*Computers, Materials & Continua*
DOI:10.32604/cmc.2021.012454
***Article***

Tech Science Press

# A Novel Anonymous Authentication Scheme Based on Edge Computing in Internet of Vehicles

**Xiaoliang Wang[1], Xinhui She[1], Liang Bai[2,*], Yang Qing[1] and Frank Jiang[3]**

[1]Hunan University of Science and Technology, Xiangtan, 411201, China
[2]Hunan University, Changsha, 410006, China
[3]School of Information Technology, Deakin University, Geelong, 3220, Australia
[*]Corresponding Author: Liang Bai. Email: a121512374@163.com

Received: 30 August 2020; Accepted: 19 November 2020

**Abstract:** The vehicular cloud computing is an emerging technology that changes vehicle communication and underlying traffic management applications. However, cloud computing has disadvantages such as high delay, low privacy and high communication cost, which can not meet the needs of real-time interactive information of Internet of vehicles. Ensuring security and privacy in Internet of Vehicles is also regarded as one of its most important challenges. Therefore, in order to ensure the user information security and improve the real-time of vehicle information interaction, this paper proposes an anonymous authentication scheme based on edge computing. In this scheme, the concept of edge computing is introduced into the Internet of vehicles, which makes full use of the redundant computing power and storage capacity of idle edge equipment. The edge vehicle nodes are determined by simple algorithm of defining distance and resources, and the improved RSA encryption algorithm is used to encrypt the user information. The improved RSA algorithm encrypts the user information by reencrypting the encryption parameters . Compared with the traditional RSA algorithm, it can resist more attacks, so it is used to ensure the security of user information. It can not only protect the privacy of vehicles, but also avoid anonymous abuse. Simulation results show that the proposed scheme has lower computational complexity and communication overhead than the traditional anonymous scheme.

**Keywords:** Cloud computing; anonymous authentication; edge computing; anonymity abuse

## 1 Introduction

In recent years, with the rapid development of scientific information technology, Internet of Things (IoT) technology has been widely used in various fields. The technical requirements for intelligent design in the IoT environment are growing [1]. With the in-depth study of relevant researchers, the IoT technology has been continuously improved and gradually matured [2], it brought a great change to the Internet of Vehicles [3]. In the Internet of Vehicles, the information communication and management handover between vehicles or between vehicles and roadside units keep growing, which leads to a large amount of traffic data transfer. Therefore, cloud computing [4] is introduced into the Internet of Vehicles. However, in cloud computing, the cloud center is far away from the terminal vehicle, which is easy to form a large network delay [5]. Meanwhile, because the open environment of Internet of Vehicles, it is more vulnerable to be attacked, so protecting the information security of vehicles focus on the top priority [6,7]. Technologies such as intrusion detection [8], data protection [9] and identity authentication are used to protect the security of vehicle information. However, most of the traditional anonymous authentication schemes [10–12] have complex computation and large communication overhead, which makes them difficult to meet the actual situation of high-speed traffic in the vehicle communication network. However, with the development of edge computing in recent years, edge computing can well meet the mobility [13], low latency [14] and trustworthiness of data [15]. Therefore, in order to ensure user information security and real-time information interaction between vehicles in the Internet of Vehicles, this paper proposes a novel anonymous authentication scheme based on edge computing. In this scheme, the concept of edge computing is introduced into the Internet of Vehicles, and the distance and computing power are used as the reference for selecting edge nodes, and vehicle information is encrypted by the improved RSA encryption algorithm to ensure the purpose of information privacy and security. This scheme can greatly reduce the burden of roadside units (RSU), effectively utilize the computing performance of the edge terminal, and thus improve the certification efficiency of the whole system.

The rest of this article is organized as follows: Section 2 describes the work, Section 3 describes the network architecture and system objectives, and Section 4 is the proposed solution. The security analysis is shown in Section 5. Experimental and performance results are described in Section 6. Finally, the article is summarized in Section 7.

## 2 Related Work

In recent years, with the continuous development of technology, the Internet of Things (IoT) has become more and more common. It has produced a lot of data, and needs to have the privilege of virtual resource utilization and storage capacity, so that the integration of the Internet of Things and cloud computing has become more and more important [16–19].

Hussain et al. [20] divided cloud-based Vehicular Ad-hoc Networks (VANET) into three main types: vehicle cloud (VC), cloud-based vehicle (VuC) and hybrid cloud (HC). VC uses vehicles to form a large cloud of services. It can be divided into two categories: static clouds and dynamic clouds. VuC allows ordinary nodes in VANET to connect to traditional clouds via RSUs. HC combines VC and VuC to get the best of both. Bhoi et al. [21] proposed an RVCloud routing protocol for VANET to effectively send data to the target vehicle using cloud computing technology. In this protocol, the vehicle beacon information is sent to the cloud storage via a RSU. Since vehicles have fewer storage and computing facilities, information on all vehicles moving in the city is maintained by clouds. After receiving the data, the RSU sends a request to the cloud to obtain the best destination RSU information, which uses the smallest packet forwarding delay to send the data to the destination.

According to a report released by Forbes [22] in 2015, cloud-based security spending is expected to increase by 42%. According to another study, IT security spending have increased to 79.1% by 2015, an increase of more than 10% per year. IDC showed in 2011 that 74.6% of corporate customers listed security as the main challenge. Therefore, protecting the safety of vehicle owner information in cloud computing is the top priority.

Zhang et al. [23] proposed two new types of lightweight networks, which can achieve higher recognition accuracy in traffic sign recognition while retaining fewer trainable parameters in the model. Li et al. [24] proposed a human pose estimation method based on knowledge transfer learning. In the estimation of human poses, first of all, by constructing a layered framework of "body–pose–attribute," an attribute-based human pose representation model is constructed. The layered architecture makes it possible to effectively infer the characteristics of new human poses even when the training samples are small. In order to ensure the security of on-board cloud computing (VCC), a new security method was designed by using software defined network (SDN) technology [25], which uses pseudonyms, key management and list cancellation to protect vehicles from the attack of malicious nodes, and provides authentication, confidentiality, integrity and availability. Melaouene et al. [26] proposed an intelligent RFID encryption and authentication scheme for filtering access applications in VANET environment. Huang et al. [27] utilized a hierarchically defined network of software to optimize network management, thereby implementing a software-defined Internet of Things (SEANET) for energy harvesting. Specifically, it is such an architecture that can achieve flexible energy scheduling and stronger communication by separating the data plane, energy plane, and control plane. In the proposed scheme, the ECC authentication model is used to protect HF or UHF tags and reader authentication. Considering the trust relationship between mobile nodes in Vehicular Ad-hoc Network (VANET) was uncertain in the transportation network-physical system (t-cps), Sun et al. [28] proposed a new t-cps VANET trust evaluation model based on member cloud. The proposed model addresses the trust uncertainty of fuzziness and randomness in the interaction between vehicles, and uses membership clouds to describe the uncertainty in the uniform format. In addition, a detailed description of the trustworthiness and an algorithm for computing cloud droplet and aggregate trust evaluation values is given. Nkenyereye et al. [29] used pseudonym technology to create anonymous certificates to ensure the privacy of the vehicle required by the service. In fact, their anonymous credentials are based on ID signatures. The authentication and revocation of anonymous credentials are accomplished by batch validation and anonymous revocation list respectively.

There have also been some progresses in privacy protection. Wang et al. [30] proposed an offline feature extraction model called LogEvent2vec, which takes log events as input to word2vec and extracts between log events and directly vectorized log events of relevance. The model reduces costs by avoiding multiple conversions, and the calculation time is 30 times shorter than word2vec. With the development of cloud computing and big data, the large amount of data collection makes the privacy of data more and more important. How to protect privacy has become an urgent problem. Wang et al. [31] designed a deep learning-based data collection and pre-processing scheme, using semi-supervised learning algorithm for data amplification and label guessing. It can perform data filtering at the edge layer and clear large amounts of similar and irrelevant data. If the edge device cannot process some complex data independently, it will send the processed reliable data to the cloud for further processing, thereby maximizing the protection of user privacy. The scheme protects the privacy of users by filtering the data.

Li et al. [32] proposed a VM packaging for page sharing, which takes into account constraints in multiple resources. The algorithm uses a heuristic algorithm that is better than the existing heuristics, which can reduce the VM required by up to 25% and reduce the memory page transfer by up to 40%. Yin et al. [33] discussed a better scheme for data aggregation. First, it maximizes the gain by considering common data pruning capabilities and aggregation, and then selects a data set with higher pruning power and smaller size, and transmits the aggregated data on subsequent nodes. The overall idea is to construct AT by connecting a group of aggregation operations with the largest aggregation gain. Ma et al. [34] proposed a caching placement strategy based on the cloud-based VANET architecture and the corresponding content retrieval process, which jointly considers the caching of vehicle layer and roadside unit layer. More specifically, the cache placement problem is modeled as an optimization problem that minimizes the average wait time while satisfying the QoE (Quality of Experience) requirements of the vehicle and is effectively solved by convex optimization and stimulus annealing (SA). Simulation results showed that the performance of this scheme is better than the existing caching schemes. Liu et al. [35] proposed a novel cloud auxiliary messages down link transmission scheme (CMDS), through the scheme, the security message first with the aid of cloud computing in the cloud server is passed to the suitable relevant road nodes (gateway is both cellular and VANET interface bus), and then by vehicle to vehicle (V2V) communication between adjacent vehicles. Wang et al. [36] proposed a safe and private-protected navigation scheme by using fog-based VANET's vehicle space crowdsourcing. Fog nodes are used to generate and release crowdsourcing tasks and collaborate to find the best route based on real-time traffic information collected by the vehicle in its coverage area. At the same time, crowdsourcing vehicles can be reasonably rewarded. While entering its coverage area, the query vehicle can continuously obtain navigation results from each fog node and follow the best route to the next fog node until it reaches its desired destination. Their solution meets the security and privacy requirements of authentication, confidentiality and conditional privacy protection. Several encryption primitives, including the Elgamal encryption algorithm, AES, random anonymous credentials, and group signatures, are used to achieve this goal.

Since the public key infrastructure (PKI) and identity-based authentication protocols cannot avoid the inefficiency of authentication that need to check the certificate revocation list (CRL), a local identity-based anonymous message authentication protocol for Van trucks was proposed in LIAP [37]. The certification authority is responsible for the long-term certification of each vehicle and roadside unit, and the RSU is responsible for the management and distribution of the master keys of local vehicles. These master keys can be used by vehicles to form pseudonyms to protect their privacy. In order to avoid inefficiency of authentication methods based on bilinear mapping and elliptic curve cryptography and to prevent illegal vehicle interference from attacking, HCPA-GKA [38] proposed a group key protocol mechanism based on China Remainder Theorem (CRT) for distributing group keys to authenticated vehicles. When a vehicle joins and leaves the group, the group key can be updated. These group keys can be used to generate anonymous messages and to be authenticated. Pournaghi et al. [39] proposed a relatively safer scheme called NECPA. NECPA stores the keys and the main parameters of the system in the tamper-proof device (TPD) of the roadside device. Because there is always a secure and fast communication link between TA and RSU, inserting TPD in RSUs is more effective than inserting TPD in vehicular OBUs. At the same time, the master secret key of TA is not stored in all OBUs in this scheme. Therefore, any attack to a single OBU will not threaten the whole network even if after attacked the whole vehicles need to be re-registered and change their secret keys.

## 3 Network Architecture and System Objectives

### *3.1 Network Architecture*

The scheme model proposed in this paper mainly includes three entities: (1) Trust Authority (TA), (2) Roadside Unit (RSU), and (3) vehicle equipped with On-board Unit (OBU). Among them, the vehicle participating in message authentication and calculation is called Edge Computing Vehicle (ECV). As shown in Fig. 1, TA acts as a registry for RSUs and vehicles, which is trusted by all entities and responsible for distributing secret keys, storing user core information, etc.

RSU acts as a gateway between the cloud center and the vehicle, and is also responsible for collecting information from the vehicle in its coverage area and passing it to the trusted agency TA through a secure channel (wired network); Vehicle OBU is divided into ordinary vehicle and ECV of edge computing vehicle. Ordinary vehicle acts as the data consumer, while edge computing vehicle and participating in the operation of data act as the data collector. Among them, Vehicle-to-Vehicle communication (V2V), Vehicle-to-RSU communication (V2R), Vehicle-to-Infrastructure communication (V2I) exist.

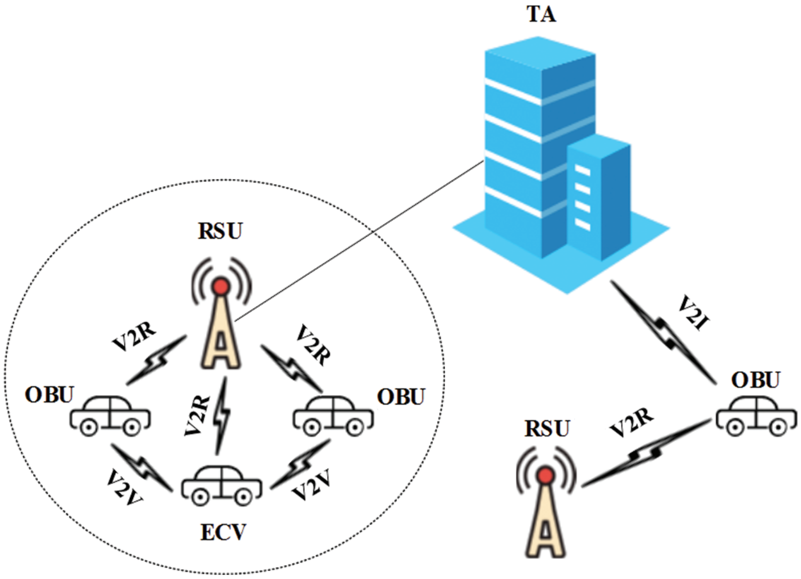

**Figure 1:** The basic network structure

### 3.2 System Objectives

While ensuring the information security of users, the real-time information interaction between vehicles in the Internet of Vehicles is guaranteed. The objectives of this paper are: (1) Message authentication and integrity, (2) Identity privacy protection, (3) Traceability, (4) Resistance to replay attack, (5) Real-time.

## 4 Proposed Scheme

In this section, we introduce a novel method of anonymous authentication of vehicle network based on edge computation. (1) System initialization phase, (2) vehicle pseudonym generation and encryption phase, (3) edge vehicle election phase, (4) vehicle authentication phase, (5) edge vehicle information gathering phase, (6) tracking illegal vehicle phase when anonymous misuse occurs.

### 4.1 Initialization Phase

We assume that communication is secure during the initialization phase of the system. At this phase, TA generates the necessary system parameters and passes them securely to the RSU and tamper-proof device. Refer to RSA algorithm [40], and the specific calculation steps after improvement are as follows:

1). TA randomly selects two different large prime numbers $p_1$ and $q_1$;
2). Calculate $n_1 = p_1 q_1$ and compute the Euler function $\Phi(n_1) = (p_1 - 1)(q_1 - 1)$;

3). Take an integer $e_1$, which satisfies $1 < e_1 < \Phi(n_1)$ and is mutually prime between $e_1$ and $\Phi(n_1)$;
4). Calculate $d_1 * e_1 = 1\, mod\, \Phi(n_1)$;
5). $\{n_1, e_1\}$ is the first layer public secret key, $\{n_1, d_1\}$ is the first layer private secret key, and $h$: $\{0, 1\}^* \rightarrow Z_q$;
6). Select the second layer of two large prime numbers $p_2$ and $q_2$, and calculate the $e_2$ and Euler function $\Phi(n_2) = (p_2 - 1)(q_2 - 1)$;
7). Like 3) and 4), compute $d_2 * e_2 = 1\, mod\, \Phi(n_2)$, and then use $\{n_2, e_2\}$ to encrypt $n_1$, let $n'_1 = n_1^{e_2}\,(mod\, n_2)$.

And then, we have obtained that the public key $(n_2, e_1, e_2)$ and private key $(n_2, d_1, d_2)$ of the double RSA algorithm.

### 4.2 Pseudonym, Encryption and Decrypt Phase

At this phase, user registration is used to participate in the calculation. First, the user submits the registration application. TA first preliminarily determines whether the user is a legitimate user (If not in the database blacklist). If so, multiple encryptions will be carried out to protect the user information. If not, denial of service.

#### 4.2.1 Generation of Pseudonym and Generation of Signature Information

The vehicle sends the *RID* of its real identity to TA for registration, TA checks whether the user exists. If it exists in the database, TA selects a random number $r_i$ (not public, stored in the tamper-proof agency), makes $VID_i^1 = r_i \cdot n_2$ and $VID_i^2 = RID \oplus h(r_i \cdot (n_2, e_1, e_2))$, then calculates the pseudonym $VID_i = \left\{VID_i^1, VID_i^2\right\}$.

#### 4.2.2 Encryption Process

When the user vehicle needs to send data, the information $M$, timestamp $t$ and pseudonym $VID_i$ are combined to form the information $M' = \{(M||t)\,||\,VID_i\}$, Then encrypt $(n_2, e_1)$ to $M'$ and get ciphertext $c = M'^{e_1}\,(mod\, n_1)$, and then encrypt $(n_2, e_2)$ to $n_1$ and get $n'_1$.

#### 4.2.3 Decryption Process

Decryption of $n'_1$ by $(n_2, d_2)$ to $n_1 = n_1'^{d_2}\,(mod\, n_2)$, then decrypt $c$ by $(n_2, d_1)$ to obtain $M' = c^{d_1}\,(mod\, n_1)$. Decryption of $n'_1$ by $(n_2, d_2)$ to $n_1 = n_1'^{d_2}\,(mod\, n_2)$, then decrypt $c$ by $(n_2, d_1)$ to obtain $M' = c^{d_1}\,(mod\, n_1)$.

### 4.3 Edge Vehicle Election Phase

The distance from the RSU and the computing resources contained in the vehicle unit determine whether the vehicle can be a marginal vehicle to participate in the calculation. Therefore, there are two measures.

#### *4.3.1 The Distance*

The distance from the vehicle to the RSU called $D(x)$. R represents the radius of the area covered by the RSU, and $dt(x)$ represents the distance between the vehicle and the RSU:

$$D(x) = \begin{cases} 1, & dt(x) < \dfrac{R}{2} \\ \dfrac{R - dt(x)}{\frac{R}{2}}, & \dfrac{R}{2} < dt(x) \leq R \\ 0, & R < dt(x) \end{cases} \tag{1}$$

#### *4.3.2 Compute Resources*

Every vehicle has computing resource function $AP(x)$, where $MVL(x)$ represents the vehicle's the amount of maximum computing resources and $UVL(x)$ represents the amount of remaining resources.

$$AP(x) = \frac{MVL(x) - UVL(x)}{MVL(x)} \tag{2}$$

Let the index be $Lk(x) = D(x) + AP(x)$. When the attribute index of each vehicle $Lk(x)$ is greater than or equal to 1, it means that the vehicle can participate in the calculation as the edge computing vehicle.

#### *4.3.3 Vehicle Certification Stage*

Any vehicle $VA_i$ sends a verification message to an unknown vehicle, that is, any number $\iota$, pseudonym $VID_i$ and timestamp $t_1$, computing $M_1' = (\iota \,||\, t_1) \,||\, VID_1$ to get a ciphertext $c_1 = M_1'^{e_1}\,(mod\,n_1)$, to the unknown vehicle. Then the unknown vehicle needs to decrypt the verification message using its private key to get $\iota$ and $t_1$. After that, the unknown vehicle needs to compute $M''_1 = ((\iota + 1) \,||\, t_1) \,||\, VID_2$ and $c_1' = M_1''^{e_1}\,(mod\,n_1)$, then send them back to $VA_i$. Subsequently, $VA_i$ verify $\iota$ and timestamp $t_1$. If successful, it determines that the user is a valid user.

#### *4.3.4 Illegal Vehicle Tracking Phase*

When vehicles use anonymous mechanisms to spread false traffic information or launch malicious wireless network attacks on nearby vehicles, we call it anonymous abuse of vehicles. When a malicious vehicle appears, the victim will send a tracking request to TA via the RSU. No matter where the encrypted message is, all of them contain the user's pseudonym $VID_i = \left\{VID_i^1, VID_i^2\right\}$, The vehicle in the attacked area only needs to pass the information sent by the attacker to the RSU calculation to obtain the user's real identity.

## 5 Security and Attack Analysis

### *5.1 Non-Forgeability of the Message Signature*

The formation of a pseudonym consists of: $VID_i^1 = r_i \cdot n_2$ and $VID_i^2 = RID \oplus h(r_i \cdot (n_2, e_1, e_2))$. Because the public key is known, if a malicious vehicle wants to forge a signature, the attacker needs to obtain his own private key to form a pseudonym. The private key is kept by tamper-proof authorities and cannot be easily obtained by an attacker. The attacker can only obtain its public key, but to forcefully crack the private key from the public key, the discrete logarithm problem needs to be solved. Moreover, this scheme adopts the double RSA encryption, which is more difficult to crack than the general algorithm, so the attacker can't get a feasible solution in polynomial time. Therefore, an attacker cannot forge the signature information of a legitimate vehicle.

### *5.2 The Anonymity of the Scheme*

Vehicles use pseudonyms when they interact with other vehicles in the Internet of Vehicle. According to the discrete logarithm problem, although other vehicles know $VID_i$ and $n_2$, there is no way to calculate $r_i$ that the user stored in the tamper-proof facility, and even the vehicle itself cannot disclose it. Therefore, for users other than the owner of the pseudonym, the real identity corresponding to the pseudonym cannot be obtained using the pseudonym name, public key, etc.

### *5.3 Resistance to Replay Attack*

In the process of information transmission, we add the concept of timestamp $t$. In order to ensure timeliness, the information receiver should check whether the information exceeds the deadline in the first time. Assume $t'$ is the message receiving time $t'$ and $\Delta t$ represents the estimated network time delay and transmission time. If $0 < t' - t < \Delta t$ is satisfied, the information is valid, otherwise the information is invalid and the service is denied.

### *5.4 Unlinkability*

The pseudonym generation of the vehicle is the $r_i$ generated by the tamper-proof mechanism, and a new pseudonym needs to be generated after every information transmission interaction. Therefore, it is impossible for the attacker to track the source according to the pseudonym, which ensures system unlinkability.

### *5.5 Traceability of the Scheme*

If a TA wants to track the real identity of the vehicle, it first finds the vehicle's pseudonym $VID_i$, and then calculates:

$$\begin{aligned}
&VID_i^2 \oplus h\left((n_2, e_1, e_2) \cdot VID_i^1 / n_2\right) \\
&\quad = RID_i \oplus h\left(r_i \cdot (n_2, e_1, e_2)\right) \oplus h\left((n_2, e_1, e_2) \cdot r_i \cdot n_2 \cdot \frac{1}{n_2}\right) \\
&\quad = RID_i \oplus h\left(r_i \cdot (n_2, e_1, e_2)\right) \oplus h\left(r_i \cdot (n_2, e_1, e_2)\right) \\
&\quad = RID_i
\end{aligned} \tag{3}$$

Then the TA can get user's real identity. So in the actual tracking process, other vehicles only need to provide the pseudonym used by attacker and a TA can find the malicious user's real identity without the participation of all vehicles. In addition, even if the malicious user has a new pseudonym, the TA can also find out its real identity through the previous pseudonym.

## 6 Performance Analyses and Simulation

### *6.1 Computational Cost Analysis*

Since Internet of Vehicles is a delay sensitive network, we take time cost as one of the comparative measures. For the sake of comparison, to facilitate subsequent comparison, $T_{mu}$ denotes the time cost of modular multiplication, $T_p$ denotes the time cost of pairing computation, and $T_h$ denotes the time cost of performing a hash operation.

Tab. 1 presents the computational overhead between LIAP [37], HCPA-GKA [38], NECPPA [39] and our scheme. We can easily find that because of the use of edge computing, our scheme greatly improves the utilization rate of resources and reduces the computing overhead.

**Table 1:** The cost of calculation

| Scheme | Total computational overhead |
|---|---|
| LIAP | $(n+1)\,T_{mu} + nT_h + T_p$ |
| HCPA-GKA | $nT_{mu} + (n+4)\,T_h$ |
| NECPPA | $nT_{mu} + nT_h + 3T_p$ |
| Our scheme | $\frac{2n}{3}T_{mu} + \frac{2n}{3}T_h + T_p$ |

### 6.2 *Performance Analysis*

Tab. 2 presents the property comparison between LIAP [37], HCPA-GKA [38], NECPPA [39] and our scheme. From Tab. 2, we can see that LIAP and HCPA-GKA scheme lack the ability of threshold tracking. NECPPA is time-consuming because it still uses the conventional cryptosystem for anonymous authentication. Generally speaking, our scheme is relatively balanced and comprehensive.

**Table 2:** The property comparison of different schemes

| Schemes comparisons | | | | |
|---|---|---|---|---|
| Property | LIAP | HCPA-GKA | NECPPA | Our scheme |
| Anonymity | √ | √ | √ | √ |
| Authentication | √ | √ | √ | √ |
| Conditional tracking | √ | √ | √ | √ |
| Threshold tracking | × | × | √ | √ |
| Timeliness | × | × | × | √ |

### 6.3 *Simulation*

This paper uses the open source Veins simulation framework to simulate the scheme. Veins is an open-source simulation system for vehicular communication network environments, which consists of event-based network simulators and road traffic simulation modules and also includes basic 802.11p/1609.4 modules and a simple application layer data generation framework. It uses OMNeT++ software as a network simulator and open source traffic simulation software SUMO as the generator for road traffic simulation scenarios. SUMO integrates important aspects such as vehicle trajectory, driving rules, driving habits, etc., and communicates with external programs such as Veins, OMNeT++, NS2 through the Traci expansion package.

In order to form a contrast, we stipulate that the speed of vehicles is 20 m/s. With the increase of average vehicle density, the network delay and packet loss rate of the four schemes are observed.

From Figs. 2 and 3, we can easily see that edge computing can greatly improve the response speed of the Internet of Vehicles, reduce the delay and packet loss rate, and ensure the information security of users under the double RSA algorithm in our scheme.

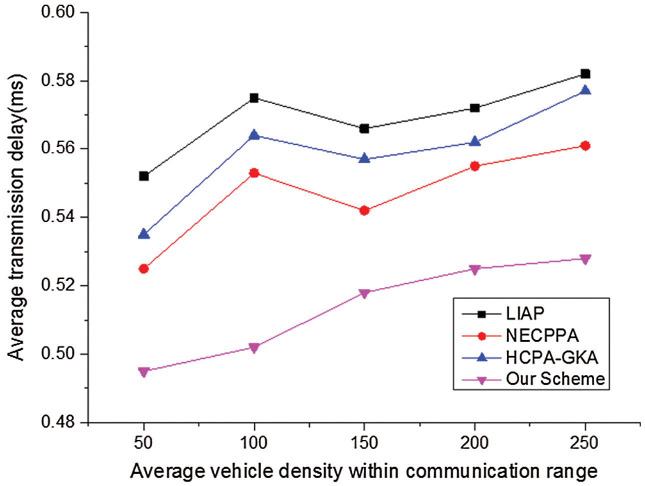

**Figure 2:** The transmission delay of four schemes at the speed of 20 m/s

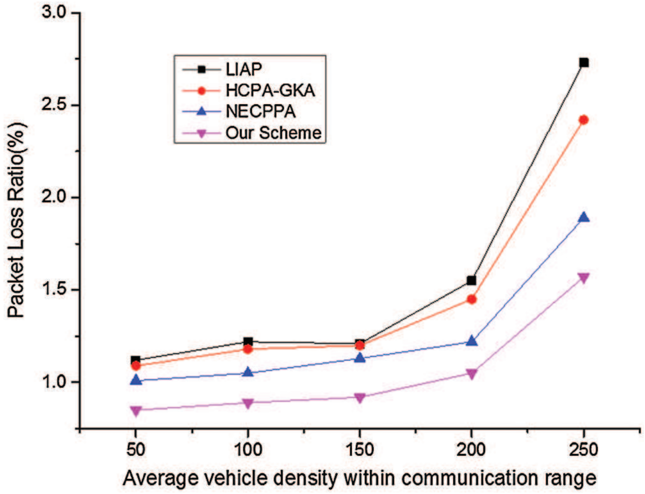

**Figure 3:** The packet loss ratio of four schemes at the speed of 20 m/s

## 7 Conclusion

The notion of cloud architecture is extensively applied in Internet of Vehicles. But for rush-hour traffic, cloud architecture has some disadvantages. In this paper, the edge computing, combined with the improved RSA algorithm, can solve the problem. First of all, the dual RSA algorithm greatly improves the information security of users, which is difficult to be cracked within the time limit. At the same time, the use of timestamp *t* prevents replay attack when information interaction. Secondly, edge computing design makes full use of the idle resources of surrounding vehicles by utilizing edge computing vehicle to serve other vehicles, which greatly improves the timeliness and reduces the transmission delay. Therefore, in general, the proposed scheme ensures low latency, low packet loss rate and high security. It is consistent with the use of Internet of Vehicles environment.

**Funding Statement:** The financial support provided from the Cooperative Education Fund of China Ministry of Education (201702113002, 201801193119), Hunan Natural Science Foundation (2018JJ2138) and Degree and Graduate Education Reform Project of Hunan Province (JG2018B096) are greatly appreciated by the authors.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] L. Wei, W. H. Huang, J. Long and K. Zhang, "Deep reinforcement learning for resource protection and real-time detection in IoT environment," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6392–6401, 2020.

[2] B. W. Wang, W. Kong and H. Guan, "Air quality forecasting based on gated recurrent long short term memory model in Internet of Things," *IEEE Access*, vol. 7, no. 1, pp. 69524–69534, 2019.

[3] H. Tang, A. Peng and D. Zhang, "SSD real-time illegal parking detection based on contextual information transmission," *Computers, Materials & Continua*, vol. 62, no. 1, pp. 293–307, 2020.

[4] M. Kumar, S. C. Sharma and A. Goel, "A comprehensive survey for scheduling techniques in cloud computing," *Journal of Network and Computer Applications*, vol. 143, pp. 1–33, 2019.

[5] T. R. Sheltami, E. Q. Shahra and E. M. Shakshuki, "Fog computing: Data streaming services for mobile end-users," *Procedia Computer Science*, vol. 134, pp. 289–296, 2018.

[6] N. Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," *Computers & Electrical Engineering*, vol. 71, pp. 28–42, 2018.

[7] X. Wang, P. Zeng, N. Patterson and F. Jiang, "An improved authentication scheme for Internet of vehicles based on blockchain technology," *IEEE Access*, vol. 7, pp. 45061–45072, 2019.

[8] L. Wei, K. Q. Li, J. Long, X. Y. Kui and Y. Zomaya, "An industrial network intrusion detection algorithm based on multifeature data clustering optimization model," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2063–2071, 2019.

[9] L. Wei, K. Q. Li, J. Long and X. Y. Kui, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6543–6552, 2020.

[10] Y. Zhou, X. Long and L. Chen, "Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs," *Journal of Information Security and Applications*, vol. 47, no. 2, pp. 295–301, 2019.

[11] H. Wang and Y. Zhang, "On the security of an anonymous batch authenticated and key agreement scheme for value-added services in VANETs," *Procedia Engineering*, vol. 29, pp. 1735–1739, 2012.

[12] X. Wang, J. M. Jiang and S. J. Zhao, "A fair blind signature scheme to revoke malicious vehicles in VANETs," *Computers, Materials & Continua*, vol. 58, no. 1, pp. 249–262, 2019.

[13] H. Lee, "Framework and development of fault detection classification using IoT device and cloud environment," *Journal of Manufacturing Systems*, vol. 43, pp. 257–270, 2017.

[14] T. Wang, L. Qiu, A. K. Sangaiah and A. Liu, "Edge-computing-based trustworthy data collection model in the Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4218–4227, 2020.

[15] W. Li, Z. Chen, X. Gao and W. Liu, "Multimodel framework for indoor localization under mobile edge computing environment," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4844–4853, 2018.

[16] J. Wang, W. Wu, Z. Liao and A. K. Sangaiah, “An energy-efficient off-loading scheme for low latency in collaborative edge computing,” *IEEE Access*, vol. 7, pp. 149182–149190, 2019.

[17] C. Stergiou, K. E. Psannis and B. G. Kim, “Secure integration of IoT and cloud computing,” *Future Generation Computer Systems*, vol. 78, pp. 964–975, 2018.

[18] P. Verma and S. K. Sood, “Cloud-centric IoT based disease diagnosis healthcare framework,” *Journal of Parallel and Distributed Computing*, vol. 116, pp. 27–38, 2018.

[19] T. C. Hsu, H. Yang and Y. C. Chung, “A Creative IoT agriculture platform for cloud fog computing,” *Sustainable Computing: Informatics and Systems*, vol. 100285, 100285, 2018.

[20] R. Hussain, J. Son and H. Eun, “Rethinking vehicular communications: Merging VANET with cloud computing,” in *4th IEEE Int. Conf. on Cloud Computing Technology and Science Proc.*, Taipei, pp. 606–609, 2012.

[21] S. K. Bhoi and P. M. Khilar, “RVCloud: A routing protocol for vehicular ad hoc network in city environment using cloud computing,” *Wireless Networks*, vol. 22, no. 4, pp. 1329–1341, 2016.

[22] G. Ramachandra, M. Iftikhar and F. A. Khan, “A comprehensive survey on security in cloud computing,” *Procedia Computer Science*, vol. 110, pp. 465–472, 2017.

[23] J. Zhang, W. Wang, C. Lu and J. Wang, “Lightweight deep network for traffic sign classification,” *Annals of Telecommunications*, vol. 75, no. 7–8, pp. 1–11, 2019.

[24] F. Li, S. R. Zhou, J. M. Zhang, D. Y. Zhang and L. Y. Xiang, “Attribute-based knowledge transfer learning for human pose estimation,” *Neurocomputing*, vol. 116, pp. 301–310, 2013.

[25] M. Bousselham and A. Abdellaoui, “Security against malicious node in the vehicular cloud computing using a software-defined networking architecture,” in *2017 Int. Conf. on Soft Computing and Its Engineering Applications*, IEEE, Changa, India, pp. 1–5, 2017.

[26] N. Melaouene and C. Elmakfalji, “A cloud-based RFID for VANET access filtering,” in *3rd Int. Conf. of Cloud Computing Technologies and Applications*, Rabat, Morocco, pp. 1–6, 2017.

[27] X. Huang, R. Yu, J. Kang and Z. Xia, “Software defined networking for energy harvesting Internet of Things,” *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1389–1399, 2018.

[28] D. Sun, H. Zhao and S. Cheng, “A novel membership cloud model-based trust evaluation model for vehicular ad hoc network of T-CPS,” *Security and Communication Networks*, vol. 9, no. 18, pp. 5710–5723, 2016.

[29] L. Nkenyereye, Y. Park and K. H. Rhee, “Secure vehicle traffic data dissemination and analysis protocol in vehicular cloud computing,” *Journal of Supercomputing*, vol. 74, no. 3, pp. 1024–1044, 2018.

[30] J. Wang, Y. Tang, S. He, C. Zhao, P. K. Sharma *et al.,* “LogEvent2vec: LogEvent-to-vector based anomaly detection for large-scale logs in Internet of Things,” *Sensors*, vol. 20, no. 9, pp. 2451, 2020.

[31] T. Wang, Z. Cao, S. Wang, J. Wang and L. Qi, “Privacy-enhanced data collection based on deep learning for Internet of vehicles,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6663–6672, 2019.

[32] H. Li, W. Li, S. Zhang, H. Wang, Y. Pan *et al.,* “Page-sharing-based virtual machine packing with multi-resource constraints to reduce network traffic in migration for clouds,” *Future Generation Computer Systems*, vol. 96, pp. 462–471, 2019.

[33] B. Yin and X. Wei, “Communication-efficient data aggregation tree construction for complex queries in IoT applications,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3352–3363, 2018.

[34] J. Ma, J. Wang and G. Liu, “Low latency caching placement policy for cloud-based vanet with both vehicle caches and RSU caches,” in *2017 IEEE Globecom Workshops*, IEEE, Singapore, pp. 1–6, 2017.

[35] B. Liu, D. Jia and J. Wang, “Cloud-assisted safety message dissemination in VANET-cellular heterogeneous wireless network,” *IEEE Systems Journal*, vol. 11, no. 1, pp. 128–139, 2015.

[36] L. Wang, G. Liu and L. Sun, “A secure and privacy-preserving navigation scheme using spatial crowdsourcing in fog-based vanets,” *Sensors*, vol. 17, no. 4, pp. 668, 2017.

[37] S. Wang and N. Yao, “LIAP: A local identity-based anonymous message authentication protocol in VANETs,” *Computer Communications*, vol. 112, pp. 154–164, 2017.

[38] J. Cui, X. Tao and J. Zhang, "HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs," *Vehicular Communications*, vol. 14, pp. 15–25, 2018.

[39] S. M. Pournaghi, B. Zahednejad and M. Bayat, "NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET," *Computer Networks*, vol. 134, pp. 78–92, 2018.

[40] M. Thangavel, P. Varalakshmi and M. Murrali, "An enhanced and secured RSA key generation scheme (ESRKGS)," *Journal of Information Security and Applications*, vol. 20, pp. 3–10, 2015.