



Article

# Authentication and Resource Allocation Strategies during Handoff for 5G IoVs Using Deep Learning

Hemavathi <sup>1,\*</sup> , Sreenatha Reddy Akhila <sup>1</sup> , Youseef Alotaibi <sup>2</sup> , Osamah Ibrahim Khalaf <sup>3</sup> and Saleh Alghamdi <sup>4</sup>

<sup>1</sup> Department of Electronics and Communication Engineering, B.M.S. College of Engineering, Bengaluru 560019, India; akhilas.ece@bmsce.ac.in

<sup>2</sup> Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah 21955, Saudi Arabia; yaotaibi@uqu.edu.sa

<sup>3</sup> Al-Nahrain Nanorenewable Energy Research Center, Al-Nahrain University, Baghdad 10001, Iraq; usama.ibrahem@coie-nahrain.edu.iq

<sup>4</sup> Department of Information Technology, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia; s.algamedi@tu.edu.sa

\* Correspondence: hemavathi.ece@bmsce.ac.in

**Abstract:** One of the most sought-after applications of cellular technology is transforming a vehicle into a device that can connect with the outside world, similar to smartphones. This connectivity is changing the automotive world. With the speedy growth and densification of vehicles in Internet of Vehicles (IoV) technology, the need for consistency in communication amongst vehicles becomes more significant. This technology needs to be scalable, secure, and flexible when connecting products and services. 5G technology, with its incredible speed, is expected to power the future of vehicular networks. Owing to high mobility and constant change in the topology, cooperative intelligent transport systems ensure real time connectivity between vehicles. For ensuring a seamless connectivity amongst the entities in vehicular networks, a significant alternative to design is support of handoff. This paper proposes a scheme for the best Road Side Unit (RSU) selection during handoff. Authentication and security of the vehicles are ensured using the Deep Sparse Stacked Autoencoder Network (DS2AN) algorithm, developed using a deep learning model. Once authenticated, resource allocation by RSU to the vehicle is accomplished through Deep-Q learning (DQL) techniques. Compared with the existing handoff schemes, Reinforcement Learning based on the MDP (RL-MDP) has been found to have a 13% lesser decision delay for selecting the best RSU. A higher level of security and minimum time requirement for authentication is achieved using DS2AN. The proposed system simulation results demonstrate that it ensures reliable packet delivery, significantly improving system throughput, upholding tolerable delay levels during a change of RSUs.

**Keywords:** Deep-Q learning; RSU; URLLC; DSRC; E2E Delay; IoV; Markov Decision Process; authentication



**Citation:** Hemavathi; Akhila, S.R.; Alotaibi, Y.; Khalaf, O.I.; Alghamdi, S. Authentication and Resource Allocation Strategies during Handoff for 5G IoVs Using Deep Learning. *Energies* **2022**, *15*, 2006. <https://doi.org/10.3390/en15062006>

Academic Editor: Sangheon Park

Received: 6 January 2022

Accepted: 4 March 2022

Published: 9 March 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Though 5G is yet to be deployed widely, it appears that 5G stands to affect nearly every part of our day to day life, be it health care, education, transportation, industry, smart grids, entertainment and media, etc. 5G is expected to power the future of people's mobility through Internet of Vehicles (IoV) technology. It can be called an Internet on wheels and can allow vehicles to communicate with their drivers, with other vehicles, with traffic signals and roadside infrastructure, or with any other internet-connected item. Features like the ability to stream full video games in vehicles, crash prevention, traffic flow monitoring, safe navigation, intelligent vehicle control, vehicle autonomy, and even electronic toll collection makes IoV one of the attractive applications of 5G.

The concept of connected vehicles is known as vehicular communications or V2X. V2X includes vehicle-to-infrastructure/network (V2I/N) and vehicle-to-vehicle (V2V) [1,2].

IoV is supported by Dedicated Short-Range Communication (DSRC) and cellular mobile communication systems for effective implementation. DSRC standards in the United States and ITS-G5 standards produced by the European Telecommunications Standards Institute (ETSI) have both been created during the last decade to coordinate with the activities of many stakeholders in vehicular communications. The ITS and smart cities protocols are grounded in IEEE 802.11p technology, which offers the framework for vehicle ad hoc network communications. The 3rd Generation Partnership Project (3GPP) has recently been working on integrating V2X services into LTE and future 5G cellular networks [3–5].

The combination of DSRC and cellular communication is capable of improving intelligence and independent driving capability in IoV, by providing safe, intelligent, comfortable, and efficient comprehensive services. With the rapid pace of 5G development, it has been possible to meet different performance criteria's in varied application scenarios [6]. The intelligent transportation system (ITS) is expected to see a boom in the upcoming days due to the unimaginable speeds that can be attained by 5G. Some of the communication requirements of ITS are the low communication delay and high reliability of vehicle status data [7]. To provide a seamless mobility experience to the user, the handoff strategy, similar to cellular communication, is used in IoV. The handoffs may be frequent due to the small coverage area of RSUs and the dynamic nature of the vehicles. V2X has become a key enabler for bringing an innovative level of connectivity to automobiles, especially when combined with onboard computing and sensor technologies.

Since Internet of Vehicles is characterized by a high level of mobility and dynamic changes in topology, handoff is one of the key technologies enabling efficient deployment of these connected and autonomous vehicles for providing seamless communication. The term handoff refers to transferring the active communication from one Road Side Unit to another seamlessly. This could be horizontal or vertical. It is termed horizontal handoff if network access technologies across the RSUs are the same and vertical handoff if access technologies across the RSUs are different.

With self-driving vehicles changing the transportation scenario, connected vehicles are becoming the core of transportation systems. This calls for redefining business models, be it transportation sector, energy sector, and even government regulations. Under such a connected scenario, security in IoV becomes one of the most important entities, since any system failure can directly impact a user's safety. Hence, secure and consistent authentication and low computation overhead are required for the amalgamation of 5G networks and vehicular network technology.

In IoV, communication is between the RSU and vehicles [8,9]. The information is transmitted over an unsecure wireless channel between two communication parties that are highly vulnerable to attacks. Having an efficient authentication scheme ensures that only authorized users are allowed into the network, and it is effective against active and passive attacks, hence satisfying the need for a secure design. In addition, it ensures that communication is amongst trustworthy entities only. For secure communication, mutual authentication among the involved entities is performed by broadcasting periodic safety messages. These messages include critical information about vehicle speed and location, traffic conditions, and braking status. Hence, it becomes significant to guarantee that an acquired safety message comes from legitimate vehicles and is not altered via attackers, as any modification and replaying of the broadcasted messages can be disastrous to drivers [10].

Every vehicle in IoV is viewed as an intelligent object with control units, computing facilities, sensing platforms, and storage that are accessible via V2X. In IoV, communication is over a wireless link that is supported by the 5G technology. Nonetheless, due to densification and with limited resources, it is difficult to schedule the resource to collect and process real-time requests from the vehicles, making it difficult to guarantee efficient and reliable data transmission by traditional IoV communications. Through resource sharing, it will be possible to increase the execution speed of a computing task and overcome the insufficient computing resource problem for the vehicle, thus providing ultra-low latency,

high bandwidth, higher responsiveness, and throughput to the users [11,12]. In reality, the network status and available resources of RSU vary dynamically due to the mobility of vehicles. This results in frequent handoffs between the vehicle and the RSU. To coordinate with V2I links, an effective resource allocation method is required. In traditional methods, resource allocation may be stated as optimization problem using global network information, where QoS requirements of V2I act as a constraint [13,14].

IoV has turned into a new, hotly contested arena for innovations in automobile industries. It calls for the development of applications such as road safety, infotainment, and efficient traffic management. With the foremost use of a vehicle still being driving, it is the automakers who will be responsible for putting IoV technologies in the vehicle [15–17]. Artificial Intelligence (AI) can explore and handle the unpredictable requirements of IoV to achieve this goal. AI with Machine Learning (ML) and Deep Learning (DL) technology can assist 5G networks in anticipating and managing variable network traffic. Reinforcement Learning (RL), being a type of ML, can effectively solve decision-making problems [18].

In this work, RL based on the Markov Decision Policy (RL-MDP) has been used for making decisions in selecting the best RSU in a reasonable time. However, this is not preferable for huge data sets since it might not lead to making the right decision. Once RSU is selected, the authentication of vehicles is done using the Deep Sparse Stacked Autoencoder Network (DS2AN). This technique has resulted in less computation complexity and communication cost, and resource allocation for the vehicle is done, using Deep Reinforcement Learning (DRL), during handoff. The contributions of this study are as follows:

- To implement a method for reducing handoff delay and to improve QoS parameter performance.
- To develop a secure and fast authentication method using DS2AN during the change of RSU.
- To implement the DQL method to analyze the node activity and resource for IoV.
- To develop the Bellman-Ford algorithm to search the shortest path between communication resources.

The paper is structured as follows: Related works are discussed in Section 2. Section 3 describes the methodology adopted in this study, with mathematical modeling of the RL-MDP for the selection of RSU, DS2AN for authentication, and DRL based resource allocation during handoff. A discussion on the results obtained is presented in Section 4, followed by the conclusion in Section 5.

## 2. Related Work

Awan et al. [19] have proposed a RSU selection method using a dynamic edge-backup node concept in IoV communication. The proposed method is based on clustering. During the discovery of a cluster head, the vehicle sends a message to its neighbors; if no response is received, it initiates a group formation process. A cluster is formed among the vehicles that are moving in the same direction; they are grouped into one cluster. Messages, which contain the location, ID, and speed, are transmitted to the peers in the group. During cluster formation, two nodes, the head node and edge backup node, are selected depending on a score. The calculation of score is dependent on parameters like storage capacity, communication range, and energy. When a new node enters the cluster, a new score will be calculated to decide on the new cluster head. The edge node provides support to the cluster head upon failure of a head node. The cluster head decides on the RSU, with which a connection is established thus enabling communication of the peers. This clustering technique has resulted in higher reliability due to the use of an edge node and an improved throughput. However, there has been no significant improvement achieved in the packet loss rate due to the overhead incurred by the cluster head. Still, seamless handoff of the cluster head is achieved due to the edge node concept used by the author. The authors in [20,21] have discussed Energy-Efficient system modeling for Ad-Hoc Networks and in [22] multipath routing protocols for MANET.

Hussain et al., in [23], have proposed a new method for network selection called the Fuzzy Convolution Neural Network. The handoff decision, based on performance metrics like vehicle speed and signal strength, is made by utilizing the Shannon entropy-based Q-learning algorithm. Metrics such as data type, spacing, vehicular density, number of obstructions, and signal strength have been used for best network selection. V2V chain routing has been achieved through the Jellyfish optimization algorithm in order to find an optimal route amongst the available routes. The authors have been able to achieve an improved throughput by over 15–20%, a minimized delay, and packet loss. The Fuzzy Convolution Neural Network has helped speed up the network selection process.

The work proposed by Fang Jia et al. [24] emphasizes the BUS-aided selection of RSUs, built upon software-defined networking (SDN) and evolutionary games. The authors have concentrated on selecting the best RSU in overlapping areas of RSU. An SDN controller is able to communicate with the vehicles, and fixed and mobile RSUs (BUSES). It gathers data related to the load, throughput, location ID, and bandwidth availability of RSUs, and the ID, route, location, speed, throughput, load, and bandwidth of the BUSES. Then, using the evolutionary game theory concept, an RSU which provides best connectivity is selected. The authors have been able to achieve load balance along with an improved throughput.

Due to the dynamic nature of the network, vehicles exchange information either with an RSU or other moving vehicles frequently. After selecting a suitable RSU for handoff, the vehicle authenticates itself to the RSU and in turn checks the RSU's authenticity. Once mutually authenticated, resource allocation by RSU to the vehicle is done successfully. In [25], the authors proposed a secure and efficient authentication protocol using cryptographic analysis. The authors have successfully addressed various attacks like the impersonation, man in the middle, smart card theft, session key disclosure, and replay attacks. The algorithm has resulted in enhanced security and has been able to preserve a low communication cost of 138 bytes and a computation cost of 2.262 ms, as compared to related schemes.

In [26], a mutual authentication method based on the identity of the RSU and vehicle has been proposed. The system related information is stored in the RSU using the bilinear pair mapping theory and elliptic curve encryption algorithm. The use of the bilinear pair mapping theory and elliptic curve encryption algorithm has guaranteed the irreversibility of group operation, making it impossible for attackers to have access to the network through reverse engineering. The legitimacy of the communicating nodes, RSU, and OBU (On Board Unit) is ensured through mutual authentication using IDs, shared keys, and the handshake principle.

Ping Li et al. [27] formulated a problem based on resource allocation to optimize the throughput of vehicular user equipment (VUEs), while balancing vehicular communications reliability and latency and Quality of Service (QoS) for Wi-Fi networks using networks that coexist with VUE and Wi-Fi User Equipment (WUEs). Authors have employed the listen-before-talk (LBT) method, which requires VUEs to regularly check for other occupants in the channel before transmitting. They estimated the ideal number of offload vehicle users and used the Lagrange Dual Method to convert the optimization issue into a convex optimization problem. Experimentation has proved that their approach performs better when compared to the Greedy method, in terms of throughput.

Pressas et al. [28] investigated the broadcast transmission in V2V using the IEEE 802.11p standard for DRSCs for a contention-based MAC protocol. With a higher packet delivery ratio and lower latency than 4G, the IEEE 802.11P protocol can provide superior performance. The authors of this work have provided a study to handle scalability issues keeping in mind the need for an ML-based approach. The authors have been able to demonstrate an effective data packet exchange, discover the best contention window for broadcast in V2V communication, along with an increased packet delivery ratio and throughput. In comparison with central TBSs, the RSUs are small and have limited resources. In reality, the network status and RSUs' resources change regularly during mobility of the vehicles. As a result, a time-varying resource allocation method that takes into account the task demands and dynamic status of vehicles is required. A novel method for network selection using the

RL-MDP, a fast and secure authentication method using DS2AN and resource allocation using DQL has been proposed.

In Wireless Sensor Networks (WSN), nodes communicate with one another by using wireless techniques and through certain routing algorithms. In [29,30], the authors proposed an Energy Efficient Routing and Reliable Data Transmission Protocol for wireless sensor nodes. In WSN, the size of the nodes are very small, hence the energy efficient mechanisms play a vital role. In this context, the Energy Efficient Routing (HEESR) protocol is implemented based on cluster head selection. Information like distance to the base station and the residual node energy is used to decide on the cluster head. This reduces the re-clustering, which subsequently leads to reduced energy usage.

In [31], the idea of device monitoring is proposed for the Internet of Things (IoT) and machine-type communication (MTC). A theoretical model for device monitoring through data analytics has been proposed. Using the concept of machine learning, the C50 model was trained and tested for data traffic collected from a cellular network. Performance parameters like latency, packet loss, and throughput were considered as indicators in the experiment. In [32], the authors have addressed management of big data.

In [33–35], the authors have addressed DSDV and OLSR, DA-AODV protocol and AODV Protocol routing protocols respectively.

The following points make it clear that the developed methods are better, compared to the prevailing approaches discussed in the literature.

1. Some of the algorithms [25,26] have resulted in a greater number of message exchanges between the UE and network, leading to an increase in computation cost and communication overhead.
2. Some algorithms have proposed [19] the concept of clustering. This increases the communication delay due to an increase in the messages exchanged between the vehicle nodes, cluster head, and RSU, which is time consuming.
3. Some literatures have considered [19,24] either decision delay alone or network selection alone. The proposed work has emphasized both, leading to best network selection and reduced decision delay.
4. The difficulty in pre-designing an accurate authentication model: Model-based authentication methods are less efficient with respect to time when they are used in a complex, time varying environment.
5. The challenge in learning time-varying attributes by the algorithm: Static authentication methods are severely affected by the unpredictable variations of attributes like wireless channel parameters.

Points 4 and 5 have been addressed in the work using RL and DQL. Table 1 summarizes the previous approaches.

**Table 1.** Summarization of previous approaches.

Reference No.	Year	Approach	Advantages	Disadvantages
[19]	2020	Smart Handoff Technique based clustering of vehicle nodes.	Decreased overhead on cluster and packet loss rate.	Consumes more time for cluster formation.
[23]	2021	Shannon entropy based Q-learning algorithm.	Throughput improved by 15–20% and decreases delay and packet losses.	Decision delay during handoff is not addressed.
[24]	2019	BUS-aided RSU selection method based on SDN and evolutionary game.	Proposed system demonstrates improvement with respect to load balance and overall throughput among RSUs.	Decision delay encountered during selection of best RSU has not been considered.

Table 1. Cont.

Reference No.	Year	Approach	Advantages	Disadvantages
[25]	2020	Secure and efficient authentication protocol using cryptographic analysis	The performance analysis is done in terms of communication (138 bytes) and computation cost (2.262 ms).	Only few attacks have been addressed, not very secure.
[26]	2021	Bidirectional authentication	Mutual authentication using ID, shared key, and handshake principle, resulted in 10% reduction in the computational cost.	Less emphasis on authentication delay.
[27]	2020	Listen-before-talk (LBT) method and Lagrange Dual Method (LDM)	Enhancement of throughput when compared to Greedy method.	Ignored Packet delivery ratio and End-to-End delay.
[28]	2017	ML-based approach	Effective data packet exchange, increased packet delivery ratio and throughput.	End-to-End delay is not considered.
[31]	2019	Machine Learning concept	Resulted in decreased Latency, packet loss and throughput.	Authentication of nodes is not discussed.
This paper	2022	RL-MDP, DS2AN and DRL	Resulted in 13% lesser decision delay for selecting the best RSU. Reliable packet delivery of 84% and system throughput of 92 Mbit/s for 28 dBm of power limitation, while upholding tolerable E2E Delay levels of 0.1 ms (for 100 vehicles). Reduced authentication delay.	Requirement of large data set for training the model. Suitable only for infrastructure based communication.

In comparison with the existing literature, it is found that RL and DQL techniques are a better option, since they lead to a reduction in computation cost and communication overhead. This advantage is attributed to the fact that the messages exchanged between the vehicle nodes and RSU are reduced by the use of DQL compared with regular cryptographic message exchange protocols, which are found to be time consuming due to the increase in the messages exchanged between the vehicle nodes, cluster head, and RSU.

The work mainly focuses on the handoff decision phase where the vehicle selects the best RSU. The obtained results are compared with TOPSIS and GRA methods. Authentication and security of the vehicles are ensured using the Deep Sparse Stacked Autoencoder Network (DS2AN) algorithm, developed using a deep learning model. Once authenticated, resource allocation by RSU to the vehicle is done through the DRL method, a DQL technique.

### 3. Proposed Methodology

The work aims to enable a vehicle to select the best RSU with minimum delay, ensuring a fair amount of resource allocation to the vehicle. Bellman-Ford algorithm is used by the RSU to determine the shortest path between itself and the destination, with help of a Q-network. AI can explore and handle the unpredictable requirements of IoV. RL, being a type of ML, can effectively solve decision-making problems. Hence, in this work, the RL-MDP has been used for making decisions in selecting the best RSU in a reasonable time. However, this is not preferable for huge data sets, since it might not lead to making the right decision. Once the RSU is selected, authentication is done using DS2AN and resource allocation for the vehicle is done using DRL during handoff. This technique has resulted in lesser computation complexity and communication cost. In recent years, there has been a surge in applications of DL due to a rise in the volume of accessible data and a decrease in the cost of processing power.

### 3.1. RSU Selection Based on the RL-MDP

This section discusses the best RSU selection during handoff using the RL technique, based on the Markov Decision process (RL-MDP) [36]. The MDP is used to model the environment consisting of five components, which are: states (s), actions (a), decision epochs, rewards (r), and transition possibilities (P). The modeling of the environment is being done with the aim of maximizing the expected total reward per connection. Each time agent changes the state when it gets a reward r (s), which is used for calculating the state value function v (s). The reward r (s, a) is obtained for being in a state “s” and taking an action “a” and r (s, a, s’) represents the reward for being in a state, taking an action, and ending up in a new state. This is done to obtain an optimal policy for making a right decision in selecting the best RSU.

#### 3.1.1. Design and Implementation

Solving the problem of identifying the best RSU using RL comprises three phases: the environment is formulated into the MDP model, the calculation of reward function, and estimating the total expected reward per connection using Bellman’s equation through the Value Iteration algorithm.

##### i. The MDP model

The network is assumed to be heterogeneous involving “M” RSUs, and at any given point of time the vehicle has access to more than one RSU. The following are defined:

State: This includes the RSU identification number, bandwidth available at the RSU, and average delay incurred in connecting to the RSU. Furthermore, it is assumed that the vehicle periodically receives all these advertised information from each RSU amongst other parameters within its receiving range. Figure 1 illustrates a block schematic of the RL technique, based on the MDP.

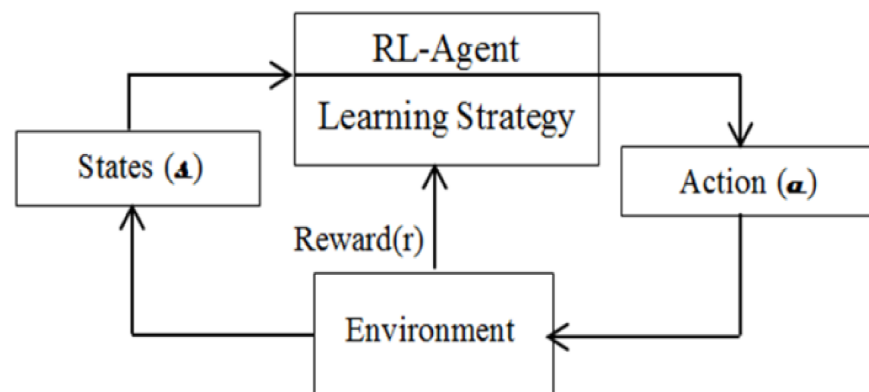


Figure 1. RL based on the MDP.

State space (S),  $S = R \times Bw \times DL = (R_1, \dots, R_M, Bw_1, \dots, Bw_M, DL_1, \dots, DL_M)$ .

$R = (R_1 \dots R_M)$ : Indicates available RSUs in the network.

$Bw = (Bw_1, \dots, Bw_M)$ : Bandwidth presented by each RSU.

$DL = (DL_1 \dots DL_M)$ : Delay presented by each RSU.

Action (a): Vehicle takes actions considering the handoff requirement Ex.:  $a = (a_1, a_2)$ .  $a_1$  indicates the necessity of handoff and  $a_2$  represents to be attached with present RSU.

State transition probability (P): The probability of switching to the subsequent state s', given the present state “s” and taken action “a”, given by:

$$P(s'|s, a) = \begin{cases} \prod_{m \in M} P[\theta'_{w'_m}, dL'_m | \theta_{w_m}, dL_m], & h' = a \\ 0, & h' \neq a \end{cases} \quad (1)$$

where,

$s = [h, \ell w_1, \dots, \ell w_M, dL_1, \dots, dL_M]$ : represents the current state.

$s' = [h', \ell w'_1, \dots, \ell w'_M, dL'_1 \dots dL'_M]$ : denotes next state;  $m = 1$  to  $M$ .

$P[\ell w'_m, dL'_m | \ell w_m, dL_m]$ : transition probability of  $m$  network’s bandwidth and delay.

ii. Computation of Reward function ( $r$ )

The calculation of reward function is explained below. A vehicle gets a reward  $r(s, a)$  immediately when the vehicle is in state “ $s$ ” and takes an “ $a$ ” action. The Equations (2) and (3) provide the bandwidth and delay reward function, respectively.

$$f_B(s, a) = f(\mathfrak{B}) = \begin{cases} 1, & \mathfrak{B} \geq U_B \\ (\mathfrak{B} - L_B)/(U_B - L_B), & L_B < \mathfrak{B} < U_B \\ 0, & \mathfrak{B} \leq L_B \end{cases} \quad (2)$$

$\mathfrak{B}$ : Total available bandwidth.  $L_B$ , and  $U_B$  indicate minimum and maximum required bandwidth by the connection, respectively.

$$f_D(s, a) = f(\zeta) = \begin{cases} 1, & 0 < \zeta \leq L_D \\ (U_D - \zeta)/(U_D - L_D), & L_D < \zeta < U_D \\ 0, & \zeta \geq U_D \end{cases} \quad (3)$$

$\zeta = \max\{d_i \cdot a_i\}$ ,  $d_i$  = RSU delay,  $i$  = RSUs,  $i = 1, \dots, M$ .

$L_D$  and  $U_D$  = minimum and maximum delay incurred in connecting to the RSU.

The Equation (3) provides the handoff cost function:

$$q(s, a) = \begin{cases} K_{h,l} & h \neq l \\ 0, & h = l \end{cases} \quad (4)$$

$K_{h,l}$ : Represents the switching or handoff cost imposed while moving from RSU “ $h$ ” to RSU “ $l$ ”.

Consequently, reward function  $r(s, a)$  for being in current state  $s$  and the chosen action  $a$  is given by,

$$f(s, a) = (1 - w_f) f_B(s, a) + w_f f_D(s, a) \quad (5)$$

$$r(s, a) = f(s, a) - q(s, a) \quad (6)$$

$w_f$  = weight factor  $0 \leq w_f \leq 1$

$r(s, a)$  = Reward function between two successive decision epochs during vertical handoff.

3.1.2. Bellman’s Optimality Equation

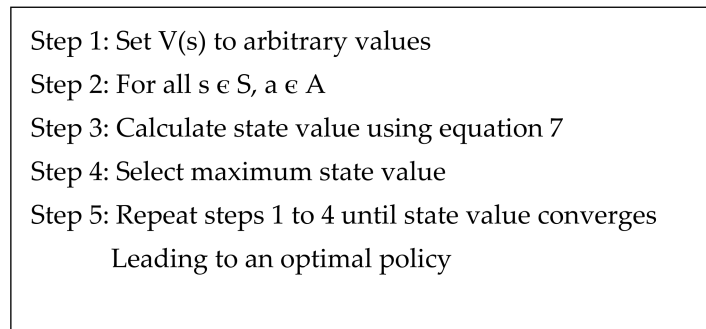
This equation is used to find the state value. The Value Iteration Algorithm (VIA) is used to determine the expected total reward and optimal policy  $g^*(s)$ . The best network is to be selected using the optimality equation, as given below:

$$v(s) = \max_{a \in A} \left\{ r(s, a) + \sum_{s' \in S} \lambda P[s' | s, a] v(s') \right\} \quad (7)$$

The VIA determines the total expected reward and the best policy, consequently this gives the optimal state value function. Being in a current state “ $s$ ”, the best RSU is selected using the optimal policy  $g^*(s)$ , which is maximum function over all policies.

Through the VIA, the ideal state value is calculated repetitively, improving the estimation of  $v(s)$ . This algorithm pseudo-code is provided in Figure 2, which starts with the initialization of  $v(s)$  to arbitrary random values. It repetitively updates the action value function and state values  $v(s)$  until it meets an optimal value [37].



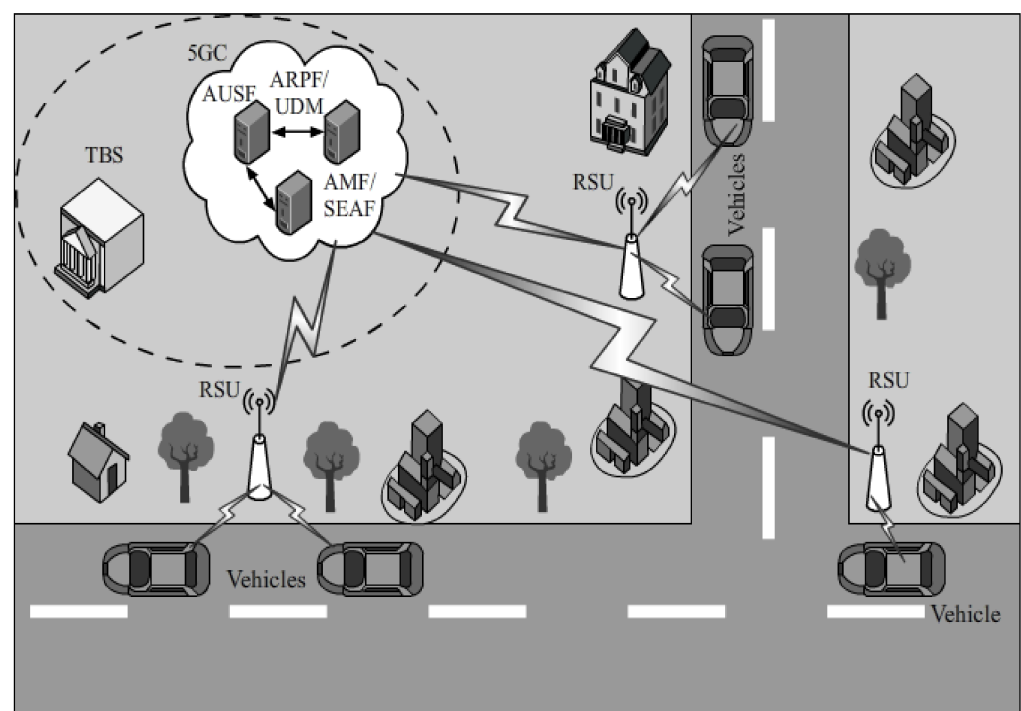


**Figure 2.** VIA pseudo-code.

This section concludes that the optimality equation leads to the maximum expected total reward  $v(s)$  and optimal policy  $g^*(s)$ . The optimal policy  $g^*(s)$  helps in making the right decision in selecting the best RSU for handoff, given that the current state is  $s$ .

### 3.2. Authentication in IoV Using DS2AN Algorithm

**System Model:** This work mainly focuses on vehicle to infrastructure communication. The system model (Figure 3) incorporates the following communication entities: The entire 5G-V2X network is controlled by the 5G core (5GC). The 5G Core network consists of the security anchor function (SEAF), access and mobility management function (AMF), unified data management (UDM), authentication server function (AUSF), and authentication credential repository and processing function (ARPF). The connection and mobility management tasks are handled by the AMF entity, communication is handled by the SEAF, identity verification is performed by the AUSF, authentication data and keys computation are done by the ARPF, and data management is carried out by the UDM. The Trusted Base Station (TBS) is a totally trusted system, which is mainly responsible for verifying the authenticity of RSUs, issuing certificates to the RSUs, generation of public and private keys, and distribution of public keys.



**Figure 3.** The System Model.

The On-Board Unit (OBU) within the vehicle collects information and transmits to other vehicles and RSUs. An anti-tampering device in the OBU protects the real identity of the vehicle.

### 3.2.1. Mathematical Model Analysis

Figure 4 depicts the schematic illustration of the DS2AN; it has three layers: encoder, code, and decoder. The encoder takes data from the network and compresses it. This is the code or bottleneck which is transmitted across the network. This code is in turn picked up by the network and decoded to get back the original values. The DS2AN is the expansion of the basic autoencoder, with sparsity applied to the hidden layers.

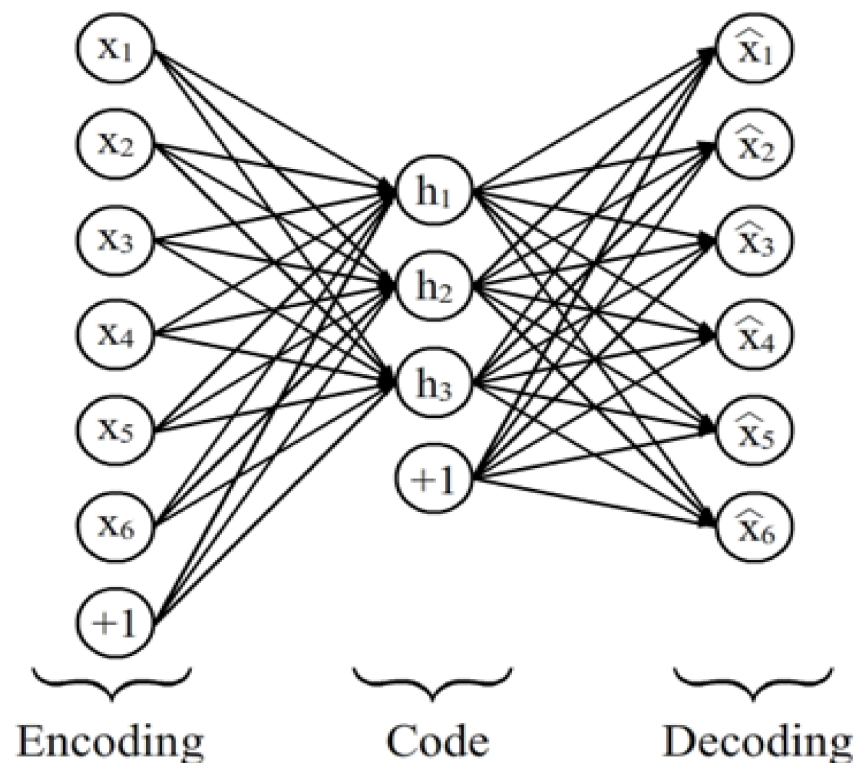


Figure 4. Schematic diagram and layers of the DS2AN.

During authentication, the RSU sends a certificate to the vehicle, which it received from the TBS, and, in response, the vehicle sends a DS2AN code. When a vehicle wants to connect to the RSU, it will scan the network for certain channel parameters, such as the Received Signal Strength Indicator (RSSI), Reference Signal Received Power (RSRP), Channel Quality Indicator (CQI), Reference Signal Received Quality measurement (RSRQ), and Signal to Noise ratio (SNR); these are the inputs to the DS2AN. The dimensionalities of these inputs are reduced to obtain a code; this code in turn is taken up by the network. The DS2AN algorithm, present on the RSU side, decodes this code to obtain the original parameters. Sparsity is applied to the hidden layers to reduce the error in replicating the input, while restricting node information such as channel availability, traffic, and connected device. The authentication of vehicles is considered to be successful if the reconstructed values match the predefined values, thus ensuring security against attacks on the system. Once authenticated, the vehicle communicates with the desired network.

In the hidden layer, the sigmoid activation function is used and the analysis is as follows:

Encoding stage: the input vector  $x_i (i = 1, 2, \dots, p)$  is converted into the hidden representation  $h_i$  by an activation function:

$$h_i = f(x_i) = \text{sigm}(W_1 x_i + b_1) \quad (8)$$

$W_1$  and  $b_1$  indicate weight matrix and bias between the input and hidden layer, correspondingly.

The  $\text{sigm}(x)$  denotes the logistic sigmoid function, which is calculated by

$$\text{sigm}(x) = (1 + \exp(-x))^{-1} \tag{9}$$

Decoding stage: Reconstructed values  $\hat{x}_i$  are mapped with the input parameters  $x_i$ , and the activation function used is the softmax function.

$$\hat{x}_i = g(h_i) = s(W_2 h_i + b_2) \tag{10}$$

$W_2$  and  $b_2$  indicate the weight matrix and bias between the hidden and output layer, correspondingly.

The reconstruction error is defined by the likelihood function:

$$L(X, \hat{X}) = \frac{1}{2} \sum_{i=1}^N \|x_i - \hat{x}_i\|^2 \tag{11}$$

$N$  = number of training samples;  $x_i$  =  $i$ th training sample.

Through backpropagation, fine tuning of the model is done by updating weights and biases, using following respective equations:

$$W = W - \eta * \frac{\partial \hat{L}(\theta)}{\partial W} \quad b = b - \eta * \frac{\partial \hat{L}(\theta)}{\partial b}$$

The dataset used for training the DS2AN model is pre-processed, which incorporates the data separation and normalization phases. Data is divided into two sets during data separation, as a training set (75%) and test set (25%), and both datasets are prone to attacks. The value of each parameter is scaled to a range between 0 and 1 in the data normalization phase. Once the model is trained with 75% of the dataset, it will be tested for working with the remaining 25% dataset. If there is any data mismatch, then the nodes will be considered as unauthorized nodes and are stopped from accessing the network. The notations used in the work are provided in Table 2.

**Table 2.** Notations used.

Notation	Definition
$x$	Training sample
$\hat{x}$	Reconstruction of input
$h$	Hidden layer
$W$	Weight
$b$	Bias
$\eta$	Learning rate
TBS	Trusted Base Station
HRSU_pkj	Public Key of Home RSU
FRSU_pkj	Public Key of Foreign RSU
RSU_SKj	jth RSU Secret key
RSU_IDj	jth RSU ID
(asyencr((V_IDj), R_Vj), HRSU_pkj)	Asymmetric encryption of the V_IDj and R_Vj using the Public key of HRSU_pkj
HRSU_SKj, FRSU_SKj	Secret key of home RSU and foreign RSU
Rq_ID, Resp_ID	Request ID and Response ID
HRSU_Cj	Home RSU certificate
5GCN	5G core network
$K_{SHRSU}, K_{SFRSU}$	Symmetric key of the HRSU and FRSU
$S_{TBS}$	System master key
$V_j$	jth vehicle
$R_{prmkey}$	Pre-master key
$K_{seaf}$	Session Key

### 3.2.2. The Authentication Process

The authentication protocol consists of three phases, namely:

1. Initialization phase—during this phase, private and public keys are generated by TBS and the same will be loaded to the RSU and vehicle. The ECDSA is used for key pair generation. Furthermore, certificates  $C_j$  are generated by TBS and issued to all RSUs. When a vehicle is on roaming mode, symmetric keys are generated amongst the HRSU and FRSU using the AES 256 algorithm and are sent to the vehicle by the HRSU for authenticating the FRSU.

2. Registration—The vehicle and RSU register with the TBS to obtain the required system parameters.

RSU registration: Initially, each RSU has to be authenticated and certified by the TBS. In this case, it assumed that the TBS is a trusted party. The RSU sends its identity,  $RSU\_ID_j$ , and location information to the TBS. After authentication, the RSU is provided with a certificate that will be saved in the RSU's local database and in the 5GCN. After checking the legitimacy of the RSUs, the TBS selects an integer and random number and computes the  $RSU\_SK_j$  (secret key) and  $RSU\_PK_j$  (public key). The TBS assigns the RSU a secret key through a secure channel, the TBS in turn stores  $\{RSU\_ID_j, RSU\_SK_j\}$  in its RSU list.

Vehicle registration: During this phase, the vehicle sends its identity,  $V\_ID_j$ , to the TBS. The TBS selects a random number and a calculates pseudonym,  $P\_ID_j = H(V\_ID_j \parallel STBS \parallel n_j)$ . The TBS stores  $V\_ID_j$  in its database, and forwards  $P\_ID_j$  to  $V_j$ . The vehicle in turn saves  $P\_ID_j$  into the OBU $_j$ . Subsequently, the registration details stored in the TBS are also shared with the 5GCN.

3. Mutual Authentication—All these three phases of the authentication protocol, along with mutual authentication, are explained in detail, below.

The  $V_j$  sends a handoff request packet  $Rq\_ID = (asyencr((P\_ID_j), R\_V_j), HRSU\_pk_j)$  to the HRSU. Upon receiving  $Rq\_ID$ , the HRSU forwards it to the 5GCN along with its  $HRSU\_C_j$ . In the 5GCN, the AUSF checks for the legitimacy of the HRSU through certificate verification. This is then forwarded to the UDM, which in turn, with the help of the SIDF, will provide the vehicle ID by decoding the received message; thus, identity of the vehicle  $V\_ID_j$  is verified. The HRSU will then share the symmetric key of itself and the FRSU to the  $V_j$   $Resp\_ID (K_{SHRSU}, K_{SFRSU})$ , and forward  $V_j$  ID,  $(P\_ID)_{HRSU}$  to the FRSU.  $V_j$  will send the start\_packet to the FRSU to initiate a handoff. The FRSU in turn sends a request packet,  $(Rq\_P\_ID)_{FRSU}$  to the  $V_j$ . The  $V_j$  responds with its identity information packet,  $Resp\_ (P\_ID_j)_{V_j}$ , to the FRSU. Once the FRSU receives the  $V_j$  identity information, it is compared with  $P\_ID_j$  for verification. Once verified, the FRSU sends a certificate and the message  $DS2AN\_START$  to the  $V_j$  to signal the starting of the DS2AN authentication procedure. On reception of this message, the  $V_j$  first verifies the certificate using the symmetric key of the FRSU, which is received from the HRSU. On successful verification, the  $V_j$  generates a pre-master key,  $R_{prmkey}$ , and sends  $DS2AN\_AuthCode = (5 \text{ parameters}, (R_{prmkey}, P\_ID_j)_{FRSU\_pk_j})$ . The  $V_j$  sends  $DS2AN\_AuthCode = (5 \text{ parameters}, (R_{prmkey}, P\_ID_j)_{FRSU\_pk_j})$  to the FRSU. The decrypted  $(R_{prmkey}, P\_ID_j)_{FRSU\_pk_j}$  gives the pre-master key and  $P\_ID_j$ . At the FRSU, input is reconstructed and compared with the predefined values, legitimacy of the  $V_j$  is decided, and  $(AUTH\_Success)$  is sent to the  $V_j$ . Thus, mutual authentication is successful. Now, the authenticated  $V_j$  generates the key  $K_{seaf}$  in the same way as the FRSU. The key,  $K_{seaf}$ , is used by the  $V_j$  and RSU for establishing communication.

### 3.2.3. Security Analysis of the DS2AN

Authentication, being an important aspect of the IoV system, protects against attacks due to malicious nodes entering the system [38,39]. Authentication can protect IoVs from internal and external attacks. Confidentiality, integrity, and availability are the three basic security requirements for wireless networks [40]. Confidentiality is preventing unauthorized nodes from reading the contents of data packets. Availability is permitting the authorized users to view data information. Integrity is avoiding unauthorized modifications for data packets. The attacks selected in this work are the major attacks that hamper these requirements. Addressing these attacks suffices to ensure reliable communication. In [41–43], the authors have discussed several attacks that need to be addressed in vehicular

networks to assure confidentiality, availability, and integrity of the data. The proposed authentication system has addressed attacks that occur on vehicular networks in addition to attacks addressed in [44], such as Sybil, DoS, masquerading attacks, message tampering, and anonymity.

1. Sybil Attack: In this attack, an attacker disseminates multiple messages using fake IDs by producing many false identities to interrupt the normal mode of operations of the IoVs. This attack can be resolved using the DS2AN, as all the participating entities will be registered with the network; only they can receive the parameters sent by the network. Therefore, no attacker can access the network without registering to the network.
2. Mutual Authentication: A security feature of 5G, mutual authentication helps prevent spoofing of messages. Authentication amongst the  $V_j$ , HRSU, and FRSU is robust by the use of the DS2AN, since authentication is performed at both the ends.
3. Vehicle Identity Protection: The encrypted  $P_{IDj}$  that is transmitted to the HRSU ensures the security of user identity.
4. Passive Attack: The authenticated  $V_j$  is identified by the RSU based on a received code. Access to the network by a malicious node is prevented when the reconstructed values do not match. Thus, the DS2AN provides protection against passive attacks.
5. Node Impersonation Attack: Guessing the valid ID of the registered users in the network is performed by the attacker effectively. This attack has been thwarted by the DS2AN, since the attacker requires the knowledge of the training done at both the  $V_j$  and the RSUs.
6. MitM Attack: The attacker acquires the  $P_{IDj}$  and tries to modify it. However, with a reduction in the dimensionality of the code containing  $P_{IDj}$ , the attacker is prevented from making modifications to the  $P_{IDj}$ .
7. Masquerading Attack: The attacker pretends to be another vehicle by using the other vehicle's identity and masking their own identity, resulting in a Masquerading Attack. This attack is thwarted due to the mismatch of the DS2AN\_AuthCode.
8. Message Tampering: One of the common attacks in which exchanged messages of V2V or V2I communication can be altered by the attacker. This can be prevented by training of the  $V_j$  and RSUs using the DS2AN.
9. DoS attack: This attack aims to make valid resources of a system inaccessible. Here, the attacker sends a message containing  $P_{IDj}$  to the network, constantly overloading the network with the purpose of stealing sensitive data or bandwidth consumption or to congest the network. This type of an attack has been successfully prevented through the identification of malicious nodes when the reconstructed values of the code do not lie in the range of pre-defined values.
10. Eavesdropping Attack: This attack is avoided as due to the training model present at the  $V_j$  and RSU.
11. Anonymity: This aspect is important for vehicle confidentiality protection. In this scheme, vehicles will communicate using the pseudonym  $P_{IDj} = H(V_{IDj} || S_{TBS} || nj)$ . Real identity of the vehicle can be restored by using the secret value  $S_{TBS}$ .

On successful completion of authentication, resources will be allocated to the vehicle by the FRSU. The next section discusses how the resource allocation is performed.

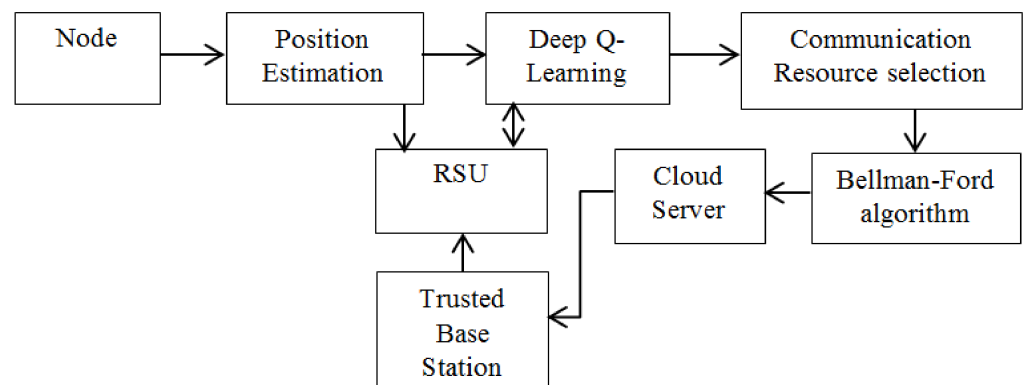
### 3.3. Resource Allocation during Handoff Using the DRL

Upon successful authentication, resources are allocated to the vehicles as per their request. Generally, vehicle applications have two components: content-requesting tasks and computation tasks. For example, in the case of autonomous vehicular applications, the vehicle requests the road conditions from the RSU, which subsequently provides the routes to the vehicles as computed results to avoid crashes of vehicles. Meanwhile, vehicles transmit local routes and traffic conditions in real-time to calculate the best driving routes. The TBS is believed to have a considerable amount of computational and storage capacity since the range of its wireless communication is wide enough to reach all vehicles. As a result, the

RSUs and TBS can work together to respond to user requests. Vehicles may concurrently receive material and upload the computing tasks from RSUs/TBSs or to them using a full-duplex radio, which is based on sophisticated 5G wireless communication technology.

The AI-based controller for the RSU has been deployed. Furthermore, the controller is made up of environment information gathered from IoVs and an AI-based agent. On the other hand, an AI-based processor takes an action based on existing conditions such as reward and current states, including caching decisions and RSU resource allocation methods. For example, in the case where a vehicle travels to RSU2 from RSU1, the computation offloading and content downloading calculation will shift to RSU2 from RSU1. When the resources available are insufficient at RSU2 for that particular vehicle in nearby RSUs to satisfy the user's demands, the work will be handed over to the TBS for collaboration.

Figure 5 depicts the block diagram of the DRL model. Here, the Supervised DQL algorithm is proposed for analyzing network activity and vehicle position in IoV and allocate the communication channel or resource.



**Figure 5.** The DRL model.

In this method, the details of vehicle location and vehicle position are stored on the RSU database. The environment is modeled as the MDP with the goal of maximizing the total expected reward per connection. The Bellman-Ford algorithm is used to search the shortest path between vehicles with the help of the Q-network. This shortest path algorithm is used to calculate the overall mobile edge node distance and weight, and to update to RSU. The algorithm avoids frequent changeover between the control of the RSU and vehicle. The RSU node tracks the velocity of the vehicle, its location and direction of travel, and detects all the neighbors of the next forwarding node with the smallest distance and the least hops [45,46].

The proposed model explanation is as follows:

**Node:** Represents a vehicular node.

**Position estimation:** The position of the vehicle is an essential factor to be determined in the IoV, to know which RSU should do the duties. The duration of time in which the links are created between the RSUs and vehicles is calculated using velocity.

**Deep-Q-Learning:** After collecting the status from the RSU, the system uses Deep-Q-Learning to understand the above details to build a scheme that directs the vehicles to upload the task to RSU and download content from them. The agent will allocate the resource dynamically for various requirements.

**Communication Resource Selection:** Communication resource selection means, during the movement of vehicles, the RSU will transmit the data based on the vehicle's request.

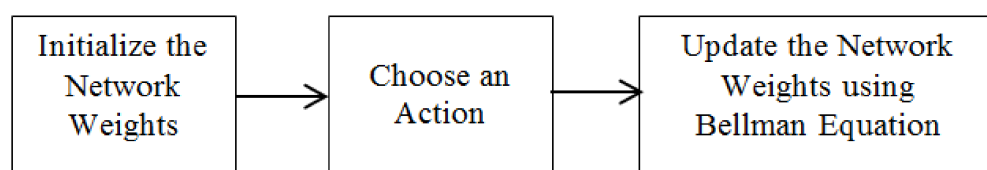
**Bellman-Ford algorithm:** The RSU will communicate and share the destination information with the vehicle. The Bellman-Ford algorithm is used to share the information using the shortest path found.

**Cloud Server:** The cloud server is the moving directions and positions of vehicles that will be stored to the cloud server from the RSU. All information regarding the location and

vehicle ID will be taken to the cloud server from the RSU. It is like a centralized server that will communicate with each RSU.

### 3.3.1. DQL Algorithm

DQL estimates the values and is a substitute for the traditional Q-table. In neural networks, input states map to (action, Q-value) pairings instead of mapping to a state-action combination to a q-value. The learning method in DQL employs two neural networks. The design of these networks is the same, but the weights are different. A target network receives the main network's weights in each of the N steps. The learning process becomes more stable when both of the networks are used and the algorithm learns more successfully. After selecting an action, the agent must carry it out and keep the target as well as main networks up to date by using the Bellman-Ford algorithm (Figure 6).



**Figure 6.** Deep-Q-Learning.

#### Algorithm Steps

1. The agent perceives the present condition of a network. If the chosen number is random and is equal to or less than epsilon, an agent will act in a random action; otherwise, the DQN will forecast Q-values and take action based on the highest Q value.
2. The following state, the reward, is kept in the replay memory, along with the terminal variable.
3. When the agent has enough instances in the memory, the DQN is trained by sampling a certain set of experiences.
4. The collection of current states is regarded as a parameter, and the calculated values are labelled as “[Target = set\_of\_reward + gamma × numpy.max(target\_net.predict(set of next\_state)) × set\_of\_done]”. The terminal variable has been constructed and thus the terminal state's value is 0.
5. Iteratively, the main and target network are updated.

### 3.3.2. Bellman-Ford Path Analysis

The Bellman-Ford method will always discover the shortest path. Although it's more time-consuming than Dijkstra's approach, it is more flexible since it can handle graphs with negative edge weights. In contrast, the Bellman-Ford addresses two major problems with this procedure:

- If weight cycles are negative, it will continue to find the shortest path, indefinitely.
- Exponential relaxation occurs when the relaxation sequence is incorrect.

Bellman-Ford's most crucial step is relaxation. This makes the distance from one vertex to another more precise. Relaxation is achieved by comparing the estimated distance between the vertices to other known distances and progressively shortening the distance calculated.

### 3.3.3. DRL for Resource Allocation

Resource allocation in V2I communications using the DRL method along with the RL framework is presented in this section.

Markov Decision Processes

The MDP formalism may be used to study learning agents mathematically. The vehicle’s status includes the vehicle’s position, velocity, and total size of the content requested by the vehicle (Figure 7). The action is the allocation of resources to vehicles. The agent accepts various requests from vehicles and assigns resources, and thus vehicles may download content from and upload tasks to various RSUs.

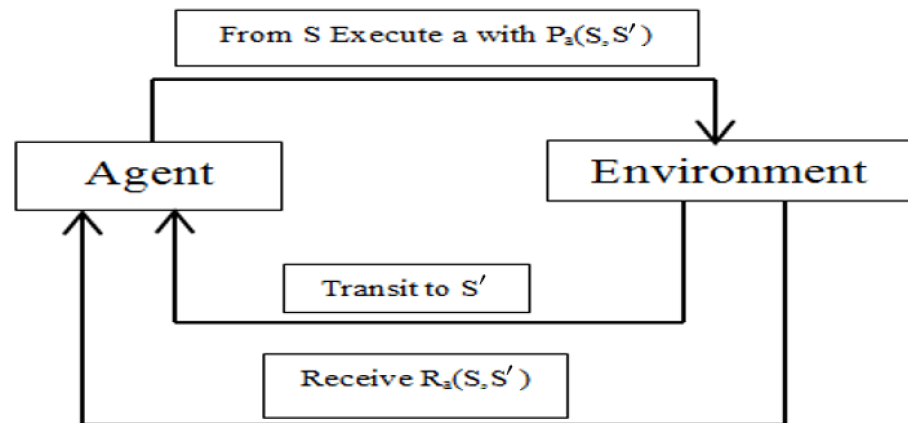


Figure 7. Abstract MDP model.

In RL, a time-homogeneous Markov chain is one in which the transition probability is independent of time, t:

$$P [S_{t+1} = s' | S_t = s] = P [S_t = s' | S_{t-1} = s] \tag{12}$$

At every instance of t, the agent which is the intended RSU link, observes state “s” from the state space, S, and makes an action, a<sub>t</sub>, from the action space, “A”, and selects the appropriate resource based on the policy, π. The Q-function, Q (s<sub>t</sub>, a<sub>t</sub>, θ), determines the decision policy π, where θ is the parameter of the Q-function; it may be acquired using deep learning.

Return and Policy

In RL, the objective is to take actions over time that maximize the expected value of the return (i.e., to select the optimum policy). Return and policy can be defined as follows: The total discounted reward from time-step t is represented by the return G<sub>t</sub> as:

$$G_t = R_{t+1} + \gamma R_{t+2} + \dots = \sum_{k=0}^{\infty} \gamma^k R_{t+k+1} \tag{13}$$

A policy π is a set of actions that the states can take,

$$\Pi (a | s) = P [A_t = a | S_t = s] \tag{14}$$

It is independent of time. A policy directs the choice of action at a specific state.

Q-learning is used to determine the best optimal policy for allocating resources in V2I communications to maximize the long-term predicted accumulated discounted rewards. Once the Q-values, Q (s<sub>t</sub>, a<sub>t</sub>), are known, an updated policy, π, may be easily created by performing the action,

$$a_t = \arg \max_{a \in A} Q (s_t, a) \tag{15}$$

(i.e., the long-term accumulated rewards are used for taking an action).



With Q-values, the optimal policy  $Q^*$  can be found based on the following updated equation; it is possible to find without any knowledge of system dynamics:

$$Q_{\text{new}}(s_t, a_t) = Q_{\text{old}}(s_t, a_t) + \alpha \left[ r_t + 1 + \gamma \frac{\max_{s \in S}}{S} Q_{\text{old}}(s, a_t) - Q_{\text{old}}(s_t, a_t) \right] \quad (16)$$

Once an optimal policy has been determined through training, it may be used to choose resources for V2I links to ensure link latency restrictions.

At each iteration, the Q-network changes its weights, minimizing the loss function obtained from the same Q-network with old weights on a data set  $D$ , as provided by (17),

$$\text{Loss}(\theta) = \sum_{(s_t, a_t) \in D} (y - Q(s_t, a_t, \theta))^2 \quad (17)$$

$$y = r_t + \frac{\max_{a \in A}}{A} Q_{\text{old}}(s_t, a, \theta) \quad (18)$$

$r_t$  denotes the related reward.

## 4. Results and Discussion

### 4.1. Best RSU Selection

The novel handoff algorithm that can perform selection of best RSU based on context information like Bandwidth and delay is developed. The work mainly concentrated on the handoff decision phase, where the vehicle selects the best RSU with maximum bandwidth and minimum delay during the handoff period. The obtained results are compared with that of existing techniques used to choose the best RSU for a seamless connection by vehicles. The comparison demonstrates less decision delay during RSU selection over the existing technique. Table 3 presents the simulation parameters.

**Table 3.** Simulation Parameters.

Parameters	Values
Version	Ns-in-all-one 2.28
Propagation Model	Two Ray Ground
Area	1200 m × 1200 m
Broadcast Area	50–250 m
Transfer pattern	UDP, CBR
Mobility Model	Random Mobility
Transfer per packet	512 bytes

A scenario where the vehicle must connect to at least one RSU during its transmission time is simulated using a ns2 simulator. Figure 8 displays the simulation scenario with 98 nodes, in which 2 are vehicle nodes, 9 are RSU nodes, and 1 is a TBS. The vehicle will run the RL-MDP algorithm to select the best network during handoff, based on the bandwidth and delay parameters associated with each RSU. The decision delay encountered during the selection of the best RSU by the vehicles is illustrated in Figure 9.

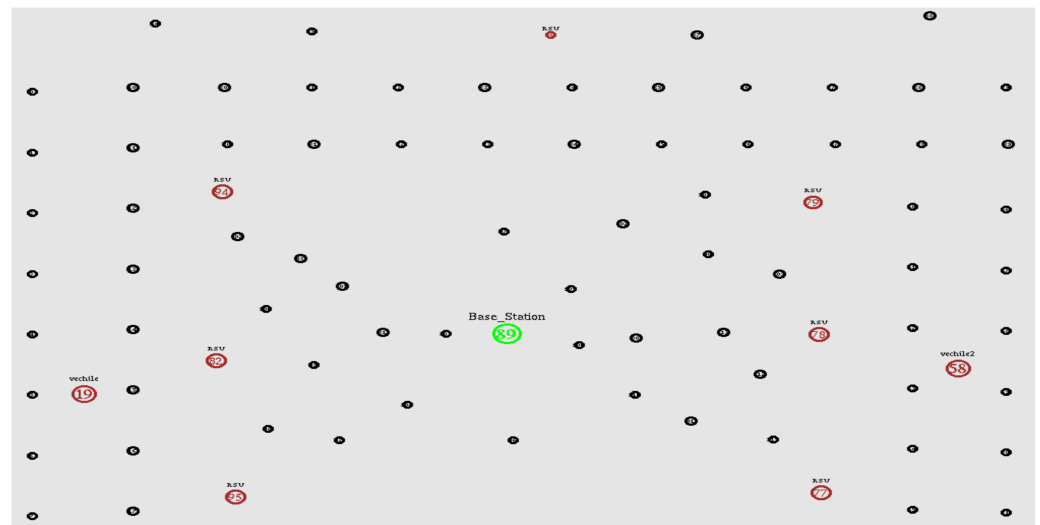


Figure 8. Simulation scenario with 98 nodes.

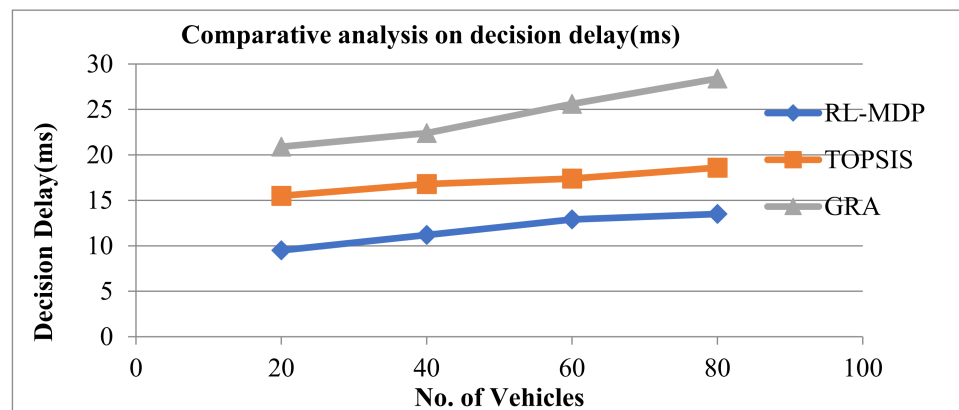


Figure 9. Comparative analysis of decision delay.

Table 4 and Figure 9 display the comparative analysis on decision delay with respect to the Technique for Order Preference by Similarity to Ideal Solutions (TOPSIS) and Grey Relational Analysis (GRA) methods. In RL-MDP, it is found that the decision delay has been reduced on an average of 13%, compared to the TOPSIS and GRA methods.

Table 4. Comparative analysis of decision delay.

No. of Vehicles	Decision Delay (ms)		
	RL-MDP	TOPSIS	GRA
20	9.5	15.5	20.9
40	11.2	16.8	22.4
60	12.9	17.4	25.6
80	13.5	18.6	28.4

#### 4.2. Security Analysis

The study is aimed at realizing a secure and fast authentication, with a reduced delay during handoff. The simulated results have been evaluated based on communication overhead and computational complexity, which has resulted in decreased authentication delays. The outcomes demonstrate that DS2AN performs better, compared to existing techniques.

The parameters used for simulation are presented in Table 5 and the model details of the DS2AN are in Table 6.

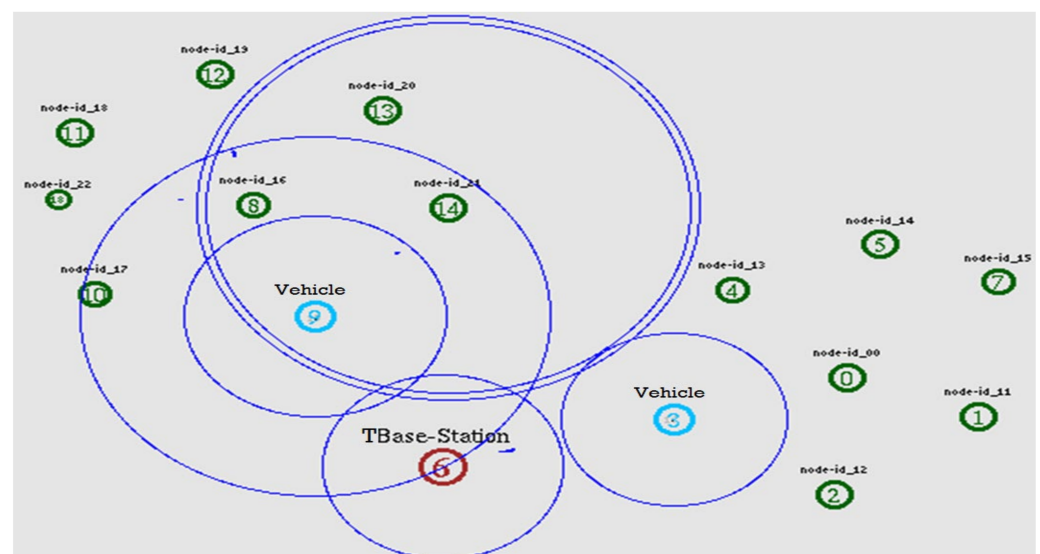
**Table 5.** Simulation parameters.

Parameters	Values
RSUs	6
$V_j$ s per RSU	6
TBS	1
Area Size	1000 × 1000 m
Simulation Duration	50 s
Traffic Model	Constant Bit Rate (CBR)
Propagation Model	Two Ray Ground model
Malicious $V_j$ per cell	1

**Table 6.** DS2AN model details.

Architecture	Encoder	Code	Decoder
	$L_1$	$L$	$L'_1$
	6	3	6
Activation function	Sigmoid and Softmax		
Regularizers	KL divergence		
Loss function	MSE		
Optimizer	Stochastic Gradient Descent		

Figure 10 displays the formation of  $V_j$ s (Vehicles) and TBase-Station (Trusted Base-Station) through the ns2 simulator. When a vehicle wants to connect to the RSU, it will scan the channel to obtain certain input parameters like RSRP, RSRQ, RSSI, SNR, and CQI from the network, and the dimension is compressed to get the code, which in turn is picked up by the network. Interchange of Req\_ID and Resp\_ID among the  $V_j$ s and TBS takes place to guarantee that the  $V_j$  is connected to the authenticated FRSU. On confirmation,  $V_j$  sends the code to the network. The DS2AN algorithm, present on the FRSU, reconstructs the original parameters from the code authenticating  $V_j$ .

**Figure 10.** Creation of  $V_j$ s and TBS using ns2.

#### 4.2.1. A Scenario for Performing DoS Attack

Figure 11 illustrates an unauthorized node (in red colour) performing a DoS attack on a network. Req\_ID and Resp\_ID are exchanged between the unauthorized  $V_j$  and the

FRSU. The FRSU\_Cj is sent by the FRSU as a response. When the code sent by the Vj to the FRSU do not match, the Vj is considered to be malicious and is dropped; this prevents a DoS attack.

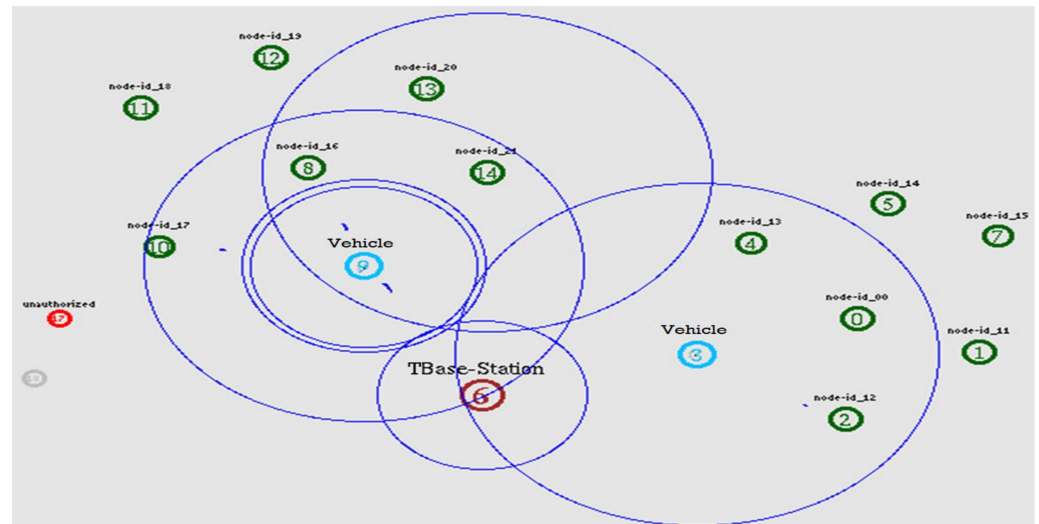


Figure 11. The scenario for performing a DoS attack.

The simulation results are evaluated based on communication and computational cost and are discussed below.

#### 4.2.2. Communication Overhead

Here, a comparison of communication overhead of the DS2AN with some of the existing methods is presented. In the DS2AN,  $Rq\_ID = (asyencr((P\_IDj), R\_Vj), HRSU\_pkj)$  needs 160 bits for encryption done by the Vj and another 160 bits for decryption at the FRSU. Further V\_IDj encryption and decryption requires 320 bits. The DS2AN\_AuthCode = (5 parameters,  $(R\_prmkey, P\_IDj)$  FRSU\_pkj) needs another 160 bits for encryption done by the Vj and another 160 bits for decryption at the FRSU. The size of messages in the DS2AN is  $(160 + 160 + 160 + 160) = 640$  bits (80 bytes). In Table 7, a comparison of the communication overhead of the DS2AN along with other schemes used for authentication has been presented. The DS2AN, developed using deep learning technique, uses fewer message exchanges between the vehicle and network, which aids in the reduction of communication overhead. Communication cost comparison across various schemes is presented in Figure 12.

Table 7. Communication overhead comparison.

Scheme	Communication Overhead in Bytes
[47]	164
[48]	996
[49]	184
[50]	102
DS2AN	80

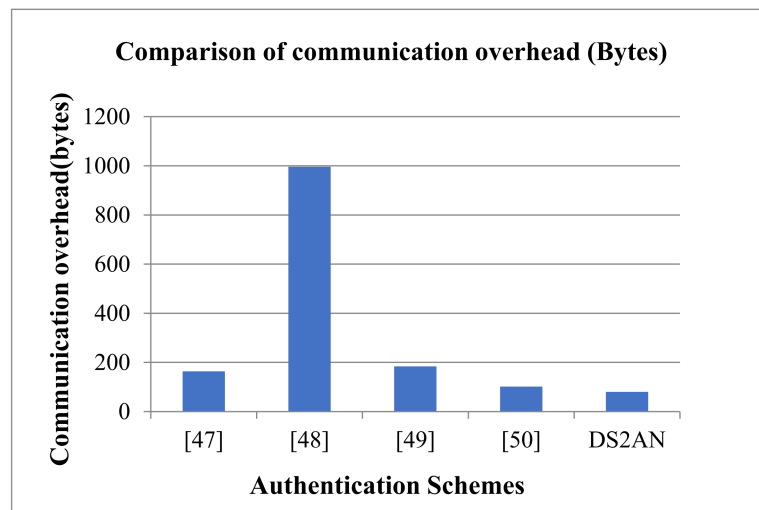


Figure 12. Communication overhead comparison.

#### 4.2.3. Computational Cost

Computational cost in the DS2AN has been minimized because of the: reduction in the cryptographic operations, system or processor related parameters used, key generation, encryption, decryption, and digital signature verification.

Table 8 displays the computation cost for different schemes. Figure 13 illustrates a comparison plot of different schemes.

Table 8. Computational cost (ms) comparison.

Scheme	Computation Cost (ms)
[47]	4.661
[48]	78.291
[49]	3.901
[50]	3.022
DS2AN	0.45

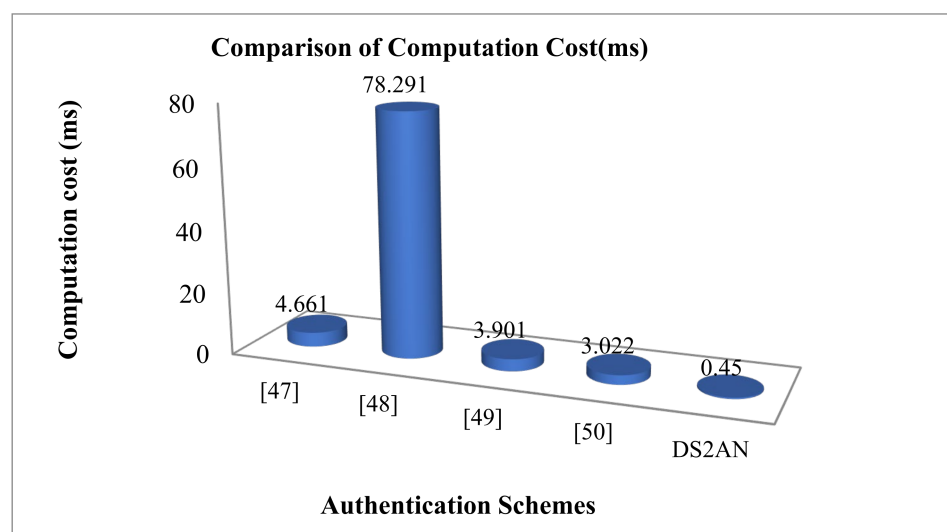
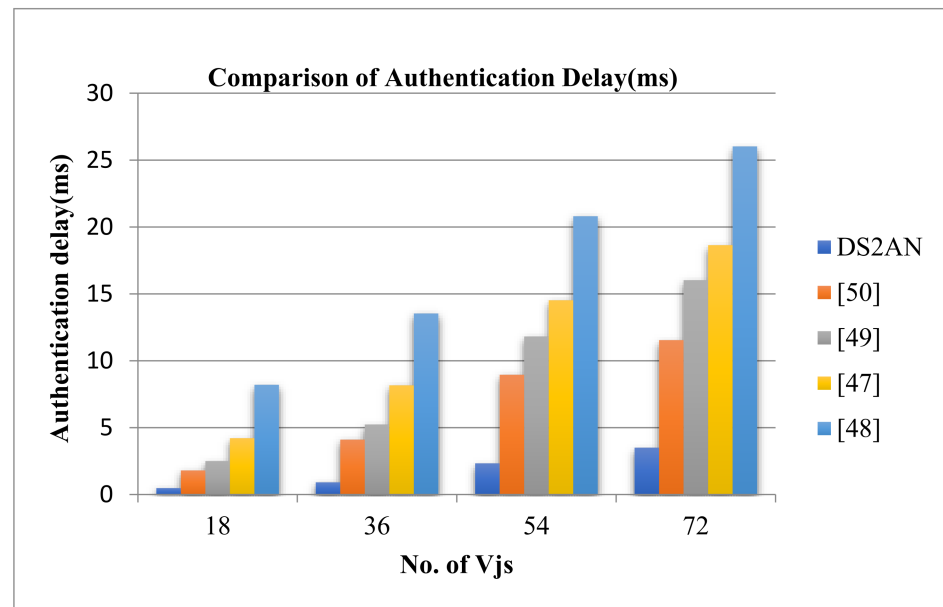


Figure 13. Computational Cost comparison.

#### 4.2.4. Authentication Delay

The authentication delay, calculated as the communication overhead and computation cost for a varying number of  $V_j$ s, has been presented. Based on the analysis, Figure 14

illustrates that the proposed DS2AN protocol has reduced authentication delay and lies well within the standard values specified by the ITU. Table 9 provides the authentication delay encountered for a varying number of  $V_j$ s.



**Figure 14.** Comparison of Authentication delay of the DS2AN.

**Table 9.** Comparison of authentication delay.

No. of $V_j$ s	Authentication Delay (ms)				
	DS2AN	[50]	[49]	[47]	[48]
18	0.48	1.8	2.5	4.21	8.2
36	0.91	4.1	5.23	8.16	13.53
54	2.33	8.95	11.81	14.52	20.8
72	3.5	11.54	16.02	18.64	26.02

#### 4.3. Resource Allocation during Handoff

In this section, for performance evaluation results of the DRL for various node densities is presented. NS2 is used to analyze the network QoS parameters, such as throughput, delivery ratio, and time delay. The proposed DQL method is compared to the existing Lagrange Duality Method (LDM). The parameters used for configuring the simulation environment are presented in Table 3. A simulation scenario with 98 nodes, in which 2 are vehicle nodes, 9 are RSU nodes, and 1 is a TBS, is presented in Figure 8. Figure 15 demonstrates that the vehicle is requesting the RSU for resource allocation. If a resource is not available, it will communicate with the next RSU by running the Bellman-Ford algorithm.

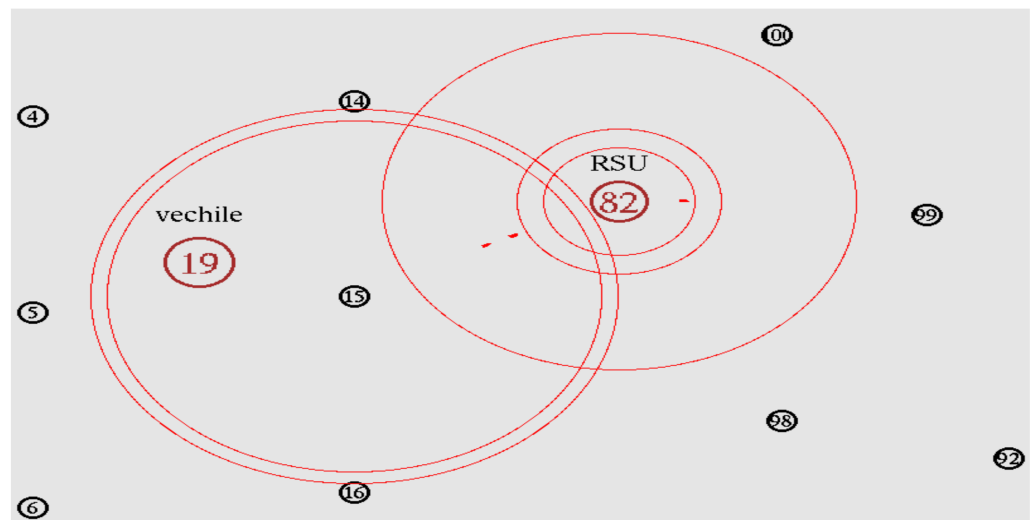


Figure 15. V2I Communication.

#### 4.3.1. Packet Delivery Ratio (PDR)

This is computed using the received and generated packets. As the number of vehicles increases, it becomes challenging to retain the established path. This results in reduced throughput, PDR, and increased delay, whereas the DRL approach provides an increased throughput and PDR, and decreased delay. This has been proven, as demonstrated from the Figures 16–18.

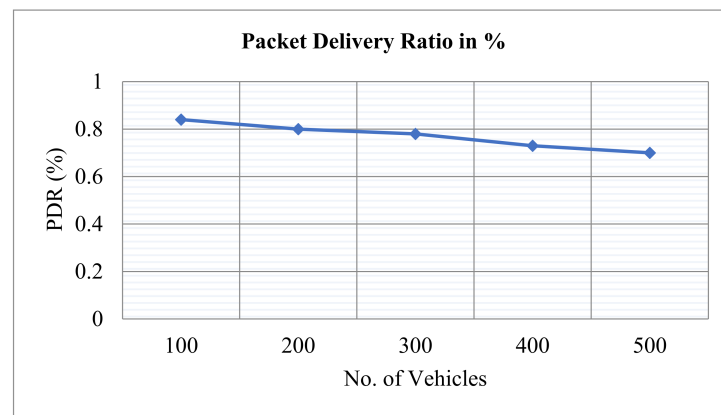


Figure 16. PDR for increase in vehicle density.

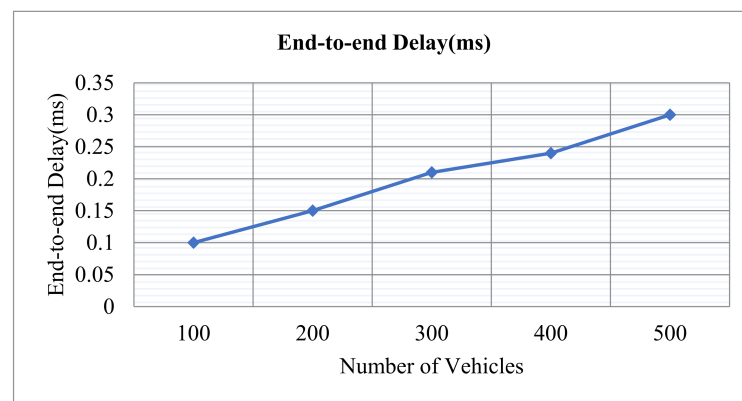
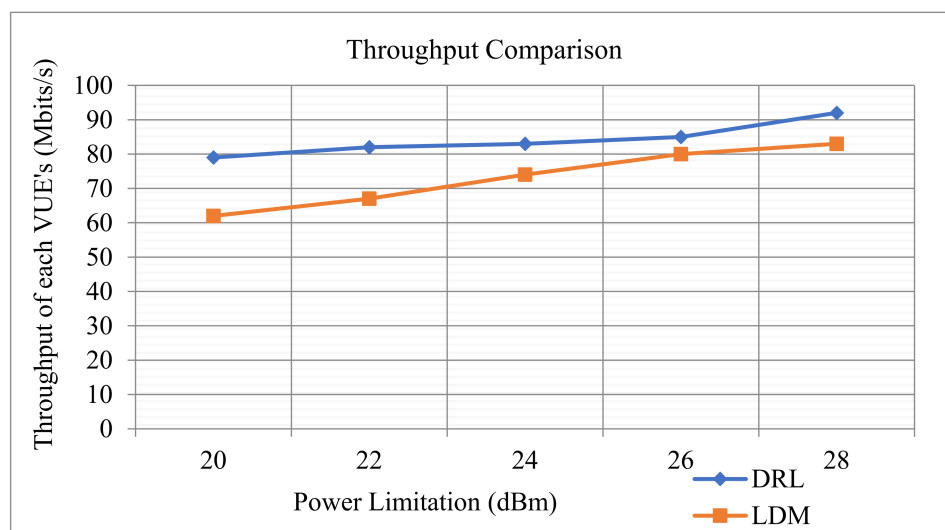


Figure 17. E2E Delay for increase in vehicle density.



**Figure 18.** Throughput comparison of Vehicle Users (VUE).

From the above graph it can be concluded that the PDR of the DRL for 100 vehicles is 84%, similarly 80%, 78%, 70%, and 68% of packet delivery for 200, 300, 400, and 500 vehicles, respectively. Figure 16 demonstrates that, with a higher density of vehicles, PDR decreases.

#### 4.3.2. End-to-End Delay (E2E Delay)

This is the time taken for the packet to traverse across the network from its source to destination. The delay encountered is the ratio of the time taken to receive the packet to the number of connections in the IoV.

From Figure 17, it is observed that, in the DRL method, for 100 vehicles the delay is about 0.1 ms, for 200 vehicles it is 0.15 ms, for 300, 400, and 500 vehicles the delay is found to be 0.21 ms, 0.24 ms, and 0.30 ms, respectively.

#### 4.3.3. Throughput

This is the total number of bits or bytes received successfully by all vehicles. This, in a communication system, can be affected by many parameters like limitation of a physical medium, available computing power of the system, and receiver behavior.

Here, comparison has been made between the Lagrange Dual Method [11] and the proposed scheme that is the DRL Model. Relation between the input and the optimization solution may be achieved using deep neural networks (DNNs) universal approximation capabilities. The new parameter is sent into the trained DNN for real-time implementation, and a satisfactory solution can be provided instantly [51–53]. Figure 18 displays the throughput of each vehicle user and the RSU performance of the proposed DRL and the existing Lagrangian Duality Method (LDM). From the graph it is observed that the DRL has 92 Mbit/s for 28 dBm of power limitation; it provides higher throughput compared to the existing method, LDM.

## 5. Conclusions

With the Internet of Vehicles technology moving towards networking and intelligentization, onboard operating systems, newer automotive electronics, and more in-vehicle communication, newer service platforms providing enhanced security are becoming research hotspots. This work has discussed the: best RSU selection, authentication of vehicles for verifying their legitimacy, resource allocation technique, and finding the shortest path to the destination node for communication during handoff. Handoff, being an important concept for providing seamless connection, decision and authentication needs to be done at a faster rate. This has been demonstrated by the RL-MDP and DS2AN methods. Re-



source allocation and finding the shortest path are done using the DRL and Bellman-Ford algorithm, respectively.

The proposed DRL relies on DQL to find the optimum resources for different vehicular applications. The dataset has been obtained from a public domain for training the parameters. The RSU tracks the speed, location, and direction of travel, and detects all the neighbors of the next forwarding node with the smallest distance and the fewest hops, so as to reduce the handoff delay. The Bellman-Ford algorithm is used to search the shortest path between the RSUs with the help of the Q-network. A reduction in handoff delay of 13% has been achieved by minimizing the decision and authentication delays. Compared to cryptographic protocols, the DS2AN algorithm has fewer cryptographic key generation and message exchanges between the vehicle and network. The efficiency of the proposed algorithm in thwarting several security attacks has also been established through simulation.

This study demonstrates that the DS2AN is more proficient when it comes to authenticating nodes, with minimum delays. Furthermore, the results demonstrate that the DRL provides a reliable packet delivery of 84% and a throughput of 92 Mbit/s, while upholding tolerable delay levels of 0.1 ms.

The requirement of a large data set for training the model becomes a major limitation of the proposed work. The model is suitable only for infrastructure-based communication. The higher the density of vehicles, the more will be the memory requirement at the RSU.

Though the addressed attacks in this work ensure a secured IoV communication and a robust model, several other attacks like the Wormhole and Route modification attacks can be looked into. As a future work, these attacks can also be addressed in the algorithm along with an emphasis on memory requirement. A further reduction in delay encountered during handoff can be achieved through Mobile Edge Computation (MEC), along with DQL.

**Author Contributions:** Conceptualization: H. and S.R.A.; methodology: H. and Y.A.; validation: H. and O.I.K.; formal analysis: S.A. and S.R.A.; investigation: S.A. and O.I.K.; resources: H.; data curation: S.R.A.; writing—original draft preparation: H. and Y.A.; writing review and editing: H. and Y.A.; visualization: O.I.K.; supervision: S.R.A. and Y.A.; project administration: H., Y.A. and S.A.; funding acquisition: S.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research is funded by Taif University, TURSP-2020/313.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The study did not report any data.

**Acknowledgments:** We deeply acknowledge Taif University for supporting this study through Taif University Researchers Supporting Project Number (TURSP-2020/313), Taif University, Taif, Saudi Arabia.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Ahmed, A.A.; Alzahrani, A.A. A comprehensive survey on handover management for vehicular ad hoc network based on 5G mobile networks technology. *Trans. Emerg. Telecommun. Technol.* **2019**, *30*, e3546. [[CrossRef](#)]
2. Fadhil, J.; Sarhan, Q. Internet of Vehicles (IoV): A Survey of Challenges and Solutions. In Proceedings of the 2020 21st International Arab Conference on Information Technology (ACIT), Giza, Egypt, 28–30 November 2020. [[CrossRef](#)]
3. Palanisamy, S.; Thangaraju, B.; Khalaf, O.I.; Alotaibi, Y.; Alghamdi, S.; Alassery, F. A Novel Approach of Design and Analysis of a Hexagonal Fractal Antenna Array (HFAA) for Next-Generation Wireless Communication. *Energies* **2021**, *14*, 6204. [[CrossRef](#)]
4. Khan, H.H.; Malik, M.N.; Zafar, R.; Goni, F.A.; Chofreh, A.G.; Klemeš, J.J.; Alotaibi, Y. Challenges for sustainable smart city development: A conceptual framework. *Sustain. Dev.* **2020**, *28*, 1507–1518. [[CrossRef](#)]
5. Muhammad, M.; Safdar, G.A. 5G-based V2V broadcast communications: A security perspective. *Array* **2021**, *11*, 100084. [[CrossRef](#)]
6. Hobert, L.; Festag, A.; Llatser, I.; Altomare, L.; Visintainer, F.; Kovacs, A. Enhancements of V2X communication in support of cooperative autonomous driving. *IEEE Commun. Mag.* **2015**, *53*, 64–70. [[CrossRef](#)]

7. Li, Z.; Chen, Y.; Liu, D.; Li, X. Performance analysis for an enhanced architecture of IoV via Content-Centric Networking. *EURASIP J. Wirel. Commun. Netw.* **2017**, *2017*, 124. [[CrossRef](#)]
8. Alotaibi, Y. A New Database Intrusion Detection Approach Based on Hybrid Meta-heuristics. *Comput. Mater. Contin.* **2021**, *66*, 1879–1895. [[CrossRef](#)]
9. Mekala, M.S.; Dhiman, G.; Patan, R.; Kallam, S.; Ramana, K.; Yadav, K.; Alharbi, A.O. Deep learning-influenced joint vehicle-to-infrastructure and vehicle-to-vehicle communication approach for internet of vehicles. *Expert Syst.* **2021**, e12815. [[CrossRef](#)]
10. Bae, M.A.R.; Simpson, L.; Boyen, X.; Foo, E.; Pieprzyk, J. Authentication strategies in vehicular communications: A taxonomy and framework. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 129. [[CrossRef](#)]
11. Zhang, Y.; Zhang, M.; Fan, C.; Li, F.; Li, B. Computing resource allocation scheme of IOV using deep reinforcement learning in edge computing environment. *EURASIP J. Adv. Signal Process.* **2021**, *2021*, 33. [[CrossRef](#)]
12. Nguyen, T.D.; Nguyen, T.D.; Nguyen, V.D.; Pham, X.Q.; Huh, E.N. Cost-Effective Resource Sharing in an Internet of Vehicles-Employed Mobile Edge Computing Environment. *Symmetry* **2018**, *10*, 594. [[CrossRef](#)]
13. Suryanarayana, G.; Chandran, K.; Khalaf, O.I.; Alotaibi, Y.; Alsufyani, A.; Alghamdi, S.A. Accurate Magnetic Resonance Image Super-Resolution Using Deep Networks and Gaussian Filtering in the Stationary Wavelet Domain. *IEEE Access* **2021**, *9*, 71406–71417. [[CrossRef](#)]
14. Alotaibi, Y. A New Secured E-Government Efficiency Model for Sustainable Services Provision. *J. Inf. Secur. Cybercrimes Res.* **2020**, *3*, 75–96. [[CrossRef](#)]
15. Alsufyani, A.; Alotaibi, Y.; Almagrabi, A.O.; Alghamdi, S.A.; Alsufyani, N. Optimized intelligent data management framework for a cyber-physical system for computational applications. *Complex Intell. Syst.* **2021**, 1–13. [[CrossRef](#)]
16. Xuemin, S.; Romano, F.; Shanzhi, C. Measuring and Imaging Permittivity of Insulators Using High-Frequency Eddy-Current Devices. *Proc. IEEE* **2020**, *108*, 242–245. [[CrossRef](#)]
17. Elsaygher Mohamed, S.A.; Al Shalfan, K.A. Intelligent Traffic Management System Based on the Internet of Vehicles (IoV). *J. Adv. Transpor.* **2021**, *2021*, 4037533. [[CrossRef](#)]
18. Mekrache, A.; Bradai, A.; Moulay, E.; Dawaliby, S. Deep reinforcement learning techniques for vehicular networks: Recent advances and future trends towards 6G. *Veh. Commun.* **2021**, *33*, 100398. [[CrossRef](#)]
19. Awan, K.M.; Nadeem, M.; Sadiq, A.S.; Alghushami, A.; Khan, I.; Rabie, K. Smart Handoff Technique for Internet of Vehicles Communication using Dynamic Edge-Backup Node. *Electronics* **2020**, *9*, 524. [[CrossRef](#)]
20. Bharany, S.; Sharma, S.; Badotra, S.; Khalaf, O.I.; Alotaibi, Y.; Alghamdi, S.; Allassery, F. Energy-Efficient Clustering Scheme for Flying Ad-Hoc Networks Using an Optimized LEACH Protocol. *Energies* **2021**, *14*, 6016. [[CrossRef](#)]
21. Memon, I.; Hasan, M.K.; Shaikh, R.A.; Nebhen, J.; Bakar, K.A.A.; Hossain, E.; Tunio, M.H. Energy-Efficient Fuzzy Management System for Internet of Things Connected Vehicular Ad Hoc Networks. *Electronics* **2021**, *10*, 1068. [[CrossRef](#)]
22. Srilakshmi, U.; Veeraiyah, N.; Alotaibi, Y.; Alghamdi, S.A.; Khalaf, O.I.; Subbayamma, B.V. An Improved Hybrid Secure Multipath Routing Protocol for MANET. *IEEE Access* **2021**, *9*, 163043–163053. [[CrossRef](#)]
23. Hussain, S.M.; Yusof, K.M.; Asuncion, R. Artificial intelligence based handover decision and network selection in heterogeneous internet of vehicles. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *22*, 1124–1134. [[CrossRef](#)]
24. Jia, F.; Chen, C.; Li, J.; Chen, L.; Li, N. A BUS-aided RSU access scheme based on SDN and evolutionary game in the Internet of Vehicle. *Int. J. Commun. Syst.* **2019**, e3932. [[CrossRef](#)]
25. Yu, S.; Lee, J.; Park, K.; Das, A.K.; Park, Y. IoV-SMAP: Secure and Efficient Message Authentication Protocol for IoV in Smart City Environment. *IEEE Access* **2020**, *8*, 167875–167886. [[CrossRef](#)]
26. Wang, C.; Dai, Z.; Zhao, D.; Wang, F. A Novel Identity-based Authentication Scheme for IoV Security In order to enhance the security of the IoV (Internet of Vehicles). *Int. J. Netw. Secur.* **2020**, *22*, 627–637. [[CrossRef](#)]
27. Li, P.; Han, L.; Xu, S.; Wu, D.O.; Gong, P. Resource Allocation for 5G-Enabled Vehicular Networks in Unlicensed Frequency Bands. *IEEE Trans. Veh. Technol.* **2020**, *69*, 13546–13555. [[CrossRef](#)]
28. Pressas, A.; Sheng, Z.; Ali, F.; Tian, D.; Nekovee, M. Contention-based learning MAC protocol for broadcast vehicle-to-vehicle communication. In Proceedings of the 2017 IEEE Vehicular Networking Conference (VNC), Torino, Italy, 27–29 November 2017.
29. Rajendran, S.; Khalaf, O.I.; Alotaibi, Y.; Alghamdi, S. MapReduce-based big data classification model using feature subset selection and hyperparameter tuned deep belief network. *Sci. Rep.* **2021**, *11*, 24138. [[CrossRef](#)]
30. Veeraiyah, N.; Khalaf, O.I.; Prasad, C.V.P.R.; Alotaibi, Y.; Alsufyani, A.; Alghamdi, S.A.; Alsufyani, N. Trust Aware Secure Energy Efficient Hybrid Protocol for MANET. *IEEE Access* **2021**, *9*, 120996–121005. [[CrossRef](#)]
31. Ogudo, K.A.; Nestor, D.M.J.; Khalaf, O.I.; Kasmaei, H.D. A Device Performance and Data Analytics Concept for Smartphones' IoT Services and Machine-Type Communication in Cellular Networks. *Symmetry* **2019**, *11*, 593. [[CrossRef](#)]
32. Chiroma, H.; Abdulhamid, S.I.; Hashem, I.A.; Adewole, K.S.; Ezugwu, A.E.; Abubakar, S.; Shuib, L. Deep Learning-Based Big Data Analytics for Internet of Vehicles: Taxonomy, Challenges, and Research Directions. *Math. Problems Eng.* **2021**, *2021*, 9022558. [[CrossRef](#)]
33. Sulaiman, N.; Abdulsahib, G.M.; Khalaf, O.I.; Mohammed, M.N. Effect of Using Different Propagations on Performance of OLSR and DSDV Routing Protocols. In Proceedings of the 2014 5th International Conference on Intelligent Systems, Modelling and Simulation, Langkawi, Malaysia, 27–29 January 2014; pp. 540–545.
34. Subramani, N.; Mohan, P.; Alotaibi, Y.; Alghamdi, S.; Khalaf, O.I. An Efficient Metaheuristic-Based Clustering with Routing Protocol for Underwater Wireless Sensor Networks. *Sensors* **2022**, *22*, 415. [[CrossRef](#)] [[PubMed](#)]

35. Ebadinezhad, S. Design and Analysis of An Improved AODV Protocol Based on Clustering Approach for Internet of Vehicles (AODV-CD). *Int. J. Electr. Telecommun.* **2021**, *67*, 13–22. [[CrossRef](#)]
36. Hemavathi; Akhila, S. Reinforcement Learning based Vertical Handoff Decision Algorithm for Next Generation Wireless Network. *J. Commun.* **2021**, *16*, 566–575.
37. Alpaydin, E. Pseudo-code for value-iteration algorithm. In *Introduction to Machine Learning*, 3rd ed.; MIT Press: Cambridge, MA, USA, 2014.
38. Shashidhara, R.; Lajuvanthi, M.; Akhila, S. A Secure and Privacy-Preserving Mutual Authentication System for Global Roaming in Mobile Networks. *Arab. J. Sci. Eng.* **2021**, *47*, 1435–1446. [[CrossRef](#)]
39. Mohan, P.; Subramani, N.; Alotaibi, Y.; Alghamdi, S.; Khalaf, O.I.; Ulaganathan, S. Improved Metaheuristics-Based Clustering with Multihop Routing Protocol for Underwater Wireless Sensor Networks. *Sensors* **2022**, *22*, 1618. [[CrossRef](#)]
40. Zhang, Z.; Boukerche, A.; Ramadan, H. Design of a lightweight authentication scheme for IEEE 802.11p vehicular networks. *Ad. Hoc. Netw.* **2012**, *10*, 243–252. [[CrossRef](#)]
41. Sheikh, M.S.; Liang, J.; Wang, W. A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs). *Sensors* **2019**, *19*, 3589. [[CrossRef](#)]
42. Bagga, P.; Das, A.K.; Wazid, M.; Rodrigues, J.J.P.C.; Park, Y. Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges. *IEEE Access* **2020**, *8*, 54314–54344. [[CrossRef](#)]
43. Dibaei, M.; Zheng, X.; Jiang, K.; Abbas, R.; Liu, S.; Zhang, Y.; Xiang, Y.; Yu, S. Attacks and defences on intelligent connected vehicles: A survey. *Dig. Commun. Netw.* **2020**, *6*, 399–421. [[CrossRef](#)]
44. Zhang, J.; Zhong, H.; Cui, J.; Xu, Y.; Liu, L. SMAKA: Secure Many-to-Many Authentication and Key Agreement Scheme for Vehicular Networks. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1810–1824. [[CrossRef](#)]
45. Machaiah, B.A.; Akhila, S. Energy-Efficient Resource Allocation using Deep Learning for Internet of Vehicles. *J. Univ. Huazhong Univ. Sci. Technol.* **2021**, *2021*, 7490689. [[CrossRef](#)]
46. Subahi, A.F.; Alotaibi, Y.; Khalaf, O.I.; Ajesh, F. Packet Drop Battling Mechanism for Energy Aware Detection in Wireless Networks. *Comput. Mater. Contin.* **2021**, *66*, 2077–2086. [[CrossRef](#)]
47. Yang, J.; Deng, J.; Xiang, T.; Tang, B. A Chebyshev polynomial-based conditional privacy-preserving authentication and group-key agreement scheme for VANET. *Nonlinear Dyn.* **2021**, *106*, 2655–2666. [[CrossRef](#)]
48. Lo, N.-W.; Tsai, J.-L. An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings. *IEEE Trans. Intell. Transp. Syst.* **2015**, *17*, 1319–1328. [[CrossRef](#)]
49. He, D.; Zeadally, S.; Xu, B.; Huang, X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [[CrossRef](#)]
50. Azees, M.; Vijayakumar, P.; Deboarh, L.J. Eaap:Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular adhoc networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2467–2476. [[CrossRef](#)]
51. Liang, L.; Ye, H.; Yu, G.; Li, G.Y. Deep-Learning-Based Wireless Resource Allocation With Application to Vehicular Networks. *Proc. IEEE* **2020**, *108*, 341–356. [[CrossRef](#)]
52. Wu, H.-H. A Comparative Study of Using Grey Relational Analysis in Multiple Attribute Decision Making Problems. *Qual. Eng.* **2002**, *15*, 209–217. [[CrossRef](#)]
53. Zulqarnain, R.M.; Saeed, M.; Ahmad, N.; Dayan, F.; Ahmad, B. Application of TOPSIS Method for Decision Making. *Int. J. Sci. Res. Math. Stat. Sci.* **2020**, *7*, 76–81.