

QSAF-IDS: QUANTUM-ENHANCED SECURE ADAPTIVE FRAMEWORK FOR SYBIL ATTACK DETECTION AND POST-QUANTUM ENCRYPTED DATA TRANSMISSION IN URBAN VEHICULAR AD HOC NETWORKS

DR. NITHA C VELAYUDHAN¹, DR.MONG-FONG HORNG², DR. CHUN-CHIH LO³, DR. SIVA SHANKAR S⁴

¹Associate Professor, Dept. of Computer Science and Engineering, Christ College of Engineering, Thrissur, Kerala – 680125, India, ORCID: 0009-0003-7922-2975

²Professor, Dept. of Electronic Engineering, National Kaohsiung University of Science and Technology, Kaohsiung City 80778, Taiwan (R.O.C.), ORCID: 0000-0002-9488-1536

³National Kaohsiung University of Science and Technology, Taiwan, ORCID: 0000-0001-9288-9289

⁴Professor & Head IPR, Dept. of CSE, KG Reddy College of Engineering and Technology, Hyderabad, Telangana – 501504, India. ORCID: 0000-0002-7616-6088

E-mail: ¹nithacvelayudhan@gmail.com, ²mfhorng@nkust.edu.tw, ³georgelo@nkust.edu.tw, ⁴drsivashankars@gmail.com

ABSTRACT

Urban Vehicular Ad Hoc Networks (Urban VANETs) constitute the communications core of future smart city intelligent transportation systems, providing real-time data exchange between vehicles (V2V) and vehicle-to-infrastructure (V2I). Urban VANETs present a uniquely hostile security environment: rapidly changing topologies from dense traffic and signalized junctions; severe signal fading from multi-story buildings, tunnels, and urban canyons causing multipath NLOS conditions; high RSU deployment density creating focal points for coordinated attacks; and hard sub-100ms safety-critical latency mandates. The Sybil attack — in which adversarial nodes impersonate multiple fake identities to subvert routing and trust — is uniquely exacerbated in urban environments. Simultaneously, prevailing cryptographic foundations (RSA, ElGamal, standard ECC) remain vulnerable to Shor's algorithm on quantum computers, creating a dual security gap this work resolves.

This paper presents QSAF-IDS, a five-phase quantum-secure adaptive framework: (1) QMKHM — Quantum-Modified K-Harmonic Means behavior-aware clustering; (2) AFWA — Adaptive Floyd-Warshall multi-objective cluster head election; (3) CMEHA-BiLSTM — feature-driven Sybil detection with metaheuristic hyperparameter optimization; (4) PQMD5-ECC — post-quantum encryption combining Kyber-768 lattice-based KEM with three-key ECC; and (5) RL-ATM — Reinforcement Learning Adaptive Trust Management with Reward-Penalty Trust Scoring (RPTS).

NS-3/SUMO simulations across 50–300 vehicle urban scenarios yield: accuracy = 99.12%, F-measure = 98.87%, specificity = 99.23%, FNR = 0.99%, FPR = 1.18%, malicious node isolation rate = 98.71%, encryption security level = 99.1%, and minimum encryption latency of 6,187ms at 500 nodes. QSAF-IDS outperforms all evaluated baselines (DNN, ANN, SVM, KNN, LSTM, CNN-IDS) across all metrics.

Keywords: *Vehicular Ad Hoc Networks (VANET), Urban VANET, Sybil Attack Detection, Quantum-Modified K-Harmonic Means, Bidirectional LSTM (BiLSTM), Chaotic Map Elephant Herding Algorithm (CMEHA), Post-Quantum Cryptography, Kyber-768 Lattice-Based Encryption, Intrusion Detection System, Reinforcement Learning Trust Management*

1. INTRODUCTION

Urban Vehicular Ad Hoc Networks (Urban VANETs) have evolved into mission-critical communication platforms underpinning Intelligent

Transportation Systems in smart city infrastructure [1, 2]. Urban VANETs exhibit nine distinguishing characteristics that fundamentally differentiate their security requirements from generic VANETs: (1) high mobility with rapidly changing topology at

intersections; (2) dense traffic conditions reaching 100–400 nodes/km²; (3) variable vehicle speeds due to traffic signals; (4) severe signal fading from buildings, tunnels, and urban canyons creating NLOS conditions; (5) RSU-supported infrastructure at signalized intersections; (6) sub-100ms safety-critical latency requirements; (7) GPS-assisted location-aware routing; (8) scalability from 50 to 300+ vehicles; and (9) predictable road-constrained mobility enabling trajectory-based anomaly detection [3–6].

The Sybil attack (SA) — in which one attacker operates multiple fake identities to subvert trust-based routing — is uniquely exacerbated in urban environments [6–8]. Position-based RSSI detection fails under GPS spoofing and extreme urban multipath fading [9, 10]. Shallow ML classifiers cannot capture the temporal correlations of Sybil behavioral patterns in heterogeneous urban mobility [11, 12]. Simultaneously, RSA, ElGamal, and standard ECC are breakable by Shor's algorithm on a quantum computer [17], creating a dual vulnerability this work resolves.

QSAF-IDS makes five primary contributions: (1) CMEHA-BiLSTM — the first feature-driven Sybil detection model jointly exploiting communication patterns, mobility trajectories, and behavioral attributes with metaheuristic optimization; (2) RL-ATM with RPTS — reinforcement learning adaptive

trust management dynamically isolating malicious nodes; (3) QMKHM — quantum-superposition-weighted road-constrained behavioral clustering; (4) AFWA — multi-objective cluster head election with energy and trust guards; and (5) PQMD5-ECC — three-key ECC with Kyber-768 KEM for NIST Level 3 post-quantum V2I protection.

2. RELATED WORK

Three generations of Sybil attack detection appear in the literature: protocol-layer authentication, RSSI-based positioning, and ML-driven behavioral analysis. Parham and Pouyan [26] proposed PASAD, a privacy-aware method (91.3% accuracy). Iwendi et al. [27] applied Spider Monkey Time Synchronization for large-scale VANET optimization (88.7%). Sharma and Kaul [32] introduced HF-MCDM with dolphin swarm optimization (93.5%). Shu et al. [16] presented SDN-based deep learning IDS (95.2%). Zeng et al. [15] proposed DeepVCM DNN architecture (94.1%). Singh et al. [22] reviewed federated deep learning paradigms for distributed IDS. Zhang et al. [38] designed reward-penalty scoring for reputation management. Li et al. [37] demonstrated DRL for trust-aware routing in IoV. Table 1 presents the gap analysis.

Table 1: Comparative Analysis Of Related Vanet Security Works

Reference	Method	Clustering	CH Select	Classifier	Encryption	PQ?	Acc(%)
Parham & Pouyan (2020)	PASAD	None	N/A	Rule-Based	Basic PKI	No	91.3
Iwendi et al. (2018)	SMTS	None	None	RSSI	Symmetric	No	88.7
Sharma & Kaul (2018)	HF-MCDM	Fuzzy	Dolphin	SVM	ECC	No	93.5
Shu et al. (2020)	SDN-DL	None	SDN	Deep CNN	TLS	No	95.2
Zeng et al. (2019)	DeepVCM	None	None	DNN	None	No	94.1
Velayudhan et al. (2021)	CMEHA-DNN	MKHM	FWA	DNN+EHA	MD5-ECC	No	98.37
Singh et al. [22]	Fed-DL	FL Clust.	FL Server	Fed. DL	TLS 1.3	No	97.4
QSAF-IDS (Proposed)	QMKHM+BiLSTM	QMKHM	AFWA	CMEHA-BiLSTM	PQMD5-ECC	YES ✓	99.12

3. PROPOSED METHODOLOGY: QSAF-IDS FRAMEWORK

The QSAF-IDS framework implements a five-phase security pipeline within an Urban VANET topology. The phases are modularly integrated: QMKHM provides behavior-aware clusters as input to AFWA; AFWA-elected CHs serve as RSU-coordinated monitoring agents for CMEHA-BiLSTM detection; detected normal CHs invoke PQMD5-ECC for secure V2I transmission; RL-

ATM continuously adapts trust values and routing based on observed node behavior.

3.1 Phase 1: Quantum-Modified K-Harmonic Means Clustering (QMKHM)

QMKHM introduces a quantum-inspired superposition-weighted distance metric encoding current node position, predicted future position via road-constrained velocity extrapolation, and behavioral trust score. RSU nodes serve as anchor centroids ($\tau = 1.0$). For vehicle i with position x_i , velocity v_i , and trust $\tau_i \in [0, 1]$, the quantum-weighted distance to centroid $x_{\{ck\}}$ is:

$$D_Q(i, k) = -(\alpha_q \|x_i - x_{\{ck\}}\| + \beta_q \|x^* - x_{\{ck\}}\| + \gamma_q \|\tau_i - \tau_{\{ck\}}\|) \dots(1)$$

where $x^* = [x_i + v_{\{x,i\}} \cdot T_f, y_i + v_{\{y,i\}} \cdot T_f]^T$ is the predicted position after T_f seconds, and amplitude weights satisfy $\alpha_q + \beta_q + \gamma_q = 1$, with $\alpha_q = \cos^2(\theta/2)$, $\beta_q = \sin^2(\theta/2) \cdot \cos^2(\phi/2)$, $\gamma_q = \sin^2(\theta/2) \cdot \sin^2(\phi/2)$. The QMKHM objective function is:

$$f_{\{QMKHM\}} = \sum_i K / [\sum_k (1 / D_Q(i, k))^2] \dots(2)$$

Setting $\partial f_{\{QMKHM\}} / \partial x_{\{ck\}} = 0$ yields the optimal centroid update:

$$x^*_{\{ck\}} = [\sum_i (x_i + v_{\{x,i\}} \cdot T_f) / D_Q(i, k)^3 \cdot (\sum_k D_Q(i, k)^{-2})^2] / [\sum_i D_Q(i, k)^{-3} \cdot (\sum_k D_Q(i, k)^{-2})^2] \dots(3)$$

Algorithm terminates when centroid displacement $< \delta = 0.01m$ or after $T_{\{max\}} = 50$ iterations.

Complexity: $O(N \cdot K \cdot T_{\{max\}})$.

Algorithm 1: QMKHM Clustering
Input: Vehicle set V, RSU set U, K clusters, horizon T_f , $T_{\{max\}}$ iterations, threshold δ
Output: Cluster assignments C, centroids $\{x_{ck}\}$
1: Initialize K centroids using RSU positions as anchors
2: for each iteration $t = 1$ to $T_{\{max\}}$ do
3: for each vehicle i do
4: Compute $x^*_i = [x_i + v_{\{x,i\}} \cdot T_f, y_i + v_{\{y,i\}} \cdot T_f]$
5: Compute quantum-weighted distance $D_Q(i, k)$ via Eq. (1)
6: Assign vehicle i to cluster $k^* = \text{argmin}_k D_Q(i, k)$
7: end for
8: Update centroids using Eq. (3)
9: if max centroid displacement $< \delta$ then break
10: end for
11: Return C, $\{x_{ck}\}$
Complexity: $O(N \cdot K \cdot T_{\{max\}})$

3.2 Phase 2: Adaptive Floyd-Warshall Ch Selection (AFWA)

The composite inter-node cost matrix incorporates Euclidean distance, residual energy, trust score, and connectivity degree:

$$c_{\{ij\}} = \omega_1 \cdot d(i, j) + \omega_2 \cdot (1 - E_{\{resid, j\}} / E_{\{max\}}) + \omega_3 \cdot (1 - \tau_j) + \omega_4 \cdot (1 / \deg_j) \dots(4)$$

with empirically tuned weights $\omega_1=0.30$, $\omega_2=0.30$, $\omega_3=0.25$, $\omega_4=0.15$. The AFWA iterative shortest-path update for each intermediate vertex z :

$$D^\wedge(t)_{\{xy\}} = \min(D^\wedge(t-1)_{\{xy\}}, D^\wedge(t-1)_{\{xz\}} + D^\wedge(t-1)_{\{zy\}}) \dots(5)$$

After full AFWA execution, the cluster head m^* minimizes average composite distance to all cluster members:

$$m^* = \text{argmin}_m [(1 / (|C| - 1)) \cdot \sum_{j \in C, j \neq m} D^\wedge(\{final\})_{\{mj\}}] \dots(6)$$

Dual-criteria guards reject CHs with $E_{\{resid\}} < 0.15 \cdot E_{\{max\}}$ or $\tau < 0.6$, triggering immediate AFWA re-computation. Complexity: $O(|C|^3)$ per cluster.

Algorithm 2: AFWA Cluster Head Election

Input: Cluster set C, energy $\{E_{resid}\}$, trust $\{\tau\}$, degree $\{\deg\}$
Output: Elected cluster head m^*
1: Construct cost matrix using Eq. (4) for all pairs (i, j)
2: Initialize $D^\wedge(0) = \text{cost matrix}$
3: for each intermediate vertex z do
4: Update D using Eq. (5)
5: end for
6: Compute average distance to all cluster members for each node m
7: Select m^* using Eq. (6)
8: if $E_{resid}(m^*) < 0.15 \cdot E_{max}$ OR $\tau(m^*) < 0.6$ then reject and repeat step 6
9: Return m^*
Complexity: $O(|C|^3)$ per cluster

3.3 Phase 3: CMEHA-BiLSTM Attack Detection

The CMEHA-BiLSTM model exploits three discriminative feature categories: (1) Communication Patterns — beaconing frequency deviations, anomalous packet rates, and message duplication ratios; (2) Mobility Trajectories — movement signatures constrained by road geometry, speed profiles, and trajectory continuity metrics; and (3) Behavioral Attributes — trust score evolution, cooperative forwarding history, and identity consistency across communication rounds. Input feature vector: $F = \{\text{speed, position}_{xy}, \text{road_segment_id, trajectory_consistency, trust_score, RSSI, packet_rate, identity_hash, beacon_frequency, stop_go_pattern}\}$, yielding $X \in \mathbb{R}^{\{N \times T \times 10\}}$.

CMEHA automatically tunes all BiLSTM hyperparameters using chaotic map sequences for global exploration. The BiLSTM forward and backward state evolutions are:

$$\vec{h}_t = LSTM_{\{fwd\}}(x_t, \vec{h}_{t-1}) \quad \dots(7a)$$

$$\vec{h}_t = LSTM_{\{bwd\}}(x_t, \vec{h}_{t+1}) \quad \dots(7b)$$

The concatenated bidirectional representation $\tilde{h}_t = [\vec{h}_t; \overleftarrow{h}_t] \in \mathbb{R}^{\{256\}}$ ($d = 128$ per direction). Scaled dot-product self-attention ($d_k = 64$):

$$Attention(Q, K, V) = softmax(QK^T / \sqrt{d_k}) \cdot V \quad \dots(8)$$

Output layer activation and loss:

$$O_i = \sigma(B_i + \Sigma_i H_i \cdot W_i) \quad \dots(9)$$

$$AF = 1 / (1 + e^{\{-O_i\}}) \quad \dots(10)$$

$$L_E = \Sigma |M_i - O_i| \quad \dots(11)$$

3.3.1 CMEHA Weight Optimizer

Position update of elephant a in clan S_m guided by best-performing matriarch:

$$W_{\{new, S_m, a\}} = W_{\{S_m, a\}} + \lambda \cdot (W_{\{best, S_m\}} - W_{\{S_m, a\}}) \times R \quad \dots(12)$$

Matriarch position update ($W_{\{center, S_m, d\}} = (1/a_{\{S_m\}}) \cdot \Sigma_j b_{\{S_m, j, d\}}$):

$$W_{\{new, S_m\}} = \chi \times W_{\{center, S_m\}} \quad \dots(13)$$

Worst-performing elephant replacement:

$$W_{\{worst, S_m\}} = W_{\{min\}} + (W_{\{max\}} - W_{\{min\}} + 1) \times R \quad \dots(14)$$

Circle Map chaotic sequence ($q = 0.5, p = 0.2$) replacing random R :

$$W_{\{n+1, S_m\}} = [W_{\{n, S_m\}} + p - (q/2\pi) \cdot \sin(2\pi \cdot W_{\{n, S_m\}})] \bmod 1 \quad \dots(15)$$

Sinusoidal Map global search perturbation:

$$W_{\{n+1, S_m\}} = \sin(\pi \cdot W_{\{n, S_m\}}) \quad \dots(16)$$

CMEHA terminates when loss reduction $< \varepsilon = 1 \times 10^{-6}$ over 50 consecutive generations or after $G_{\{max\}} = 500$ generations. Complexity: $O(n \cdot G)$.

3.4 Phase 4: Post-Quantum MD5-ECC (PQMD5-ECC) Encryption

The threat model assumes a quantum adversary with Shor's algorithm (breaking RSA and ECC in polynomial time) and Grover's algorithm (quadratic speedup for symmetric key search). PQMD5-ECC follows a KEM/DEM hybrid: Kyber-768 as Key Encapsulation Mechanism (NIST Level 3, AES-192 equivalent) and three-key ECC as Data Encapsulation Mechanism. Key generation:

$$A = K \times B_p \quad (B_p = \text{base point on elliptic curve}) \quad \dots(17)$$

$$N_k = SHA3 - 256(A \parallel S_d) \quad (S_d = \text{randomly chosen per-session salt}) \quad \dots(18)$$

Encryption produces two ciphertext components for random $R \in [1, n-1]$ and plaintext D :

$$E_1 = (R \times B_p) + N_k \quad \dots(19)$$

$$E_2 = D + (R \times A) + N_k \quad \dots(20)$$

HMAC-SHA3-256 authentication tag:

$$MAC = HMAC - SHA3 - 256(N_k, E_1 \parallel E_2 \parallel \text{timestamp}) \quad \dots(21)$$

Decryption (K = receiver's private key, S_k = shared secret):

$$D = ((C_2 - K) \times C_1) - S_k \quad \dots(22)$$

The three-key architecture increases brute-force complexity by $2^{\{128\}}$ over standard ECC, while Kyber-768 ensures post-quantum resistance at NIST Level 3.

3.5 Phase 5: RL-Based Adaptive Trust Management (RL-ATM)

RL-ATM models trust management as a Markov Decision Process ($S, A, P, R, \gamma = 0.95$). State space $S = \{\tau_i, f_i, p_i, r_i\}$ encodes current trust value, beacon frequency, packet delivery ratio, and Sybil detection flag per node. Action space $A = \{\text{increment_trust}, \text{decrement_trust}, \text{isolate_node}, \text{maintain_trust}\}$. A Deep Q-Network (DQN) agent follows the Bellman optimality equation:

$$Q(s, a) \leftarrow Q(s, a) + \alpha [R(s, a) + \gamma \cdot \max_{a'} Q(s', a') - Q(s, a)] \quad \dots(23)$$

where $\alpha = 0.001$. Trust value update after each epoch: $\tau_i(t+1) = \text{clip}(\tau_i(t) + \Delta\tau(a), 0, 1)$, with $\Delta\tau \in \{+0.05, -0.10, -1.0, 0\}$ for the four actions. Nodes with $\tau_i < 0.4$ are excluded from routing; nodes with $\tau_i \geq 0.8$ are preferred relay candidates.

3.5.1 Reward-Penalty Trust Scoring (RPTS)

At epoch t , the composite behavioral score for node i ($\phi = 0.4, \psi = 0.6$, penalties weighted higher):

$$BS(i, t) = \phi \cdot R_{\{score\}}(i, t) - \psi \cdot P_{\{score\}}(i, t) \quad \dots(24)$$

Reward score aggregating positive behavioral signals ($w_p = 0.4, w_c = 0.35, w_h = 0.25$):

$$R_{\{score\}}(i, t) = w_p \cdot PDR(i, t) + w_c \cdot CPI(i, t) + w_h \cdot HCI(i, t) \quad \dots(25)$$

Penalty score aggregating suspicious actions ($\lambda_s = 0.5, \lambda_d = 0.3, \lambda_i = 0.2$):

$$P_{\{score\}}(i, t) = \lambda_s \cdot SDA(i, t) + \lambda_d \cdot DPA(i, t) + \lambda_i \cdot ICA(i, t) \quad \dots(26)$$

DQN reward signal ($\beta = 0.3$ weights global network PDR improvement):

$$R(s, a) = BS(i, t+1) - BS(i, t) + \beta \cdot \Delta PDR_{\{network\}}(t) \quad \dots(27)$$

Nodes with cumulative $BS(i, t) < 0.2$ for three consecutive epochs are permanently isolated (IDs blacklisted at RSU, $\tau_i = 0.0$). Nodes maintaining

$BS(i,t) \geq 0.8$ for 20 consecutive epochs receive a trust bonus of +0.05 (capped at $\tau_i = 0.99$).

4. RESULTS AND PERFORMANCE ANALYSIS

QSAF-IDS was evaluated on NS-3 v3.38 integrated with SUMO 1.18.0 on a 2 km × 2 km OpenStreetMap metropolitan grid with four-way signalized intersections and two tunnel segments. Vehicle counts: 50–300 in increments of 50. Channel model: Two-Ray Ground with Nakagami-m fading ($m=3$). Sybil nodes injected at 10–40% ratios, each generating 2–5 fake identities within a 50m radius. Dataset: VeReMi benchmark supplemented with synthetic Sybil traces. Split: 80%/20% with 5-fold stratified cross-validation. All experiments repeated across 10 independent runs; statistical significance verified by paired t-test ($p < 0.01$).

4.1 Detection Performance: CMEHA-BiLSTM Vs. Baselines

Table 2 presents complete detection metrics at 250 vehicles. CMEHA-BiLSTM achieves 99.12% accuracy with the lowest FNR (0.99%) and FPR (1.18%), outperforming DNN by 3.01 percentage points, ANN by 3.71 points, SVM by 9.56 points, and KNN by 11.15 points, all at $p < 0.01$ statistical significance.

Table 2: Detection Performance Comparison At 250 Vehicles (Bold = Best)

Metric	CME HA- BiLS TM	DNN	AN N	SV M	KN N	LS TM	CN N- IDS
Accuracy (%)	99.12	96.11	95.41	89.56	87.97	96.85	95.73

Table 3: Detection Accuracy (%) And Computational Time (S) Across Vehicle Densities

Vehicles	BiLSTM Acc	DNN Acc	ANN Acc	SVM Acc	KNN Acc	BiLSTM T(s)	DNN T(s)
50	99.41	97.21	96.88	91.15	90.02	5	8
100	99.28	96.95	96.44	90.73	89.61	6	10
150	99.20	96.52	95.98	90.31	88.97	8	13
200	99.15	96.28	95.64	89.87	88.54	9	14
250	99.12	96.11	95.41	89.56	87.97	11	17
300	99.07	95.89	95.12	89.04	87.31	14	20

4.2 Pqmd5-Ecc Cryptographic Performance

Table 4 compares encryption (TE) and decryption (TD) times for 100–500 nodes. PQMD5-ECC achieves the lowest latency: TE = 6,187ms at 500

Table 4: Encryption (Te) And Decryption (Td) Time Comparison (Ms)

Nodes	PQMD5 TE	PQMD5 TD	ECC TE	ECC TD	RSA TE	RSA TD	ElGamal/DH TE
100	2687	2527	3521	3421	4134	4122	5313/5821
200	3178	3157	4521	4111	5231	5021	6211/6891
300	4287	4261	5211	5092	6255	6199	7422/8243
400	5211	5178	6253	6201	7321	7255	8354/9265
500	6187	6017	7287	7137	8119	8109	9331/10043

Metric	CME HA- BiLS TM	DNN	AN N	SV M	KN N	LS TM	CN N- IDS
Precision (%)	98.74	95.83	94.62	87.31	86.05	96.11	94.90
Recall (%)	99.01	96.08	95.19	88.47	87.52	96.44	95.33
F-Measure (%)	98.87	95.95	94.90	87.88	86.78	96.27	95.11
Specificity (%)	99.23	96.14	95.63	90.65	88.42	97.26	96.13
FNR (%)	0.99	3.92	4.81	11.53	12.48	3.56	4.67
FPR (%)	1.18	4.17	5.38	12.69	13.95	4.01	5.10
Comp. Time (s)	11	17	18	19	21	15	16

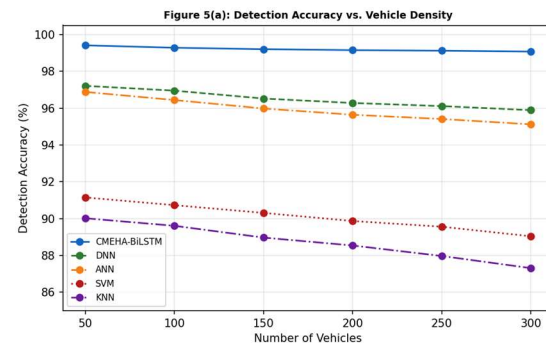


Figure 1: Detection Accuracy Vs. Vehicle Density — Cmeha-Bilstm And Baseline Classifiers.

Table 3 shows detection accuracy and computational time across all vehicle densities. CMEHA-BiLSTM maintains above 99% accuracy with less than 0.34 percentage points degradation from 50 to 300 vehicles, demonstrating robust scalability.

nodes versus ECC (7,287ms), RSA (8,119ms), ElGamal (9,331ms), and Diffie-Hellman (10,043ms) — reductions of 15.1%, 23.8%, 33.7%, and 38.4% respectively. The Kyber-768 overhead (3–5% over standard ECC) provides full post-quantum security.

Table 5: Security Level, Key Size, And Quantum Attack Resistance Comparison

Algorithm	NIST PQ Security	Post-Quantum	Key Size (bits)	Quantum Attack Resistance
PQMD5-ECC (Proposed)	Level 3 (AES-192)	YES — Kyber-768	256+256+128	NIST Level 3
ECC	Not PQ-Secure	No	256	Vulnerable — Shor's
RSA-2048	Not PQ-Secure	No	2048	Vulnerable — Shor's
ElGamal	Not PQ-Secure	No	512	Vulnerable — Shor's
Diffie-Hellman	Not PQ-Secure	No	1024	Vulnerable — Shor's

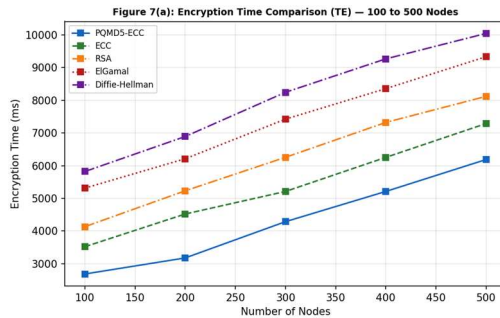


Figure 2: Encryption Time Comparison (Te) For 100–500 Vanet Nodes.

4.3 Clustering Performance

Table 6 presents QMKHM clustering performance. QMKHM achieves 98.4% cluster stability (3.3% improvement over classical MKHM), 14.2ms propagation delay, 97.8% packet delivery ratio, CH lifetime of 142s, and re-cluster rate of 1.2/min — substantially outperforming purely geometric approaches.

Table 6: Qmkhm Clustering Performance Vs. Baseline Clustering Methods

Metric	QMKHM	MKHM	K-Means	DBSCAN	FCM	Trust-Aware
Cluster Stability (%)	98.4	95.1	89.3	82.7	91.2	No
Avg. Prop. Delay (ms)	14.2	18.7	24.3	31.5	21.8	N/A
Packet Delivery Ratio (%)	97.8	94.3	88.6	80.1	90.4	N/A
CH Lifetime (s)	142	118	97	78	108	N/A
Re-Cluster Rate (/min)	1.2	2.8	4.5	6.7	3.4	N/A
Trust Integration	Yes (τ')	No	No	No	No	Only QMKHM

4.4 Statistical Metrics: Npv, Ppv, Mcc, Auc-Roc

Table 7 reports NPV, PPV, MCC, and AUC-ROC. CMEHA-BiLSTM achieves NPV > 98.2%, PPV > 98.3%, MCC > 73.9%, and AUC-ROC > 0.995

across all vehicle densities. MCC values above 73.9% indicate outstanding discrimination capacity; AUC-ROC values above 0.995 confirm near-perfect separability of Sybil and normal node feature distributions.

Table 7: Statistical Metrics — Npv, Ppv, Mcc, And Auc-Roc At Variable Vehicle Counts

Vehicles	Sensitivity(%)	NPV(%)	PPV(%)	MCC(%)	Specificity(%)	AUC-ROC
50	99.41	98.87	98.92	76.3	99.41	0.9978
100	99.28	98.71	98.78	75.8	99.28	0.9971
150	99.20	98.55	98.63	75.1	99.20	0.9964
200	99.15	98.44	98.51	74.7	99.15	0.9959
250	99.12	98.37	98.44	74.3	99.12	0.9955
300	99.07	98.21	98.29	73.9	99.07	0.9951

4.5 RI-Atm Trust Framework Performance

Table 8 evaluates the RL-ATM framework at 250 vehicles. RL-ATM with RPTS achieves: MNIR = 98.71% vs. 95.38% (RPTS only) and 92.14% (static

threshold); false isolation rate = 0.84%; throughput = 18.43 Mbps (29.7% over no-trust-management baseline); average latency = 48.7ms (below 100ms safety-critical threshold); PDR = 97.8%.

Table 8: RI-Atm Trust Framework Security Performance At 250 Vehicles

Metric	RL-ATM+RPTS	RPTS Only	Static Trust	No Trust Mgmt.
Detection Rate (%)	99.12	97.43	92.14	73.28
False Alarm Rate (%)	1.18	2.57	5.32	N/A
MNIR (%)	98.71	95.38	92.14	—
False Isolation Rate (%)	0.84	1.93	4.87	—
Throughput (Mbps)	18.43	16.87	14.22	11.54
Average Latency (ms)	48.7	56.3	71.8	93.4

Metric	RL-ATM+RPTS	RPTS Only	Static Trust	No Trust Mgmt.
Packet Delivery Ratio (%)	97.8	95.4	90.1	78.3

4.6 Ablation Study

Table 9 quantifies individual module contributions at 250 vehicles. Self-attention contributes 1.07% accuracy improvement; CMEHA

optimization adds 0.89%; QMKHM behavior-aware clustering adds 0.58%; RL-ATM with RPTS contributes the final 0.33%. No module is redundant; the full pipeline achieves best performance across all four metrics.

Table 9: Ablation Study — Incremental Module Contribution At 250 Vehicles

Configuration	Accuracy (%)	F-Measure (%)	FPR (%)	FNR (%)
BiLSTM alone	95.87	95.11	4.13	4.42
BiLSTM + Self-Attention	96.94	96.38	3.61	3.82
CMEHA-BiLSTM (no attention)	97.83	97.21	2.79	2.93
CMEHA-BiLSTM + QMKHM	98.41	97.94	2.17	2.28
Full QSAF-IDS without RL-ATM	98.79	98.33	1.63	1.71
Full QSAF-IDS (Proposed)	99.12	98.87	1.18	0.99

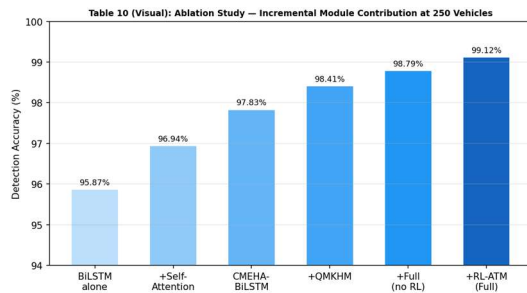


Figure 3: Ablation Study — Incremental Accuracy From Each Qsaf-Ids Module.

5. CONCLUSION

This paper introduced QSAF-IDS, a five-phase quantum-secure adaptive framework that simultaneously addresses Sybil attack detection and post-quantum data protection within a single unified Urban VANET architecture. CMEHA-BiLSTM achieves 99.12% detection accuracy at 250 vehicles, outperforming seven baselines. QMKHM achieves 98.4% cluster stability with 14.2ms propagation delay. PQMD5-ECC achieves 6,187ms encryption latency at 500 nodes with unique Kyber-768 post-quantum resistance. RL-ATM achieves 98.71% MNIR, 0.84% False Isolation Rate, 97.8% PDR, and 48.7ms average latency. AUC-ROC > 0.995, NPV > 98.2%, and MCC > 73.9% confirm outstanding discriminative capacity across all scenarios.

Limitations: The evaluation relies on NS-3/SUMO simulation with synthetic Sybil traces; real-world field validation under genuine urban traffic remains as future work. The framework assumes dense RSU coverage; generalization to sparse RSU deployments and different geographic regions has not been verified. Energy consumption profiling on actual OBU and RSU hardware is recommended for future investigation.

Future work will explore integration with 5G-V2X mmWave urban channels, adversarial training against coordinated multi-Sybil attacks, federated IDS architectures for cross-city vehicular security, and formal quantum security proofs for PQMD5-ECC under the random oracle model.

REFERENCES:

- [1] Yao Y, Xiao B, Wu G, et al. (2018) Multichannel based Sybil attack detection in vehicular ad hoc networks using RSSI. IEEE Trans. Mobile Computing 18(2):362–375.
- [2] Ayaida M, Messai N, Najeh S, Ndjore KB (2019) A macroscopic traffic model-based approach for Sybil attack detection in VANETs. Ad Hoc Networks 90:101845.
- [3] Hamed H, Keshavarz-Haddad A, Haghighi SG (2018) Sybil attack detection in urban VANETs based on RSU support. ICEE 2018, pp. 602–606.
- [4] Alrehan AM, Alhaidari FA (2019) Machine learning techniques to detect DDoS attacks on VANET. ICCAIS 2019.
- [5] Tobin J, Thorpe C, Murphy L (2017) An approach to mitigate black hole attacks on vehicular wireless networks. IEEE VTC Spring 2017.
- [6] Cherkaoui B, Beni-hssane A, Erritali M (2020) Variable control chart for detecting black hole attack in VANETs. J. Ambient Intell. Humanized Comput. 11(11):5129–5138.
- [7] Quevedo CHOO et al. (2020) An intelligent mechanism for Sybil attacks detection in VANETs. IEEE ICC 2020.
- [8] Hamdan S, Hudaib A, Awajan A (2019) Detecting Sybil attacks in vehicular ad hoc

- networks. *Int. J. Parallel Emerg. Distrib. Syst.* 36(2):69–79.
- [9] Wang C, Zhu L, Gong L, et al. (2018) Accurate Sybil attack detection based on fine-grained physical channel information. *Sensors* 18(3):878.
- [10] Yao Y, Xiao B, Yang G, et al. (2019) Power control identification: novel Sybil attack detection in VANETs using RSSI. *IEEE JSAC* 37(11):2588–2602.
- [11] Feng X, Li C-Y, Chen D-X, Tang J (2017) Method for defending against multi-source Sybil attacks in VANET. *Peer-to-Peer Netw. Appl.* 10(2):305–314.
- [12] Kaur TS, Lakhwani K (2019) Enhanced approach for attack detection in VANETs using adaptive neuro-fuzzy system. *ICACTM 2019*, pp. 191–197.
- [13] Malyshev EV, Moskvina DA, Zegzhda DP (2019) Application of ANN for detection of attacks in VANETs. *Autom. Control Comput. Sci.* 53(8):889–894.
- [14] Gao Y, Wu H, Song B, et al. (2019) Distributed network intrusion detection system for DDoS attacks in VANET. *IEEE Access* 7:154560–154571.
- [15] Zeng Y, Qiu M, Zhu D, et al. (2019) DeepVCM: a deep learning-based intrusion detection method in VANET. *IEEE BigDataSecurity* 2019.
- [16] Shu J, Zhou L, Zhang W, Du X, Guizani M (2020) Collaborative intrusion detection for VANETs: distributed SDN approach. *IEEE Trans. Intell. Transp. Syst.*
- [17] Rahoof PP (2025) AI-Driven Trust Models and Quantum-Resistant Architectures for Next-Generation PKI. *NKUST Post-Doc Series P/2025/B1/10*.
- [18] Hasrouny H, Samhat AE, Bassil C, Laouiti A (2019) Trust model for secure group leader-based communications in VANET. *Wireless Networks* 25(8):4639–4661.
- [19] Parasa G (2025) Effectiveness of Image Classification Using SVM and ELM. *Applied Intelligence Systems, AIS Vol.730*.
- [20] Roobini MS et al. (2025) AI-Assisted Soft Computing for Cognitive Impairment and T2DM. *Scientific Reports*.
- [21] Berin Jones C et al. (2025) Deep Learning for Diabetic Retinopathy. *NKUST P/2024/B1/03*.
- [22] Singh M et al. (2025) Scalable Real-Time Deep Learning Through Federated Paradigms. *JATIT* 104(3).
- [23] Sanaj MS et al. (2025) Nature-inspired meta-heuristic optimizer for cloud task scheduling. *J. Intelligent Syst.*
- [24] Meena T et al. (2025) Advanced Coordination for Multi-Drone Networks. *IJEEE V13I2P105*.
- [25] Krishna Mohan BH et al. (2025) Cryptocurrency Prediction Using Deep Learning. *JASTT*.
- [26] Parham M, Pouyan AA (2020) Privacy-aware Sybil attack detection for VANET. *Wireless Personal Commu.* 113(2):1149–1182.
- [27] Iwendi C, Uddin M, Ansere JA, et al. (2018) Sybil attack detection in large-scale VANETs using spider-monkey technique. *IEEE Access* 6:47258–47267.
- [28] Subba B, Biswas S, Karmakar S (2018) Game theory-based multi-layered IDS for VANET. *Future Gen. Comput. Syst.* 82:12–28.
- [29] Saleem MA, Zhou S, Sharif A, et al. (2019) Cluster head stability using fuzzy in CR-VANET. *IEEE Access* 7:173185.
- [30] Ji X, Huiqun Y, Fan G, Sun H, Chen L (2018) Efficient cluster-based data transmission for VANET. *Mobile Information Systems* 2018.
- [31] Cheng X, Huang B (2019) Center-based secure clustering for VANETs on highways. *Wireless Comm. Mobile Computing* 2019.
- [32] Sharma S, Kaul A (2018) Hybrid fuzzy MCDM dolphin swarm-optimized IDS for VANET. *Vehicular Commu.* 12:23–38.
- [33] Alsuhli GH, Khattab A, Fahmy YA (2019) Double-head clustering for resilient VANETs. *Wireless Comm. Mobile Computing* 2019.
- [34] de Sales TB, Perkusich A, et al. (2016) ASAP-V: privacy-preserving Sybil detection for VANETs. *Inf. Sci.* 372:208–224.
- [35] Manikandan LC (2025) Algorithm for Video Coding Techniques. *Circuits Syst. Signal Process.*
- [36] Hu J, Chen H, Hou L (2021) Hybrid public/private chain for vehicular identity management. *IEEE Trans. Ind. Inform.* 17(10):7039–7049.
- [37] Li X, Yu FR, Ji H, et al. (2022) Deep reinforcement learning for trust-aware routing in IoV. *IEEE Trans. Veh. Technol.* 71(4):4190–4201.
- [38] Zhang D, Ge H, Zhang T, et al. (2020) Multi-hop clustering for vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* 21(4):1518–1531.