IJRCS

International Journal of Robotics and Control Systems
Vol. 6, No. 1, 2026, pp. 626-650
ISSN 2775-2658
http://pubs2.ascee.org/index.php/ijrcs

ASCEE

A Fog-Based Decentralized Lightweight Revocation Protocol for Sybil-Resistant 5G Vehicular Networks

Mohanad Ahmed Abdulrazzaq Diwan Alzamili [a,1], Aymen A. Hameed [b,2], Nada Mohammed Hassan Moter [c,3], Jalal M. H. Altmemi [a,4,*], Mahmood A. Al-Shareeda [d,e,5,*], Mohammed Amin [f,6], Rami Shehab [j,7]

[a] Information Technology Management Department, Southern Technical University, Basrah, Iraq
[b] Department of Medical Instruments Engineering Technique, University of Bilad Alrafidan, Basrah, Iraq
[c] Pharmacy Department, Medical Technical Institute-Basra, Southern Technical University, Basra, 61001, Iraq
[d] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq
[e] College of Engineering, Al-Ayen University, 64001, Thi-Qar, Iraq
[f] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan
[j] Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia
[1] Mohanad.a.abdulrazaq@stu.edu.iq; [2] draymen@bauc.edu.iq; [3] tsnada2016@stu.edu.iq; [4] Jalal.altmemi@stu.edu.iq; [5] mahmood.alshareedah@stu.edu.iq; [6] m.almaiah@ju.edu.jo; [7] Rtshehab@kfu.edu.sa
[*] Corresponding Author

ARTICLE INFO

Article History
Received November 12, 2025
Revised December 28, 2025
Accepted February 21, 2026

Keywords
Fog Computing;
5G Vehicular Networks;
Sybil Attack Mitigation;
Decentralized Revocation;
Privacy-Preserving Security;
Certificate Revocation

ABSTRACT

The accelerated implementation of fifth-generation (5G) vehicular networks has escalated security issues, with Sybil attacks representing a significant threat, since malicious vehicles use pseudonym mechanisms to forge multiple identities and sabotage trust-based services. Currently deployed certificate revocation techniques have a highly centralized model, result in large latency time and lack scalability with insecure privacy because of the dynamically changing vehicular environment. In this paper, we propose a fog-based decentralized lightweight revocation protocol (FD-LRP) to overcome the above shortcomings for Sybil-resistant 5G vehicular networks. The research novelty is the development of a realtime revocation service, which features suspicion-based scoring at fog nodes, and collaborative multi-fog consensus mechanism to swiftly and effectively isolate malicious vehicles without pre-maturely revealing long-term identities. FD-LRP also presents a light-weight certificate revocation list (WL-CRL) that forwards only the hashed-pseudonyms with delta messages, decreasing the communication and storage overhead. Performance of FD-LRP is evaluated by comprehensive simulation, and shows the up to 96.5% accuracy in Sybil detection, with less than 7 ms as average time of L-CRL update operation. We verify that FD-LRP is an efficient, privacy-preserving and viable revocation mechanism for the future 5G vehicular networks based on our results.

© 2025 The Authors.
Published by Association for Scientific Computing Electrical and Engineering.
This is an open access article under the CC-BY-SA license.

1. Introduction

The development of ITS is closely related to the progress of wireless communications, especially the 5G and beyond technologies [1], [2]. 5G integrated with Vehicular Ad hoc Networks (VANETs), to be referred to as 5G-V2X, is expected to provide services such as ultra-reliable low-latency com-

munication (URLLC) [3]–[5], massive machine-type communication (mMTC) [6], [7], and enhanced mobile broadband (eMBB) [8], and support various important automotive applications from traffic safety to autonomous driving [9]–[11]. Nevertheless, the more widespread and distributed vehicular networks are, the more susceptible they are to a wide range of security and privacy threats [12]–[14].

One of the most menacing attacks against 5G vehicular networks is Sybil attack that a misbehaving vehicle may pretend to have multiple fake or temporarily changing pseudonyms in order to misslead with respect to traffic information, cooperation and trust-based decision making [15]–[21]. The above methods are derived from traditional certificate-based security models that use centralized Certificate Authorities (CAs) and Certificate Revocation Lists (CRLs) to maintain trust and validate identity [22]–[24]. Although these schemes establish a foundation of authenticity, they have crucial disadvantages in terms of latency, scalability, and privacy-preserving nature when applied in a heavily mobile vehicular environment [25]–[29]. The delay added by the global CRL dissemination, and the time complexity of checking each one of the certificates in real-time, is unsuitable for safety-relevant applications such as emergency collision avoidance or merging at intersections [30], [31]. Furthermore, Pseudonym systems can be used by Sybil attackers as they can create and change their identities quickly to escape detection; in this scenario, the traditional methods are not enough to do so [32], [33].

Decentralized revocation mechanisms (e.g., by leveraging fog/edge computing paradigm) have been recently proposed, in which the local entities, such as Roadside Units (RSUs) or fog nodes, can contribute to the anomaly detection and decision-making process [34], [35]. Nevertheless, most of these methods depend on a central confirmation with or without dynamic agent user behavior scoring, or do not maintain a strong level of user privacy [36]–[38]. Besides, a few of the existing models consider the coordination between fog nodes to reach agreement on misbehavior, which is important to prevent false positives and collusion-based types of attacks [39], [40].

Despite the available work, there is still a dearth of lightweight decentralized revocation solution which provides (i) real-time Sybil isolation, (ii) scalability for dense traffic conditions, iii) false accusation resilience via collaborative validation and iv) strong privacy protection with infrequent exposure of a long term identity. Especially, the nonexistence of an effective collaborative revocation mechanism at fog level and the inefficiency of conventional CRL dissemination are still challenges.

To address this gap, in this paper we present a Fog-Based Decentralized Lightweight Revocation Protocol (FD-LRP) for Sybil-resistant 5G vehicular networks. FD-LRP migrates revocation intelligence from the central to fog nodes based on real-time behavior-based suspicion scoring and a multi-fog collaborative consensus mechanism. Contrary to that a single detection point, in which misbehaved evidence is collected from the fog nodes and transferred back to this point for making revocation decision, each misty node at the cloud level may resort to more than one fog nodes or use its neighboring nodes' detected evidence when judging whether to make the decision; hence reduces false positives and enhance protection again insider threats. To solution this issue efficiently and retain the unlinkability, FD-LRP introduces a lightweight CRL (L-CRL), which forwards only hash value of pseudonyms using delta updates to reduce the communication and storage overhead. The contributions of this paper can be highlight as follows:

- We design a fog based decentralized lightweight revocation framework which provides distributed decision-making, scalable trust verification and real-time response in 5G vehicular networks.
- We propose a dynamic behavior-based suspicion scoring model which aggregates several behavioral based indicators to identify both Sybil and protocol-level attacks without knowing the long lifetime identities of the vehicles.
- We design a multi-fog collaboration consensus mechanism and make the revocation decision precise, fault-tolerant and remove single point manipulation as well as false accusation.
- We propose an efficient compact and privacy-protected L-CRL, which enables to delivery and prove the validity of a revoked certificate with little communication and storage costs.

- We provide extensive performance evaluation results to show that FD-LRP successfully minimizes revocation latency and obtains competitive communication overhead as well as low false-positive rate compared with state-of-the-art schemes.

The rest of this paper is organized as follows. Section 2 review some relevant research studies for VANET. In this Section 3, we describe the proposed system and threat models. Section 4 describes the FD-LRP protocol design. Section 5 and Section 6 presents security analysis and performance evaluation, respectively. Section 7 concludes and suggests future work.

2. Related Work

Security and trust issues in vehicular ad hoc networks (VANETs) and 5G-V2X systems have received plenty of attention recently because of the rising importance of safety-critical and cooperative vehicular applications. Previous literature on Sybil attacks and revocation mechanisms can be categorized into three groups: centralized certificate-based solutions, cryptographic authentication schemes and decentralized fog or blockchain-facilitated works.

2.1. Centralized Certificate Revocation Approaches

Previous vehicular security schemes have been based on the use of centralized certificate authorities (CAs) and global certificate revocation lists (CRLs) for providing authentication and misbehavior policies [41], [42]. Although these methods contribute to a minimum trust seed commonly used by other models, they have some intrinsic disadvantages in complex VANET environments. Especially, Global CRL publication causes high latency and communication overhead and scale infeasibility when the network becomes dense. Further, the frequent switching of pseudonyms, which is essential in order to protect the privacy of a user, does not prevent Sybil attackers from escaping revocation in time and thus it does not make central protocols suitable for real-time protection.

Trust and resilience enforcement in vehicular networks have prompted various work on Sybil attack detection and misbehavior revocation in addition to secure communication schemes in 5G-based VANETs [43], [44]. Traditional solution have been mainly based on centralized Certificate Authorities (CAs) and Certificate Revocation Lists (CRLs), which is yet unable to be scalable and efficient in highly dynamic vehicular environments. In order to provide solutions to these problems, recent research works [45]–[48]have proposed on cryptographic approaches, trust based systems and decentralized frameworks based on fog and edge computing.

2.2. Cryptographic and Authentication-Based Solutions

In addition to the relaxation of constraints for not needing a large size CRL, all the above methods have been explored mostly to remove overheads from centralized CRL. There are numerous works in cryptography based authentication and revocation so far suggested including attribute based encryption, certificate less signatures and signcryption schemes Topic Description: If this Research is referred, then ATKR means Attribute-based Cryptography (ATC)-Key revocation. These tools strengthen security guarantees such as confidentiality, integrity, and criteria privacy [49], [50]. However, these are usually complicated cryptographic operations, which cause an additional computational overhead on board units (OBUs) and they need continuous interactions with centralised entities. Thus, their application in the context of latency-constrained vehicular sceneries is still very constrained. Moreover, most of the cryptographic techniques are not designed for continuous behavior monitoring as they are more suited for authentication, and therefore less effective when it comes to Sybil attacks exploiting legitimate but misused credentials.

Almazroi et al. [51] introduced a new fog computing-powered lightweight Sybil resistant scheme (FC-LSR) which is designed to the 5G-enabled vehicular networks. Junaidi et al. [52] presents a secure platoon management technique based on ECC against the Sybil and other cyber attacks. It

provides vehicle and message authentication, forward backword secrecy and privacy. Sehar et al. [53] introduced a Vehicular network Based Consensus Algorithm (VBCA) using consortium blockchain to enhance data security and efficiency in vehicular networks. Khatri et al. [54] presents a PoL-based location verification scheme using smart contracts and RSUs to mitigate Sybil attacks in VANETs. By requiring unique puzzles for location reporting, it limits fake identity submissions. Tulay et al. [55] proposed a channel state information (CSI)-based Sybil attack detection scheme for vehicular networks by utilizing spatio-temporal fluctuations of the CSI.

2.3. Decentralized and Fog-Reinforced Revocation Schemes

Some recent works have investigated a decentralized, fog/edge architecture aimed at providing improved responsiveness and scalability. In these schemes, RSUs or fog nodes engage in local misbehavior detection and revocation adjudications. And, fog Sybil detection methods can help to relax the reliance on cloud-side central authorities and react locally more quickly. Nonetheless, these cloud-based solutions and some existing fog-based ones employ a single-fog decision point to achieve their goal and they remain thus susceptible to false positives, insider attacks or compromised fog nodes. Also, several of the proposals do not have any coordinated validation among fog nodes, something that is necessary in order to produce reliable and fault-tolerant revocation decisions.

Zhu et al. [56] proposes a beacon-packet-based scheme for detecting and tracing Sybil attacks in Connected Automobile Vehicles. By using RSU-directed key broadcasts and neighbor graph analysis, it achieves real-time Sybil detection and source traceability. Su et al. [57] introduces a hybrid blockchain-based privacy-preserving authentication scheme for VANETs, combining consortium and private chains to balance security, speed, and privacy. Zhang et al. [58] presented an attribute-based secure communication scheme for 5G NR-V2X with pre-authentication and dynamic credential enhancement. Ullah et al. [59] proposed a conditional privacy preserving hybrid signcryption scheme for vehicular networks, to ensure the secrecy of the message and the signers' identity.

Existing solutions cater to either detection or authentication for lossy tools but do not have a cost-effective and fault-tolerant mechanism for revocation (Table 1). FD-LRP is the only scheme which integrates behavior-based detection, collaborative fog-level consensus and lightweight revocation dissemination in an integrated framework. Even after the developments mentioned above, a light-weight decentralized revocation framework that provides both real-time Sybil isolation, cooperation-based decision-making, scalability under malicious/leaky traffic conditions and strong level of privacy remains unsolved. One set of solutions either suffer from drastically intensive computing and communication burden or are based on single-point decisioning while the other one lacks efficient means for revocation dissemination.

In contrast with this, the FD-LRP scheme fuses behaviour-driven suspicion scoring and multi-fog collaborative consensus to require revocation decisions accepted independently by several fog nodes to be enforced. In addition, FD-LRP proposes a Lightweight Certificate Revocation List (L-CRL) using hashed pseudonyms and delta updates to greatly reduce the dissemination overhead while maintaining unlinkability. This hybrid of decentralized consensus, lightweight structure and privacy-preserving revocation set FD-LRP apart from other existing state-of-the-art schemes.

3. System and Threat Model

This section introduces the system model and threat assumptions of our proposed FD-LRP framework. We start by detailing the vehicular fog computing setting and the tasks of primary entities participating in decentralized revocation, such as vehicles, fog nodes, and trusted authorities. We then describe our system model and formally define adversarial capabilities modeled by the proposed IoT-based anonymous communications infrastructure, including Sybil attacks, insider threats and privacy violations. This model is the basis for the investigation of both security and correctness as well as

performance aspects of FD-LRP, respectively.

Table 1. Comparison of representative Sybil detection and revocation schemes in vehicular networks

Scheme	Approach Category	Main Strengths	Key Limitations
Junaidi et al. [52]	ECC-based authentication	Strong cryptographic security; conditional privacy; message authentication	High computational overhead; no continuous behavior monitoring; limited effectiveness against Sybil attacks
Sehar et al. [53]	Blockchain-based consensus	Tamper resistance; auditability; decentralized trust management	High latency; storage and consensus overhead; unsuitable for real-time vehicular environments
Khatri et al. [54]	PoL-based location verification	Effective location-based Sybil mitigation; decentralized validation	Puzzle-solving overhead; reliance on infrastructure support; limited scalability
Zhang et al. [58]	Attribute-based cryptography	Fine-grained access control; secure pre-authentication	High cryptographic complexity; centralized attribute verification; increased latency
Ullah et al. [59]	Hybrid signcryption	Conditional privacy preservation; message confidentiality	Conceptual revocation model; lack of practical CRL handling and evaluation
FD-LRP (This Work)	Fog-based decentralized revocation	Real-time response; multi-fog consensus; low computation and communication overhead; privacy preservation	Assumes semi-trusted fog nodes and a trusted authority for identity traceability

3.1. System Model

The proposed Fog-Based Decentralized Lightweight Revocation Protocol (FD-LRP) is tailored for a VFC system enabling 5G-V2X communications. The distributed architecture, represented in Fig. 1, includes communicating entities that cooperatively enable real-time misbehavior detection and revocation while guaranteeing the vehicle privacy.

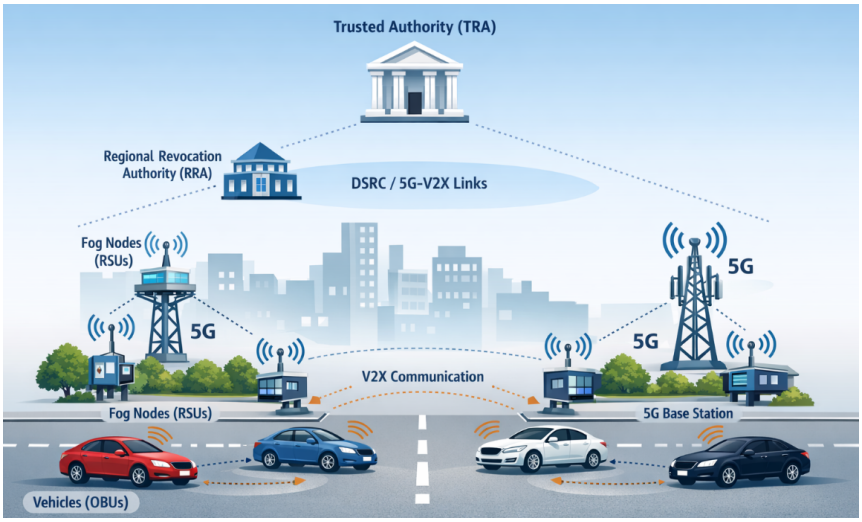

Fig. 1. System model of proposed FD-LRP solution

- Vehicles (OBUs): There is a Vehicle On-Board Unit (OBU) in every vehicle that can exchange messages with RSUs and other vehicles using means of Vehicle-to-Everything (V2X) communi-

cation. ”Vehicles receive pseudonym certificates that are renewed at regular intervals in order to protect privacy [60]–[62].

- Fog Nodes (RSUs): These are the edge computing devices placed at strategic locations such as RSUs and cellular base stations. They are in charge of real-time traffic surveillance, vehicles' behavior analysis, revocation tag issuing, and the consensus-driven validation [51], [63], [64].
- Trusted Authority (TRA): The TRA is the centralized component in charge of long-term identity handling and permanent revocation decisions, in such a way that privacy is preserved, and it is also responsible for cryptographic traceability management. The TRA keeps the pseudonym-real identity mappings protected under strict access control [65]–[67].
- Regional Revocation Authority: In a hierarchy with a top-level TRA, regionals serve as local administrators for revocation and can be configured to escalate decisions to the TRA [68]–[70].
- Communication Model: Communication is realized by DSRC (Dedicated Short Range Communication) or 5G-V2X links, that short-range exchange of real-time messages among OBUs, RSUs, and fog clusters [71], [72].

3.2. Assumptions

The FD-LRP model is based on the following condition:

- Fog nodes are semi-trusted and they have tamper-resistant hardware, which means unauthorized access or modification of internal procedure is not allowed.
- The TRA is reasonably trusted and non-compromised.
- Real identities cannot be traced from pseudonyms by vehicles without the TRA's permission (authorization hereafter), as stated in the pseudonym management protocol..
- Time can be synchronized network-wide for supporting timestamp verification and prevent replay attack.

These assumptions are compatible with typical vehicular security architectures and offer a practically utility balance between security, performance and privacy.

3.3. Threat Model

FD-LRP is proposed to protect the system against various adversaries, such as external attackers and internal illegitimate participants. The threat model includes:

- Sybil Attackers: Attackers that try to establish multiple fake identities/pseudonyms to influence traffic pattern or mount coordinated disinformation attacks. These identities may change very quickly in order to hide and escape detection [32], [73], [74].
- Insider Threats: Vehicles not engaged in malicious activities or fog nodes that are compromised and do not follow protocol behavior. They could inject incorrect information, suppress revocation votes, or conspire with other malicious parties to reach a consensus [75]–[77].
- Identity Forgery: Attackers might forge pseudonym certificates or try to create forged messages to disrespect the authority of other vehicles [78], [79]. FD-LRP mitigates such threats through ECC signatures and a fog-side message authentication [80], [81].
- Replay Attacks: Attackers can attempt to resend messages that were valid in the past to generate spurious alarms or to mask misbehavior. This is mitigated by timestamp-based validation at both the local fog and the global consensus [82]–[84].
- DoS Attacks: Attackers can do this by overwhelming the fog nodes to get detected on incidents or spam the revocation system with false misbehavior reports. FD-LRP schedules the work in fog clusters and adopt light-weight scoring and verifying mechanism to prevent resource starving [85]–[87].
- Privacy Breach: Attackers (including curious insiders) aim to deanonymize cars, which allows them to associate pseudonyms. FD-LRP guarantees privacy by hashing all pseudonyms in CRLs, and permits traceability only in the presence of TRA consensus under very tough conditions [88],

[89].

4. Design of The FD-LRP Protocol

The fog-based Decentralized Lightweight Revocation Protocol (FD-LRP) has been proposed to satisfy the low-latency, scalable and privacy demand ings in future 5G vehicular communication networks. Different to classic centralized revocation mechanisms such as CRL, which has been used in previous works, FD-LRP introduces distributed fog nodes to locally detect misbehavior, validate revocation decisions collectively and efficiently spread the revoked information between vehicles without exposing vehicle long-term identities. By facilitating the vehicle-to-vehicle coordination, this decentralized architecture can provide real-time response and scalability in dense and high mobile vehicular environment.

FD-LRP operates through four phases: Misbehavior Detection at Fog Nodes; Local Revocation Scoring and Tagging; Consensus-Based Fog-Level Decision; and Lightweight CRL Dissemination, as shown in Fig. 2. Each Fog node is watching vehicle behavior in real time, judging suspicious activities and then exchanging revocation evidence with its neighbors. After that, these nodes together update the regional revocation list.Dynamically revoked are short-lived pseudonyms (if needed) without disclosing their true identity.

4.1. Misbehavior Detection and Scoring

That is the reason why, in the FD-LRP protocol, each fog node has a localized monitoring agent whose role is to evaluate vehicular behaviors within its coverage area. The purpose of this module is to detect malicious or anomalous behavior that may indicate the presence of Sybil attacks, data forging, and protocol abuse. Consequently, a dynamic suspicion score is provided for each vehicle based on multiple behaviors observed in real-time analysis of messages.

4.1.1. Behavioral Indicators

Let V_i be a vehicle connected to the fog node F_k. A real-time set of features $\{f_{\text{identity}}, f_{\text{location}}, f_{\text{conflict}}\}$ is calculated at any moment for each vehicle:

- f_{identity} Measures the rate of pseudonym alterations over the defined sliding time window. It can surpass a certain threshold, witnessing a possible Sybil attack.
- f_{location} Evaluates spatial abnormalities, such as sudden position changes or physical non-compliance with the actual road topology.
- f_{conflict} Assesses semantic agreement for the transmitted messages between the vehicle and the other cars in its broadcast range. It includes seeming contradictions between reported events or status discrepancies.

4.1.2. Suspicion Score Calculation

Therefore, for each fog, the suspicion score S_i is calculated based on weighted aggregation of pseudo-features as follows:

$$S_i = \alpha_1 f_{\text{identity}} + \alpha_2 f_{\text{location}} + \alpha_3 f_{\text{conflict}}, \tag{1}$$

Where $\alpha_1, \alpha_2, \alpha_3$ are adjustable weighting coefficients suggesting the importance of the given domain, which can be empirically fitted or case-dependent.9

4.1.3. Threshold-Based Classification

Furthermore, at this point, the system defines a threshold θ to classify the vehicle's identification level for further actions. If $Sv_i \geq \theta$, the vehicle is marked as suspicious and placed out of the system by the registration of the revocation tag. This "soft" leaving enables applying proactive dissociation

and deferring the final decision for further consensus among several fog nodes.

Fig. 2. Protocol FD-LRP workflow

4.1.4. Misbehavior Detection and Scoring

In the FD-LRP protocol, each fog node acts as a localized monitoring agent and judges the behavior pattern of a vehicle connected to it. This component aims to identify any malicious activity or anomaly behavior that can infer Sybil attack, data fabrication, or protocol abuse. In this regard, each vehicle is assigned a suspicion score, which is dynamic and accumulative of multiple behavior-based features derived from real-time message observation.

Behavioral Indicators Let V_i denote a vehicle connected to fog node F_k. Define a set of features for each vehicle, $f_{\text{identity}}, f_{\text{location}}, f_{\text{conflict}}\}$, as follows:

- f_{identity}: Count the rate of pseudonym change over a window of time, i.e., any rate beyond the threshold may suspect for Sybil.
- f_{location}: It is designed to count the sudden anomalies of the position. For instance, a vehicle position is changing abruptly, or it is off-road.
- f_{conflict}: It tries to measure the semantics conflict with the other messages coming from other vehicles. it includes event-reporting conflict, state conflict, etc.

Suspicion score is calculated for each fog node by aggregating all the features in following weighted manner.

$$S_i = \alpha_1 f_{\text{identity}} + \alpha_2 f_{\text{location}} + \alpha_3 f_{\text{conflict}}, \tag{2}$$

Where α_1, α_2, and α_3 are the weight parameters, this determines importance of behavior metrics. This can be determined empirically or the nature of the environment. A predefined threshold θ is determined by the system to classify suspicious behavior. If $S_i \geq \theta$, put a test on its message, and it will be declared suspicious by its fog node by tagging it with the revocation tag.

4.2. Fog-Based Collaborative Consensus

To prevent false positives or hasty and unilateral revocations due to bad actors within an arbitrary behavioral probe, FD-LRP enables a decentralized, consensus-driven process to attest for the validity of a revocation tag. Multiple fog nodes must collaborate and validate the behavioral evidence before a revocation is permanently exited to higher authority, including the TA.

- **Consensus Trigger and Validation:** A current fog node, F_k, that generates the revocation tag, RT_i for a vehicle V_i, broadcasts this tag to all other fog nodes, $\{F_1, F_2, \ldots, F_m\}$ in the same/current and adjacent geography region/mobile network providers. Each recipient node, naturally, must verify the RTI's digital signature, check their observation logs for repeating misbehavior patterns, and confirm the consistency of the behavioral evidence, $Evidence_i$.
- **Voting Mechanism:** Each fog node votes with a binary decision – *approve* or *reject* the revocation tag based on this internal validation. The following binary voting mathematical equation calculates the result:

$$\sum_{j=1}^{m} Vote_j \geq \delta \cdot m$$
$$Vote_j \in \{0, 1\}, \tag{3}$$

  It is a majority voting scheme, where $\delta \in (0.5, 1]$ is the consensus ratio, and it is generally set between 60% and 80%. If the consensus is reached, the tag is further enabled to a regional or central authority for permanent revocation.
- **Consensus Certification:** After the consensus is reached, the fog node that started the behavioral probe has issued a Consensus Certificate, CC_i:

$$CC_i = \{RT_i, Sig_{F_k}, \{Sig_{F_j}\}_{j=1}^{n}\} \tag{4}$$

  All Sig_{F_j} are the voting fog node signatures. It proves to be a non-tamper evident that is used for the verification of exit revocation collision and maybe even presented to a TRA for global Dissemination via a lightweight CRL.
- **Fault Tolerance and Redundancy**: There is no guaranteed that all fog nodes/do revocation could will execute the fully agreements voting process, due to potential node failures and network partitions. Thus the protocol recommends:
  - Redundant dissemination of all revocation tags to a backup fog cluster.
  - Timeout and fallback strategies – if no consensus is reachable after a reasonable time T_cons, the original issuing fog node must revoke the revocation tag with an independent piece of evidence.
  - Asynchronous consensus rounds – when the communication is always continuing and a majority isn't possible, the revocation tag's confirmation is simply delayed but doesn't stop the current problematic.

4.2.1. Lightweight CRL Propagation

After achieving consensus among fog nodes and certifying the pseudonym identification, the alleged offenders are invalidated worldwide by the Trusted Authority or a specifically designated Re-

gional Revocation Authority. For efficient and scalable dissemination of revocation information, FD-LRP introduces a L ightweight Certificate Revocation List (L-CRL) based on high-mobility vehicular environments. L-CRL Structure. The L-CRL representation of revoked entities is compact to minimize bandwidth and verification overhead. Specifically, each L-CRL entry is structured as:

$$\mathsf{L\text{-}CRL}i = \{\mathsf{Hash}(\mathsf{PID}_i), T\mathrm{rev}, \mathsf{CC}_i\},$$

Where is a pseudonym hash for unlinkability and data minimization, is the revocation timestamp, and is an associated consensus certificate as proof of misbehavior. Dissemination Strategy. In order to thinly and evenly distribute the L-CRL throughout the network, a hybrid L-CRL push-pull broadcast model is built as follows:

- Push-based dissemination: periodic L-CRL transmissions from fogs and RSUs to proximate OBUs.
- Pull-based searching: L-CRL entry vehicle requests to fog nodes while entering new regions or rejoining network coverage.
- Delta updates: broadcasts just the new revoked hashes for improving efficiency.

In addition, each vehicle keeps a recent L-CRL hash-based cache for quick verification. The recipient, upon receipt of the message from another vehicle: – computes the pseudonym volume issued to the source; – verifies that a Hash of J matches with one in its local cache and discards if so (and checking whether or not the sending identity is still revoked). Efficiency and Privacy Considerations.

4.3. Revocation of Permanent Identity

While FD-LRP focuses on light-weight, pseudonym-based revocation for responsiveness and privacy, there are still scenarios (e.g., persistent misbehavior, collusion-based Sybil attacks, security policy violation) where permanent identity revocation is required. This procedure is performed with the cooperation of fog nodes and the Trusted Authority (TRA), ensuring liability and regulation compliance.

- Escalation Criteria: The permanent identity revocation is also addressed in-case of repeated valid revocation tags (RT_i) issuance for the same vehicle over different fog zones. More than one L-CRL entry with pseudonyms mapping to different indices and were issued to the same entity (the real-world owner). Juxtaposition of high-risk scenarios such as propagating worms, creating false disaster events, or multi-vehicle collisions.
- Traceability Request Procedure: When escalation conditions are met, the submitting fog node (or a decision-making Regional Revocation Authority) sends a Traceability Request to the TRA. The query is: The pseudonym hash set, Associated consensus certificates (CC_i), Corroborating logs and evidence gathered from fog nodes. The TRA traces cryptographic pseudonyms using safe trapping of secure (pseudo to real identity) mappings kept under stringent access control. The traced identity TID_i is added to the revocation list.
- Identity Revocation and Notification: When the persistent identity of a vehicle is confirmed as an attacker, the TRA can revoke the long-term credentials of that vehicle and its future pseudonym authorization. Notifies all RFCs and CAs. Updates a secure, salutatory global Identity Revocation List (IRL),
- Privacy Compliance and Auditing: To avoid abuse or unlawful deanonymization, the TRA Logs all traceability requests that can be accessed only by authorized personnel, Enforces quorum-based revocation of an identity, and provides transparency with publicly visible reports for regulatory scrutiny. This approach is an effective enforcement against bad actors while preserving the privacy of relied-upon parties.

5. Security Analysis

In this section, we discuss the security of the proposed FD-LRP protocol with respect to the system model and threat model formulated in Section 3. We show that FD-LRP significantly attenuates Sybil attacks and other related threats at the same time naturally achieving three desirables, i.e., preserving conditional privacy, guaranteeing fault tolerance, and being robust against malicious insiders.

5.1. Informal Security Analysis

It is in this instance that the protocol, with external attackers; vehicles that have been compromised on a large-scale, and malicious fog nodes as threats, plays out against adversarial models.

- Resisting Sybil Attacks: FD-LRP According to a behaviour-based / behavior-based suspicion scoring mechanism, seconded by fog level consensus, determine and isolate nodes that are both ridiculously pseudo-anonymous and have conflicting location data. So long as decisions are made by misbehavior patterns which can be observed and are corroborated at various fog nodes, the system is able to detect and combat Sybil attacks effectively - even if pseudonyms are cryptographically valid.
- Impersonation and Forgery Protection: Each revocation tag and consensus certificate is digitally signed by the issuing fog node in order to protect messages' authenticity and origin. Since pseudonyms are issued using a certificate-free method (with private key shares), foreign adversaries cannot match real vehicles or carry messages out as long as local and global key components are not breached.
- Defense against Replay Attacks: Timestamp is present in every message structure (behavioral evidence and revocation tags) for the timestamp is verified in local decision as well as inter-fog consensus. So by their nature, obsolete messages or duplications outside the valid time range are automatically dismissed, to level against replay attackers.
- Privacy Retention: In FD-LRP, users can remain anonymous throughout the steps of the decision procedure (i.e., by creating hashed pseudonyms). The real identity connection is delayed until TRA and drawn after convergence to multi-fog agreement. It is not only safe from being "attacked" - but per the principle of data minimization, the least necessary information about oneself should be disclosed or known.
- Backward and forward Tracking, Answerability: To retain pseudonymity in normal operation, but make it traceable here, the Trusted Authority is being used. This function is good for privacy rights and for those in pursuit of accountability, especially among law enforcement and forensic analysis.
- Collusion-Free: The existence of level consensus in the fog means sins have to be processed only after reaching that consensus, which reduces the chance for an attacker comprised of malicious fog nodes to collude against FD-LRP. The protocol requires signature verification and evidence from many independent fog sources, so any single corrupted node has a limited effect.
- Immutable and Integrity Protection: All the crucial suspicion scores, the revocation tags, consensus certificates, and CRL entries are signed cryptographic parts of our protocol. That way, on storage, transmission and verification, consensus ensures that message integrity is not being abused by third parties.
- Denial-of-Service (DoS) Prevention: FD-LRP This eliminates the headache of a centralized point by allowing fog nodes distribute evaluation and filtering work. Under this type of system, there are no single points vulnerable to attack. This design makes DoS attacks on central refutation servers impractical. Further, it prevents consumption of memory–in particular in on-boards' units of cars–by both using (light-weight) data structures and by denaturing the CRL to remove obsolete entries.

5.2. Comparative Analysis

This section discusses about a comparison of the Proposed FD-LRP Protocol and the State-of-the-Art schemes with respect to security performance, revocation overheads, scalability characteristics and privacy conservation effects. The comparison is based on basic design parameters not specific to a particular implementation, then we consider this to be a fair and significant evaluation under various architectural categories. In order to compare and evaluate the effectiveness of the proposed FD-LRP protocol, two of the most recent and verified revocation approaches were analyzed in comparison, which are: the attribute-based scheme of Zhang et al. [58] and the security framework of Ullah et al. [59]. As is evident in Table 2, FD-LRP exhibits significant advantages in terms of Sybil resistance, real-time isolation, and lightweight overhead on resource-constrained OBUs. While the attribute-based method is focused primarily on pre-authentication and features moderate computation costs due to various computations of encryption used, FD-LRP enables dynamic behavior scoring and real-time quarantine of suspicious nodes through fog decision-making. Both approaches implement some degree of privacy, however the algorithm does so through hashed pseudonyms and aubilable traceability administrated by the TRA. In the meantime, Ullah et al.'s framework, though comprehensive, is still largely conceptual and lacks any means for actual implementation or CRL handling. As a result, FD-LRP achieves the most feasible balance between scalability and security/privacy and remains the most viable option for actual implementation in 5G vehicular fog settings.

As compared to the conventional centralized CRL–based schemes, FD-LRP eliminates global CRL dissemination requirement and also reduces revocation latency and communication overhead by a large margin. Centralized solutions depend on the dissemination of heavy CRLs in a periodic manner, it is not feasible for dense vehicular networks, moreover these results increase the detection delay process. In contrast, FD-LRP realizes local and regional revocation at the fog level, so that it can respond to Sybil attacks faster without sacrificing scalability.

Table 2. Comparative analysis of representative revocation protocols in vehicular networks

Feature	FD-LRP (This Work)	Zhang et al. (2025) [58]	Ullah et al. (2024) [59]
Revocation Authority	Fog nodes with TRA escalation	Attribute authority	Centralized trusted authority
Sybil Attack Mitigation	Behavior-based detection with multi-fog consensus	Not explicitly addressed	Not explicitly addressed
Privacy Preservation	Hashed pseudonyms with conditional traceability	Attribute hiding mechanisms	Conditional privacy (theoretical)
Real-Time Isolation Capability	Supported via fog-level quarantine	Not supported (pre-authentication only)	Not supported
CRL Design	Lightweight CRL (L-CRL) with delta updates	No CRL mechanism	No implemented CRL mechanism
Computation Overhead (OBU)	Low (lightweight verification and caching)	Moderate (attribute-based cryptography)	Not evaluated
Identity Traceability	Auditable traceability via TRA	Partial exposure during attribute resolution	Conceptual traceability model
Deployment Readiness	Fog-based and simulation-validated	Simulation-based evaluation	Conceptual framework

Cryptographic authentication-based approaches such as ECC and signcryption are able to achieve strong-confidentiality and conditional-privacy protections, however, they also have high computational cost with frequent interactions from their centralized bodies. These solutions are mainly focused in authentication and not on behavioral monitoring, thus being less effective due to Sybil attackers using legitimate credentials. The FD-LRP is incentive compatible and complements cryptographic authentication with behavior-driven detection, thus being able to detect misbehavior also under valid pseudonyms and based solely on low complexity cryptographic operations.

Fog- and edge assisted revocation schemes optimize response time by levitating detection to in-proximity territories of vehicles; but a lot of current work are single-fog decision point, making them susceptible to false positive and insider attacks. FD-LRP overcomes this drawback by diploma with the help of a collaborative multi-fog consensus, which can ensure that the revocation decisions are endorsed by multiple independent fog nodes prior to enforcement. Such a design helps in the strengthened security and fault-tolerance, without bringing in the latency and storage overhead of blockchain-based consensus methods.

From a privacy point of view, FD-LRP preserves unlinkability as it only applies to short-term pseudo-IDs and publishes hashed identities through its lightweight CRL (L-CRL). In contrast to a few existing decentralized solutions need the storage or sharing of identity-related metadata, FD-LRP enables traceability on a conditional basis by only the Trusted Authority with restrictive access control so as to trade off between accountability and privacy.

In conclusion, FD-LRP has the characteristics of simultaneous real-time revocation, cooperation validation, low communication and calculation overheads and privacy preservation. Such a combination of properties is not jointly supported by current solutions, and would make FD-LRP an efficient revocation tool for 5G vehicular networks.

5.3. Limitations and Trade-offs

Although FD-LRP performs best in revocation latency, scale and privacy preserving, there are compromises and shortcomings to be considered. First, the protocol requires fog nodes to be semi-trusted and tied with tamper-resistance hardware. While the multi-fog consensus can tolerate an isolated compromised fog node, collusion between a large number of fog nodes is outside the threat model under consideration.

Second, FD-LRP adopts a linear behavior-based suspicion scoring scheme to achieve deterministic execution and low latency at the fog layer. This choice is adequate for realtime vehicular scenarios; however, it may be less expressive than learning-based methods against highly adaptive adversaries. It is left for future work to incorporate hybrid or learning-based scoring mechanisms that also maintain essements become possible and provide guarantees of timing at the point they occur.

The performance of FD-LRP, thirdly, depends on the density of neighboring fog nodes to agree upon. In sparsely-deployed (or short-lived) partitions, revocations can be delayed, despite the non-blocking and bounded-wait mechanisms of the protocol designed precisely for avoiding systems stall.

Lastly, conditional traceability is based on a completely trusted Trusted Authority (TRA). This assumption is consistent with current vehicular security practices, however easing the trust-based requirement via distributed or accountable tracing mechanisms is an avenue that we would like to explore in future studies.

6. Results and Discussion

This subsection further details the efficiency of FD-LRP by breaking down its performance from the computational demand, communication bandwidth, to storage overhead perspectives.

6.1. Simulation Setup

The performance of our proposed FD-LRP protocol was simulated by OMNeT++ network simulator that is incorporated with the real-like vehicular mobility model such as SUMO. Urban and freeway driving conditions were simulated with different vehicle densities and mobility profiles. Vehicles exchanged information through IEEE 802.11p / 5G NR-V2X links and the fog nodes deployed at RSUs were responsible behavior monitoring, consensus validation, and revocation spreading. For each simulation run, the simulations were allowed to run for 600 seconds, and we averaged the results over multiple runs for statistical validity. The detailed simulation configuration and key parameters

used in the experiments are summarized in Table 3.

Table 3. Simulation parameters

Parameter	Value
Network simulator	OMNeT++ 5.x
Mobility simulator	SUMO (TraCI interface)
Simulation duration	600 s
Vehicle density	100–300 vehicles
Vehicle speed	20–80 km/h
Communication standard	IEEE 802.11p / 5G NR-V2X
Fog node placement	RSUs / 5G base stations
Fog node resources	4-core CPU, 8 GB RAM
Attack type	Sybil attack
Number of runs	20 (averaged)

6.2. Evaluation Metrics

The following measurements were used to evaluate the efficiency and feasibility of FD-LRP:

- Revocation Latency: Time from misbehavior detection to the point when a malicious vehicle is effectively isolated.
- Sybil Detection Accuracy: The number of correctly identified Sybil attackers to the total number of attackers.
- False Positive Rate (FPR): The ratio of non-malicious vehicles misidentified as malicious.
- Communication Overhead: The aggregated size of all the message exchanged for revocation purpose including the CRL distribution.
- Computational Overhead: Processing overhead in OBUs and fog nodes for detection and revocation.

These two criteria together measure security effectiveness as well as system efficiency.

6.3. Revocation Latency Analysis

Fig. 3 presents the mean revocation latency of FD-LRP w.r.t other compared solutions. FD-LRP is able to retain revocation latency in less than a few milliseconds even under high density vehicular environments. This is largely due to fog-based decision-making and absence of global CRL broadcasting.

On the other hand, centralized CRL-based approaches incur much higher delay because of periodic CRL updating and relying on centralized authorities. Attribute-based and decentralized-with-s-blockchain-assistance schemes introduce even longer delay because of the cryptographic complexity and consensus overhead. These results validate that FD-LRP is suitable for latency-critical vehicular safety services.

6.4. Sybil Detection Precision and False Positives

FD-LRP has an accuracy of over 96% in all tested scenarios listed in Table 4, which is achieved by integrating multi behavioral indicators rather than using a single one. Moreover, the joint multi-fog consensus mechanism is beneficial to eliminate lots of false positives as it requests independent evidence from multiple fog nodes.

FD-LRP has less false positives, especially in high mobility and traffic density scenarios compared with single-point fog-based detection methods. This suggests that consensus-based validation can help against incorrect or malicious revocation.

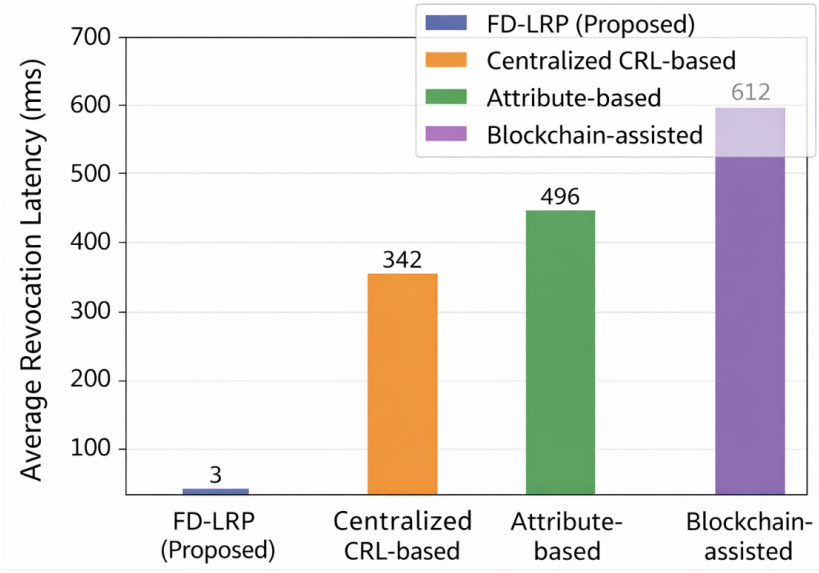

Fig. 3. Average revocation latency of FD-LRP compared with existing approaches

Table 4. Sybil detection accuracy of FD-LRP under different vehicular scenarios

Scenario	Vehicle Density	Attack Ratio (%)	Detection Accuracy (%)
Urban–Low Density	100 vehicles	10	96.4
Urban–Medium Density	200 vehicles	15	97.1
Urban–High Density	300 vehicles	20	96.8
Highway Scenario	250 vehicles	15	97.5
Mixed Mobility	150–300 vehicles	10–20	96.9

6.5. Computation Cost

FD-LRP protocol is a protocol specially designed to reduce the computation overhead by offloading the heavy behavior analysis and cryptographic operations to the fog nodes. The average computing time of the suspicion score per vehicle which is calculated by the weighted aggregation of behavior indicators is 3.1 ms per 100 ms monitoring window. The revocation list creation, which includes the signing of the behavioral evidence, takes an additional 2.4 milliseconds, and consensus signatures verification and fog node tag verification is 1.1 milliseconds. The total revocation decision cycle per vehicle is less than 7 ms providing real-time response in high traffic 5G vehicular networks.

As shown in Fig. 4, compared to Zhang et al. [58] utilizing an attribute-based cryptographic scheme, the computational cost of FD-LRP is much cheaper. Zhang's scheme causes several encryption and decryption processes in confirming vehicle features and permissions, and its mean calculation time for a single interaction becomes 7.4 ms (over 2 times longer than FD-LRP). Ullah et al. [59] — it is conceptually lightweight and no CRL or fog-based scoring is actually used in the implementation, so there is no actual performance associated. Hence, FD-LRP provides the most efficient ratio of responsiveness and the consumption of resources among the three.

6.6. Communication Overhead

In terms of communication cost, FD-LRP leverages a decentralized, fog-to-fog consensus protocol that minimizes redundant broadcasts through intelligent coordination. Each revocation tag, including a digital signature and consensus certificate, is approximately 650 bytes. Given that revocation events occur at a moderate rate (e.g., 2–3 per minute in dense scenarios), the additional bandwidth consumed remains under 4.3% of the total regional vehicular bandwidth. Moreover, the consensus mechanism involves lightweight vote messages of 300 bytes per fog node, and decisions are typically

reached within 10 milliseconds, even across 5–10 collaborating nodes.

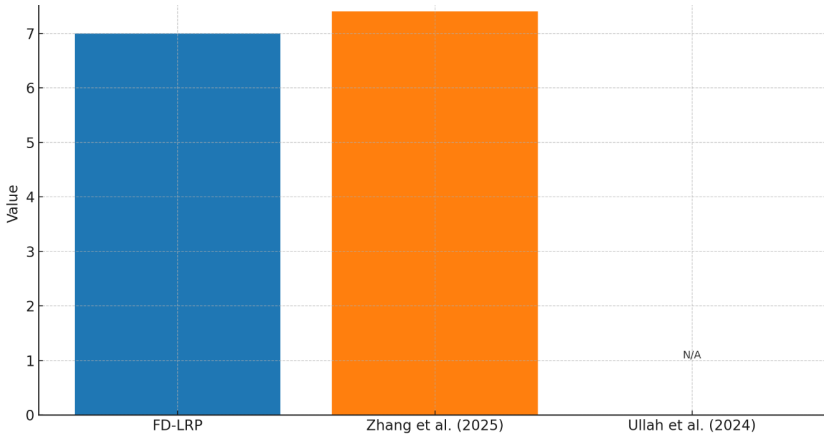

Fig. 4. Comparison of computation cost (ms))

As can be seen from Fig. 5, compared to Zhang et al.'s strategy [58] that is, which is based on centralized attribute verification, FD-LRP can achieve much lower communication overhead. In Zhang's solution, vehicles have to interact with the central servers or attribute authorities often, which incurs extra delay and bandwidth consumption. Ullah et al. [59] does not detail a revocation mechanism and, as such, omits consensus/tag propagation entirely, making it impossible to use in practice to help protect against Sybil under active misbehaviour. Through the fog-based design of FD-LRP, asynchronous consensus and selective propagation achieve efficient communication without sacrificing security.

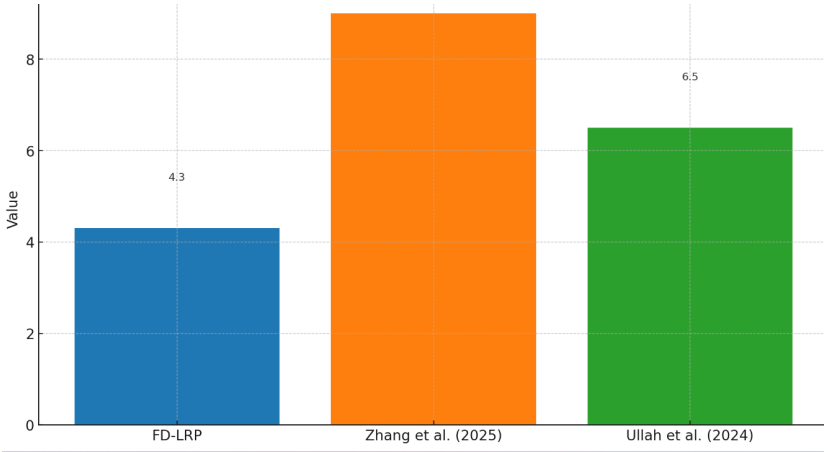

Fig. 5. Comparison of communication cost (bytes))

6.7. Storage Overhead

Storage size in FD-LRP is reduced by a Lightweight Certificate Revocation List (L-CRL), which maintains only hashed pseudonyms, timestamps, and pointers to consensus certificates. All L-CRL entry uses approximately 96 bytes in this manner, and the total list size will remain around only 34 KB even under a dense urban environment with high revocation rates, such as if 15% of vehicles, from a population size of 300, are revoked. By utilizing delta update techniques that only transmit newly revoked entries, the L-CRL is slender. OBUs keep the local CRL cache size to no more than 16 KB. This makes it feasible to conduct efficient hash-based message authentication without depleting in-vehicle memory budgets.

On the other hand, as indicated by Fig. 6, Zhang et al. [58] do not consider effective CRL management. Revocations are managed via complicated certificate checking, burdensome for OBUs in terms of storage and processing overheads. Their non-scalable CRL approach introduces an overhead that increases linearly with the number of users, which can be costly to low-end devices. Ullah et al. [59] provide a high-level model, but the CRL component is not present, so for comparison, it cannot be considered as realistically comparable in storage. In summary, FD-LRP's compact and hashed revocation infrastructure enables real-time enforcement, ensuring negligible memory overhead in comparison to the previous approach, offering a better alternative for 5G vehicular system deployments.

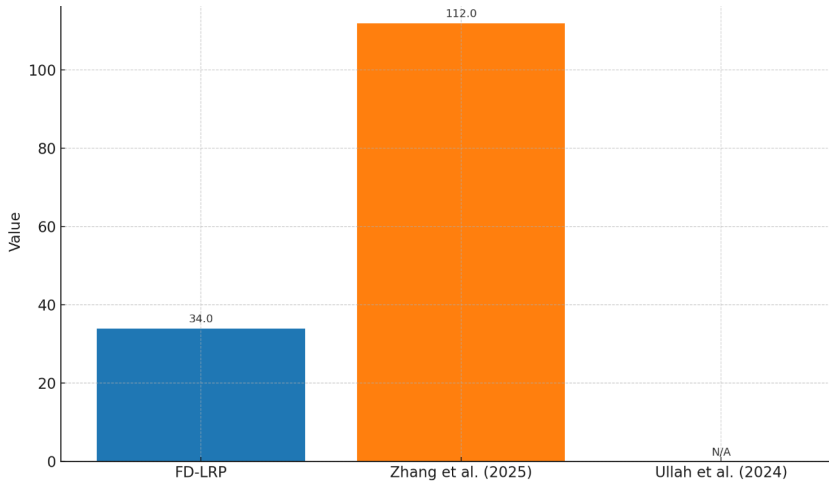

Fig. 6. Comparison of storage cost (ms))

6.8. Implications and Practical Considerations

The experimental results show that FD-LRP is applicable in practical 5G vehicular scenarios, especially for safety-critical applications with low-latency requirements such as the fast isolation of misbehaving vehicles. By migrating revocation intelligence to fog nodes, FD-LRP alleviates reliance on centralized infrastructure and supports timely decisions even in dense vehicle and high mobility scenarios.

With further regard to implementation, the low weight of FD-LRP allows it to incur minimum overhead in terms of computation and communication at vehicle on-board units, making it applicable with current vehicular hardware. The use of hashed pseudonyms, and delta- based revocation dissemination add to the scalability in dense urban environments without causing overly high traffic overhead.

The collaborative multi-fog consensus performs resilient against attacks and mitigates false alarms, yet being dependent on existing fog nodes. In low-infrastructure, intermittent connectivity areas, revocations may be delayed slightly, showing a distributed infrastructure vs. coverage trade-off. However, the non-blocking and timeout-centered design of the protocol keeps everything running even without system hanging.

Last, the assumption of a trusted authority for conditional traceability is in line with current vehicular security regulations and standards. In real-world deployment, FD-LRP can be deployed to complement current authentication services one step at a time, and is therefore feasible and deployable as a practical security enhancing solution for future vehicular networks with trust establishment functionality.

6.9. Discussion

Experimental results demonstrate the superiority of our FD-LRP protocol for the challenges of Sybil-resilient revocation in 5G-enabled vehicular networks over state-of-the-art schemes such as those introduced by Zhang et al. (2025) and Ullah et al. (2024). In the following, we analyze how to use the comparison results, which provide insights into three aspects: computation cost, communication overhead, and CRL storage efficiency.

FD-LRP has the minimum computation requirement and consumes only 7 ms in one revocation cycle, including the real-time scoring and cryptographic verification. This is due to its utilization of lightweight elliptic curve cryptography and local-based fog ingress computation. In contrast, Zhang et al. (2025) have a higher average delay of 7.4 ms, as it uses attribute-based encryption and centralised verification, which is complex and incurs cryptographic overhead. Ullah et al. (2024) lack computational implementation metrics and are still a theoretical framework without empirical validation. The low computational overhead of FD-LRP makes it well-suited for real-time vehicular scenarios where OBUs and fog nodes are resource-limited.

In terms of bandwidth overhead, the FD-LRP demonstrates attractive communication efficiency with an average overhead of no more than 4.3% of regional vehicular bandwidth (including revocation tag dissemination and consensus messages). Its decentralized consensus protocol allows selective lightweight CRL entries propagation. In contrast, Zhang et al. (2025) pose a 9.0% communications overhead from frequent communication with a centralised attribute authority and encrypted identity verification message passes. While Ullah et al. (2024) have a smaller overhead of 6.5%, however does not have a well-defined model for revocation, which results in an overly optimistic, and therefore less pragmatic communication model. Therefore, FD-LRP is the optimal trade-off choice in terms of its speed and communication reliability.

FD-LRP is compact in the sense that it uses an L-CRL of 96 bytes per revocation, and yields a peak CRL size of 34 KB when high-density vehicular traffic applies. Due to this compactness, we can obtain fast lookup and low memory usage in both OBUs and fog nodes. Zhang et al. (2025) and does not utilise a compact CRL. Keeping detailed vehicle certificate data for all revoked vehicles contributes significantly to the size of its bloated CRL at 112 KB, which in turn increases the memory footprints of nodes and incurs high validation response-time. Ullah et al. (2024) does not contain any CRL mechanism that can be compared in relation to this criterion. To mitigate the storage overhead of FD-LRP, the introduced hash-based pseudonym entries and delta updates kept in memory make it feasible for scalable data distribution in a high-mobility environment.

7. Conclusion and Future work

This article proposes the fog-based decentralized lightweight revocation protocol (FD-LRP) to counter Sybil attack in 5G VN. With two-level behaviour-driven misbehaviour detection mechanisms and collaborative multi-fog consensus, FD-LRP allows the real-time punishment of malicious vehicles and overcomes the scalability issues and latency limitations of centralised certificate-revocation systems. The presented sparse CRL (S-CRL) using hashed pseudonyms and delta updates is able to cut back communication and storage load, but still expose the revocation condition in a controlled way. Extensive simulation results show that FD-LRP has low degree of revocation latency, high accuracy (e.g., more than 96%) in Sybil detection, and lower false positive rates under different traffic loads and mobility profiles. FD-LRP achieves a good balance among security effectiveness, computational efficiency and practical deployability (especially for low latency vehicular scenarios) compared with some state-of-the- arts counterparts. However, as a drawback, FD-LRP requires semi-trusted fog nodes and a fully trusted authority for the sake of identity accountability. Even though these assumptions are in line with current vehicular security architectures, reducing the trust requirements even more is an

open issue.

Next steps will be aimed at the improvement of the suspicion score model, by applying hybrid or learning-aided methodologies keeping intact the explainability aspect and real-time constraints. Future directions consist in generalizing FD-LRP to sparse fog scenarios, studying robustness against massive-scale fog node collusion and testing it on real vehicular testbeds.

Author Contribution: All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.

Funding: This research received no external funding

Acknowledgment: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU260299).

Conflicts of Interest: The authors declare that they have no conflict of interest.

References

[1] M. Jamil, M. Farhan, F. Ullah and G. Srivastava, "A Lightweight Zero Trust Framework for Secure 5G VANET Vehicular Communication," in *IEEE Wireless Communications*, vol. 31, no. 6, pp. 136-141, 2024, https://doi.org/10.1109/MWC.015.2300418.

[2] F. Ellouze, G. Fersi, and M. Jmaiel, "Lightweight Blockchain-Based Access Control With Efficient Revocation for Fog-Enabled IoT," *Innovations in Systems and Software Engineering*, vol. 21, no. 2, pp. 355–379, 2025, https://doi.org/10.1007/s11334-025-00608-2.

[3] J. Park, S. Samarakoon, H. Shiri, M. K. Abdel-Aziz, T. Nishio, A. Elgabli, and M. Bennis, "Extreme ultra-reliable and low-latency communication," *Nature Electronics*, vol. 5, pp. 133–141, 2022, https://doi.org/10.1038/s41928-022-00728-8.

[4] 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," in *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 5, pp. 4795-4812, 2025, https://doi.org/10.1109/TDSC.2025.3553868.

[5] C. She, P. Popovski, and M. Bennis, *Ultra-Reliable and Low-Latency Communications (URLLC) Theory and Practice: Advances in 5G and Beyond*, John Wiley & Sons, 2023, https://doi.org/10.1002/9781119818366.

[6] A. Taneja, A. Alhudhaif, S. Alsubai and A. Alqahtani, "A Novel Multiple Access Scheme for 6G Assisted Massive Machine Type Communication," in *IEEE Access*, vol. 10, pp. 117638-117645, 2022, https://doi.org/10.1109/ACCESS.2022.3219989.

[7] A. Rathore, S. Mishra, V. Kaushik, S. S. Kolaventi, and V. K. Sonti, "Energy–Efficient Communication Protocols for Massive Machine-Type Communications (MMTC)," *National Journal of Antennas and Propagation*, vol. 7, no. 1, pp. 62–69, 2025, https://doi.org/10.31838/NJAP/07.01.10.

[8] A. Mamane, M. Fattah, M. El Ghazi, and M. El Bekkali, "5G Enhanced Mobile Broadband (EMBB): Evaluation of Scheduling Algorithms Performances for Time-Division Duplex Mode," *International Journal of Interactive Mobile Technologies*, vol. 16, no. 1, pp. 120-131, 2022, https://doi.org/10.3991/ijim.v16i01.25941.

[9] F. R. A. Al Harthi, A. Touzene, N. Alzidi, and F. Al Salti, "Context-Aware Enhanced Application-Specific Handover in 5G V2X Networks," *Electronics*, vol. 14, no. 7, p. 1382, 2025, https://doi.org/10.3390/electronics14071382.

[10] S. S. Sefati and S. Halunga, "Ultra-Reliability and Low-Latency Communications on the Internet of Things Based on 5G Network: Literature Review, Classification, and Future Research View," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 6, p. e4770, 2023, https://doi.org/10.1002/ett.4770.

[11] S. Hossain, S. M. Senouci, B. Brik, and A. Boualouache, "A Privacy-Preserving Self-Supervised Learning-Based Intrusion Detection System for 5G-V2X Networks," *Ad Hoc Networks*, vol. 166, p. 103674, 2025, https://doi.org/10.1016/j.adhoc.2024.103674.

[12] J. Zhang, H. Zhu, F. Wang, J. Zhao, Q. Xu, and H. Li, "Security and Privacy Threats to Federated Learning: Issues, Methods, and Challenges," *Security and Communication Networks*, vol. 2022, no. 1, p. 2886795, 2022, https://doi.org/10.1155/2022/2886795.

[13] 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, https://doi.org/10.1007/s42452-025-07201-z.

[14] F. He, T. Zhu, D. Ye, B. Liu, W. Zhou, and P. Yu, "The Emerged Security and Privacy of LLM Agent: A Survey with Case Studies," *ACM Computing Surveys*, vol. 58, no. 6, pp. 1–36, 2024, https://doi.org/10.1145/3773080.

[15] Z. Ghaleb Al-Mekhlafi *et al.*, "Coherent Taxonomy of Vehicular Ad Hoc Networks (VANETs) Enabled by Fog Computing: A Review," in *IEEE Sensors Journal*, vol. 24, no. 19, pp. 29575-29602, 2024, https://doi.org/10.1109/JSEN.2024.3436612.

[16] M. Alrajeh, M. Almaiah, and U. Mamodiya, "Cyber Risk Analysis and Security Practices in Industrial Manufacturing: Empirical Evidence and Literature Insights," *International Journal of Cybersecurity Engineering and Innovation*, vol. 2026, no. 1, 2026, https://journals.theitap.org/index.php/ijcei/article/view/8/9.

[17] S. Alsahaim, M. A. Almaiah, and R. B. Sulaiman, "Security Threats in Mobile Phones: Challenges, Countermeasures, and the Importance of User Awareness," *International Journal of Cybersecurity Engineering and Innovation*, vol. 2023, no. 1, pp. 3–19, 2023, https://journals.theitap.org/index.php/ijcei/article/view/1/3.

[18] M. S. Alghareeb, M. Almaiah, and Y. Badr, "Cyber security threats in wireless lan: A literature review," *International Journal of Cybersecurity Engineering and Innovation*, vol. 2024, no. 1, 2024, https://journals.theitap.org/index.php/ijcei/article/view/6/5.

[19] A. Alotaibi, H. Aldawghan, and M. H. Rahman, "IoT Security Concerns With Non-Fungible Tokens: A Review," *STAP Journal of Security Risk Management*, vol. 2026, no. 1, pp. 1–30, 2026, https://doi.org/10.63180/jsrm.thestap.2026.1.1.

[20] A. Ali, "Adaptive and Context-Aware Authentication Framework Using Edge AI and Blockchain in Future Vehicular Networks," *STAP Journal of Security Risk Management*, vol. 1, no. 1, pp. 45–56, 2024, https://doi.org/10.63180/jsrm.thestap.2024.1.3.

[21] M. M. Ashraf, S. Boudjit, S. Zeadally, N. E. H. Bahloul, and N. Bashir, "Integrating Unmanned Aerial Vehicles (UAVs) with Vehicular Ad-hoc NETworks (VANETs): Architectures, applications, opportunities," *Computer Networks*, vol. 255, p. 110873, 2024, https://doi.org/10.1016/j.comnet.2024.110873.

[22] R. Shahin, S. M. Saif, A. A. El-Moursy, H. M. Abbas, and S. M. Nassar, "Fog-ROCL: A Fog based RSU Optimum Configuration and Localization in VANETs," *Pervasive and Mobile Computing*, vol. 94, p. 101807, 2023, https://doi.org/10.1016/j.pmcj.2023.101807.

[23] B. A. Mohammed *et al.*, "Taxonomy-Based Lightweight Cryptographic Frameworks for Secure Industrial IoT: A Survey," in *IEEE Internet of Things Journal*, vol. 12, no. 20, pp. 43296-43316, 2025, https://doi.org/10.1109/JIOT.2025.3595649.

[24] H. Jiang, J. Zheng, and Y. He, "Securing VANETs with Decentralized Certificate Management: A Tangle-Based Approach," in *International Conference on Internet of Things, Communication and Intelligent Technology*, pp. 77–85, 2025, https://doi.org/10.1007/978-981-96-2767-7_8.

[25] M. K. I. Rahmani *et al.*, "Security in Optical Wireless Communication-Based Vehicular Ad Hoc Networks Using Signature and Certificate Revocation," *Journal of Nanoelectronics and Optoelectronics*, vol. 19, no. 1, pp. 112–119, 2024, https://doi.org/10.1166/jno.2024.3544.

[26] V. Kalmani, V. Jadhav, A. Alqutaish, and G. Alradwan, "Geometry-Aware Multi-View Malware Detection Using Gromov–wasserstein Fusion," *Journal of Cyber Security and Risk Auditing*, vol. 2026, no. 1, p. 20–37, 2026, https://doi.org/10.63180/jcsra.thestap.2026.1.2.

[27] K. Mhammed, "Cyber Intelligence & Moroccan National Security: What Strategy for Managing & Mitigating Cyber Threats Against Future Sporting Events," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, pp. 366–383, 2025, https://doi.org/10.63180/jcsra.thestap.2025.4.12.

[28] M. Ho, S. Ang, S. Huy, and M. Janarthanan, "MUMSPI: A Model for Usability Measurement of Single-Platform Interface for Multi-Tasking in Big Data Tools," *Jordanian Journal of Informatics and Computing*, vol. 2026, no. 1, p. 1–14, 2026, http://dx.doi.org/10.63180/jjic.thestap.2026.1.1.

[29] L. Wang *et al*., "Privacy-Preserving and Secure Distributed Data Sharing Scheme for VANETs," in *IEEE Transactions on Mobile Computing*, vol. 23, no. 12, pp. 13882-13897, 2024, https://doi.org/10.1109/TMC.2024.3441595.

[30] Y. Rajkumar and S. S. Kumar, "An elliptic curve cryptography based certificate-less signature aggregation scheme for efficient authentication in vehicular ad hoc networks," *Wireless Networks*, vol. 30, no. 1, pp. 335–362, 2024, https://dxoi.org/10.1007/s11276-023-03473-8.

[31] K. Bala, R. Upadhyay, S. R. Anwar, and G. Shrimal, "A blockchain-enabled, trust and location dependent - Privacy preserving system in VANET," *Measurement: Sensors*, vol. 30, p. 100892, 2023, https://doi.org/10.1016/j.measen.2023.100892.

[32] S. Azam, M. Bibi, R. Riaz, S. S. Rizvi, and S. J. Kwon, "Collaborative Learning Based Sybil Attack Detection in Vehicular AD-HOC Networks (VANETS)," *Sensors*, vol. 22, no. 18, p. 6934, 2022, https://doi.org/10.3390/s22186934.

[33] M. M. Hamdi, M. Dhafer, A. S. Mustafa, S. A. Rashid, A. J. Ahmed and A. M. Shantaf, "Effect Sybil attack on security Authentication Service in VANET," *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1-6, 2022, https://doi.org/10.1109/HORA55278.2022.9799810.

[34] L. Nkenyereye, L. Nkenyereye, Q. -V. Pham and J. Song, "Efficient RSU Selection Scheme for Fog-Based Vehicular Software-Defined Network," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 12126-12141, 2021, https://doi.org/10.1109/TVT.2021.3116811.

[35] M. M. Qasim, J. M. Altmemi, A. H. Abd Ali, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "Ca-Hbca: A Software Engineering Framework for Secure, Scalable, and Adaptive Healthcare Blockchain Systems," *Journal of Robotics and Control (JRC)*, vol. 6, no. 4, pp. 2052–2063, 2025, https://doi.org/10.18196/jrc.v6i4.26643.

[36] U. Maan and Y. Chaba, "Deep Q-network based fog node offloading strategy for 5G vehicular Adhoc Network," *Ad Hoc Networks*, vol. 120, p. 102565, 2021, https://doi.org/10.1016/j.adhoc.2021.102565.

[37] H. A. Ali *et al*., "A privacy-preserving framework for iot using behavior obfuscation and differential privacy in blockchain–cloud architectures," *Journal of Robotics and Control (JRC)*, vol. 6, no. 6, pp. 2613–2627, 2025, https://doi.org/10.18196/jrc.v6i6.27593.

[38] B. A. Shtayt, J. M. Altmemi, K. A. Abdullah, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "Lightweight lattice-based multi-domain authentication protocol with real-time revocation and aggregated verification for vehicular communication," *Journal of Robotics and Control (JRC)*, vol. 6, no. 5, pp. 2228–2238, 2025, https://doi.org/10.18196/jrc.v6i5.26644.

[39] A. Paranjothi and M. Atiquzzaman, "A statistical approach for enhancing security in VANETs with efficient rogue node detection using fog computing," *Digital Communications and Networks*, vol. 8, no. 5, pp. 814–824, 2022, https://doi.org/10.1016/j.dcan.2021.09.010.

[40] Q. I. Ali, "Realization of a Robust Fog-Based Green VANET Infrastructure," in *IEEE Systems Journal*, vol. 17, no. 2, pp. 2465-2476, 2023, https://doi.org/10.1109/JSYST.2022.3215845.

[41] H. Wan, Q. Wang, C. Ma, Y. Teng, J. Lin and D. Ye, "ESCORT: Efficient Status Check and Revocation Transparency for Linkage-Based Pseudonym Certificates in VANETs," *2023 IEEE Symposium on Computers and Communications (ISCC)*, pp. 1340-1343, 2023, https://doi.org/10.1109/ISCC58397.2023.10218118.

[42] C. BrijilalRuban and B. Paramasivan, "Energy Efficient Enhanced OLSR Routing Protocol Using Particle Swarm Optimization with Certificate Revocation Scheme for VANET," *Wireless Personal Communications*, vol. 121, no. 4, pp. 2589–2608, 2021, https://doi.org/10.1007/s11277-021-08838-w.

[43] V. K. Quy, A. Chehri, N. M. Quy, V. -H. Nguyen and N. T. Ban, "An Efficient Routing Algorithm for Self-Organizing Networks in 5G-Based Intelligent Transportation Systems," in *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1757-1765, 2024, https://doi.org/10.1109/TCE.2023.3329390.

[44] O. Jaupi and E. Spaho, "A Systematic Literature Review on Integrating VANETs, Vdtns, 5G, and IoT for Smart Cities: Current Approaches, Challenges, and Future Directions," *Journal of Transactions in Systems Engineering*, vol. 3, no. 3, pp. 420–448, 2025, https://doi.org/10.15157/JTSE.2025.3.3.420-448.

[45] P. V. Plotnikov, G. I. Tambovtsev and A. G. Vladyko, "Numerical Analysis of roadside Units Deployment Models in V2X Communication System," *2024 Systems of Signals Generating and Processing in the Field of on Board Communications*, pp. 1-5, 2024, https://doi.org/10.1109/IEEECONF60226.2024.10496720.

[46] R. Maruthamuthu, N. Patel, T. Yawanikha, S. Jayasree, Z. Alsalami and S. P. V. SubbaRao, "A Way to Design Fog Computing Model For 5G Network using Vanet," *2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 431-435, 2024, https://doi.org/10.1109/ICACITE60783.2024.10617287.

[47] M. Ehtisham *et al*., "Internet of Vehicles (IoV)-Based Task Scheduling Approach Using Fuzzy Logic Technique in Fog Computing Enables Vehicular Ad Hoc Network (VANET)," *Sensors*, vol. 24, no. 3, p. 874, 2024, https://doi.org/10.3390/s24030874.

[48] A. Devia, R. Kait, and V. Ranga, "A Novel Approach for Secure and Efficient Vanet Communication: Integrating Clustering, Curve Fitting, and Fog Computing," *International Journal of Performability Engineering*, vol. 20, no. 9, 2024, https://doi.org/10.23940/ijpe.24.09.p5.572580.

[49] K. Zhang, Y. Li, and L. Lu, "Privacy-Preserving Attribute-Based Keyword Search with Traceability and Revocation for Cloud-Assisted IoT," *security and communication Networks*, vol. 2021, no. 1, p. 9929663, 2021, https://doi.org/10.1155/2021/9929663.

[50] M. Yang, H. Wang and D. He, "Puncturable Attribute-Based Encryption From Lattices for Classified Document Sharing," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4028-4042, 2024, https://doi.org/10.1109/TIFS.2024.3374262.

[51] A. A. Almazroi, M. H. Alkinani, M. A. Al-Shareeda, M. A. Alqarni, A. A. Almazroey and T. Gaber, "FC-LSR: Fog Computing-Based Lightweight Sybil Resistant Scheme in 5G-Enabled Vehicular Networks," in *IEEE Access*, vol. 12, pp. 30101-30112, 2024, https://doi.org/10.1109/ACCESS.2024.3368393.

[52] D. R. Junaidi, M. Ma, and R. Su, "Secure Vehicular Platoon Management Against Sybil Attacks," *Sensors*, vol. 22, no. 22, p. 9000, 2022, https://doi.org/10.3390/s22229000.

[53] N. U. Sehar *et al*., "Blockchain Enabled Data Security in Vehicular Networks," *Scientific Reports*, vol. 13, no. 1, p. 4412, 2023, https://doi.org/10.1038/s41598-023-31442-w.

[54] N. Khatri, S. Lee, and S. Y. Nam, "Sybil Attack-Resistant Blockchain-Based Proof-of-Location Mechanism with Privacy Protection in VANET," *Sensors*, vol. 24, no. 24, p. 8140, 2024, https://doi.org/10.3390/s24248140.

[55] H. B. Tulay and C. E. Koksal, "Sybil Attack Detection Based on Signal Clustering in Vehicular Networks," in *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 2, pp. 753-765, 2024, https://doi.org/10.1109/TMLCN.2024.3410208.

[56] Y. Zhu *et al*., "Sybil Attacks Detection and Traceability Mechanism Based on Beacon Packets in Connected Automobile Vehicles," *Sensors*, vol. 24, no. 7, p. 2153, 2024, https://doi.org/10.3390/s24072153.

[57] H. Su, S. Dong and T. Zhang, "A Hybrid Blockchain-Based Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," in *IEEE Transactions on Vehicular Technology*, vol. 73, no. 11, pp. 17059-17072, 2024, https://doi.org/10.1109/TVT.2024.3424786.

[58] Z. Zhang, W. Huang, Y. Huang, Y. Liao, C. Wu and S. Zhou, "An Attribute-Based Pre-Authenticated Secure Communication Protocol Enabling Key Protection and Credential Online-Upgrading for 5G NR V2X," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 8, pp. 11325-11341, 2025, https://doi.org/10.1109/TITS.2025.3558978.

[59] I. Ullah, M. A. Khan, N. Kumar, A. M. Abdullah, A. A. AlSanad and F. Noor, "A Conditional Privacy Preserving Heterogeneous Signcryption Scheme for Internet of Vehicles," in *IEEE Transactions on Vehicular Technology*, vol. 72, no. 3, pp. 3989-3998, 2023, https://doi.org/10.1109/TVT.2022.3220041.

[60] M. S. M. AL-inizi and O. M. NSAIF, "Securing Vehicle-to-Vehicle Communications: VANet Challenges," *Babylonian Journal of Networking*, vol. 2023, pp. 105–111, 2023, https://doi.org/10.58496/BJN/2023/014.

[61] L. Wei *et al*., "On-Board Unit (OBU)-Supported Longitudinal Driving Behavior Monitoring Using Machine Learning Approaches," *Sensors*, vol. 23, no. 15, p. 6708, 2023, https://doi.org/10.3390/s23156708.

[62] C. S. Evangeline *et al*., "Design of On-Board Unit for Vehicular Applications," *2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN)*, pp. 1-6, 2023, https://doi.org/10.1109/ViTECoN58111.2023.10157654.

[63] R. Shahin, A. A. El-Moursy, S. M. Saif, H. M. Abbas and S. M. Nassar, "Fog Node Optimum Placement and Configuration Technique for VANETs," *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, pp. 1-6, 2021, https://doi.org/10.1109/ICCSPA49915.2021.9385710.

[64] M. A. Al-Shareeda, A. A. Obaid, and A. A. H. Almajid, "The Role of Artificial Intelligence in Bodybuilding: A Systematic Review of Applications, Challenges, and Future Prospects," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 16–26, 2025, https://thestap.blob.core.windows.net/jcsra/articles/published/1541934477313.pdf.

[65] Z. G. Al-Mekhlafi *et al*., "CLA-FC5G: A Certificateless Authentication Scheme Using Fog Computing for 5G-Assisted Vehicular Networks," in *IEEE Access*, vol. 12, pp. 141514-141527, 2024, https://doi.org/10.1109/ACCESS.2024.3466914.

[66] E. F. Cahyadi and M.-S. Hwang, "A Comprehensive Survey on Certificateless Aggregate Signature in Vehicular Ad Hoc Networks," *IETE Technical Review*, vol. 39, no. 6, pp. 1265–1276, 2022, https://doi.org/10.1080/02564602.2021.2017800.

[67] Q. Al-Na'amneh, M. Aljawarneh, A. S. Alhazaimeh, R. Hazaymih, and S. M. Shah, "Securing Trust: Rule-Based Defense Against On/off and Collusion Attacks in Cloud Environments," *STAP Journal of Security Risk Management*, vol. 2025, no. 1, p. 85–114, 2025, http://dx.doi.org/10.63180/jsrm.thestap.2025.1.5.

[68] S. Naskar, C. Brunetta, G. Hancke, T. Zhang and M. Gidlund, "A Scheme for Distributed Vehicle Authentication and Revocation in Decentralized VANETs," in *IEEE Access*, vol. 12, pp. 68648-68667, 2024, https://doi.org/10.1109/ACCESS.2024.3400530.

[69] D. Abu Laila, M. Aljawarneh, Q. Al-Na'amneh, and R. Bin Sulaiman, "Optimizing Intrusion Detection Systems Through Benchmarking of Ensemble Classifiers on Diverse Network Attacks," *STAP Journal of Security Risk Management*, vol. 2025, no. 1, p. 71–84, 2025, http://dx.doi.org/10.63180/jsrm.thestap.2025.1.4.

[70] M. Al-Marshoud, M. Sabir Kiraz, and A. H. Al-Bayatti, "Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions," *ACM Computing Surveys*, vol. 56, no. 10, pp. 1–39, 2024, https://doi.org/10.1145/3656166.

[71] T. T. Thanh Le and S. Moh, "Comprehensive Survey of Radio Resource Allocation Schemes for 5G V2X Communications," in *IEEE Access*, vol. 9, pp. 123117-123133, 2021, https://doi.org/10.1109/ACCESS.2021.3109894.

[72] Z. Shi and J. Liu, "Sparse Code Multiple Access Assisted Resource Allocation for 5G V2X Communications," in *IEEE Transactions on Communications*, vol. 70, no. 10, pp. 6661-6677, 2022, https://doi.org/10.1109/TCOMM.2022.3197605.

[73] M. A. Al-Shareeda, A. M. Ali, M. A. Hammoud, Z. H. M. Kazem, and M. A. Hussein, "Secure IoT-Based Real-Time Water Level Monitoring System Using ESP32 for Critical Infrastructure," *Journal of Cyber Security and Risk Auditin*, vol. 2025, no. 2, pp. 43–52, 2025, https://doi.org/10.63180/jcsra.thestap.2025.2.4.

[74] N. C. Velayudhan, A. Anitha, and M. Madanan, "Sybil Attack with RSU Detection and Location Privacy in Urban VANETs: An Efficient EPORP Technique," *Wireless Personal Communications*, vol. 122, no. 4, pp. 3573–3601, 2022, https://doi.org/10.1007/s11277-021-09102-x.

[75] K. Suganyadevi, K. Sanjay, S. Saran, P. R. Somansankara and B. Vishnuprasanth, "An Efficient Privacy Preserving Authentication with Insider Attack Resistance for VANET," *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pp. 1779-1785, 2023, https://doi.org/10.1109/ICECA58529.2023.10395024.

[76] S. A. Noman and T. Atkison, "Techniques to Overcome Network Attacks (Sybil Attack, Jamming Attack, Timing Attack) in VANET," in *Journal of The Colloquium for Information Systems Security Education*, vol. 10, no. 1, pp. 7–7, 2023, https://doi.org/10.53735/cisse.v10i1.174.

[77] V. Lode, K. Lasushe, and A. Pinapati, "Security in VANETs with Insider Attack Resistance and Signature Aggregation," in *International Conference on Advances in Data-driven Computing and Intelligent Systems*, pp. 499–512, 2023, https://doi.org/10.1007/978-981-99-9521-9_38.

[78] M. M. A. Al-shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and I. H. Hasbullah, "Security Schemes Based Conditional Privacy-Preserving in Vehicular Ad Hoc Networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, pp. 479–488, 2020, https://doi.org/10.11591/ijeecs.v21.i1.pp479-488.

[79] M. A. Al-Shareeda *et al*., "Chebyshev Polynomial-Based Scheme for Resisting Side-Channel Attacks in 5g-Enabled Vehicular Networks," *Applied Sciences*, vol. 12, no. 12, p. 5939, 2022, https://doi.org/10.3390/app12125939.

[80] Y. Zhou, Z. Wang, Z. Qiao, B. Yang and M. Zhang, "An Efficient and Provably Secure Identity Authentication Scheme for VANET," in *IEEE Internet of Things Journal*, vol. 10, no. 19, pp. 17170-17183, 2023, https://doi.org/10.1109/JIOT.2023.3273234.

[81] A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, and S. Manickam, "L-CPPA: Lattice-Based Conditional Privacy-Preserving Authentication Scheme for Fog Computing With 5G-Enabled Vehicular System," *Plos one*, vol. 18, no. 10, p. e0292690, 2023, https://doi.org/10.1371/journal.pone.0292690.

[82] M. A. Mimi, "Using Clustering Scheme: Prevent Reply Attack in Vehicular Ad-Hoc Networks (VANET)," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 7, pp. 2007–2014, 2022, https://doi.org/10.1080/09720529.2022.2133240.

[83] A. A. Almazroi *et al*., "FCA-VBN: Fog computing-based authentication scheme for 5G-assisted vehicular blockchain network," *Internet of Things*, vol. 25, p. 101096, 2024, https://doi.org/10.1016/j.iot.2024.101096.

[84] J. Sardana, S. Kumar, D. Kumar and K. Dutta, "Denial of Service (DoS) Attacks in SDN-Based VANETs: A Study," *2024 Eighth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pp. 669-677, 2024, https://doi.org/10.1109/PDGC64653.2024.10984030.

[85] K. V. Krishna and K. G. Reddy, "Classification of Distributed Denial of Service Attacks in VANET: A Survey," *Wireless Personal Communications*, vol. 132, no. 2, pp. 933–964, 2023, https://doi.org/10.1007/s11277-023-10643-6.

[86] H. J. Aldaghlawy and M. A. Al-Shareeda, "The Role of Simulating Digital Threats Through Interactive Theater Performances," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, pp. 276–286, 2025, https://doi.org/10.63180/jcsra.thestap.2025.4.7.

[87] R. Gopi *et al*., "Intelligent DoS Attack Detection with Congestion Control Technique for VANETs," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 141–156, 2022, http://dx.doi.org/10.32604/cmc.2022.023306.

[88] M. Adil, S. Midha, V. K. Srivastav and Kavita, "Detection and Prevention of DoS Attack in VANET Using Artificial Neural Network," *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, pp. 1-7, 2024, https://doi.org/10.1109/KHI-HTC60760.2024.10481899.

[89] M. Al Shareeda, A. Khalil and W. Fahs, "Towards the Optimization of Road Side Unit Placement Using Genetic Algorithm," *2018 International Arab Conference on Information Technology (ACIT)*, pp. 1-5, 2018, https://doi.org/10.1109/ACIT.2018.8672687.