mathematics

MDPI

Article

A Secure Message Authentication Method in the Internet of Vehicles Using Cloud-Edge-Client Architecture

Yuan Zhang [1], Zihan Zhou [2,*], Chang Jiang [2], Wei Huang [2], Yifei Zheng [2], Tianli Tang [3] and Khadka Anish [4]

[1] Network and Information Center, Southeast University, Nanjing 211189, China
[2] School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China
[3] School of Civil and Transportation Engineering, Guangdong University of Technology, Guangzhou 510006, China
[4] Department of Civil & Environmental Engineering, University of Auckland, Auckland 1142, New Zealand
* Correspondence: 230239757@seu.edu.cn

Abstract

With the rapid deployment of intelligent transportation systems (ITS), the Internet of Vehicles (IoV) has become an increasingly vital component in the development of smart cities. However, the openness of IoV also gives rise to critical issues such as message security and identity privacy. Consequently, addressing message authentication in the IoV environment is a fundamental requirement for ensuring its sustainable and stable evolution. Firstly, this paper proposes an adaptive traffic authentication strategy (ATAS) By integrating traffic flow dynamics evaluation, traffic status scoring, time sensitivity assessment, and comprehensive strategy decision-making, the scheme achieves an effective balance between authentication efficiency and security in IoV scenarios. Secondly, to tackle the high overhead and security issues caused by multiple message transmissions in large-scale IoV application scenarios, this paper proposes a secure message transmission and authentication method based on the cloud-edge-client collaborative architecture. Leveraging aggregate message authentication code (AMAC) technology, this method validates both the authenticity and integrity of messages, effectively reducing communication overhead while maintaining reliable authenticated transmission. Finally, this paper builds an IoV co-simulation experimental environment using the SUMO 1.19.0, OMNeT++ 6.0.3, and Veins 5.0.0 software platforms. It simulates the interactive authentication process among vehicles, Road Side Units (RSUs), and the cloud platform, as well as the effects of traffic response strategies under different scenarios. The results demonstrate the potential of IoV authentication technology in improving traffic management efficiency, optimizing road resource utilization, and enhancing traffic safety, providing strong support for the secure communication and efficient management of IoV.

Keywords: internet of vehicles; message security; message authentication; cloud-edge-client collaboration; internet of vehicles simulation

MSC: 37M05

check for updates

Academic Editor: Cheng-Chi Lee

Received: 24 August 2025
Revised: 25 September 2025
Accepted: 14 October 2025
Published: 29 October 2025

Citation: Zhang, Y.; Zhou, Z.; Jiang, C.; Huang, W.; Zheng, Y.; Tang, T.; Anish, K. A Secure Message Authentication Method in the Internet of Vehicles Using Cloud-Edge-Client Architecture. *Mathematics* **2025**, *13*, 3446. https://doi.org/10.3390/math13213446

Copyright: © 2025 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

The safety research of complex systems has always been a hot topic [1,2]. Complex traffic system is the foundation to ensure the smooth operation of the city [3,4], and it is necessary to focus on its safety research [5]. The Internet of Vehicles (IoV) is one of the important research contents in complex traffic system, and it is also one of the research fields

that researchers focus on in recent years. The Internet of Vehicles is a key component of the Internet of Things (IoT), with vehicles serving as primary sensors [6,7]. It leverages cutting-edge information and communication technologies to establish efficient networks that connect vehicles and infrastructure [8]. Its main goal is to enhance vehicular intelligence using communication technologies, thereby enhancing driving experiences, improving the quality of transportation services [9], and fostering the development of safe and efficient transportation systems [10]. However, such developments in the automotive industry have introduced a range of complex security challenges, mainly concerning the safety of vehicle operations, data protection, and network security [11].

By analyzing the security vulnerabilities and attack methods of the IoV system, our research aims to propose security measures that can effectively safeguard the IoV system. Furthermore, the research offers practical suggestions and guidance to automobile manufacturers and technology developers on improving the security of the IoV system [12,13]. Ultimately, this work contributes to the broader objective of advancing intelligent transportation systems and smart city initiatives by ensuring the secure and reliable operation of IoV networks.

1.1. Literature Review

1.1.1. Message Authentication in IoV

As a crucial part of the modern transportation system, ensuring the security of wireless communication within IoV is vital [14]. However, this wireless communication method is highly vulnerable to attacks, including detection, interception, modification, and replay. These security risks may lead to the transmission of false messages, potentially resulting in severe outcomes such as traffic crashes [15]. To avoid these security attacks and ensure the integrity and reliability of messages, researchers have applied message signing and authentication technology to IoV. To protect intelligent connected vehicles from spoofing attacks, researchers have proposed a variety of lightweight message authentication protocols for vehicle-mounted Controller-Area Networks (CAN) [16]. Jo, Kim [17] proposed an improved authentication protocol, Message Authentication-CAN, which eliminated the need to modify the CAN controller hardware, reduced the load of the CAN bus, and defended against DoS attacks. Subsequently, Kang [18] proposed a lightweight authentication protocol that could be easily deployed on CAN by executing electronic control units (ECU) firmware updates. It was found to attain high security and authentication efficiency. Kim, Jo [19] proposed a formalized CAN model that could capture the timing behavior of CAN at the Media Access Control (MAC) layer of the data link layer and be used to verify the security of other CAN applications. At present, lightweight message authentication protocols are designed with high real-time performance to support fast data processing and transmission. While ensuring the security and integrity of the message, it can also adapt to the environment with limited vehicle network resources. Considering the current bandwidth resources and message response time requirements of vehicular networks, the existing research fails to address three key questions: (i). how security can be enhanced without significantly increasing computational burden, (ii). how to address advanced network attack techniques, and (iii). how can standardization and interoperability be achieved while maintaining lightweight characteristics?

To further address the issues of computational and communication overhead, building on solutions proposed by Zhang, Ho [20] and Huang, Yeh [21], Lee and Lai [22] proposed a vehicular network message authentication scheme based on elliptic curve signatures. The scheme maintained efficiency while improving security. Bayat, Barmshoory [23] analyzed and proved that the scheme proposed by Lee and Lai [22] was vulnerable to masquerading attacks. Subsequently, they proposed an improved solution and demonstrated its security

and correctness. Ali, Chen [24] proposed an elliptic curve cryptosystem-based hybrid signcryption (ECCHSC) protocol. Implementing smart cities while leveraging IoV would also increase security threats that arise due to insecure communication between entities. To solve this problem, Bagga, Sutrala [25] proposed a new blockchain batch authentication scheme, BBAS-IoV, to register vehicles and RSUs before vehicle deployment. Moreover, as many existing IoV message authentication schemes lack support for mutual authentication between nodes, Qureshi, Sandila [26] proposed an efficient security application authentication scheme for IoV messages. This scheme constructed a lightweight authentication protocol utilizing Radio-Frequency Identification Devices (RFID) while employing a mutual message authentication mechanism between drones and vehicle nodes to ensure robust security and authentication within IoV.

1.1.2. Cloud-Edge-Client Collaborative Architecture

Cloud computing is a technology that uses the Internet to provide computing resources and data storage [27]. It enables users and enterprises to access software, storage services, and processing power via the Internet without purchasing or managing physical servers [28]. This model provides elasticity, scalability, and cost efficiency, and users can instantly increase or decrease resources according to demand, thereby, optimizing the cost structure [29]. With the advancement of technology, cloud computing has become an infrastructure that supports advanced applications such as remote work, data analysis, artificial intelligence, and machine learning [30].

Edge computing is a distributed computing architecture that transfers data processing tasks from central servers to clients at the edge of the network, that is, close to the location where data is generated or collected, which can significantly reduce data transmission delays and improve response speed and system efficiency [31]. After a large amount of data is processed locally, only part of the necessary information needs to be sent to the central server, thereby easing the pressure on the central cloud server, improving bandwidth utilization, and enhancing data security and privacy protection [32]. Edge computing has become an ideal choice for applications with high real-time data processing requirements, such as the Internet of Things, smart cities, and autonomous vehicles [33–36]. Cui, Wei [37] proposed a security privacy protection authentication scheme that incorporates edge computing concepts to the message authentication process of vehicular ad hoc networks (VANETs). Subsequently, Cui, Zhang [38] proposed a secure vehicle network authentication scheme using a cloud broker (*CB*) as an intermediary in a multi-cloud environment. They proposed a new vehicle network architecture suitable for a multi-cloud environment. The CB, managed by a trusted authority (*TA*), selects a suitable cloud service provider (CSP) for the vehicle. To address the authentication challenge in a multi-cloud environment, Zhang, Zhong [39] proposed a many-to-many authentication and key agreement scheme between vehicles and CSPs. This approach ensures data security and user privacy by establishing session keys in multi-party mutual authentication.

Due to the ongoing increase in data volume and computing demand, the collaboration between cloud computing and edge computing has become the key to improving application performance. It can not only reduce data transmission delay but also reduce energy consumption and improve user experience. However, the development of cloud-edge-client collaboration is still in the exploratory stage, and research is mainly focused on areas such as the Internet of Things and the Industrial Internet that particularly require fast response and efficient data processing capabilities. Ren, He [40] proved that the collaboration between cloud computing and edge computing can effectively improve latency performance. Ding, Zhou [41] proposed a cloud-edge collaboration framework for deep learning models of cognitive services, which has faster response and higher accuracy. Zhang, Chen [42]

proposed a device management service system based on cloud-edge collaboration, which not only improved the system's response speed but also reduced the data transmission pressure of the central cloud server.

1.2. Main Contributions

Message authentication in IoV has been proven to be a crucial means to address security issues. The core objective of existing research is to ensure the security and authenticity of communications among vehicles and between vehicles and infrastructure. The broader focus is on preventing various attacks, optimizing system scalability, reducing computational and communication overhead to adapt to high-speed and high-volume vehicular environments, and providing privacy protection for vehicle data. These measures aim to ensure the efficient and reliable operation of intelligent transportation systems. However, current research still exhibits some limitations regarding security and efficiency.

Moreover, the existing cloud-edge-client technology of the Internet of Vehicles proposes an architectural model in which multiple cloud devices are organized hierarchically from the end devices upward. It generally adopts the traditional top-down control and instruction processing method and fails to emphasize and apply cloud computing architecture and cloud control technology.

To address the security issues in IoV, this paper analyzes and studies the existing message authentication schemes and proposes an improved solution algorithm. The contributions of this research are as follows:

(1) An efficient and secure adaptive traffic flow authentication strategy (ATAS) is proposed based on the ECDSA and Ed25519 digital signature algorithms with high authentication efficiency. The introduction of this scheme makes the security authentication process in IoV more efficient and reliable while ensuring the information exchange between vehicles and infrastructure is secure.

(2) Leveraging Message Authentication Code (MAC) technology, the aggregated MAC technology is adopted to propagate data in large-scale IoV scenarios. Additionally, a cloud platform is established to monitor RSUs and report security issues to vehicles in a timely manner. Also, an IoV authentication model is developed based on a cloud-edge-client collaborative architecture. The model effectively reduces network latency and load, enhances data security and privacy, and provides a new solution for secure communications in IoV.

(3) We proposed traffic response strategies for incidents using a simulation platform, analyzing IoV incident scenarios with different connected vehicle rates, congestion levels, and locations. The effectiveness of post-incident IoV message authentication was assessed, and the potential of IoV authentication to boost traffic management, optimize road use, and enhance safety was analyzed.

2. Materials and Methods

2.1. Security Message Authentication Scheme for IoV

Considering the variability of IoV under different traffic flow conditions, safety message authentication schemes must consider safety, efficiency, and adaptability. To address these requirements, this paper proposes an Adaptive Traffic Authentication Strategy (ATAS), which combines the security and efficiency advantages of the Elliptic Curve Digital Signature Algorithm (ECDSA) [43] and Edwards-curve Digital Signature Algorithm (EdDSA) [44] with the dynamic characteristics of IoV, taking into account the dynamic changes in traffic flow. ATAS intelligently selects the most appropriate digital signature algorithm by analyzing real-time traffic flow data, e.g., vehicle count, average speed, and detector occupancy, allowing it to adjust the authentication process dynamically. This ensures optimal

efficiency and response speed, providing an efficient, reliable, and adaptable solution for safety authentication while maintaining acceptable safety levels.

To meet the complex and evolving demands of IoV environments, the ATAS (See Figure 1) is designed to maintain prompt communication in high-traffic scenarios. The strategy also enhances security measures in low-traffic situations by utilizing additional computational resources. This adaptive approach allows the system to optimize performance without compromising safety.

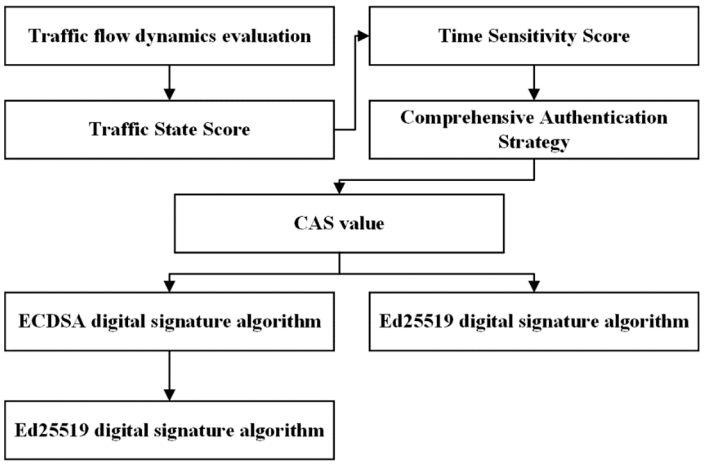


Figure 1. Adaptive Traffic Authentication Strategy.

By leveraging the characteristics of the IoV environment, such as high dynamics and uncertainty, ATAS makes full use of real-time traffic flow information to implement intelligent and adaptive authentication strategies that improve overall system performance and user experience. This method ensures robust communication security and supports the ongoing advancement of intelligent transportation systems.

(i) Decision Model

The parameters used in the ATAS are defined in Table 1.

Table 1. Parameter Definition for ATAS.

Parameter	Description
T_l	Time since the last detection.
P_c	The percentage of time during the current time interval that the detector was occupied by vehicles.
P_l	The percentage of time during the last time interval that the detector was occupied by vehicles.
V_c	The average speed of vehicles during the current time interval.
V_l	The average speed of vehicles during the last time interval.
N_c	The number of vehicles that passed the detector during the current time interval.
N_l	The number of vehicles that passed the detector during the last time interval.
R_d	Detection range of the detector.

(a) Traffic flow dynamics evaluation

To evaluate the dynamics of traffic flow, the changing rate of traffic flow between the current and previous time intervals can be calculated as:

$$\Delta P = P_c - P_l,\ \Delta V = V_c - V_l,\ \Delta N = N_c - N_l \tag{1}$$

(b) Traffic State Score (TSS)

TSS is calculated by considering both the dynamic changes and the current state of traffic flow.

$$TSS = (V_c + \Delta V) \cdot (N_c + \Delta N) \cdot |1 - P_c - \Delta P| \tag{2}$$

(c) Time Sensitivity Score (TSSe)

To account for the impact of time, TSSe is introduced. TSSe incorporates the time since the last detection and the detection range of the detector:

$$TSSe = \eta_1 \cdot \frac{1}{T_l} + \eta_2 \cdot R_d \tag{3}$$

where η_1 and η_2 are weight coefficients.

(d) Comprehensive Authentication Strategy (CAS)

The final CAS is formulated by integrating the TSS and the TSSe.

$$CAS = TSS + TSSe \tag{4}$$

Based on the CAS value, an appropriate authentication policy can be dynamically selected according to a predetermined threshold.

For lower CAS values, indicating a lower current security message authentication load within the IoV, more computational resources are available. In such cases, a more complex but secure authentication method, combining the ECDSA digital signature algorithm with the Ed25519 digital signature algorithm, may be selected. For higher CAS values, indicating a larger current security message authentication load and fewer available resources, the system may opt for a simpler authentication method using only the Ed25519 digital signature algorithm. The algorithm is suitable for high traffic flow and high time sensitivity scenarios.

(ii) System initialization (Algorithm 1)

Algorithm 1 System Initialization

Step 1:	The *TA* randomly selects two large prime numbers p and q and a non-singular elliptic curve E defined over a finite field $\mathbb{F}_p$, described as $y^2 = x^3 + ax + b \ mod \ q$. A generator point P is randomly selected from the elliptic curve group.
Step 2:	The *TA* randomly selects a system private key $P_{pri} \in Z_q^*$ and calculates the system public key $P_{pub} = P_{pri} \cdot P$.
Step 3:	The *TA* randomly selects $PK_R \in Z_q^*$ as the private key for the RSU and calculates the corresponding RSU public key: $PK_R = SK_R \cdot P$.
Step 4:	The *TA* selects a secure hash function h: $h : \{0,1\}^* \rightarrow Z_q$.
Step 5:	The *TA* securely transmits the private key SK_R to the RSU.
Step 6:	The *TA* publishes the system's public parameters $\left\{p, q, a, b, P, P_{pub}, PK_R, h\right\}$ to the RSU and all vehicles.

(iii) Key generation

Given the use of both ECDSA and Ed25519 in the ATAS, the key generation processes for both algorithms are outlined below (Algorithms 2 and 3).

Algorithm 2 ECDSA key generation

Step 1:	Select the elliptic curve and the base point. Vehicle V selects a base point G_1 on the elliptic curve E with order n.
Step 2:	Generate the private key. Vehicle V randomly generate $SK_{EC} \in [1, n-1]$ as its ECDSA private key.
Step 3:	Calculate the public key. Vehicle V calculates its ECDSA public key $PK_{EC} = SK_{EC} \cdot G_1$.

Algorithm 3 Ed25519 key generation

Step 1:	Select the elliptic curve and the base point. Vehicle V uses the predefined base point G_2 of Ed25519, with order l.
Step 2:	Generate private key. Vehicle V generates a 256-bit random number SK_{Ed} as its Ed25519 private key.
Step 3:	Calculate the public key. Vehicle V calculates its Ed25519 public key $PK_{Ed} = SK_{Ed} \cdot G_2$.

(iv) Message Signature

When vehicle V enters the range of RSU, the RSU uses the ATAS to analyze the relevant traffic detection parameters and decide on the appropriate authentication method. If the decision results in a lower CAS value, a combination of the ECDSA and Ed25519 digital signature algorithm is employed (Algorithm 4).

Algorithm 4 Combination of ECDSA and Ed25519

Step 1:	Select a random number k, $k \in [1, n-1]$.
Step 2:	Calculate the solution point $R = (x, y) = SK_{EC} \cdot G_1$ and set $r = R_x \ mod \ n$. If $r = 0$, reselect k.
Step 3:	Calculate the signature value s: $s = k^{-1}(H(m) + SK_{EC} \cdot r) \ mod \ n$. If $s = 0$, reselect k.
Step 4:	Calculate the random number $t = H(SK_{Ed}\|\|s)$.
Step 5:	Calculate the temporary solution point $R' = t \cdot G_2$.
Step 6:	Calculate the final signature value s': $s' = (t + H(R'\|\|PK_{Ed}\|\|s)) \cdot SK_{Ed} \ mod \ l$.
Step 7:	Transmit the signature value s, the final signature value s', the message m, and the related publicly available parameters to the RSU.

If the decision results in a higher CAS value, only the Ed25519 digital signature algorithm is used (Algorithm 5).

Algorithm 5 Ed25519 Digital Signature

Step 1:	Calculate the random number $t = H(SK_{Ed}\|\|m)$.
Step 2:	Calculate the temporary solution point $R' = t \cdot G_2$.
Step 3:	Calculate the final signature value s': $s' = (t + H(R'\|\|PK_{Ed}\|\|m)) \cdot SK_{Ed} \ mod \ l$.
Step 4:	Transmit the signature value s', message m, and related publicly available parameters to the RSU.

(v) Message Verification

Upon receiving the message, the RSU verifies the message signature from the combination of the ECDSA and Ed25519 digital signature algorithm as follows (Algorithm 6).

Algorithm 6 Message Verification of Combination

Step 1:	Calculate $R'' = s' \cdot G_2 - H(R'\|\|PK_{Ed}\|\|s)$.
Step 2:	Verify that if $R'' \neq R'$, it indicates a failure in the Ed25519 digital signature authentication, and the message is discarded. Verify that if $R'' = R'$, it indicates that the Ed25519 digital signature authentication is successful, and then proceed to the next step.
Step 3:	Verify whether r and s are within the interval $[1, n-1]$.
Step 4:	Calculate $\omega = s^{-1}\ mod\ n,\ \mu_1 = H(m) \cdot \omega\ mod\ n,\ \mu_2 = r \cdot \omega\ mod\ n$.
Step 5:	Calculate the solution point $X = (x_1, y_1) = \mu_1 \cdot G + \mu_2 \cdot PK_{EC}$.
Step 6:	Verify that if $X \neq O$ (not equal to the point at infinity) and $r = x_1\ mod\ n$, it indicates that both digital signature authentications are successful, and the message is accepted.

When only the Ed25519 digital signature algorithm is employed, the RSU performs the following verification process upon receiving the message (Algorithm 7).

Algorithm 7 Message Verification of Ed25519

Step 1:	Calculate $R'' = s' \cdot G_2 - H(R'\|\|PK_{Ed}\|\|m)$.
Step 2:	Verify that if $R'' \neq R'$, it indicates a failure in the Ed25519 digital signature authentication, and the message is discarded. Verify that if $R'' = R'$, it indicates that the Ed25519 digital signature authentication is successful, and the message is accepted.

2.2. Internet of Vehicles Authentication Based on Cloud-Edge-Client Collaborative Architecture

To solve the transmission speed and overhead problems in message authentication, this paper proposes a secure message transmission and authentication method based on the cloud-edge-client collaborative architecture. This method employs aggregated message authentication code (MAC) technology to verify the authenticity and integrity of messages, reducing communication overhead. Within this framework (shown in Figure 2), the cloud platform functions as a "cloud" endpoint overseeing RSU message broadcast, the RSUs serve as the "edge" endpoints, and vehicles act as the "client" endpoints. This structure ensures the accuracy and security of authenticated message transmission.

In this architecture, vehicles communicate with each other or RSUs through the dedicated short-range communication (DSRC) protocol. The system model comprises four primary entities: the cloud platform (*C*), the trusted authority (*TA*), the road side unit (RSU), and on-board units (OBUs). The *TA* is responsible for registering RSUs and OBUs, generating public–private key pairs, and managing the privacy of all vehicles, including the driver's identity information. RSUs, fixed along the roadside, verify the authenticity and integrity of the message and forward the authentic message to vehicles within their coverage area or beyond via interconnected RSUs. RSUs also manage the privacy information of all vehicles within their communication range, including the identity, public key, shared key, and timestamp. OBUs, installed in vehicles, are responsible for sensing the road conditions. However, compared to RSUs, OBUs have shorter communication distances and limited computing power. The cloud platform supervises the correctness of message broadcasts by synchronizing authentication and decryption processes with RSUs

and monitoring RSU activities. This collaborative effort culminates in a cloud-edge-client collaboration authentication model. In this model, the *TA* is assumed to be a trusted entity, while RSUs are considered potentially untrustworthy. We summarize in Table 2 the parameter definitions that will be used in the future.

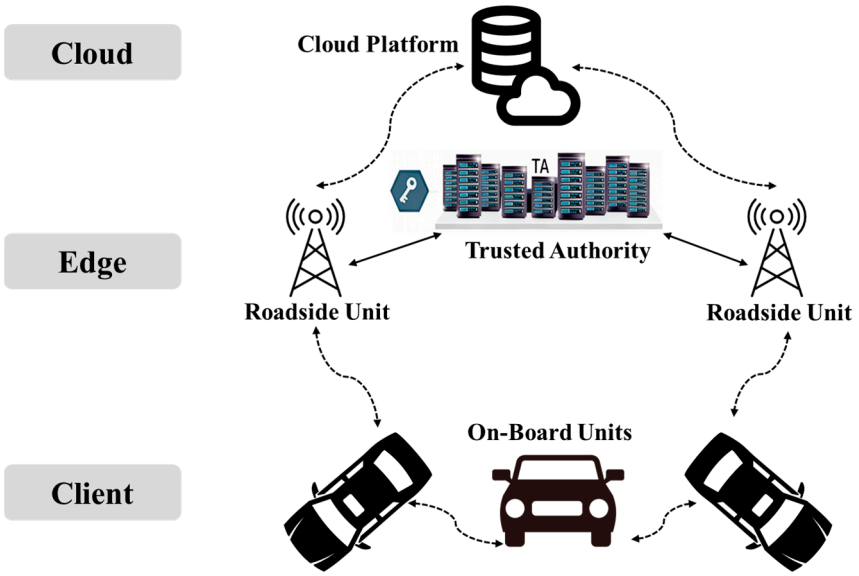


Figure 2. Cloud-Edge-Client Collaborative Architecture.

Table 2. Parameter Definition for Internet of Vehicles Authentication.

Parameter	Description
V_i	Vehicle i
V_t	Forwarding node vehicle
R_j	Road Side Unit RSU
g, a, b	Diffie-Hellman key exchange protocol parameters
ID_{v_i}	Identifier of vehicle V_i
ID_{R_j}	Identifier of $RSU(R_j)$
PID_{v_i}	Pseudo-identity of vehicle V_i
PK_{v_i}	Public key of vehicle V_i
SK_{v_i}	Private key of vehicle V_i
PK_{R_j}	Public key of $RSU(R_j)$
SK_{R_j}	Private key of $RSU(R_j)$
K_{ij}	Shared key between vehicles V_i and R_j
$MAC_{K_{ij}}$	Aggregate authentication tags
Ts	Timestamp
Sq	Message sequence number
n	Number of vehicles sending and forwarding messages

(i) Establishing a Shared Key

When the vehicle V_i enters the communication range of an $RSU(R_j)$, both parties initiate the process to establish a shared key. This process utilizes the Diffie-Hellman key exchange protocol [45] for mutual authentication and shared key establishment, as illustrated in Figure 3.

In this protocol, g^a and g^b are two parameters of the Diffie-Hellman key exchange protocol, through which the shared key K_{ij} of vehicle V_i and $RSU(R_j)$ can be calculated. On receiving the first message from vehicle V_i, $RSU(R_j)$ decrypts the message using its private key SK_{R_j} to extract the vehicle identifier ID_{v_i}, parameter g^a, and timestamp Ts. It then uses the public key PK_{v_i} to authenticate vehicle V_i. If the authentication is successful, $RSU(R_j)$

assigns a pseudo-identity PID_{v_i} to vehicle V_i, which is associated with the shared key K_{ij}. This pseudo-identity allows $RSU(R_j)$ to find the vehicles sending messages. Similarly, vehicle V_i decrypts the second message and authenticates $RSU(R_j)$. If successful, vehicle V_i signs $\left\{g^b, Ts\right\}_{SK_{v_i}}$ using its private key SK_{v_i} and sends the signature to $RSU(R_j)$.

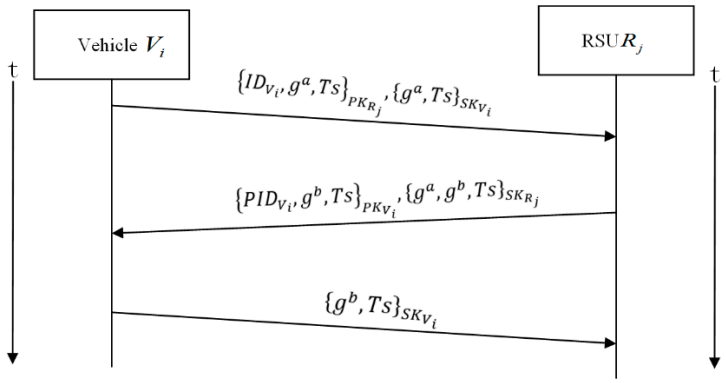


Figure 3. Mutual authentication and shared key establishment process.

(ii) Aggregate Message Authentication Code

After establishing the shared key, when vehicle V_i detects an event M and wants to communicate it to other vehicles, it first encrypts the event M using the shared key K_{ij} with $RSU(R_j)$ to obtain the message $M_i = \{M, Ts, Sq\}_{K_{ij}}$. Vehicle V_i then generates an aggregate authentication tag for M_i.

$$tag = MAC_{K_{ij}}(M_i) \tag{5}$$

Finally, vehicle V_i sends ID_{R_j}, PID_{v_i}, M_i and tag to R_j. The process is shown in Figure 4.

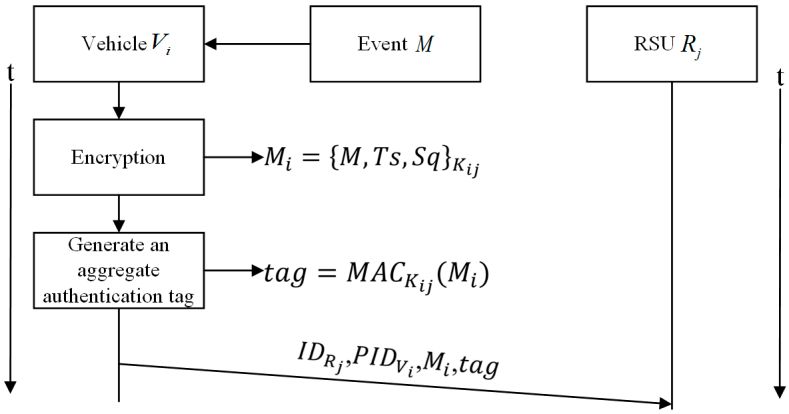


Figure 4. Event perception processing flow.

During the transmission, if vehicle V_i moves beyond the communication range of $RSU(R_j)$, the aggregate authentication tag tag_i of vehicle V_i must be forwarded to $RSU(R_j)$ using an appropriate routing protocol. To prevent the forwarding node from forging or tampering with the message and reduce the additional communication overhead, this method employs an aggregate message authentication code to verify the authenticity and integrity of the message.

If vehicle V_i moves out of the communication range of $RSU(R_j)$, the message must be forwarded by a forwarding node vehicle V_t. The process is shown in Figure 5 and Algorithm 8.

Algorithm 8 Event message forwarding process

Step 1:	After receiving the message from vehicle V_i, the forwarding node vehicle V_t uses the shared key K_{tj} with $RSU(R_j)$ to generate an aggregate authentication tag for message M_i: $tag' = MAC_{K_{tj}}(M_i)$.
Step 2:	XOR with the aggregate verification tag of vehicle V_i to obtain the aggregate verification tag of forwarding node vehicle V_t: $tag_t = tag \oplus tag'$.
Step 3:	Send ID_{R_j}, PID_{v_i}, PID_{v_t}, M_i, and tag_t to the next forwarding node V_x.
Step 4:	Repeat the cycle process Step1~3 until the message reaches R_j.

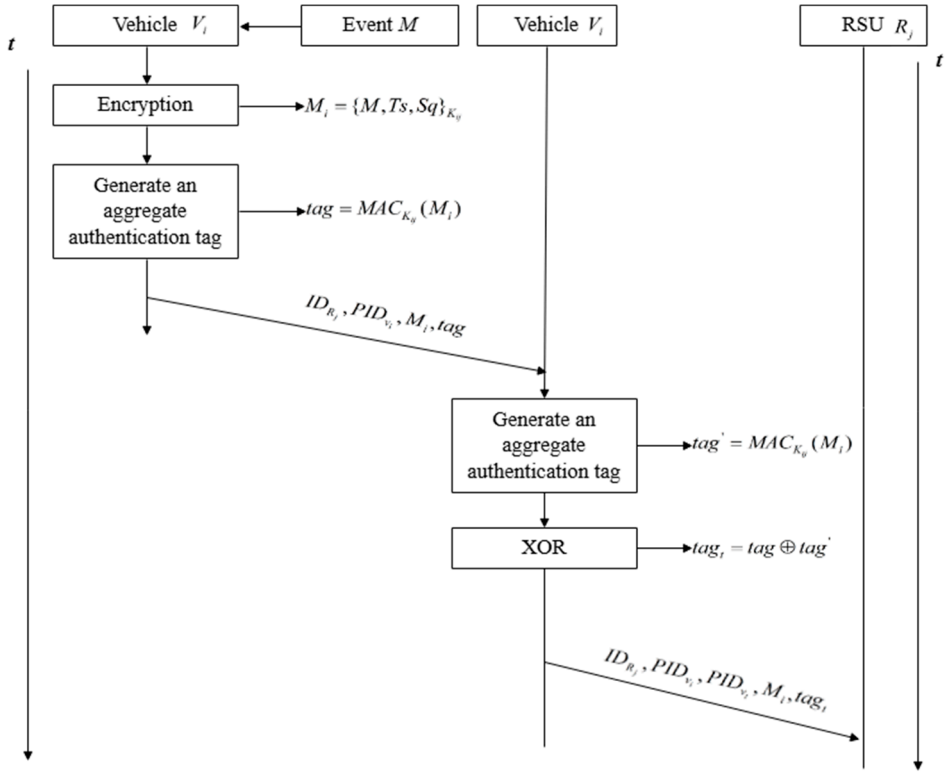


Figure 5. Event message forwarding process.

(iii) Message Authentication and Dissemination

Since the $RSU(R_j)$ has a shared key with each forwarding node, when receiving a message from a forwarding node vehicle V_x, an aggregate verification tag can be calculated to verify the authenticity and integrity of the received message (l is the number of vehicles sending and forwarding information).

$$tag_c = \oplus_{p=1}^{l} MAC_{k_{pj}}(M_i) \tag{6}$$

If $tag_c = tag_t$, the message is considered to have not been tampered with, the message integrity can be determined, and the message M_i is broadcast to other vehicles within the range.

If $tag_c \neq tag_t$, the message is considered to have been tampered with or forged during transmission, and $RSU(R_j)$ will reject the message.

(iv) Cloud-Edge-Client Collaborative Authentication

In the process of broadcasting messages, $RSU(R_j)$ may be used by attackers to spread false information to other vehicles. To further ensure the authenticity and integrity of the message broadcast process, the message forwarded by V_x to R_j will be synchronously

verified through the cloud platform C. Among them, since the cloud platform C and $RSU(R_j)$ are in fixed positions, the two-party communication adopts the commonly used encryption algorithm in China by default to achieve the highest security message transmission efficiency.

In this scheme, if the last forwarding node vehicle V_x sends a message to $RSU(R_j)$, the synchronous verification process at this time is shown in Figure 6 and Algorithm 9.

Algorithm 9 Synchronous verification process

Step 1:	The last forwarding node vehicle V_x sends ID_{R_j}, PID_{v_i}, PID_{v_t}, M_i and tag_t to the cloud platform C at the same time.
Step 2:	Cloud platform C and $RSU(R_j)$ perform authentication and decryption operations synchronously to obtain message M_i'. At this time, cloud platform C conducts directional monitoring of $RSU(R_j)$ through the received ID_{R_j}.
Step 3:	After receiving the message and verifying the authenticity and integrity of the message, $RSU(R_j)$ broadcasts the received message M_i to the vehicles within the range.
Step 4:	Cloud platform C compares the message M_i obtained by monitoring $RSU(R_j)$ with the message M_i' obtained by authentication and decryption. ① If $M_i' = M_i$, no action is taken. ② If $M_i' \neq M_i$, the correct message is immediately sent to the vehicle within the range of $RSU(R_j)$ for maintenance correction and a prompt warning is issued to the vehicle.

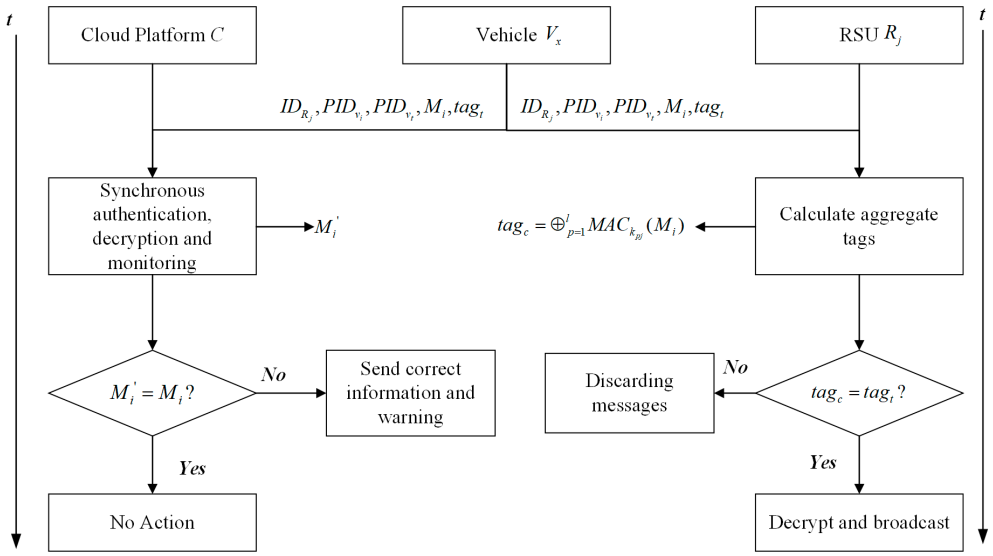


Figure 6. Cloud-edge-client collaborative process.

3. Results and Discussion

3.1. Performance Analysis of Adaptive Traffic Authentication Strategy

When evaluating the performance of different security authentication algorithms, the primary focus will be on analyzing the algorithm's processing time, given the limited system resources and computing power. The evaluation was conducted on a computer with an AMD Ryzen 5 5600X 6-Core Processor at 3.70 GHz, 16 GB RAM, and running Windows 10.

As shown in Figure 7, following a series of comparisons of security authentication algorithm efficiency, the performance characteristics observed are as follows.

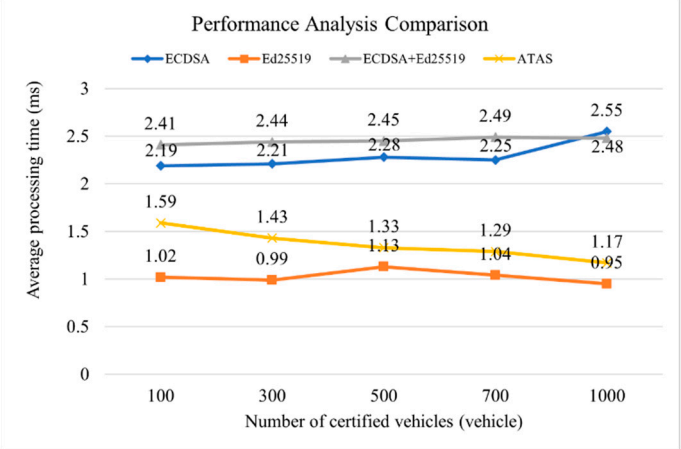


Figure 7. Performance Analysis Comparison.

At a relatively low number of authenticated vehicles (100 vehicles), the ECDSA digital signature algorithm exhibits the best processing time performance. However, as the number of authenticated vehicles increases, its processing time increases linearly from 2.19 milliseconds to 2.55 milliseconds. This indicates that ECDSA may encounter performance bottlenecks when processing large amounts of data.

In all tests, Ed25519 shows relatively consistent processing time and outperforms ECDSA. Although its processing time increases under high load (500 vehicles authenticated), the overall increase is small, up to 1.13 milliseconds. This reflects the scalability advantage of the Ed25519 digital signature scheme.

When the ECDSA and Ed25519 algorithms are used in simple combination (ECDSA+Ed25519), the processing time is significantly higher than when either algorithm is used individually. Especially when there are a large number of vehicles, the processing time increases from 2.41 milliseconds to 2.48 milliseconds, which is almost twice as long as when Ed25519 is used alone.

After introducing the Adaptive Traffic Flow Authentication Strategy (ATAS), the performance of the combined algorithm was significantly improved. ATAS effectively reduces the processing time, especially in the case of a high number of vehicle authentication, from 1.59 milliseconds to 1.17 milliseconds, showing the significant role of ATAS in performance optimization.

Overall, the Ed25519 digital signature algorithm excelled in the single algorithm test, and the ATAS further improved the performance when the number of vehicles is large. When selecting an appropriate vehicle network security authentication scheme, it is crucial to consider multiple factors such as the algorithm's computational complexity, system resources, and processing time.

3.2. Security Analysis of IoV Authentication Based on Cloud-Edge-Client Collaborative Architecture

3.2.1. Message Integrity and Traceability

In the Internet of Vehicles, ensuring the integrity and traceability of messages is crucial to ensuring the security of the network. Attackers may try to tamper with messages in transit or insert forged messages into the network in order to mislead the receiver or disrupt the normal operation of the system. For example, attackers may tamper with traffic information or forge emergency notifications, causing serious traffic chaos or safety

accidents, which not only threatens the correctness of the decision-making of the message receiver, but also poses a direct threat to personnel safety; and the lack of traceability will make it extremely difficult to track the source of the attack, thereby increasing the challenges of network management and security maintenance. Therefore, the Internet of Vehicles security authentication scheme must ensure that the message has not been tampered with during transmission and can be accurately traced back to the sender.

In this scheme, when the RSU receives a message, it will find the shared key k of the sender and all forwarding nodes based on the vehicle pseudo-identity *PID*, and use the shared key *k* to calculate the aggregate message authentication code *AMAC* for the received message *M*, *PID*, etc.:

$$AMAC = MAC_{K_{1j}}(M_1) \oplus MAC_{K_{2j}}(M_1) \oplus \cdots \oplus MAC_{K_{nj}}(M_1) \tag{7}$$

Subsequently, the RSU compares the calculated aggregate message authentication code AMAC with the received aggregate message authentication code $AMAC'$ for verification:

(1) If $AMAC = AMAC'$, the message is considered to have not been tampered with and the message integrity can be determined.

(2) If $AMAC \neq AMAC'$, the message is considered to have been tampered with or forged during transmission and the RSU will reject the message.

In addition, each vehicle has an independent shared key with the RSU. If the RSU can find a shared key, the RSU can obtain the identity of the message sender through a decryption operation, thereby authenticating the message source and preventing identity forgery. $Dec(\cdot)$ is the decryption function and $Lookup(\cdot)$ is the operation function for querying the mapping table.

$$ID = Dec(k, Lookup(PID)) \tag{8}$$

3.2.2. Identity Privacy Protection

Identity privacy protection is another important security issue in the Internet of Vehicles. In the Internet of Vehicles, the communication of vehicles is public, and attackers can track the action patterns of specific vehicles and even identify the real identity of the vehicle by analyzing the exchanged messages. This attack on personal information not only violates the privacy rights of users, but may also be used for illegal purposes, such as targeted attacks or fraud. If the attacker can forge the identity of the vehicle, it may also send false information to interfere with the operation of the network or conduct malicious attacks. Therefore, while ensuring the efficiency and accuracy of Internet of Vehicles communication, it is also necessary to pay attention to the effective protection of the identity privacy of the vehicle.

In this scheme, in order to better protect the identity privacy of the vehicle, a new pseudo-identity is generated every time the vehicle enters the communication range of an RSU, so as to avoid the identity being tracked due to the long-term use of the same pseudo-identity. The RSU maintains a mapping table from pseudo-identity to real identity, and only when necessary (for example, when the vehicle spreads false information) can the real identity of the vehicle be queried through the pseudo-identity $ID = Dec(k, Lookup(PID))$. In this process, the RSU uses the shared key *k* to decrypt the mapping result, ensuring that even if the mapping table is leaked, the attacker cannot directly obtain the real identity information of the vehicle from it, thereby further enhancing the privacy protection of the vehicle.

3.2.3. Internal Attack Protection

Internal attacks refer to attacks launched after legitimate nodes within the network are controlled by attackers. In the Internet of Vehicles, internal attacks are particularly dangerous. Attackers can use the vehicle's own communication capabilities and network permissions to launch more covert and effective attacks. For example, a vehicle controlled by an attacker can send false traffic reports, mislead other vehicles, or spread malware in the network. The concealment of internal attacks makes them particularly difficult to detect and defend against. Conventional defense mechanisms based on trust management and behavioral analysis are often limited in effectiveness when facing the highly dynamic and large-scale Internet of Vehicles.

In this scheme, the Diffie-Hellman public key protocol is used in the symmetric key establishment process. When establishing the symmetric key, private key information does not need to be sent, which reduces the risk of internal attacks. At the same time, since the shared key is updated every time, the vehicle enters the communication range of an RSU, even if some information of the vehicle is obtained by the attacker, the key has been updated, and the new communication content cannot be decrypted using this information.

Through this solution, attackers cannot obtain the communication content of each message during the forwarding process, effectively preventing the impact of internal attacks on the Internet of Vehicles.

3.2.4. Replay Attack

Replay attacks are a common type of network attack, where attackers intercept legitimate messages and resend them at different times or contexts to deceive the recipient. In the Internet of Vehicles, replay attacks may cause disruption to traffic flow by replaying outdated traffic information, or replaying old authentication messages to bypass security checks. Due to the high mobility of the Internet of Vehicles, replay attacks become easier to perform and more difficult to detect. Attackers can take advantage of the high-speed movement of vehicles to capture messages from one location and then replay them in another location, causing time and space dislocation of information. And because of the large number of nodes in the Internet of Vehicles, attackers can choose to replay captured messages in different parts of the network, increasing the difficulty of network security defense. Therefore, the most important thing to defend against replay attacks is to design effective mechanisms to ensure the timeliness and context relevance of messages.

In this scheme, each message is accompanied by a timestamp Ts to ensure the freshness of the message; each message is also accompanied by a message sequence number Sq. The replayed message will be identified and rejected by the RSU because the message sequence number does not match. After receiving the message, the RSU will check the message sequence number and the difference between the timestamp and the current time:

$$\Delta Ts = Ts_{current} - Ts_{message} \tag{9}$$

(1) If the difference between the timestamp and the current time is within an acceptable range and the message sequence number matches, the message is considered fresh.

(2) If the time difference is too large, or the message sequence number does not match, the message is considered part of a replay attack and is ignored.

Through the timestamp Ts attached to each message, even if an attacker obtains and attempts to replay old messages, these messages will not be accepted for processing.

3.2.5. Man-in-the-Middle Attack

Man-in-the-Middle Attack (MitM) is a common attack form in network security. The attacker inserts himself between the two communicating parties to intercept, modify

and forward the messages between the two communicating parties. In the Internet of Vehicles environment, the risk of MitM attack is particularly prominent. Attackers can easily put themselves between the two communicating parties by taking advantage of the openness of wireless communication and the frequent message exchange between vehicles. Once the MitM attack is successful, the attacker can not only eavesdrop on the communication content of the two communicating parties, but also tamper with the exchanged information, such as forging traffic instructions or sending false messages by impersonating other vehicles. This attack poses a direct threat to vehicle driving decisions and road safety management.

In this scheme, the communicating parties not only need to verify each other's identity, but also need to establish a shared session key through a secure key negotiation process:

$$k = g^{ab} \ mod \ p \tag{10}$$

Since the key negotiation process relies on the private keys of both parties and the negotiation results are unknown to both parties, even if the middleman intercepts the information of the negotiation process, he cannot calculate the session key. At the same time, each message is accompanied by an aggregate message authentication code (*AMAC*) based on a shared key to verify the integrity and source authenticity of the message, which can fully protect the communication between the vehicle and the RSU.

3.3. Performance Analysis of IoV Authentication Based on Cloud-Edge-Client Collaborative Architecture

In this section, we evaluate the average processing time required for a vehicle V to send data to an RSU and complete the authentication process under three different scenarios, as defined below.

Scenario 1: Vehicle V remains within the communication range of the RSU and does not need to forward data to other forwarding node vehicles. This scenario is referred to as "No forwarding".

Scenario 2: Vehicle V has exited the communication range of the RSU while sending data, necessitating the forwarding of data to another vehicle V_1. In this case, Vehicle V_1 remains within the RSU's communication range, allowing it to send the data including the aggregated message authentication code to the RSU. This scenario is referred to as "1 forwarding".

Scenario 3: Vehicle V has exited the RSU's communication range while sending data, requiring the data to be forwarded to vehicle V_1. However, vehicle V_1 also exits the RSU's communication range during forwarding, necessitating a further forward to vehicle V_2. Vehicle V_2 remains within the RSU's communication range and sends the data, including the re-aggregated message authentication code, to the RSU. This scenario is referred to as "2 forwarding".

Mohamed, Ahmed [46] proposed a new message passing and authentication protocol using an optimized version of the RSA protocol to reduce the total computation time of each forwarding node. In our performance analysis, we compare the proposed scheme with the work of Mohamed, Ahmed [46] in terms of processing time for no forwarding, 1 forwarding, and 2 forwarding. The analysis results are presented in Table 3.

The experimental results show that, as the number of forwarding steps increases, the processing time of the two schemes shows a linear growth trend. In the scenario of no forwarding, our scheme improves the authentication processing efficiency by an average of 24.7% per message. In the scenario of 1 forwarding and 2 forwarding, our scheme achieves an average efficiency improvement of 8.3% and 5.0% per message, respectively.

Table 3. Solution performance comparison.

Scenario	Mohamed, Ahmed [46]	Our Solution	Decrease
No forwarding	0.089 s	0.067 s	24.72%
1 forwarding	0.168 s	0.154 s	8.33%
2 forwarding	0.239 s	0.227 s	5.02%

In the no forwarding scenario, the aggregation of message authentication codes is not required, resulting in significant efficiency improvement due to the inherent characteristics of message authentication codes. In the scenarios involving 1 or 2 forwarding, the use of Diffie-Hellman key exchange protocol to establish a shared key introduces additional computational overhead, leading to a decrease in efficiency improvement. However, the proposed scheme still demonstrates superior overall performance.

Leveraging the cloud-edge-client collaborative architecture, cloud platform *C* performs synchronous decryption, authentication, and monitoring, improving both the authentication efficiency and security within the vehicle network. This makes the proposed scheme more practical and applicable in real-world IoV scenarios.

3.4. Traffic Response Strategy Simulation Experiment Under Vehicle Networking Authentication

Due to the complex and dynamic organizational structure of the IoV and the mobile nature of its nodes, accurately validating real vehicle experiments is challenging. Therefore, simulation software is utilized for experimental purposes [47–49]. This section presents a simulation experiment designed to evaluate the authentication process within an IoV scenario and assess the impact of message transmission on the traffic system improvements following an accident. Through these simulations, we aim to verify the practical application value of the proposed scheme and offer a novel solution for enhancing urban traffic conditions and improving traffic safety.

In this research, we simulate the impact of vehicle networking under varying connected vehicle rates, congestion levels, and networking scenarios in diverse traffic conditions, focusing on authentication and response strategies.

3.4.1. Simulation Experiment Design

The simulation experiments were conducted using OMNeT++6.0.3, Veins5.0.0 and SUMO1.19.0, as shown in Figure 8. The SUMO simulation was first employed to configure the road traffic environment and generate the traffic flow and vehicle motion models. Subsequently, OMNeT++ simulation was used to set up the vehicle network communication environment. Finally, the Veins platform was utilized to integrate SUMO and OMNeT++ and conduct simulation experiments.

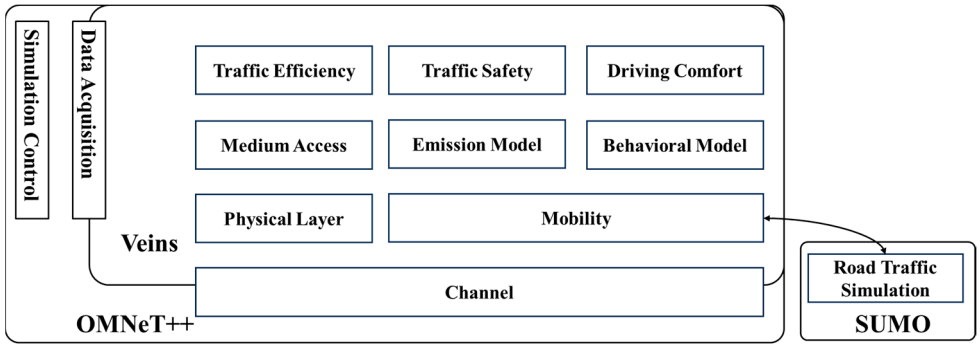


Figure 8. Joint simulation framework.

3.4.2. Simulation Results Analysis

(1) Traffic Parameter Analysis under Varying Connected Vehicle Penetration Rates

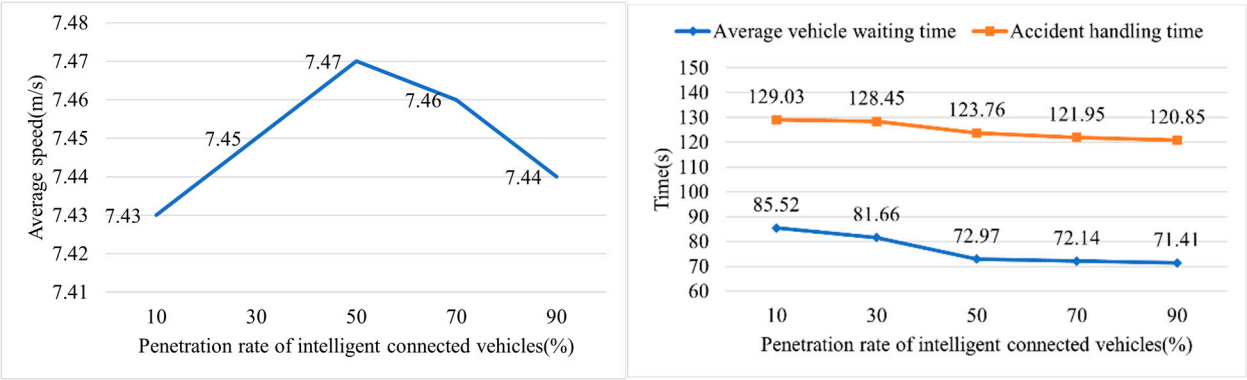
Intelligent connected vehicles have communication capabilities that allow them to receive and send critical information, such as accident warnings and traffic control instructions. In contrast, non-intelligent connected vehicles lack these functionalities. For the simulation, two main vehicle types were defined: vehicle-to-everything-equipped vehicles (V2X-equipped vehicles) and non-vehicle-to-everything-equipped vehicles (non-V2X-equipped vehicles). By simulating different levels of connected vehicle penetration, we aimed to evaluate the potential effectiveness of the IoV authentication based on the proposed cloud-edge-client collaborative architecture, focusing on its application to future transportation systems.

To control the penetration rate of intelligent connected vehicles, we adjusted the probability values assigned to V2X-equipped and non-V2X-equipped vehicles. The penetration rates were set to 10%, 30%, 50%, 70%, and 90%, as detailed in Table 4.

Table 4. V2X-equipped vehicles penetration rate configuration.

Probability Value	Penetration Rate of V2X-Equipped Vehicles
0.1/0.9	10%
0.3/0.7	30%
0.5/0.5	50%
0.7/0.3	70%
0.9/0.1	90%

To effectively evaluate the performance of traffic response strategies under different penetration rates of V2X-equipped vehicles, we calculated key traffic parameters, including average vehicle speed, average vehicle waiting time, and accident handling time for each penetration rate scenario. The results are shown in Figure 9.



(**a**) (**b**)

Figure 9. Traffic parameters under different penetration rates of connected vehicles. (**a**) average speed and (**b**) average vehicle waiting time and accident handling time.

Regarding the average vehicle speed parameter, the results indicate a clear trend that as the penetration rate of V2X-equipped vehicles increases, the average speed first increases, peaks at a 50% penetration rate, and then slightly decreases. The initial increase in speed may be attributed to the fact that non-V2X-equipped vehicles, lacking the ability to receive control speed limit commands, avoid unnecessary deceleration before reaching the accident site. As the penetration rate continues to increase, the slight decrease in speed suggests that a majority of V2X-equipped vehicles have responded to the speed limit control command, thereby reducing their driving speed.

Regarding average waiting time and the accident handling time, results show that both parameters decrease significantly as the penetration rate of non-V2X-equipped vehicles increases from 10% to 50%. However, as the penetration rate increases from 50% to 90%, the reductions in both waiting time and handling time become more gradual and eventually stabilize.

For all three parameters, the scenario with a 50% penetration rate of V2X-equipped vehicles appears to yield the best accident response outcomes under the IoV authentication. However, this result is inconsistent with real-world expectations. The discrepancy may be due to the simplified speed limit strategy used in the simulation and the performance differences between non-V2X-equipped vehicles in simulation versus those in real-world scenarios.

(2) Analysis of Traffic Parameters under Different Congestion Conditions

Examining different congestion scenarios allowed us to demonstrate the adaptability and efficiency of traffic response strategies during peak and off-peak hours under the proposed authentication system. This analysis facilitates the study of optimizing information transmission and accident response strategies across varying traffic densities. In the simulation, traffic flow parameters were configured to represent various traffic environments in the real world, ranging from low to high congestion. The definitions of low, moderate, and high congestion are provided in Table 5.

Table 5. Definition of different traffic congestion situations.

Congestion Level	Vehicle Flow (veh/h)	Average Distance Between Vehicles (m)
Low congestion	1500	40
Moderate congestion	3000	20
High congestion	4500	13

This paper sets up simulation experiments with and without authentication and response control and assesses their impact under different congestion conditions. The results of these simulations are illustrated in Figure 10.

(3) Traffic Parameter Analysis at Different Locations

The IoV environment exhibits diverse communication and traffic characteristics across various geographical locations, such as city centers, suburbs, and highways. These differences in road conditions, traffic flow, and accident processing times can significantly impact the effectiveness of IoV authentication and response strategies. Therefore, it is crucial to assess the performance of authentication and traffic accident response solutions in these varied traffic environments. This section focuses on three different road networks: Urban areas, suburbs, and highways, as illustrated in Figure 11. The specific attribute characteristics are shown in Table 6.

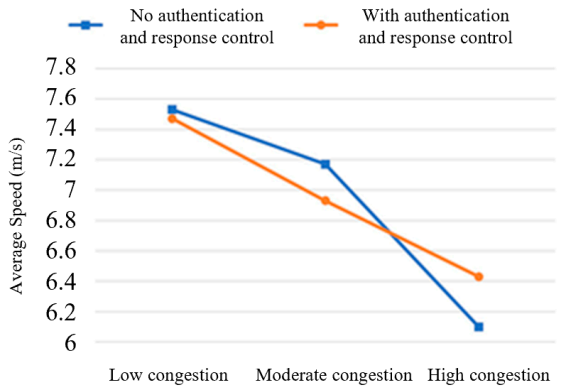
The simulation results at different locations reflect the different traffic characteristics of urban areas, suburbs and highway networks. The specific results are shown in Figure 12.

In the urban road network, the average speed of vehicles is 7.44 m/s, the average waiting time of vehicles is 411.43 s, and the accident handling time is 448.06 s. These data show that urban road networks face severe congestion and traffic problems, particularly during accidents. The low average speed and long waiting time are caused by factors such as high road network density, frequent intersections and traffic signal control. Future research could focus on improving the use of infrastructure, such as integrating intelligent traffic signal control systems to adjust signal duration based on real-time traffic conditions to reduce congestion.

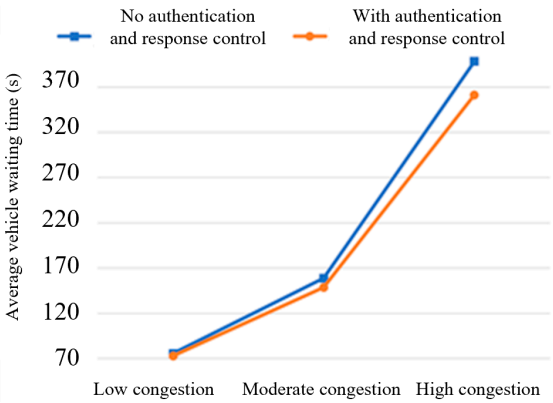
In contrast, the traffic conditions in suburban road networks are better than those in urban areas. The average speed is 12.35 m/s, the average waiting time is 212.75 s, and

the accident handling time is 262.24 s. It shows that due to the low traffic density, small traffic flow, and wide roads, the traffic flow and accident handling efficiency of suburban road networks in accidents are still high. However, the suburban road network is relatively simple and has less infrastructure, which may lead to traffic pressure concentrated on a few main roads. We can strengthen the information construction of suburban roads and use smart traffic management systems for real-time monitoring and control.

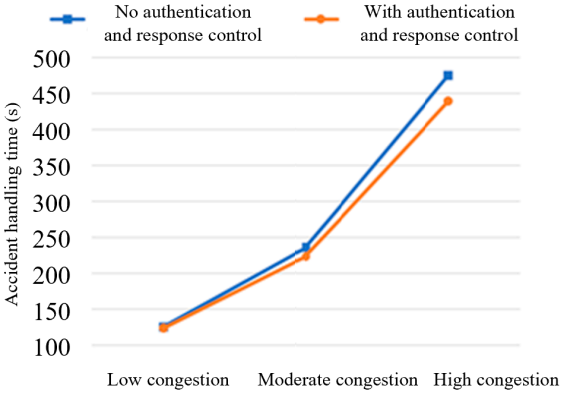
The highway network has the highest average vehicle speed, reaching 18.03 m/s, the average waiting time is only 1.28 s, and the accident handling time is 21.47 s. This shows that the traffic flow on the highway section is extremely high, the vehicle speed is fast, and the vehicle waiting time and accident handling time are very short. However, the high speed of the highway will also increase the risk and severity of accidents. We can strengthen the construction of smart highways, predict and warn possible accidents, reduce the accident rate and mitigate the consequences of accidents.



(**a**) Average speed.

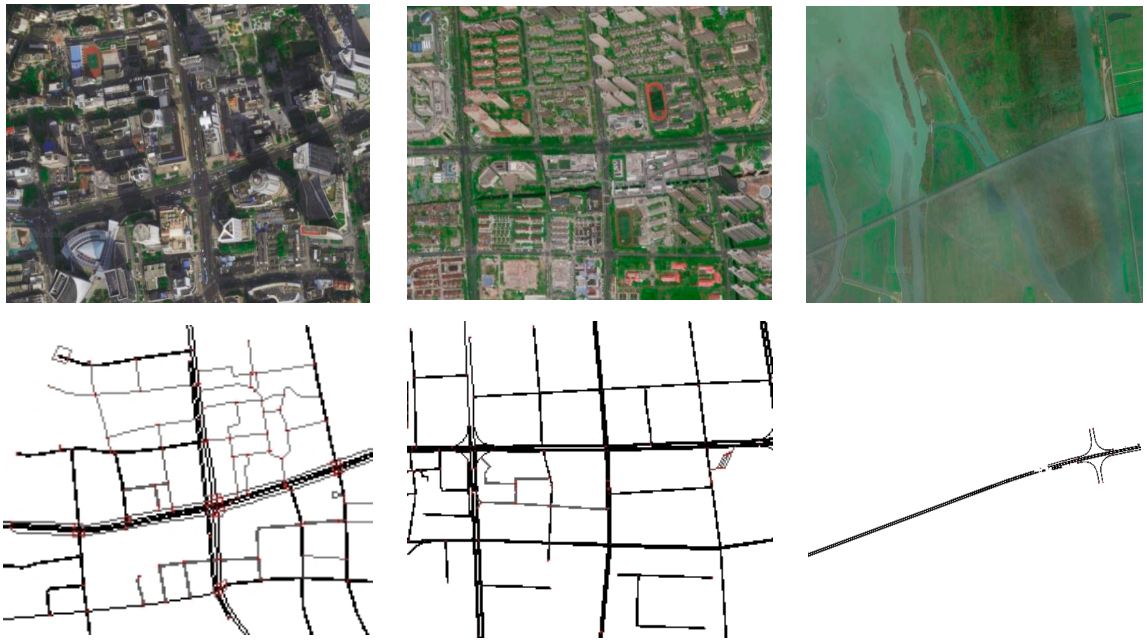


(**b**) Average vehicle waiting time.



(**c**) Accident handling time.

Figure 10. Traffic parameters under different congestion conditions.

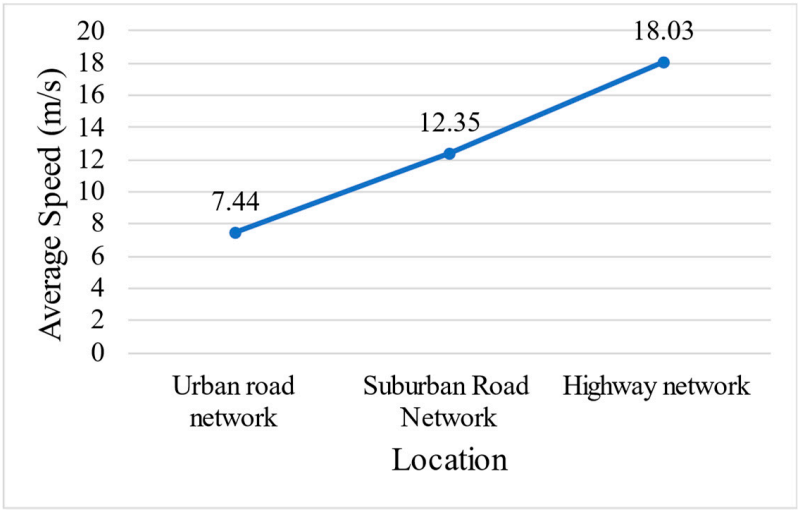


(**a**) Urban road network (**b**) Suburban Road Network (**c**) Highway network

Figure 11. Simulation of road networks at different locations.

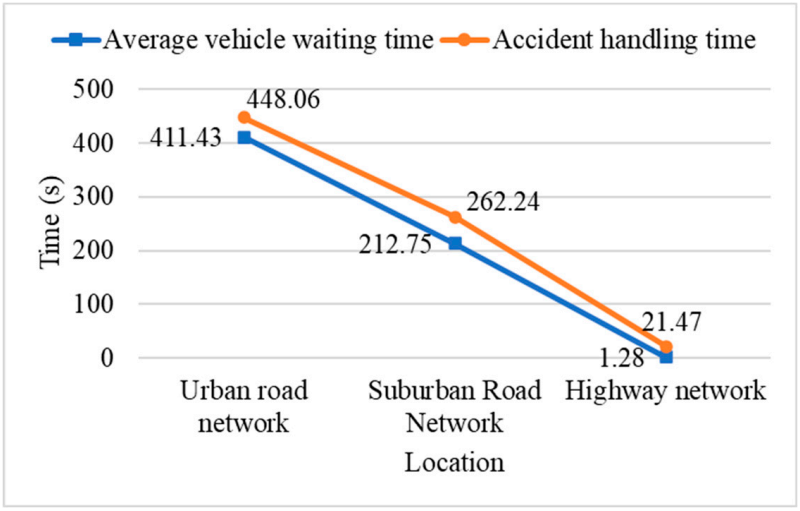
Table 6. Comparison of traffic attributes in different locations.

Attributes	Urban	Suburban	Highway
Traffic density	High	Medium	Low
Average vehicle speed	30 km/h	50 km/h	100 km/h
Traffic density	1200 veh/h	800 veh/h	600 veh/h
Vehicle traffic efficiency	Low	Medium	High
Communication infrastructure construction	High	Medium	Low



(**a**) Average speed

Figure 12. *Cont.*



(**b**) Average vehicle waiting time and Accident handling time

Figure 12. Traffic parameters at different locations.

4. Conclusions

This paper addresses IoV security by integrating network security's message authentication, proposing an adaptive traffic authentication strategy and a cloud-edge-client IoV authentication scheme. Additionally, it utilizes a joint simulation of traffic and network models to validate and analyze the authentication and traffic response strategies.

(1) The performance and characteristics of several key digital signature schemes in the context of vehicle network authentication have been analyzed and tested. Based on the standard elliptic curve ECDSA and Edwards curve EdDSA, and by integrating various parameters of vehicles in the IoV scenario, an adaptive traffic authentication strategy, ATAS, has been proposed. By assessing the dynamics of traffic flow, scoring the traffic state, evaluating time sensitivity, and constructing a comprehensive authentication strategy decision-making process, an authentication scheme has been developed that can automatically balance efficiency and security according to traffic volume. This scheme takes into account both the efficiency and security of message authentication in the IoV scenario. Under different numbers of vehicle authentications, ATAS effectively reduces the processing time. Especially in the case of a high number of vehicle authentications, the processing time decreases from 1.59 milliseconds to 1.17 milliseconds, demonstrating the significant role of ATAS in performance optimization.

(2) In response to the high overhead and security issues associated with multiple message forwarding in large-scale IoV application scenarios, this paper proposes a secure message transmission and authentication scheme based on a cloud-edge-client collaborative architecture. By utilizing the technology of aggregate message authentication codes to verify the authenticity and integrity of messages, communication overhead is reduced. Meanwhile, a cloud platform is set up as a 'cloud' end that supervises the broadcasting of RSU messages, the RSU is positioned as the 'edge' end in the architecture, and the vehicles are considered as the 'client' end within the architecture, ensuring the correctness of the transmission of authenticated messages. This scheme outperforms existing schemes in scenarios with no forwarding, 1 forwarding, and 2 forwarding, demonstrating higher efficiency and lower communication costs. Particularly in the scenario with no forwarding, the average authentication processing efficiency per message is improved by 24.7% when adopting this scheme.

(3) Utilizing the software SUMO, OMNeT++, and the Veins simulation platform, a joint simulation experimental environment for the vehicle network was established. The

interactions and authentication processes between vehicles, RSUs, and cloud platforms, as well as the impact of response strategies on traffic parameters after incidents, were simulated under different intelligent connected vehicle penetration rates, varying congestion conditions, and diverse location scenarios. This provides strong support for secure communication and efficient management in the vehicle network. For scenarios with different penetration rates of connected and autonomous vehicles, the accident response effect under Internet of Vehicles (IoV) authentication is optimal when the penetration rate reaches 50%. For scenarios with different congestion levels, particularly in highly congested scenarios, the average vehicle speed increases from 6.1 m/s to 6.43 m/s; the average vehicle waiting time decreases from 398.56 s to 361.38 s, representing an improvement of 9.3%; and the accident handling time drops from 475.26 s to 439.41 s, with an improvement of 7.54%. For scenarios in different locations, this paper explores the impacts of urban road networks, suburban road networks, and highway road networks on IoV authentication and response strategies.

Some of the shortcomings and areas in this research that can be further studied and improved are as follows:

(1) In the ATAS, this paper uses the percentage of detector occupancy by vehicles in the current and previous time intervals, the average vehicle speed, and the number of vehicles for assessment and decision-making. Such decision-making still has a certain degree of one-sidedness. In actual IoV scenarios, traffic characteristic parameters such as vehicle travel paths and speeds are more complex. Therefore, in future research, it should be considered to combine more parameters, such as vehicle travel paths and vehicle locations, or to integrate analysis with multi-source traffic big data from radar and video.

(2) In the security message transmission and authentication scheme based on the cloud-edge-client collaborative architecture, this paper utilizes cloud platform C to authenticate and decrypt the received messages synchronously and monitor the RSU to ensure the correctness and integrity of the RSU's broadcast messages. However, in real IoV scenarios, the cost is relatively high. Future research could consider using some slow-moving vehicles to replace the functions of the cloud platform or RSU, under the premise of ensuring safety, improving the efficiency of information transmission, reducing the operating costs of the vehicle network, and strengthening the practical recommendations.

(3) In the simulation experiments of traffic response strategies under vehicle network authentication, although different locations of road networks were selected, only one scenario was chosen for each of the three types of road networks. Road traffic conditions at diverse locations may vary significantly. Future research could consider enriching the simulation scenarios, such as conducting simulation experiments in diverse locations, different scales, and other scenarios, to assess the feasibility and guidance of the scheme.

(4) Regarding the conclusion that the optimal response is achieved at a 50% penetration rate of connected and autonomous vehicles, we will integrate multiple measures into the response strategy in future research, such as variable speed limit [50], ramp control [51] and emergency lane control [52].

(5) This paper does not explore the impacts of different types of OBUs. In future research, we will design optimized algorithms specifically for OBUs to ensure the compatibility of the proposed scheme with various types of OBUs.

(6) The current simulation is based on a small-scale scenario and does not fully consider the scalability challenges (e.g., the number of RSUs) in real-world deployments. In subsequent studies, we plan to explore optimized schemes through large-scale simulations.

Author Contributions: Conceptualization, Y.Z. (Yuan Zhang) and C.J.; methodology, Y.Z. (Yuan Zhang), Z.Z. and C.J.; validation, Z.Z., Y.Z. (Yuan Zhang) and W.H.; writing—original draft preparation, Y.Z. (Yuan Zhang), C.J. and T.T.; writing—review and editing, Z.Z., T.T. and K.A.; visual-

ization, Y.Z. (Yifei Zheng) and K.A. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported by the Youth Science Fund Project (Category A, No. T2525020), the Key Project (No. 52131203) and the Youth Program (No. 72301066) of the National Natural Science Foundation of China, the Fundamental Research Funds for the Central Universities, China (No. 2242024RCB0048), and the Wuxi Science and Technology Development Fund Project (No. K20231014).

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Shen, D.; Sui, S.; Chen, C.L.P. Event-Trigger Bipartite Consensus Secure Control for NMASs with Deception Attacks and Full-States Asymmetric Constraints. *Int. J. Fuzzy Syst.* **2025**. [CrossRef]
2. Xu, H.; Dong, D.; Yu, D.; Liu, Y.J. Predefined-Time Fuzzy Adaptive Control for Spacecraft Pose Tracking With Asymptotic Error. *IEEE Trans. Fuzzy Syst.* **2025**, *33*, 971–981. [CrossRef]
3. Zhang, K.; Zhang, H.; Dong, Y.; Wu, Y.; Chen, X. An ADMM-based parallel algorithm for solving traffic assignment problem with elastic demand. *Commun. Transp. Res.* **2023**, *3*, 100108. [CrossRef]
4. Cheng, Q.; Lin, Y.; Zhou, X.; Liu, Z. Analytical formulation for explaining the variations in traffic states: A fundamental diagram modeling perspective with stochastic parameters. *Eur. J. Oper. Res.* **2024**, *312*, 182–197. [CrossRef]
5. Zhang, Z.; Wei, Z.; Chen, Z.; Pei, M. A real-time collision risk assessment method at tunnel entrance based on safety field theory. *Multimodal Transp.* **2024**, *3*, 100139. [CrossRef]
6. Zhang, J.; Huang, D.; Liu, Z.; Zheng, Y.; Han, Y.; Liu, P.; Huang, W. A data-driven optimization-based approach for freeway traffic state estimation based on heterogeneous sensor data fusion. *Transp. Res. Part E Logist. Transp. Rev.* **2024**, *189*, 103656. [CrossRef]
7. Cheng, Q.; Dai, G.; Ru, B.; Liu, Z.; Ma, W.; Liu, H.; Gu, Z. Traffic Flow Outlier Detection for Smart Mobility Using Gaussian Process Regression Assisted Stochastic Differential Equations. *Transp. Res. Part E Logist. Transp. Rev.* **2025**, *193*, 103840. [CrossRef]
8. Huang, D.; Gu, Y.; Wang, S.; Liu, Z.; Zhang, W. A two-phase optimization model for the demand-responsive customized bus network design. *Transp. Res. Part C Emerg. Technol.* **2020**, *111*, 1–21. [CrossRef]
9. Huang, D.; Liu, Z.; Liu, P.; Chen, J. Optimal transit fare and service frequency of a nonlinear origin-destination based fare structure. *Transp. Res. Part E Logist. Transp. Rev.* **2016**, *96*, 1–19. [CrossRef]
10. Liu, Y.; Liu, Z.; Jia, R. DeepPF: A deep learning based architecture for metro passenger flow prediction. *Transp. Res. Part C Emerg. Technol.* **2019**, *101*, 18–34. [CrossRef]
11. Huang, D.; Zhang, J.; Liu, Z.; He, Y.; Liu, P. A novel ranking method based on semi-SPO for battery swapping allocation optimization in a hybrid electric transit system. *Transp. Res. Part E Logist. Transp. Rev.* **2024**, *188*, 103611. [CrossRef]
12. Sharma, S.; Kaushik, B. A survey on internet of vehicles: Applications, security issues & solutions. *Veh. Commun.* **2019**, *20*, 100182. [CrossRef]
13. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibañez, J.A. Internet of vehicles: Architecture, protocols, and security. *IEEE Internet Things J.* **2017**, *5*, 3701–3709. [CrossRef]
14. Huang, D.; Zhang, J.; Liu, Z. A robust coordinated charging scheduling approach for hybrid electric bus charging systems. *Transp. Res. Part D Transp. Environ.* **2023**, *125*, 103955. [CrossRef]
15. Liu, Z.; Chen, X.; Meng, Q.; Kim, I. Remote park-and-ride network equilibrium model and its applications. *Transp. Res. Part B Methodol.* **2018**, *117*, 37–62. [CrossRef]
16. Van Herrewege, A.; Singelee, D.; Verbauwhede, I. CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus. In Proceedings of the ECRYPT Workshop on Lightweight Cryptography, Louvain-la-Neuve, Belgium, 28–29 November 2011. ECRYPT.
17. Jo, H.J.; Kim, J.H.; Choi, H.-Y.; Choi, W.; Lee, D.H.; Lee, I. Mauth-can: Masquerade-attack-proof authentication for in-vehicle networks. *IEEE Trans. Veh. Technol.* **2019**, *69*, 2204–2218. [CrossRef]
18. Kang, K.D. A Practical and Lightweight Source Authentication Protocol Using One-Way Hash Chain in Can. Master's Thesis, Daegu Gyeongbuk Institute of Science and Technology, Daegu, Republic of Korea, 2017.
19. Kim, J.H.; Jo, H.J.; Lee, I. Model Checking Resiliency and Sustainability of In-Vehicle Network for Real-Time Authenticity. *Appl. Sci.* **2021**, *11*, 1068. [CrossRef]
20. Zhang, C.; Ho, P.-H.; Tapolcai, J. On batch verification with group testing for vehicular communications. *Wirel. Netw.* **2011**, *17*, 1851–1865. [CrossRef]

21. Huang, J.-L.; Yeh, L.-Y.; Chien, H.-Y. ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2010**, *60*, 248–262. [CrossRef]
22. Lee, C.-C.; Lai, Y.-M. Toward a secure batch verification with group testing for VANET. *Wirel. Netw.* **2013**, *19*, 1441–1449. [CrossRef]
23. Bayat, M.; Barmshoory, M.; Rahimi, M.; Aref, M.R. A secure authentication scheme for VANETs with batch verification. *Wirel. Netw.* **2015**, *21*, 1733–1743. [CrossRef]
24. Ali, I.; Chen, Y.; Pan, C.; Zhou, A. ECCHSC: Computationally and bandwidth efficient ECC-based hybrid signcryption protocol for secure heterogeneous vehicle-to-infrastructure communications. *IEEE Internet Things J.* **2021**, *9*, 4435–4450. [CrossRef]
25. Bagga, P.; Sutrala, A.K.; Das, A.K.; Vijayakumar, P. Blockchain-based batch authentication protocol for Internet of Vehicles. *J. Syst. Archit.* **2021**, *113*, 101877. [CrossRef]
26. Qureshi, K.N.; Sandila, M.A.S.; Javed, I.T.; Margaria, T.; Aslam, L. Authentication scheme for unmanned aerial vehicles based internet of vehicles networks. *Egypt. Inform. J.* **2022**, *23*, 83–93. [CrossRef]
27. Voorsluys, W.; Broberg, J.; Buyya, R. Introduction to cloud computing. In *Cloud Computing: Principles and Paradigms*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2011; pp. 1–41. [CrossRef]
28. Chen, X.; Liu, Z.; Zhang, K.; Wang, Z. A parallel computing approach to solve traffic assignment using path-based gradient projection algorithm. *Transp. Res. Part C Emerg. Technol.* **2020**, *120*, 102809. [CrossRef]
29. Kumar, M.; Sharma, S.C.; Goel, A.; Singh, S.P. A comprehensive survey for scheduling techniques in cloud computing. *J. Netw. Comput. Appl.* **2019**, *143*, 1–33. [CrossRef]
30. Cheng, Q.; Liu, Z.; Lu, J.; List, G.; Liu, P.; Zhou, X.S. Using frequency domain analysis to elucidate travel time reliability along congested freeway corridors. *Transp. Res. Part B Methodol.* **2024**, *184*, 102961. [CrossRef]
31. Cao, K.; Liu, Y.; Meng, G.; Sun, Q. An overview on edge computing research. *IEEE Access* **2020**, *8*, 85714–85728. [CrossRef]
32. Xiao, Y.; Jia, Y.; Liu, C.; Cheng, X.; Yu, J.; Lv, W. Edge computing security: State of the art and challenges. *Proc. IEEE* **2019**, *107*, 1608–1631. [CrossRef]
33. Garg, S.; Singh, A.; Kaur, K.; Aujla, G.S.; Batra, S.; Kumar, N.; Obaidat, M.S. Edge computing-based security framework for big data analytics in VANETs. *IEEE Network* **2019**, *33*, 72–81. [CrossRef]
34. Liu, C.; Wang, Z.; Liu, Z.; Huang, K. Multi-Agent reinforcement learning framework for addressing Demand-Supply imbalance of Shared Autonomous Electric Vehicle. *Transp. Res. Part E Logist. Transp. Rev.* **2025**, *197*, 104062. [CrossRef]
35. Huang, K.; Han, X.; An, K.; Liu, Z. Short-term and long-term impacts of shared autonomous vehicle choice behavior. *Transp. Res. Part D Transp. Environ.* **2024**, *132*, 104221. [CrossRef]
36. Huang, K.; Zhou, P.; Liu, Z.; Tang, T.; Zhang, H.; Jiang, W. The calculation and distribution of CAV carbon emissions on urban transportation systems: A comparative analysis of renewable and non-renewable energy sources. *Renew. Energy* **2024**, *230*, 120884. [CrossRef]
37. Cui, J.; Wei, L.; Zhang, J.; Xu, Y.; Zhong, H. An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 1621–1632. [CrossRef]
38. Cui, J.; Zhang, X.; Zhong, H.; Zhang, J.; Liu, L. Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 1654–1667. [CrossRef]
39. 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.* **2020**, *16*, 1810–1824. [CrossRef]
40. Ren, J.; He, Y.; Yu, G.; Li, G.Y. Joint communication and computation resource allocation for cloud-edge collaborative system. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakech, Morocco, 15–19 April 2019; IEEE: Piscataway, NJ, USA, 2019. [CrossRef]
41. Ding, C.; Zhou, A.; Liu, Y.; Chang, R.N.; Hsu, C.-H.; Wang, S. A cloud-edge collaboration framework for cognitive service. *IEEE Trans. Cloud Comput.* **2020**, *10*, 1489–1499. [CrossRef]
42. Zhang, H.; Chen, S.; Zou, P.; Xiong, G.; Zhao, H.; Zhang, Y. Research and application of industrial equipment management service system based on cloud-edge collaboration. In Proceedings of the 2019 Chinese Automation Congress (CAC), Hangzhou, China, 22–24 November 2019; IEEE: Piscataway, NJ, USA, 2019. [CrossRef]
43. Johnson, D.; Menezes, A.; Vanstone, S. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* **2001**, *1*, 36–63. [CrossRef]
44. Josefsson, S.; Liusvaara, I. *RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA)*; Internet Research Task Force (IRTF): Fremont, CA, USA, 2017. [CrossRef]
45. Boyko, V.; MacKenzie, P.; Patel, S. Provably secure password-authenticated key exchange using Diffie-Hellman. In Proceedings of the Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, 14–18 May 2000.
46. Mohamed, T.M.; Ahmed, I.Z.; Sadek, R.A. Efficient VANET safety message delivery and authenticity with privacy preservation. *PeerJ Comput. Sci.* **2021**, *7*, e519. [CrossRef]

47. Martinez, F.J.; Toh, C.K.; Cano, J.C.; Calafate, C.T.; Manzoni, P. A survey and comparative study of simulators for vehicular ad hoc networks (VANETs). *Wirel. Commun. Mob. Comput.* **2011**, *11*, 813–828. [CrossRef]
48. Xu, Z.; Zheng, N. Integrating connected autonomous shuttle buses as an alternative for public transport—A simulation-based study. *Multimodal Transp.* **2024**, *3*, 100133. [CrossRef]
49. Ferjani, A.; El Yaagoubi, A.; Boukachour, J.; Duvallet, C. An optimization-simulation approach for synchromodal freight transportation. *Multimodal Transp.* **2024**, *3*, 100151. [CrossRef]
50. Khondaker, B.; Kattan, L. Variable speed limit: An overview. *Transp. Lett.* **2015**, *7*, 264–278. [CrossRef]
51. Shaaban, K.; Khan, M.A.; Hamila, R. Literature review of advancements in adaptive ramp metering. *Procedia Comput. Sci.* **2016**, *83*, 203–211. [CrossRef]
52. Ma, J.; Hu, J.; Hale, D.K.; Bared, J. Dynamic hard shoulder running for traffic incident management. *Transp. Res. Rec.* **2016**, *2554*, 120–128. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.