Cyberattack Defense in Smart Cities: Leveraging Quantum Neural Networks for Secure Route Planning in ADAS

Mahdi Seyfipoor[1], Mohammad Javad Samii Zafarqandi[2], Siamak Mohammadi[3]

[1] *PhD Student at School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Iran*
`mahdiseyfipoor@ut.ac.ir`

[2] *Undergraduate Student in Computer Engineering at Faculty of Engineering, College of Farabi, University of Tehran, Iran*
`mjavadsamii@ut.ac.ir`

[3] *Associate Professor at School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Iran*
`smohamadi@ut.ac.ir`

Abstract

In the context of smart cities, real-time route planning systems are essential for both autonomous and conventional vehicles. However, the reliance on Advanced Driver Assistance Systems (ADAS) introduces cybersecurity vulnerabilities. This paper proposes a framework using Quantum Neural Networks (QNNs) to address these issues by combining quantum computing's data processing capabilities with neural networks' decision-making strengths. The framework incorporates real-time threat detection using quantum parallelism and neural network pattern recognition to identify and mitigate cyberattacks at an early stage. Quantum algorithms, such as Grover's and Shor's, are utilized to optimize search processes and secure communications. QNNs enable dynamic feedback, refining decision-making to adapt to evolving threats while maintaining computational efficiency. The integration of QNNs enhances route planning and protects transportation systems against emerging cyber threats, contributing to improved operational efficiency and cybersecurity resilience in smart cities.

Keywords: *Cyberattack, Smart City, QNN, Route Planning, ADAS.*

1 Introduction

1.1 Smart Cities and Urban Mobility

Smart cities are urban environments that leverage advanced technologies to improve the quality of life for citizens by optimizing infrastructure, services, and communication systems. Central to the smart city concept is the integration of digital technologies, data analytics, and automation to manage resources more efficiently and sustainably. In this context, the transportation sector plays a pivotal role, with technologies such as Advanced Driver Assistance Systems (ADAS) and autonomous vehicles facilitating efficient, safe, and eco-friendly mobility solutions. These systems rely on real-time data processing and intelligent decision-making to enable smooth operation within densely populated urban areas.

1.2 Cybersecurity Challenges in Smart Cities

Despite their potential, smart cities are vulnerable to a range of security threats stemming from the heightened interconnectivity of devices and systems. The extensive use of sensors, networks, and software in managing urban infrastructure presents numerous entry points for cyberattacks. Threat actors can target a wide range of city functions, including power grids, public transportation, traffic management, and communication networks. Successful cyberattacks on these systems could disrupt essential services, compromise citizen privacy, and cause severe economic damage. Thus, cybersecurity has become a critical concern for the reliable functioning and future development of smart cities.

1.3 Cyber Attacks on Vehicles and ADAS

Among the various smart city components, the transportation sector, especially vehicles equipped with ADAS, is particularly vulnerable to cyber threats. ADAS enhances vehicle safety [1] by offering features like automatic braking, lane departure warnings, and adaptive cruise control, relying heavily on data inputs from external sensors and systems for route planning, traffic updates, and vehicle-to-vehicle communication. Cyberattacks on ADAS can target these critical functions, disrupting route planning algorithms, misinforming vehicle navigation systems, or even overriding essential safety features. Such attacks could lead to traffic accidents, endanger passengers, and disrupt urban mobility on a large scale.

1.4 Preventing Cyberattacks with Quantum Neural Networks

To counter these cybersecurity threats, several solutions have been proposed, ranging from enhanced encryption techniques to advanced intrusion detection systems. Among these, Quantum Neural Networks (QNN) have emerged as a promising approach. QNN [2] combines the computational power of quantum computing with the adaptability of neural networks, offering potential breakthroughs in real-time threat detection and response. By leveraging quantum algorithms, QNN can process vast amounts of data at unprecedented speeds, significantly accelerating decision-making processes, which is essential for time-sensitive applications like route planning in ADAS. Furthermore, QNN enhances security by making it more difficult for attackers to predict or manipulate system behavior, providing an additional layer of defense against increasingly sophisticated cyberattacks.

2 Related Works

Cyberattacks present significant threats across various sectors, exploiting vulnerabilities in critical industries such as healthcare, finance, and infrastructure. In healthcare, ransomware attacks compromise patient data, disrupt essential services, and lead to substantial financial losses, underscoring the need for enhanced cybersecurity measures [3]. In the financial sector, Distributed Denial of Service (DDoS) attacks exploit the expanding digital presence of banks, with advanced models such as Support Vector Machines (SVM) proving effective in detecting these attacks [4]. Critical infrastructure, including energy and manufacturing, is increasingly vulnerable due to digital transformation, with many risks stemming from outdated legacy systems and inadequate cybersecurity investments [5].

To mitigate the risks posed by cyberattacks, various approaches have been developed across industries. Traditional methods such as encryption and Intrusion Detection Systems (IDS) are commonly employed, while newer technologies like blockchain and machine learning (ML) are gaining traction. Data encryption, including the use of AES algorithms, ensures secure data transmission, particularly in high-stakes applications like those in the mining sector [6]. IDS remain vital in detecting network intrusions, with innovations like the Neighborhood Outlier Factor significantly improving anomaly detection in distributed systems [7]. Blockchain provides decentralized solutions but still faces challenges related to scalability and security [8]. Meanwhile, machine learning plays a critical role in cybersecurity by analyzing large datasets, improving threat detection capabilities, and adapting to the ever-evolving threat landscape [9].

In this paper, we employ QNN to counter cyberattacks on ADAS and route planning, harnessing its speed and adaptability to significantly improve threat detection and response in these critical, time-sensitive systems.

3 Optimizing Route Planning and Security in Dynamic Urban Environments

3.1 Dynamic Urban Environments

One significant advancement in dynamic urban environments is the rise of autonomous vehicles. These self-driving cars use advanced technologies, such as real-time object detection, parallel processing, and route planning, to navigate city streets efficiently and safely. Their capability to process extensive data in real-time allows for rapid decision-making, obstacle avoidance, and the selection of optimal routes [10]. This significantly reduces traffic jams and enhances overall transportation efficiency.

Despite these advancements, there are still significant challenges in optimizing route planning in such complex and ever-changing environments. Quantum computing, particularly QNNs, offers a promising solution. Quantum computing leverages the principles of quantum mechanics to perform computations much faster and more efficiently than classical computers. QNNs can process and analyze large and complex datasets more effectively, enabling more accurate and efficient route optimization in dynamic urban settings.

In this paper, we first define route planning in urban environments and explain the fundamentals of QNNs. We then introduce strategies for enhancing QNNs' performance and compare these strategies based on specific criteria.

3.2 Advanced Driver Assistance Systems (ADAS)

ADAS refers to a collection of technologies designed to enhance vehicle safety and facilitate more efficient driving by assisting the driver in various scenarios. This system uses sensors, cameras, and other technologies to monitor the vehicle's surroundings and provide real-time feedback or assistance. ADAS offers support in decision-making during driving, especially in complex, dynamic environments, such as urban areas with heavy traffic, unpredictable pedestrian movements, and frequent changes in road conditions.

ADAS plays a significant role in enhancing driver awareness by issuing warnings and taking partial control of the vehicle when necessary [11]. In Fig. 1, ADAS Sensors are shown. The data from these sensors is fused to enable real-time processing and decision-making. This system can detect potential hazards, issue alerts, and intervene to prevent or mitigate accidents. They are designed to assist, not replace, human drivers, but in certain situations, such as route planning or avoiding obstacles, ADAS may temporarily assume control over specific vehicle functions. One crucial aspect of ADAS is its contribution to route planning. By continuously analyzing traffic patterns, road conditions, and other variables, ADAS helps drivers select optimal routes. This feature is especially valuable in dynamic urban environments, where traffic congestion, roadwork, and other obstacles frequently arise. By making real-time adjustments to routes, ADAS can improve efficiency and safety, reducing the cognitive load on drivers.

With the growing reliance on ADAS for tasks such as route planning, the system becomes increasingly susceptible to cyber-attacks, particularly in scenarios where control is delegated to ADAS. Cybercriminals target these systems to exploit vulnerabilities, leading to potential disruptions. These attacks can manipulate or disable ADAS-controlled features like route planning, creating hazardous conditions for drivers. For instance, an attack could alter the vehicle's routing algorithms or deactivate critical safety functions when ADAS is in control, severely undermining the system's reliability. Protecting ADAS from such threats is vital, as a compromised system in urban environments, where split-second decisions are essential, could result in catastrophic consequences.

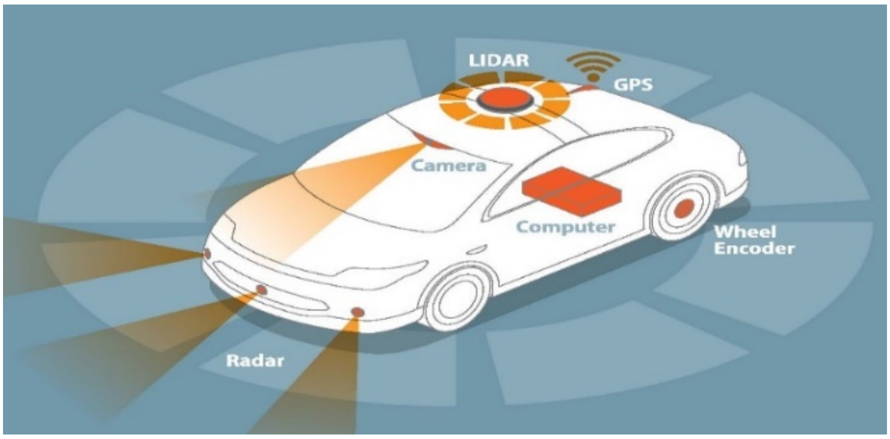

Figure 1: Overview of ADAS Sensors, Including Radar, LIDAR, Camera, and GPS

3.3 Route Planning

Route planning is a process used to determine the most optimal path from a starting point to a destination, considering various factors such as distance, time, traffic conditions, and user preferences. As illustrated in Fig. 2, the process involves collecting and analyzing large volumes of data, including map data, traffic information, speed limits, and real-time data such as traffic congestion [12]. This information is critical for determining the best possible route.

To achieve optimal pathfinding, route planning systems rely on sophisticated algorithms. Common examples include Dijkstra's algorithm and the A* algorithm, which evaluate nodes and edges in a graph to calculate the shortest or fastest route based on predefined metrics. These algorithms efficiently process potential routes and identify the most suitable path for navigation. As these systems advance, they increasingly integrate real-time data and user preferences to provide more effective navigation solutions [13]. However, the increasing complexity and connectivity of route planning systems in smart cities also introduce significant security risks. These systems, which manage both machine and human transportation, are vulnerable to cyberattacks. Malicious actors could attempt to take control of the system, manipulating route suggestions and creating a controlled environment that favors their objectives. By controlling critical transportation routes, attackers could generate widespread disruptions, traffic jams, or even chaos across a city.

4 Cybersecurity Risks

The concept of control is fundamental to understanding the threats posed by cyberattacks on route planning systems. Attackers aim not just to disrupt navigation but to take control of the system itself. By manipulating data inputs, altering suggested

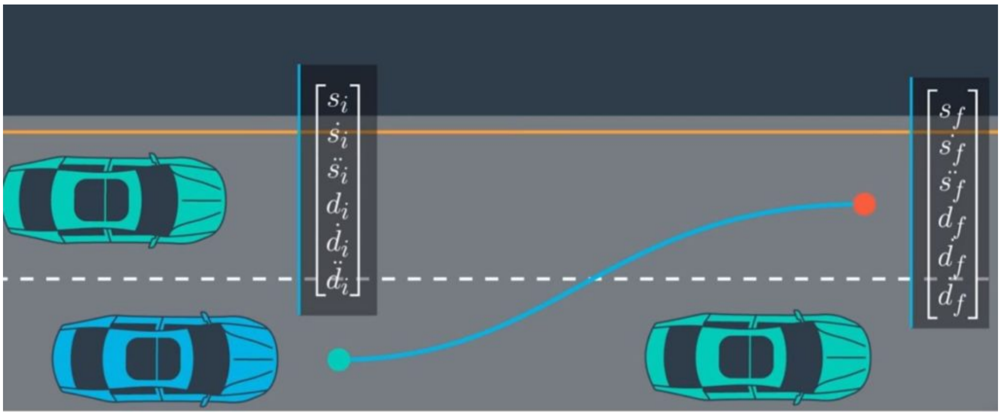

Figure 2: Route Planning Utilizing Map Data, Traffic Information, Speed Limits, and Real-Time Data

routes, or intercepting communications between the user and the navigation system, cybercriminals [14] can direct vehicles along paths that serve their interests, potentially leading to hazardous or destructive outcomes in urban environments. Given the high stakes in smart city ecosystems—where both machines and humans rely on seamless transportation—robust, real-time cybersecurity measures are essential. These systems must be capable of detecting and responding to threats in real time, preventing attackers from gaining control over critical urban infrastructure.

4.1 Types of Cyberattacks on ADAS

Cyberattacks on ADAS, particularly in relation to route planning, take several forms:

Data Manipulation: By tampering with sensor inputs or traffic data, attackers can mislead the system into making incorrect routing decisions.

Man-in-the-Middle (MitM) Attacks: Intercepting communications between the ADAS and external data sources allows attackers to inject false information or reroute vehicles.

Denial-of-Service (DoS) Attacks: Overwhelming the system with illegitimate requests can render the ADAS unresponsive, disrupting real-time route updates.

Algorithm Exploitation: Exploiting weaknesses in the route-planning algorithms can lead to unsafe or inefficient decisions.

4.2 Cybersecurity Framework for Route Planning in ADAS

To address these vulnerabilities, a comprehensive cybersecurity framework for ADAS is proposed, focusing on three main components: detection, prevention, and post-attack correction.

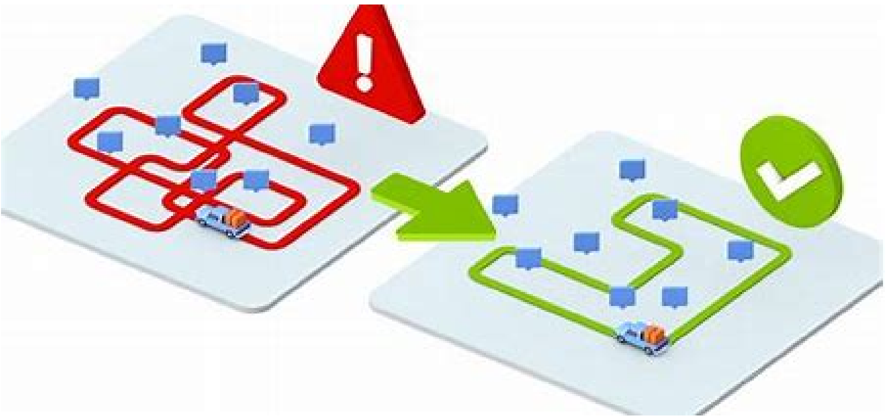

Figure 3: Post-Attack Route Correction

Detection of Cyberattacks: The system's first responsibility is identifying when a cyberattack is taking place. Continuous, real-time monitoring of ADAS inputs and outputs enables the detection of anomalies. Neural networks (NNs), known for their strength in pattern recognition, are utilized to detect deviations from normal behavior, such as sudden route changes or inconsistencies between sensor data and external communications. These networks can learn and adapt to new threats over time, improving their accuracy in identifying attacks.

Prevention of Cyberattacks: Once an attack is detected, the system must act immediately to prevent further damage. This includes blocking unauthorized data inputs, stopping suspicious communications, and verifying the accuracy of incoming data. Predictive analytics help anticipate potential attack methods by analyzing past data, allowing the system to take preemptive measures. If needed, the system can assume temporary control, rerouting the vehicle or implementing safety protocols to avoid high-risk areas or dangerous situations.

Post-Attack Correction: In situations where the attack is not detected or prevented in real time, the system must be able to diagnose and correct the effects of the attack. As Shown in Fig. 3, Post-attack correction is initiated when the system identifies deviations from pre-set constraints programmed into the ADAS. Neural networks trained under specific guidelines—such as avoiding highly congested areas, quiet backroads, or one-way streets—play a key role in identifying compromised routes. If the vehicle enters restricted or dangerous zones, the system will recognize this as an attack and respond by either rerouting the vehicle to a safer path or correcting the route to ensure passenger safety.

4.3 Leveraging Neural Networks for Advanced Cybersecurity Solutions

Neural networks are a key component of this cybersecurity framework due to their ability to identify patterns, handle complex data, and continuously learn from new information. These characteristics are essential for detecting anomalies that may signal a cyberattack [15], as well as for real-time decision-making. NNs excel at analyzing large, multifaceted datasets—such as traffic conditions, sensor inputs, and communication streams—and making quick, accurate decisions that prevent or mitigate attacks. Moreover, neural networks' learning capabilities allow them to adapt to evolving threats, improving the system's ability to detect new types of cyberattacks over time.

In the event that an attack has caused the vehicle to be directed onto an incorrect or unsafe route, neural networks also play a critical role in post-attack correction. By quickly assessing the situation and comparing it against known safe parameters, the system can autonomously reroute the vehicle or make necessary adjustments to ensure a safe journey.

4.4 Real-Time Processing and Quantum Computing

Given the rapidly changing and unpredictable nature of urban environments, real-time processing is critical to the success of this cybersecurity framework. The system must handle large volumes of sensor data, vehicle communications, and traffic information simultaneously and without delay. To meet these demands, parallelism is required, allowing multiple processes to run concurrently to ensure that threat detection, prevention, and route correction occur in real time. Quantum computing offers a powerful solution to this challenge. Quantum computers can process large datasets in parallel, significantly reducing the time needed for complex calculations. When integrated with neural networks, quantum computing enhances the system's ability to detect cyber threats, optimize routes, and secure communications. This combination provides the computational power required to process vast amounts of data in real time, while also improving the system's accuracy and speed in responding to threats.

The integration of quantum computing with neural networks, resulting in QNNs, presents a promising direction for enhancing the cybersecurity of ADAS-controlled systems. In the subsequent sections, the potential of quantum computing to enhance neural network performance will be examined, particularly in the context of real-time threat detection, decision-making, and route optimization. By leveraging the strengths of both technologies, the system can offer robust protection for critical transportation infrastructure, ensuring both safety and operational efficiency amid evolving cyber threats.

5 Quantum Computing

Quantum computing is a new approach to calculation that uses principles of fundamental physics to solve extremely complex problems very quickly. Quantum computing uses subatomic particles, such as electrons or photons. Quantum bits, or qubits, allow these particles to exist in more than one state (i.e., 1 and 0) at the same time. Quantum neural networks are computational neural network models which are based on the principles of quantum mechanics.

5.1 The Fundamentals of Quantum Computing

In quantum computing, superposition refers to the ability of a qubit to exist in multiple states simultaneously. Unlike classical bits, which can be either 0 or 1, qubits can be in a state that is a combination of both 0 and 1 [16]. This is a fundamental concept of quantum mechanics and is crucial for the power of quantum computing.

Quantum computers operate with the so-called qubits, which are quantum states that are allowed to be in a superposition of the two orthonormal vectors:

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \;,\; |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \tag{1}$$

The symbol $|\rangle$ is called a ket. It is used to denote a column vector. These two vectors form the canonical basis of C^2 and are referred to as the computational basis. Now, qubits in a pure state can be expressed as:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2}$$

A general qubit state $|\Psi\rangle$ can be expressed as a linear combination of these basis states

where $\alpha, \beta \in C$ and fulfill [17]:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{3}$$

5.2 Quantum Gates

Quantum gates and qubits are the fundamental elements of gate-based quantum computations. These gates are unitary operators that act on qubits, represented by unitary matrices of size $2^n \times 2^n$, where n is the number of qubits the gate operates on.

The Pauli X, Y, and Z gates are fundamental examples of single-qubit gates. These gates can be represented in the standard basis $\{|0\rangle, |1\rangle\}$ as follows:

$$X = \sigma_x = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} \quad,\quad Y = \sigma_y = \begin{pmatrix}0 & -i\\i & 0\end{pmatrix} \quad,\quad Z = \sigma_z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix} \tag{4}$$

which represent a π radians rotation around the x, y, or z axis respectively. Note that this gate functions similarly to the logical NOT gate, which converts 0 bits to 1 bits and vice versa. Also, Hadamard gate could be introduced as below:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \tag{5}$$

which creates a superposition of $|0\rangle$ and $|1\rangle$. The Hadamard gate can also be interpreted as a $\frac{\pi}{2}$ radians rotation in y, followed by a π radians rotation in x. There also exist gates that act on multiple qubits. An essential type of these multiple qubit gates is the controlled gate. Given a unitary matrix U of dimension n. The $(d+n)$-dimensional controlled-U gate, C-U, is the matrix of the form:

$$\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} \tag{6}$$

where I is the d-dimensional identity matrix. An important example of controlled gates is the controlled-NOT (CNOT) gate. When expressed in the basis $\{\,|00\rangle\,,|01\rangle\,,|10\rangle\,,|11\rangle\}$, it is:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{7}$$

5.3 Quantum Algorithms

Quantum computing enables parallel processing on an unprecedented scale, allowing the system to monitor and process multiple data streams simultaneously. In the context of route planning, quantum computers can be employed to ensure real-time analysis and decision-making without compromising the speed or accuracy of the route suggestions.

For example, Grover's algorithm, a quantum algorithm designed for search optimization, can be used to rapidly scan through vast datasets to detect anomalies or malicious activities within the system [18]. It achieves this in significantly fewer steps than classical algorithms, making it highly effective in identifying and mitigating security threats in real time.

Additionally, Shor's algorithm can be applied to enhance the cryptographic security of communication channels used by route planning systems. While traditionally used to break classical encryption methods, Shor's algorithm can also be utilized to develop quantum-resistant encryption protocols. This helps secure the transmission of data between different components of the system, ensuring that hackers cannot intercept or manipulate the information flowing through the route planning infrastructure.

6 Hybrid Approach: Quantum Neural Networks (QNNs)

QNNs combine the computational power of quantum mechanics with the learning capabilities of neural networks. By harnessing quantum computing's ability to process complex data and neural networks' capacity for pattern recognition and decision-making, QNNs offer an advanced framework for optimizing systems like ADAS (Advanced Driver Assistance Systems), particularly in the context of cybersecurity and real-time route planning.

6.1 Structure of QNNs

QNNs integrate the computational capabilities of quantum circuits with the learning power of neural networks to enhance performance, particularly in tasks involving high-dimensional data and complex decision-making. The structure of QNNs is built to capitalize on quantum parallelism, where quantum gates and circuits perform operations like superposition and entanglement, allowing the system to explore multiple possibilities simultaneously. This quantum parallelism accelerates the processing of complex input data, such as sensor readings or environmental information, by transforming it into quantum states that can be analyzed more efficiently.

Once the input data is encoded into quantum states, the quantum circuits process it, handling tasks like feature extraction, optimization, or pattern recognition [19]. This processing in the quantum layer enables the system to rapidly explore multiple scenarios, ensuring that computationally intensive tasks are managed effectively. The refined quantum data is then converted back into classical information and passed to the neural network layers for further interpretation. The neural networks, leveraging the optimized quantum data, make predictions and decisions based on the refined information, such as identifying cyberattacks or determining optimal routes.

In certain QNN configurations, the interaction between quantum and neural components extends to a feedback loop, where the output from the neural network is reintroduced into the quantum layer for further optimization or refinement. This iterative process creates a dynamic flow of information between the two systems, allowing for continuous learning and real-time adaptation to evolving scenarios. The quantum feedback loop ensures that QNNs remain flexible and responsive to new data or threats, improving the overall decision-making process.

A key advantage of QNNs lies in the quantum speedup they provide. Quantum algorithms enable the system to perform complex tasks such as optimization and pattern recognition more rapidly than classical methods, particularly when dealing with large datasets or intricate decision-making scenarios. This hybrid architecture ensures that QNNs can efficiently process and analyze high-dimensional data, making them ideal for real-time applications like cybersecurity in dynamic environments.

By combining the strengths of quantum computing and neural networks, QNNs create a powerful system that not only handles vast amounts of data but also improves decision-making and optimization processes. This integration enhances the system's ability to learn from new information and adapt to changes, making it a crucial tool in advanced applications requiring real-time processing and high accuracy.

6.2 Application of QNNs in Cybersecurity for ADAS

QNNs offer significant improvements to the cybersecurity of ADAS, particularly in the areas of detection, prevention, and post-attack correction.

In cyberattack detection, QNNs can process vast amounts of sensor data and communications in parallel, identifying anomalies faster and more accurately. Quantum circuits preprocess complex data, such as sensor inputs and external communication patterns [20], identifying early signs of an attack before they become critical. The neural network interprets this quantum-processed data to detect deviations from expected behavior, such as sudden route changes or inconsistencies in data inputs.

In the prevention phase, QNNs use quantum algorithms to predict and prevent vulnerabilities by analyzing real-time data, optimizing the input for neural network layers to make immediate decisions. If a potential threat is identified, the system can block unauthorized inputs, reroute the vehicle, or trigger safety protocols. The combination of quantum speed and neural adaptability allows for proactive prevention, minimizing the potential for damage before an attack escalates.

And in post-attack correction, QNNs handle the complex task of diagnosing and correcting the effects of undetected or unresolved attacks. The quantum layer rapidly performs optimization tasks, such as finding alternative routes or restoring compromised systems, while neural networks apply the corrected information in real time. If the vehicle has been directed into dangerous or restricted zones, the QNN will promptly identify the issue and reroute the vehicle to safety, ensuring the attack's impact is neutralized.

6.3 Advantages of QNNs in System Security and Performance

QNNs provide several critical benefits in the context of ADAS cybersecurity. The combination of quantum data processing and neural network learning enables enhanced detection and decision-making capabilities, allowing the system to rapidly identify cyber threats and formulate accurate responses. QNNs' ability to process large volumes of data in real time is essential for dynamic urban environments, where fast and reliable decisions are crucial to maintaining safety.

Additionally, QNNs continuously learn and adapt, improving their effectiveness in detecting emerging threats. This learning ability, combined with quantum optimization, enhances the system's capacity to reroute vehicles during cyberattacks, ensuring passenger safety and minimizing disruption. The integration of quantum computing for complex tasks like real-time optimization and error correction ensures that ADAS can quickly recover from attacks and maintain operational efficiency.

The subsequent sections will delve deeper into the specific quantum algorithms and neural network structures employed in the QNN framework, illustrating their practical application in safeguarding ADAS-controlled systems from evolving cyber threats.

7 Experimental Results

This section presents a comparative analysis of classical and QNN-based route planning systems under various cyberattack scenarios. The results highlight the superior performance of QNN-based systems in terms of security and efficiency.

Table 1: Security robustness and recovery time comparison under cyberattacks

METRIC	CLASSICAL ROUTE PLANNING	QNN-BASED ROUTE PLANNING
DATA MANIPULATION ATTACK	Fails to detect subtle changes in sensor/traffic data, leading to incorrect routing decisions.	quickly identifies tampered data, ensuring minimal route deviations.
MITM ATTACK	Communication interceptions often lead to rerouting or incorrect decisions.	Detects and mitigates false information early, ensuring secure and accurate routing.
DOS ATTACK	System becomes unresponsive, causing significant delays in route updates.	Detects and isolates attack traffic, maintaining real-time updates with minimal delay.
ALGORITHM EXPLOITATION	Susceptible to algorithmic weaknesses, causing inefficient or unsafe decisions.	Strong resilience to exploitation, detecting anomalies and recalculating efficiently.
RECOVERY TIME	Takes longer to recover and recalibrate after attacks.	Recovers faster by quickly isolating and responding to attacks.
DETECTION ACCURACY	May miss sophisticated attacks or react too late.	Detects attacks more accurately due to quantum-enhanced pattern recognition.
SYSTEM DOWNTIME	High downtime due to delayed detection and mitigation.	Minimal downtime; recovers swiftly from attacks and resumes normal operations.

Table 1 shows that QNN-based systems respond to cyberattacks like Data Manipulation, MitM, and DoS more effectively, offering quicker detection and recovery compared to classical systems. Similarly, Table 2 demonstrates that QNN-based systems provide higher route accuracy, faster processing times, and better resilience to attacks, especially under heavy loads or attack conditions, while also being more power-efficient.

8 Conclusion

In dynamic urban environments, particularly with the rise of autonomous vehicles, efficient route planning is a critical challenge. Traditional algorithms like Dijkstra's and A* have served as foundational methods for navigating complex cityscapes, but they are now increasingly supplemented by quantum computing innovations. The combination of real-time data processing, advanced algorithms, and the growing integration of machine-to-human interactions has made route planning systems indispensable in smart cities. However, these systems are vulnerable to cybersecurity threats, where attackers seek to gain control and manipulate routes to create disruptions.

Quantum computing, with its unique properties such as superposition and entanglement, offers transformative potential for addressing these vulnerabilities. Quantum

Table 2: Performance metrics comparison in normal and attack conditions

Scenario	Route Accuracy	Processing Time	Attack Resilience	Power Efficiency
Classical (Normal Operation)	Good accuracy but vulnerable to incorrect decisions in complex environments.	Relatively slower, especially under high data loads.	Low resilience to attacks, leading to significant route deviations.	Moderate but increases significantly under attack conditions.
Classical (Under Attack)	Low accuracy during attacks; hard to maintain optimal routes.	Slows down further, exacerbating response time.	Vulnerable to repeated attacks with delayed recovery.	Increased power consumption due to repeated recalculations.
QNN (Normal Operation)	High accuracy, even in complex and dynamic conditions.	Faster computations due to quantum enhancements.	Naturally more resilient to attacks, ensuring accurate routing.	Efficient with minimal energy overhead.
QNN (Under Attack)	Maintains high accuracy even during sustained attacks.	Processes data efficiently with minimal delays, even under attack.	Strong resilience to attacks, detecting and responding early.	Slightly increased power, but more efficient under attack than classical systems.

Neural Networks (QNNs), Grover's algorithm, and Shor's algorithm provide tools for enhancing both the efficiency of route planning and the security of the system. QNNs enable more efficient data processing and better route optimization, while quantum algorithms can strengthen anomaly detection and cryptographic security, protecting the integrity of the system against malicious control. Furthermore, the integration of quantum machine learning ensures that route planning systems can adapt in real time, identifying and neutralizing potential threats before they escalate.

By leveraging the capabilities of quantum computing, urban route planning systems can not only optimize navigation but also defend against emerging cyber threats, ensuring secure, efficient, and resilient transportation networks in smart cities. As technology continues to evolve, the role of quantum computing will become increasingly essential in maintaining the balance between efficiency and security in these interconnected urban ecosystems.

References

[1] F. Jiménez, J. E. Naranjo, J. J. Anaya, F. García, A. Ponz, and J. M. Armingol, "Advanced Driver Assistance System for Road Environments to Improve Safety and Efficiency", Transportation Research Procedia, vol. 14, pp. 2245–2254, Jan. 2016.

[2] A. Kukliansky, M. Orescanin, C. Bollmann and T. Huffmire, "Network Anomaly Detection Using Quantum Neural Networks on Noisy Quantum Computers", in IEEE Transactions on Quantum Engineering, vol. 5, pp. 1-11, 2024.

[3] E. A. Al-Qarni, "Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies", International Journal of Advanced Computer Science and Applications, vol. 14, no. 5, 2023.

[4] U. Islam et al., "Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models", Sustainability, vol. 14, no. 14, p. 8374, Jan. 2022, doi: https://doi.org/10.3390/su14148374.

[5] D. A. S. George, D. T. Baskar, and D. P. B. Srikaanth, "Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors", Partners Universal International Innovation Journal, vol. 2, no. 1, pp. 51–75, Feb. 2024.

[6] Y. Yu, "Encryption Technology for Computer Network Data Security Protection", Security and Communication Networks, vol. 2022, p. e1789222, Aug. 2022.

[7] J. Jabez and B. Muthukumar, "Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach", Procedia Computer Science, vol. 48, pp. 338–346, 2015, doi: https://doi.org/10.1016/j.procs.2015.04.191.

[8] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017.

[9] U. I. Okoli et al., "Machine learning in cybersecurity: A review of threat detection and defense mechanisms", World Journal of Advanced Research and Reviews, vol. 21, no. 1, pp. 2286–2295, 2024.

[10] M. M. Diaz and F. Soriguera, "Autonomous vehicles: theoretical and practical challenges", Transportation Research Procedia, vol. 33, pp. 275–282, 2018.

[11] S. L. Page, J. Millar, K. Bronson, S. Rismani, and Aj. Moon, “Driver perceptions of advanced driver assistance systems and safety”, arXiv:1911.10920 [cs], Sep. 2021.

[12] D. Delling, P. Sanders, D. Schultes, and D. Wagner, “Engineering Route Planning Algorithms”, Algorithmics of Large and Complex Networks, pp. 117–139, 2009.

[13] D. Luxen and C. Vetter, “Real-time routing with OpenStreetMap data”, Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems - GIS ’11, 2011.

[14] A. Giannaros et al., “Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions”, Journal of Cybersecurity and Privacy, vol. 3, no. 3, pp. 493–543, Sep. 2023.

[15] R. K. Vigneswaran, R. Vinayakumar, K. P. Soman and P. Poornachandran, ”Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security”, 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 2018.

[16] R. D. Schafer, “An Introduction to Nonassociative Algebras”, 1996.

[17] G. Ortega Ballesteros and D. Cirici, “GRAU DE MATEMÀTIQUES Treball final de grau Quantum algorithms for function optimization”, 2021.

[18] A. M. Dalzell et al., “Quantum algorithms: A survey of applications and end-to-end complexities”, arXiv.org, 2023. https://arxiv.org/abs/2310.03011.

[19] K. Beer, D. Bondarenko, T. Farrelly, T. J. Osborne, R. Salzmann, D. Scheiermann, R. Wolf, “Training deep quantum neural networks”, Nature Communications, vol. 11, no. 1, p. 808, Feb. 2020.

[20] M. J. H. Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, “A Review of Quantum Cybersecurity: Threats, Risks and Opportunities”, arXiv:2207.03534 [cs], Jul. 2022.