Improving the Routing Process in Vehicular Networks While Considering Both Security and Quality of Service (QoS) through the Use of Machine Learning and Fuzzy Logic, within the Framework of Fog Computing Architectures and Software-Defined Networking (SDN)

Saif Thamer Mohammed Museedi[1], Hardik Joshi[2]

[1]Ph.D. student in department of computer science Gujarat University,
Email: saif.thamer@gujaratuniversity.ac.in
[2]Department of Computer Science, Gujarat University, Emai: hardikjoshi@gujaratuniversity.ac.in

Abstract
There are several challenges for routing protocols, some of which are associated with security concerns and others are with Quality of Service (QoS). The highly dynamic and distributed nature of the network topology further exacerbates these challenges.
This paper aims to offer a comprehensive solution that concurrently tackles security and QoS issues. After an authentication phase, machine learning classifiers installed in the SDN controller and fog nodes are used to analyze network activity behaviorally. Under a load-balancing policy controlled by the software-defined controller, these nodes process data based on priority levels. An adaptive aerial path is incorporated into a reinforcement learning mechanism for route discovery that is conditioned by security and QoS standards. The suitability of the relay drone is assessed using an applied fuzzy logic technique.
Using computer simulations, the suggested model was assessed according to several important performance factors, such as attack success rate, packet delivery ratio, throughput, and end-to-end delay. These factors have been tested under varying parameters such as the number of vehicles in the network, the proportion of malicious nodes, and vehicle speed. The outcomes showed that the suggested model outperformed the benchmark protocol (QL-TRT).

Keywords: Secure routing, reinforcement learning, fuzzy logic, fog computing, software-defined networking (SDN), unmanned aerial vehicles (UAVs), hierarchical machine learning, authentication, load balancing.

1. Introduction

Vehicular Ad Hoc Networks (VANETs) form a crucial element of Intelligent Transportation Systems (ITS). They facilitate the transmission of messages between vehicles and also between vehicles and infrastructure components like Roadside Units (RSUs), pedestrians, and external networks—known as Vehicle-to-Everything (V2X) communication [1]. VANETs improve public safety by facilitating emergency and essential services, help decrease traffic congestion via effective traffic management, and offer a range of infotainment and comfort services [2,3]

Despite these advantages, VANETs show highly dynamic topological characteristics due to the high mobility of their nodes [4], which introduces several challenges for traditional routing protocols originally designed for Mobile Ad Hoc Networks (MANETs) —of which VANETs are considered a special case. Such protocols often face high packet loss rates and increased end-to-end delays because of the frequent need for route rediscovery [5,6], the thing which has motivated researchers to develop new routing protocols or enhance existing ones to adapt to the rapidly changing topology of vehicular environments [7–10].
In addition to routing efficiency and data delivery performance, VANETs also have significant security challenges, which are further intensified by their distributed nature and the absence of centralized control over network nodes [11–13].
Considering all the challenges mentioned above, this study will tackle both Quality of Service (QoS) and Security issues. The proposed model uses reinforcement learning that successfully captures the environmental characterization & selects the ground relay node to forward data on its own. This model is based on the working of the AODV protocol. It also uses fog computing – the processing power located at the 'edge of the network', near the data source – to process application data according to packet priority and time-sensitivity constraints. The load on fog nodes has a substantial impact on the efficiency of task migrations, emphasizing the requirement of a central controller capable of fog level load balancing. The SDN controller is assigned to make intelligent decisions on dispersing loads to low loaded nodes.
The proposed framework on the security side begins with authentication among vehicles based on elliptic curves for trusted communication. Security is also boosted through a machine learning model at an SDN controller-fog layer in a hierarchical form. Fuzzy logic is used for the final decision-making of routing in the presence of alternative relays which are UAVs.

The following sections of of this paper are organized as follows:
The literature reviewed is presented in section 2. This is important for the conceptual development of the model proposed. Section 3 discusses the fundamentals of reinforcement learning, fuzzy logic, fog computing and SDN along with its functioning principles. Section 4 contains the general flow diagram of the proposed system. Section 5 of the study focuses on performance evaluation and analysis using simulation. The paper is concluded with key findings, recommendations, and directions for future research.

2. Literature Review

Study [14] proposed a framework that intended to achieve secure, low-latency routing for vehicular networks using SDN and fog computing with adaptive encryption and blockchain. In this study, SDN controller always observes the network traffic and security threats. It automatically chooses between encrypting AES-GSM when there is little traffic and a low threat level and using ChaCha20-Poly1305 when there are greater load or more serious threats. The controller additionally identifies anomalies through a trust factor that is calculated from various weighted security criteria including the authentication success rate and packet integrity. To prevent impersonation attacks, Blockchain technology is used to create hashed identifiers for vehicles. Fog nodes process application data of high priority by decrypting and processing packets with shared session keys. This is done near the data source for quick responses. Apart from choosing the encryption, the measured network load is also used as a rerouting trigger.
The study presented in [15] pointed out that in AODV-based vehicular networks secure data transmission is vital mainly in the case of black hole attacks. As a solution they came up with an entity-based trust model that would help in detecting malicious nodes by giving different weights to data (depending on its priority) and to nodes (according to their roles). The model separates direct trust based on the immediate sender-receiver relationship and recommended trust based on evaluation by neighboring nodes. The final trust score is achieved through fuzzy logic that considers both direct and recommended trust levels. Fuzzy logic was chosen because of the uncertainty that was common in trust evaluation, hence it was not appropriate to use deterministic weighting for a reliable trust computation.
The presented study in [16] suggested a routing protocol that is both secure and delayed efficient, and which detects the malicious nodes responsible for black hole attacks using deep learning techniques. An Artificial Neural Network (ANN) model is employed by the Roadside Units (RSUs) to detect bad nodes, and afterwards, trustworthy vehicles are grouped based on several factors; relative velocity, distance, and neighborhood density among them. The enhanced version of the AODV protocol, which is modified to recognize the most stable and trustworthy routes, is used for route discovery. Stability and trust are considered the main parameters of the routing process in this improvement. Furthermore, the approach leads to a decrease in control overhead, and efficient resource utilization in large networks. When the inter-cluster communication needs to be secured, authentication keys are generated for this purpose.
In study [17], the authors proposed a Quality of Service (QoS)-aware routing method that merged trust assessment with reinforcement learning in order to avert black hole and gray hole attacks. The QL-TRT protocol developed by the authors determines the trust of a link through three criteria that are weighed differently: packet forwarding ratio, energy consumption, and expected transmission time. Every car acts as an agent in a Q-learning scenario where the reward is based on the most trustworthy neighboring vehicle being selected for data forwarding. The relay is chosen to be the node with the maximum Q-value, which thus ensures a dependable, secure, and flexible connection between the source and destination, and at the same time, it remains undetectable by the malicious entities.
A two-tier blockchain-based trust management system was presented in study [18] which allows for secure routing. In the first tier, the neighboring nodes compute the trust scores using AODV routing parameters, like the packet delivery ratio, the time gap between route request and reply, and variations in the destination sequence number (DSN). The trust values are sent as digitally signed transactions to roadside units (RSUs) that form the second tier of trust. An assigned leader RSU collects the distributed transactions and updates the blacklist of vehicles whose trust scores have fallen below a certain threshold. The updated list is then recorded on the blockchain after consensus is reached by a Byzantine Fault Tolerance (BFT) protocol, and it is then broadcast to all vehicles for the purpose of verifying the relay nodes. The system gives a misbehaving vehicle the chance of making up to three registration attempts before being permanently excluded, thus providing opportunities for correction of the behavior.
Study [19] aimed to accomplish a reliable and secure routing system by utilizing the interplanetary file system (IPFS) and blockchain technology for the filtering of malicious messages, backed by a machine learning classifier (IIVM) for anomaly detection. The K-Means algorithm is used to cluster vehicles, and the node with the highest reputation is chosen as the cluster head. The events occurring in the network are documented on IPFS, which leads to the generation of hash values that are then saved on the blockchain. The triggering of the artificial intelligence model for the classification of the event messages is done by smart contracts, which in turn successfully repels the network from the attacks of false data insertion.
The study presented in [20] applied a clustering-based framework that highly enhanced the efficiency and security of routing in fog-assisted vehicular networks. Grouping of vehicles was done to lower routing overhead and to create a more stable topology. The selection of cluster heads was done according to the Euclidean distance

criterion, whereby the vehicle with the shortest cumulative distance to its neighboring vehicles takes over as the cluster head. The reliability of the vehicles is measured through a polynomial behavior model, which is used to predict the expected behavior of the nodes and to locate the trusted ones. In this architecture, the use of fog nodes for supporting vehicular applications calls for a dynamic load-balancing strategy among the fog nodes. The weight of each node is calculated by dividing its available bandwidth by the number of requests it receives. A dual-threshold mechanism is employed thereafter to dynamically redistribute the requests—more tasks are assigned to the less loaded nodes, while the overloaded nodes are relieved of some of their tasks.

Finally, [21] proposed a novel routing protocol based on trust that is deployed together with Untrust Scores (US) calculated through a sequence detection system operated on a fog server. The system consists of three different machine learning classifiers—Decision Tree, Random Forest, and Extra Trees, which are combined by a majority voting scheme to classify traffic patterns as either normal or abnormal. Consequently, the untrust scores of vehicles are tweaked: they go up for the detection of anomalies, and they stay the same for all other cases. The modified AODV protocol which is used for routing decisions, picks the optimal path with the least number of hops and the lowest overall untrust score, thus guaranteeing both the efficiency and security of data transmission.

To sum up, the current literature points out that machine learning, fuzzy logic, blockchain, and fog computing are the main players in the area of security, reliability and performance of vehicular networks and have the strongest integrations. Nevertheless, the majority of the surveys consider these aspects separately by either giving priority to security or Quality of Service and not merging them into a single adaptable framework. This deduction encourages the current research which aims at developing a wide-ranging routing scheme that will mutually enhance the three factors of security, QoS, and energy consumption by means of a blended machine learning-fuzzy logic technique under the scenarios of fog and SDN-enabled networks.

3. Fundamentals of the Proposed Mechanism

This section dwells on the core components on which the proposed model is constructed. Its aim is to achieve secure and reliable routing within vehicular networks.

3.1 Reinforcement Learning

The model proposed in this study utilizes a constrained Q-Learning algorithm. It limits the action space by putting restrictions on the candidate actions. This approach seeks to improve AODV protocol-based route discovery. A two-step process is used to filter candidate vehicles for data transfer. Overall trust level is assessed as a weighted function of Direct Trust (DT), Recommended Trust (RT) from neighboring nodes, and Machine Learning-based Contextual Trust (MT), which is determined by the following equation:

$$\mathrm{TTS_i}\,(t) = \mathrm{w_d}\,\mathrm{DT_i}(t) + \mathrm{w_r}\mathrm{RT_i}(t) + \mathrm{w_m}\mathrm{MT_i}(t) \quad (1)$$

Direct Trust (DT) is defined as a weighted combination of two main factors: the Authentication Success Rate (ASR) between the source vehicle and the candidate relay vehicle, which is determined during a specific time period, and Packet Integrity. The ASR is determined by dividing the number of successful authentication attempts by the total number of attempts made during the monitored period. The overall Packet Integrity assessment includes quality of the communication link, authentication indicators, and a security factor which is derived from machine learning outputs, and indicates potential attacks. The following formula indicates this kind of trust (developed with reference to [14,22] and augmented in the current research):

$$\mathrm{DT_i}(t) = (\omega_1 \mathrm{ASR}(t) + \omega_2 \mathrm{Pac_{integrity}}(t)) * \mathrm{P\_N}(t) \quad (2)$$

In order to make Direct Trust (DT) more sensitive to potential assaults, a penalty factor is contained in the previous equation. This modification guarantees that the trust value decreases significantly as the number of suspicious events increases within the monitoring time window T. It is worth mentioning that the authentication process among cars relies on Elliptic Curve Cryptography (ECC) and in particular, uses the Curve25519 algorithm [23].

Recommended Trust (RT), which is sometimes called neighbor-based trust, is determined by the mean trust that the sender vehicle's neighbors have for the target vehicle (i.e., the candidate relay). During this computation, the direct trust of each neighbor for the target is scaled by the sender vehicle's direct trust with that neighbor, which acts as the weighting factor. This relationship is mathematically presented in the equation [15]:

$$\mathrm{RT_i}(t) = \frac{\sum_{j=1}^{R} \mathrm{DT_{Src,j}} * \mathrm{DT_{j,i}}}{\sum_{j=1}^{R} \mathrm{DT_{Src,j}}} \quad (3)$$

Finally, Machine Learning-based Trust (MT) is achieved via the hierarchical machine learning model's outputs that are spread along the SDN controller and the fog nodes in our framework (more detail in Section 3.3). This trust standard is shaped according to the prediction of the probability that a vehicle is showing some kind of suspicious or abnormal behavior, and it is defined as follows:

$$\mathrm{MT_i}(t) = 1 - \mathrm{pro_{attack}} \quad (4)$$

The lowest trust nodes will always be eliminated from the selection process, which implies that the process will be looking for the highest-quality candidate nodes determined by two metrics: Packet Forwarding Ratio (PFR) and Expected Transmission Time (ETT). The PFR is the portion of the packets successfully passed from one

vehicle to another, with the total being the sum of packets sent to that vehicle from the first one and the second one. The formal definition of this metric is given in the following equation [17]:

$$PFR_t(v_j)=\frac{F_{t(v_j)}}{S(v_i,v_j)} \quad (5)$$

The Expected Transmission Time (ETT) from vehicle $i$to vehicle $j$is measured according to four parameters. These are: the packet size M, the network data rate B, the probability of successful packet reception by vehicle j, and the probability of successfully receiving an acknowledgment from vehicle j. The relationship is formally revealed in the following equation [17]:

$$ETT=\frac{1}{D_f(v_i,v_j)*D_r(v_i,v_j)}*\frac{M}{B} \quad (6)$$

Generally, the two formerly defined quality metrics (presented in Equations (5) and (6), which also reflect a form of trust, are combined through a weighted function. The greedy-£ policy then adopts action from the set of acceptable candidates (the reduced action space), preventing the reinforcement learning algorithms from exploring unsuitable options, such as forwarding to untrustworthy nodes. This is particularly important given the highly dynamic nature of vehicular networks, where the neighbor list changes rapidly. Since the vehicular network under study employs Unmanned Aerial Vehicles (UAVs) as aerial relays, it is necessary to establish a dedicated strategy for handling the aerial network, which is addressed in the following section.

3.2 Fuzzy Logic

The proposed model applies fuzzy logic to make decisions about using aerial relays as part of the routing process. The designed inference system depends on three input parameters, which begin with the aerial node congestion index as the initial parameter. The index measures performance by dividing the average queue length during a specific time frame by the highest recorded queue length. This follows the formula presented in equation [24]:

$$UNCI_u=\frac{AQL_u}{MQL_u} \quad (7)$$

The second parameter is associated with the dependability of the ground pathway, which is the mean trust rating given to the nodes that make up that route. Route dependability is revealed in the following equation:

$$T_{avg}=\frac{\sum_{i=1}^{n} TTs_i}{n} \quad (8)$$

The third parameter is concerned with the data significance. In the proposed model, importance is divided into three tiers: high, for packets linked to critical transmission services; medium, for real-time application data; and low, for data from entertainment or non-essential applications.

The exact values of the input parameters are initially changed into fuzzy values by the fuzzifier, which utilizes the related membership functions. Then, the fuzzy inference engine assesses the if-then rules set in the rule base (Table 1), which identify whether utilizing the aerial relay for data forwarding is appropriate. Finally, the defuzzifier changes the inferred fuzzy outputs back into exact values using the Center of Gravity (CoG) approach [15].

Thus, according to the resulting suitability score, the model determines the proportion of reliance on the aerial path versus the terrestrial path. In addition to that, when making the routing decision, the system combines data priority in accordance with the computed proportions.

Table (1). Fuzzy Rule Base

Priority	Congestion	Reliable	suitability score
High	Low	Low	Excellent
High	Medium	Low	Good
High	High	Low	Fair
High	Low	Medium	Good
High	Medium	Medium	Fair
High	High	Medium	Poor
High	Low	High	Fair
High	Medium	High	Poor
High	High	High	Reject
Medium	Low	Low	Good
Medium	Medium	Low	Fair
Medium	High	Low	Poor
Medium	Low	Medium	Fair
Medium	Medium	Medium	Poor
Medium	High	Medium	Reject

Medium	Low	High	Poor
Medium	Medium	High	Reject
Medium	High	High	Reject
Low	Low	Low	Fair
Low	Medium	Low	Poor
Low	High	Low	Reject
Low	Low	Medium	Poor
Low	Medium	Medium	Reject
Low	High	Medium	Reject
Low	Low	High	Reject
Low	Medium	High	Reject
Low	High	High	Reject

3.3 Centralized Control and Distributed Computing

The framework proposed in this study employs both the SDN controller and the fog computing layer to detect security threats, particularly abnormal traffic flows, using a hierarchical machine-learning model [25, 26]. Moreover, it balances the load across the network, thus improving the QoS performance. At the heart of the system is a centralized anomaly classifier, which employs the Random Forest algorithm and bases its decisions on flow-level features, such as flow rate, duration, total number of bytes and packets, and other similar indicators. On the other hand, the fog-level anomaly classifier, which is built using a Decision Tree, relies on packet-level features such as packet length, the TCP sliding-window value, and more. We chose this classifier beacause of its favorable compromise among precision, speed, and power consumption in environments that have limited resources such as fog nodes.

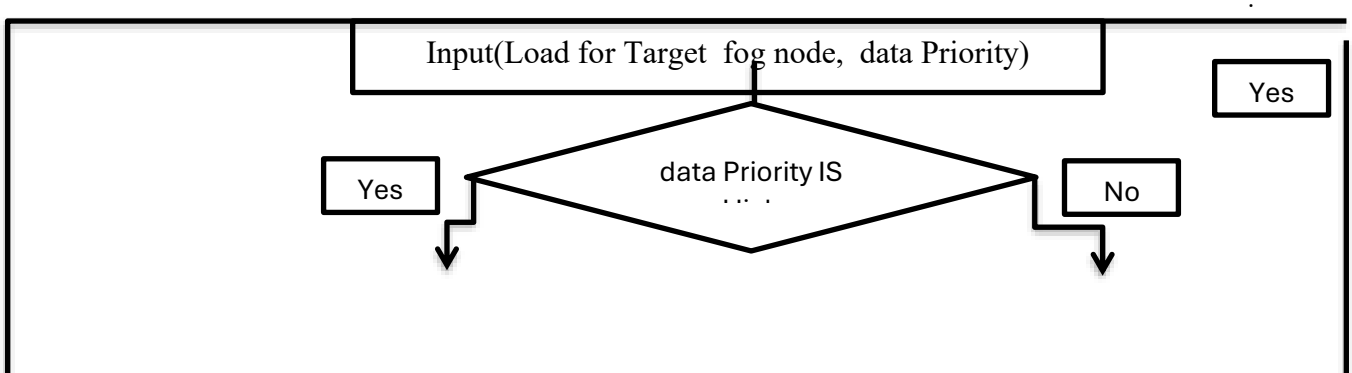
In order to increase accuracy, we use a rule-based classifier (GARP) along with the Decision Tree at the fog level. This classifier works using Gene Expression Programming which develops and optimizes fuzzy rules automatically [27, 28, 29]. The rule sets formed are categorized in behavioral anomalies, security and threat indicators, network-performance situations, temporal and spatial context, and emergency situations, respectively. Thus, beside the outputs of the Decision Tree, including the anomaly score and the confidence associated with the classification decision, the classifier is given information on the rule-set categories that are being used. The chromosomes of the genetic algorithm in this setting signify the fuzzy rules, and their quality is gauged through a fitness function that relies on two weighted criteria were—accuracy and simplicity—expressed as follows:

$$\text{Fitness}_{\text{rule}}=(0.7*\text{Accuracy})+(0.3*\text{Simplicity}) \quad (9)$$

The superior rules selected from the earlier set are the basis for the generation of new rules (i.e., reproduction) by means of crossover and mutation operations. The cycle is repeated, removing less effective rules and putting in new ones until the point of the best performance is reached. Consequently, the classifier is considered appropriate to find security threats that were unknown before.

A weighted voting technique is applied to the integration of two classifiers, where the weights receive continuous updates according to a coefficient which indicates the system's trust in the outputs of the classifiers. This trust is based on historical usage patterns that have been monitored over a time window of duration t.

Back to the Software-Defined Networking (SDN) controller, it plays a role of a load balancer between fog nodes, relying on two major metrics: the node load and the predicted task response time (Pre_Res_Time). A Linear Regression machine-learning model [30] is used for estimating the predicted response time, which is trained on historical data that covers the Round-Trip Time (RTT) between vehicles and fog nodes—this can signal the state of congestion in the wireless medium—processing time, and actual observed response times as well. The predicted response time is then put through a dual-threshold system to determine whether the task needs to be moved to another fog node, or if a different task should be selected especially in situations where a fog node is overloaded. It is worth mentioning that data priority is considered in the decision-making process and serves as a determining factor in whether task migration should take place when the load condition is not enough by itself. Figure (1) shows the flow diagram of the load-balancing mechanism in our study.



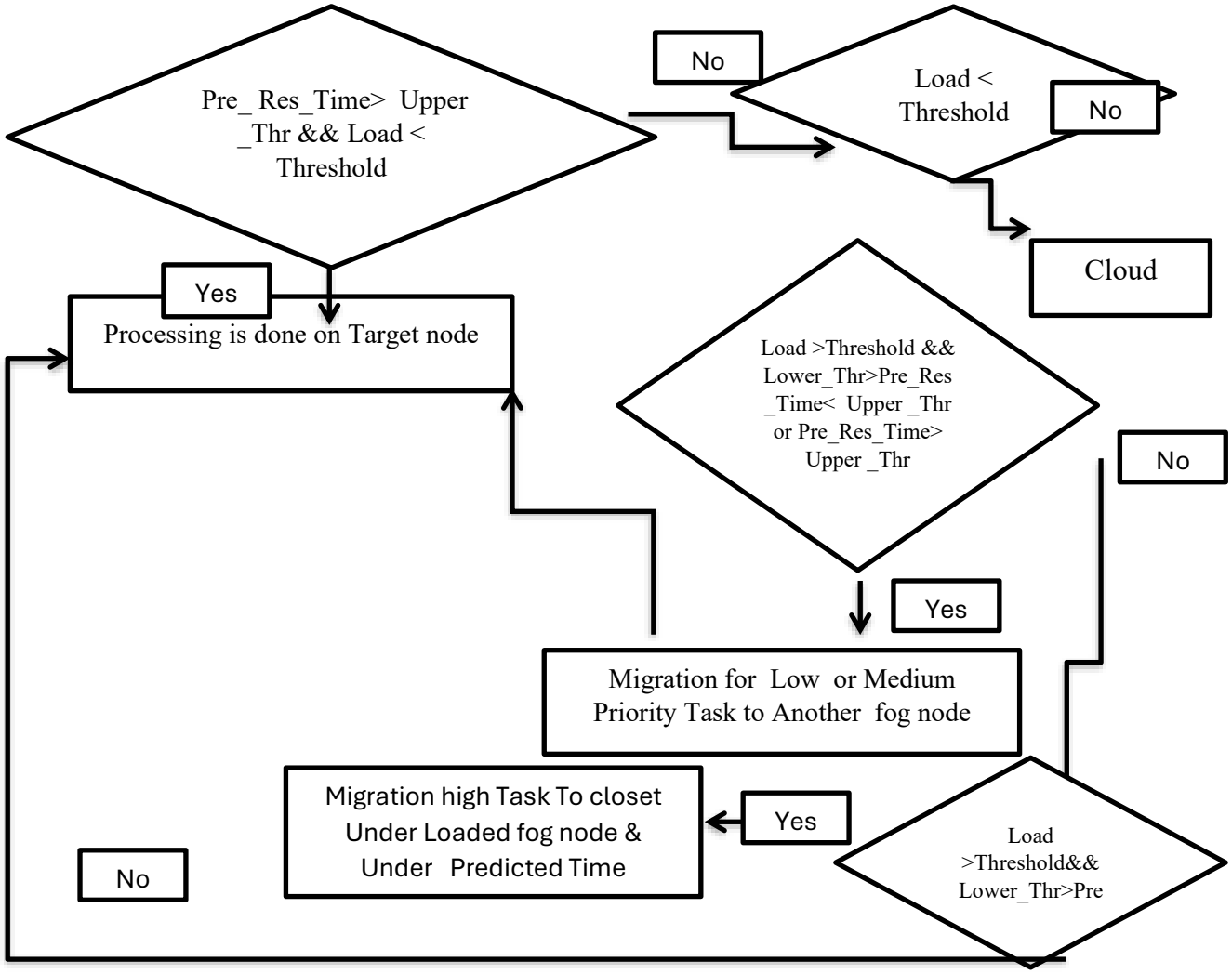


Figure (1): Flow Diagram of the Proposed Load-Balancing Mechanism in Our Study

4. Proposed Framework

The proposal is factualized in the design of a network comprising a Software-Defined Networking (SDN) controller, fog cells, and a UAV-assisted VANET which facilitates the transfer of data through air. As depicted in Figure (2), the structure seeks to improve the routing by elevating the Quality of Service (QoS) and by data protection through the identification and disallowance of irregular node.

The proposal is factualized in the design of a network comprising a Software-Defined Networking (SDN) controller, fog cells, and a UAV-assisted VANET which facilitates the transfer of data through air. As depicted in Figure (2), the structure seeks to improve the routing by elevating the Quality of Service (QoS) and by data protection through the identification and disallowance of irregular nodes.

In the first layer made up of terrestrial vehicles, every car serves as a worker in the Q-Learning reinforcement algorithm to appoint a neighboring node for the data transfer. Only trustworthy neighbors meeting the application-specific performance requirements will be the candidates. Trust is calculated as a composite trust factor where three elements: Direct Trust, Recommended Trust, and Machine Learning-based Trust, are summed up with different weights. FIFO and ETT are the metrics used when picking the neighbor besides the ECC-based authentication that is used in the beginning of all communication.

In the view of an airborne network, it becomes imperative to assess the best use of UAVs. Fuzzy logic is put into practice, down to the fog cell level, for the purpose of determining aerial forwarding. The inference engine takes three input parameters into account: data priority, reliability of the ground route, and the aerial node congestion index. Depending on the obtained suitability score and the use of a dual-threshold system, the architecture makes the choices about the share of the traffic going through ground and aerial paths in such a way that the routing decisions are in compliance with the data priorities.

Two functions that complement each other are put into practice at the fog layer. The first one concerns data processing, while the second one deals with security. For security purposes, a supervised Decision Tree classifier is used which has been trained on packet-level features and it provides very good accuracy in catching anomalies, but it introduces the drawback of taking a longer time for processing. This classifier works hand in hand with a gene-generated rule-based classifier (GARP), and a voting mechanism is used to combine their outputs. The

combined result of the classifiers is then given to the SDN-level Random Forest classifier, which is based on flow-level features and is able to discern temporal aspects more effectively, but it does this at the cost of precision. This multi-tiered strategy greatly minimizes false positives.

The real-time, latency-sensitive handling is required for certain vehicular applications in data processing. The highest-priority data is processed at the fog layer itself, without the cloud's involvement, by picking fog nodes having suitable loads and making sure that the expected response time aligns with the time-critical applications' constraints. The SDN controller receives all the load balancing parameters periodically from the fog layer.

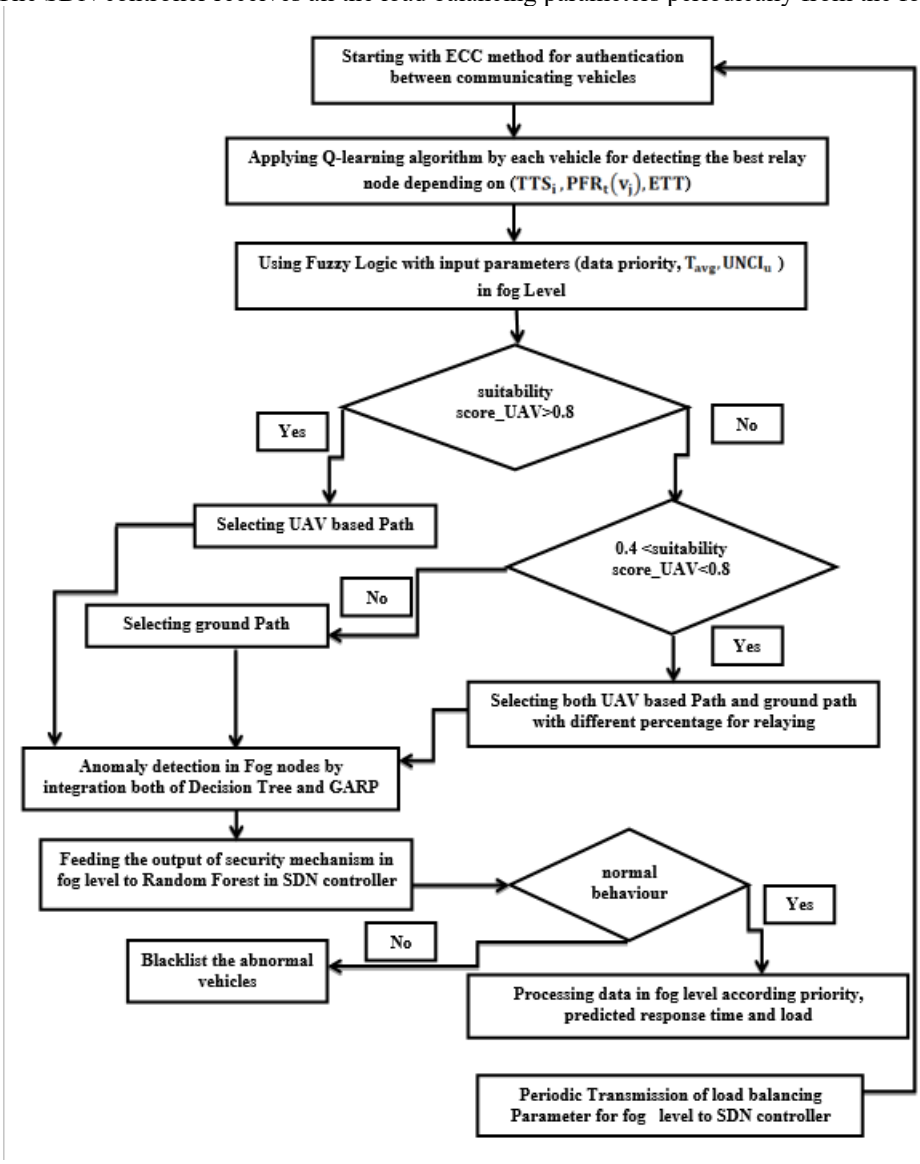


Figure (2): Flow Diagram of the Proposed Framework

5. Performance Evaluation

The NS-3 simulation was utilized to evaluate the proposed framework performance, and the results obtained were compared with those of the QL-TRT protocol [17]. The effectiveness of the framework was measured by four KPIs: end-to-end delay, throughput, packet delivery ratio, and attack success rate including Black Hole (BHA) and Gray Hole (GHA) scenarios.

The analysis of these metrics was done by tweaking significant network parameters like the number of vehicles, vehicle speeds, and the portion of nodes compromised in the network. The simulation settings are stated in Table (2). The results reported are the averages of 100 independent simulation runs for each scenario.

It should be noted that during the performance testing with respect to network density, 10% of the total vehicles were considered malicious nodes. In the experiments regarding the effect of different proportions of malicious nodes, the total number of vehicles was always 40 to achieve consistency in the evaluation.

Table (2): Simulation Parameters

parameter	Value
Simulation area	6 km × 6 km
Communication protocol	IEEE 802.11p

Transmission range	250 m
Mobility model of vehicles	Random-Way point
Q-Learning -learning rate	0.5
Q-Learning discount factor	0.9
Vehicle velocity	20-80Km/h
Application-USM traffic(Size/Rate)	Exp.256 bytes/ Exp.10 rps
Application –RTS traffic(Size/Rate)	Con. 1500 bytes/Con. 10 rps
Application-COP traffic(Size/Rate)	Exp. 256 bytes/Exp. 10 rps
Number of Vehicles	20,40,60,80,100
Percentage of Malicious Vehicles	5%,10%,15%,20%,25%,30%
Number of UAVs	12
Simulation time	1000 s

The results shown in Figure (3) refer to that the suggested structure produced smaller end-to-end delay as the network's vehicular population grew, when compared with the QL-TRT protocol. The reason behind this superiority in performance can be understood by analyzing the major elements of the proposed system that improve temporal efficiency, despite the fact that a security layer consisting of hierarchical machine learning and elliptic curve-based authentication for recognizing abnormal behavior is in place.
The most tremendous benefit of the framework comes from the UAV-assisted forwarding, which is used not only to fill the gaps caused by the unreliability of ground paths but also to provide support for different types and levels of data, depending on the services and UAV's load index. It is also worth mentioning that fog computing does the processing of locality-critical data and thus effectively manages latency. Finally, the reinforcement learning technique is applied to optimize the ground paths selection, which directly considers the Quality of Service (QoS) metrics as a part of the decision-making process.

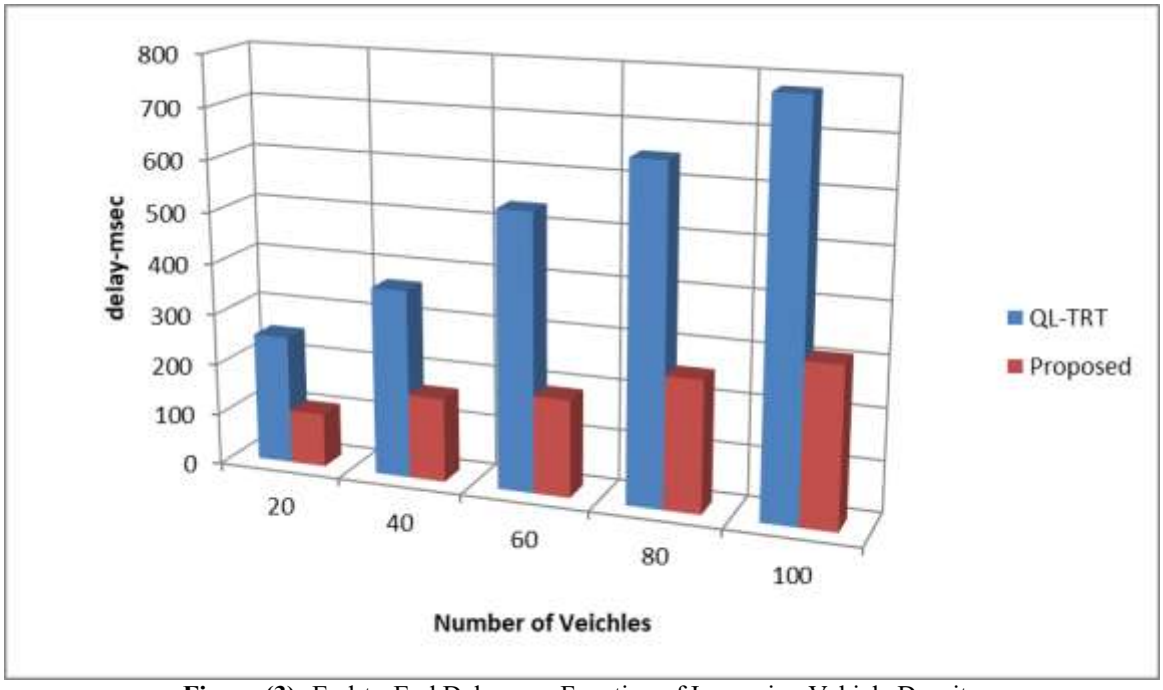


Figure (3): End-to-End Delay as a Function of Increasing Vehicle Density

In Figure (4) throughput is depicted in relation to the rising vehicle population. Despite the overall throughput being gradually reduced with the network's increased congestion, the proposed framework still considerably surpasses the QL-TRT protocol. The main reason for this improvement lies in the strategic and smart handling of QoS metrics by the framework at both the fog level and during the choosing of ground and UAV-assisted paths. The framework's use of a hybrid ground-and-air network for data forwarding cuts down the effect of congestion in the network on transmission delays, which in turn results in better throughput. Besides, the application of preliminary authentication before depending on the outputs of the hierarchical machine learning classifiers is beneficial in preventing packet loss, thus further contributing to the throughput that has been gained.

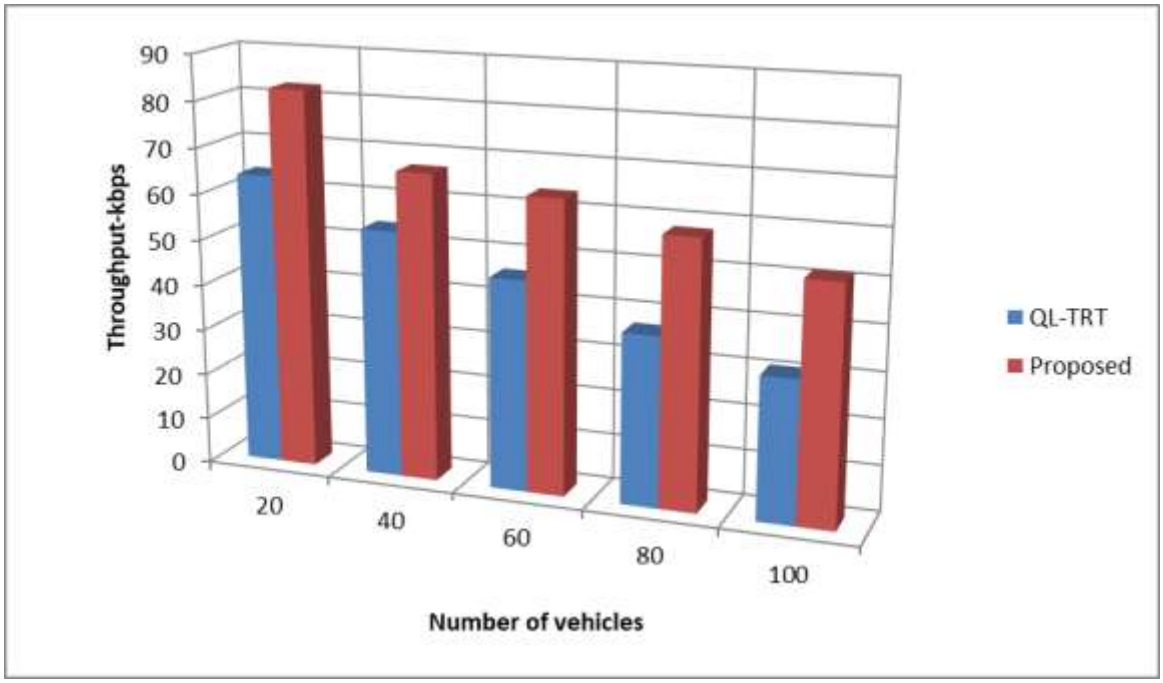


Figure (4): Throughput as a Function of Increasing Vehicle Density

Figure (5) clearly depicts the proposed framework's superiority over the QL-TRT protocol in terms of packet delivery ratio, especially with the increase of the malicious nodes in the network. The image reflects the performance of the two methods in filtering out the untrustworthy nodes from the routes taken by the data, thus minimizing the loss of packets and raising the overall delivery rates.

The framework we proposed, along with the consortium of authentication and machine learning-based attack detection, intensifies the identification of the bad nodes. While on the other hand, the QL-TRT protocol invests only in judging node trustworthiness through packet forwarding ratio and expected transmission time assessment, which is an ineffective defense against sophisticated attacks.

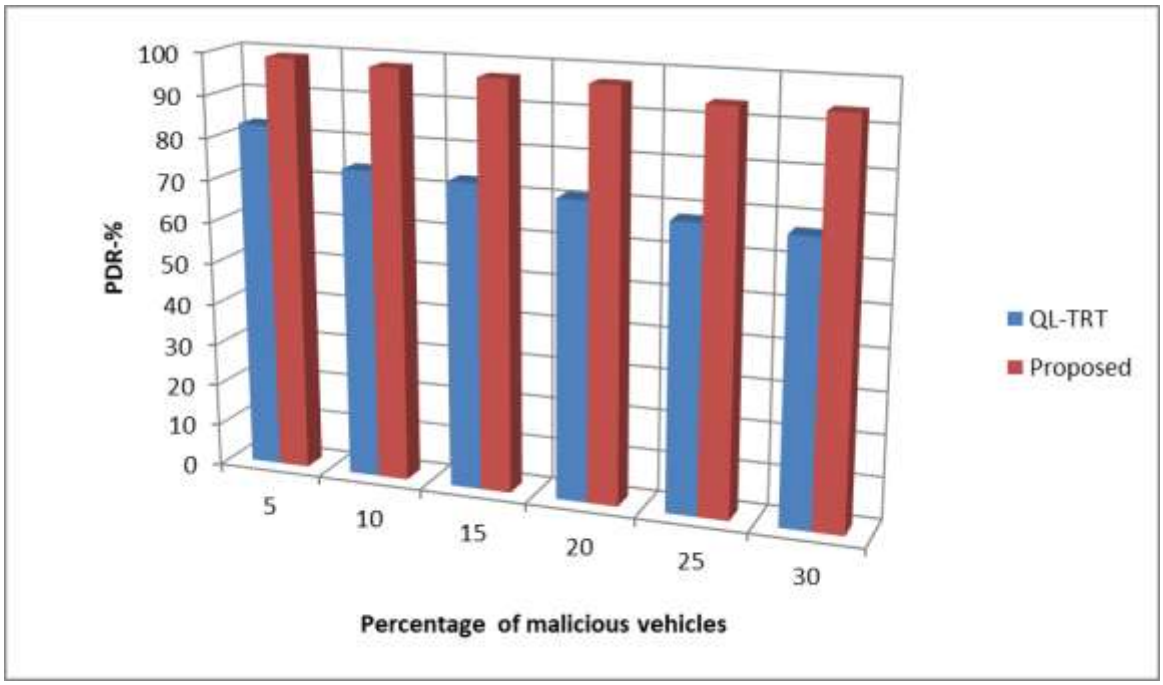


Figure (5): Packet Delivery Ratio as a Function of the Percentage of Malicious Nodes in the Network

The results presented in Figure (6) not only support but also confirm the superiority of the new structure, in the sense of the packet delivery ratio, over the QL-TRT protocol as the speed of the vehicles rises. Fast movement of vehicles results in quick alterations of the network topology and this can lead to packet loss which in turn might result in the process of route discovery to be repeated, the selection of new forwarding nodes being needed for every hop.

The reason for this performance advantage is the framework's architecture allowing for the incorporation of link quality in the trust assessment of the nodes. In cases where link quality affects the integrity of the packets, it has

a direct impact on the trust score, possibly promoting the UAV-assisted paths over the unreliable land routes. The reverse is true for the QL-TRT protocol, which mainly works on the basis of the expected transmission time, a parameter that is only indirectly dependent on the speed of the vehicles. Hence, even though this enables some adjustments to the mobility, it is more sluggish and less dynamic than the proposed approach.

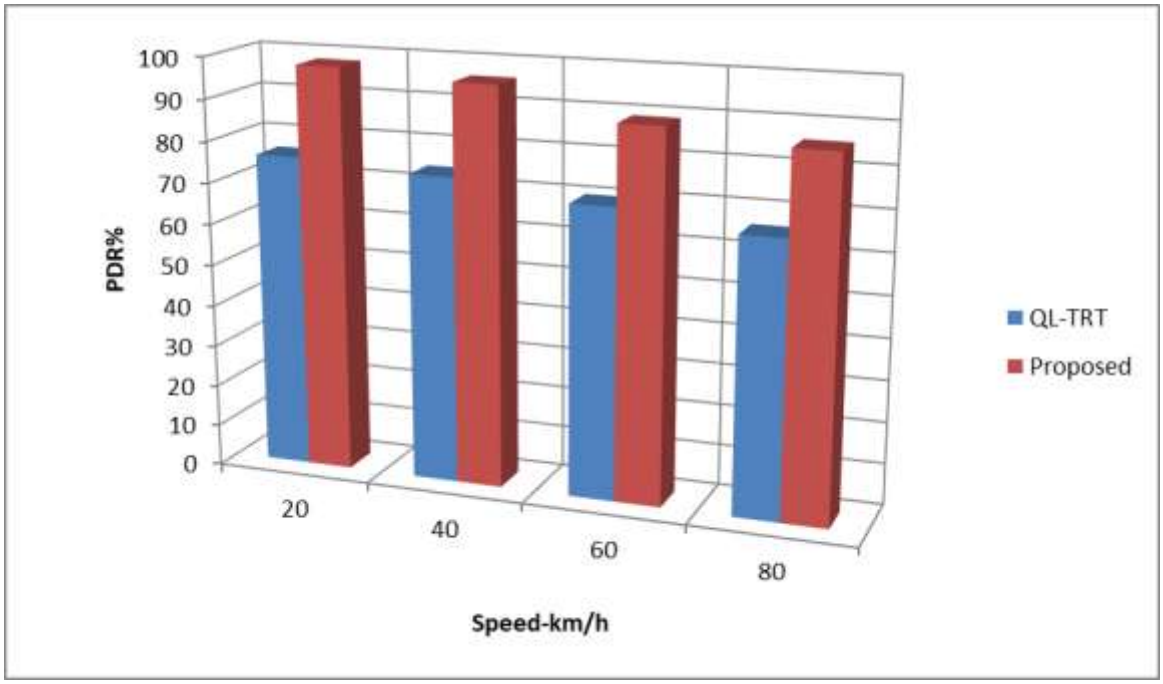


Figure (6): Packet Delivery Ratio as a Function of Increasing Vehicle Speed

Figure (7) presents the capability of the security mechanisms used in both protocols with respect to malicious node detection. From the data, it is observed that the detection rate of the suggested framework is superior to that of the QL-TRT protocol, especially when the ratio of malicious nodes goes up. Hence, it can be said that the attack success rate is inversely proportional to the attack detection rate, as the initial authentication plus behavioral analysis combination filters out a large number of attacks effectively. After that, the SDN controller applies the right security measures at the data tier to segregate the identified attacker.

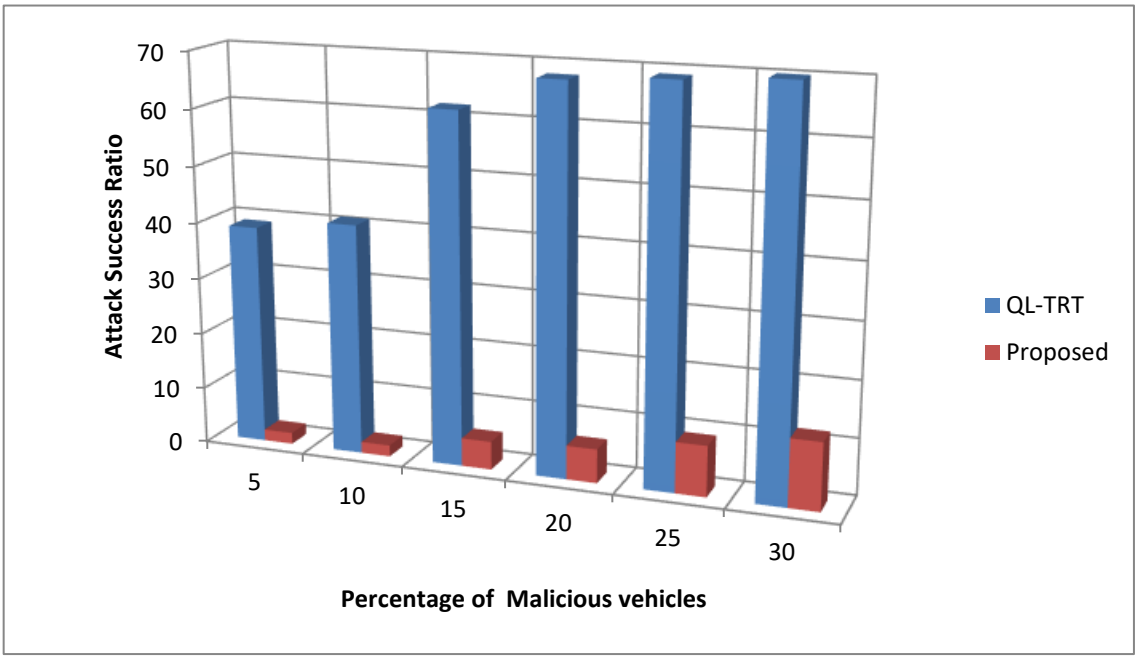


Figure (7): Attack Success Rate as a Function of the Percentage of Malicious Nodes in the Network

6. Conclusion

To conclude, the proposed framework in this paper has sought to obtain secure and efficient routing by combining the advantages of SDN and fog computing in resolving the security problem through a hierarchy of machine learning, while at the same time, ensuring Quality of Service (QoS) through a load-balancing technique in the fog layer up to the ranking of data, controlled by the SDN controller. Furthermore, both issues—security and QoS—

are not only considered separately but rather at the vehicular network level, where the network is modeled as hybrid that includes aerial relays decided by fuzzy logic after ground paths identified through reinforcement learning, together with ECC-based authentication among the cars that are connected.

The framework has been tested through NS3 simulations, and the outcome shows that it outperforms the QL-TRT protocol in all measured aspects even though there were some malicious nodes existing in the network. This includes metrics related to QoS, such as end-to-end delay and throughput at different vehicle densities as well as packet delivery ratio which was studied at different network densities and vehicle speeds. Security aspects were also enhanced, especially the attack success rate which was measured as a function of the percentage of bad nodes in the network.

The findings of this study have led to the conclusion that the proposed framework can be implemented in densely populated urban areas, as it provides a good trade-off between security and attacks and makes use of both aerial relays and fog to diminish the negative impacts of security mechanisms.

For future studies, we will continue with evaluations of performance along with examining the use of other methodologies for authentication, like those based on blockchain, and these will be compared with ECC to find out which parts contribute the most to the security of the framework. Also, it is possible that future studies will challenge the use of Information-Centric Networking (ICN) in vehicular networks (VANETs) in order to gain even better efficiency and reliability..

7. References

1. Al-essa, R., & Al-suhail, G. (2023). AFB-GPSR: Adaptive beaconing strategy based on fuzzy logic scheme for geographical routing in a mobile ad hoc network (MANET). *Computation, 11*, 174. https://doi.org/
2. Ali, I., Chen, Y., Ullah, N., Kumar, R., & He, W. (2021). An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs. *IEEE Transactions on Vehicular Technology, 70*(2), 1278–1291. https://doi.org/
3. Belamri, F., Boulfekhar, S., & Aissani, D. (2021). A survey on QoS routing protocols in vehicular ad hoc network (VANET). *Telecommunication Systems, 78*(1), 117–153. https://doi.org/
4. Banafshehvaragh, S., Zarei, M., & Rahmani, A. (2025). A reliable score-based routing protocol using a fog-assisted intrusion detection system in vehicular ad-hoc networks. *Scientific Reports, 15*, 25709. https://doi.org/
5. Brown, M. S., Alandur, M. S. R., Chaudhari, S., & Sistla, S. (2025). A genetic algorithm for rule generation to predict student success. In *2025 IEEE Integrated STEM Education Conference (ISEC)* (pp. 1–5). Princeton, NJ, USA. https://doi.org/
6. Chiang, C. (2010). A genetic programming based rule generation approach for intelligent control systems. In *2010 International Symposium on Computer, Communication, Control and Automation (3CA)*. Tainan, Taiwan: IEEE. https://doi.org/
7. Devi, A., Kait, R., & Ranga, V. (2025). Secure and efficient routing in fog-enabled VANETs: A clustering-based approach. *International Journal of Current Science Research and Review, 8*(3). https://doi.org/
8. El-Shafai, W., Azar, A. T., & Ahmed, S. (2025). AI-driven ensemble classifier for jamming attack detection in VANETs to enhance security in smart cities. *IEEE Access, 13*, 50687–50713. https://doi.org/
9. Falahatraftar, F., Pierre, S., & Chamberland, S. (2020). A multiple linear regression model for predicting congestion in heterogeneous vehicular networks. In *2020 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 93–98). Thessaloniki, Greece. https://doi.org/
10. Fardad, M., Mianji, E. M., Muntean, G.-M., & Tal, I. (2022). A fast and effective graph-based resource allocation and power control scheme in vehicular network slicing. In *2022 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)* (pp. 1–6). IEEE. https://doi.org/
11. Ghorai, C., Shakhari, S., & Banerjee, I. (2021). A SPEA-based multimetric routing protocol for intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems, 22*, 6737–6747. https://doi.org/
12. Honarmand, F., & Keshavarz-Haddad, A. (2024). T-AODV: A trust-based routing against black-hole attacks in VANETs. *Peer-to-Peer Networking and Applications, 17*(3), 1–13. https://doi.org/
13. Khan, A., Siddiqui, A. A., Ullah, F., Bilal, M., Piran, M. J., & Song, H. (2022). VP-CAST: Velocity and position-based broadcast suppression for VANETs. *IEEE Transactions on Intelligent Transportation Systems, 23*, 18512–18525. https://doi.org/
14. Koshiyama, A. S., Tanscheit, R., & Vellasco, M. M. B. R. (2019). Automatic synthesis of fuzzy systems: An evolutionary overview with a genetic programming perspective. *WIREs Data Mining and Knowledge Discovery, 9*(2). https://doi.org/
15. Kudva, S., Badsha, S., Sengupta, S., La, H., Khalil, I., & Atiquzzaman, M. (2021). A scalable blockchain-based trust management in VANET routing protocol. Elsevier Inc. https://doi.org/
16. Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. A., Panigrahi, B. K., & Veluvolu, K. C. (2021). Black-hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocessors and Microsystems, 80*, 103352. https://doi.org/
17. Luo, L., Sheng, L., Yu, H., & Sun, G. (2022). Intersection-based V2X routing via reinforcement learning in vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems, 23*, 5446–5459. https://doi.org/

18. Mekonen, B., Bane, L., & Fite, N. B. (2025). Detection of false position attacks in VANETs through bagging ensemble learning. *PLOS ONE, 20*(8). https://doi.org/
19. Mianji, E. M., Muntean, G. M., & Tal, I. (2023). 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). Florence, Italy. https://doi.org/
20. Mustafa, S., Khattab, M., & Abdul, K. (2023). An assessment of ensemble voting approaches, random forest, and decision tree techniques in detecting distributed denial of service (DDoS) attacks. *Journal of Electrical and Electronic Engineering, 20*, 16–24. https://doi.org/
21. Roh, B.-S., Han, M.-H., Ham, J.-H., & Kim, K.-I. (2020). Q-LBR: Q-learning based load balancing routing for UAV-assisted VANET. *Sensors, 20*, 5685. https://doi.org/10.3390/s20195685
22. Samara, G., Odeh, M., Aldaoud, E., Sabbah, S., Al-Mousa, M. R., & Alluwaici, M. (2025). Secure routing in VANET systems using fog computing and software defined networks. *International Journal of Advanced Soft Computing and Applications, 17*(2). https://doi.org/
23. Sree, A., & Sharma, K. (2025). Blockchain-based machine learning model for secure data transfer and route preservation in UAV integrated VANET systems. *Journal of Machine and Computing*. https://doi.org/10.53759/7669/jmc202505182
24. Shen, Y., Shen, S., Li, Q., Zhou, H., Wu, Z., & Qu, Y. (2023). Evolutionary privacy-preserving learning strategies for edge-based IoT data sharing schemes. *Digital Communications and Networks, 9*, 906–919. https://doi.org/
25. Sreenivasulu, K. N., Vinay, N. A., & Shwetha, M. (2025). Systematic implementation of ECC Curve 25519 for enhancing the fingerprint security. In *2025 International Conference on Next Generation Communication & Information Processing (INCIP)* (pp. xx–xx). Bangalore, India. https://doi.org/
26. Stepien, K., & Poniszewska-Maranda, A. (2020). Security methods against black hole attacks in vehicular ad-hoc network. In *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)* (pp. 1–4). Cambridge, MA, USA. https://doi.org/
27. Tal, I., & Muntean, G.-M. (2017). Towards reasoning vehicles: A survey of fuzzy logic-based solutions in vehicular networks. *ACM Computing Surveys (CSUR), 50*(6), 1–37. https://doi.org/
28. ul Hassan, M., Al-Awady, A. A., Ali, A., Sifatullah, Akram, M., Iqbal, M. M., Khan, J., & Abdelrahman Ali, Y. A. (2024). ANN-based intelligent secure routing protocol in vehicular ad hoc networks (VANETs) using enhanced AODV. *Sensors, 24*, 818. https://doi.org/
29. Wang, X., Weng, Y., & Gao, H. (2021). A low-latency and energy-efficient multimetric routing protocol based on network connectivity in VANET communication. *IEEE Transactions on Green Communications and Networking, 5*, 1761–1776. https://doi.org/
30. Zhang, X., Xia, W., Wang, X., Liu, J., Cui, Q., Tao, X., & Liu, R. P. (2022). The block propagation in blockchain-based vehicular networks. *IEEE Internet of Things Journal, 9*(11), 8001–8011. https://doi.org/