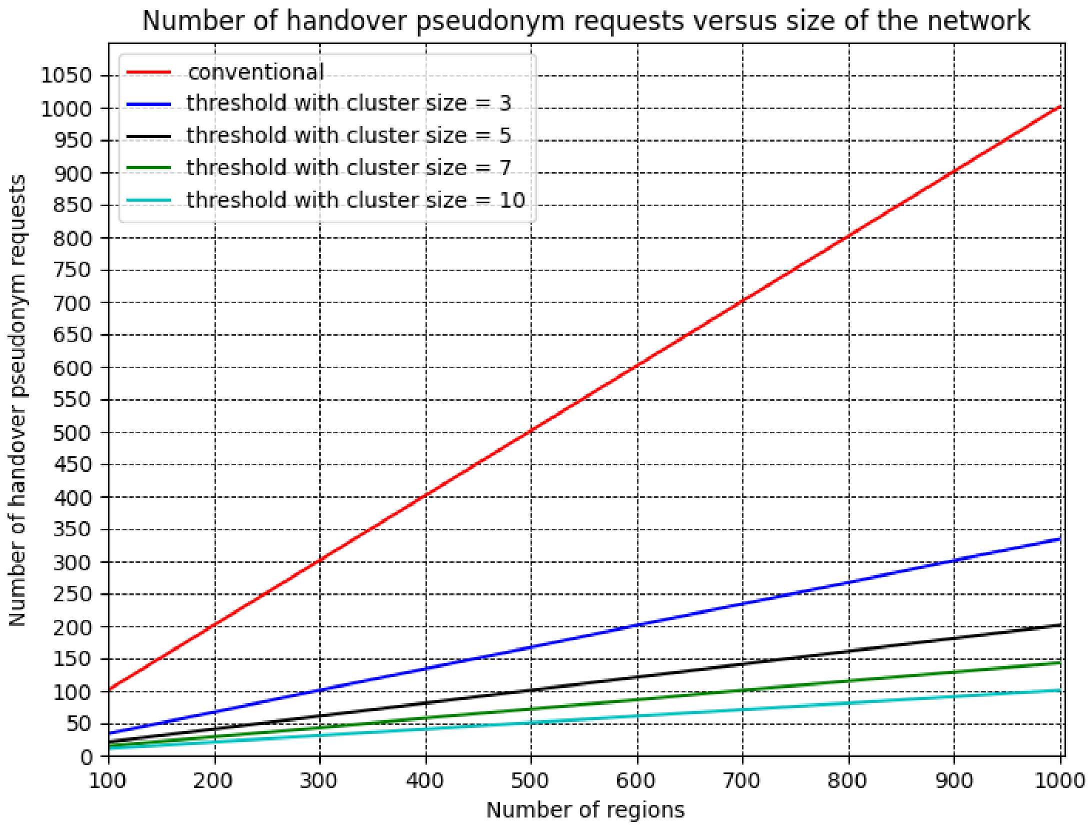
Public key (PK_i) = 32 bytes
Time period (T) = 4 bytes
AES Encryption Key (K_{enc}) = 32 bytes
Batch size (B) = 30

Auth token = Schnorr signature (64bytes) + Anonymous Identifying information (4bytes)
Cred size = Schnorr signature (64bytes) + prefix information (4bytes)
Pseudonym certificate = Schnorr signature (64bytes) + metadata (8bytes)
Hash of RA-to-PCA request size = 32 bytes

Analytical Results of Proposed Architecture

Oregon State University
College of Engineering





Computational Overheads

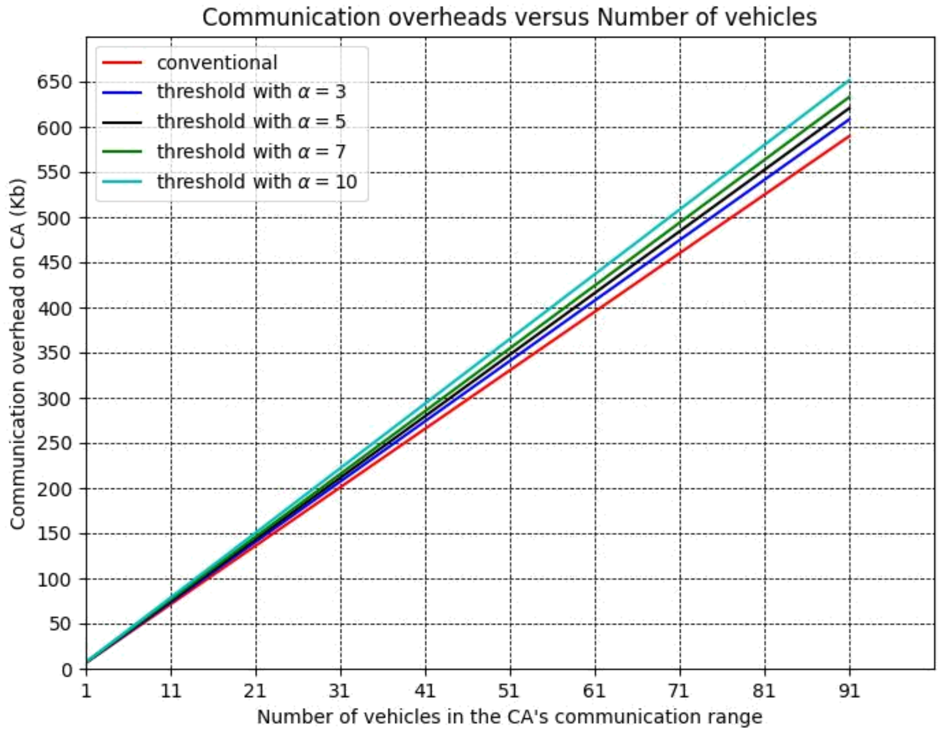
No of vehicles	1	10	20	30	40	50	60	70	80	90
Conventional	56.56	622.19	1187.82	1753.45	2319.08	2884.71	3450.34	4015.97	4581.6	5147.23
Threshold with α = 3	64.19	706.09	1348	1989.9	2631.81	3273.71	3915.61	4557.52	5199.4	5841.33
Threshold with α = 5	74.05	814.55	1555.05	2295.55	3036.05	3776.55	4517.05	5257.55	5998.1	6738.55
Threshold with α = 7	87.49	962.41	1837.33	2712.25	3587.17	4462.09	5337.01	6211.93	7086.9	7961.77
Threshold with α = 10	114.4	1258.1	2401.81	3545.53	4689.25	5832.97	6976.69	8120.41	9264.1	10407.9

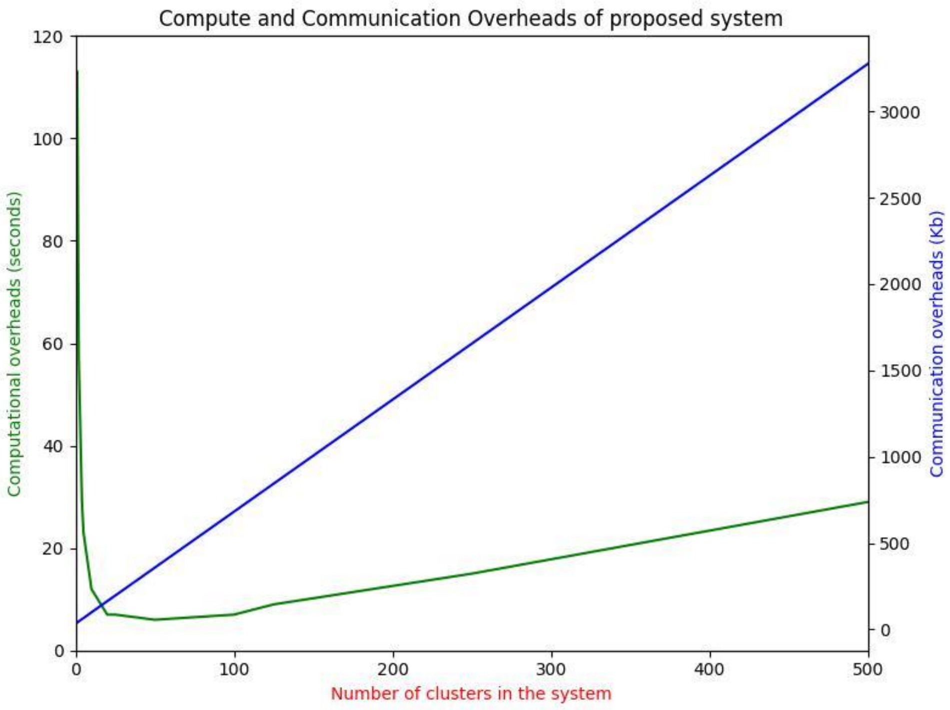
Handover Requests

No of regions	100	200	300	400	500	600	700	800	900	1000
Conventional	99	199	299	399	499	599	699	799	899	999
Threshold with a = 3	34	67	101	134	167	201	234	267	301	334
Threshold with a = 5	21	41	61	81	101	121	141	161	181	201
Threshold with a = 7	15	29	43	58	72	86	101	115	129	143
Threshold with a = 10	11	21	31	41	51	61	71	81	91	101

Analytical Results of Proposed Architecture

Oregon State University
College of Engineering





Communication Overheads

No of vehicles	1	10	20	30	40	50	60	70	80	90
Conventional (Kb)	6.48	71.28	136.08	200.88	265.68	330.48	395.28	460.08	524.88	589.68
Threshold with a = 3 (Kb)	6.68	73.52	140.36	207.2	274.04	340.88	407.72	474.56	541.4	608.24
Threshold with a = 5 (Kb)	6.82	75.02	143.22	211.42	279.62	347.82	416.02	484.22	552.42	620.62
Threshold with a = 7 (Kb)	6.96	76.52	146.08	215.64	285.2	354.76	424.32	493.88	563.44	633
Threshold with a = 10 (Kb)	7.16	78.76	150.36	221.96	293.56	365.16	436.76	508.36	579.96	651.56

Overheads vs no of clusters in the system

No of clusters	1	2	4	5	10	20	25	50	100	125	250	500
computational overheads (s)	113	57	29	23	12	7	7	6	7	9	15	29
communication overheads (Kb)	40	47	60	66	99	164	196	358	682	844	1654	3274

Other Performance Metrics for Proposed Scheme

Oregon State University
College of Engineering

1) End-to-end processing delay for long-term certificate issuance (threshold vs conventional)

2a) End-to-end processing delay for pseudonym provisioning threshold vs conventional)

2b) Threshold scalability: Number of batch pseudonym requests versus the end-to-end processing delay

2c) Threshold vs. Conventional: Number of pseudonym requests versus size of the network

2d) Threshold vs. Conventional: Number of mobility-induced pseudonym requests versus the size of the network

2e) Threshold scalability: End-to-end processing delay against cluster size

3) CRL scalability: Time to fetch CRL revocation (delay to fetch CRL information) vs. number of revoked vehicles in the network

4a) End-to-end delay for V2V communication

4b) Message loss ratio for V2V communication

Thank you!

Questions ?