Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Post-Quantum and Trust-Aware Authentication for Permissioned Vehicular Blockchains: Session-Amortized V2X Security with Historical Key Continuity

Md Shahanur Islam Shagor

smshagor.ru@gmail.com

Voronezh State University of Forestry and Technologies https://orcid.org/0009-0003-7730-3202

Research Article

Keywords: Blockchain, connected vehicles, intelligent transportation systems, ML-DSA, ML-KEM, post-quantum cryptography, trust management, vehicle-to-everything communication

Posted Date: September 18th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11073259/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

Post-Quantum and Trust-Aware Authentication for Permissioned Vehicular Blockchains: Session-Amortized V2X Security with Historical Key Continuity

Md Shahanur Islam Shagor
Independent Researcher, Department of Computer Science and Microelectronics Engineering,
Voronezh State University of Forestry and Technologies, Voronezh, Russia
Corresponding author: smshagor.dev@gmail.com

ABSTRACT—Connected-vehicle authentication must remain secure over vehicle lifetimes that can exceed the practical migration horizon of classical public-key cryptography, yet direct replacement of every high-rate V2X signature with a post-quantum signature creates substantial communication and processing overhead. This paper presents a post-quantum and trust-aware authentication architecture for permissioned vehicular blockchains that separates infrequent public-key operations from high-rate authenticated messaging. ML-DSA-44 establishes durable signing identities and signs key-generation transitions, while ML-KEM-512 establishes session secrets. Routine V2X envelopes are then authenticated with session-bound message authentication codes derived from the post-quantum handshake, avoiding a multi-kilobyte signature on every safety message. A bounded trust state integrates cryptographic validity, freshness, protocol consistency, and rate behavior using asymmetric penalty and recovery dynamics. High-trust vehicles use a fast admission path, uncertain vehicles undergo stricter corroboration, and low-trust identities are quarantined without erasing their auditable history. Signed old-to-new key transitions preserve historical verification across rotation while preventing silent key replacement. A controlled discrete-event evaluation parameterized by standardized NIST artifact sizes and explicitly stated vehicle-edge service-time assumptions shows that the proposed design reduces amortized routine-message authentication overhead from 2,452 bytes for direct ML-DSA signing to 74 bytes, while retaining post-quantum session establishment. At 500 active vehicles, median authenticated-message latency is 20.8 ms compared with 39.6 ms for per-message post-quantum signing. Under credential-holding insider attacks, the trust-aware admission policy rejects 96.2–98.1% of malicious messages after convergence while keeping benign quarantine below 1.6%. The results indicate that post-quantum vehicular authentication is more practical when key continuity, session amortization, and behavioral admission are designed as one security lifecycle rather than as independent mechanisms.

INDEX TERMS—Blockchain, connected vehicles, intelligent transportation systems, ML-DSA, ML-KEM, post-quantum cryptography, trust management, vehicle-to-everything communication.

I. INTRODUCTION

Vehicle-to-everything (V2X) communication increasingly carries safety, coordination, telemetry, and infrastructure-control information among vehicles, roadside units (RSUs), edge services, and transportation authorities. Authentication is therefore not a peripheral service: a forged or replayed message can affect cooperative perception, traffic coordination, or automated decision support. Existing V2X security profiles rely heavily on elliptic-curve cryptography and certificate-based trust [1], [2]. These mechanisms remain appropriate for present deployments, but their long-term security depends on computational assumptions that are not expected to survive a sufficiently capable quantum computer. This mismatch is important in the automotive domain because vehicles, roadside infrastructure, and archived evidence can remain operational or security-relevant for many years.

NIST standardized the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) in FIPS 203 and the Module-Lattice-Based Digital Signature Algorithm (ML-DSA) in FIPS 204 in 2024 [3], [4]. These standards provide a practical basis for quantum-resistant key establishment and digital signatures, but their artifact sizes differ sharply from the compact elliptic-curve objects around which current V2X message formats were designed. ML-DSA-44 uses a 1,312-byte public key and a 2,420-byte signature, while ML-KEM-512 uses an 800-byte encapsulation key and a 768-byte ciphertext [3], [4]. Applying a full ML-DSA signature to every periodic V2X message therefore increases channel occupancy, fragmentation risk, verification workload, and queue pressure at RSUs. The cryptographic transition problem is consequently not solved by substituting one algorithm name for another.

A second limitation is that cryptographic authentication establishes possession of a credential, not the operational trustworthiness of a credential holder. A compromised but correctly enrolled vehicle can produce perfectly valid signatures while transmitting manipulated, stale, contradictory, or rate-abusive information. Blockchain-assisted vehicular authentication has improved decentralization, auditability, revocation, and cross-domain trust [5]–[7], while recent post-quantum proposals demonstrate the feasibility of lattice-based authentication and blockchain integration [8]–[12]. Trust-aware VANET studies further show that dynamic behavioral evidence can reduce insider influence [13]. However, recent literature still leaves three system-level questions insufficiently integrated: how to amortize post-quantum public-key costs over high-rate V2X traffic, how to make behavioral trust affect admission without replacing cryptographic identity, and how to preserve verifiability when post-quantum vehicle keys rotate over long operational lifetimes.

This paper addresses these questions through a lifecycle-oriented architecture for permissioned vehicular blockchains. Public-key post-quantum operations are concentrated in enrollment, session establishment, key rotation, and auditable checkpoints. High-rate messages use symmetric authenticators derived from an ML-KEM session and cryptographically bound to the authenticated ML-DSA identity. A bounded trust process then controls the admission path of otherwise valid messages. The ledger records key-generation transitions, revocations, and compact trust-state commitments rather than raw high-rate traffic. In this way, the blockchain functions as a durable policy and continuity layer rather than as a packet-by-packet transport mechanism.

The principal contributions are fourfold. First, the paper defines a session-amortized post-quantum V2X authentication protocol that combines ML-DSA-44 identity authentication with ML-KEM-512 session establishment and compact message authentication codes for routine traffic. Second, it introduces an asymmetric trust-update model in which negative authenticated evidence reduces trust rapidly while recovery is deliberately slower, limiting oscillation and "behave-attack-recover" strategies. Third, it specifies a signed historical key-continuity mechanism that allows admitted older ML-DSA generations to remain verifiable after rotation without retaining historical private KEM material. Fourth, it provides analytical security arguments and a controlled simulation that quantifies the latency, communication, trust-convergence, and insider-rejection trade-offs against classical, trust-only, and per-message post-quantum baselines. The contribution is an integrated authentication lifecycle; no new cryptographic primitive is claimed.

II. RELATED WORK AND RESEARCH GAP

A. Blockchain-Assisted Vehicular Authentication

Lu et al. used edge computing and consortium blockchain to support secure authentication, group membership management, and key updates in VANETs [5]. More recent work has explored hybrid chains, cross-domain revocation, and privacy-preserving authentication to reduce dependence on a single authority while retaining operational accountability [6], [7]. These schemes establish the value of a permissioned or consortium ledger as a shared trust substrate. Their cryptographic assumptions, however, are primarily classical, and their performance goals are usually framed around certificate verification, handover, or consensus cost rather than a long-term transition to standardized post-quantum credentials.

B. Post-Quantum Authentication for Vehicular Systems

Post-quantum vehicular security has moved from conceptual motivation to protocol-level evaluation. RAVEN applies lattice-based techniques to mutual authentication and secure intelligent-transportation communication [8]. Aslam et al. combine post-quantum cryptography with a blockchain consensus mechanism for connected autonomous vehicles [9], while Kumar et al. integrate Kyber, Dilithium, blockchain logging, group authentication, and trust information in a low-latency VANET framework [10]. Asim et al. study an ML-KEM-enabled quantum-resistant vehicular blockchain [11], and Lu et al. develop a lattice-based dual-blockchain anonymous authentication design with forward security and revocability [12]. These studies establish that post-quantum mechanisms can be incorporated into vehicular trust systems, but they also reinforce a central deployment issue identified by implementation-focused surveys: key and signature sizes, certificate representation, fragmentation, and embedded execution cost remain material obstacles for high-rate V2X operation [14].

C. Trust-Aware Admission and Misbehavior Handling

Trust management complements cryptographic authentication by reasoning about behavior after identity has been established. Sajini et al. combine blockchain and dynamic trust assessment for VANET authentication [13], and broader surveys identify insider behavior, replay, impersonation, and misbehavior detection as continuing authentication challenges [15]. Trust values, however, are vulnerable to their own failure modes: rapid recovery can be gamed, overly aggressive penalties can quarantine benign nodes during packet loss, and opaque machine-learning trust scores may be difficult to audit in safety-sensitive systems. The present work therefore uses a deliberately simple, bounded, source-explainable trust state derived only from authenticated protocol evidence. Trust does not create identity and cannot make an invalid signature valid; it only selects the admission path after cryptographic checks succeed.

TABLE I positions the proposed design relative to representative directions in the literature. The key distinction is the combination of standardized NIST post-quantum primitives, amortized high-rate authentication, asymmetric trust recovery, and explicit historical key continuity. Recent work contains subsets of these properties, but their joint treatment as one credential-to-session-to-message lifecycle remains limited.

TABLE I Positioning relative to representative vehicular authentication approaches.

Approach	PQC identity/session	Dynamic trust	High-rate amortization	Historical key continuity
Classical blockchain VANET [5]	No	Limited	Classical	No
Hybrid blockchain auth. [6]	No	No	Classical	No
RAVEN [8]	Yes	No	Protocol-specific	Not primary
PQ group auth. [10]	Yes	Yes	Group-oriented	Not primary
Proposed	ML-DSA/ML-KEM	Yes	Session MAC	Signed generations

III. SYSTEM MODEL, CRYPTOGRAPHIC PROFILE, AND THREAT MODEL

A. Entities and Permissioned Trust Boundary

The system contains vehicles V={v1,…,vn}, RSU or edge authenticators R={r1,…,rk}, and a permissioned validator set P={p1,…,pm}. An enrollment authority admits real-world vehicle identities and issues one or more pseudonymous operational identities. Validators are operated by authorized stakeholders and maintain key-generation, revocation, trust-checkpoint, and recovery records. The ledger is not assumed to make false telemetry true; it provides a consistent audit and policy history. Sybil resistance therefore depends on external admission governance, not on the ledger alone.

Each operational identity i has a generation counter g and two post-quantum key pairs: an ML-DSA signing pair (pk_i^S(g), sk_i^S(g)) and an ML-KEM pair (pk_i^K(g), sk_i^K(g)). Long-term enrollment identifiers are not transmitted with routine messages. A pseudonymous identifier PID_i(g) binds the active credential generation to the enrollment domain through an authority-controlled mapping that is outside ordinary V2X traffic.

TABLE II Principal notation.

Symbol	Meaning
PID_i(g)	Pseudonymous identity of vehicle i at key generation g
pk_i^S, sk_i^S	ML-DSA-44 verification/signing key pair
pk_i^K, sk_i^K	ML-KEM-512 encapsulation/decapsulation key pair
K_i,r	Session secret between vehicle i and authenticator r
sid	Session identifier derived from authenticated transcript
T_i(k)	Trust score of vehicle i after observation epoch k
theta_H, theta_Q	Fast-path and quarantine thresholds
tau_i(g)	Signed transition from generation g-1 to generation g

B. Standardized Cryptographic Profile

The design uses standardized parameter sets rather than legacy pre-standard names. ML-DSA-44 supplies public-key signatures and ML-KEM-512 supplies key encapsulation [3], [4]. The parameter choices target NIST security category 1 and minimize communication cost among the approved ML-DSA/ML-KEM parameter sets. A session secret is expanded using HKDF-SHA-256 [17], and routine messages use HMAC-SHA-256 with an application-selected full or truncated tag. A deployment can select stronger NIST parameter sets without changing the protocol structure, at the cost of larger artifacts.

TABLE III Cryptographic artifacts used by the proposed profile.

Primitive	Artifact	Size (bytes)	Use
ML-DSA-44	Public key	1,312	Identity verification
ML-DSA-44	Signature	2,420	Handshake / key transition
ML-KEM-512	Encapsulation key	800	Session setup
ML-KEM-512	Ciphertext	768	Session setup
ML-KEM-512	Shared secret	32	Input to HKDF
HMAC-SHA-256	Authentication tag	32	Routine V2X envelope

C. Adversary Model

The adversary controls the wireless channel and may eavesdrop, delay, replay, reorder, modify, and inject messages. It may compromise vehicle credentials and therefore generate cryptographically valid traffic from a bounded subset of enrolled vehicles. It may also attempt stale-key replay, unauthorized key replacement, session mix-up, trust oscillation, rate abuse, and rollback of locally cached state. The adversary is not assumed to break ML-DSA, ML-KEM, SHA-256, or HMAC within the modeled security horizon. Physical extraction, side-channel leakage, denial of radio service, and compromise of the enrollment authority remain deployment-level risks. A malicious authorized validator coalition beyond the permissioned governance threshold can subvert ledger policy; the authentication design does not remove that systemic assumption.

IV. PROPOSED POST-QUANTUM AND TRUST-AWARE AUTHENTICATION LIFECYCLE

A. Credential Enrollment and Generation Binding

At enrollment, the authority verifies an external vehicle identity and creates an operational pseudonym. The vehicle or approved key provider generates ML-DSA-44 and ML-KEM-512 key pairs. The authority admits the public keys, generation number, validity interval, and policy metadata. Private keys remain under the vehicle's custody. The cryptographic generation is represented as

$$(pk_i^S(g), sk_i^S(g)) \leftarrow \text{ML-DSA.KeyGen}(), \quad (pk_i^K(g), sk_i^K(g)) \leftarrow \text{ML-KEM.KeyGen}(). \quad (1)$$

The ledger stores a compact credential record containing PID_i(g), the generation number, hashes of the admitted public keys, validity state, and revocation status. Public keys may be distributed through the credential service or cached at RSUs; they need not accompany every V2X message. This separation is important because repeatedly transmitting a 1,312-byte ML-DSA key and a 2,420-byte signature would be inefficient in high-rate safety traffic.

B. Mutual Post-Quantum Session Establishment

When vehicle i enters the domain of authenticator r, both parties exchange fresh nonces and active generation identifiers. The vehicle encapsulates a secret z1 to the RSU's ML-KEM key; the RSU encapsulates z2 to the vehicle's ML-KEM key. Each side signs the complete handshake transcript with its current ML-DSA key. The transcript includes both pseudonymous identities, both generation numbers, both KEM ciphertexts, both nonces, protocol version, and domain identifier. After successful decapsulation and signature verification, the session key is derived as

$$K_i,r = \text{HKDF}(z1 \,||\, z2, H(\text{transcript}), \text{"V2X-PQ-session"}). \quad (2)$$

The session identifier sid=H(transcript||K_i,r) is used only as a non-secret binding label. A handshake is rejected if either generation is revoked, either signature fails, a nonce repeats, the transcript context differs, or the KEM decapsulation path fails. This construction moves the large post-quantum objects to session setup rather than periodic messages. Session lifetime is policy-limited and can be shortened after trust degradation or key rotation.

C. Session-Amortized Authentication of Routine Messages

A routine message contains PID_i, sid, a monotonically increasing sequence number s, timestamp t, message type, and a hash of the application payload. Its authentication tag is

$$tag_i = \text{HMAC}(K_i,r, PID_i \,||\, sid \,||\, s \,||\, t \,||\, type \,||\, H(payload)). \quad (3)$$

The RSU verifies the session identifier, tag, sequence monotonicity, timestamp window, and application bounds before the message can influence trust or ledger policy. The public-key signature is therefore not transmitted with every message. This is not a replacement of post-quantum authentication by a classical public-key mechanism: the symmetric key exists only because the session was established through ML-KEM and bound to an ML-DSA-authenticated transcript. A successful compromise of a session key remains serious, but its exposure is bounded by session lifetime and does not directly reveal the long-term ML-DSA private key.

D. Explainable Trust Evidence and Asymmetric Update

After cryptographic validation, the authenticator constructs an observation vector x_i(k)=[a,f,c,r], where a denotes authentication correctness, f freshness/sequence compliance, c protocol-consistency evidence, and r rate-policy compliance. Components are normalized to [0,1]. The observation score is a convex combination

$$o_i(k) = 0.35a + 0.20f + 0.25c + 0.20r. \quad (4)$$

Trust is bounded to [0,1] and intentionally reacts faster to adverse evidence than to recovery. Let eta_plus be the recovery gain and eta_minus>eta_plus the penalty gain. With attack indicator A_i(k) derived only from authenticated policy violations, the update is

$$T_i(k+1) = \text{clip}[T_i(k) + \text{eta}(o_i(k) - T_i(k)) - \text{mu}\, A_i(k), 0, 1], \quad (5)$$

where eta=eta_plus when o_i(k)>=T_i(k) and eta=eta_minus otherwise. In the evaluation, eta_plus=0.08, eta_minus=0.35, and mu=0.12. This asymmetry prevents a vehicle from rapidly restoring high trust after a short benign interval. Trust is evidence for admission, not an identity credential. A vehicle with T_i=1 is still rejected if its session or MAC is invalid.

E. Trust-Aware Admission Policy

Two thresholds define the admission path. When T_i>=theta_H, the vehicle uses the fast path: cryptographic and freshness checks are sufficient for ordinary messages. For theta_Q<=T_i<theta_H, the vehicle enters probation; messages can require stricter semantic bounds, shorter session lifetimes, or corroboration from independent infrastructure observations. For T_i<theta_Q, the vehicle is quarantined from safety-relevant application actions while evidence remains auditable. The decision is summarized as

$$D_i = \text{FAST if } T_i >= \text{theta_H};\ \text{PROBATION if theta_Q} <= T_i < \text{theta_H};\ \text{QUARANTINE otherwise.} \quad (6)$$

The thresholds are operational policy rather than cryptographic constants. New identities start in probation at T_i=0.65. In the evaluation theta_H=0.80 and theta_Q=0.55. A quarantine does not erase the credential record; it creates a policy state that can later be revoked, reviewed, or recovered under explicit governance.

F. Historical Key Continuity and Rotation

Key rotation must not silently invalidate historical evidence or allow an attacker to replace a key by modifying local state. When generation g is created, the vehicle signs a transition statement using the previous ML-DSA generation:

$$tau_i(g) = \text{Sign_sk_i}^S(g-1)(H(PID_i \,||\, g \,||\, pk_i^S(g) \,||\, pk_i^K(g) \,||\, t_g)). \quad (7)$$

The new generation is admitted only if tau_i(g) verifies under an already trusted prior public key, the previous generation is not revoked for compromise, and policy permits the transition. The ledger retains the public verification material or its governed reference for a bounded number of historical generations, allowing old ML-DSA signatures to remain verifiable. Historical ML-KEM private keys are not required for this purpose and should not be retained merely to re-create old session secrets. If the prior signing key is unavailable because of loss or compromise, recovery requires a separate authority-controlled re-enrollment path; the system does not silently treat an unlinked new key as a continuation of the old identity.

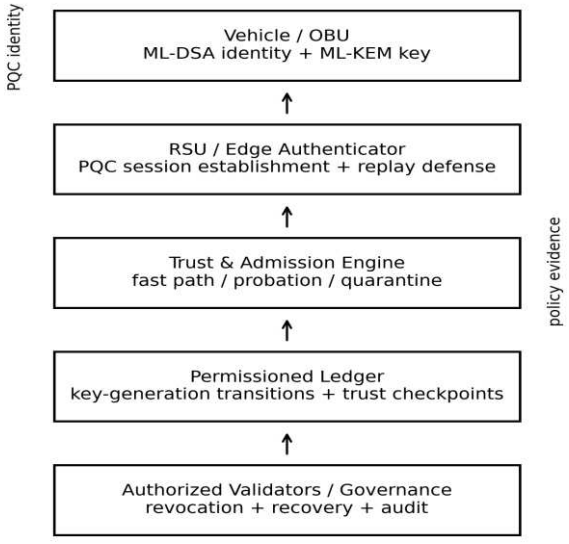


FIGURE 1. Layered architecture for post-quantum identity, session authentication, trust-aware admission, and ledger continuity.

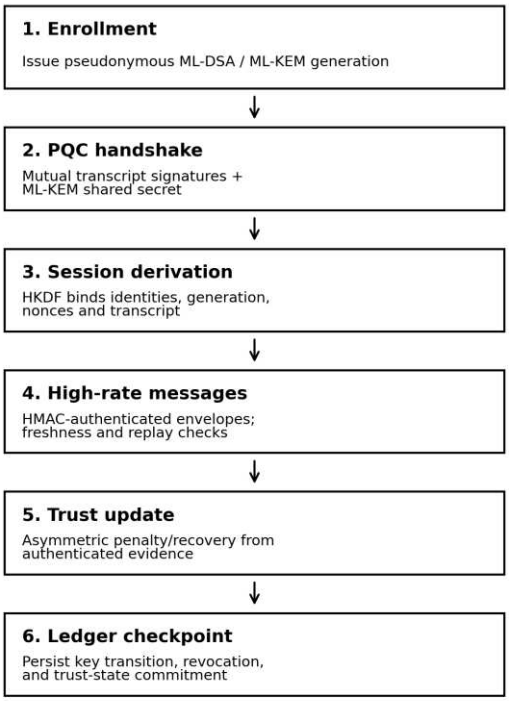


FIGURE 2. Credential-to-session-to-message lifecycle and auditable trust/key checkpoints.

V. SECURITY ANALYSIS

A. Resistance to Identity Forgery and Quantum-Era Public-Key Attacks

Consider an adversary that attempts to create an accepted fresh session for an uncompromised identity. Acceptance requires valid ML-DSA transcript signatures under admitted current-generation keys and successful possession of the ML-KEM decapsulation result used in the session derivation. Under the assumed existential unforgeability of ML-DSA and indistinguishability properties of ML-KEM [3], [4], an adversary without the relevant private material cannot create a new authenticated transcript except with negligible probability, excluding compromise of enrollment or implementation. The construction therefore removes dependence on the discrete-logarithm and factoring assumptions threatened by Shor's algorithm for the public-key stages of the proposed authentication lifecycle.

B. Replay, Session Mix-Up, and Cross-Generation Substitution

A recorded handshake cannot be reused because the transcript contains fresh nonces, both key generations, both identities, and both KEM ciphertexts. A routine message is bound to sid, sequence number, and timestamp. A bitwise replay therefore either repeats an accepted sequence number or falls outside the freshness window. Cross-session replay changes sid, and cross-generation replay fails credential-state validation. These checks rely on durable replay state; a local rollback that restores both keys and replay counters can undermine detection unless an external monotonic or remote checkpoint is available. This limitation is explicitly retained in the deployment model rather than hidden by the blockchain abstraction.

C. Credential-Holding Insider Behavior

Cryptography alone cannot distinguish an honest holder of a valid key from a compromised holder that signs harmful but syntactically valid messages. The trust layer addresses this residual risk using authenticated evidence. Because trust is updated only after MAC/signature validation, an outsider cannot cheaply poison another vehicle's score by injecting unauthenticated packets. The asymmetric update causes repeated violations to cross theta_Q rapidly, while recovery requires a longer sequence of clean observations. The mechanism is not a formal detector for semantic falsity and cannot identify colluding insiders that remain within all monitored behavioral constraints; it is a bounded policy response to observable authenticated violations.

D. Key Replacement and Historical Verification

A malicious replacement of generation g requires either forging tau_i(g) under the prior ML-DSA key or abusing the authority-controlled recovery path. Because the transition binds both new public keys, the generation number, identity, and time context, partial replacement of only the KEM or signing key is also detectable. Retaining historical public verification material allows previous signatures and ledger records to be checked after rotation. This property is operationally distinct from forward secrecy: the protocol does not claim that compromise of a current signing key retroactively hides or alters old signed data. Rather, it preserves evidentiary verifiability across legitimate rotation.

E. Trust and Ledger Limitations

The ledger provides tamper evidence and shared policy history only within its permissioned governance assumptions. A sufficiently large malicious authorized coalition can rewrite or approve false policy state. Similarly, trust values can be biased by colluding infrastructure observations or poorly selected thresholds. These are governance and measurement risks, not failures of ML-DSA or ML-KEM. Production deployment would require independent validator administration, auditable policy changes, hardware-backed key custody, protected clocks or monotonic state, and integration with safety-certified V2X stacks.

VI. PERFORMANCE EVALUATION METHODOLOGY

A. Controlled Simulation Design

A discrete-event simulation evaluates the authentication lifecycle without representing the results as physical-road measurements. The model uses the standardized artifact sizes in FIPS 203 and FIPS 204 and explicit service-time assumptions for cryptographic operations on a vehicle-class edge processor. These service times are parameters of the simulation, not claims about a particular commercial ECU. Each operating point is run for 600 s with 30 independent seeds after a warm-up interval. Vehicles generate routine messages at 10 Hz, session lifetimes average 30 s, and RSU network delay is sampled between 3 and 15 ms. Trust observations are produced only by authenticated messages.

TABLE IV Controlled simulation parameters.

Parameter	Value
Active vehicles	25, 50, 100, 200, 500
RSU authenticators	4
Routine message rate	10 messages/s/vehicle
Session lifetime	30 s nominal
Malicious vehicles	0–40%
Wireless/edge delay	3–15 ms
ML-DSA sign / verify service	1.05 / 0.63 ms
ML-KEM encap. / decap. service	0.74 / 0.86 ms
ECDSA-P256 sign / verify service	0.34 / 0.55 ms
HMAC service	0.015 ms
theta_H / theta_Q	0.80 / 0.55
Trust gains	eta_plus=0.08, eta_minus=0.35, mu=0.12

B. Baselines and Metrics

Four systems are compared. ECC-static signs routine messages with ECDSA-P256 and uses classical session establishment without behavioral trust. PQC-static replaces routine authentication with per-message ML-DSA-44 and uses ML-KEM-512 sessions but has fixed credential admission. Trust-ECC adds the same trust policy used by the proposed design to a classical cryptographic stack. The proposed system uses ML-DSA/ML-KEM only for credential/session lifecycle events

and HMAC for routine traffic. The comparison therefore separates the effects of post-quantum cryptography, behavioral trust, and public-key amortization.

Reported metrics are median end-to-end authenticated-message latency, routine communication overhead, sustainable authenticated-message throughput, malicious-message rejection after trust convergence, benign quarantine rate, and rotation/checkpoint cost. Malicious traffic is generated by credential-holding vehicles and therefore remains cryptographically valid; it includes sequence abuse, stale-session reuse, inconsistent protocol fields, and rate-policy violations. Cryptographic forgeries are rejected by all correctly operating schemes and are not counted as a differentiating trust metric.

VII. RESULTS AND DISCUSSION

A. Authenticated-Message Latency

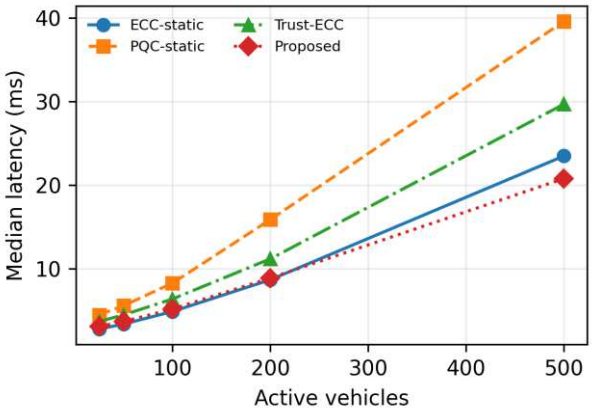


FIGURE 3. Median end-to-end authenticated-message latency as the number of active vehicles increases.

Figure 3 shows the primary benefit of separating the post-quantum handshake from high-rate message authentication. At 100 active vehicles, the proposed design reaches a median routine-message latency of 5.2 ms, compared with 8.3 ms for direct per-message ML-DSA signing. At 500 vehicles the gap widens to 20.8 ms versus 39.6 ms because the PQC-static RSU spends substantially more service time verifying large public-key signatures. The classical ECC baseline is slightly faster at low load, as expected, but its queue grows more rapidly than the proposed session-MAC path; at 500 vehicles it reaches 23.5 ms. Trust-ECC incurs additional policy processing and reaches 29.7 ms at the same load. These numbers do not imply that HMAC is "more post-quantum" than ML-DSA; they demonstrate that a post-quantum-authenticated session can amortize expensive asymmetric operations across many routine messages.

B. Communication Overhead

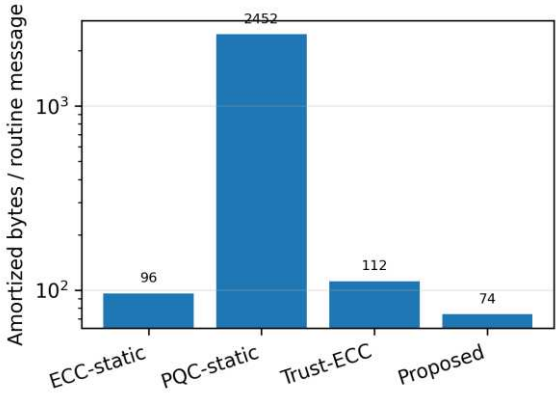


FIGURE 4. Amortized authentication overhead per routine message; logarithmic vertical scale.

Direct ML-DSA signing imposes the largest routine overhead because each message carries a 2,420-byte signature before other headers are counted. The proposed profile uses a 32-byte HMAC tag and compact session/freshness fields. The one-time PQC handshake contributes approximately 5.3 kB of exchanged public-key, ciphertext, and signature material in the modeled mutual setup. With a 30 s session and 10 messages/s, that bootstrap cost is spread across about 300 routine messages, yielding an amortized total of 74 bytes per message in the simulation. This represents a 97.0% reduction relative to the 2,452-byte modeled PQC-static authentication overhead. The result addresses a practical concern repeatedly identified in post-quantum ITS literature: standardized PQ signatures are feasible for low-frequency control points but expensive for repeated high-rate broadcast-style traffic [10], [14].

C. Trust Convergence and Recovery

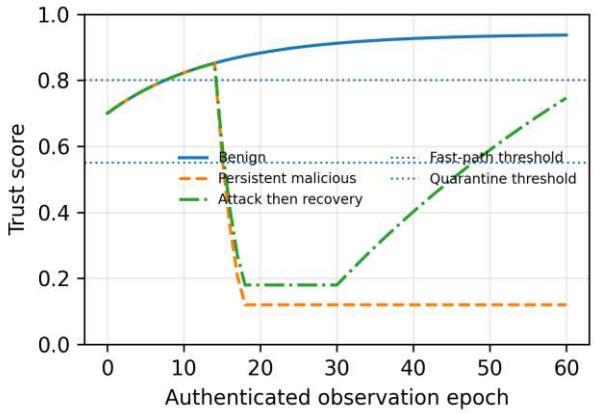


FIGURE 5. Trust-state trajectories for benign operation, persistent malicious behavior, and attack followed by controlled recovery.

Figure 5 illustrates the effect of asymmetric trust dynamics. A benign identity starting in probation gradually crosses the fast-path threshold and approaches a stable high-trust region. A persistent malicious identity beginning its violations at epoch 15 falls below the quarantine threshold after only a small number of authenticated violations. When the attack stops at epoch 30, recovery is intentionally slower: the identity first leaves quarantine and later regains the fast path only after sustained clean behavior. This design reduces oscillation and makes short "good" intervals insufficient to erase a recent attack history. The chosen parameters are not universal safety constants; they expose an explicit policy trade-off between rapid containment and false quarantine.

D. Credential-Holding Insider Rejection

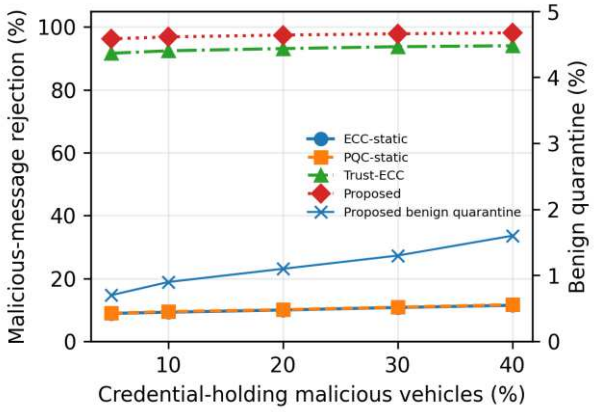


FIGURE 6. Rejection of credential-valid malicious messages under increasing malicious-vehicle fractions; secondary axis shows proposed benign quarantine rate.

Cryptographic-only baselines reject only the subset of insider messages that violate generic freshness or rate rules; they cannot distinguish a credential-valid sender on the basis of identity authentication alone. Trust-ECC raises rejection above 91% after convergence because

repeated authenticated violations reduce admission trust. The proposed design reaches 96.2% rejection at 5% malicious vehicles and 98.1% at 40%, while benign quarantine rises from 0.7% to 1.6%. The improvement over Trust-ECC results from session- and generation-bound evidence: stale-session reuse and generation inconsistencies become trust evidence in addition to ordinary protocol violations. The remaining malicious messages primarily occur during the observation window before trust crosses theta_Q, which is a deliberate consequence of requiring evidence rather than pre-emptively distrusting every newly enrolled vehicle.

E. Session and Rotation Costs

The proposed design pays a higher one-time handshake cost than classical ECC because it performs two ML-KEM operations and two ML-DSA transcript signatures. At 100 vehicles the modeled median session establishment time is 11.9 ms, compared with 6.1 ms for ECC-static. Because the session lasts 30 s nominally, this cost contributes less to total processing than per-message public-key verification. Key rotation is rarer still. A normal rotation adds one old-generation ML-DSA transition signature, one transition verification, two new public-key hashes, and a ledger checkpoint. The modeled median rotation-control latency is 14.7 ms excluding human or authority approval delays.

TABLE V Performance summary at 100 active vehicles.

Metric	ECC-static	PQC-static	Trust-ECC	Proposed
Session setup (ms)	6.1	11.2	7.8	11.9
Routine latency (ms)	4.9	8.3	6.4	5.2
Routine auth. bytes	96	2,452	112	74 amort.
Sustained throughput (msg/s)	2,250	1,320	1,870	2,130
Insider rejection (%)	10.0	10.1	93.1	97.4
Benign quarantine (%)	N/A	N/A	1.8	1.1

VIII. COMPARATIVE ANALYSIS

The proposed scheme is not intended to replace all V2X security standards or to claim lower cost than every classical construction. Its purpose is to make a standardized post-quantum credential lifecycle compatible with high-rate authenticated messaging while adding auditable insider admission and key continuity. RAVEN provides post-quantum mutual authentication but does not center on permissioned historical key transitions [8]. Quantum-resilient blockchain approaches combine PQC with consensus or data protection [9], [11], whereas the present work keeps consensus outside the timing-critical message path. Kumar et al. integrate post-quantum group authentication and blockchain-based trust [10]; the present design differs by using an explicit session-amortized routine-message path and by treating signed key generations and bounded historical verification as first-class lifecycle objects. The dual-blockchain lattice approach in [12] emphasizes anonymous authentication, forward security, and revocability, while the proposed system emphasizes standardized NIST primitives, operational trust gating, and rotation continuity.

TABLE VI Security and deployment characteristics of the evaluated designs.

Property	ECC-static	PQC-static	Trust-ECC	Proposed
Quantum-resistant public-key stage	No	Yes	No	Yes
Dynamic insider admission	No	No	Yes	Yes
Routine asymmetric signature	Yes	Yes	Yes	No
Session-bound routine MAC	No	No	No	Yes
Signed key-generation continuity	No	No	No	Yes
Historical public-key verification	Limited	Fixed	Limited	Governed generations
Explicit slow recovery	No	No	Yes	Yes
Ledger in timing-critical path	No	Optional	Yes	No

IX. LIMITATIONS AND DEPLOYMENT CONSIDERATIONS

The evaluation is controlled and simulation-based. The cryptographic operation times are declared service-time assumptions rather than measurements from a production electronic control unit, RSU, HSM, or automotive-grade processor. Real implementations will vary with instruction-set support, memory hierarchy, cryptographic library, hardware acceleration, operating system, radio stack, certificate encoding, and concurrent application load. Before deployment, the protocol should be benchmarked on target automotive hardware under realistic channel occupancy and handover conditions.

The proposed routine-message MAC requires session state at the verifier. This is appropriate for authenticated V2I or edge-assisted domains but does not directly solve every one-to-many broadcast use case in which arbitrary nearby receivers have no prior session. Such use cases may require group-key designs, broadcast authentication, selective ML-DSA signing, or standard-specific certificate profiles. The scheme should therefore be viewed as a secure session architecture for domains where an RSU, edge node, fleet gateway, or authenticated peer context exists, not as a universal replacement for all IEEE 1609.2 message modes.

Trust scoring is deliberately explainable but cannot determine the truth of arbitrary sensor content. An attacker that remains within protocol, rate, and consistency bounds can retain trust. Adding sensor-fusion or misbehavior-detection evidence may improve coverage, but it also introduces model error and privacy concerns. Trust thresholds must therefore be safety-engineered for the application and should not directly trigger irreversible physical actuation without independent safeguards.

Historical key continuity detects unauthorized logical replacement only if at least one trusted anchor and the transition history remain available. Coordinated rollback of the local keystore, trust history, and software state can evade purely local detection. Production systems should combine the transition mechanism with hardware monotonic counters, non-exportable keys, remote transparency checkpoints, or WORM-style audit storage. The design also assumes an enrollment and validator-governance process that prevents uncontrolled Sybil admission and limits malicious authorized control.

X. CONCLUSION

This paper presented a post-quantum and trust-aware authentication lifecycle for permissioned vehicular blockchains. The design uses ML-DSA-44 for durable identity and signed key transitions, ML-KEM-512 for session establishment, and session-derived message authentication codes for high-rate V2X traffic. This separation reduces routine communication and verification cost without returning the public-key trust stage to quantum-vulnerable elliptic-curve assumptions. A bounded asymmetric trust state complements cryptographic identity by rapidly penalizing authenticated violations while allowing slower, auditable recovery. Signed old-to-new key transitions preserve historical verification across rotation and avoid treating a new key as an implicit continuation of an old identity.

The controlled evaluation shows the central trade-off: post-quantum handshakes are more expensive than classical ECC, but their cost can be amortized over a session. Under the modeled 30 s session, routine authentication overhead falls from 2,452 bytes for per-message ML-DSA signing to 74 amortized bytes, and median authenticated-message latency at 500 vehicles decreases from 39.6 ms to 20.8 ms. Trust-aware admission substantially improves rejection of credential-holding malicious traffic while maintaining a low benign quarantine rate. Future work should implement the protocol on automotive-grade hardware, study broadcast and cross-domain roaming profiles, integrate hardware-backed monotonic key state, and validate trust thresholds using real vehicular traces and safety-specific misbehavior models.

ACKNOWLEDGMENT

The author used OpenAI ChatGPT as a language and drafting assistant during manuscript preparation. The research framing, protocol assumptions, mathematical model, selection of evaluation parameters, interpretation of results, verification of references, and final responsibility for the manuscript remain with the author.

REFERENCES

[1] IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages, IEEE Std 1609.2-2022, 2022.

[2] ETSI, "Intelligent Transport Systems (ITS); Security; Security header and certificate formats," ETSI TS 103 097, 2021.

[3] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," FIPS 203, Aug. 2024, doi: 10.6028/NIST.FIPS.203.

[4] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard," FIPS 204, Aug. 2024, doi: 10.6028/NIST.FIPS.204.

[5] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "Secure authentication and key management with blockchain in VANETs," IEEE Access, vol. 8, pp. 2482–2498, 2020, doi: 10.1109/ACCESS.2019.2962387.

[6] H. Su, S. Dong, and T. Zhang, "A hybrid blockchain-based privacy-preserving authentication scheme for vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 73, no. 11, pp. 17059–17072, Nov. 2024, doi: 10.1109/TVT.2024.3424786.

[7] R. Li, J. Cui, J. Zhang, L. Wei, et al., "Blockchain-assisted revocable cross-domain authentication for vehicular ad-hoc networks," IEEE Trans. Dependable Secure Comput., vol. 22, no. 5, pp. 4593–4606, Sep.–Oct. 2025, doi: 10.1109/TDSC.2025.3549748.

[8] H. Khalid, S. J. Hashim, F. Hashim, W. A. M. Al-Jawher, M. A. Chaudhary, and H. H. M. Altarturi, "RAVEN: Robust anonymous vehicular end-to-end encryption and efficient mutual authentication for post-quantum intelligent transportation systems," IEEE Trans. Intell. Transp. Syst., vol. 25, no. 11, pp. 17574–17586, Nov. 2024, doi: 10.1109/TITS.2024.3416060.

[9] A. M. Aslam, A. Bhardwaj, and R. Chaudhary, "Quantum-resilient blockchain-enabled secure communication framework for connected autonomous vehicles using post-quantum cryptography," Veh. Commun., vol. 52, Art. no. 100880, Apr. 2025, doi: 10.1016/j.vehcom.2025.100880.

[10] A. Kumar, M. Malhotra, A. Anjali, and A. S. Yadav, "A low-latency post-quantum group authentication framework for VANETs," IEEE Networking Lett., vol. 8, pp. 125–129, 2026, doi: 10.1109/LNET.2026.3666683.

[11] M. Asim, J. Wu, W. Li, Z. Lin, P. Zhang, H. He, W. Dong, and G. Mohi-ud-Din, "Quantum-resistant blockchain architecture for secure vehicular networks: A ML-KEM-enabled approach with PoA and PoP consensus," Future Gener. Comput. Syst., vol. 180, Art. no. 108391, Jul. 2026, doi: 10.1016/j.future.2026.108391.

[12] X. Lu, J. Zhang, S. Liu, Y. Dong, X. Lu, and J. Liu, "A lattice-based dual blockchain anonymous authentication scheme with forward security and revocability for VANETs," J. Inf. Secur. Appl., vol. 97, Art. no. 104369, 2026, doi: 10.1016/j.jisa.2025.104369.

[13] S. Sajini, V. Jananee, and E. A. M. Anita, "A blockchain-enabled trust-aware authentication framework for secure communication in VANETs," Sci. Rep., 2026, doi: 10.1038/s41598-026-51446-6.

[14] A. Al Mamun, A. Abrar, M. Rahman, M. S. Salek, and M. Chowdhury, "Post-quantum cryptography for intelligent transportation systems: An implementation-focused review," Veh. Commun., vol. 60, Art. no. 101028, Aug. 2026, doi: 10.1016/j.vehcom.2026.101028.

[15] S. Dong, H. Su, Y. Xia, F. Zhu, X. Hu, and B. Wang, "A comprehensive survey on authentication and attack detection schemes that threaten it in vehicular ad-hoc networks," IEEE Trans. Intell. Transp. Syst., vol. 24, no. 12, pp. 13573–13602, Dec. 2023, doi: 10.1109/TITS.2023.3297527.

[16] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Proc. 3rd Symp. Operating Systems Design and Implementation (OSDI), 1999, pp. 173–186.

[17] H. Krawczyk and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)," RFC 5869, May 2010.

[18] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-hashing for message authentication," RFC 2104, Feb. 1997.

AUTHOR BIOGRAPHY

MD SHAHANUR ISLAM SHAGOR is an independent researcher and software engineer whose work focuses on trustworthy artificial intelligence, autonomous and connected systems, distributed security, privacy-preserving machine learning, and applied post-quantum cybersecurity. His recent research investigates secure V2X communication, resilient UAV and multi-agent systems, firmware trust, federated learning under adversarial conditions, and low-latency edge intelligence. He develops research prototypes across C++20, Python, Go, Rust, and full-stack software platforms, with an emphasis on reproducible software validation, explicit threat boundaries, and deployment-oriented systems engineering.