International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/31 Volume 12, Issue 4, July – August (2025)

RESEARCH ARTICLE

Quantum -Inspired and Probabilistic Zone Adaptive Routing Protocol for Gray Hole Attack Detection in VANETS

V. Sakthi Priyanka
Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India.
✉ vsakthipriyanka@gmail.com

V. Radha
Department of Computer Science, Dean School of Physical Sciences and Computational Sciences, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India.
radha_cs@avinuty.ac.in

Received: 03 May 2025 / Revised: 10 July 2025 / Accepted: 27 July 2025 / Published: 30 August 2025

Abstract – Vehicular Ad Hoc Networks (VANETs) are the backbone of contemporary intelligent transport systems. These are vulnerable to the security attacks like grayhole attacks that contaminate data exchange with packets lost in an unfair manner. To overcome these deficits, Integrated Quantum Inspired Secure Routing Framework (IQSRF) is introduced. It's a novel, end-to-end solution that morphs into the fusion of four cutting-edge algorithms. Efficient and scalable zone-based routing is attained through the framework using Quantum-inspired Zone Adaptive Routing Protocol (QZARP) for optimizing the vehicular communication across dynamic vehicular environments. Quantum-Inspired Probabilistic Routing Algorithm (QIPRA) improves path reliability using model-based probabilistic in order to calculate an optimal path. Dynamic Trust and Reputation Management Algorithm (DTRMA) ensures security through node trust confirmation and dynamic behavior, marking the nodes malicious to counter the grayhole attack. Adaptive Layered Quantum Resilient Encryption Algorithm (ALQREA) utilizes the multilayer encryption for ensuring confidentiality and data integrity. It is strongly immune to classical computer-based and quantum computer-based attacks. By the implementation of these algorithms through blending, there exists highly effective and efficient paradigm. This paradigm has not only identified grayhole attacks but also provides secure, reliable and best communication for VANETs in achieving the most essential needs of next-generation vehicular communications.

Index Terms – Data Security, Dynamic Trust and Reputation Management, Encryption, Grayhole Attack, Quantum Computing, Vehicular Ad Hoc Networks.

1. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) [1], [2] are the key component in implementing intelligent transportation [3] systems, which allows the vehicles and infrastructure to communicate for the applications such as navigation, traffic management and safety. But VANETs [4], [5] are plagued with several security challenges such as grayhole attacks [6-8], in which the arriving packets are dropped selectively by the attacking nodes, disrupting communication and incurring loss in system performance. But with no central authority and dynamic nature of VANETs, detection and prevention of this type of attack turn into an exhausting process. Along with the increase in size and complexity of the network, the need for safe data transmission and improved route decision making also increases.

To implement these solutions, various algorithms have been suggested. One approach to achieve this is the Zone Adaptive Routing Protocol (ZARP) [9-13], which segments the network into zones and enables localized routing [14] decisions to improve efficiency and reduce the overhead of far communication. A more efficient path finding is ensured within every zone. Thus, the communication performance in VANETs is enhanced [15], [16]. Complementing ZARP, the Quantum-Inspired Probabilistic Routing Algorithm (QIPRA) dynamically chooses the best paths to traverse the network by probabilistic methods. Further, it takes node mobility, network conditions and reliability into account for assuring the high success rate of data delivery.

Although routing is paramount [17], [18], securing the communication of VANETs has to be advocated. The Dynamic Trust and Reputation Management Algorithm (DTRMA) is useful for preventing attacks such as grayhole attacks [19], [20], where the trustworthiness of nodes is evaluated based on the past behaviors. Network is able to

RESEARCH ARTICLE

identify and isolate the real time malicious nodes through the dynamic evaluation process as well as only the trustworthy nodes are allowed to participate in communication process [21], [22]. Resilient Encryption Algorithm is used to guard against the confidentiality and integrity of transmitted data using strong cryptographic methods which are resilient to classical and quantum computing threats [23-25].

In this paper, an integrated solution, Integrated Quantum-Inspired Secure Routing Framework (IQSRF) is proposed which integrates the benefits of these individual algorithms to form a collective mechanism against the grayhole attacks with secure and efficient data transmission. This framework unifies Quantum-Inspired Zone Adaptive Routing Protocol (QZARP) for zone-based, Quantum-Inspired Probabilistic Routing Algorithm (QIPRA) for path selection, Dynamic Trust and Reputation Management Algorithm (DTRMA) for real-time grayhole attacks detection and Adaptive Layered Quantum-Resilient Encryption Algorithm (ALQREA) for data security. Specifically, this integrated approach not only optimizes routing performance but also substantially enhances the security of VANETs and provides robustness against both conventional and new security threats.

1.1. Contribution

Here, new contributions are made towards a new, integrated system for securing and optimizing VANETs using quantum-inspired routing, dynamic trust management and forward-secure encryption. Specifically:

- Introduced the IQSRF to improve VANET security.
- Developed QZARP for the efficient and scalable zone-based routing in dynamic vehicular networks.
- Developed QIPRA to optimize the routes for higher reliability via probabilistic modeling.
- Suggested DTRMA for the dynamic control of trust and grayhole attack detection.
- Suggested ALQREA for multilayered quantum-resistant encryption.
- Combined routing, trust and encryption within an end-to-end framework.
- Experimentally validated the suggested framework to prove its efficacy.

This holistic solution overcomes key VANET challenges and presents an extensible solution for secure and robust communication.

1.2. Motivation

This paper is motivated by the rising demand for secure and efficient communication associated with VANETs, prone to grayhole attacks as well as other security risks. Unfortunately, current routing and security mechanisms have not been sufficient for addressing these issues. This paper integrates quantum-inspired routing protocols, dynamic trust management and advanced encryption to develop a holistic approach for protecting data transmission and making it reliable over malicious attacks in VANETs.

Advanced routing protocols and cryptographic solutions assist to improve the security and efficiency in VANETs. Recent works have enhanced security and bandwidth requirements. In Quantum-Inspired Zone Adaptive Routing Protocol and QIPRA, the techniques inspired by quantum are used for zone-based and optimum path selection. Dynamic Trust and Reputation Management Algorithms are utilized for detection and prevention of greyhole attacks, as well as the data security with the ALQREA has been used.

These innovations work cooperatively in terms of improving the communication efficiency in VANET without degrading the security and reliability of communication.

1.3. Paper Organization

In this paper, related works are discussed in section 2. In section 3, the proposed Integrated Quantum-Inspired Secure Routing Framework methods are discussed. In section 4, the results and discussions are added and finally in section 5, conclusions are discussed.

2. BACKGROUND STUDY

Vehicular Ad-Hoc Networks (VANETs) were vulnerable to black hole and gray hole attacks because the packets were maliciously dropped to undermine the communication. To solve this problem, Q learning based approach for trustworthy routing was discussed by Mianji et al. [26] This method also had dynamical learning and adaptation capability to secure the routes in network. This work proposed a solution to these attacks and significantly improved routing security in dynamic environments. However, the approach was computationally expensive and relied heavily on the availability of symmetric training data. It also restricted the practical real time applicability.

High mobility and dynamic topology had created challenges for routing in VANETs. To tackle these problems, Naeem et al. [27] proposed an improved cluster-based routing protocol. Cluster head selection was optimized using the method that resulted in minimum packet loss and efficient routing. Although the approach was effective for high mobility, it hampered poor scalability and added overhead in cluster management that negatively impacted network performance in peak traffic.

The viability of various routing strategies in VANET setting was introduced by Nair [28] that aimed at related position and topology, as well as more current and complex routing systems. The properties and operations of VANETs were

RESEARCH ARTICLE

quite interesting. This paper discussed the numerous VANET routing algorithms based on topology and position. Among the other factors, scalability, latency and packet delivery ratio of different systems were assessed.

In VANETs, Nandagopal et al. [29] presented mobility aware zone-based routing protocol using the hybrid of metaheuristic algorithm to enhance route reliability. The hybrid method was the combination of Ant Colony Optimization (ACO) and Artificial Bee Colony (ABC) optimization. It was also optimal for path selection that combined multiple optimization techniques. This method had been presented to improve reliability and robustness at the expense of requiring significant computational resources. Being highly dependent on the fine tuning of heuristic parameters, it had also limited its capacity to scale the larger networks.

Determination of congestion control had been the important feature of VANETs. To ease congestion with predictive analytics and content pre-caching strategies, Nazar et al. [30] proposed a zone-based pre-caching method. This intelligent approach provided better data accessibility and lowered latency in high traffic locations. When the traffic pattern was unpredictable, it suffered in highly dynamic environments. Thus, its applicability was limited in some scenarios of VANET.

Communication reliability in sparse VANET environments was exposed to challenges. In this work, a hybrid geographic Delay Tolerant Network (DTN) routing protocol was suggested that fused geographic routing with fuzzy logic decision making, as proposed by Rahimi and Jamali [31]. In the case of sparse networks, this hybrid method exhibited higher packet delivery ratios and lower latencies than the other approaches. This approach had its advantages but limited in the dense traffic scenario with high mobility, where the routing delay increased.

Vehicular Ad-Hoc Network operations included secure operations in blackhole and grayhole attacks. A swarm inspired algorithm that used Artificial Neural Networks (ANN) was presented by Rani et al. [32]. It was used to detect and mitigate those attacks. The effectiveness of this method was applied in dynamic environments. Nevertheless, those methods rely on a Neural Network (NN) that raised computational complexity and energy consumption, hindered its applicability on resource constrained environments. In the field of data transportation, VANET security induced a critical research area where the attacks such as blackhole and grayhole attacks had to be detected. Analysis of detection schemes was presented by Rathod and Patel [33] and its effectiveness along with limitation were analyzed. This study delivered an in-depth description of existing strategies, but it had not included the real implementation or performance evaluation. Hence, it was less practical regarding the direct use for developing the practical solutions in VANET security.

Using Wi-Fi Direct technology, Saleh [34] proposed a Secure Optimized Request Zone Location-Aided Routing (SORZLAR) protocol to enhance secure routing in VANETs. It optimized secure routing by optimizing request zones that reduced the communication overhead and improved security. Yet, relying on Wi-Fi Direct, generalization was reduced to the other VANET conditions where this technology was not available.

To improve the routing precision and reduce delays, Saleh [35] introduced a Secure Tilted Rectangular Shaped Request Zone Location Aided Routing (STRS RZLAR) protocol. The optimized geometry for this approach enhanced routing efficiency with respect to specific zones. However, this approach struggled with the problems of scalability and adaptability, as its performance was highly sensitive to the fixed configuration and pre-defined zones. Therefore, it was not highly efficient in dynamic environments.

Grayhole attacks were addressed by Schweitzer et al. [36] through the contradiction-based detection mechanisms. This method exposed contradictions in the behavior of malicious nodes and it minimized the impact of such attacks. The approach was efficient and imposed minimal overhead but was only applicable for small-scale networks. It was highly susceptible to false positives, which led to the degradation of the network.

In Shi et al. [37], a social-based routing scheme was proposed for fixed-line VANETs to increase route stability and data delivery. In stable environments, this method improved the reliability by referencing socially significant nodes. Nevertheless, it was ineffective in dynamic and highly mobile environments. Social metrics had not reflected the network conditions that made it difficult to use in real-life VANET deployments. Table 1 compares the various related works onrouting in VANET. This table compares the focus area, methods, merits and demerits of various authors' research work.

Shoaib and Song [38] designed an optimized traffic-aware zone-based hierarchical link-state routing protocol specifically for VANETs. Their approach focused on enhancing traffic management and scalability by partitioning the network in a hierarchical manner and basing routing decisions on real-time traffic concentration within assigned zones. The protocol eliminated redundant broadcasts and enhanced data diffusion efficiency. But it introduced a lot of communication overhead in highly changing or complex network topologies, thereby constraining its scalability and applicability to highly dynamic environments.

Tassoult et al. [39] had conducted a thorough survey of VANET routing protocols, creating a classification on the basis of routing approach (topology-based, position-based, and hybrid) and the problems occurring with each of these,

RESEARCH ARTICLE

such as scalability, mobility, and security. Their work was a valuable resource for protocol evolution comprehension but was short on new proposal or real implementation of the solution, thus negating its contribution to theoretical analysis only.

Umre et al. [40] devised a zone-based routing scheme enhanced with bio-inspired clustering algorithms for optimizing communication efficiency in VANETs. Their scheme utilized swarm intelligence for stable cluster formation at the zone level, which helped reduce packet loss and ensure route stability. Despite its merits, the scheme suffered from increased algorithmic complexity and difficulties encountered in parameter tuning for dynamic environments.

Wahid et al. [41] provided a thorough overview of emerging VANET routing protocols and compared their performance based on several parameters including packet delivery ratio, end-to-end delay, and overhead. Their paper provided valuable observations regarding the pros and cons of different routing schemes. The survey didn't incorporate experimental evidences and simulation-based performance comparison and was therefore not as appropriate for real-time system implementation.

Yazdanypoor et al. [42] have also proposed a novel hybrid detection process with a blend of anomaly-based and signature-based methods towards detecting blackhole and grayhole attacks in VANETs. Hybridization provided more precise detection and recognition rate of the intruder node. It was energy-consuming and needed continuous observation and was hence not feasible for low-end or real-time application.

Yelure et al. [43] offered an informed explanation of the vulnerability of the routing protocol of VANETs to every kind of attack. The authors contrasted via empirical experiments the impact of common routing attacks such as blackhole, grayhole, and wormhole on network performance metrics. The study presented details of the attack behavior but was not useful in terms of offering effective mitigation approaches and could not provide suggestions for improving protocols.

Younas et al. [44] proposed a cooperative detection model of blackhole and grayhole attacks in VANETs. The model leveraged node cooperation to achieve optimal detection accuracy at the lowest possible false positives. Although the model improved detection credibility, it needed profound inter-node trust and synchronization that may be difficult to maintain with dynamic and large-scale VANETs.

Table 1 Comparison Table on Existing Works

Reference	Focus Area	Methods Used	Merits	Demerits
Mianji et al. [26]	Secure routing under dynamic topology	Q-learning-based trustworthy routing	Dynamic learning, improved routing security	High computational cost, dependency on training data
Naeem et al. [27]	Efficient routing in high-mobility VANETs	Improved cluster-based routing with optimized CH selection	Reduced packet loss, efficient routing	Poor scalability, clustering overhead
Nair [28]	Comparative analysis of routing strategies	Topology- and position-based routing evaluation	Evaluates PDR, latency, scalability	No new algorithm proposed
Nandagopal et al. [29]	Reliable routing with metaheuristics	ACO + ABC hybrid zone-based routing	Reliable path selection, improved robustness	High computational cost, parameter sensitivity
Nazar et al. [30]	Congestion control in VANETs	Zone-based content pre-caching	Reduced latency, improved data availability	Limited adaptability in highly dynamic traffic
Rahimi & Jamali [31]	Sparse network routing	Hybrid geographic + DTN + fuzzy logic	High PDR, lower latency in sparse networks	Not effective in dense/high mobility scenarios
Rani et al. [32]	Security against blackhole/grayhole	ANN + swarm intelligence	Adaptive attack mitigation	High computational load, energy inefficiency
Rathod & Patel [33]	Security threat survey	Analysis of detection schemes	Detailed overview of detection methods	Lacks implementation and real-world evaluation

RESEARCH ARTICLE

Saleh [34]	Secure zone-based routing	SORZLAR with Wi-Fi Direct	Reduces overhead, enhances security	Limited to environments with Wi-Fi Direct support
Saleh [35]	Geometry-aware routing	STRS-RZLAR (tilted rectangular zones)	Enhanced zone routing efficiency	Poor adaptability and scalability
Schweitzer et al. [36]	Detection of grayhole attacks	Contradiction-based behavior analysis	Lightweight detection, low overhead	High false positives, suited only for small networks
Shi et al. [37]	Social-based routing	Social node-based path selection	Improved stability in static environments	Ineffective in highly mobile settings
Shoaib & Song [38]	Traffic-aware hierarchical routing	Zone-based hierarchical link-state routing	Improved scalability and traffic management	High overhead in complex scenarios
Tassoult et al. [39]	Protocol taxonomy	Classification of VANET routing protocols	Broad protocol overview and challenges	No practical solution proposed
Umre et al. [40]	Bio-inspired zone-based routing	Cluster-based routing with swarm intelligence	Stable communication, efficient clustering	Complexity in cluster tuning
Wahid et al. [41]	Review of routing protocols	Comparative analysis	Summarizes protocol evolution and strengths	No performance simulation or validation
Yazdanypoor et al. [42]	Security attack detection	Hybrid (anomaly + signature) detection	High accuracy, robust detection	Real-time implementation challenges
Yelure et al. [43]	Attack impact analysis	Assessment of routing attack effects	Quantifies vulnerabilities	No proposed mitigation
Younas et al. [44]	Collaborative attack detection	Cooperative node-based detection	Reduced false positives, high reliability	Needs high trust and coordination overhead

2.1. Problem Identification

Vehicular Ad-Hoc Networks play a key role in communication among the intelligent transportation systems but the network has a dynamic topology and high mobility with the associated challenges for routing efficiency and security. One of the threats to the reliability and integrity of VANETs is posed by gray hole and black hole attacks, in which the malicious nodes disrupt the communication by selectively or fully dropping the packets. Moreover, traditional routing protocols are typically unable to cope with rapid network changes, causing higher packet loss and latency.

Thereby, data safety is also compromised. Zone-based routing, clustering and hybrid approaches have been proposed but typically undergo issues including high computational complexity, scalability issues and vulnerability to advanced threats. This creates the need for robust, adaptive and secure means of setup to enforce efficient routing and resilient communication in VANET environments.

Inspired Zone Adaptive Routing Protocol for zone-based routing, Quantum-Inspired Probabilistic Routing Algorithm for optimal path selecting, Dynamic Trust and Reputation Management Algorithm for grayhole attack predicting and

2.2. Problem Statement

Vehicular Ad-Hoc Networks are among the key elements of intelligent transport systems, facilitating real-time vehicle-to-infrastructure and vehicle-to-vehicle communication. Yet, the topology is dynamic, highly mobile and lacks central control. VANETs are most critically vulnerable to security attacks, most notably grayhole attacks, where an attacker node opportunistically discards malicious packets, obstructing communication and impairing network performance. Typical routing and security mechanisms tend to fall short in addressing such problems in practical and mobile environments. There is an urgent need for an integrated, intelligent and secure system providing guaranteed trustworthy routing, proactive attack detection and strong encryption to ensure the safe and reliable communication in VANET environments.

3. MATERIALS AND METHODS

In this paper, Integrated Quantum-Inspired Secure Routing Framework (IQSRF) is introduced. Combining Quantum-Adaptive Layered Quantum-Resilient Encryption Algorithm for data security in VANET for grayhole attack prevention. Figure 1 illustrates the overall prevention architecture from grayhole attack.

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/31 Volume 12, Issue 4, July – August (2025)

RESEARCH ARTICLE

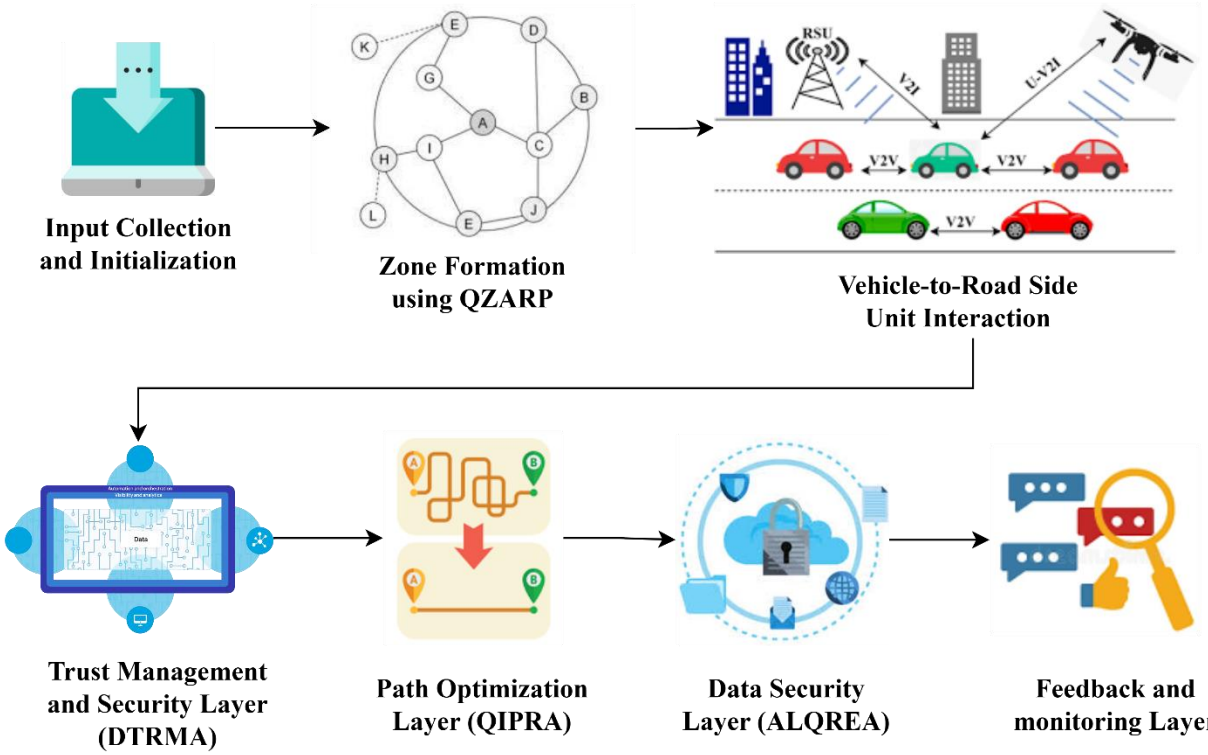

Figure 1 Overall Architecture for Grayhole Attack Prevention

3.1. Quantum-Inspired Zone Adaptive Routing Protocol (QZARP)

A highly efficient routing mechanism, Zone Adaptive Routing Protocol (ZARP) is designed to handle the intricacies of dynamic and large-scale networks like VANETs. High mobility, high frequency topological changes and variable densities creates the challenges in these environments. To address these problems, ZARP breaks the network into small and high manageable areas referred to as zones. These zones act as a chunk of the overall network. With this division, routing decisions are confined within zones. It necessitates far global topology updates and greatly reduces the routing overhead. Finally, intra-zone routing is performed over the zone using the routing protocols. These methods are similar to the Advanced Development of Vehicles (AODV) for the highly efficient local communication within zones. Inter-zone communication is realized through zone leaders, in which the intermediate members of each zone are used as intermediaries in communication. Thus, the utility keeps routing information about its zone and communicate with each other to forward the packets towards neighbor zones. The dynamic adaptability strength of ZARP is its key strength. Zone adjustment is adapted based on the real-time network conditions such as vehicular density and mobility pattern to optimize the performance. For instance, smaller zones are used in dense network to reduce the contentions and utility of larger zones in sparse environment to provide connectivity. Due to the adaptability of ZARP, it is capable of producing high performance in several different scenarios. Moreover, ZARP uses a hierarchical routing structure for the reduction of latency along with the lowering of computational and communication costs while maintaining global routing tables. This protocol picks the path based on reliable and energy efficient metrics like distance, residual energy and trust along the paths.

Quantum-Inspired Zone Adaptive Routing Protocol, an advanced routing Protocol for dynamic network combines zone-based routing for dynamic network such as VANETs with the principles inspired from quantum techniques. Local routing is handled by splitting the network into geographical zones. Hence, this research improves scalability and reduces the communication overhead. Further, nodes are able to utilize the quantum inspired states to evaluate the appropriateness for using routing in accordance with the metrics such as trust, energy and distance. This method uses a collapse mechanism to select the optimal path from the multiple paths, which is examined at once using a quantum superposition. The routing is trust based to detect the malicious nodes and is enhanced against security through quantum entanglement to reevaluate the neighbors. Dense and sparse environments are considered, in which the zone sizes and routes are dynamically changed with real time network. The method prioritizes its choices of energy efficient nodes and obtains a packet delivery ratio higher than pure energy

RESEARCH ARTICLE

and pure node constrained networks while increasing the network lifespan. With an innovative design, it provides secure, adaptive and efficient communication over large and complex networks.

In equation (1), ZARP divides the network into zones based on a predefined zone radius$R$. If its distance from the zone center is less than or equal to$R$, the A node v belongs to zone z_i.

$$z_i = \{v \in V | D(v, zonecenter) \leq R\} \quad (1)$$

The distance (D) between a node v and the zone center is calculated using the Euclidean distance formula:

$$D(v, zonecenter) = \sqrt{(x_v - x_c)^2 + (y_v - y_c)^2} \quad (2)$$

Where, $(x_v - x_c)$ is the coordinates of node and $(y_v - y_c)$ refers to the coordinates of zone center. Equation (2) defines it such that each node determines the zone membership independently. In addition, R is adjusted dynamically in accordance with the network density. Smaller R is used for dense networks in order to reduce congestion. For sparse networks, larger R is needed to maintain connectivity.

Each node v in network is represented by a quantum state in equation (3):

$$\psi_v = \alpha|0\rangle + \beta|1\rangle \quad (3)$$

Where, $|0\rangle$ Node is available for routing. $|1\rangle$Node is excluded from routing. $|\alpha^2|$ + $|\beta^2|$ = 1: Probabilities of the node being in states $|0\rangle$and$|1\rangle$.The probabilities $|\alpha^2|$ and $|\beta^2|$ in equation (4), (5) are determined based on node parameters:

$$|\alpha^2| = w_1 \cdot \frac{1}{d(v,D_i)} + w_2 \cdot T(v) + w_3 \cdot E(v) \quad (4)$$

$$|\beta^2| = 1 - |\alpha^2| \quad (5)$$

Where, $d(v, D_i)$ is the distance of node v to destinationD_i. $T(v)$ is the trust score of node$v$. $E(v)$ is the residual energy of the node v.w_1,w_2 and w_3 are the weight coefficients assigned to each metric, which are tuned based on network requirements. Equation (6) minimizes latency by selecting the nodes toward destination based on the distance. It favors the reliable nodes to secure the communication and its works by selecting the energy efficient node that prolongs network lifetime. It probabilistically assesses the suitability for routing by relying on more than one metric in same time using this representation. This method evaluates the possible paths P_p between a source s and destination D as a quantum superposition:

$$P_p = \sum_{i=1}^{n} p_i |p_i\rangle \quad (6)$$

$p.R(v)$ is the cost related to the appropriate node. This equation (13p calculates the overall path by aggregating the $R(v)$ values of all nodes v along path$p$. Each variable is

Where, $|p_i\rangle$ represents the i -th path. $p_i$refers to the weight of i-th path based on its suitability.

In equation (7), weight p_ii of a path $p_i$is calculated as:

$$p_i\text{i} = \prod_{v \in p_i} R(v) \quad (7)$$

In the following equation (8), $R(v)$ is the routing metric of node v on path. w_1, w_2 and w_3 indicates the weight assigned to each factor. Distance betwixt the vehicle node v and destination node p_i is represented as $d(v, D_i)$. Energy level of node v is indicated as $E(v)$.

$$R(v) = w_1 \cdot \frac{1}{d(v,D_i)} + w_2 \cdot T(v) + w_3 \cdot E(v) \quad (8)$$

Once the path is evaluated, quantum state $P_p$collapses to the optimal path $|p^*\rangle$ as in equation (9):

$$p^* = \arg\max_{p_i \in p_p} p_i \quad (9)$$

Equation (10) calculates the trust score $T(v)$ which quantifies the reliability of a node based on its forwarding behavior:

$$T(v) = \frac{packetforwardbyv}{packetsenttov} \quad (10)$$

Nodes with a high trust score ($T(v)$≈1) are considered reliable and included in routing paths. Nodes with $T(v) <$ T *(threshold)* are indicated as unreliable or malicious and excluded from the routing. As per equation (11), Residual energy $E(v)$ of a node is calculated as:

$$E(v) = \frac{Currentenergyofnodev}{Initialenergyofnodev} \quad (11)$$

This ensures that a node left with high energy is preferred for routing than the node which depletes anytime depriving the network creating a network partition. In equation (12), zone radius R is dynamically adjusted based on network density:

$$R = \frac{f}{\sqrt{\rho}} \quad (12)$$

Where, f is the scaling factor andρrefers to node density within the network. Static zone sizes are dynamic, providing optimal performance as the network goes from dense to sparse. For a given route p consisting of nodes $\{v_1, v_2, \ldots, v_n\}$, the total route cost $c(p)$ is calculated as in the following equation (13):

$$c(p) = \sum_{v \in p} R(v) \quad (13)$$

The optimal path is selected as route with highest total score $c(p)$. An individual node v, is a part of the route

crucial when simulating the effects of performance requirements such as latency, dependability on VANET communication or resource usage. This method guarantees that the chosen path is secure, energy efficient and occurs in a

RESEARCH ARTICLE

geographically plausible setting. Figure 2 and algorithm 1 illustrates the functioning of QZARP protocol.

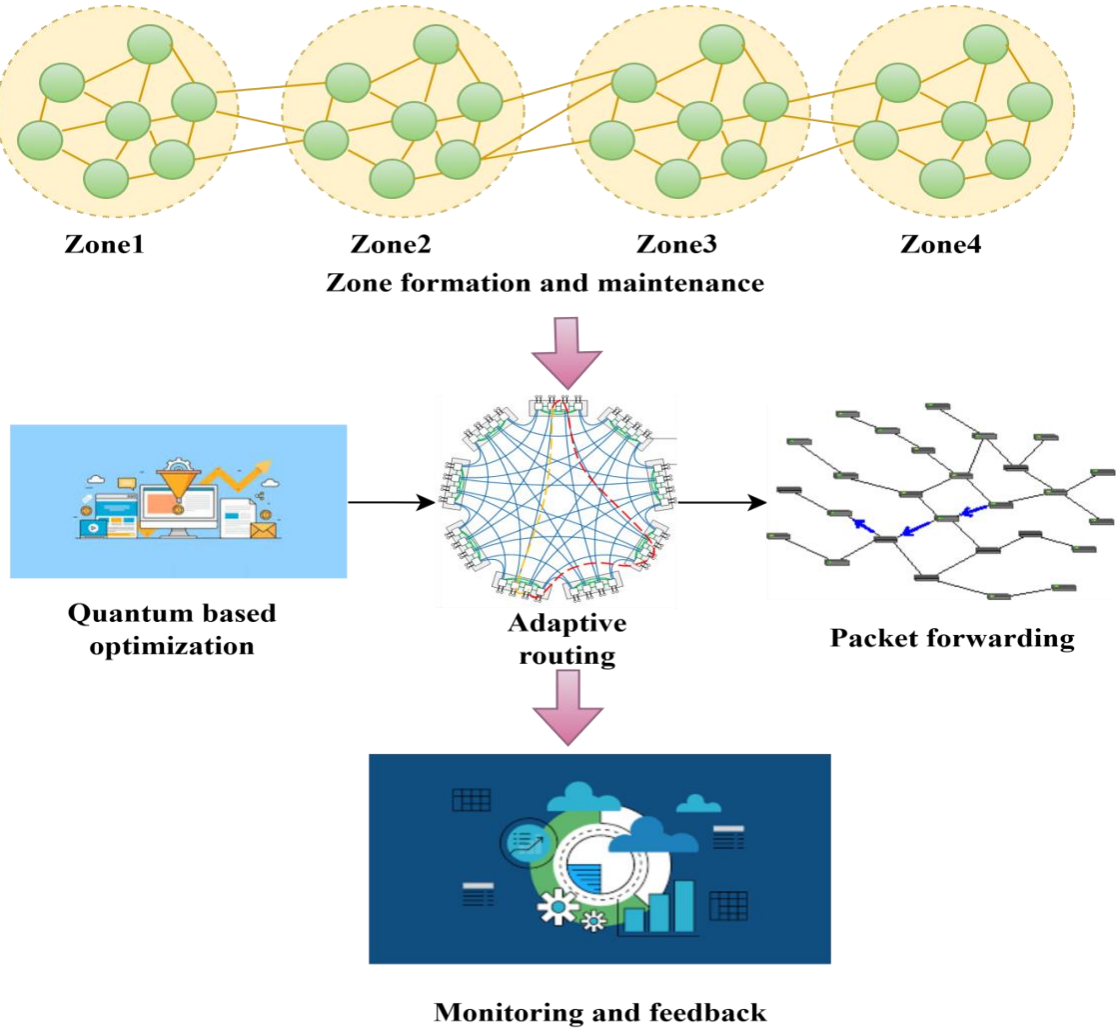

Figure 2 Quantum -Inspired Zone Adaptive Routing Protocol

Input:

- Network Topology: Data regarding the locations in space of road segments and vehicles.
- Trust Metrics: Algorithmic and parametric measures to calculate the trust of adjacent nodes.
- Gray Hole Attack Detection Mechanisms: Malicious and suspicious node behavior detection algorithms.
- Range of Communication: Cars can communicate with each other at extreme range.
- Traffic Condition: Real-time traffic congestion, speed of vehicles, and road conditions.

3. Grayhole Attack Detection:

Step:

1. Zone Partitioning:

Divide the network into geographic areas according to vehicle proximity and communication range.

$\text{Trust}_i = f(\text{behavior}_i, \text{interactions}_i)$

2. Trust Evaluation:

Evaluate neighboring nodes in each area for trustworthiness by means of trust metrics and algorithms.

Monitor is network traffic for suspicious behavior and activity that suggested grayhole attacks.

RESEARCH ARTICLE

$R_{ij} = argmin_{k \in N_i}[Cost_{ik} + Cost_{kj}]$

Anomaly detection algorithms and behavior analysis methods have to the used to classify the nodes for potential malicious activities.

4. Localized Routing Decisions:

Route at the local level for each zone, routing preferentially to the trusted nodes and not to suspicious nodes.

5. Adaptive Routing Updates:

Reconstitute routing path routes dynamically based on immediate changes in network topological structure, traffic flows and trust values.

6. Message Propagation:

Disseminate routing information and trust data to the neighboring zones in order to give the network coherence and consistency.

7. Grayhole Mitigation:

Put in place countermeasures to neutralize the impact of identified Grayhole attacks, for instance, by using the trusted nodes to forward packets or isolate offending ones.

Output:

Best Route Paths: Routes upon which data packets has been transmitted from source to destination without being subjected to grayhole attacks.

Algorithm 1 Quantum -Inspired Zone Adaptive Routing Protocol

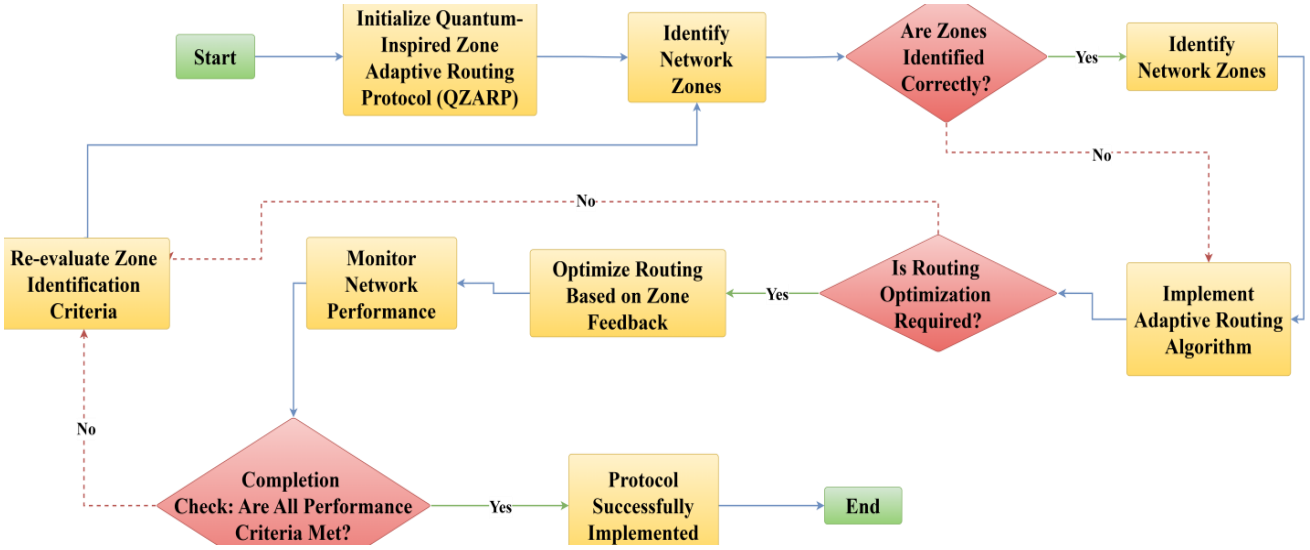

Figure 3 Flowchart of Quantum-Inspired Zone Adaptive Routing Protocol

Figure 3 illustrates the step-by-step process for adopting the QZARP for VANETs. The process begins with zone detection, followed by validation and adaptive routing. It has ongoing performance monitoring and iteratively optimal routing until all the requirements are fulfilled to provide efficient and secure communication.

3.2. Quantum-Inspired Probabilistic Routing Algorithm (QIPRA)

In (VANETs), where the topology frequently changes due to high mobility in vehicles, the Probabilistic Routing Algorithm (PRA) is a primary approach for path finding. In the case of deterministic algorithms other than probabilistic routing, fixed methods are used for estimation. In contrast, the latter uses stochastic methods to estimate the probability of successful packet delivery along a particular path. Besides that, this selection. It is compared with the conventional algorithms to infer the distance traveled by vehicle.

algorithm is based on the number of metrics like vehicle density, signal strength, delivery success rates in the past, real-time traffic conditions, etc. It chooses the paths dynamically such that the probability of a successful completion is as high as possible with the minimum delay. Because of this adaptability, it is especially suitable to deal with the grayhole attacks where the malicious nodes continually drop packets. In addition, probabilistic routing is able to detect and compromise nodes while the deviations are detected in packet delivery rates for improving the data integrity. Furthermore, algorithm uses load balancing to run traffic over multiple possible paths to reduce congestion and boosts the network efficiency. Depending on its robustness and adaptability, it is very suited for the applications in VANET such as real time communication and optimal route

Using the principals of quantum computing such as entanglement and super position, QIPRA utilizes the

RESEARCH ARTICLE

principles to move the routing on dynamic networks like VANETs. This algorithm simultaneously evaluates the multiple routes as quantum states for potential paths. In complex settings with rapidly changing dynamics, this parallelism reduces some decision latency in deliberation. Distance, traffic, node reliability and historical success rate determines the probability of each path and the algorithm is assigned suitable probabilities to each path. It is dynamically adaptive to the topology fluctuations in network topology by the principals of quantum systems. Thereby, communication robustness and efficiency is achieved. Alongside, it uses probabilistic weighting which features better reliable paths but enables it to explore the alternate routes. It helps to detect the packet delivery anomalies. Thus, the malicious nodes such as grayhole attacks are avoided. This design is an innovative one and the packet delivery ratio is improved. Further, latency is decreased and the provided attack tolerant support offers better security and routing efficiency in VANETs.

This method applies the quantum principles like superposition and probability distribution to dynamically choose the route by considering some parameters. And so, route selection is been optimized. Path reliability (R_i), congestion factor (c_i) and distance (D_i) input metrics for N paths in VANET are

$$P_i = R_i \times (1 - C_i) \quad (14)$$

In i^{th}, P_i represents the performance metrics like packet delivery ratio, throughput and R_i indicate the reliable factor. Meanwhile, C_i points out the congestion level of the same node. Probabilities are calculated based on the reliability and congestion factors. This equation (14) demonstrates the performance of node as the product of its reliability. R_i is modified for congestion (1 - C_i). Normalize the probabilities so it sums to 1:

$$P_{total} = \sum_{i=1}^{N} P_i \quad (15)$$

The total P value indicates an added quantity across the various elements. Equation (15) is a summation process, in which P_i' is added to the elements from $i=1$ over N elements. Each path is in a superposed state with its normalized probability amplitude of existence. Normalized probabilities (P_i') is calculated as:

$$P_i' = \frac{P_i}{P_{total}} \quad (16)$$

After measurement (decision making), the probabilities collapse to a single path based on the highest value. This equation (16) is used to calculate a normalized value P_i' or probability distribution P_i based on the individual values scaled in respect to the total sum. It ensures that each value manifests itself as a part of the total. If the selected path fails due to grayhole attack, a backup based on the second-highest probability has to be utilized. The following figure 4 and algorithm 2 describe the working of the QIPRA method.

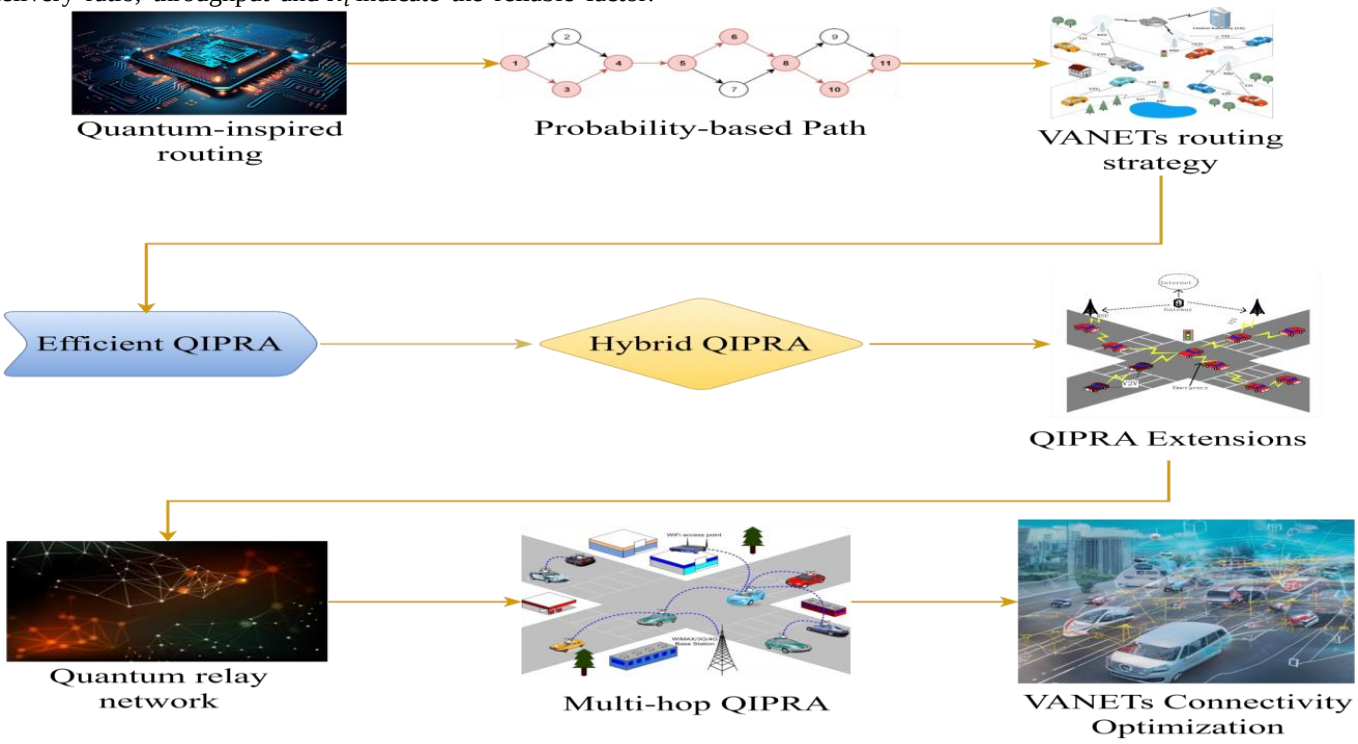

Figure 4 Quantum-Inspired Probabilistic Routing Architecture

RESEARCH ARTICLE

Initialization:

VANET graph *G (V, E)*, a graph with node set V with vehicles and edge set E, comprises of all communication links between the vehicles.

For all links $(i,j) \in E$, initialize quantum inspired probability amplitudes $\psi(i,j)$.

Calculate Link Probabilities:

Compute the probability $P(i,j)$ for any connection (i,j) depending on its dependability $R(i,j)$, stability $S(i,j)$ and congestion $C(i,j)$ using quantum-inspired ideas:

$$P(i,j) = \frac{|\psi(i,j)|^2}{\sum_{(k,l)\in E} |\psi(k,l)|^2}$$

Route Evaluation:

Calculate every possible path R_p from the source *S* to the destination *D*.

The total probability of every possible path is estimated as:

$$P(R_p) = \prod_{(i,j)\in R_p} P(i,j)$$

Path Selection:

Determine the path with greatest total likelihood:

$$R_{best} = arg \max_{R_p} P(R_p)$$

Quantum Probability Update:

Update the quantum probability amplitudes $\psi(i,j)$ using a reinforcement learning to rank successful linkages after route selection.

$$\psi(i,j) = \psi(i,j) + \eta \cdot \Delta\psi(i,j)$$

The second constraint is on $\Delta\psi(i,j)$, which refers to reward punishment term on the basis of link performance and the learning rate η.

Iterative Refinement:

Iteration is repeated periodically to regulate the network topology and conditions.

Algorithm 2 Quantum-Inspired Probabilistic Routing Algorithm

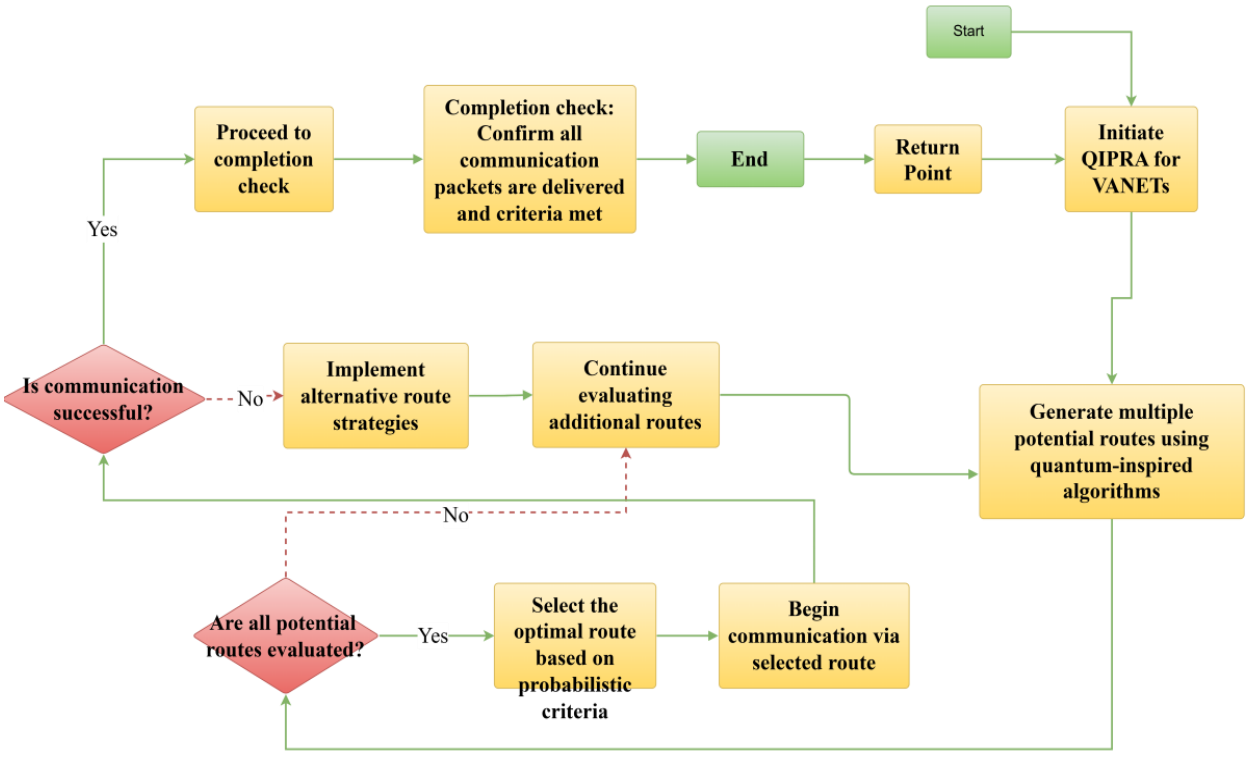

Figure 5 Flowchart of Quantum-Inspired Probabilistic Routing

RESEARCH ARTICLE

Figure 5 illustrates the flow of QIPRA method. This method is initiated for VANETs. If the communication is successful, the optimal route is selected based on the probabilistic values. In case of unsuccessful communication, alternative strategies have to be utilized to produce multiple routes.

3.3. Dynamic Trust and Reputation Management Algorithm (DTRMA)

Trust and Reputation Management Algorithm (DTRMA) is a critical defense mechanism to defeat grayhole attacks in VANETs. It observes and assesses the behavior of nodes, spotting malicious entities perturbing the network links by selectively dropping packets. This trust algorithm determines the trust values with node metrics of packet forwarding rate, historical interactions and neighbor node feedback. The reputation of node is updated dynamically on the basis of its consistency in forwarding data. While a node's trust value drops below some predefined threshold, the node is marked malicious and excluded from the routing. One mechanism ensures the neglecting of false positives by cross verifying the trust values obtained from multiple nodes to ensure reliability. Besides, grayhole attacks impact is mitigated by this approach resulting in the enhancement of security and whole data transmission efficiency. This algorithm sustains a reliable and adaptive environment for VANET, by encouraging collaboration among the trusted nodes. Thus, unremitting communication and optimal routing is maintained.

A robust mechanism to prevent grayhole attacks in VANETs is DTRMA. As the packets are selectively discarded, grayhole attacks are difficult to detect and disrupt the network operations. This is addressed in DTRMA by evaluating the possible trustworthiness of neighbors in accordance with behavior. It computes trust scores based on the combination of direct observations via indirect feedback from neighboring vehicles. Real time scores are updated for any malicious actions. These nodes are tagged and blocked, which have low trust score from passing out to vital data transfer. In addition, DTRMA uses a reputation system which collects and sums up the trust history of nodes to defeat malicious nodes. This algorithm assures of data delivery through combing the trust evaluation with optimal route selection mechanism. The approach of VANET through proactiveness minimizes the grayhole risk by preserving the VANET's efficiency and security.

Direct Trust (T_d) is calculated based on the observed packet forwarding behavior of node:

$$T_d = \frac{P_f}{P_s} \quad (17)$$

According to equation (17), P_f is the number of packets successfully forwarded by node. P_s is the total number of packets sent to the node. Based on direct observation of node's behavior, it determines the trustworthiness of node. The fraction of packets forwarded by a node it is sent. More value it has, indicate its high reliability. Direct trust makes the detection of packet possible which drops the behavior as an immediate key sign for grayhole attacks. In equation (18), the weighted average value T_{id} is estimated as:

$$T_{id} = \frac{\sum_{i=1}^{N} w_i \cdot T_i}{\sum_{i=1}^{N} w_i} \quad (18)$$

Where, w_i is the weight assigned to feedback from i-th neighbor based on its own trustworthiness.T_i is the trust value reported by i-th neighbor. N is the total number of neighbors providing feedback. It indirectly evaluates the behavior of node by aggregating trust feedback from neighboring nodes. A trust score T_i provided by each neighbor is weighted with the trustworthiness (w_i) of the reporting neighbor. It guarantees that the feedback has more influence because of its reliablility. Indirect trust integrates the exclusive overhead on local observations for reliance and detects the malicious nodes from a broader network perspective.

The combined trust score integrates both direct and indirect trust is calculated in equation (19):

$$T_i = \alpha \cdot T_{id} + \beta \cdot T_{id} \quad (19)$$

In equation (20), Parameters α and β control the weight between direct and indirect trust, while the preference goes to locally observed result versus network wide feedback. So by adjusting these weights, algorithm is tuned to be more or less sensitive for the particular type attack scenarios. Here, α and β are the weighting factors ($\alpha + \beta = 1$).

$$T_i(t+1) = T_i(t) \cdot e^{-\lambda \cdot \Delta t} \quad (20)$$

Here, $T_i(t)$ is trust value at time$t$. Δt is the time elapsed since the last interaction. $e^{-\lambda \cdot \Delta t}$ represents the exponential decay factor. λ points out the decay factor which controls the rate of trust reduction in equation (21). Trust value is incremented using exponential decay applied on the elapsed time (Δt) from the last interaction. For every unit of time, λ determines the lost trust. This encourages the prolonged inactivity of attackers which are used to evade detection.

$$S = \begin{cases} Trustworthy if T_i \geq T(threshold) \\ Malicious if T_i < T(threshold \end{cases} \quad (21)$$

Potentially malicious nodes and trustworthy are distinguished by threshold value. Those nodes below the threshold are flagged and get some further action. Equation (22) provides a clear decision-making criterion for not using the compromised nodes in network. A node is flagged as a grayhole attacker if it's Packet Drop Rate (P_d) exceeds a specified threshold:

$$P_d = 1 - T_d \quad (22)$$

$P_d > P_{d\_threshold}$, the node is suspected of malicious behavior. At lower direct trust score (T_d), the packet drop rate

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/31 Volume 12, Issue 4, July – August (2025)

RESEARCH ARTICLE

(P_d) becomes high which indicates the behavior of malicious packet drop. Detects nodes performing selective packet dropping have the characteristic of grayhole attacks. For allowing the falsely flagged nodes to regain trust, recovery is based on the weighted score as in equation (23):

$$T_i = \frac{P_{rf}}{P_{rs}} + \gamma \cdot T_i \quad (23)$$

Here, P_{rf} is a recent forwarded packet. P_{rs} is recent sent packets. γ is recovery factor ($0 \leq \gamma \leq 1$). The node's trust scored combines with the recent forwarding performance, getting weighted by the recovery factor. This is a guarantee toward restoring the trust gradually. Has not permanently removed the nodes labeled as malicious. For routing decisions, an aggregated trust score of all possible paths:

$$T_p = \sum_{j=1}^{M} \frac{T_j}{M} \quad (24)$$

Where, T_j is the trust score of j-th node in the path. M is the number of nodes in path. Equation (24) evaluates path reliability by aggregating the trust scores of all nodes in a path. The greater T_p is safer and more trustworthy the route. It makes sure data is routed via the most reliable path (not via some malware or compromised nodes).

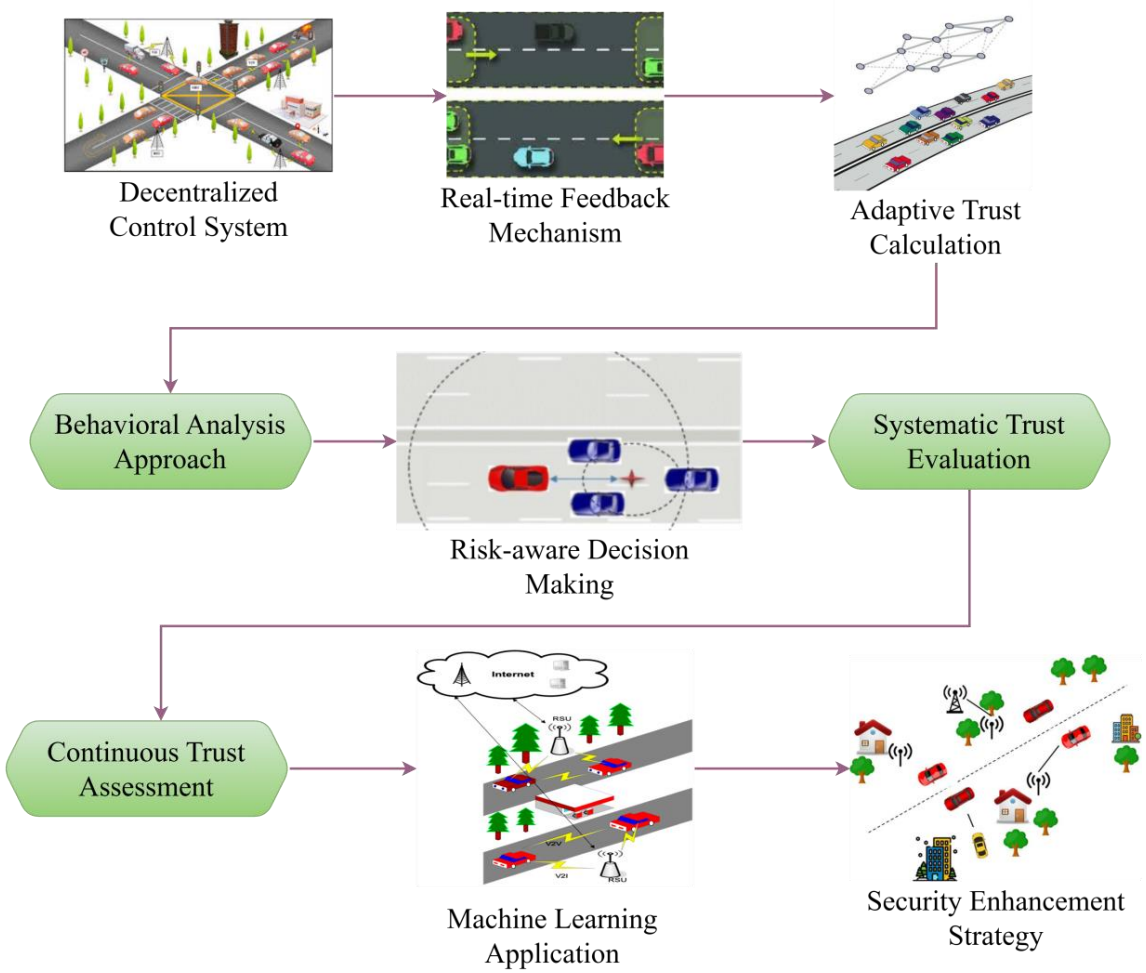

Figure 6 Dynamic Trust and Reputation Management Architecture

Figure 6 and Algorithm 3 indicate the method of Dynamic Trust and Reputation Management. Here, processes such as the adaptive trust calculation, behavioral analysis and trust assessment are carried out.

Trust Calculation:

After each interaction, a node updates its trust data for other node. Only the success and failure are considered.

$$T(A,B) = \begin{cases} 1 & if interaction is successful \\ 0 & if interaction fails \end{cases}$$

If node A interacts successfully with node B, $T(A,B) = 1$.

In the other case, if the interaction between node A and node B fails or becomes zero, $T(A,B) = 0$.

Reputation Calculation:

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/31 Volume 12, Issue 4, July – August (2025)

RESEARCH ARTICLE

A node reputation is the average trust which the other nodes possess.

$$R(A) = \frac{1}{N}\sum_{i=1}^{N} T(B_i, A)$$

Number of nodes interacted with node A is represented by N.

Let's state as $T(Bi, A)$, the trust each node Bi has in A.

Gray Hole Detection:

A node is considered grayhole if its reputation has fallen under a certain threshold in a certain number of interactions.

$$Gray\ Hole\ Detection\colon\ R(A) < R_{threshold} for\ k\ interactions$$

$R_{threshold}$ is defined as minimum reputation of a user considered acceptable.

The number of interactions where the reputation goes below the threshold (and so can be perceived as inconsistent behavior) is k.

Dynamic Update:

The implementation of trust values is on a per interaction basis. A node's trust decreases if its behavior is bad (that is, it fails an interaction) and increases otherwise.

Algorithm 3 Dynamic Trust and Reputation Management Algorithm

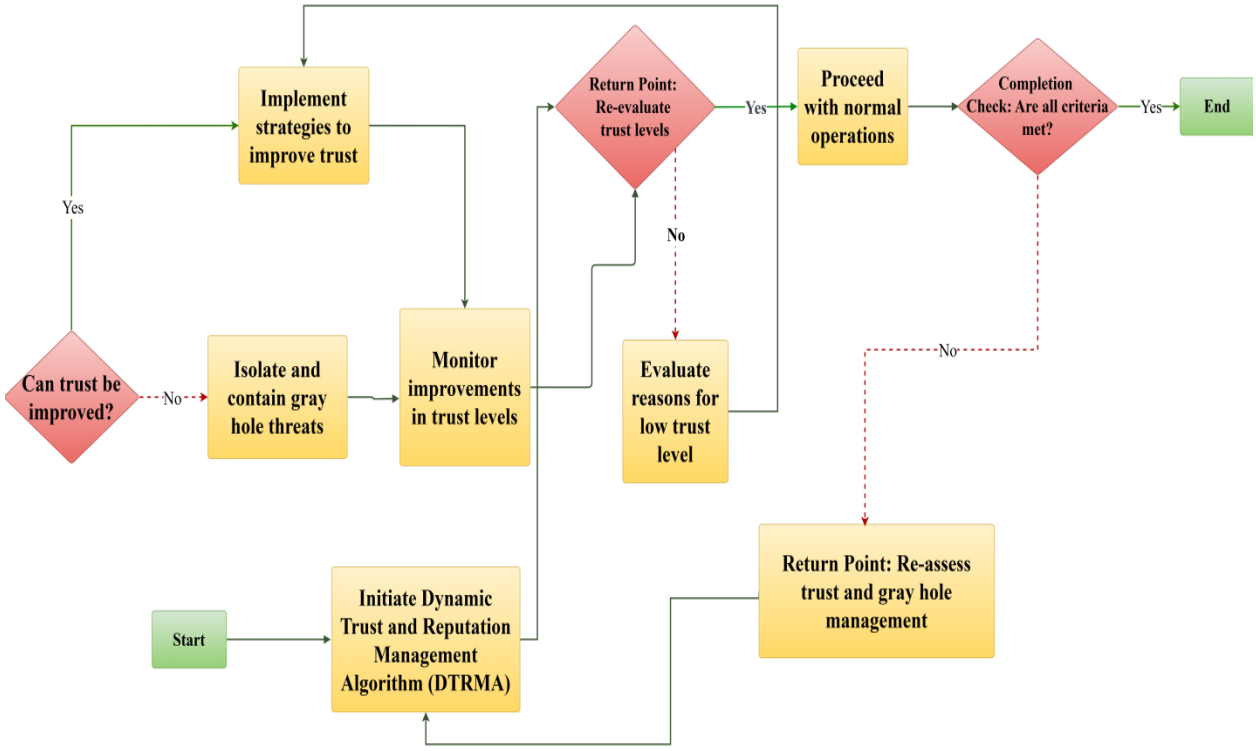

Figure 7 Flowchart of Dynamic Trust and Reputation Management

Figure 7 refers to the DRTRM flowchart. This method assesses the trust and grayhole attack. If there are any chances for trust improvement, proceed with the strategies for assessing the reduced trust levels. Or else, separate it and administer the improvements of trust levels.

3.4. Adaptive Layered Quantum-Resilient Encryption Algorithm (ALQREA)

Resilient encryption algorithm improves data security in terms of securing data against future threats and unauthorized access. The cryptographic techniques such as dynamic key generation and multi-layer encryption are also used to protect the data even under very harsh conditions. The algorithm changes in the space of changing the security conditions so as to provide constant security without vulnerabilities. Resilience of Sensor Network (SN) makes it feasible for protecting the sensitive data in dynamic networks such as VANETs and other critical systems.

Quantum Resilient Encryption Algorithm (QREA) protects data from potential threats by the forthcoming quantum computers that decrypt a Rivest Shamir Adleman (RSA) or Elliptic Curve Cryptography (ECC) protected data. Such algorithms take advantage of quantum-resistant cryptographic

RESEARCH ARTICLE

techniques like the use of lattice-based, hash-based or code-based cryptography in order to maintain strong data protection. At the core, it is solved only with the mathematical problems that remain computationally infeasible to perform on both classical and quantum computers. Quantum resilient encryption provides long term security which makes it as the preferred choice while dealing with sensitive data that leaks soon due to the emerging quantum computing technologies.

A sophisticated cryptographic method to improve data security in quantum era is the Adaptive Layered Quantum-Resilient Encryption Algorithm (ALQREA). It is designed based on the multi layered encryption framework; each layer is based on different quantum resistant cryptographic techniques such as lattice based, code based and hash-based cryptography. This adaptive mechanism permits to dynamically modulate the encryption strength with respect to data sensitivity and the resources which allocates computation. With this, it optimizes security throughout efficiency. This technique combines multiple layers with different cryptographic methods to create a robust quantum as well as classical attack defense integrity and confidentiality of sensitive information in dynamic and high-risk environments. The layers of encryption $L_1, L_2, \dots, L_n$ are dynamically selected based on the security level S and resource factors F.

$$L' = \{L_i | \ Threshold\ (S, F) \geq \tau_i, \quad i = 1,2, \dots, n\} \qquad (25)$$

Where, L′ is selected subset of encryption layers. S is the required security level. F is the available resources such as computation power. τ_i is the security threshold for layer i. Equation (25) guarantees that only such layers are selected which meet required security and resource constraints. Multiple layers from 1 to n are indicated as $i = 1,2, \dots, n$. For each selected layer L_i, a unique encryption key is generated using a key generation function G:

$$K_i = G(H_i) \qquad (26)$$

Here, K_i is the encryption key for layer i. G is the key generation algorithm. H_i is the specific parameters or initial values for layer i. Equation (26) is used to generate a unique encryption key. The data D is encrypted sequentially through the selected layers L′:

$$C = E_L(E_{L-1}(\dots E_{Li}(D))) \qquad (27)$$

Where, C is the final ciphertext. E_{Li} is the encryption function for layer i and D is input data. Equation (27) applies the multiple layers of encryption, with each layer providing an additional level of security.

Decryption is the reverse of encryption using the corresponding decryption keys K_i:

$$D = D_{L1}(D_{L2}(\dots D_{Lm}(C))) \qquad (28)$$

Adaptive Mechanism

In equation (28), $D_{Lm}(C)$ decryption function for layer i is applied to ciphertext C. K_i is the keys used for decryption. To balance security and efficiency, the algorithm evaluates the computational cost T and adjusts layers:

$$L'' = \arg\min_{L'}\{T(L', D) | T(L', D) \leq R\} \qquad (29)$$

L'' is the optimized subset of layers. $T(L', D)$ is the time complexity of encryption for layers L' and data D. R is the maximum allowable resource usage. Equation (29) ensures the algorithm adaptation to resource constraints while maintaining robust encryption. As per equation (30), the cumulative security level S_t achieved through the selected layers is:

$$S_t = \sum_{i \in L'} S_i \qquad (30)$$

S_t is the security contribution of the layer i. L is the selected layer. This ensures the total security level matches or exceeds the required level S.

Integrated Quantum-Inspired Secure Routing Framework algorithms are a robust mechanism that prevents grayhole attacks and guarantees data transfer in VANETs. It partitions the network into zones and utilizes quantum-inspired principles for zone-based communications to optimize routes based on quantum problem-inspired principles. This algorithm also provides the dynamic finding of optimal paths which is achieved at the cost of reliability using probabilistic decision making. The Dynamic Trust and Reputation Management Algorithm is used for the removal of malicious nodes in VANET using the evaluation of node behavior and preventing grayhole attack for security purposes. Thirdly, Adaptive Layered Quantum-Resilient Encryption Algorithm) utilizes multi-layered quantum resilient encryption so that the data is secured from extra-terrestrial or any domain. It constitutes an integrated solution to the problem of secure, efficient, attack-resilient data transmission and route optimization in VANETs. The working of ALQRE is depicted in figure 8 and algorithm 4.

Key Generation

Create keys using lattice-based techniques (such as NTRU or Learning with Errors (LWE)) are secure against quantum attacks.

Using these methods define the public key PK and private key SK.

Layered Encryption

Apply several quantum resistant algorithm encryption layers.

Each layer transforms the plaintext P into progressively encrypted forms:

$$C_1, C_2, \dots, C_n, \ \ Where\ C_i = Enc_i(C_i, PK_i)$$

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/31 Volume 12, Issue 4, July – August (2025)

RESEARCH ARTICLE

n, number of layers (or another parameter to control) is dynamically adjusted to the security requirements or computational capabilities.

Failures in decryption should be overloaded either by a fallback or the recovery mechanism.

Decryption

Reverse the encryption layers:

$$P = Dec_1(Dec_2(\dots Dec_n(C_n, SK_n) \dots, SK_2), SK_1)$$

Algorithm 4 Adaptive Layered Quantum-Resilient Encryption Algorithm

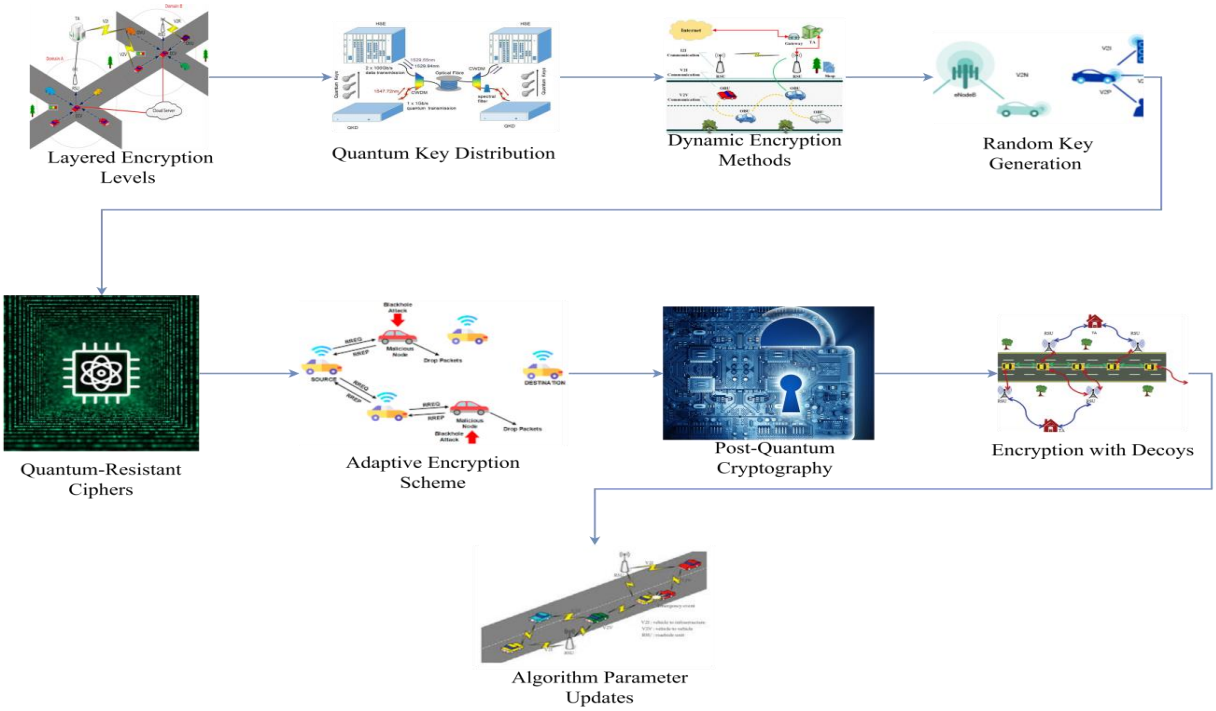

Figure 8 Adaptive Layered Quantum-Resilient Encryption Architecture

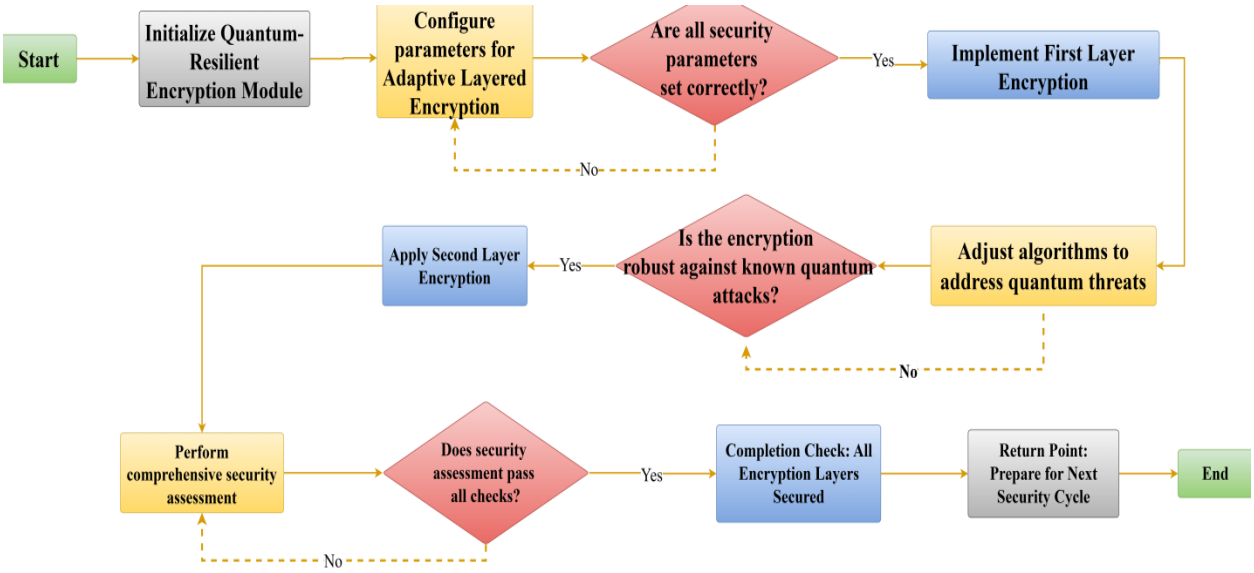

Figure 9 Flowchart of Adaptive Layered Quantum-Resilient Encryption

RESEARCH ARTICLE

Figure 9 describes the flowchart of the ALQRE method. In this method, encryption is done and adjusted. Again, encryption is carried out which further performs the security assessment.

4. RESULTS AND DISCUSSIONS

Furthermore, the Integrated Quantum-Inspired Secure Routing Framework is implemented to show the improvements in routing efficiency and security in VANET using the elements of quantum computing. Results show that the QZARP and QIPRA algorithms effectively optimized path selection, which reduced latency and improved route stability.

This focused on real-time grayhole attack identification and mitigation to improve the reliability of data transmission by neglecting the malicious nodes in real-time. Simultaneously, ALQREA has provided strong data protection against classical and quantum adversaries, protecting the integrity and confidentiality of transmitted information.

Overall, this framework offered a balanced approach to combine routing network optimization and security as well as boost the network performance, reduces packet loss and vulnerability to attacks. These outcomes identify quantum inspired routing techniques for the integration with more advanced mechanisms for VANETs security.

4.1. Performance Metrics

4.1.1. Throughput

Throughput computation refers to the process of assessing the transmission of efficient data via the network or system at a given moment. The information flow of data transmission is often shown in bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps) or even gigabytes per second (Gbps).

$$\text{Throughput} = \frac{N}{T \times S} \quad (31)$$

Where, N= Number of packet size, T= Time duration, S= Successful average Packet size. Equation (31) quantifies how well data or packets are delivered successfully via a network or communications system.

Table 2 Throughput Comparison

Throughput Levels					
Packet Size	ACO [3]	ANN [32]	DyTE [16]	Fuzzy [31]	IQSRF
50	0.169	0.211	0.239	0.356	0.632
100	0.360	0.429	0.440	0.561	0.761
150	0.516	0.664	0.719	0.836	0.946
200	0.708	0.861	0.891	0.971	1.134
250	0.965	1.079	1.201	1.235	1.540

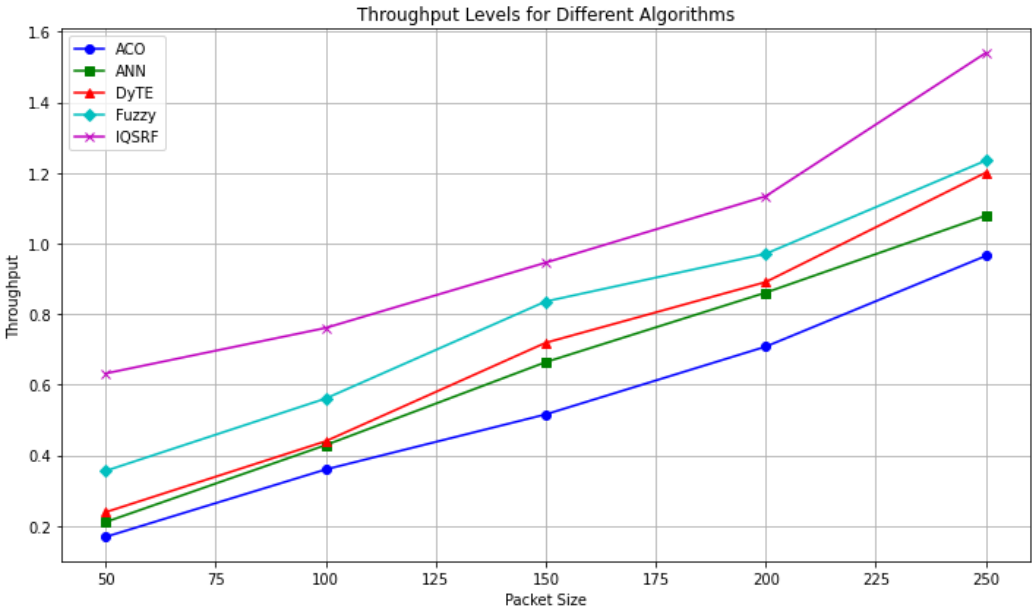

Figure 10 Throughput Levels Across Compared Algorithms

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/31 Volume 12, Issue 4, July – August (2025)

RESEARCH ARTICLE

Table 2 compares the throughput values among the different methods such as ACO, ANN, DyTE, Fuzzy and IQSRF. It reveals that the proposed IQSRF method has exhibited the highest through put values. Here, the packet sizes from 50 to 250 are utilized.

Throughput levels are compared in Figure 10 over the various algorithms. Packet sizes from 50 to 250 are represented on the X-axis, whereas the Y-axis indicates the throughput values.

4.1.2. Packet Delivery Ratio (PDR)

In networking, PDR is the performance metric of data transit reliability. It displays the fraction of successfully received packets to the total packet count. AS more packets are efficiently delivered, high PDR indicates improved network performance. It is calculated using equation (32):

$$PDR = \frac{R}{T} * 100 \quad (32)$$

R = Total number of packets received, T = Total number of packets.

Table 3 Packet Delivery Ratio Comparison

PDR					
Number of packets	ACO [3]	ANN [32]	DyTE [16]	Fuzzy [31]	IQSRF
50	96.64	97.03	97.87	98.01	98.25
100	97.31	97.50	98.00	98.21	98.85
150	97.45	97.87	98.01	98.31	99.05
200	98.10	98.01	98.14	98.45	99.42
250	98.12	98.72	98.90	99.20	99.70

Table 3 compares the PDR values with the packet sizes ranging from 50 to 250. Among the contrasted methods, the presented IQSRF approach performs better than the other approaches.

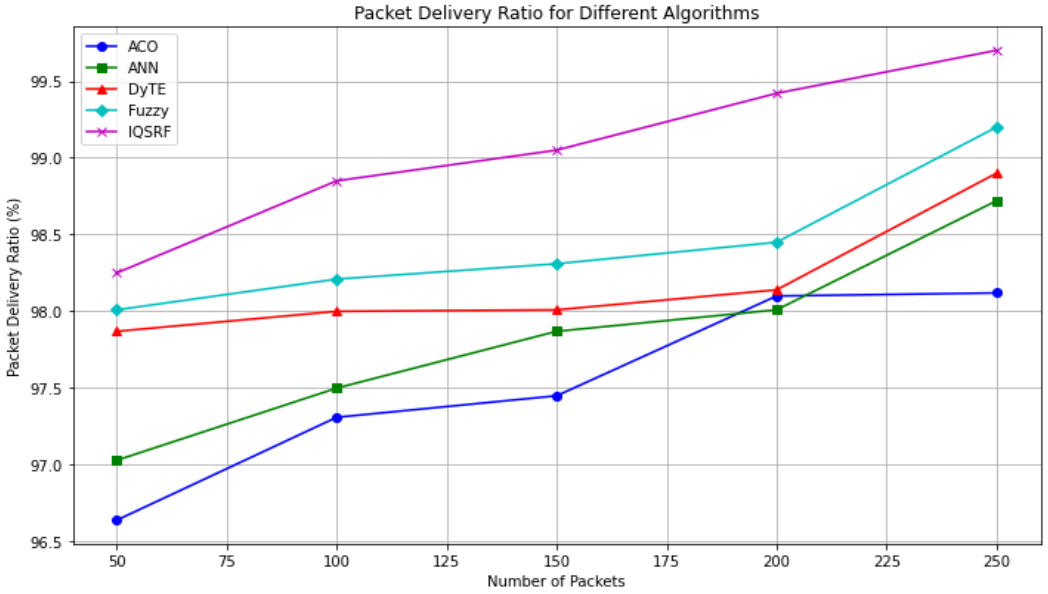

Figure 11 PDR Comparison

The compared PDR values in figure 11 show that the presented model has better formed than the other approaches. Here, Packet counts are represented on the X-axis while the PDR values are plotted on the Y-axis.

4.1.3. Time delay

Time delay seems to be calculated in a sensor network using sensor node count, energy utilization and forwarding time during data transmission.

$$\text{Time Delay} = \frac{NS}{E \times T} \quad (33)$$

NS= Number of sensor nodes, E=Energy consumption for sending packets at a times, T=Forwarding time in ms. Equation (33) describes how delay grows with more data and shrinks with more energy available and quicker transmission: If additional packets (N) or bigger packets (S) are being sent, delay grows. If the system is given more energy (E) or additional time (T) to send, delay shrinks.

End–to–end delay represented in Table 4 depicts the comparison among the various methods. Here, the presented IQSRF model outperforms the other methods.

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/31 Volume 12, Issue 4, July – August (2025)

RESEARCH ARTICLE

Table 4 Comparison of Time Delay

Time (End-to-End Delay)					
Number of Nodes	ACO [3]	ANN [32]	DyTE [16]	Fuzzy [31]	IQSRF
10	0.068	0.064	0.064	0.059	0.034
20	0.136	0.131	0.129	0.120	0.114
40	0.271	0.263	0.259	0.241	0.238
60	0.409	0.399	0.389	0.378	0.362
80	0.543	0.532	0.519	0.501	0.498
100	0.672	0.671	0.649	0.631	0.613

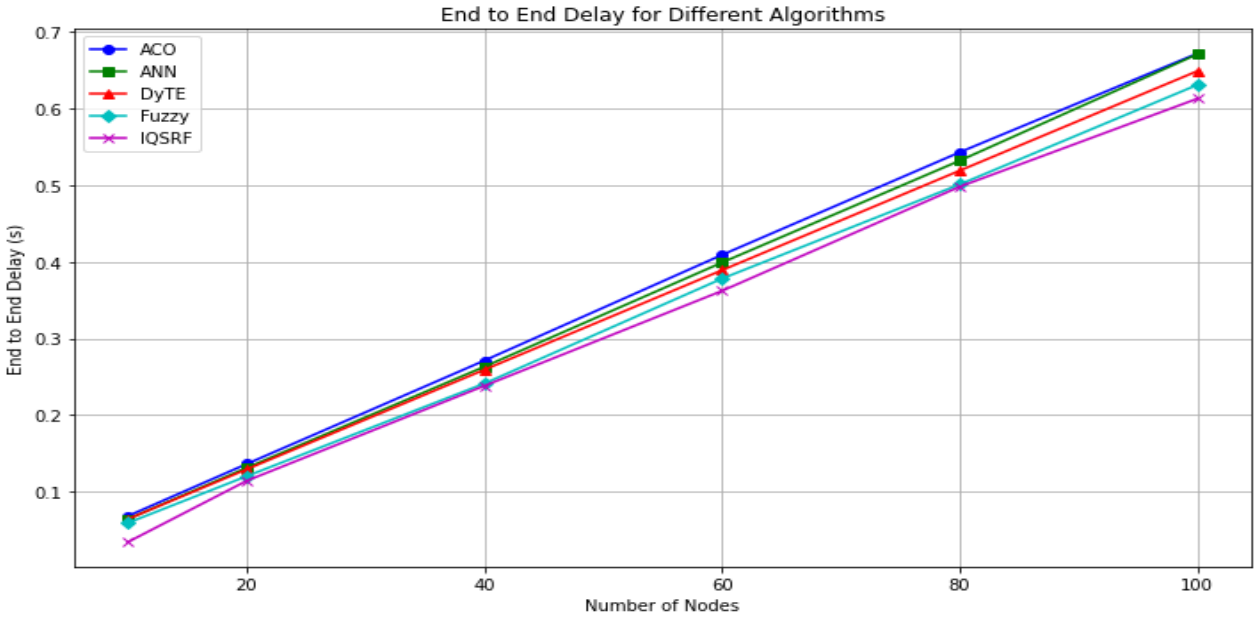

Figure 12 Time Delay Comparison

The compared delay values in figure 11show that the presented model has better formed than the other approaches. Here, Packet counts are represented on the X-axis while the delay values are plotted on the Y-axis.

4.1.4. Energy Consumption

Energy consumption refers to the evaluation of a system's or device's energy consumption for task performance. Energy performance is a critical element in networking and computing, particularly in resource-constrained environments like VANETs, which rely on battery-powered devices. The energy consumption is calculated using equation (34).

$$\text{Energy} = \frac{NS}{E} \times 100 \quad (34)$$

NS = Number of sensor nodes, E = Energy consumption for sending packets at a time.

Energy levels of the algorithms like ACO, ANN, DyTE, Fuzzy and ISQRF are compared in Table 5. The results have shown that the proposed method has revealed comparatively low energy levels. It indicates the outstanding performance of the presented method.

The comparison made in Figure 13 indicates the energy levels of the algorithms. Here, 10 to 100 nodes are taken into consideration. Out of the comparisons, the framed algorithm exhibits the lower energy levels.

RESEARCH ARTICLE

Table 5 Energy Level Comparison

Energy Level in Joules					
Number of Nodes	ACO [3]	ANN [32]	DyTE [16]	Fuzzy [31]	IQSRF
10	83	79	73	65	55
20	156	153	141	136	128
40	345	326	289	276	255
60	485	481	441	421	409
80	652	610	581	540	520
100	801	762	713	701	694

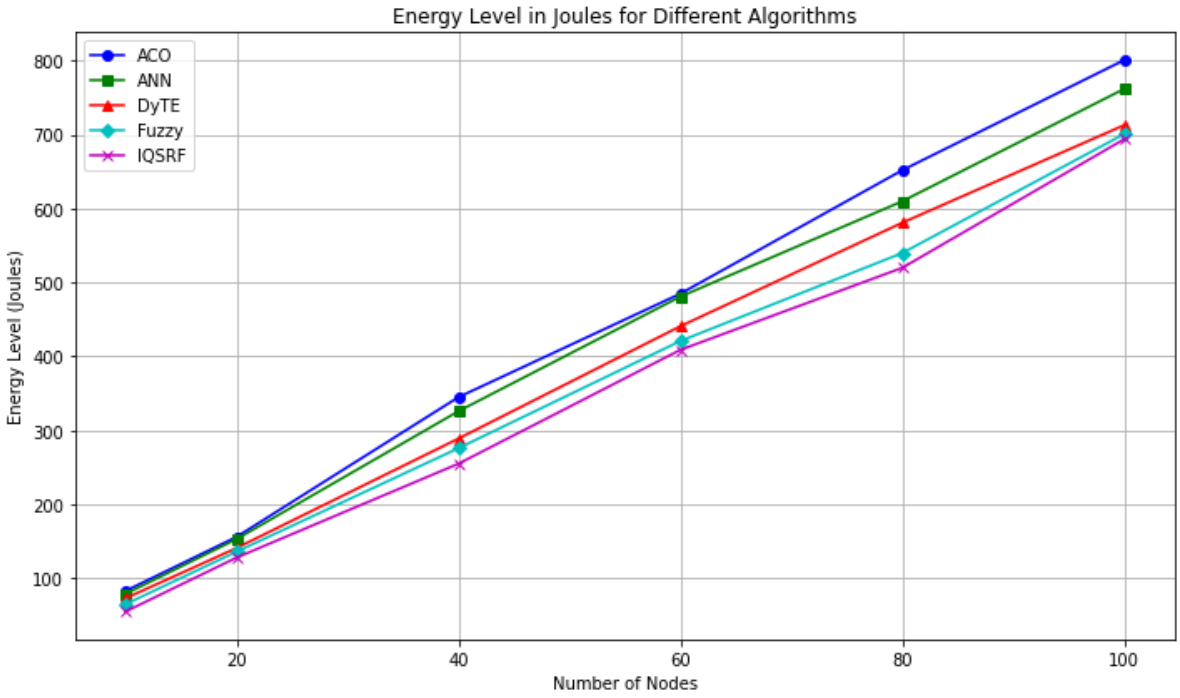

Figure 13 Comparison of Energy Levels in Joules

4.1.5. Grayhole Detection Rate

The Grayhole Detection Rate (GDR) is the ability to identify nodes that drop packets selectively when transmitting. It indicates that better isolation and identification of grayhole nodes lead to a higher detection rate, which guarantees effective data transmission. Equation (35) is used to calculate the GDR.

$$GDR = \frac{N_{detected}}{N_{total}} \times 100 \quad (35)$$

Where, $N_{detected}$ is the number of Grayhole nodes successfully detected by the system. N_{total} is the total number of actual Grayhole nodes present in the network. Detection rate levels of the algorithms like ACO, ANN, DyTE, Fuzzy and ISQRF are compared in Table 6. The results have shown that the proposed method has revealed comparatively high detection rate. It indicates the outstanding performance of the presented method. Comparison of grayhole detection rate is illustrated in figure 14. The number of nodes is indicated on the X-axis, whereas the detection rate of grayhole is indicated on the Y-axis.

RESEARCH ARTICLE

Table 6 Comparison of Grayhole Detection

Grayhole Detection Rate					
Number of Nodes	ACO [3]	ANN [32]	DyTE [16]	Fuzzy [31]	IQSRF
10	0.45	0.52	0.57	0.61	0.65
20	0.52	0.60	0.65	0.70	0.79
40	0.67	0.71	0.73	0.82	0.86
60	0.75	0.83	0.85	0.91	0.92
80	0.80	0.85	0.86	0.92	0.95
100	0.84	0.89	0.95	0.95	0.97

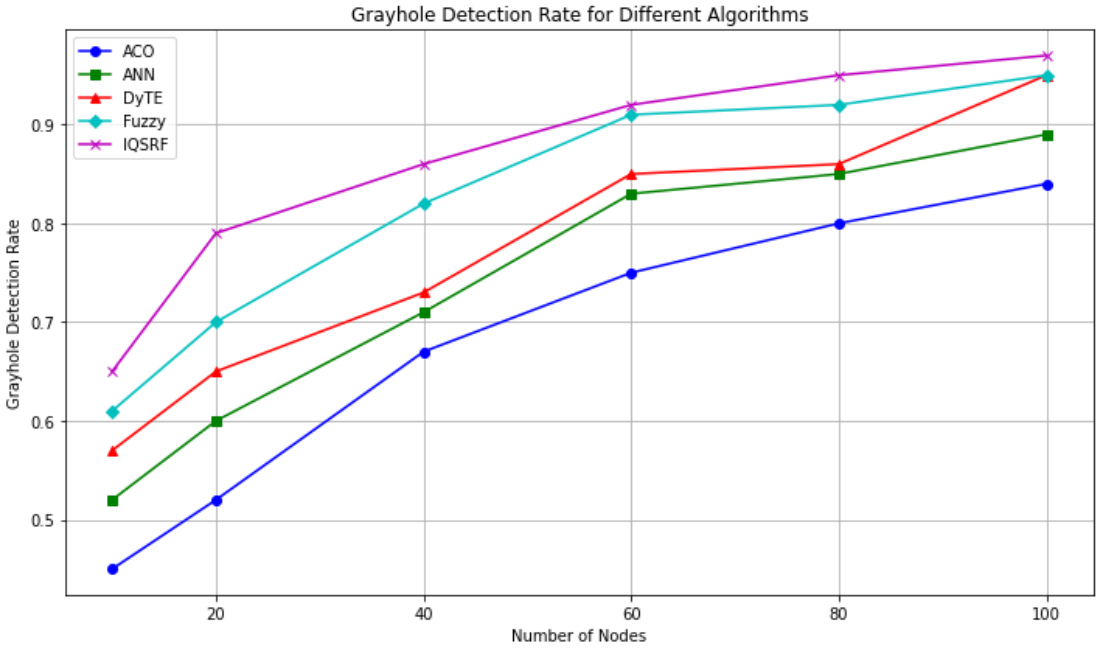

Figure 14 Grayhole Rate Comparison

4.2. Discussions

The improved performance of the proposed IQSRF architecture stems from its comprehensive characteristics, which greatly enhance the efficiency, reliability and security of VANET communications. QZARP facilitates scalable communication through adaptive partitioning by zones, which effectively optimizes routing overhead and response time for highly dynamic environments.

The Quantum-Inspired Probabilistic Routing Algorithm improves route reliability by choosing stable, yet reliable and routes with probabilistic models are best suited under high mobility conditions. The Dynamic Trust and Reputation Management Algorithm preserve network integrity by monitoring node behavior in real-time, allowing for real-time detection and dynamic isolation of grayhole attacks. In tandem, Adaptive Layered Quantum Resilient Encryption Algorithm maintains end-to-end data confidentiality and integrity by using multi-layered encryption with resistance to attacks at both the classical and quantum level. There is also optimization based on the feedback loop for real-time monitoring of performance and dynamic routing mechanism adjustments.

The combination of these elements in a single framework generates fewer packet losses, less latency and greater security resilience without compromising the scalability in large and rapidly expanding vehicular networks. Such benefits result from synergistic combinations of contributions summing to the enhanced performance under test conditions.

RESEARCH ARTICLE

5. CONCLUSION

By incorporating quantum-inspired principles into IQSRF, a more comprehensive and more adaptive solution to the challenges of VANETs has been proposed in this paper. The framework combines the Quantum-Inspired Zone Adaptive Routing Protocol and Quantum-Inspired Probabilistic Routing Algorithm to make efficient zone-based and reliable route selection. Meanwhile, the Dynamic Trust and Reputation Management Algorithm effectively prevents grayhole attacks by continuously sampling node behaviors and forbids the malicious nodes in the network. On the other hand, Adaptive Layered Quantum Resilient Encryption Algorithm enhances data security by offering multi-layered, quantum and classical computing threats resistant encryption. After deployment, these algorithms create a layered defense against the attacks for secure, reliable and efficient communication within VANETs. In addition to meeting the current routing and security challenges, the IQSRF framework sets the stage for future-proofing VANETs in the era of quantum computing, positioning it well to improve the performance and resiliency of VANETs in dynamic environments.

REFERENCES

[1] Gillani, M., Niaz, H. A., Farooq, M. U., & Ullah, A. (2022). Data collection protocols for VANETs: a survey. Complex & Intelligent Systems, 8(3), 2593-2622.

[2] Malik, A., Khan, M. Z., Faisal, M., Khan, F., &Seo, J. T. (2022). An efficient dynamic solution for the detection and prevention of black hole attack in VANETs. Sensors, 22(5), 1897.

[3] Goudarzi, F., Asgari, H., & Al-Raweshidy, H. S. (2018). Traffic-aware VANET routing for city environments—A protocol based on ant colony optimization. IEEE Systems Journal, 13(1), 571-581.

[4] Almutairi, H., Chelloug, S., Alqarni, H., Aljaber, R., Alshehri, A., &Alotaish, D. (2014, September). A new black hole detection scheme for VANETs. In Proceedings of the 6th International Conference on Management of Emergent Digital EcoSystems (pp. 133-138).

[5] Bibhu, V., Roshan, K., Singh, K. B., & Singh, D. K. (2012). Performance analysis of black hole attack in VANET. International Journal of Computer Network and Information Security (IJCNIS), 4(11), 47-54.

[6] Ourouss, K., Naja, N., & Jamali, A. (2021). Defending against smart grayhole attack within MANETs: A reputation-based ant colony optimization approach for secure route discovery in DSR protocol. Wireless Personal Communications, 116, 207-226.

[7] Yazdanypoor, M., Cirillo, S., & Solimando, G. (2024). Developing a Hybrid Detection Approach to Mitigating Black Hole and Gray Hole Attacks in Mobile Ad Hoc Networks. Applied Sciences, 14(17), 7982.

[8] Gowdhami, K. T., & Nithya, D. (2017). Design and analysis of secure VANET framework preventing sink hole and gray hole attack. International Journal of Advanced Trends in Engineering and Technology, 2(1), 55-59.

[9] Ali, S., Chaudhary, A., & Pasricha, H. (2020). A novel modified zone multicasting routing protocol for path establishment in VANET. Int J Comput Sci Netw, 9, 38-45.

[10] Brendha, R., & Prakash, V. S. J. (2018). Geographical Zone based Cluster Head for Routing in Sparse Vehicular Networks. International Journal of Engineering & Technology, 7(3), 1910-1914.

[11] Dharani, P., Chakkaravarthy, S. S., Ganesan, M., Kamalanaban, E., Visu, P., Patil, P. R., & Mahesh, C. (2015). An unidentified location-based efficient routing protocol in VANET. In Artificial Intelligence and Evolutionary Algorithms in Engineering Systems: Proceedings of ICAEES 2014, Volume 1 (pp. 415-421). Springer India.

[12] Mehdi, B., Moussaoui, S., & Mohamed, G. (2022, October). A geographic routing based on road traffic and multi-hop intersections in VANETs (GRBRT-MI). In 2022 2nd International Conference on Advanced Electrical Engineering (ICAEE) (pp. 1-6). IEEE.

[13] Lin, D., Kang, J., Squicciarini, A., Wu, Y., Gurung, S., &Tonguz, O. (2016). MoZo: A moving zone based routing protocol using pure V2V communication in VANETs. Ieee transactions on mobile computing, 16(5), 1357-1370.

[14] (Tabassum, M., & Oliveira, A. (2022). Cyber-resilient routing for internet of vehicles networks during black hole attack. Int. J. Wirel. Microw. Technol, 12, 1-14.)

[15] Abdalla, A. M., & Salamah, S. H. (2022). Performance comparison between delay-tolerant and non-delay-tolerant position-based routing protocols in VANETs. International Journal of Communications, Network and System Sciences, 15(1), 1-14.

[16] Kazi, A. K., & Khan, S. M. (2021). DyTE: An effective routing protocol for VANET in urban scenarios. Engineering, Technology & Applied Science Research, 11(2), 6979-6985.

[17] Husain, A., & Sharma, S. C. (2018). Implementation of geographical location-based routing protocols in vehicular environment. International Journal of System Assurance Engineering and Management, 9, 18-25.

[18] Kandali, K., & Bennis, H. (2020). An Efficient Routing Protocol Using an Improved Distance-Based Broadcasting and Fuzzy Logic System for VANET. International Journal of Intelligent Engineering & Systems, 13(6).

[19] Alheeti, K. M. A., Gruebler, A., & McDonald-Maier, K. D. (2015, September). On the detection of grey hole and rushing attacks in self-driving vehicular networks. In 2015 7th Computer science and electronic engineering conference (CEEC) (pp. 231-236). IEEE.

[20] Kaur, G., Khurana, M., & Kaur, A. (2022, November). Gray hole attack detection and Prevention system in vehicular adhoc network (VANET). In 2022 3rd International Conference on Computing, Analytics and Networks (ICAN) (pp. 1-6). IEEE.

[21] Ahmed, A. K., Abdulwahed, M. N., & Farzaneh, B. (2020). A distributed trust mechanism for malicious behaviors in VANETs. Indonesian Journal of Electrical Engineering and Computer Science, 19(3), 1147-1155.

[22] Hassan, Z., Mehmood, A., Maple, C., Khan, M. A., &Aldegheishem, A. (2020). Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles. IEEE Access, 8, 199618-199628.

[23] Hassan, S. M., Mohamad, M. M., &Muchtar, F. B. (2024). Advanced Intrusion Detection in MANETs: A Survey of Machine Learning and Optimization Techniques for Mitigating Black/Gray Hole Attacks. IEEE Access.

[24] Alabdulatif, A., Alharbi, M., Mchergui, A., &Moulahi, T. (2024). Mitigating Blackhole and Greyhole Routing Attacks in Vehicular Ad Hoc Networks Using Blockchain Based Smart Contracts. CMES-Computer Modeling in Engineering & Sciences, 138(2).

[25] Hayat, S., Liu, X., Li, Y., & Zhou, Y. (2019, May). Comparative analysis of vanet's routing protocol classes: an overview of existing routing protocol classes and futuristic challenges. In 2019 IEEE 2nd International Conference on Electronics Technology (ICET) (pp. 1-7). IEEE.

[26] Mianji, E. M., Muntean, G. M., & Tal, I. (2023, June). Trustworthy routing in VANET: a Q-learning approach to protect against black hole and gray hole attacks. In 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring) (pp. 1-6). IEEE.

[27] Naeem, A., Rizwan, M., Alsubai, S., Almadhor, A., Akhtaruzzaman, M., Islam, S., & Rahman, H. (2023). Enhanced clustering-based routing protocol in vehicular ad-hoc networks. IET Electrical Systems in Transportation, 13(1), e12069.

[28] Nair, C. R. (2016). Analysis and comparative study of topology and position-based routing protocols in VANET. International journal of Engineering Research and general science, 4(1), 43-52.

RESEARCH ARTICLE

[29] Nandagopal, C., Kumar, P. S., Rajalakshmi, R., &Anandamurugan, S. (2023). Mobility Aware Zone-Based Routing in Vehicle Ad hoc Networks Using Hybrid Metaheuristic Algorithm. Intelligent Automation & Soft Computing, 36(1).
[30] Nazar, K., Saeed, Y., Ali, A., Algarni, A. D., Soliman, N. F., Ateya, A. A., ... & Jamil, F. (2022). Towards intelligent zone-based content pre-caching approach in VANET for congestion control. Sensors, 22(23), 9157.
[31] Rahimi, S., &Jabraeil Jamali, M. A. (2019). A hybrid geographic-DTN routing protocol based on fuzzy logic in vehicular ad hoc networks. Peer-to-Peer Networking and Applications, 12, 88-101.
[32] Rani, P., Verma, S., & Nguyen, G. N. (2020). Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network. IEEE access, 8, 121755-121764.
[33] Rathod, A., & Patel, S. (2017). A survey on black hole & gray hole attacks detection scheme for vehicular ad-hoc network. International Research Journal of Engineering and Technology, 4(11), 1508-1511.
[34] Saleh, M. (2022). Secure optimized request zone location-aided routing protocols with Wi-Fi direct for vehicular ad hoc networks. Journal of Communications, 17(3), 156-166.
[35] Saleh, M. E. (2019). Secure tilted-rectangular-shaped request zone location-aided routing protocol (STRS-RZLAR) for vehicular ad hoc networks. Procedia Computer Science, 160, 248-253.
[36] Schweitzer, N., Stulman, A., Margalit, R. D., & Shabtai, A. (2016). Contradiction based gray-hole attack minimization for ad-hoc networks. IEEE Transactions on Mobile Computing, 16(8), 2174-2183.
[37] Shi, J., Wang, X., Huang, M., Li, K., & Das, S. K. (2017). Social-based routing scheme for fixed-line VANET. Computer Networks, 113, 230-243.
[38] Shoaib, M., & Song, W. C. (2013, September). Traffic aware optimized zone based hierarchal link state routing protocol for VANET. In 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (pp. 3117-3122). IEEE.
[39] Tassoult, N., Amad, M., MOUMEN, H., & Kalla, H. (2019). A Survey on vehicular ad-hoc networks routing protocols: classification and challenges. Journal of Digital Information Management, 17(4), 227.
[40] Umre, S. A., Mehta, K., & Malik, L. (2014, December). Performance improvement of communication in zone-based routing that uses cluster formation and bio-inspired computing in VANET. In 2014 IEEE International Conference on Vehicular Electronics and Safety (pp. 147-151). IEEE.
[41] Wahid, I., Ikram, A. A., Ahmad, M., Ali, S., & Ali, A. (2018). State of the art routing protocols in VANETs: A review. Procedia computer science, 130, 689-694.
[42] Yazdanypoor, M., Cirillo, S., & Solimando, G. (2024). Developing a Hybrid Detection Approach to Mitigating Black Hole and Gray Hole Attacks in Mobile Ad Hoc Networks. Applied Sciences, 14(17), 7982.
[43] Yelure, B., Patokar, A., Patil, S., Mawale, R., Nemade, S., & Gaikwad, V. (2024). Impact and Analysis of Attacks on Routing Protocols in Vehicular Ad hoc Network (VANET): Assessing Security Threats. IEIE Transactions on Smart Processing & Computing, 13(3), 294-302.
[44] Younas, S., Rehman, F., Maqsood, T., Mustafa, S., Akhunzada, A., & Gani, A. (2022). Collaborative detection of black hole and gray hole attacks for secure data communication in VANETs. Applied Sciences, 12(23), 12448.

Authors

Mrs. V. Sakthi Priyanka is a full-time Ph.D. Research Scholar in the Department of Computer Science at Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India. She holds a Bachelor of Science (B.Sc.) degree in Computer Science from VLB Janakiammal College of Arts and Science, Coimbatore, and both a Master of Science (M.Sc.) and Master of Philosophy (M.Phil.) in Computer Science from Sri Krishna Arts and Science College, Coimbatore. Her M.Phil. research focused on "Efficient Energy Consumption Using Dynamic Watchdog Optimization in Wireless Sensor Networks." Her current research interests include Vehicular Ad-Hoc Networks (VANETs), Wireless Sensor Networks (WSNs), Mobile Ad-Hoc Networks (MANETs), and Network Security. She has presented papers at national and international conferences and published research articles in peer-reviewed journals. She also has six years of teaching experience.

Dr. V. Radha is currently serving as the Dean of the School of Physical Sciences and Computational Sciences and as a Professor in the Department of Computer Science at Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India. With over 36 years of teaching experience, she has been actively engaged in research since 1999. Her research interests include Image Processing, Optimization Techniques, Speech Signal Processing, Data Mining, Data Warehousing, and Relational Database Management Systems (RDBMS). Dr. Radha has authored six books, contributed 16 book chapters, and published more than 166 research papers in reputed international journals and conference proceedings. She has received five Best Paper Awards at IEEE, Springer, and Elsevier conferences. She has also completed funded research projects under UGC-MRP and DST-WOS (A) schemes. She serves as a reviewer for journals including the American Journal of Operational Research and the American Journal of Signal Processing, and is the Editor-in-Chief of the International Journal of Computational Science and Information Technology (IJCSITY). Dr. Radha is a member of several international professional organizations such as IEEE, IAENG, AIRCC, IACSIT, and STRA. She holds a patent titled "A Device for Converting E-text to Refreshable Braille Display." Her academic contributions have taken her to international conferences in the USA, UK, and Singapore, where she has also chaired technical sessions.

How to cite this article:

V. Sakthi Priyanka, V. Radha, "Quantum -Inspired and Probabilistic Zone Adaptive Routing Protocol for Gray Hole Attack Detection in VANETS", International Journal of Computer Networks and Applications (IJCNA), 12(4), PP: 500-522, 2025, DOI: 10.22247/ijcna/2025/31.