ENHANCING SECURITY IN THE IOV: A QUANTUM-BASED SOLUTION

Krishna geetha Karuppasamy, Abinash Borah, Anirudh Paranjothi, and Johnson P Thomas

Department of Computer Science, Oklahoma State University, Stillwater, OK 74075, USA.

ABSTRACT

The Internet of Vehicles (IoV) offers various services for road safety and user comfort. However, they face security vulnerabilities such as false data injections which need to be mitigated for public safety. The security solutions for IoV should have minimal processing delay and be scalable to deal with the large-scale IoV. While classical machine learning techniques have been adopted for malicious node detection in IoV, these solutions face computational challenges and scalability limitations. To deal with these challenges, in this paper, we propose a novel quantum-based MaxCut graph detection mechanism for identifying malicious nodes transmitting false messages in IoV. As validated by the performance evaluation results, the proposed quantum-based detection approach offers significantly lower data processing delay compared to the classical approach, especially as the data size increases.

KEYWORDS

Internet of vehicles, security, false message detection, quantum

1. INTRODUCTION

The Internet of Vehicles (IoV) represents a significant advancement over traditional Vehicular Ad Hoc Networks (VANETs), enabling seamless real-time communication between vehicles (V2V), between vehicles and roadside infrastructure (V2I), and cloud services. These networks offer diverse services; they enhance road safety, improve traffic efficiency, and deliver real-time updates on traffic conditions, accidents, and emergency events.

Vehicles within this system are equipped with On-Board Units (OBUs), which facilitate the transmission and reception of messages from other vehicles and the roadside infrastructure. The roadside infrastructure comprises of Road-Side Units (RSUs) strategically deployed along roadways, cameras, sensors, and traffic lights. Together, these components ensure efficient information dissemination and network reliability [1]. The IoV system underpins essential applications, including traffic management, collision avoidance, and autonomous driving, contributing to safer and more efficient transportation systems. However, the open and dynamic nature of IoV introduces significant security vulnerabilities [2]. Threats such as false data injection and malicious node activities pose considerable risks, potentially compromising communication reliability, degrading network performance, and endangering public safety.

To address these challenges, researchers have explored various anomaly detection and intrusion prevention mechanisms. Classical machine learning algorithms such as Gradient Boosting

David C. Wyld et al. (Eds): CMLA, CSEIT, NLPD, GRAPH-HOC, SPM, NeTCoM, NCS, ArIT, DMSE – 2025
pp.207 -223, 2025. CS & IT - CSCP 2025 DOI: 10.5121/csit.2025.151317

Decision Trees (GBDT) [3] and Random Forests have been employed for traffic anomaly detection and falsification prevention, demonstrating commendable accuracy. Additionally, vehicle consensus and clustering techniques such as K-means++ have further improved false message separation by optimizing centroid initialization. However, these methods face computational bottlenecks, scalability limitations, and delays when applied to large-scale, real-time IoV environments.

Recent advancements in quantum computing have opened new possibilities for overcoming these limitations. Quantum algorithms, particularly those leveraging Variational Quantum Eigen solvers (VQE) and quantum clustering frameworks, offer computational advantages in efficiently solving combinatorial optimization problems [4]. The Maximum Cut (MaxCut) problem [5], a well-known NP-hard problem in graph theory, has been effectively addressed using quantum approaches to partition graph nodes based on trust and communication metrics. This formulation is highly suitable for distinguishing between honest and malicious nodes in IoV, where each node represents a vehicle, and edges represent communication or trust-based connections.

Our approach formulates node classification as a graph partitioning problem, leveraging trust metrics, vehicle speed, accelerations, and position as edge weights. By employing a hybrid quantum-classical Variational Quantum Eigen solver (VQE) algorithm, we optimize graph partitions to separate rogue and legitimate nodes with minimal data processing delay and high accuracy.

In this paper, we propose a novel quantum-based MaxCut graph detection mechanism for identifying malicious nodes transmitting false or misleading messages within IoV networks. In highly dynamic vehicular environments, ensuring the authenticity and reliability of shared information such as position, speed, and traffic alerts is critical for maintaining safety and communication integrity. However, the open and decentralized nature of IoV systems makes them particularly vulnerable to adversarial behaviors, where compromised or rogue nodes may inject falsified data to disrupt network operations or mislead nearby vehicles.

To address this challenge, our approach reformulates the problem of malicious node detection as a graph-based clustering task. Each vehicle node is represented as a vertex in a fully connected, weighted graph, where edge weights are computed using a combination of trust metrics, relative speed, acceleration, and positional information. These weights reflect the similarity or dissimilarity between pairs of nodes and serve as input to a MaxCut formulation, aiming to partition the graph into two disjoint sets such that the sum of weights across the cut is maximized. This setup naturally encourages the separation of honest and malicious nodes based on anomalous behavior patterns.

To solve the MaxCut problem efficiently, we adopt a hybrid quantum-classical optimization strategy using the Variational Quantum Eigensolver (VQE) algorithm. The MaxCut cost function is encoded as a quantum Hamiltonian, and a parameterized quantum circuit (ansatz) is optimized to find a low-energy eigenstate, corresponding to an optimal or near-optimal cut. By leveraging the expressive power of quantum computing and the flexibility of classical optimizers, our framework achieves robust classification with minimal data processing latency a critical requirement in real-time vehicular networks. The proposed method exhibits the following key advantages, which are the contributions to this work:

1. The quantum MaxCut algorithm dynamically adjusts to the ever-changing nature of IoV.
2. Incorporating multiple trust metrics into edge weight calculations improves detection accuracy while maintaining computational efficiency.

3. The use of quantum algorithms offers faster convergence and scalability compared to traditional clustering methods like K-means++.

We validate our approach using numerical simulations conducted on IBM's Statevector Simulator. Performance is evaluated using standard metrics such as accuracy, True Positive Rate (TPR), F1 score, and execution time. The results demonstrate that the proposed quantum clustering method consistently outperforms classical approaches across varying proportions of malicious nodes, maintaining high accuracy and robust scalability.

The rest of this paper is organized as follows: Section 2 discusses related work; Section 3 details the proposed quantum-based detection technique; Section 4 presents performance evaluation results; and finally, Section 5 provides the conclusions.

2. RELATED WORK

In [6], a hybrid approach is proposed to detect false messages on the IoV by combining traffic anomaly detection, vehicle consensus mechanisms, and data clustering. Gradient Boosting Decision Trees (GBDT) analyze time-series data to predict normal vehicle densities and identify anomalies by comparing predicted and observed values, while Practical Byzantine Fault Tolerance (PBFT) validates unclear anomalies through consensus among vehicles. The K-means++ clustering algorithm then separates malicious from benign messages by analyzing deviations from cluster centroids, optimizing centroid initialization probabilistically to improve clustering accuracy and reduce suboptimal results. However, the computational demands of GBDT and PBFT can introduce latency, and while K-means++ enhances clustering precision, it requires higher computational cost compared to the traditional K-means algorithm.

Reference [7] proposes a method for detecting and preventing false nodes and messages in VANETs by leveraging a combination of mesh network structures and profile-based evaluation techniques. The mesh network ensures consistent connectivity and reduces the risk of frequent disconnections. Nodes are monitored using profiles that include attributes such as vehicle ID, make, model, location, and performance history, which are evaluated through a reward/penalty system. Nodes that fail to meet the defined threshold are reported as fake to RSUs and eliminated. To prevent the propagation of malicious data, messages are similarly assessed using their profiles, which include attributes like message ID, routing details, and reward/penalty scores. Messages identified as fake are promptly removed from the network, enhancing overall communication reliability. The limitation of this approach includes lack of scalability and infrastructure dependance resulting in large propagation delays.

In [8], the Randomized Search Optimization-based Ensemble Falsification Detection System (RSO-FDS) was proposed. This system leverages an ensemble Random Forest (RF) classifier, enhanced with hyperparameter tuning through Randomized Search Optimization (RSO**)**, to detect falsified data in (IoV). The model evaluates Basic Safety Messages for anomalies and disseminates alerts across the IoV network. Performance was assessed using datasets such as VeReMi, BurST-ADMA, and V2X. fabrication. Despite its strengths, the RSO-FDS requires hyperparameter tuning, a computationally intensive process that introduces high latency, making it less suitable for the real-time demands of VANETs. While the model demonstrates strong performance in addressing known falsification scenarios, its scalability and adaptability to the dynamic and evolving IoV environment remain uncertain.

In [9] the Secure Vehicular Quantum Communication Protocol (SVQCP) is proposed as a security mechanism that leverages the entanglement property of qubits, a fundamental principle of quantum mechanics, to prevent collisions and detect falsification in vehicular networks. The

protocol ensures the secure distribution of shared traffic signals using Quantum Fourier Transform (QFT). The Traffic Control System (TCS) generates a single secret signal and securely distributes portions of it to participating vehicles. These vehicles then collaborate to reconstruct the original signal. Successful reconstruction verifies their legitimacy, while any failure in this process identifies the vehicle as falsified or dishonest. Though the method ensures secure and reliable communication, the protocol demands significant quantum resources, which poses challenges for scalability.

In [10], the authors propose a hybrid quantum-classical intrusion detection system that integrates the strengths of quantum computing and classical machine learning is proposed. Their approach utilizes Quantum Neural Networks (QNNs), beginning with the encoding of features into quantum states, followed by the design of a parameterized quantum circuit optimized iteratively to minimize a loss function. The system demonstrates strong performance, reducing computational time and overhead while maintaining high detection accuracy compared to traditional neural networks. However, while the model excels at detecting well-known attack patterns, the dynamic and unpredictable nature of VANETs demands a more adaptable and resilient system capable of identifying emerging and previously unseen threats in real time.

Reference [11] introduces three hybrid quantum KMeans algorithms that enhance clustering efficiency by integrating quantum computation into key steps. Quantum circuits calculate Euclidean distances using amplitude encoding and FF-QRAM, while the centroid update step remains classical, and the cluster assignment step is accelerated with quantum circuits. The three variants: *q1*:1-KMeans, *q1*, and *qM* differ in how they handle record-to-centroid assignments, either one-to-one, one-to-many, or many-to-many. Preprocessing with Inverse Stereographic Projection reduces feature dimensions and improves centroid initialization. However, the method relies heavily on post-selection, where invalid quantum states are discarded after measurement. As the number of qubits increases, the quantum state space grows exponentially, reducing the probability of obtaining valid results. This issue worsens when data sizes do not align with powers of two, causing misalignment with the quantum circuit structure and increasing invalid outcomes. Consequently, repeated circuit executions are required, impacting both efficiency and scalability.

These studies have several common limitations that include high computational overhead, scalability constraints, dependence on extensive infrastructure, and challenges adapting to the dynamic nature of IoV networks. Many classical methods introduce significant latency (e.g., GBDT, RSO-FDS) and face difficulties in large-scale deployment (e.g., profile-based evaluation). While quantum-based approaches demonstrate potential, they encounter scalability issues due to hardware limitations and inefficiencies associated with post-selection.

To address the above challenges in detecting malicious nodes within the IoV, we propose a novel quantum-enhanced MaxCut clustering method. This approach leverages the adaptability and computational efficiency of quantum algorithms to effectively identify and isolate malicious nodes in IoV networks. By integrating quantum computing principles, our method aims to enhance detection accuracy and scalability, addressing the limitations of classical approaches in dynamic and large-scale IoV environments. Unlike classical clustering techniques, which may struggle with the dynamic and unpredictable nature of IoV topologies, our method seamlessly adjusts to changes in network structure, ensuring robust detection capabilities in highly mobile environments. The integration of quantum-enabled MaxCut algorithms brings significant computational advantages over classical methods. Quantum algorithms excel at handling large and complex graph structures with improved scalability, making them particularly well-suited for large-scale IoV deployments where node density and communication patterns vary frequently.

Moreover, the computational efficiency of our quantum-based method is independent of feature dimensions, ensuring robust performance even as the complexity of the data increases.

3. METHODOLOGY

The proposed quantum-enabled clustering method targets the classification of nodes in Internet of Vehicles (IoV) environments by leveraging the MaxCut framework a classical NP-hard problem in combinatorial optimization. In this context, the MaxCut problem seeks to divide a network of vehicles into two disjoint clusters (e.g., honest vs. malicious) such that the sum of dissimilarities (edge weights) between nodes in opposite clusters is maximized. In the IoV context, this corresponds to identifying an optimal separation between potentially malicious and honest nodes based on their behavioural or contextual features.

In classical computing, the time complexity of solving the MaxCut problem is $O(n^3)$, which can become computationally prohibitive in the dynamic and time-sensitive environment of IoV. These networks demand real-time decision-making, where delays can compromise communication reliability and network performance. We Propose a quantum-based approach to solve the MaxCut problem and apply it to the classification of nodes in IoV. By leveraging quantum algorithms, we can efficiently partition the graph representing the network into two groups, distinguishing between honest and malicious nodes. This quantum approach provides a significant advantage in handling the dynamic and time-sensitive nature of IoV, offering faster and more accurate solutions compared to traditional methods.

3.1. Problem Mapping: MaxCut Formulation for Clustering of IoV Nodes

Let $D = \{x_1, x_2 \dots x_n\}$ denote the set of IoV node's data, where each $x_i \in R^d$ is a feature vector representing the i^{th} vehicle and d is the feature vector dimension. These features may include physical and behavioral attributes such as position, velocity, acceleration, and direction. To ensure that all features contribute proportionally to the clustering process, we apply min-max normalization to each dimension of the feature vectors:

$$x'_{ij} = \frac{x_{ij} - \min(x_j)}{\max(x_j) - \min(x_j)} \quad (1)$$

Where x_{ij} is the j^{th} feature of the i^{th}node, and $\min(x_j), \max(x_j)$ are the minimum and maximum values of feature j across the dataset. This normalization rescales all features to the range [0,1], ensuring that features with large numeric ranges (e.g., position) do not dominate over others (e.g., acceleration).

Using the normalized vectors, we compute the pairwise distances $w_{ij} = dist(x_i, x_j)$. (using Euclidean distance) to quantify behavioural dissimilarity between vehicles. We use Euclidean distance quantify differences in position, speed and acceleration:

$$w_{ij} = \sqrt{\sum_k (x_{ik} - x_{jk})^2} \quad (2)$$

Where w_{ij} distance between i^{th} and j^{th} feature vector, $x_{ik,}$ x_{jk} are the k^{th} feature (e.g., speed) of node i and j respectively. Higher weights indicate greater behavioral divergence.

Attributes such as GPS consistency, message frequency, and signal strength play a critical role in refining edge weights to enhance detection accuracy. For instance, a malicious node attempting to

spoof its location may exhibit discrepancies between its reported GPS coordinates and positions inferred via neighboring node, resulting in elevated edge weights to honest vehicles. Similarly, sudden acceleration or deceleration spikes inconsistent with surrounding traffic patterns can further increase these weights, signaling anomalous behavior.

These distances define the edge weights in an undirected, weighted graph $G = (V, E)$, where each node $v_i \in V$ corresponds to vehicle v_i, and each edge $(i, j) \in E_{ij}$ is weighted by w_{ij}. This graph structure provides the basis for formulating the MaxCut clustering problem. Figure 1 illustrates the MaxCut problem representation of IoV environment.

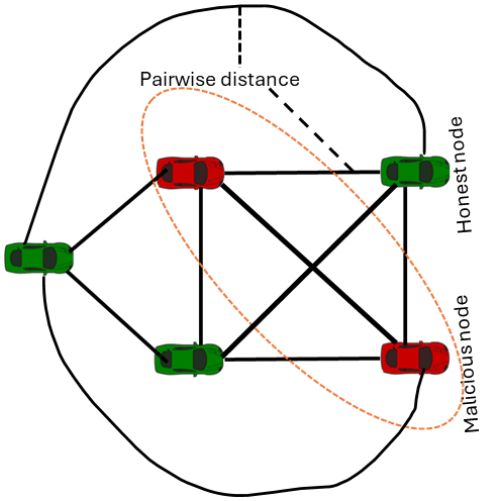

Figure 1 Malicious node detection in IoV using MaxCut

Traditional machine learning methods such as KMeans, Gradient Boosting Decision Trees (GBDT), and Random Forests are inherently limited when applied to the highly dynamic nature of the Internet of Vehicles (IoV). These approaches operate on static datasets and are not designed to update their internal state in real time. In environments where vehicle behaviour (e.g., speed, acceleration, GPS position) can change every second, such models struggle to incorporate new data without complete or partial retraining, leading to significant delays.

To support the highly dynamic nature of IoV environments, our model continuously recalculates these edge weights in real time. As vehicles move, change speed, or experience connectivity fluctuations, the feature vectors are updated at regular time intervals, and the graph representation is refreshed accordingly. This ensures that transient malicious behaviors such as short bursts of false data injections are not overlooked, while persistent anomalies are reinforced through consistently elevated edge weights.

By contrast to the traditional approach, our proposed quantum-based MaxCut approach recalculates edge weights in real time and reformulates the graph as a Hamiltonian, which is then solved using a variational quantum eigensolver (VQE). This allows the model to adapt instantly to transient anomalies without costly reprocessing, enabling rapid detection of both short-lived and persistent malicious behaviors. This dynamic adaptivity, coupled with the efficient structure of quantum circuits, offers a substantial advantage over classical approaches in real-time IoV security scenarios.

Once the updated weight matrix is established, the graph is re-encoded into the MaxCut Hamiltonian and passed through the VQE. The quantum component thus operates on the most

recent behavioral snapshot of the network, allowing for timely and accurate partitioning of malicious and honest nodes. This tight feedback loop between real-time edge weight updates and quantum optimization enables the system to maintain robust detection accuracy under fast-changing conditions, making it especially well-suited for real-world vehicular network security scenarios.

In [11], the classical MaxCut cost function C is given by:

$$C = \frac{1}{2}\sum_{(i,j)\epsilon\, E} w_{ij}\left(1 - \sigma_z^i \sigma_z^j\right) \quad (3)$$

Wherew_{ij} is a pairwise similarity distance. $\sigma_z \epsilon \{+1, -1\}$. The term $w_{ij}\left(1 - \sigma_z^i \sigma_z^j\right)$ in the cost function C evaluates how the edge weight w_{ij} contributes to the total energy based on the nodes assignments as follows:

Case(i): $\sigma_z^i \neq \sigma_z^j$ nodes i and j belong to different clusters and the term $\left(1 - \sigma_z^i \sigma_z^j\right)$ becomes 2. In this case, the energy contribution corresponding to the vertex is maximized.

Case(ii): $\sigma_z^i = \sigma_z^j$ nodes i and j belong to the same cluster and the term $\left(1 - \sigma_z^i \sigma_z^j\right)$ becomes 0. In this case, the energy contribution corresponding to the vertex is zero.

By finding the optimal separation of the nodes we will get the maximum value of C. Finding all the combinations of clustering using the brute force approach is impractical for larger networks. So, we convert this cost function into the quantum framework.

3.2. Quantum Reformulation: Hamiltonian Encoding

In quantum mechanics, a Hamiltonian (H) represents the total energy of a system, including both kinetic and potential energies. For computational problems like MaxCut, the Hamiltonian is mathematically constructed so that its ground state (lowest energy state) corresponds to the optimal solution of the problem. This mapping is made possible by translating the MaxCut problem into a physical system where different states represent possible solutions, and the energy levels correspond to the cost function values of those solutions.

Quantum computer is designed to find minima (typically the lowest energy state of a system) rather than maxima. Therefore, instead of directly maximizing the objective function C in the MaxCut problem, we minimize a corresponding Hamiltonian H.

$$Min\ H = -C \quad (4)$$

In Equation 2, Hamiltonian is constructed to encode the MaxCut problem such that minimizing its energy corresponds to maximizing the cut.

3.3. Illustrative Example: MaxCut Hamiltonian Construction from IoV Data

To demonstrate the proposed method, consider a simple Internet of Vehicles (IoV) environment with three vehicles, each characterized by two features**:** position (in coordinates) and speed (in miles per hour)**.**

Step 1: *Feature Extraction and Normalization*

let the feature vectors are: $x_0 = [100, 30]$, $x_1 = [200, 40]$, $x_2 = [150, 80]$ Applying min-max normalization feature-wise:

- For position: $\min = 100,\ \max = 200$
- For speed: $\min = 80,\ \max = 30$

The normalized feature vectors are:
$x'_2 = \left[\frac{150-100}{200-100},\ \frac{80-30}{80-30}\right] = [0.5,1]$ like wise $x'_0 = [0,0]$ and $x'_1 = [1,0.2]$

Step 2: *Distance matrix calculation*
Compute the distance between x_0 and x_1

$w_{01} = \sqrt{(0-1)^2 + (0-0.2)^2} = 1.02$, like wise $w_{12} = 0.94,\ w_{02} = 1.12$
The distance matrix $W = \begin{bmatrix} 0 & 1.02 & 1.12 \\ 1.02 & 0 & 0.94 \\ 1.12 & 0.94 & 0 \end{bmatrix}$

Step 3: *Classical MaxCut Cost Function*
cost function $C = \frac{1}{2}\ [1.02(1 - \sigma_z^0\sigma_z^1) +\ 1.12(1 - \sigma_z^0\sigma_z^2) + 0.95(1 - \sigma_z^1\sigma_z^2)]$

$$C = 1.54 - 0.54\ \sigma_z^0\sigma_z^1 - 0.56\ \sigma_z^0\sigma_z^2 - 0.47\sigma_z^1\sigma_z^2$$

Step 4: *Hamiltonian Construction for Quantum Solver*
The problem Hamiltonian is defined as: $H = -C$, $H = 0.54Z_0Z_1 + 0.56Z_0Z_2 + 0.47Z_1Z_2 - 1.54I$ Where: $Z_0, Z_{1,}Z_2$ are Pauli Z operator acting on the corresponding qubit.

3.4. Quantum implementation

To find the ground state energy of H and its corresponding ground state we use the Variational Quantum Eigen solver (VQE) algorithm, leveraging quantum principles to efficiently optimize the separation. The VQE is a hybrid quantum-classical algorithm designed to find the ground state energy of a Hamiltonian efficiently. In this method, A quantum circuit is constructed to represent the trial wavefunction $|\psi(\theta)\rangle$, where θ is a set of adjustable parameters. This circuit is known as an ansatz.

The ansatz prepares the state $|\psi(\theta)\rangle$ and measures the expectation value of the Hamiltonian $\langle\psi(\theta)|H\ |\psi(\theta)\rangle$. So, choosing the ansatz is more crucial to get the accurate result. We choose Matrix product state (MPS) ansatz [12] to prepare the trial state. The MPS ansatz circuit shown in Figure 2 is structured as a sequence of alternating layers of rotations gates and nearest-neighbor entangling gates (two qubit gates such as CNOT, CZ). Each qubit first undergoes parameterized single-qubit rotations using $R_y(\theta)$ gates, which control the local amplitudes associated with the qubit's state. After the local rotations, entangling gates are applied only between neighboring qubits (e.g., between q_0 and q_1, then q_1 and q_2, and so on). This local entanglement is introduced incrementally across layers, using a staggered pattern that ensures all adjacent qubit pairs become entangled over time. The repetition of this structure across multiple layers increases the expressive power of the ansatz without significantly increasing circuit depth. Because of its strictly local connectivity and shallow depth, this MPS ansatz is efficient to implement on NISQ hardware and naturally suited to graph-based problems.

Once ansatz prepares the state $|\psi(\theta)\rangle$ and measures the expectation value of the Hamiltonian $\langle\psi(\theta)|H\ |\psi(\theta)\rangle$. Since direct measurement of H is not feasible, the Hamiltonian is in the form a sum of measurable terms (e.g., Pauli operators) such that $H = \sum_k a_k P_k$, where P_k is a tensor

product of single-qubit Pauli operators such as I,Z and a_k are real coefficients. The expectation value of H is then computed by individually measuring the expectation values of each P_k term. After collecting all term-wise expectation values, they are aggregated classically to compute the total expectation value ⟨ H ⟩. This value is then fed to a classical optimizer, which updates the parameters θ to reduce the expectation value further.

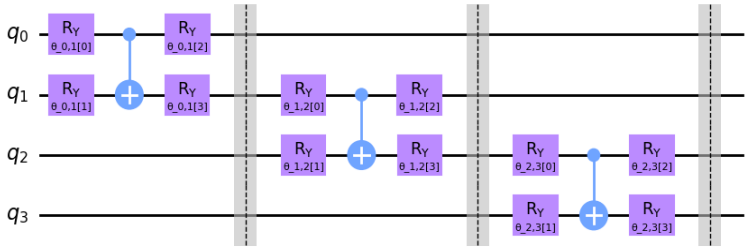

Figure 2 MPS ansatz

In this work, we utilize the Simultaneous Perturbation Stochastic Approximation (SPSA) algorithm [13] as the classical optimizer within the VQE loop. SPSA is a stochastic gradient-based optimization method known for its efficiency and robustness in high-dimensional, noisy optimization problems making it particularly well-suited for variational quantum algorithms on NISQ devices.

Upon convergence, the optimized parameters θ^* define a quantum state $|\psi(\theta^*)\rangle$ that approximates the ground state of H, and the measurement outcomes can be decoded to determine the final cluster assignments (e.g., honest vs. malicious nodes in IoV). This method is outlined in the following algorithm.

Algorithm 1: VQE for Binary Clustering

Input: Dataset D
Output: Classification label (honest/malicious)

$n = len(D)$
$W_{n\,x\,n} = 0$
for each i from 1 to n
    for each j from 1 to n
        $W[i,j] = distance\ (D[i] - D[j])$
    end for
end for
H = Hamiltonian (W)
Initialize the ansatz with default parameter (θ)
prepare the state ⟨ψ(θ)| **H** |ψ(θ)⟩
for each iteration until $minimum$(⟨ψ(θ)| **H** |ψ(θ)⟩)
    Adjust the θ value
    |output⟩ = measure ⟨ψ(θ)| **H** |ψ(θ)⟩
end for
for each i from 1 to len(output)
    if output [i] == 1
        $D[i]$ is a honest vehicle
    else
        $D[i]$ is a malicious vehicle
    end if
end for
end

Algorithm 1 presents a VQE-based binary clustering approach for detecting malicious nodes in IoV environments. Given a dataset D consisting of feature vectors for each vehicle, the algorithm first constructs a pairwise distance matrix W, where each entry represents the dissimilarity between two vehicles. This matrix is then encoded into a cost Hamiltonian H representing a MaxCut problem, which aims to partition the nodes into two honest and malicious clusters based on their feature distances. An ansatz (parameterized quantum circuit) is initialized with default parameters θ, and the expectation value $\langle\psi(\theta)|H|\psi(\theta)\rangle$ is iteratively minimized using a classical optimizer. Once the optimal parameters are found, the quantum state is measured to produce a binary output indicating the cluster assignment for each vehicle. Nodes corresponding to output bit '1' are labeled as honest, while those with bit '0' are identified as malicious. This approach leverages quantum optimization to efficiently detect anomalous behavior in a scalable and noise-resilient manner, suitable for real-time IoV security applications.

3.5. Complexity Analysis

Circuit Depth (d): The depth of the quantum circuit depends on the number of layers l in the ansatz and g is the maximum number of gate operations per layer. Therefore, the total circuit depth is approximately: $d = l.g$

Number of Qubits (N): The number of qubits used in the quantum circuit depends on the size of the problem. In our case, this scales linearly with the size of the dataset (i.e., the number of vehicles)

Overall Complexity: $O(m.d)$ Let L is number of layers. Which depends on the complexity of the problem and m is the number of iterations to optimize the parameters.it depends on number of parameters and the initial point of gradient and the classical optimizer.

Let the $number\ of\ parameter = (2N-2)\,.\,(l+1)$ then

$$m \propto \mathrm{N} \tag{5}$$

$$m = op_{const}\,.N \tag{6}$$

$$complexity = d.op_{const}\,.N \tag{7}$$

$$complexity = Const\,.N \tag{8}$$

$complexity = O(N)$ **polynomial.**

4. PERFORMANCE ANALYSIS

We present numerical simulations using data generated with the SUMO simulator, from which we obtain numerical estimates of the quantum running time. These simulations were conducted on a classical computer that emulates the quantum steps in an ideal, noise-free environment.

4.1. Simulation Setup

We generate traces of vehicle movements using SUMO [14], comprising of speed, position, and acceleration importing a map of the city of Stillwater, Oklahoma, United States of America from OpenStreetMap. The vehicles in the simulation scenario travel at speeds in the 40-50 mph range. The legitimate vehicles transmit their actual speeds in the BSMs, while the malicious vehicles transmit false information to create the illusion of false road congestion. We use IBM's StatevectorEstimator [15] to execute the quantum model. StatevectorEstimator is a widely used quantum simulation tool provided by IBM designed to emulate the behaviour of quantum circuits. Unlike physical quantum processors, which are subject to noise and gate errors, the state

vector simulator operates in an idealized environment that assumes perfect quantum states. This allows for the precise execution of algorithms.

4.2. Performance Metrics

The following metrics were used to evaluate the performance of quantum-enabled clustering in comparison to classical KMeans clustering (as discussed in Section I).

Data processing delay: This metric quantifies the time required for the model to classify each node as either malicious or honest.

Data processing time: The duration required to execute the clustering algorithm and classify nodes as either rogue and honest nodes refer data processing time or latency. A low latency clustering approach ensures prompt identification and isolation of malicious nodes, minimizing potential damage or disruptions to network performance and safety. Conversely, higher latency indicates delayed processing and increased vulnerability.

Accuracy: The ratio of correctly classified instances (both rogue and honest nodes) to the total number of instances.

F1 Score: The F1 Score is the harmonic mean of precision and recall (TPR), balancing the trade-off between them. It is defined as

$$F1\ Score = 2\ X\ \frac{precision\ X\ recall}{precision + recall}$$

Where precision measures the proportion of correctly identified positive instances among all instances predicted as positive. It is calculated as

$$\text{Precision} = \frac{True\ positives}{True\ positives + False\ positives}$$

The F1 Score is useful when the data is imbalanced, as it considers both false positives and false negatives. In malicious node prediction, where precision and recall are equally important, a high F1 Score indicates a well-performing model.

True Positive Rate (TPR): TPR also known as sensitivity or recall, measures the proportion of actual malicious nodes that are correctly identified by the model. It is defined as:

$$TPR = \frac{True\ positives}{True\ positives + False\ negatives}$$

It quantifies the model's ability to detect malicious nodes effectively. High TPR indicates that the model successfully identifies most rogue nodes, a critical feature for security-sensitive applications.

False Positive Rate (FPR): FPR also known as fall-out, measures the proportion of rogue nodes that are incorrectly classified as malicious by the model. It is defined as:

$$FPR = \frac{False\ positives}{False\ positives + True\ negatives}$$

It quantifies the model's ability to detect malicious nodes effectively. Low FPR indicates that the model successfully identifies most rogue nodes, a critical feature for security-sensitive applications.

4.3. Results

4.3.1. Date Processing Delay

The execution time for large data sizes was evaluated using the theoretical assumption of CLOPs (Circuit Layer Operations per Second), which is a standard metric in quantum computing to measure the performance of quantum processors [16]. The IBM Strasbourg QPU has a CLOPs rating of 37,000 CLOPs, and for efficient data processing, we assumed the quantum circuit depth to be $log_2 n$ layers. This assumption is based on the standard theoretical models for quantum circuit complexity and execution time, described in [17] which are used to estimate the ideal processing time under optimal conditions. While real-world quantum computers face issues like noise and decoherence, these factors are not accounted for in this theoretical framework. Thus, the execution times we report are intended as theoretical upper bounds, demonstrating the quantum model's potential scalability without the interference of practical limitations.

While the execution time of the classical k-means algorithm is highly dependent on the choice of initial centroids, we averaged the execution time over 100 runs to ensure reliability and consistency in our measurements. Figure 3 shows that as data size increases, the prediction time for the classical model grows significantly, whereas the quantum model remains nearly constant with minimal increase. The quantum model demonstrates advantage in scalability, maintaining efficient prediction times even as the data size grows. This suggests that quantum computing can handle large datasets more effectively in real-time applications for rogue node detection.

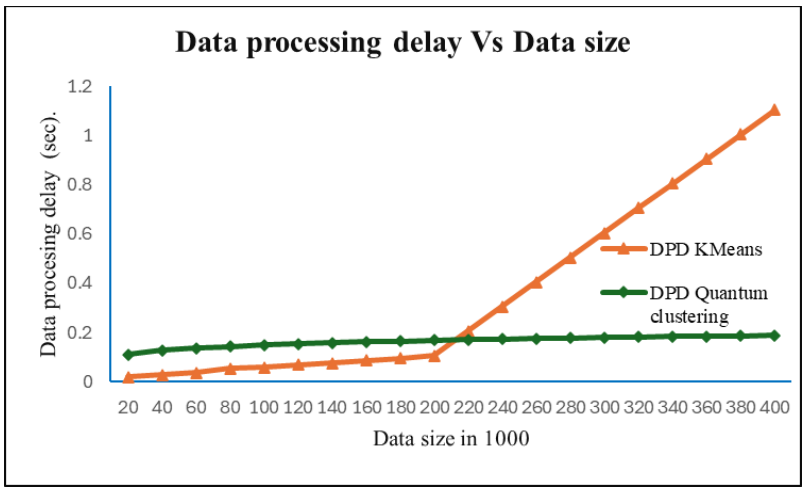

Figure 3 Data processing time Analysis

4.3.2. Accuracy

Quantum computers have the potential to globally optimize solutions due to their ability to evaluate all possibilities simultaneously. The expected high accuracy is aligned with theoretical models of quantum advantage, which suggest that, under ideal conditions, quantum models outperform classical ones in certain types of optimization tasks. Thus, we assumed the quantum model's accuracy would remain high across malicious rates, which has been observed in other theoretical and experimental studies of quantum. On the other hand, classical K-Means explores

the solution space iteratively, reassigning points to clusters based on local decisions. It is prone to converging to local minima, depending on the initial random starting points. Figure 4 shows that the proposed quantum model maintains a consistently high accuracy, close to 1, across different malicious node rates, whereas the classical model's accuracy decreases steadily as the malicious node rate increases. The quantum model exhibits superior robustness in maintaining high accuracy across varying malicious node rates.

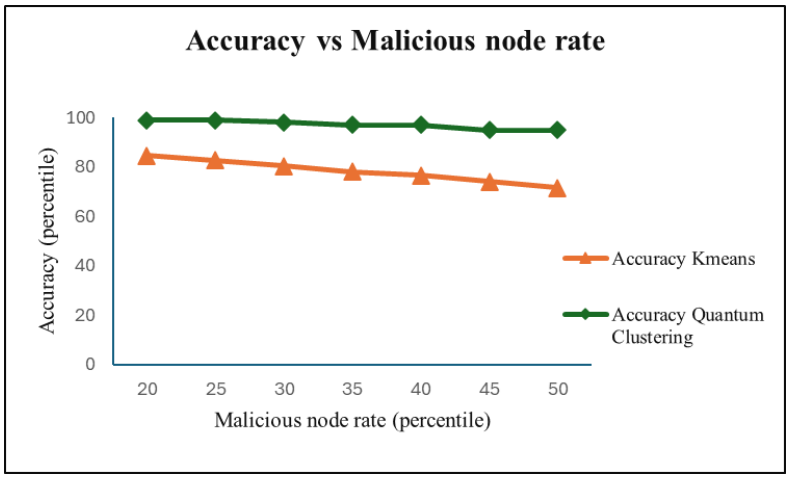

Figure 4 Impact of Malicious node rate on Detection Accuracy

4.3.3. F1 Score

The F1 score is a key metric for measuring the effectiveness of classification models. The expected high F1 score for the quantum model assumes that quantum clustering can identify malicious nodes with greater precision and recall, as it can evaluate a larger solution space and overcome the limitations of classical algorithms. Classical K-Means, while effective, often suffers from errors introduced by random initialization, which would result in a lower and more stable F1 score. These results highlight the potential of our quantum enabled clustering model as an effective solution for detecting false nodes in the IoV environment

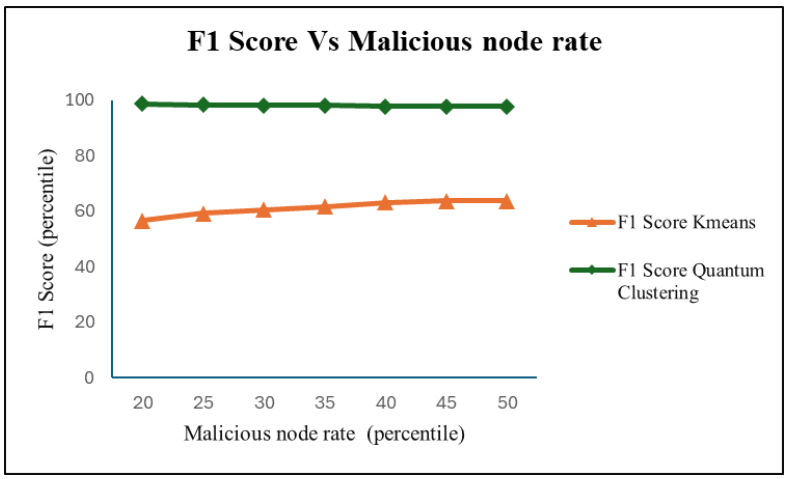

Figure 5 F1 Score Variation with Malicious node rate

Figure 5 demonstrates the F1 score comparison between quantum and KMeans clustering which highlights the superior detection performance and stability of the quantum-based clustering method over classical KMeans, in scenarios with varying levels of malicious activity.

4.3.4. TPR

The proposed method's TPR remains consistently high, close to 1, across different malicious node rate percentages. This stability suggests that the quantum algorithm is robust and effective at detecting rogue nodes, regardless of the malicious node rate in the network. The classical algorithm, which hovers around 0.5 across all malicious node rate percentages. This indicates that the classical approach has limited effectiveness in accurately identifying malicious nodes.

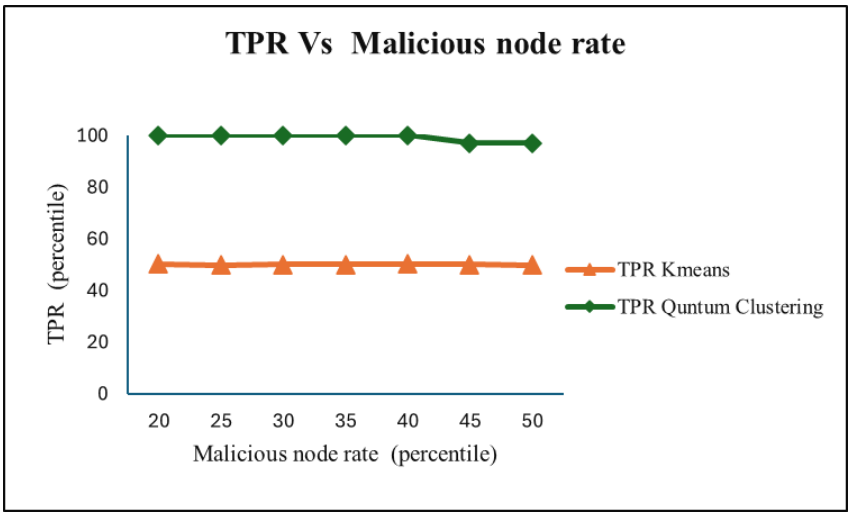

Figure 6 True Positive Rate across different Malicious node rates

Figure 6 compares the TPR of the quantum and classical models with respect to the varying malicious node rate in the dataset. The quantum model maintains a high and consistent TPR across varying malicious rates, demonstrating its robustness in detecting malicious nodes. In contrast, the classical model shows a significantly lower TPR, indicating its limited effectiveness in identifying malicious nodes as the malicious node rate increases.

4.3.5. FPR

The proposed method's FPR remains consistently low, close to 0.01, across different malicious node rate percentages. This stability suggests that the quantum algorithm is robust and effective at detecting rogue nodes, regardless of the malicious node rate in the network. The classical algorithm, which hovers around 0.5 across all malicious node rate percentages. This indicates that the classical approach has limited effectiveness in accurately identifying malicious nodes. Figure 7 compares the FPR of the quantum and classical models with respect to the varying malicious node rate in the dataset. The quantum model maintains a low and consistent FPR across varying malicious rates, demonstrating its robustness in detecting malicious nodes. In contrast, the classical model shows a significantly higher FPR, indicating its limited effectiveness in identifying malicious nodes as the malicious node rate increases.

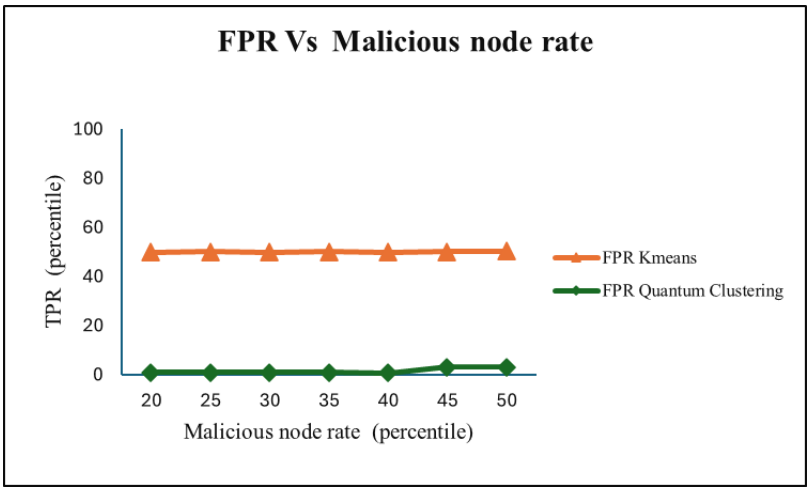

Figure 7 False Positive Rate across different Malicious node rates

5. CONCLUSIONS

In this paper, we proposed a quantum enabled clustering mechanism for identifying malicious nodes in the IoV. Our approach leverages the VQE to solve the MaxCut problem efficiently, offering significant advantages in terms of scalability and computational efficiency over KMeans clustering algorithm. The proposed method dynamically adapts to the changing nature of IoV, and significantly reduces data processing delay compared to classical clustering techniques. Performance evaluations conducted using numerical simulations on IBM's Statevector Simulator demonstrated that our quantum clustering approach consistently outperforms classical K-means clustering in terms of accuracy, true positive rate (TPR), F1-score, and execution time. The quantum method exhibited robust performance even as the malicious node rate increased, maintaining high detection accuracy and efficient execution times. The results validate the feasibility of using quantum computing for real-time security applications in IoV, making it a promising approach for large-scale vehicular networks.

Our experiments were conducted on an idealized quantum simulator, assuming a perfect quantum environment. Future work will focus on testing the method on real quantum hardware to evaluate its performance in the presence of noise and quantum decoherence. Additionally, further research should explore error mitigation techniques and fault-tolerant strategies to enhance the robustness of the method when deployed on near-term noisy quantum devices. This will ensure its practical applicability in real-world quantum computing scenarios.

ACKNOWLEDGEMENTS

The authors would like to thank everyone, just everyone!

REFERENCES

[1] Bayat, Majid, Morteza Pournaghi, Majid Rahimi, and Mostafa Barmshoory. "NERA: A new and efficient RSU based authentication scheme for VANETs." Wireless networks 26 (2020): 3083-3098

[2] Kumar, Raman, Rupali Gill, Amrita Singh, Rahul Kumar, Devendra Singh, and Mohammed Al-Farouni. "A Comprehensive Analysis of Internet of Vehicle Security Vulnerabilities in Smart Cities." In 2024 International Conference on Data Science and Network Security (ICDSNS), pp. 1-6. IEEE, 2024.

[3] Taslimasa, Hamideh, Sajjad Dadkhah, Euclides Carlos Pinto Neto, Pulei Xiong, Suprio Ray, and Ali A. Ghorbani. "Security issues in Internet of Vehicles (IoV): A comprehensive survey." Internet of Things 22 (2023): 100809.

[4] Cerezo, Marco, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean et al. "Variational quantum algorithms." Nature Reviews Physics 3, no. 9 (2021): 625-644.

[5] Commander, Clayton W. "Maximum cut problem, MAX-cut." Encyclopedia of Optimi-zation 2 (2009).

[6] Cheong, Chaklam, Sifan Li, Yue Cao, Xiaoling Zhang, and Dong Liu. "False message detection in Internet of Vehicle through machine learning and vehicle consensus." Information Processing & Management 61, no. 6 (2024): 103827.

[7] Masood, Sadaf, Yousaf Saeed, Abid Ali, Harun Jamil, Nagwan Abdel Samee, Hayam Alamro, Mohammed Saleh Ali Muthanna, and Abdukodir Khakimov. "Detecting and preventing false nodes and messages in vehicular ad-hoc networking (VANET)." IEEE Access (2023).

[8] Anyanwu, Goodness Oluchi, Cosmas Ifeanyi Nwakanma, Jae-Min Lee, and Dong-Seong Kim. "Falsification detection system for IoV using randomized search optimization ensemble algorithm." IEEE Transactions on Intelligent Transportation Systems 24, no. 4 (2023): 4158-4172.

[9] Sutradhar, Kartick, and Ranjitha Venkatesh. "SVQCP: A Secure Vehicular Quantum Communication Protocol." IEEE Transactions on Network Science and Engineering (2024).

[10] Manavi, Mahdi, Yunpeng Zhang, and Guoning Chen. "A Cutting-Edge Solution for Intrusion Detection Using Hybrid Quantum-Classical Computing." Available at SSRN 4646636.

[11] Poggiali, Alessandro, Alessandro Berti, Anna Bernasconi, Gianna M. Del Corso, and Riccardo Guidotti. "Quantum clustering with k-means: A hybrid approach." Theoretical Computer Science 992 (2024): 114466.

[12] Huggins, W., Patil, P., Mitchell, B., Whaley, K.B. and Stoudenmire, E.M., 2019. Towards quantum machine learning with tensor networks. Quantum Science and technology, 4(2), p.024001.

[13] Spall, J.C., 1997. A one-measurement form of simultaneous perturbation stochastic approximation. Automatica, 33(1), pp.109-112.

[14] https://eclipse.dev/sumo/ simulator to generate data set (last accessed 0n 2/10/2025).

[15] https://docs.quantum.ibm.com/api/qiskit/qiskit.primitives.StatevectorEstimator. (accessed on 2/14/25)

[16] Wack, Andrew, Hanhee Paik, Ali Javadi-Abhari, Petar Jurcevic, Ismael Faro, Jay M. Gambetta, and Blake R. Johnson. "Scale, Quality, and Speed: three key attributes to measure the performance of near-term quantum computers." arXiv preprint arXiv:2110.14108 (2021).

[17] Liu, Xiaoyuan, Anthony Angone, Ruslan Shaydulin, Ilya Safro, Yuri Alexeev, and Lukasz Cincio. "Layer VQE: A variational approach for combinatorial optimization on noisy quantum computers." IEEE Transactions on Quantum Engineering 3 (2022): 1-20..

AUTHORS

Krishnageetha Karuppasamy, a Ph.D. candidate in Computer Science at Oklahoma State University, with a research focus on quantum algorithms and their practical applications. She is working on quantum circuit design, variational quantum algorithms (VQAs), and methods for transforming non-unitary operators into efficient unitary representations tailored for NISQ-era hardware. Driven by the goal of bridging theoretical advances with real-world impact.

Abinash Borah is a PhD candidate in the Department of Computer Science, Oklahoma State University, USA. He previously obtained his MS in Computer Science from the University of Oklahoma, USA, and a Bachelor of Engineering from Dibrugarh University, India. His research interests are vehicular networks, data mining, machine learning, and parallel computing.

Dr. Anirudh Paranjothi is an Assistant Professor in the Department of Computer Science at Oklahoma State University. He received Ph.D. in computer science from the University of Oklahoma, an M.S. in computer science from Texas A&M University, and a B.S. degree in computer science from Anna University. His primary research interests are in the areas of networking, security, and computing, with an emphasis on wireless systems. The overarching motivation of Anirudh's research is to enhance security along with efficient routing and data forwarding on complex dynamic network systems like Vehicular Ad hoc Networks (VANETs) using next-gen technologies like edge computing, 6G and beyond. His research philosophy strongly emphasizes end-to-end framework design and development for real-world problems in wireless networks. His secondary research interests are in the area of social networks, mobile cloud computing, and IoT.

Dr. Johnson P Thomas is a Professor in the Department of Computer Science at Oklahoma State University His research interests include Applied Machine Learning and Quantum Computing. Dr. Thomas holds a Ph.D. in Computer Science from the University of Reading, England, an M.Sc. in Electrical Engineering and Computer Science from the University of Edinburgh, Scotland, and a B.Sc. in Electrical Engineering from the University of Wales.