International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 21s, 2025
https://theaspd.com/index.php

Quantum-Resilient Secure Context-Aware Trust-Based Routing with Preemptive Verifiable Key Handover for Vehicular Ad Hoc Networks

Anupama K N[1], Dr. R. Nagaraj[2]
[1]Research Scholar, Department of Computer Science, Kaamadhenu Arts and Science College, Sathyamangalam, Erode, Tamil Nadu, India, anupama.kn@gmail.com
[2]Associate Professor, Department of Computer Science, Kaamadhenu Arts and Science College, Sathyamangalam, Erode, Tamil Nadu, India

Abstract
Vehicular Ad Hoc Networks (VANETs) face unprecedented security challenges due to their dynamic topology, heterogeneous node capabilities, and vulnerability to quantum computing threats. Traditional trust-based routing protocols rely on classical cryptographic primitives that become obsolete in the post- quantum era, while context- awareness remains superficial in existing approaches. This paper presents a novel Quantum-Resilient Secure Context-Aware Trust-Based Routing with Preemptive Verifiable Key Handover (QR-SCTR-PVKH) protocol for VANETs that integrates lattice-based cryptography with multi- dimensional trust evaluation and proactive key management. Our approach incorporates direct trust computation based on packet delivery ratio, indirect trust propagation through witness testimonies, contextual trust adaptation considering traffic density and node mobility patterns, and historical trust evolution using temporal decay functions. The preemptive verifiable key handover mechanism employs Learning With Errors (LWE) problem-based key generation with forward secrecy guarantees and quantum-resistant signature schemes. Extensive simulations using SUMO-integrated NS-3 demonstrate 23.7% improvement in packet delivery ratio, 31.2% reduction in end-to-end delay, and 89.4% attack detection accuracy compared to state-of-the-art protocols. The protocol maintains IEEE 1609.2 compliance while ensuring GDPR compliance through privacy-preserving trust aggregation. Security analysis confirms resistance against quantum attacks, Sybil attacks, blackhole attacks, and replay attacks with computational overhead remaining within 15% of classical approaches.

Keywords: *Vehicular Ad Hoc Networks, Quantum-Resistant Cryptography, Context-Aware Trust, Lattice- Based Cryptography, Key Management, Post-Quantum Security, VANET Routing, Trust Propagation*

I. INTRODUCTION

A. Motivation and Background

Vehicular Ad Hoc Networks (VANETs) play a pivotal role in the future of Intelligent Transportation Systems (ITS), enabling seamless communication between vehicles (V2V) and between vehicles and roadside infrastructure (V2I). These networks aim to enhance road safety, automate traffic management, and improve the driving experience. However, their inherently dynamic structure—with fast-moving nodes, ever-changing network topologies, and variable connectivity—demands highly adaptive and secure routing strategies.

The earlier protocols for routing in VANETs tended to rely on physical distance and deal with geographical consideration without taking into account the trust metrics or the reputation of the nodes involved in the routing process. This gap gave rise to the trust-based routing protocols that incorporated some form of trust metrics or some form of behavior evaluation to make routing decisions. Despite this progress, many of these systems are still based on classical cryptographic methods (RSA, ECC) that are under the threat of quantum computing, particularly with the impact of Shor's or Grover's algorithms. In addition, the trust models that are used in VANETs still tend to be static and do not take into consideration surrounding contextual factors like traffic, signal noise, or even thepatterns of drivers behavior

B. Problem Statement and Challenges

As we approach the new quantum era of VANETs, it is crucial to sustain security and trust. The systems in place have not yet solved the following critical concerns.

1. Trust Computation Complexity: Current trust models don't present the complex spectrum of node trust as they should. They do not include direct experience, indirect recommendations, context related

variables, and they don't account for change over time which is a issue [8].
2. We are also seeing that present solutions pay attention to very basic context elements which mainly include mobility patterns they ignore traffic density, road conditions, communication interference which in turn greatly play a role in performance of the routing [9].
3. Lagged Key Management: Numerous systems implement a reactive, or post-handover, key management approach, leading to delays during critical shifting periods, exacerbating system vulnerabilities.
4. Limited Scalability: Strained operational effectiveness under high-load conditions is a challenge for exiting solutions as VANETs expand within congested metropolitan smart cities.
5. Compliance Barriers: Non-adherence to contemporary regulatory benchmarks like IEEE 1609.2, ISO 26262 or legal frameworks such as GDPR diminishes practical deployment prospects.

C. Problem Statement and Challenges

The present security in Vanets is a issue which has been brought forward by the introduction of quantum computing. What once was very secure with crypto algorithms such as RSA, ECC, and traditional hash functions we see now is not sufficient against quantum attack which is made possible by the Shor and Grover algorithms. Also because the road side and vehicle nodes in Vanet are out in the field for long periods of time which makes them a target for a wide range of attacks which are both constant and which change over time this issue is very much so a reality in the Vanet setting. Also in the trust based routing we see large scale issues which beyond the crypto issues which we are seeing. We put forth the main issues which are:

1. **Reductionist Trust Computation:** Current node trust models do not capture the entirety of the trustworthy behavior phenomenon. Trust, for example, how exchanges build or erode trust over time, remains static in node trust models. Judging trust by past interactions, third-party evaluations, or external observations is not incorporated in node trust models. The coherence of these models in dynamically changing network environments is unreliable.
2. **Limited Contextual Awareness:** Many routing protocols give preference to basic mobility metrics and position, ignoring more complex environmental processes. Wireless signal interference, traffic congestion, and even changing surface conditions on roads are overlooked.
3. **Key Management Inefficiency**: Reactive key management schemes cause significant delays during security updates, creating periods of vulnerability during handover processes [10].
4. **Scalability Concerns:** Current protocols struggle with scalability when used in crowded urban areas with thousands of vehicles participating [11].
5. **Compliance and Standardization:** The lack of adherence to emerging automotive security standards and privacy regulations creates obstacles to real-world deployment [12]. .

Research Contributions

In this document, the following major developments respond to the challenges noted:

1. Cryptography that is resilient to quantum computing: For the security of VANET, we employ lattice-based techniques, particularly the Learning With Errors (LWE) and Ring-LWE-based approaches.
2. Comprehensive Trust Management: Evaluation of the nodes in our trust model is done automately based on context-aware adaptations, reputation collaborations, personal transations, and trust over time using advanced algorithms.
3. Proactive Key Exchange: Our approach sets encrypted keys in anticipation of shifting network topologies, establishing them with forward secrecy, instead of waiting to respond after the shifts have happened.
4. Standards and Privacy Compliance: Compliance alongside privacy safeguards guarantees minimal leakage of personally identifiable information and the relevant protocols are designed around industry benchmarks including IEEE 1609.2 and GDPR.
5. High Efficiency: The model performance we propose is derived from smart trust metrics and optimized cryptographic algorithm application. These achieve efficiency in processing and ensure strong trust even when operating at an urban scale.

Paper Organization

This is the paper structure. In Section II we present a literature review of what is current in terms of trust based routing protocols and quantum resistant crypto techniques in VANETs. In Section III we put forth the system model and mathematical basis. We detail the put forth QR-SCTR-PVKH protocol architecture and algorithms in Section IV. In Section V we do formal verification and extensive security analysis. In Section VI we present comprehensive simulation results and performance evaluation. In Section VII we look at adherence to auto regulations and standards. In Section VIII we present in depth case studies of urban VANET settings. In Section IX we look at the limitations of our work and probe into future research directions. A summary of the key findings and their real-world applications is provided in Section X.

II. LITERATURE REVIEW

A. Trust-Based Routing in VANETs

One key strategy for improving the security and dependability of communication in VANETs is trust based routing. In the early days of this field simple trust estimation which looked at node performance in terms of packet forward and communication success was the primary focus. As time went on more complex models which included additional parameters into the trust evaluation were developed to over come the issues of the early models. A Kumar and Singh put forth a complex trust management system which also looked at social interaction between vehicles, mobility patterns and communication performance. This approach did see an improvement in routing accuracy but also ran into issues with scale which grew as the network did and in which we saw an increase in the amount of trust data. Also the protocol still had large scale vulnerabilities to coordinated malevolent attacks which in turn brought to light the need for more flexible and perceptive trust systems. In response to this we see scientists turn to machine learning (ML) methods for better VANET anomaly detection and trust inference. The case of Li et al. is a point of note which we put forth a deep learning based trust assessment model which they developed using Recurrent Neural Networks. In very dynamic vehicular settings this approach did prove to be effective in the detection of trust behavior changes. But what it lacked was real time application ability which it had in its heavy computation requirement. Also it required large amounts of labeled training data which in turn made it prone to hidden or changing attack patterns.. The interest in blockchain technology has surged recently as a decentralized trust management tool for vehicle ad-hoc networks (VANETs). A blockchain-based trust protocol proposed by Sharma et al. demonstrate secure storage and verification of trust-related data using distributed ledgers. This enhances security by ensuring transparency and preventing data tampering. On the other hand, the solution has drawbacks: the observable delays caused by the consensus processes required for blockchain operations as well as the required network operating energy, which raises concerns about.

B. Context-Awareness in VANET Routing

By which the field of VANETs has seen growth in that of intelligent and flexible decision making we have seen the application of context awareness in routing. In the early days of context aware routing protocols node speed and geographic location which were the main focus of basic mobility indicators did which in turn informed routing choices. Though at time successful which is to say that they did improve the picture they presented, these methods also had their short comings in that they did not in fact take into account the full spectrum of environmental and situational factors which play a role in network performance. Today we see a larger set of contextual variables which include traffic density, road conditions, vehicle behavior patterns, and wireless interference levels which modern routing algorithms process.The issue of improved accuracy and response in routing decisions is present in the use of these factors' which at the same time is also our challenge in that we are to implement into practice what we collect, interpret, and use in real time which in the case of vehicles is very hard to do as they have limited processing powerWhat we are also currently noticing is a shift towards the implementation of hybrid models that integrate context aware information and trust based systems. Aspatial frameworks are designed to create multi-layered routing protocols that assess the trustworthiness of a node as well as the context where the nodes are situated. Typcially, these systems are very useful, but they need to find the optimal efficiency balance of real-time responsiveness, low system resource computation, and ability to scale.

C. Cryptographic Security in VANETs

In the past vehicular ad hoc networks (VANET) have turned to traditional public key crypto techniques which included ECC and RSA for secure communication. Although these have done a good job at securing traditional computing they are proving to be inadequate against the new quantum computing

threats. Johnson et al. did a through analysis of the flaws in these traditional algorithms as used in VANETs which brought to light the urgent need to transition to quantum resistant alternatives. Early research tried to solve this by adapting well known post quantum crypto algorithms to the specific needs of vehicle networks. To illustrate, Brown and Lee have looked into hash-based signature schemes and reached the finding that although achievable, the real world implementation of quantum-safe authentication is challenging. The large size of the signatures and the high computational requirements, two primary concerns in resource-limited vehicular systems, is what worried them the most. Because of its strong security guarantees and fairly efficient operation, lattice-based cryptography has become very popular among the new post-quantum alternatives. Anderson et al. proposed a lattice-based key agreement protocol for vehicle-to-vehicle (V2V) communication and demonstrated its resistance to quantum attacks. Regardless of the potential of their approach, it was lacking in two important components for practical use: a comprehensive key management system and incorporation with trust-aware routing protocols. Building out from this framework which we present scholars have looked at the application of lattice based solutions in VANET settings. For example Chen et al. put forth a lattice based group signature which they used to develop a forward secure authentiction scheme. Also they achieved in this what they set out to do which was to present a quantum resistant solution at the same time make it a fit within current VANET standards thus at the same time making it more of a practical solution. But we do see a issue which is to date is preventing wide scale use which is computational over head in particular for the low power vehicle nodes. More recent work has looked into certificate less lattice based crypto techniques which they put forth as a solution to key management complexity. Also what Wu et al. presented was an optimized signature scheme which does away with the traditional issues of certificate issuance and validation. Their protocol that we have designed for VANET specific use cases reduces cryptographic overhead which in turn guarantees quantum resistance. But we still have questions regarding the scale of these systems in large scale deploys which require more empirical research.

D. Key Management in VANETs

Key management is very much a part of secure VANET communication which we at the same time find to be a great challenge in very large scale networks. We see constant changes in network topology which is a result of vehicle mobility as a reason many traditional methods do not work in real time..Historically, centralized key management has been the dominant approach, often relying on trusted Certificate Authorities (CAs) and periodic key renewal mechanisms . Although these techniques provide robust security and simple certificate validation, they significantly increase delays and hinder scalability in widespread implementations, particularly in cities with high vehicle congestion and unpredictable network connectivity. To address the problems posed by centralized systems, some researchers have suggested distributed frameworks for managing keys. An example of such an attempt is the work done by Thompson et al. in which they proposed a distributed key generation protocol based on secret sharing techniques. This approach enabled vehicles to work together to form cryptographic keys in a decentralized manner. The approach advanced network scalability and distributed trust, yet introduced other problems as well. In that which we see, we have added complexity in achieving that consensus and also we see the risk of coordinated attacks on key generating nodes which in turn degrades the robustness of the system. As of recent we have seen growth in pro active key management strategies. These put forth solutions which try to predict coming topology changes and in advance put in place secure communication lines which in turn minimize disruptions caused by hand over delays. For instance Garcia et al. developed a mobility aware key pre distribution scheme which uses prediction algorithms to go ahead and model vehicle movement. What they put forth did see success in that it reduced key handover latency which in turn made for a smoother transition. That said this work did not include elements of trust based routing or post quantum crypto which in turn limits its' play field in terms of future proofing VANE security against what is to come.

E. Quantum-Resistant Protocols for Wireless Networks

The development of post-quantum cryptographic protocols which are resistant to quantum enabled attacks has grown to accelerate as we see the growing threat of quantum computing. In wireless networks which include VANETs and which require that secure communication be maintained in dynamic and resource constrained environments this is very urgent. Early work in this area was put into developing what are essentially post- quantum crypto algorithms for wireless settings which included code based,

multivariate polynomial, and lattice based approaches. Each of these crypto families has its tradeoffs in terms of implementation complexity, key size and computational load. It is because of the balance it has between security and performance that lattice based cryptography has become the most practical solution for VANET applications.. The Learning With Errors (LWE) problem is a cornerstone of modern cryptography, offering strong protection even against future quantum computers. Approaches based on LWE form the backbone of secure encryption and digital signature systems, especially when high security can't come at the cost of speed or efficiency. Researchers like Chen and colleagues proved this by successfully running LWE-based security on low-power wireless devices, showing that quantum-resistant security doesn't have to slow things down.Ring-LWE, a refined version of LWE, has gained popularity in settings like connected cars. Thanks to its clever use of polynomial rings, Ring-LWE delivers faster computations—crucial for automotive networks where quick responses are essential. For instance, Kim and Park developed an authentication method using Ring-LWE tailored for vehicle networks (VANETs), achieving an ideal mix of speed, efficiency, and quantum-proof security.However, while Ring- LWE brings several advantages, current research—like that of Kim and Park—mainly focuses on verifying identities. There's still work to be done to fully integrate these quantum-resistant protocols with trust-based routing and comprehensive systems for managing cryptographic keys, which are vital for end-to-end security in vehicle networks.

F. Taxonomy and Comparative Analysis

We present a thorough taxonomy of current approaches and their attributes in order to give a thorough understanding of the current state of research. The salient characteristics and constraints of representative protocols from each category are enumerated in Table I.

Table I: Comparative Analysis of Existing VANET Security Protocols

Protocol	Trust Model	Context-Awareness	Cryptographic Approach	Key Management	Quantum Resistance	Scalability	Compliance
Zhang et al. [14]	Bayesian	Limited	ECC	Centralized	No	Medium	Partial
Kumar- Singh [15]	Multi-parameter	Basic mobility	RSA	Distributed	No	Low	No
Li et al. [16]	ML-based	Traffic patterns	AES	Reactive	No	Medium	Partial
Hassan et al. [18]	Basic	Geographic	ECC	Centralized	No	High	No
Wang et al. [19]	Trust-context	Environmental	RSA	Periodic	No	Medium	Partial
Martinez et al [20]	Crowdsourced	IoT-enhanced	ECC	Hybrid	No	High	GDPR
Brown- Lee [23]	None	None	Hash-based	Static	Yes	Low	No
Anderson et al [24]	None	None	Lattice-based	Pairwise	Yes	Medium	Partial
Thompso n et al [26]	Basic	None	ECC	Distributed	No	High	No
Garcia et al. [27]	None	Mobility	ECC	Proactive	No	Medium	Partial
Chen et al. [30]	None	None	LWE	Basic	Yes	Medium	No
Kim-Park [31]	None	None	Ring-LWE	Pairwise	Yes	High	Partial

A. Research Gaps and Limitations

The comprehensive literature review reveals several critical research gaps that motivate the development of our proposed protocol:

Lack of Integrated Approaches: Existing research has primarily focused on individual aspects of VANET security with limited integration between trust management, context-awareness, and quantum-resistant cryptography.

Insufficient Context Modeling: Current context-aware protocols consider limited environmental factors and fail to integrate contextual information with trust computation effectively.

Reactive Key Management: Most existing key management schemes operate reactively, introducing latency during security parameter updates and creating vulnerability windows.

Limited Quantum Resistance: While some protocols claim quantum resistance, few provide comprehensive

integration with routing mechanisms and practical deployment considerations.
Scalability Challenges: Many proposed solutions exhibit poor scalability characteristics when deployed in realistic large- scale urban environments.
Compliance Gaps: Limited attention has been paid to compliance with emerging automotive security standards and privacy regulations.
Evaluation Limitations: Most existing evaluations focus on limited metrics and fail to provide comprehensive security analysis under diverse attack scenarios.

III. Mathematical Foundations and System Model

A. Network Model

We consider a VANET consisting of a set of vehicles $V = \{v_1, v_2, ..., v_n\}$ operating within a geographical region R. Each vehicle v_i is equipped with wireless communication capabilities and maintains a unique identity ID_i. The network topology is represented as a dynamic graph $G(t) = (V(t), E(t))$, where V(t) represents the set of active vehicles at time t, and E(t) represents the set of communication links between vehicles within transmission range.
The communication model assumes that each vehicle has a transmission range R_{tx}, and two vehicles v_i and v_j can establish a direct communication link if their Euclidean distance $d(v_i, v_j) \leq R_{tx}$. The network topology changes dynamically due to vehicle mobility, with topology updates occurring at discrete time intervals Δt.

B. Mobility Model

Vehicle mobility is characterized by position vectors $p\square_i(t) = (x_i(t), y_i(t))$ and velocity vectors $v\square_i(t) = (v_{xi}(t), v_{yi}(t))$ for each vehicle v_i at time t. The mobility pattern follows realistic vehicular movement constraints, including road topology adherence, traffic signal compliance, and inter-vehicle spacing requirements.
The relative mobility between vehicles v_i and v_j is quantified using the relative velocity: $v\_rel(v_i, v_j, t) = ||v\square_i(t) - v\square_j(t)||$ (1)
Link stability between vehicles is estimated using the link lifetime prediction:
$LT(v_i, v_j, t) = (R_{tx} - d(v_i, v_j, t)) / v\_rel(v_i, v_j, t)$ (2)

C. Trust Model Foundation

Our trust model is built upon four fundamental components: direct trust, indirect trust, contextual trust, and historical trust. The overall trust value $T(v_i, v_j, t)$ between vehicles v_i and v_j at time t is computed as: $T(v_i, v_j, t) = \alpha_1 T\_direct(v_i, v_j, t) + \alpha_2 T\_indirect(v_i, v_j, t) + \alpha_3 T\_context(v_i, v_j, t) + \alpha_4 T\_history(v_i, v_j, t)$ (3)

IV. Proposed QR-SCTR-PVKH Protocol

A. Protocol Architecture Overview

The Quantum-Resilient Secure Context-Aware Trust-Based Routing with Preemptive Verifiable Key Handover (QR- SCTR-PVKH) protocol integrates four main components: (1) Multi-dimensional trust management, (2) Context- aware routing decision engine, (3) Quantum-resistant cryptographic layer, and
(4) Preemptive key handover mechanism. The protocol operates in a distributed manner where each vehicle maintains local trust tables, context information, and cryptographic keys while participating in collaborative routing decisions.

B. Trust Management Component

The trust management component implements the multi-dimensional trust model described in Section III-C. Each vehicle maintains a local trust table TT i that stores trust values for all encountered vehicles within a specified time window. The trust table entry for vehicle v_j observed by vehicle v_i contains: $TT\_i[v_j] = \{T\_direct, T\_indirect, T\_context, T\_history, timestamp, update\_count\}$

Trust updates occur periodically based on new observations and recommendations from trusted neighbors. The trust update process involves recalculating all trust components and aggregating them according to equation (3).
where $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1$ and $\alpha_i > 0$ for $i \in \{1, 2, 3, 4\}$.

1) Direct Trust Computation

Direct trust $T\_direct(v_i, v_j, t)$ is computed based on direct interactions between vehicles v_i and v_j. The direct trust evaluation considers packet delivery success rate, communication quality, and behavioral consistency:

$T\_direct(v_i, v_j, t) = \beta_1 PDR(v_i, v_j, t) + \beta_2 CQ(v_i, v_j, t) + \beta_3 BC(v_i, v_j, t)$ (4) where $\beta_1 + \beta_2 + \beta_3 = 1$.

The packet delivery ratio $PDR(v_i, v_j, t)$ is calculated as: $PDR(v_i, v_j, t) = N\_success(v_i, v_j, t) / N\_total(v_i, v_j, t)$ (5) where $N\_success(v_i, v_j, t)$ represents the number of successfully delivered packets and $N\_total(v_i, v_j, t)$ represents the total number of packets transmitted from v_i to v_j within the evaluation window.

Communication quality $CQ(v_i, v_j, t)$ incorporates signal strength, delay, and jitter measurements: $CQ(v_i, v_j, t) = \gamma_1 RSSI\_norm(v_i, v_j, t) + \gamma_2(1 - Delay\_norm(v_i, v_j, t)) + \gamma_3(1 - Jitter\_norm(v_i, v_j, t))$ (6) where $\gamma_1 + \gamma_2 + \gamma_3 = 1$ and normalized values range from 0 to 1.

Behavioral consistency $BC(v_i, v_j, t)$ measures the predictability and reliability of vehicle v_j's communication behavior: $BC(v_i, v_j, t) = \exp(-\sigma^2\_behavior(v_i, v_j, t))$ (7)

where $\sigma^2\_behavior$ represents the variance in communication behavior metrics over the evaluation window.

2) Indirect Trust Propagation

Indirect trust $T\_indirect(v_i, v_j, t)$ is computed based on recommendations from intermediate nodes that have direct experience with vehicle v_j. Let $W(v_i, t) = \{v_k \mid T\_direct(v_i, v_k, t) > \theta\_witness\}$ represent the set of witness nodes trusted by vehicle v_i, where $\theta\_witness$ is the minimum trust threshold for witness qualification.

$T\_indirect(v_i, v_j, t) = \Sigma(v_k \in W(v_i,t)) w(v_i, v_k, t) \times T\_direct(v_k, v_j, t) / \Sigma(v_k \in W(v_i,t)) w(v_i, v_k, t)$ (8)

The witness weight $w(v_i, v_k, t)$ is determined by the trustworthiness and relevance of witness v_k: $w(v_i, v_k, t) = T\_direct(v_i, v_k, t) \times \exp(-\delta_1 d(v_k, v_j, t)) \times \exp(-\delta_2 |t - t\_last(v_k, v_j)|)$ (9)

where δ_1 and δ_2 are decay parameters for distance and time relevance, respectively.

3) Contextual Trust Adaptation

Contextual trust $T\_context(v_i, v_j, t)$ adapts the trust evaluation based on environmental and situational factors that influence communication reliability. The contextual factors include traffic density, road conditions, weather conditions, and communication interference:

$T\_context(v_i, v_j, t) = \varepsilon_1 TD(v_i, v_j, t) + \varepsilon_2 RC(v_i, v_j, t) + \varepsilon_3 WC(v_i, v_j, t) + \varepsilon_4 CI(v_i, v_j, t)$ (10) where $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 = 1$.

Traffic density factor $TD(v_i, v_j, t)$ is computed based on the local vehicle density:

$TD(v_i, v_j, t) = \exp(-\lambda_1 \rho(v_i, t))$ (11)

where $\rho(v_i, t)$ represents the vehicle density within the communication range of vehicle v_i at time t, and λ_1 is a density impact parameter.

Road condition factor $RC(v_i, v_j, t)$ considers road surface quality and topology: $RC(v_i, v_j, t) = \zeta_1 RSQ(v_i, v_j, t) + \zeta_2 RT(v_i, v_j, t)$ (12)

where RSQ represents road surface quality and RT represents road topology complexity, with $\zeta_1 + \zeta_2 = 1$.

4) Historical Trust Evolution

Historical trust $T\_history(v_i, v_j, t)$ incorporates the temporal evolution of trust values using an exponential decay function: $T\_history(v_i, v_j, t) = \Sigma(k=0 \text{ to } H-1) \mu^k T(v_i, v_j, t-k\Delta t) / \Sigma(k=0 \text{ to } H-1) \mu^k$ (13)

where $\mu \in (0, 1)$ is the temporal decay factor, H is the history window size, and Δt is the time interval between trust evaluations.

C. Quantum-Resistant Cryptographic Framework

Our quantum-resistant cryptographic framework is based on lattice-based cryptography, specifically utilizing the Learning With Errors (LWE) problem and Ring-LWE variants for efficient implementation.

1) Learning With Errors Foundation

The LWE problem is defined over a finite field Z_q for a prime q. Given m samples (a_i, b_i) where $a_i \in$

Z_q^n is uniformly random and $b_i = \langle a_i, s \rangle + e_i \bmod q$ for a secret vector $s \in Z_q^n$ and small error terms e_i sampled from a discrete Gaussian distribution, the LWE problem requires finding the secret vector s. The security of our cryptographic framework relies on the hardness of the decisional LWE problem, which remains intractable even for quantum computers under current knowledge.

2) Key Generation Protocol

The key generation protocol utilizes the LWE problem structure for creating public-private key pairs. For each vehicle v_i, the key generation process involves:

1. Select a secret key $s_i \in Z_q^n$ sampled from a discrete Gaussian distribution χ_σ
2. Generate a random matrix $A_i \in Z_q^{(m \times n)}$ uniformly at random
3. Sample error vector $e_i \in Z_q^m$ from distribution χ_σ
4. Compute public key $PK_i = A_i s_i + e_i \bmod q$
5. Set private key $SK_i = s_i$

The public key PK_i is distributed to neighboring vehicles through authenticated channels, while the private key SK_i remains confidential to vehicle v_i.

3) Ring-LWE for Efficiency

To improve computational efficiency, we utilize Ring-LWE over polynomial rings $R_q = Z_q[x]/(x^n + 1)$ where n is a power of 2. The Ring-LWE problem maintains similar security guarantees while reducing key sizes and computational overhead.

For Ring-LWE based operations, polynomials are represented as $a(x) = \Sigma(i=0 \text{ to } n-1)\ a_i x_i$ where coefficients $a_i \in Z_q$. Multiplication operations are performed modulo $(x^n + 1)$, enabling efficient implementation using Number Theoretic Transform (NTT).

4) Signature Scheme

Our signature scheme is based on the Fiat-Shamir transform applied to a Ring-LWE identification protocol. For a message m, vehicle v_i with key pair (PK_i, SK_i) generates a signature $\sigma = (z, c)$ where:

1. Sample random polynomial y uniformly from R_q
2. Compute commitment $w = Ay \bmod q$
3. Generate challenge $c = H(w \,||\, m)$ using cryptographic hash function H
4. Compute response $z = y + c \times SK_i$
5. If $||z|| >$ bound B, restart the process
6. Output signature $\sigma = (z, c)$

Verification involves checking that $c = H(Az - c \times PK_i \,||\, m)$ and $||z|| \leq B$.

D. Context-Aware Routing Metrics

The context-aware routing component utilizes multiple metrics to evaluate path quality and select optimal forwarding decisions. The routing metric M(P, t) for path P at time t is computed as:

$M(P, t) = \eta_1 RT(P, t) + \eta_2 TS(P, t) + \eta_3 LC(P, t) + \eta_4 EC(P, t)$ (14)

where $\eta_1 + \eta_2 + \eta_3 + \eta_4 = 1$.

Route trust RT(P, t) represents the minimum trust value along path P: $RT(P, t) = \min\{T(v_i, v_j, t) \mid (v_i, v_j) \in P\}$ (15)

Route stability RS(P, t) considers the expected lifetime of links along the path: $RS(P, t) = \min\{LT(v_i, v_j, t) \mid (v_i, v_j) \in P\}$ (16)

Link capacity LC(P, t) estimates the available bandwidth along the path: $LC(P, t) = \min\{BW(v_i, v_j, t) \mid (v_i, v_j) \in P\}$ (17)

Energy consumption EC(P, t) considers the communication energy requirements: $EC(P, t) = \Sigma\{E\_tx(v_i, v_j, t) \mid (v_i, v_j) \in P\}$ (18)

Algorithm 1: Trust Update Procedure

Algorithm 1: UpdateTrust(vi, vj, observation_data, timestamp)

Input: Observer vehicle vi, target vehicle vj, observation data, current timestamp

Output: Updated trust value T(vi, vj, t)
1: BEGIN
2: // Compute direct trust component
3: PDR ← CalculatePDR(vi, vj, observation_data) 4: CQ ← CalculateCommunicationQuality(vi, vj, observation_data) 5: BC ← CalculateBehavioralConsistency(vi, vj, observation_data) 6: T_direct ← β_1 × PDR + β_2 × CQ + β_3 × BC
7:
8: // Collect indirect trust recommendations 9: witness_set ← GetTrustedWitnesses(vi, θ_witness) 10: T_indirect ← 0
11: total_weight ← 0
12: FOR each vk ∈ witness_set DO
13: weight ← CalculateWitnessWeight(vi, vk, vj, timestamp) 14: T_indirect ← T_indirect + weight × T_direct(vk, vj, timestamp) 15: total_weight ← total_weight + weight 16: END FOR
17: IF total_weight > 0 THEN 18: T_indirect ← T_indirect / total_weight 19: ELSE
20: T_indirect ← 0.5 // Default neutral value
21: END IF
22:
23: // Compute contextual trust
24: TD ← CalculateTrafficDensityFactor(vi, vj, timestamp)

REFERENCES

[1] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in Proc. IEEE World Forum Internet Things (WF-IoT), Seoul, South Korea, Mar. 2014,pp. 241-246.

[2] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," J. Netw. Comput. Appl., vol. 37, pp. 380-392, Jan. 2014.

[3] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey,"Veh. Commun., vol. 7, pp. 7-20, Jan. 2017.

[4] J. Zhang, "A survey on trust management for VANETs," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl. (AINA), Gwangiu, South Korea, Mar. 2013, pp. 105-112.

[5] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," Sensors, vol. 18, no. 11, p. 4040, Nov. 2018.

[6] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484-1509, Oct. 1997.

[7] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proc. 28th Annu. ACM Symp. Theory Comput., Philadelphia, PA, USA, May 1996, pp. 212-219.

[8] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," Int. J. Commun. Syst., vol. 26, no. 1, pp. 90-109, Jan. 2013.

[9] N. Kumar, S. Misra, and M. S. Obaidat, "Collaborative learning automata-based routing for rescue operations in dense urban regions using vehicular sensor networks," IEEE Syst. J., vol. 9, no. 3, pp. 1081- 1090, Sep. 2015.

[10] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the internet of drones: Challenges and solutions," IEEE Commun. Mag., vol. 56, no. 1, pp. 64-69, Jan. 2018.

[11] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen, "Secure intelligent traffic light control using fog computing," Future Gener. Comput. Syst., vol. 78, pp. 817-824, Jan. 2018.

[12] IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages, IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), pp. 1-240, Mar. 2016.

[13] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39- 68, Jan. 2007.

[14] J. Zhang, "Trust management for VANETs: Challenges, desired properties and future directions," Int. J. Distrib. Syst. Technol., vol. 3, no. 1, pp. 48-62, Jan. 2012.

[15] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs,"Comput. Electr. Eng., vol. 40, no. 6, pp. 1981-1996, Aug. 2014.

[16] W. Li, A. Joshi, and T. Finin, "CAST: Context-aware security and trust framework for mobile ad-hoc networks using policies," Distrib. Parallel Databases, vol. 31, no. 2, pp. 353-376, Jun. 2013.

[17] P. Sharma, A. Kumar, A. Gupta, and A. Nayyar, "A scalable blockchain based trust management inVANET routing protocol," J. Parallel Distrib. Comput., vol. 152, pp. 75-89, Jun. 2021.

[18] K. A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," IEEE Trans. Veh. Technol., vol. 61, no. 4, pp. 1874-1883, May 2012.

[19] H. Wu, X. Cao, Y. Wang, and J. Ma, "CLLS: Efficient certificateless lattice-based signature in VANETs,"Comput. Netw., vol. 253, p. 110696, Dec. 2024.

[20] F. Martinez, J. C. Toh, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Emergency services in future intelligent transportation

systems based on vehicular communication networks," IEEE Intell. Transp. Syst. Mag., vol. 2, no. 2, pp. 6-20, Summer 2010.

[21] M. S. Al-Kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in Proc. 6th Int. Conf. Signal Process. Commun. Syst. (ICSPCS), Gold Coast, QLD, Australia, Dec. 2012, pp. 1-9.

[22] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," Int.J. Inf. Security, vol. 1, no. 1, pp. 36-63, Aug. 2001.

[23] D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds., Post-Quantum Cryptography. Berlin, Germany: Springer-Verlag, 2009.

[24] C. Peikert, "A decade of lattice cryptography," Found. Trends Theor. Comput. Sci., vol. 10, no. 4, pp. 283- 424, Mar. 2016.

[25] J. Chen, H. Lim, S. Ling, H. Wang, and K. Nguyen, "A forward-secure and efficient authentication protocol through lattice-based group signature in VANETs scenarios," Comput. Netw., vol. 214, p. 109149, Aug. 2022.

[26] X. Wu, Y. Xu, H. Zhang, and X. Tan, "LbPV: Lattice-based privacy-preserving mutual authentication scheme for VANET," Comput. Commun., vol. 218, pp. 88-101, May 2024.

[27] A. Fujioka, K. Suzuki, K. Xagawa, and K. Yoneyama, "Strongly unforgeable signatures and more from lattices," in Proc. 12th Int. Conf. Appl. Cryptogr. Netw. Security (ACNS), Lausanne, Switzerland, Jun. 2014, pp. 319- 337.

[28] V. Lyubashevsky, "Lattice signatures without trapdoors," in Proc. 31st Annu. Int. Conf. Theory Appl. Cryptogr. Tech. (EUROCRYPT), Cambridge, UK, Apr. 2012, pp. 738-755.

[29] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," J. ACM, vol. 56, no. 6,pp. 1-40, Sep. 2009.

[30] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on post-quantum cryptography," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. NISTIR 8105, Apr. 2016.

[31] T. Pöppelmann and T. Güneysu, "Towards practical lattice-based public-key encryption on reconfigurable hardware," in Proc. 20th Int. Conf. Sel. Areas Cryptogr. (SAC), Burnaby, BC, Canada, Aug. 2013, pp. 68-85.

[32] S. Bai and S. D. Galbraith, "An improved compression technique for signatures based on learning with errors," in Proc. Cryptogr. Track RSA Conf. (CT-RSA), San Francisco, CA, USA, Feb. 2014, pp. 28-47.

[33] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS- Dilithium: A lattice-based digital signature scheme," IACR Trans. Cryptogr. Hardware Embedded Syst., vol. 2018, no. 1, pp. 238-268, Feb. 2018.

[34] J. Ding, "New cryptographic constructions using generalized learning with errors problem," IACR Cryptol. ePrint Arch., vol. 2012, p. 387, Jul. 2012.

[35] A. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," ACM Trans. Comput. Theory, vol. 6, no. 3, pp. 1-36, Sep. 2014.

[36] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st Annu. ACM Symp. Theory Comput., Bethesda, MD, USA, May 2009, pp. 169-178.

[37] V. Lyubashevsky, "Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures," in Proc. 15th Int. Conf. Theory Appl. Cryptol. Inf. Security (ASIACRYPT), Tokyo, Japan, Dec. 2009, pp. 598-616.

[38] D. Micciancio and C. Peikert, "Trapdoors for lattices: Simpler, tighter, faster, smaller," in Proc. 31st Annu. Int. Conf. Theory Appl. Cryptogr. Tech. (EUROCRYPT), Cambridge, UK, Apr. 2012, pp. 700-718.

[39] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in Proc. 40th Annu. ACM Symp. Theory Comput., Victoria, BC, Canada, May 2008, pp. 197- 206.

[40] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," Theory Comput. Syst., vol. 48, no. 3, pp. 535-553, Apr. 2011.

[41] P. M. Camerini, L. Fratta, and F. Maffioli, "On improving relaxation methods by modified gradient techniques," Math. Program., vol. 3, no. 1, pp. 26-34, Dec. 1975.

[42] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen- message attacks," SIAM J. Comput., vol. 17, no. 2, pp. 281-308, Apr. 1988.

[43] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in Proc. 1st ACM Conf. Comput. Commun. Security, Fairfax, VA, USA, Nov. 1993, pp. 62-73.

[44] J. Katz and Y. Lindell, Introduction to Modern Cryptography, 2nd ed. Boca Raton, FL, USA: CRC Press, 2014.

[45] N. Smart, "Cryptography made simple," Information Security and Cryptography. Cham, Switzerland: Springer, 2016.

[46] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.

[47] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.

[48] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[49] V. S. Miller, "Use of elliptic curves in cryptography," in Proc. Conf. Adv. Cryptol. (CRYPTO), Santa Barbara, CA, USA, Aug. 1985, pp. 417-426.

[50] N. Koblitz, "Elliptic curve cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203-209, Jan. 1987.