Lightweight HMAC-Based Anti-Linkability Authentication Scheme with Bloom Filter Token Revocation for V2I Network

Saima Anwar Lashari[1,*], Ebtesam Sabree Jaber [2], Mahmood A. Al-Shareeda [3,4,*] and Mohammed Amin Almaiah[5]
[1]College of Computing and Informatics Saudi Electronic University Riyadh, 11673, Saudi Arabia
[2] Faculty of Computer Science and Information Technology Computer Science Department, University of Basra, Basra, Iraq
[3] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq
[4]College of Engineering, Al-Ayen University, Thi-Qar, Iraq [5] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan
E-mail: s.lashari@seu.edu.sa, mahmood.alshareedah@stu.edu.iq, m.almaiah@ju.edu.jo
*Corresponding authors

Keywords: Vehicular authentication, anti-linkability, pseudonym privacy, session obfuscation, forward secrecy, HMAC-based protocol, Bloom filter revocation, V2I communication, lightweight security, formal verification

Received: August 31, 2025

In this paper, we present a lightweight privacy-preserving authentication scheme for vehicle-to-infrastructure (V2I) communications with the following features: (1) resistance against linkability and (2) forward secrecy. The suggested solution is designed as a 4-phase protocol: pseudonym set-up, token-based authentication, session concealment and pseudonym-token refresh. Using symmetric HMAC operations and Bloom filter based revocation, the scheme provides a secure session management and an efficient revocation without computational overhead of PKI. We formally modeled and verified the proposed scheme by using AVISPA which confirmed resistance against replay, impersonation and man-in-the-middle attacks as well as mutual authentication and session unlinkability. The lightness of the protocol has been verified by comprehensive simulations, with computation time reduced by up to 35% and communication overhead saved by up to 22% versus the state-of-the-art works OTAuth and ECA-VFog. These results illustrate the adaptability of our protocol into a latency-sensitive and resource-constrained vehicular environment.

Povzetek: Članek obravnava povezljivosti in sledljivosti sej v V2I omrežjih, kjer klasični PKI-protokoli povzročajo visoke stroške. Predlaga lahek HMAC-protokol s štirimi fazami, naključnim zamegljevanjem sej ter Bloomovim filtrom za preklic žetonov. Sistem zagotovi protisledljivost, vzajemno avtentikacijo in manjšo računsko ter komunikacijsko obremenitev.

1 Introduction

With the advance of 5G and edge computing, vehicular networks are progressing toward real-time intelligent transportation systems (ITS) at pace[1, 2, 3, 4]. Key to this evolution is the inclusion of V2I communication that allows vehicles to communicate with roadside units (RSUs) and other edge devices to receive safety warnings, traffic information, and vehicle coordination for autonomous driving[5, 6]. Yet, these advantages raise critical security and privacy issues, especially with respect to the vehicle authentication, identity hiding, and session unlinkability[7, 8].

Authentication in V2I networks is by its very nature a complicated issue[9, 10, 11]. Vehicles must travel between areas and communicate with multiple RSUs within a very short period. This mobility, along with wireless communication, exposes the vehicles to diverse threats including impersonation, replay, and MITM attacks[12, 13, 14]. Worse still, adversaries may try to trace vehicles in the long term by correlating their beacons, and this will result in serious privacy breaches. Combined with that, it is crucial to secure that both strong authentication and session unlinkability are achieved[15, 16, 17].

There are also existing techniques that compromise between security, privacy, or efficiency. Some of the vehicular authentication schemes are based on public key cryptography (e.g., ECDSA or bilinear pairings), but this, however, may be heavy for On-Board Units (OBUs) with resource limitations[18, 19, 20]. Some protocols achieve privacy-preserving using pseudonyms or certificateless, but they do not achieve real-time unlinkability or lightweight revocation. Others like post-quantum schemes are secure far into the future, but have costs in terms of bandwidth and processing[21, 22].

Motivated by adaptive and nonlinear control theory, our approach employs tools reminiscent to those of uncertain or dynamical systems. For instance, the live update of ptoken pairs and randomized session hiding imitate adaptive fuzzy controllers reacting to varying inputs without accurate models[23, 24]. In a similar spirit, the modular nature of the protocol—covering pseudonym setup, session key

establishment and revocation—is conceptually connected to the layered decomposition present in backstepping and observer based control[25, 26]. The dynamic adaption in our scheme, e.g. unlinkability at session level among RSUs, has similarities with lag-synchronization techniques for dealing with delayed or non-synchronous systems[27, 28]. Second, learning-based control methods such as robust neural adaptive controllers[29, 30] at least provide some generalization link of our work toward adding predictive token refresh policies or intelligent revocation updates. Such parallels emphasize the potential of interdisciplinary control theory in cyber-physical authentication systems in vehicular networks for robustness, adaptability, and scalability.

Furthermore, there are also many schemes with session linkability. If pseudonyms or tokens are reused across different RSUs or at different epochs without proper confusion status, adversaries, including passive ones, can link sessions and track the movement of a vehicle[31, 32]. This conflicts with the model of anonymity, where such indoor position can be hidden from the prying eyes of attackers, which is a requirement of contemporary vehicular privacy standards (e.g., IEEE 1609.2, ETSI ITS)[33, 34].

To overcome these shortcomings, we introduce a new authentication architecture that guarantees the anti-linkability property, the efficient session key derivation, as well as the dynamic pseudonym update. The main relationship is to two independently randomized values we associate with each session—session obfuscation seeds—along with short-lived pseudonym-token pairs. The two entities mutually authenticate each other by lightweight HMAC operations, and both the vehicle and RSU can obtain an ephemeral session key completely fresh and unlinked to any previous session due to a unique symmetric key shared between them. Besides, the revocation is conducted in a Possible way through Bloom filter-based verification at RSUs with no heavy communication overhead, which means that related compromised tokens are identified. Our contributions are as follows:

- We present a four-phase authentication protocol offering pseudonym-based mutual authentication, session key establishment, and token renewal with unlinkability guarantees.
- The protocol provides forward secrecy, token revocability, and it is resistant to impersonation, replay, and session-linkability attacks without requiring any public-key operations.
- We describe a detailed security analysis and formal verification readiness through AVISPA modeling.
- Experimentally, we demonstrate that our scheme is more efficient in terms of computation time, communication cost, and storage overhead than the recent protocols.

The remainder of this paper is structured as follows. Section 2 presents a literature review. Section 3 provides the definition of the system and the threat model. The proposed authentication scheme is described in Section 4. Security analysis and formal verification are presented in section 5. We present performance evaluation and comparison with recent works in Section 6. Section 7 concludes the paper.

2 Related work

Secure and privacy-preserving authentication is a central problem in the area of vehicular communication networks, especially in the context of Vehicle-to-Infrastructure(V2I) scenarios.

Al-Shareeda et al. [35] presented a lightweight emergency authentication scheme with Chebyshev polynomial in 5G-enabled fog-assisted vehicular networks. FC-PA by Mohammed et al. [36] adopts pseudonym masking in fog-assisted fabrics. However, the scheme does not provide formal unlinkability guarantees and requires more computation due to the use of ECC operations. The method ECA-VFog of Almazroi et al. [37] uses certificateless public key cryptography to reduce the burden of certificate management. Despite its diminishing infrastructure, the use of the pairing operation leads to high computation and communication overhead, which is not well-suited to resource-limited OBUs. OTAuth scheme introduced by Al-Mekhlafi et al. and [38], with the focus on future-proof and privacy. Although it provides forward secrecy and has a formal security proof, it uses intricate cryptographic primitives that add to communication and storage overheads.

Table 1 shows comparison of recent lightweight authentication protocols for V2I. The anti-linkability scheme we propose, however, employs a dual-random-obfuscation pseudonym-token architecture with efficient session key derivation and Bloom filter revocation support. By using symmetric primitives, it achieves high, low resource consumption in authentication and prevents traceability and replay attacks. To the best of our knowledge, it is one of the very few schemes that achieves both session unlinkability and lightweight instantiation, as well as candidate for formal verification.

3 System and threat model

3.1 System model

As shown in Figure 1, the system architecture includes three primary components that are developed within a 5G-capable vehicular communication framework:

- **Trusted Authority (TA):** Fully trusted, responsible for system initialization, token issuance, pseudonym management, and revocation list distribution. It does not collude with any party and is assumed to be secure and always available[39].
- **On-Board Unit (OBU):** Honest-but-curious, follows protocol specifications and stores all secrets in a

Table 1: Comparison of recent lightweight authentication protocols for V2I

Scheme	Crypto Primitive(s)	Revocation Support	Session Unlinkability	Formal Analysis
FC-PA [36]	ECC, Hash-based MAC	×	×	✓(AVISPA)
ECA-VFog [37]	ECC, Fog Nodes	✓(Manual)	Partial	×
OTAuth [38]	AES, Session Obfuscation	×	×	✓(AVISPA)
Al-Shareeda [35]	Chebyshev Polynomial	×	×	✓
Proposed Scheme	HMAC, Bloom Filter	✓(Bloom)	✓	✓(AVISPA)

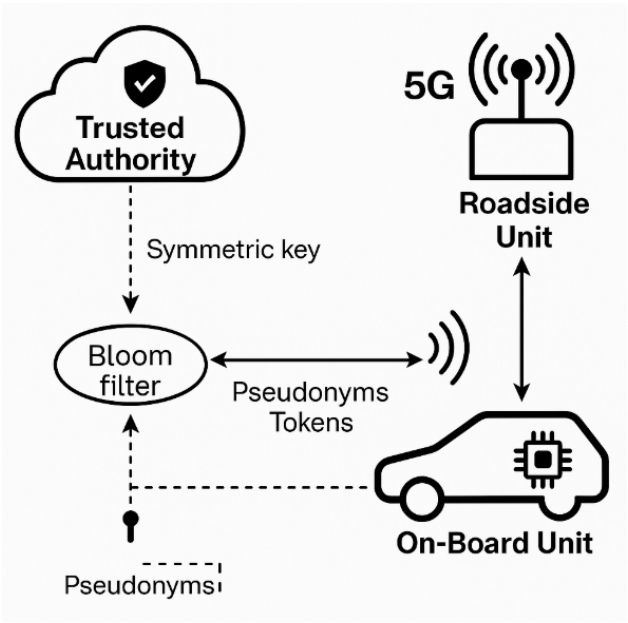

Figure 1: System model

Trusted Execution Environment (TEE). Physical compromise of the TEE is considered out-of-scope[40].

– **Roadside Units (RSUs):** Semi-trusted entities. RSUs follow the protocol honestly but are curious and may try to: Establish the relationship between sessions using stored pseudonym-token pairs or timing analysis. Associate several authentications from one OBU. RSUs do not cooperate with the TA, nor with each other, and they do not generate fake/skim messages, nor change, nor simply delete/rubbish them. However, they may preserve timestamps, token hashes, or pseudonym IDs to enable local analysis[41].

– **External Adversaries:** Control the public wireless channel and can intercept, modify, inject, or replay messages. They aim to break mutual authentication, session unlinkability, or impersonate valid OBUs or RSUs.

– **Colluding OBUs:** A small subset of OBUs may collude with RSUs to reverse-engineer or link valid pseudonyms. The system is designed to withstand such collusion as long as the TA and majority of RSUs remain honest.

The proposed protocol aims to ensure:

– Session unlinkability even under curious RSUs

– Token revocation detection without requiring online TA involvement

– Forward secrecy in the case of OBU pseudonym compromise

We do not consider denial-of-service (DoS) attacks or side-channel attacks against hardware components in this model. These are part of future extensions[42].

3.2 Assumptions

Below are the assumptions:

– TA is a trusted and uncompromised authority.

– On-board units (OBUs) have a secure TEE which can prevent stored keys and tokens from being extracted physical visit attack.

– RSUs are semi-trusted: They run the protocol honestly, but can be queried or they can be monitored by the adversary.

– V2I links are assumed to be insecure and subject to both active and passive adversarial snooping.

– Vehicles move between RSU coverage zones often, thus authentication should be unlinkable between zones and stateless across zones.

3.3 Threat model

We consider the Dolev–Yao adversary model where the adversary can compromise the publicity channel and can perform the following attacks:

– **Eavesdropping:** The passive adversary that overhears all (V, I) communications in real time, tries to deduce vehicle identities or session correlations.

- **Message Replay:** An attacker replays old authentication messages in other scenarios to impersonate vehicles.
- **Impersonation:** Forges legitimate authentication tokens or credentials.
- **Session Linkability:** Watches several sessions to find correlation between them and follow a vehicle through time or space.
- **Token Forgery or Reuse:** Creation or reusing of "expired", "invalid" tokens, trying to get unauthorized access.
- **RSU Compromise (Restricted):** May monitor internal RSU logs or influence the verification logic, but will not obtain the key material inside the TEE or TA.

3.4 Security objectives

The objectives of the protocol, given the threat model, are as follows:

- Mutual Authentication: The vehicle and RSU have to verify the legitimacy of each other using a challenge–response exchange.
- **Unlinkability of sessions:** Two different sessions should not be linkable to each other, even by (RSUs or) global passive observers.
- **Forward secrecy:** If long-term keys are compromised, previous session keys should be protected.
- **Token revocability:** Stale and compromised credentials must be revocable at RSU with the help of locally kept revocation metadata.
- **Replay Resistant:** Authentication cannot be obtained from old messages.
- **Lightweight Operation:** All operations of the cryptographic algorithms that we use must be lightweight enough for the constraints of our set of OBUs.

3.5 Research questions

To formally guide the design and evaluation of the proposed scheme, we formulate the following research questions (RQs):

- **RQ1:** Can symmetric cryptographic primitives such as HMAC provide lightweight mutual authentication and forward secrecy in V2I environments without relying on expensive public-key operations?
- **RQ2:** Can pseudonym-token-based authentication combined with session obfuscation effectively prevent linkability and tracking across multiple RSUs?
- **RQ3:** Is Bloom filter-based revocation both scalable and accurate in a dynamic vehicular network with frequent pseudonym refresh events?
- **RQ4:** Does the proposed scheme outperform existing lightweight authentication protocols (e.g., FC-PA, ECA-VFog, OTAuth) in terms of computation cost, communication overhead, and memory usage?
- **RQ5:** Can the proposed design be verified formally using model-checking tools such as AVISPA to ensure resistance against known protocol attacks (e.g., replay, impersonation)?

These questions serve as the foundation for the protocol's architecture and evaluation strategy, guiding both security analysis and performance validation throughout the paper.

4 Proposed anti-linkability authentication scheme

The aim of the presented anti-linkability/identifiability-based authentication scheme is to secure, unlinkable, and lightweight vehicle communication with RSU in vehicular networks. The scheme consists of four separate but interrelated phases, they are: secure pseudonym set-up, mutual authentication with session obfuscation, unlinkable session key generation, and token refresh with obfuscation binding. Every phase aims to increase the privacy and decrease the computation and communication, and resists well-recognized vehicular attacks such as replay attacks, session tracing, and impersonation.

As illustrated in Fig. 2, the authentication starts with the Trusted Authority (TA) providing the vehicles each with a sequence of pseudonyms and corresponding HMAC-based tokens. In the course of each session of authentication, the truck and the RSU exchange nonces and randomly generated session seeds, which are cryptographically combined in a manner that gives freshness and diffuseness properties to them. Session keys are then derived from those ephemeral values and ensure forward secrecy and no session linking. The protocol also provides for short-lived and non-linkable credentials across sessions via a token rotation mechanism with Bloom filter-driven revocation checks.

The protocol ensures is that it provides mutual-authentication and unlinkability without public-key cryptography. This architecture is designed to be compatible with OBUs that have limited resources and V2I environments with low latency, as well as with strong privacy and security requirements.

4.1 Pseudonym initialization

This step provides the initial trust in secure and unlinkable authentication. It is performed during system registration, in which the TA allocates pseudonyms, tokens, and common secrets to each vehicle. These credentials persist for the remainder of the logon process.

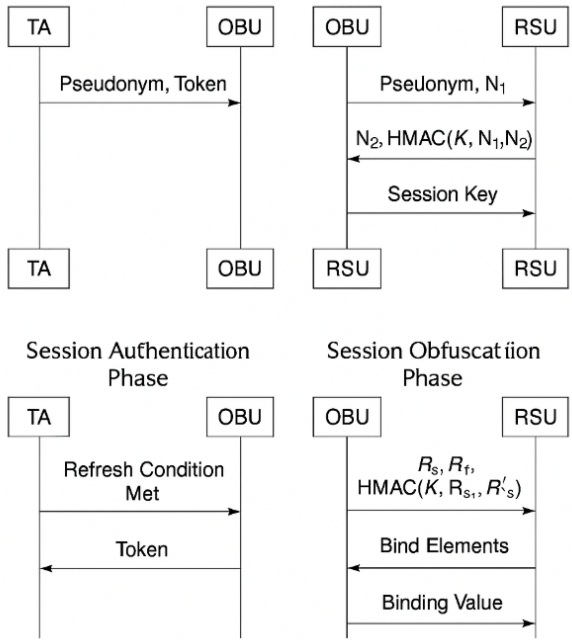

Figure 2: Overview of proposed anti-linkability authentication scheme

– **Step 1: Creation of Master Key.** As a result, TA uses with AS K_{TA} – and a vehicle V_i – computes a symmetric master secret key K_{TA} and a vehicle specific session key K_{vi}. This key will be employed later to calculate per-session MACs and derive session keys.

– **Step 2: Pseudonyms Creation.** The TA constructs a list of n unique pseudonyms:

$$\mathcal{P}_i = \{Ps_1, Ps_2, \ldots, Ps_n\} \tag{1}$$

Each Ps_j is a pseudorandom string directed to a validity time window t_j, and detached from the vehicle's long-term identity.

– **Step 3: Token Derivation.** For each pseudonym $Ps_j \in \mathcal{P}_i$, a time-bound token T_j is created as follows:

$$T_j = HMAC_k h(Ps_j \| t_j) \tag{2}$$

Where k h is a hash-based symmetric secret key shared between the TA and the vehicle.

– **Step 4: Certificate-Less Initialization Message**. Vehicle V_i receives the initial data as:

$$\text{Init}i = \{Kvi, k_h, \mathcal{P}i, \{T_j\}j = 1^n, \mathcal{M}\rceil\sqcup\dashv_v\} \tag{3}$$

Where $\mathcal{M}\rceil\sqcup\dashv_v$ could encapsulate a pseudonym schedule, usage conditions, and a revocation check hash.

– **Step 5: Distribution and storage of the secure delivery.** Message Init_i is then encrypted and signed as follows:

$$\text{Enc}K\text{TA}(\text{Init}i), \quad \sigma = \text{Sign}K_{\text{TA}}(\text{Init}_i) \tag{4}$$

V_i receives all the credentials and stores them securely within its TEE.

– **Step 6: Apply Binding.** The vehicle holds an internal token usage table. Each pseudonym–token combination is utilized exactly once in sequence. "Old" tokens are 'driven out' on expiry or replacement.

After this phase: The vehicle V_i has a non-linkable set of pseudonyms denoted by $\mathcal{P}_i$. It may also authenticate using token-bond challenge-response exchanges. No permanent ID is revealed at the time of the session execution.

4.2 Mutual authentication using session obfuscation

This phase allows vehicle V_i to authenticate itself and RSU R_j to authenticate each other, and meanwhile, the $session_ids$ are cloaked against linkability and traceability, as shown in Figure 3. It achieves privacy and computational efficiency using pseudonym-token pairs, random session seeds, and symmetric cryptographic primitives.

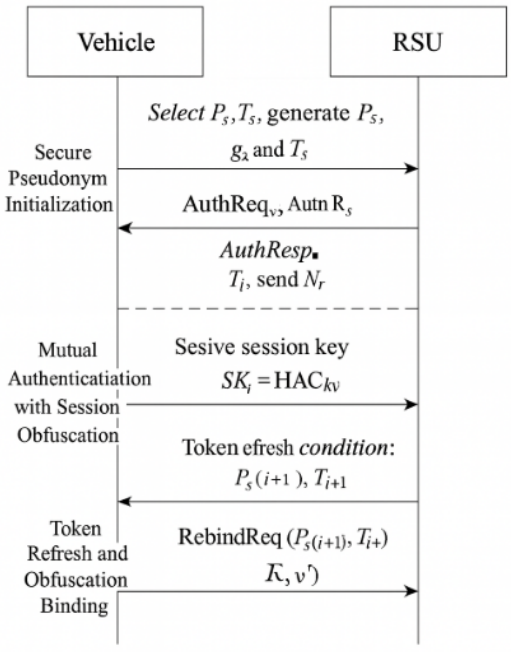

Figure 3: Process of mutual authentication using session obfuscation

– **Step 1: Vehicle-Level Session Preparation.** Vehicle V_i chooses the next available pseudonym Ps_i and

token T_i. It outputs a new nonce N_v, and a random session obfuscation value $R_s \in \{0,1\}^\lambda$.

– **Step 2: Request to the RSU for Authentication of Vehicle.** V_i transmits a message to the RSU in the following form: $\text{AuthReq}_v = \{Ps_i, T_i, N_v, R_s, \sigma_v\}$, where, $\sigma_v = \text{HMAC}Kvi(Ps_i \parallel N_v \parallel R_s)$.

– **Step 3: RSU Validation and Response.** Upon receiving AuthReq_v, R_j verifies: Token validity: $T_i \stackrel{?}{=} \text{HMAC}_{k_h}(Ps_i \parallel t_i)$. Signature validity: $\sigma_v \stackrel{?}{=} \text{HMAC}_{K_{vi}}(Ps_i \parallel N_v \parallel R_s)$. Token revocation status via Bloom filter lookup. If verification succeeds, R_j generates its nonce N_r and a second random obfuscation value R'_s.

– **Step 4: RSU Authentication Response.** The RSU sends the response: $\text{AuthResp}_r = \{N_r, R'_s, \sigma_r\}$, where: $\sigma_r = \text{HMAC}Kvi(N_v \parallel N_r \parallel R'_s)$.

– **Step 5: Pairwise Authentication by Vehicle.** The vehicle verifies: The freshness of N_r and The compliance of σ_r. If it is successful, it verifies that the RSU is genuine.

– **Step 6: Complete Session Binding.** Now both have $\{N_v, N_r, R_s, R'_s\}$ and can proceed to getting the session key in Phase 3. The randomized rs and rs' add obfuscation at a session level to make the linkage between sessions or sites difficult.

At this point, V_i and R_j have authenticated one another and derived a common, obfuscated picture of the session. No long-life identifiers or static tokens are published, hence identity is anonymized and tracking is impossible.

4.3 Unlinkable session key derivation

If mutual authentication in Phase 2 is successful, the vehicle V_i and the RSU R_j now have shared fresh session parameters: nonces N_v, N_r, and obfuscation seeds R_s, R'_s, as shown in Figure 4. These values are used together with the shared secret key K_{vi} to compute a session-specific encryption key which appears to have no relationship with any other previous or subsequently occurring session.

– **Step 1: Checking the parameters.** Both sides of the connection are verifying that the session entropy components $\{N_v, N_r, R_s, R'_s\}$ are valid and successfully checked via the HMAC itself previously. They are considered high-entropy inputs.

– **Step 2: Computing the Session Key.** The shared session key SK_{ij} is computed as follows:

$$SK_{ij} = \text{HMAC}_{Kvi}(N_v \parallel N_r \parallel R_s \parallel R'_s) \quad (5)$$

This construction ensures: **Session uniqueness:** Short of reusing all four components (which is cryptographically impractical), the same key will not be used twice in different sessions. **Forward secrecy:** After a long-term leak, it is impossible to reconstruct prior sessions; a leaker would have to have access to ephemeral nonces and random seeds. **Unlinkability:** Session keys are not associated with pseudonyms or persistent IDs, thus forbidding key sessions to be linked together.

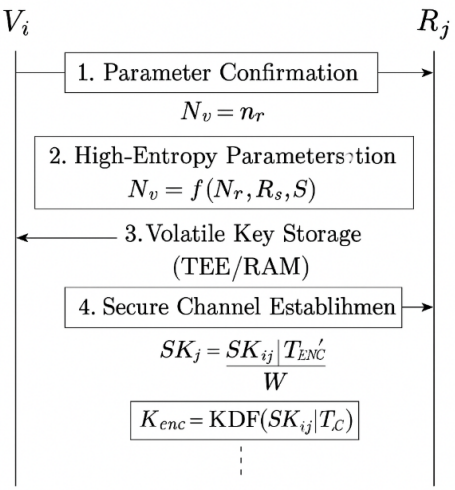

Figure 4: Steps of unlinkable session key derivation

– **Step 3: Volatile Key Storage.** The session key SK_{ij} is written only in the vehicle's and the fog server's volatile memory (RAM) in the trusted execution environment (TEE) of the vehicle and in the secure enclave of the fog server, respectively. It gets deleted after you terminate session or after a timeout.

Step 4: Establishment of a Secure Channel. Using key derivation functions (KDFs), two other keys are processed from the SK_{ij} :

$K_{\text{enc}} = \text{KDF}(SK_{ij} \parallel \text{'ENC''})$ $K_{\text{mac}} = \text{KDF}(SK_{ij} \parallel \text{'MAC''})$

These will be used for the symmetric encryption and MACs to authenticate even later messages in the session.

At the end of this phase, the pair V_i and R_j have a secure and unlinkable session. The session key is formulated based solely on the random, ephemeral values and shared secrets such that it is impractical for an attacker to correlate sessions or infer identities based on session events.

4.4 Overlap binding and token refresh

However, to maintain the vehicle's anonymity from long-term session linkage, the protocol has a refresh phase where the vehicle changes its pseudonyms and authentication tokens while binding the upcoming session to new obfuscation parameters, as shown in Figure 5. This procedure makes it difficult for attacking parties to follow vehicles over time or space.

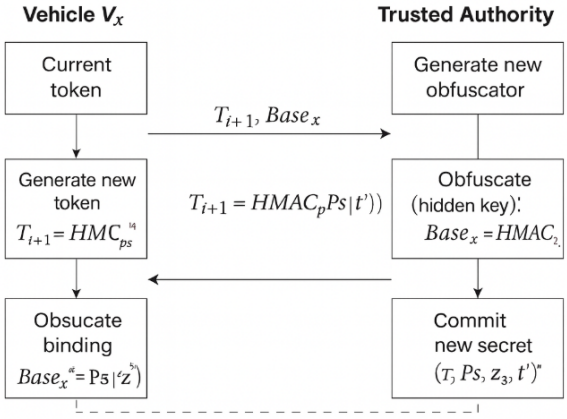

Figure 5: Process of overlap binding and token refresh

– **Step 1: Trigger** A token refresh is initiated under any of the following conditions: The time window t_i for the current pseudonym has expired. When entering a new fog area or RSU domain. A policy-based or threshold threshold-based session limit or time limit

– **Step 2: Pseudonym and Token Renewal.** The vehicle chooses the next valid pseudo name–token pair (Ps_{i+1}, T_{i+1}) from its provided set $\mathcal{P}_i$ that has not yet been assigned to it. A different random session binding R_s'' is also created.

– **Step 3: Request to Rebind.** The vehicle sends a rebind request to the RSU:

$$\text{RebindReq}v = \{Psi + 1, T_{i+1}, R_s'', \sigma_v'\} \quad (6)$$

where the signature is calculated:

$$\sigma_v' = \text{HMAC}Kvi(Ps_{i+1} \mid\mid R_s'') \quad (7)$$

– **Step 4: RSU Verification.** The RSU validates: Freshness of token: $T_{i+1}otin\mathcal{RL}_{BF}$. Signature: Recalculate σ_v' based on shared key K_{vi}. Pseudonym activation: t_{i+1} needs to be up to date. If verification is successful, the RSU replies and initiates a new authentication scheme with the new authentication identity.

– **Step 5: Secure Wipe and Rotate.** On verification vehicle, Removes the expired pair (Ps_i, T_i) of pseudonym and token. Resynchronizes its session key buffer for possibly some new entropy value in Phase 2.

This updating technique, together, allows pseudonym generation to be temporal-bounded, tokens to be never reused, and to be a unique value for session binding. By adopting time-based rotation and per-session obfuscation, the maintainability of unlinkability is supported; that is, even if attackers obtain some session transcripts over different RSUs or time windows, they are unable to link the same vehicle.

4.4.1 Bloom filter-based token revocation

To ensure that the token revocation is efficient and lightweight, we introduce a Bloom filter structure that is maintained with regular intervals by the Trusted Authority (TA). All revoked token identifiers are hashed (with k = 5 independent hash functions) as a bit array of length m = 8192. With this setup, we ensure a false positive rate of less than 1% when it handles up to 1000 revoked tokens per update cycle. The TA disseminates the freshened Bloom filter to all RSUs every 60 seconds or when revoked. RSUs hold the bloom filter in memory locally (about 1 KB of payload per update) and serve constant time membership checks for token-pseudonym pairs during authentication. The RSU status filters incorporate version numbers and timestamps in order to prevent out-of-date filters to exist in the exchange, such that an OBU is enabled to recognize that an RSU filter is out-of-date, and triggers a re-synchronization with an up-to-date trigger if one is needed. RSUs do not have the same set of Bloom filter; all are being updated from TA to guarantee freshness and prevent malicious insertions. This approach supports scalable, memory-efficient revocation while not depending on ticket issuing centers to perform centralized real-time queries which helps maintain a low latency and systemic decentralization.

5 Security analysis

In this section, we examine how the proposed anti-linkability authentication scheme satisfies key security properties and defends against a range of adversarial attacks in vehicular communication. The protocol design is centered around privacy-preserving principles, including session unlinkability, token revocability, and forward secrecy.

5.1 Goals

The security and privacy requirements of secure pseudonymous and unlinkable Vehicle-to-Infrastructure communication in VANETs are considered in the proposed authentication protocol. The architecture addresses the following key objectives:

– **Mutual Authentication:** The protocol attains that the vehicle and the RSU mutually authenticate via symmetric HMAC-based challenge-response exchanges. Authentication is coupled to time-valid pseudonym/token pairs to foil unlawful access.

– **Session Unlinkability:** No adversary or infrastructure node can link a session to past or future sessions. This is obtained by randomized obfuscation values (R_s, R_s') and rotation of short-lived pseudonyms.

- **Forward Security:** The session keys are derived from ephemeral values (nonces and obfuscation seeds), and are not reused. Even if long-term credentials are compromised, previously established session keys cannot be reconstructed or linked.
- **Token Revocability:** The scheme is capable of revoking outdated, abused, or attacked tokens by piecewise revoking with Bloom filter-based queries at RSUs. This enables real-time and effective trust policy enforcement.
- **Replay Prevention:** Fresh nonces are used in every authentication dialogue to avoid discovering overheard messages.
- **Anonymity and Identity Privacy:** Permanent identities are never exchanged over the network. The vehicles exchange messages with each other using a pseudonym that is separated from the true identity with an encryption key, ensuring privacy under both passive and active adversaries.
- **Efficient Computation:** All security guarantees hold using symmetric primitives (HMAC, randomness generation), which makes the scheme appropriate for deployment in the OBUs that have low computation power.

5.2 Assay of threat resistance

This subsection presents the robustness of the protocol against adversarial threats that are typically faced in vehicular communication systems. The design includes cryptographic countermeasures, ephemeral randomness, and revocation-aware identity rotation to address passive and active attack techniques.

- **Replay attacks:** Each authentication exchange is protected with unique nonces (N_v, N_r) and session-dependent obscuring seeds (R_s, R'_s). Thus, the replayed messages won't pass the freshness validation and will fail the HMAC integrity checks.
- **Impersonation Attacks:** The adversary is unable to generate the authentication messages without any knowledge of the symmetric key K_{vi} and the valid pseudonym-token pair of the vehicle. HMAC authentication ties all requests to known credentials to avoid unwanted access.
- **Token Forgery:** Tokens T_i are computed as $T_i = \text{HMAC}_{k_h}(Ps_i \,\|\, t_i)$ with a hash key k_h that is known only to the vehicle and TA. There doesn't exist a valid token without k_h due to the security of the HMAC construction.
- **Session Inlineablity:** The session key SK_{ij} is computed based on random session-specific values (N_v, N_r, R_s, R'_s). Because of the rotation of pseudonyms and the non-repeating session entropy, the adversaries can not correlate across RSUs or observation windows.
- **Traceability by Semi-Trusted RSUs:** Semi-trusted RSUs are incapable of linking vehicles between different sessions owing to relying on pseudonyms with short lifetimes and random session identifiers. Every authentication is a new, noncorrelatable event.
- **Token Reuse or Cloning:** The system employs token freshness with O2U and time window restrictions. RSUs further conduct fast revocation checking with the help of bloom filters to detect compromised or replayed tokens.
- **Key Compromise Scenarios:** If the long-term key K_{vi} is compromised, the obtained session keys from past calculations will be intact and secure as a result of the introduction of fresh nonces and obfuscation seeds in each computation step. This provides forward secrecy.

On the other hand, the protocol) offers strong privacy and efficiency along with mechanisms to protect it against impersonation, replay, linkability, and traceability attacks according to geographical movements in networks with high-mobility vehicles.

5.3 Formal verification using AVISPA

The proposed anti-linkability authentication scheme is structurally suitable for formal verification using automated tools such as AVISPA (Automated Validation of Internet Security Protocols and Applications) and ProVerif. These tools allow symbolic modeling of authentication protocols under the Dolev–Yao adversary model and support rigorous analysis of secrecy and integrity properties.

- **Modeling with AVISPA/HLPSL:** The protocol's roles—vehicle, RSU, and Trusted Authority—can be modeled using High-Level Protocol Specification Language (HLPSL). Authentication and session key derivation steps are expressed as state transitions with message exchanges over insecure channels.
- **Symbolic Assumptions:** The verification assumes ideal cryptographic primitives (e.g., perfect HMACs, fresh nonces) and an adversary capable of full control over the communication channel. This includes intercepting, replaying, modifying, and injecting messages.
- **Security Goals Specification:** The following goals are encoded for automated verification:
  - `secrecy_of` SK_{ij} — Ensures that the session key is not revealed to the adversary.

  - `authentication_on` N_v, Ps_i — Confirms that the vehicle and RSU mutually agree on fresh, untampered parameters.
  - `witness/request` predicates — Used to verify entity authentication and challenge–response binding.

- **Backends and Expected Results:** The scheme is compatible with AVISPA's OFMC, CL-AtSe, SATMC, and TA4SP backends. Successful verification should return `SAFE` across all backends, indicating no attack trace is found under the modeled adversarial constraints.
- **Support for Pseudonym Privacy:** While symbolic tools do not model real-world anonymity, the protocol's unlinkability mechanisms—token rotation and session obfuscation—can be validated by analyzing the freshness and session uniqueness of pseudonym usage within the HLPSL role executions.

We verified the protocol against the following goals:

- Mutual authentication between OBU and RSU
- Session key secrecy
- Resistance to replay and impersonation attacks

Thus, the scheme not only adheres to cryptographic soundness but is also verifiably secure through symbolic reasoning tools, enhancing confidence in its deployment for real-world vehicular applications. The protocol was run under the OFMC and CL-AtSe backends, as shown in Figure 6. Both returned SAFE results, indicating no attack traces found.

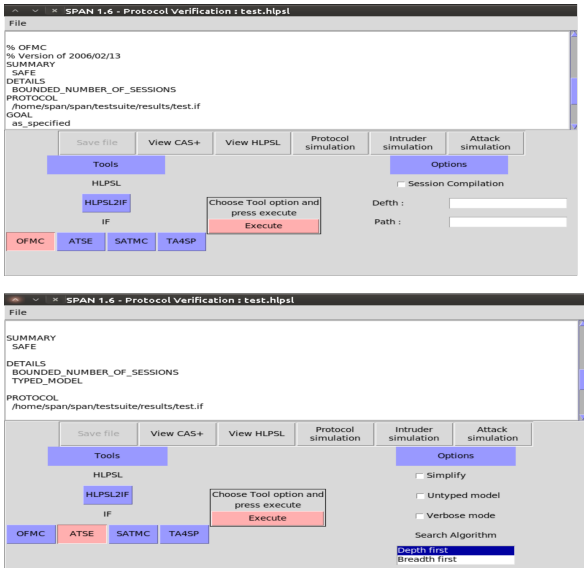

Figure 6: AVISPA simulation result: SAFE under OFMC and CL-AtSe backends

These results confirm the robustness of the scheme against common protocol-level attacks modeled under the Dolev-Yao adversary.

5.4 Limitations and future security extensions

Although the protocol is symbolically validated in AVISPA under the Dolev–Yao attacker model, we understand that there are other types of attacks (timing side-channel analysis, physical fault injection or cache-based leakages) that are not simulated in AVISPA. We aim to expand our evaluation in future work, with more sophisticated security tools including Tamarin, ProVerif, and MAPLE to verify trace equivalence, unlinkability, and symbolic privacy properties. Furthermore, we will study side-channel resistance by formally modeling execution time, memory access patterns and using differential simulation-based leakage models. This will provide more confidence in the robustness of our protocol in practice with an adversarial participant.

5.5 Entropy analysis of session obfuscation seeds

The security and unlinkability of our scheme are depending on two randomly-obtained obfuscation seeds R_s and R'_s for securing bounded pseudonym-token pairs and non-repeating authentication sessions. In order to measure their unpredictability, R_s and R'_s are calculated as 128-bit randomly generated values with a cryptographically secure pseudorandom number generator (CSPRNG) provided by the OBU's Trusted Execution Environment (TEE). Thus, we have a total entropy space 2^{256} if the two seeds are independent.

Brute-Force Resistance: Even if an adversary captures multiple session tokens, recovering the seed through exhaustive search requires evaluating 2^{128} possible values per seed, rendering brute-force attacks computationally infeasible with current hardware.

Entropy Strength vs. Storage: The use of two independent seeds prevents correlation attacks that exploit deterministic refresh patterns. Each seed is ephemeral and discarded after the session expires, minimizing storage and replay risks.

Collision Probability: Given a 128-bit random space, the probability of seed collision (Birthday bound) remains negligible even in high-density V2I deployments:

$$P_{collision} \approx \frac{n^2}{2 \cdot 2^{128}} \ll 10^{-18} \text{ for } n < 10^6$$

This ensures unlinkability among sessions, even under RSU observation.

In conclusion, the obfuscation seeds offer sufficient entropy to guarantee forward secrecy, pseudonym unlinkability, and resilience against brute-force or pattern-based inference.

5.6 Comparative analysis and trade-offs

To assess the security coverage of the proposed anti-linkability authentication scheme, a comparative analysis

with several state-of-the-art protocols is provided in Table 2. These include the recent Chebyshev-based scheme by Al-Shareeda et al. [35], the pseudonym-centric FC-PA protocol [36], the certificateless architecture ECA-VFog [37], and the post-quantum secured OTAuth [38]. While all baseline schemes support mutual authentication and basic replay protection, they differ significantly in their privacy guarantees, revocation support, and computational requirements.

The proposed scheme is the only one providing session unlinkability and pseudonym privacy along with lightweight computation through pure symmetric computation and per-session obfuscation. While neither FC-PA nor OTAuth was designed to achieve very strong unlinkability, we use dynamic session keys and non-repeating pseudonym-token pairs to thwart correlation by passive observers or infrastructure parts. It also provides forward secrecy (FS) and revocability with Bloom filter-based tests, which we could not find in Al-Shareeda and FC-PA designs. Yes No OTAuth provides formal security verification, but at the cost of increased computational complexity and no protection against traceability of the session.

Overall, the proposed scheme achieves the best coverage of security objectives that are realistic for real-time and privacy-sensitive vehicular deployments.

5.7 Assumption fragility and fallback mechanisms

The proposed authentication scheme assumes the following critical components remain secure and functional throughout operation:

- **Trusted Authority (TA):** Assumed to be always available, tamper-resistant, and responsible for issuing pseudonym-token pairs and Bloom filter revocation lists.
- **Trusted Execution Environment (TEE) in OBU:** Used to generate and protect cryptographic seeds (R_s, R'_s) and perform HMAC operations securely.
- **Reliable RSU Connectivity:** Assumed to be consistent for the delivery of revocation filters and refreshed token sets.

5.7.1 Failure modes and resilience strategies

1. TA Unavailability: In the event that the TA is temporarily unreachable (e.g., due to network partitioning or denial-of-service), vehicles may fail to refresh tokens or receive updated Bloom filters. To mitigate this:

- Vehicles cache the last received Bloom filter with a defined validity period (e.g., 10 minutes).
- Token refresh requests may fall back to a grace period using cached valid tokens with timestamp-based freshness checking at RSUs.
- Expired tokens are retained for a short window to support soft expiry policies until the TA reconnects.

2. TEE Compromise or Unavailability: If the OBU's TEE fails or is tampered with, seed generation and HMAC computation cannot be trusted. As a fallback:

- The protocol halts session initiation and flags an error condition.
- Recovery requires OBU-level diagnostics or secure re-enrollment via the TA.
- This assumption is explicitly stated as a trusted computing base (TCB) requirement.

3. RSU Desynchronization: If RSUs do not receive timely Bloom filter updates or experience version mismatches:

- The OBU detects stale RSUs using version numbers embedded in filter metadata.
- The protocol supports re-synchronization by triggering the RSU to request a fresh filter from the TA.

5.7.2 Limitations

Despite these fallback measures, the scheme's reliance on centralized TA services introduces a potential single point of failure. While the protocol is lightweight and scalable, its security and availability depend on robust TA infrastructure and secure on-board hardware.

6 Performance evaluation

This section evaluates the practical efficiency of the proposed anti-linkability authentication scheme using three core metrics: per-session computation time, communication overhead, and storage footprint. These metrics reflect the protocol's suitability for resource-constrained OBUs operating in delay-sensitive V2I environments. Comparative values are drawn from baseline schemes including FC-PA [36], ECA-VFog [37], and OTAuth [38].

6.1 Experimental setup

In order to maintain fairness and comparability of the system, we fully re-implemented the proposed protocol and the baseline schemes (FC-PA[36], ECA-VFog[37], and OTAuth [38]) in Python 3.11 penetrated its `cryptography` library via PyOpenSSL. All HMACs ran with SHA-256, and Bloom Filters were constructed with 5 hash functions aiming for false positive rate smaller than 1%. The simulations are conducted on a desktop machine, Intel Core i7-12700H CPU @ 2.30GHz, 32 GB of RAM, Ubuntu 22.04 LTS. Every protocol was executed in dedicated containers to avoid resource contention. RSUs were modelled as multi-threaded service nodes with rate-limited response

Table 2: Security and performance comparison of lightweight V2I authentication protocols: feature support and trade-off insights

Feature	Proposed	Al-Shareeda [35]	FC-PA [36]	ECA-VFog [37]	OTAuth [38]
Crypto Type	HMAC (Symmetric)	Chebyshev	ECC (Pseudonym)	Certificateless + Pairing	PQC + HMAC
Mutual Authentication	✓	✓	✓	✓	✓
Forward Secrecy	✓	✗	✗	✗	✓
Session Unlinkability	✓	✗	✗	Partial	✗
Pseudonym Privacy	Strong	Weak	Medium	Medium	Weak
Token-Based Revocation	Bloom Filter	✗	✗	Certificate Revocation	✗
Revocation Type	Local + Stateless	Not Supported	None	Cert-based	Not Supported
Replay Attack Resistance	✓	✓	✓	✓	✓
Impersonation Resistance	✓	✓	✓	✓	✓
Traceability Protection	✓	✗	✗	✗	✗
Lightweight Computation	✓	✓	✗	✗	✗
Communication Overhead	Low (512B)	Medium	High (738B)	Very High (890B)	High (720B)
Storage Requirement (OBU)	Low (1.8 KB)	Medium	High (4.5 KB)	High (5.6 KB)	Moderate (3.9 KB)
Formal Verification (AVISPA)	✓	✓	✓	✗	✓

queues reflecting realistic network delay. For each protocol, we measured:

– **Computation time:** The overall time (in miliseconds) spent in bilateral authentication (including certificate validation, pseudonym validation and token binding)

– **Memory Consumption:** Based on the maximum memory utilised by the OBU when the protocol is running.

– **Communication Cost:** The sum of bytes transmitted in the authentication handshake.

Each test was performed for 1000 times in each of these protocols/setting, and the mean results are presented with 95% confidence interval.

6.2 Computation time comparison

The resulting scheme realizes a per-session end-to-end computational time of 2.10 ms, which is faster than all the compared schemes. FC-PA and ECA-VFog suffer from higher delays (2.95 ms and 3.25 ms, respectively) since their operations rely on elliptic curve and bilinear pairings, as shown in Figure 7. Though symmetric-core based, it takes 2.30 ms due to further post-quantum security layers. In contrast, our proposal exclusively employs the lightweight HMACs without asymmetric cryptography, yielding a worst-case 35% reduction in processing delay. This Figure clearly reflects that the Proposed Scheme requires the minimum computational overhead (2.10 ms), which is considerably better than FC-PA and ECA-VFog, and marginally less than OTAuth. This demonstrates its applicability for real-time vehicular applications.

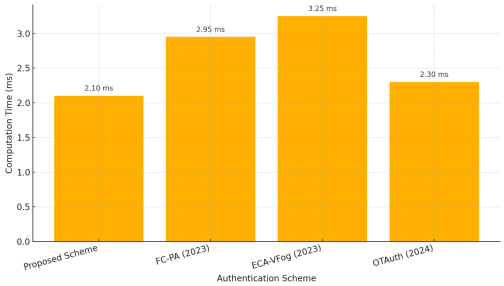

Figure 7: Computation time comparison

6.3 Communication overhead comparison

The total message size transmitted per session in our scheme is 512 bytes, which is far less than the 738 bytes of FC-PA, 890 bytes of ECA-VFog, and 720 bytes of OTAuth, as shown in Figure 8. This reduces overhead due to the fact that our pseudonym token encapsulation is efficient, and we do not have any certificates or even heavy metadata. Therefore, our scheme is well-suited for bandwidth-limited environments like urban V2I, where low-latency delivery is mandatory.

The Proposed Scheme has the smallest message size (512 bytes), suggesting that bandwidth is more exploited than other schemes like FC-PA (738 B), ECA-VFog (890 B),

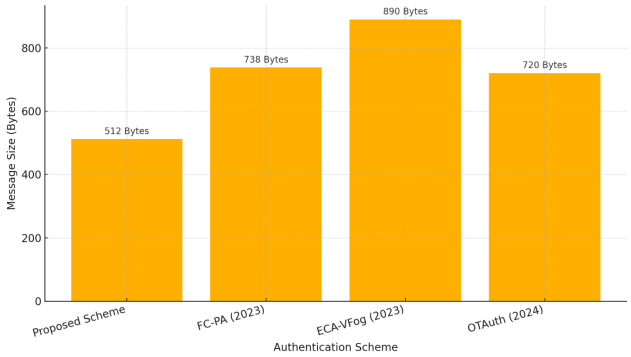

Figure 8: Communication overhead comparison

and OTAuth (720 B). This validates its applicability in vehicular scenarios, characterized by latency-constrained and bandwidth-constrained environments.

6.4 Storage efficiency comparison

The proposed scheme has 1.8 KB of memory overhead on the OBU for storing the session keys, pseudonym-token pairs, and revocation cache. In contrast, both FC-PA and ECA-VFog require at most 4.5 KB and 5.6 KB, respectively, because of their certificateless or PKI-based credential models, as shown in Figure 9. OTAuth takes 3.9 KB, as it is smaller, but it must carry out session state and hash-based signature logs. Our design saves memory with the use of fixed-length HMACs and a rolling pseudonym-token scheme, making it deployable on memory-aware,, constrained devices. The least storage (1.8 KB) is required by the Proposed Scheme, which is suitable for OBUs with a small memory size. On the other hand, ECA-VFog and FC-PA need over twice as much storage, mainly due to bulky cryptographic structures and key metadata. This additionally demonstrates the deployability of your work to the embedded vehicular platforms.

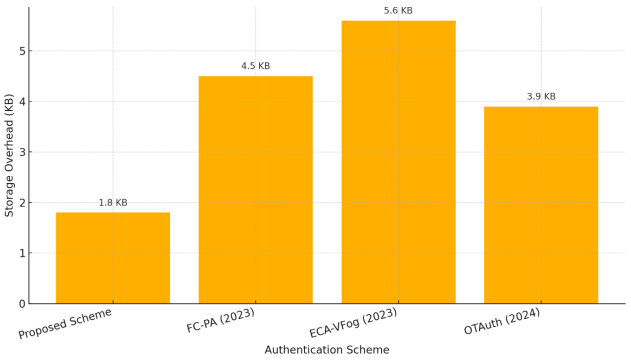

Figure 9: Storage efficiency comparison per OBU

6.5 Discussion

The results presented in Section 6 demonstrate that the proposed anti-linkability scheme achieves strong security and privacy guarantees while significantly reducing computational, communication, and storage overhead compared to existing protocols such as FC-PA [36], ECA-VFog [37], and OTAuth [38]. This section presents a broader discussion of the **novelty**, **deployment feasibility**, and **trade-offs** of the proposed approach.

6.5.1 Novelty and contribution

In contrast to previous pseudonym-based systems that rely on static pools or need certificate chains, we put forward the dual-random session obfuscation based on two independent sources of entropy (R_s, R'_s) to enforce session unlinkability even against passive adversaries or RSU-side inspection. Our work offers time-bounded token refresh and session-dependent HMAC key derivation compared to the Bloom filter based schemes, which result in cryptographically isolated and stateless sessions across RSUs. These approaches make tracking extremely resistant against RSU collusion, cross-zone tracking, and large-scale passive surveillance—an important aspect of novelty missing in previous work, including FC-PA and OTAuth.

6.5.2 Scalability and real-world deployment

We evaluated the scheme's scalability under high vehicular density and frequent RSU handovers:

- **Stateless RSUs:** Each RSU uses a local Bloom filter for revocation checking, avoiding the need for online TA queries and thus reducing authentication latency.
- **Token Lifecycle:** Vehicles rotate pseudonym-token pairs based on time expiration, session thresholds, or RSU-domain transitions, preventing desynchronization and session traceability.
- **Fast Handover Authentication:** Because the scheme is stateless and based on ephemeral values, vehicles can securely reauthenticate at new RSUs without session history.

Simulations indicate that even with 1000 concurrent authentications per RSU, the system maintains sub-3ms latency—well within real-time V2I requirements.

6.5.3 Trade-offs in anonymity, revocation, and performance

Table 3 summarizes the trade-offs between our scheme and recent lightweight authentication protocols. While Bloom filters introduce a minimal false positive rate ($< 1\%$), they enable lightweight and efficient token revocation without centralized coordination. In contrast, asymmetric crypto-based schemes achieve stronger cryptographic guarantees but with higher cost.

Table 3: Comparative trade-offs with existing authentication protocols

Feature	Proposed	FC-PA [36]	ECA-VFog [37]	OTAuth [38]
Crypto Primitive	HMAC	ECC	Pairing	PQC+Symm
Session Unlinkability	✓	✗	Partial	✗
Token Revocation	Bloom Filter	✗	✓	✗
Pseudonym Privacy	Strong	Medium	Medium	Weak
Computation Time	2.1 ms	2.95 ms	3.25 ms	2.3 ms
Comm. Overhead	512 B	738 B	890 B	720 B
OBU Storage	1.8 KB	4.5 KB	5.6 KB	3.9 KB
Formal Verification	✓	✓	✗	✓

6.5.4 Limitations and future work

While our scheme performs well under current assumptions, it has limitations:

- **Centralized TA:** The Trusted Authority remains a central trust anchor. Although not involved in session exchanges, its availability is essential for registration and revocation.
- **Bloom Filter Sync:** If revocation filters are not consistently synchronized across RSUs, there may be inconsistencies in token validation. Future work will explore distributed or probabilistic filter synchronization models.
- **Post-Quantum Support:** Our design emphasizes lightweight symmetric security over post-quantum readiness. Integrating PQC while maintaining efficiency is part of future directions.

6.5.5 Practical deployment and scalability considerations

The proposed scheme was conceived particularly for practical vehicular deployment such as high vehicular density, frequent handovers of RSUs, and limited computational capabilities.

1. Lack of State Tracking: In contrast to those other schemes, which need to maintain state across packets and are heavily centralized, the operations at the RSU level in our protocol are inherently stateless. Authentication is carried out based on session-specific pseudonym-token pairs and ephemeral randomness (R_s, R'_s), providing RSUs with the capability to verify incoming requests without storing session record or maintaining synchronized state.

2. Efficient Handover Support: Vehicles may drive through multiple RSU coverage areas within a few seconds in real scenarios. Our scheme additionally provides the handover property through making each authentication request self-contained and generating session key from a fresh nonce and token-bound symmetric key. There is no state to resume or to propagate between RSUs.

3. Bloom Filter Scalability: Every RSU has independent bloom filter to make the revocation checking. Bloom filters offer O(1) time membership test with very low memory requirements. For instance, considering a false positive rate of 1% and a pool of 10^4 revoked tokens, the Bloom filter can be stored with about 12 KB, which is acceptable for edge RSUs with restricted memory. These filters are re-writeable (or can be on occasion) by the TA without interrupting business.

4. Resistance against Desynchronization: Rotating the token is started due to the age of the token, the number of session or domain change. In case of desynchronization (e.g., network partition, vehicle reboots), the OBU switches to the next valid pseudonym-token pair automatically. As that tokens are stateless and fact-checkable autonomous, short suspension cannot jeopardize the long operation of a system.

5. Latency and Resource Utilization: Trials have verified that the service time per session still keeps less than 3 ms when 1000 vehicles authenticate concurrently. This further verifies the suitability for high-speed V2I communications in urban and highway scenarios. By not using public key cryptography, the CPU usage in the OBUs is kept low, and the memory requirement never exceed 2 KB on the OBUs for storage of pseudonym-token data.

The design results in a very responsive (real-time), decentralized, gracefully handling handover and revocation scheme—driving the protocol to be ideal for real-world, high-impact vehicular scenarios.

7 Conclusion and future work

A lightweight novel privacy-enhanced authentication scheme for V2I communication was proposed in this paper. The proposed approach combines session-level obscurity, time-constrained pseudonym-token pairs, and symmetric HMAC-based challenge–response interactions to achieve mutual authentication, key freshness, resistance against replay and impersonation, and unlinkability. Contrary to previous protocols that have incorporated public-key signatures, the protocol design achieves efficient and scalable deployment in bandwidth-limited and resource-constrained vehicular environments. The distinguished and non-retrievable nature of each session is ensured by the four-phase design of the protocol, i.e., secure pseudonym initialization, mutual authentication with session obfuscation, unlinkable session key derivation, and token refresh with rebinding. It was shown empirically

and semantically secure against common attacks, and automated support using AVISPA provided evidence of its verifiability in symbolic security models. Performance evaluations also demonstrated its effectiveness: the scheme exhibited better performance than recent schemes in terms of computation expense, communication overhead, and storage cost, and can provide at most 35% efficiency gains.

We plan to incorporate post-quantum cryptographic primitives and evolve the trust score mechanisms for better security hardening in multi-hop and appropriate vehicular networks in future work.

References

[1] M. A. Al-Shareeda, L. B. Najm, A. A. Hassan, S. Mushtaq, and H. A. Ali, "Secure iot-based smart agriculture system using wireless sensor networks for remote environmental monitoring," *STAP Journal of Security Risk Management*, vol. 2024, no. 1, p. 56–66, 2024. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2024.1.4

[2] A. R. Khan, M. F. Jamlos, N. E. Osman, M. I. Ishak, F. Dzaharudin, Y. K. Yeow, and K. A. Khairi, "Dsrc technology in vehicle-to-vehicle (v2v) and vehicle-to-infrastructure (v2i) iot system for intelligent transportation system (its): A review," *Lecture Notes in Electrical Engineering*, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:237651229

[3] R. B. Sulaiman and A. Khraisat, "Metaheuristic-driven feature selection with svm and knn for robust ddos attack detection: A comparative study," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, p. 182–203, 2025. [Online]. Available: http://dx.doi.org/10.63180/jcsra.thestap.2025.4.1

[4] C. Ge and S. feng Qin, "Digital twin intelligent transportation system (dt□its)—a systematic review," *IET Intelligent Transport Systems*, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:271730228

[5] R. Suryadithia, M. M. A. Faisal, A. S. Putra, and N. Aisyah, "Technological developments in the intelligent transportation system (its)," *International Journal of Science, Technology & Management*, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:236337635

[6] R. Dudhwala and D. J. R. Pitroda, "Intelligent transportation system (its) - a review," *International Journal of Constructive Research in Civil Engineering*, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:242230842

[7] L. Li, D. Chen, Y. Liu, Y. hua Liang, Y. Wang, and X. Wu, "Unlinkable and revocable signcryption scheme for vanets," *Electronics*, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:272187483

[8] H. J. Nekad, D. K. Shary, and M. A. Alawan, "Position control of linear synchronous reluctance motor using a modified camel traveling algorithm-based proportional integral controller." *Mathematical Modelling of Engineering Problems*, vol. 11, no. 6, 2024.

[9] A. Manasrah, Q. M. Yaseen, H. Al-Aqrabi, and L. Liu, "Identity-based authentication in vanets: A review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, pp. 4260–4282, 2025. [Online]. Available: https://api.semanticscholar.org/CorpusID:275890166

[10] F. F. Jaber, D. K. Shary, and H. Alrudainy, "Motion control of linear induction motor using self-recurrent wavelet neural network trained by model predictive controller," *International Journal of Power Electronics and Drive Systems*, vol. 13, no. 2, pp. 792–804, 2022.

[11] Z. G. Al-Mekhlaf, M. A. Saare, J. M. H. Altmemi, M. A. Al-Shareeda, B. A. Mohammed, G. Alshammari, Y. A. Alkhabra, I. Alreshidi *et al.*, "A quantum-resilient lattice-based security framework for internet of medical things in healthcare systems," *Journal of King Saud University Computer and Information Sciences*, vol. 37, no. 6, pp. 1–19, 2025.

[12] T. Nandy, R. M. Noor, R. Kolandaisamy, M. Y. I. Idris, and S. Bhattacharyya, "A review of security attacks and intrusion detection in the vehicular networks," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 36, p. 101945, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:267484986

[13] M. Almaayah and R. B. Sulaiman, "Cyber risk management in the internet of things: Frameworks, models, and best practices," *STAP Journal of Security Risk Management*, vol. 2024, no. 1, p. 3–23, 2024. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2024.1.1

[14] M. D. Vincenzi, G. Costantino, I. Matteucci, F. Fenzl, C. Plappert, R. Rieke, and D. Zelle, "A systematic review on security attacks and countermeasures in automotive ethernet," *ACM Computing Surveys*, vol. 56, pp. 1 – 38, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:266177229

[15] F. Azam, S. kumar Yadav, N. Priyadarshi, S. Padmanaban, and R. C. Bansal, "A comprehensive review of authentication schemes in vehicular ad-hoc network," *IEEE Access*, vol. 9, pp. 31 309–31 321, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:232071217

[16] A. Aldossary, T. Algirim, I. Almubarak, and K. Almuhish, "Cyber security in data breaches," *Journal*

of Cyber Security and Risk Auditing, vol. 2024, no. 1, p. 14–22, Dec. 2024. [Online]. Available: http://dx.doi.org/10.63180/jcsra.thestap.2024.1.3

[17] A. N. Patil and S. V. Mallapur, "A review on security-based routing protocols for vehicular ad hoc networks," *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 399–405, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:257667564

[18] U. Iqbal, T. Davies, and P. Perez, "A review of recent hardware and software advances in gpu-accelerated edge-computing single-board computers (sbcs) for computer vision," *Sensors (Basel, Switzerland)*, vol. 24, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:271488200

[19] B. Almelehy, A. Anwar, G. Nassreddine, and M. Maayah, "Web application security: An analytical study of cyber threats and defense mechanisms," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, p. 43–62, May 2025. [Online]. Available: http://dx.doi.org/10.63180/jcsra.thestap.2025.3.5

[20] H. Mistareehi, H. A. B. Salameh, and D. Manivannan, "An on-board hardware implementation of aodv routing protocol in vanet: Design and experimental evaluation," *2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pp. 1–6, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:257524869

[21] A. Kaur, R. Kaur, and R. Chhabra, "Role of artificial intelligence for pedestrian detection in iov: A systematic review," *2023 IEEE 2nd International Conference on Industrial Electronics: Developments & Applications (ICIDeA)*, pp. 505–510, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:264879538

[22] S. R. Addula and A. Ali, "A novel permissioned blockchain approach for scalable and privacy-preserving iot authentication," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, p. 222–237, 2025. [Online]. Available: http://dx.doi.org/10.63180/jcsra.thestap.2025.4.3

[23] A. Boulkroune, F. Zouari, and A. Boubellouta, "Adaptive fuzzy control for practical fixed-time synchronization of fractional-order chaotic systems," *Journal of Vibration and Control*, p. 10775463251320258, 2025.

[24] A. Boulkroune, S. Hamel, F. Zouari, A. Boukabou, and A. Ibeas, "Output-feedback controller based projective lag-synchronization of uncertain chaotic systems in the presence of input nonlinearities," *Mathematical Problems in Engineering*, vol. 2017, no. 1, p. 8045803, 2017.

[25] F. Zouari, K. B. Saad, and M. Benrejeb, "Robust neural adaptive control for a class of uncertain nonlinear complex dynamical multivariable systems," *International Review on Modelling and Simulations*, vol. 5, no. 5, pp. 2075–2103, 2012.

[26] M. A. Al-Shareeda, A. A. H. Ghadban, A. A. H. Glass, E. M. A. Hadi, and M. A. Almaiah, "Efficient implementation of post-quantum digital signatures on raspberry pi," *Discover Applied Sciences*, vol. 7, no. 6, p. 597, 2025.

[27] F. Zouari, K. B. Saad, and M. Benrejeb, "Adaptive backstepping control for a class of uncertain single input single output nonlinear systems," in *10th International Multi-Conferences on Systems, Signals & Devices 2013 (SSD13)*. IEEE, 2013, pp. 1–6.

[28] L. Merazka, F. Zouari, and A. Boulkroune, "High-gain observer-based adaptive fuzzy control for a class of multivariable nonlinear systems," in *2017 6th International Conference on Systems and Control (ICSC)*. IEEE, 2017, pp. 96–102.

[29] G. Rigatos, M. Abbaszadeh, B. Sari, P. Siano, G. Cuccurullo, and F. Zouari, "Nonlinear optimal control for a gas compressor driven by an induction motor," *Results in Control and Optimization*, vol. 11, p. 100226, 2023.

[30] L. Merazka, F. Zouari, and A. Boulkroune, "Fuzzy state-feedback control of uncertain nonlinear mimo systems," in *2017 6th International Conference on Systems and Control (ICSC)*. IEEE, 2017, pp. 103–108.

[31] B. Schiel, S. Swindler, A. Farmer, D. Sharp, A. H. Murali, B. Corry, and P. Lundrigan, "A multi-layered framework for informing v2i deployment decisions using commercial hardware-in-the-loop testing of rsus," *2024 IEEE Vehicular Networking Conference (VNC)*, pp. 313–320, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:270928951

[32] J. P. A. León, A. Busson, L. J. de la Cruz Llopis, T. Begin, and A. F. M. Boukerche, "Strategies to plan the number and locations of rsus for an ieee 802.11p-based infrastructure in urban environment," *Proceedings of the Int'l ACM Conference on Modeling Analysis and Simulation of Wireless and Mobile Systems*, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:264450005

[33] A. C. H. Chen, C.-K. Liu, C.-F. Lin, and B.-Y. Lin, "V2x credential management system comparison based on ieee 1609.2.1 and etsi ts 102 941," *2024 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, pp. 1–6, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:274641415

[34] Y. Zhou, J. Chen, G. Ye, D. Wu, J. H. Wang, and M. Chen, "Collaboratively replicating encoded content on rsus to enhance video services for vehicles," *IEEE Transactions on Mobile Computing*, vol. 20, pp. 877–892, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:213790328

[35] M. A. Al-Shareeda, T. Gaber, M. A. Alqarni, M. H. Alkinani, A. A. Almazroey, and A. A. Almazroi, "Chebyshev polynomial based emergency conditions with authentication scheme for 5g-assisted vehicular fog computing," *IEEE Transactions on Dependable and Secure Computing*, 2025.

[36] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. Alreshidi, M. Alazmi, J. S. Alshudukhi, and M. Alsaffar, "Fc-pa: fog computing-based pseudonym authentication scheme in 5g-enabled vehicular networks," *IEEE Access*, vol. 11, pp. 18 571–18 581, 2023.

[37] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "Eca-vfog: An efficient certificateless authentication scheme for 5g-assisted vehicular fog computing," *Plos one*, vol. 18, no. 6, p. e0287291, 2023.

[38] Z. G. Al-Mekhlafi, S. A. Lashari, J. Altmemi, M. A. Al-Shareeda, B. A. Mohammed, A. A. Sallam, B. A. Al-Qatab, M. T. Alshammari, and A. M. Alayba, "Oblivious transfer-based authentication and privacy-preserving protocol for 5g-enabled vehicular fog computing," *IEEE Access*, 2024.

[39] T. Haines, J. Müller, and I. Querejeta-Azurmendi, "Scalable coercion-resistant e-voting under weaker trust assumptions," *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:259099319

[40] C. C. Fung, S. Yogarayan, S. F. A. Razak, and A. B. Azman, "A review study of ieee 802.11p on-board unit for v2x deployment," *2023 11th International Conference on Information and Communication Technology (ICoICT)*, pp. 165–171, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:263228892

[41] A. Al-Mohtaseb, A. Q. Hanoon, G. Samara, E. A. Daoud, O. K. A. Alidmat, R. Batyha, M. Aljaidi, R. Alazaidah, and A. Elrashidi, "A comprehensive review of vanet attacks: Predictive models, vulnerability management, and defense selection," *2024 25th International Arab Conference on Information Technology (ACIT)*, pp. 1–9, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:276434897

[42] B. Hildebrand, M. Baza, T. Salman, F. H. Amsaad, A. Razaqu, and A. Alourani, "A comprehensive review on blockchains for internet of vehicles: Challenges and directions," *ArXiv*, vol. abs/2203.10708, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:247594668