Reliable and Efficient Content Sharing for 5G-Enabled Vehicular Networks

Jie Cui, Jiayi Chen, Hong Zhong, Jing Zhang, Lu Liu

***Abstract*—Conditional privacy preservation and message authentication serve as the primary research issues in terms of security in vehicular networks. With the arrival of 5G era, the downloading speed of network services and the message transmission speed have significantly improved. Consequently, the content exchanged by users in vehicular networks is not limited to traffic information, and vehicles moving at high speeds can share a wide variety of contents. However, sharing content reliably and efficiently remains challenging owing to the fast-moving character of vehicles. To solve this problem, we propose a reliable and efficient content sharing scheme in 5G-enabled vehicular networks. The vehicles with content downloading requests quickly filter the adjacent vehicles to choose capable and suitable proxy vehicles and request them for content services. Thus, the purpose of obtaining a good hit ratio, saving network traffic, reducing time delay, and easing congestion during peak hours can be achieved. The security analysis indicates that the proposed scheme meets the security requirements of vehicular networks. Our cryptographic operations are based on the elliptic curve, and finally, the proposed scheme also displays favorable performance compared to other related schemes.**

***Index Terms*—Message authentication, content sharing, elliptic curve, vehicular networks, privacy preservation.**

I. Introduction

THE intelligent transportation systems (ITS) aim to provide vehicles and pedestrians with safer, smarter and more efficient comprehensive services. The vehicular network is an important part of the ITS. With the advent of 5G era, each vehicle connected to the vehicular network is considered to be equipped with a state-of-the-art wireless communication device for vehicle-to-everything (V2X) communication [1], [2], [3]. In terms of latest technology, V2X refers to the exchange of information between a vehicle and the outside world. Because the communication is wireless, the messages sent by vehicles might be tampered with if malicious attackers exist. The message should be verified by the recipient to determine if it is trustworthy [4].

Drivers in vehicular networks can obtain the moving state of adjacent vehicles and road situations, such as speed, direction and emergencies. Therefore, they can utilize the advance response and the processing time for contingency to ensure improved transportation security. Through vehicular networks, information gathering, processing, computing and transmission become feasible and convenient, which are important for promoting ITS.

After travel needs are met, users will also wish to obtain a variety of on-board services. For example, when a user arrives in a new area, he wants to gain maps and smart city scenarios probably [5]. The acquisition of such content, the corresponding time and the hit ratio are also worthy of public attention.

Nowadays, the number of urban vehicles is rapidly growing, and users' demands are diversifying. Therefore, the vehicular ad hoc networks (VANETs) under the traditional 4G networks are unable to meet the requirements of high-speed transmission and low delay for current application environment [6], [7]. The 5G mobile network has the characteristics of wide coverage and high bandwidth. It brings many opportunities and challenges to vehicular networks [8]. According to the data, under 5G wireless networks, the data transmission rate can reach 20Gb/s during the peak period, and the average data transmission rate is over 100Mb/s [9]. The supported network capacity is 1000 times that of the existing networks, and it can provide a more stable connection [10].

A wide variety of downloading tasks can be requested by many vehicles in the heartland of some bustling cities during peak time [11]. The overloads and the congests of networks come subsequently, leading to the probable occurrence of message latency, request neglect and packet loss. In 5G-enabled vehicular networks, caching mobile content to the edge of network effectively alleviates these problems and meets the traffic demands during the peak period with a lower time delay [12].

Based on the 80/20 rule, we know that 80% of users might take only 20% of the content [13]. In the vehicular networks with a large number of users, a small amount of content is likely to be required by most of users. Assuming a scenario wherein a vehicle (V_i) makes a downloading request for content $R1$ (falls within category A). There is a piece of content $R1$ (or a piece of another content belongs to category A as well) in the content storage block of a passing vehicle which named V_j. Obviously, the goal will be achieved quickly if V_i directly requests to V_j for $R1$ instead of asking the content server (CS) for $R1$ via a transceiver. This not only saves network traffic but also avoids repeating content requests to the CS. That's what motivates us.

We introduce the message authentication mechanism into the process of content sharing. Further, we propose a method for sharing content reliably and efficiently between vehicles. In the meanwhile, the characteristics of moving vehicles and

J. Cui, J. Chen, H. Zhong and J. Zhang are with the Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, School of Computer Science and Technology, Anhui University, Hefei 230039, China, the Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, Hefei 230039, China, and the Institute of Physical Science and Information Technology, Anhui University, Hefei 230039, China (e-mail: zhongh@ahu.edu.cn).

L. Liu is with the School of Informatics, University of Leicester, LE1 7RH, UK (email: l.liu@leicester.ac.uk).

the objective of saving network overhead are also taken into account.

Our scheme is design for content sharing in 5G-enabled vehicular networks. The roadside units (RSUs) are usually required for authentication schemes in traditional VANETs [4], [14]. RSUs are responsible for computing and storage which will introduce security risks and the increase of transmission overhead. Deploying RSUs in large-scale vehicular networks is also costly. These authentication schemes under the traditional VANETs are difficult to apply to the 5G-enabled vehicular networks. There is no need for RSUs in the content sharing process, and the 5G base station (5G-BS) is not involved in the computation. Therefore, our scheme is secure and efficient. Compared with traditional VANETs using IEEE 802.11p standard, 5G could support large-scale mobile vehicular communications with lower time delay better [15], [16].

A. Our Contributions

Our main contributions are summarized as following :

1) The proposed scheme achieves the fast forwarding of content between vehicles based on personal preferences without exposing the details of the content. Vehicles have the characteristics of high mobility, and there is a large probability of opportunistic communication [12]. The content forwarding is carried out between the two vehicles with high data similarity. This process is fast and convenient, and it also solves the problems of network congestion and time delay.
2) A lightweight authentication scheme is proposed for 5G-enabled vehicular networks. The forwarding of content and the transmitting of requests are done by 5G-BS without secure computing.

B. Organization of This Paper

The remainder of the paper is organized as follows. Section II introduces the related work. Section III provides the preliminaries. The scheme is described in detail in Section IV. Then, in Section V, we prove and analyze the security aspect. Section VI gives the time consumption of the proposed scheme. Finally, we summarize our work and look forward to the future work in Section VII.

II. Related Work

The vehicular network is always a hot topic, especially in recent years. The security issues are well worth studying [17], [18]. A great deal of authentication schemes based vehicular networks have been proposed in order to achieve the security and privacy during wireless communication. In 2007, with the purpose of completing the message integrity check, Raya and Hubaux [19] came up with a method to make the real identities of users invisible by using anonymous certificates. This category of papers which based on public key infrastructure (PKI) adopted digital signatures to construct the authentication schemes [19], [20], [21]. PKI-based scheme is a favorable choice since information in vehicular networks that has not yet been identified as trustworthy is subject to be authenticated [4]. Nevertheless, its shortcomings are also evident [17]. Each vehicle carries a great deal of certificates to reach anonymity [4]. Hence, vehicles have to explore a lot of space to store public/private key pairs. Furthermore, the trusted authority (TA) also needs to store the anonymous certificates of all registered vehicles, high storage costs come with it especially when the number of vehicles is rising rapidly. Searching for the real identities of malicious vehicles in a vast database can also be exhausting [1].

Some group signature-based authentication schemes [22], [23] were proposed to solve the certificate management problem [24]. Each vehicle stores the same public key and a unique private key. It takes a lot of effort to maintain the vehicle revocation list, and the group signature is longer than the common signature in length [1].

In order to settle the problem of the costly verification process of group signature, some researchers proposed identity-based batch authentication schemes [25], [26]. It is obvious that batch authentication of messages is faster than individual authentication because the verification delay is reduced. Vehicles use fake identities to exchange information without revealing their real identities. However, identity-based authentication schemes are not appropriate when the number of vehicles is particularly large [4].

As infrastructure, RSUs sometimes serve as auxiliaries to complete part of the authentication work [27] because the computing power of mobile vehicles is limited [4]. Liu et al. [27] proposed a proxy-based distributed authentication scheme to reduce the computation overhead of RSUs. Proxy vehicles are applied to verify multiple messages simultaneously. The computation overhead of RSUs can also be shared by the proxy vehicles.

With the development of modern vehicular networks, the information circulating in networks is not limited to the traffic information. Content distribution [28] based on vehicular networks has been widely studied and discussed. The opportunistic resource exchange algorithm in vehicular ad hoc networks [29], the vehicular cooperative media access control (VC-MAC) for gateway-downloading scenarios [30] and the network coding method [31] are several approaches used for content distribution in vehicular networks.

A particular and convenient service named popular content distribution (PCD) [32] was presented in 2013. The multimedia content is transmitted from RSUs to the on board units (OBUs) equipped on vehicles. First, a popular file was downloaded by the RSU. In order to enable vehicles to copy the full content of the RSU, a cooperative approach was proposed [32]. Moreover, many papers focused on finding the best way to distribute content. Xing et al. [33] proposed a maximizing problem based utility for finding the best delivery strategy and choosing the best path for multimedia data propagation. A vehicle-to-vehicle (V2V) caching strategy upon content-centric network (CCN) was designed [34], which taken into account the requirements of different types of applications and the characteristics of vehicles. Routing protocols are also options to provide better services to users in VANETs [35]. Research based on intelligent vehicles also aims to make

vehicular networks more efficient and seure [36].

For the better performance, one problem of these papers is that they all assume that user-related data is available without paying attention to users' privacy. However, this is unrealistic in practical vehicular networks. A security incentive model was also designed to achieve reliable sharing in vehicular networks [37]. Obviously, the complex collaborative downloading process caused communication delay to some extent.

III. Preliminaries

In this section, we introduce some related knowledge and several constituent entities of the application environment.

A. Related Knowledge

We adopt a simple method with a certain degree of accuracy to measure the similarity between two sets of data. This method is called Euclidean distance. In mathematics, it means the common straight-line distance between two points in a space and has been used extensively in many researches [38], [39]. The spatial distance between two points is the difference between them.

Even to one user, different categories of contents have different degrees of importance at different time, and it changes dynamically over time. Users are significantly more interest in map information than in others during short trips. When users are on their way home from work, they may would like to access content like music to have a relax. Besides, considering that different users have different hobbies, weighted Euclidean distance is a good way to show the difference in users' evaluation of several types of contents [40].

B. Attack Model

Generally, there are two types of attackers: external attackers and internal attackers. External attackers are more powerful than vehicles but have limited computational power. They do not exist in vehicular networks, so they cannot decrypt messages and they can only get information from messages transmitted on open channels. Usually, external attackers need to join forces with each other to attack the entire system. Internal attackers are legitimate but malicious vehicles. They are legitimate in the system which have access to confidential information shared within the system. So they are also highly destructive.

Here we show some of the methods used by attackers in the vehicular networks. An attacker can (i) link multiple messages to track identity, (ii) tamper with messages, (iii) replay sent messages, (iv) forge messages to impersonate vehicles, or (v) guess passwords. These attacks may be carried out by the attackers alone or in collusion. The scheme we will describe in detail can provide anonymity to vehicles while resisting these attacks.

C. System Model

As illustrated in Fig. 1, there are four entities in the application environment : trusted authority (TA), content server (CS), 5G base station (5G-BS) and vehicle (V). We describe

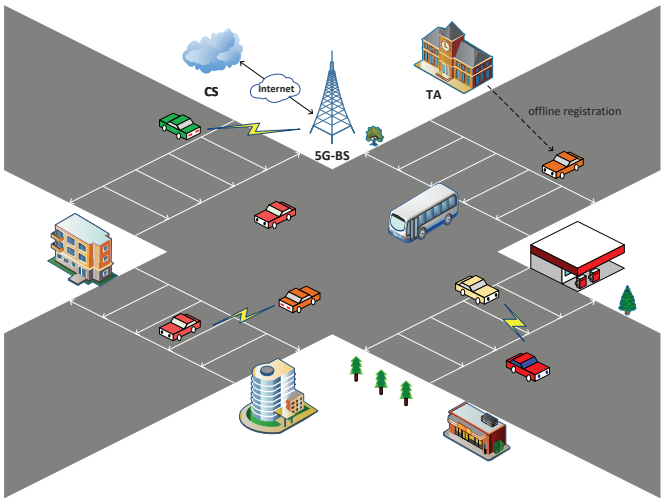


Fig. 1. System model

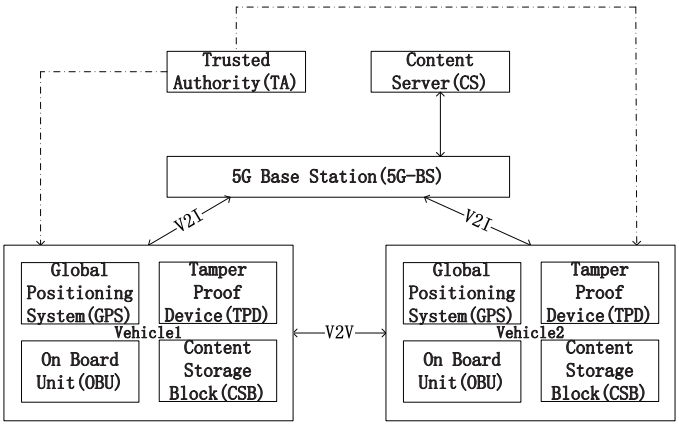


Fig. 2. Abstract network model

the functions of these entities. The abstract system model diagram is shown in Fig. 2.

1) Trusted authority (TA) : TA has enough computing power and storage capacity. In addition, there are a number of redundant for TAs to prevent bottlenecks and single points of failure [14]. In real-world application environment, the role of TA is usually played by a trusted authoritative government agency, such as the traffic administration etc. TA generates system parameters such as the system private key, defines two global parameters N, k. When a vehicle leaves the factory, TA registers it and records some basic information of it, generates the real identity RID_i and password PW_i for each vehicle, and preloads $\{RID_i, PW_i, s_{TA}\}$ into the tamper proof device (TPD) of the vehicle for legitimate user.
2) Content server (CS) : CS has powerful storage capacity which provides content services to all users. A large amount of contents are stored, including instant video, map, music, intelligent scene etc. All the contents that circulating in networks come from the CS. Specifically, CS is usually a cloud sever.
3) 5G base station (5G-BS) : 5G-BS works as a transceiver

with super-fast speed and wide coverage in vehicular networks, aims at relaying content between vehicles and forwarding vehicular requests to the CS.

4) Vehicle (V) : A terminal node in networks which enjoys all kinds of services. It refers to a vehicle equipped with the latest wireless communications equipment. A vehicle includes global positioning system (GPS), on board unit (OBU), tamper proof device (TPD), content storage block (CSB) and some other relevant modules. OBU does computation works for cryptographic operations. TPD stores secret information about the vehicle. GPS is used to determine the distance from other vehicles. The contents of vehicle are kept in the CSBs. An example distribution of CSBs is shown in Fig. 3.

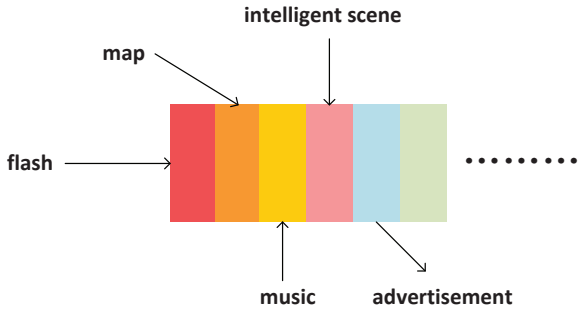


Fig. 3. Distribution of CSBs

D. Notations and Assumptions

In this subsection, we define the notations used in our scheme and describe the assumptions that the system should satisfy.

- **Notations**

The main notations and their definitions are shown in TABLE I.

- **Assumptions**

1) The TA is fully trusted by all entities and users.
2) The vehicle can communicate with other vehicles (V2V) and the infrastructure (V2I) through wireless communication.
3) TPD stores secret information about the vehicle which never be disclosed.

E. Overview of Scheme

A more detailed system model is shown in Fig. 4. There are four types of vehicles in the network :

1) Client vehicle (V_c).
2) Alternative vehicle (V_a).
3) Proxy vehicle (V_p).
4) Other vehicles.

After the vehicle enters the coverage of 5G-BS, according to the user's personal preference and real-time needs, the user requests some contents from CS through 5G-BS. Then the vehicle stores these contents in N CSBs according to the corresponding classification. Each vehicle has N CSBs to store

TABLE I
NOTATIONS

Notations	Definitions
TA	The trusted authority
5G-BS	The 5G base station
N	The number of CSBs in each vehicle
P	The generator of $E(F_p)$ with order q
q	The order of the generator P
s_{TA}	The system private key
P_{pub}	The system public key
V_i	The i-th vehicle
RID_i	The real identity of the i-th vehicle
PID_i	The pseudo-ID of the i-th vehicle
PW_i	The password of the i-th vehicle
V_{ci}	The i-th client vehicle
V_{ak}	The k-th alternative vehicle
V_{pj}	The j-th proxy vehicle
h, H_1, H_2	The secure hash functions
$EVAL_i[N]$	The evaluation array of V_i
tag_i	The flag of V_i
$R(DT_i)$	The content request sent by V_{ci} to V_p(s)
DT_{ij}	The content sent by V_{pj} to V_{ci}
E^t_{ik}	The weighted Euclidean distance between V_{ci} and V_{ak} at time t
$\|\|$	The concatenation operation
$\oplus$	The exclusive-OR operation

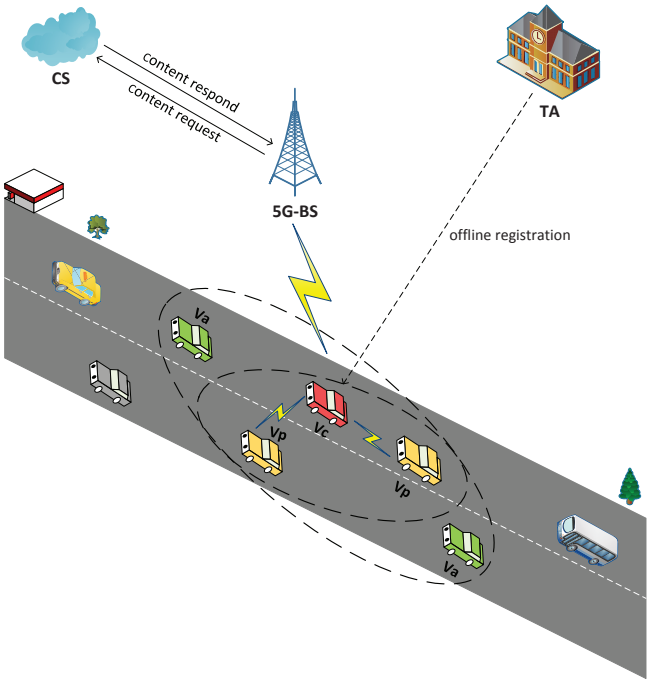


Fig. 4. Detailed system model

N types of contents. TA defines N at system initialization, the following factors will be considered: the number of vehicles in the network, the capacity of the CS, the degree of congestion in the network etc.

Users can enjoy the content that has been downloaded to local area, and score the classified contents subjectively according to their own satisfaction. The scores will be stored in the evaluation array $EVAL_i[N]$ of each vehicle.

Once a vehicle with non-empty CSBs has a content request, it becomes a client vehicle V_{ci}. Then, V_{ci} selects the alternative vehicles V_a(s) with "The Election Strategy

of ECV" of Cui et al. [4] and the alternative vehicles are marked as $V_{ak}(k = 1, 2, 3....)$. Thus, a neighborhood group centered on V_{ci} that is feasible in both realistic distance and computable resource is formed. According to the data similarity, V_{ci} selects m proxy vehicles in V_a(s) called as V_p(s), like $V_{p1}, V_{p2}, ...V_{pj}, ...V_{pm}(1 \leq j \leq m)$, and makes content requests to them respectively.

After receiving the request, V_{pj} picks the suitable content named DT_{ij}. DT_{ij} will be signed by V_{pj}, then V_{pj} sends it to V_{ci}. V_{ci} will decide whether to accept this content or not after verification. The operations of our scheme are based on the elliptic curve cryptosystem so the lower computation overhead could be achieved. Batch verification is supported to save time.

It is worth noting that, during the completion of a content request, there is one and only one V_{ci}. Nevertheless, there may be many or one alternative vehicle and the same is true for proxy vehicles in the neighborhood group of V_{ci}. Proxy vehicles are a subset of the alternative vehicles.

So far, an integrated system that separating the content from the evaluation has been established. Using classified storage and public evaluation allows users to learn the similarity between what is owned by themselves and the content kept by other vehicles without exposing cached content.

F. Brief Review of the Election Method

For the alternative vehicles selection of the proposed scheme, we use the election strategy of ECV in Cui et al.' scheme [4]. Here we substitute the entities in the proposed scheme into this election strategy, then make a brief review of it.

We consider two indicators to select alternative vehicles: close enough to the client vehicle, having sufficient available computing resource. A vehicle will not be selected as a V_a when it is very close to the client vehicle but has few available computing resource. Therefore, we use fuzzy logic to determine how to choose $V_a s$.

Conceptually, we take the distance from a vehicle to the V_{ci} and its available computing resource as binary inputs. After fuzzy processing, fuzzy rules will output a usable level. For example, when a vehicle is close to the V_{ci} and its available computing resource is sufficient, it will get a "Very Good" rating. We divided the output into five categories: "Very Good", "Good", "Unpreferable", "Bad", "Very Bad". In practical application, we use the distance membership function and the available performance index membership function to defuzzify the fuzzy rules. Then, we use the center of gravity (COG) method to calculate the results of these two functions. Finally, a value QD representing the qualified degree of the vehicle will be got. When $QD > k$ (k is positively correlated with the traffic density), it indicates that the vehicle is suitable to become a V_a.

IV. Proposed Scheme

Now we describe the proposed scheme in detail.

A. System Initialization

In this phase, TA generates system parameters and finishes the registration of vehicles.

- **Setup**

1) Let F_p be the finite field over p, and p is a prime number denotes the size of finite field. The elliptic curve $E(F_p)$ is defined on finite field F_p. Find the generator P with order q over elliptic curve $E(F_p)$, and then a cyclic addition group G with order q is generated.
2) TA chooses three one-way secure hash functions $h : \{0,1\}^* \rightarrow Z_q^*$, $H_1 : \{0,1\}^* \rightarrow Z_q^*$, $H_2 : \{0,1\}^* \rightarrow Z_q^*$.
3) TA randomly selects $s_{TA} \in Z_q^*$ as the system private key, and calculates the corresponding system public key $P_{pub} = s_{TA} \cdot P$.
4) TA defines two integers N, m.
5) TA keeps s_{TA} secretly, and publishes system parameters $\{E(F_p)$,h,H_1,H_2,q,P,$P_{pub}\}$.

- **Registration**

1) TA randomly selects a real identity RID_i and a password PW_i, assigns to vehicle V_i, then preloads $\{RID_i$, PW_i, $s_{TA}\}$ to the TPD of vehicle.
2) For the entire system, the content evaluation standard is separated from the content. TA develops N blocks of buffers as CSBs for each vehicle to store contents, and each CSB stores different types of content. For different vehicles, the CSBs of the same number store the same type of contents. Therefore, different users' evaluations of contents can be compared.
3) TA assigns an evaluation array $EVAL_i[N]$ to each vehicle, this array is dynamically updated once contents of CSBs change.
4) Each vehicle sets a flag tag_i that is initially 0, once the vehicle has requested content from CS successfully, turns the tag_i to 1.

- **Login**

When a user will use the vehicle, the real identity RID_i and the password PW_i should be entered. Only after the verification of TPD can the user obtain the right to use the vehicle.

B. Data Matching

- **Alternative Vehicles Selection**

Firstly, the wireless communication quality between vehicles is largely limited by distance due to the high speed of the vehicles. For example, V_j was very close to V_i originally. Maybe after only a few minutes, V_j has drove away from V_i's wireless communication range. Then the possibility of interaction between two vehicles has lost. So the appropriate distance is an important factor for content forwarding between vehicles.

Secondly, since each vehicle has N CSBs, and CSBs and the $EVAL_i[N]$ will be updated after each change for the content. It is necessary for vehicles to have sufficient available computing resource.

Therefore, not all vehicles covered by the same BS with the V_{ci} are eligible to be alternative vehicles for the V_{ci}. Due to the characteristics of vehicles, only the following two conditions are met can a vehicle be possible to carry out efficient content forwarding.

1) Alternative vehicle is close enough to the client vehicle.
2) There is sufficient available computing resource of alternative vehicle.

We consider two criteria mentioned above when selecting vehicles as the qualified alternative vehicles for V_{ci}. In the proposed scheme, we adopt the same election method of selecting V_a(s) as that of the scheme of Cui et al. [4] to choose ECVs. The validity of this election method has been illustrated in the scheme of Cui et al. [4].

- **Similarity Screening**

After the selection of V_a(s) is completed, the evaluation array $EVAL_k[N]$ of each V_{ak} is utilized to match the data similarity $E_{ik}^{(t)}$ with the evaluation array $EVAL_i[N]$ of V_{ci} at time t. For each alternative vehicle ($V_{a1}, V_{a2}, ...V_{ak}$,.....), V_{ci} performs the following operations:

1) V_{ci} gets the current evaluation array $EVAL_k[N]$ of V_{ak}.
2) Then, V_{ci} calculates the weighted Euclidean distance $E_{ik}^{(t)}$ between V_{ci} and V_{ak} at time t. The specific calculation process is shown in Algorithm 1.
3) $E_{ik}^{(t)}$ will be stored by V_{ci}.

Algorithm 1 The Weighted Euclidean Distance Calculation Process

Input:

$EVAL_k[N] = (y_1, y_2, ...y_N), tag_k$
$EVAL_i[N] = (x_1, x_2, ...x_N), tag_i$
//$EVAL_k[N]$ denotes the evaluation array produced by V_{ak} after using content for a while
//$EVAL_i[N]$ denotes the evaluation array produced by V_{ci} after using content for a while
//tag_k denotes a flag of V_{ak} indicates whether content is requested from the CS or not
//tag_i denotes a flag of V_{ci} indicates whether content is requested from the CS or not

Output:

$E_{ik}^{(t)}$: the numerical result of data similarity between evaluation arrays of V_{ci} and V_{ak} at time t

for each V_{ak} **do**
  while $tag_k == 1$ && $tag_i == 1$ **do**
    Sets a set of weights $w_N^{(t)} = (w_1, w_2.....w_N)$
    Gets V_{ci}'s own evaluation array $EVAL_i[N]$
    //$w_N^{(t)}$ is set by V_{ci} according to the degree of attention for N contents classified
    //$w_1 + w_2..... + w_N = 1$
    Calculates $E_{ik}^{(t)} = \sqrt{\sum_{i=1}^{N} w_i \cdot (x_i - y_i)^2}$
  end while
end for

After the above works, V_{ci} obtains the $E_{ik}^{(t)}$(s) between V_{ak}(s) and it. Then V_{ci} selects m objects with the minimum value named proxy vehicles V_p(s). At this time, V_p(s) are the vehicles with the most matching data similarity of V_{ci}. There is a very large probability that these vehicles will contain content that is either similar to or most similar to what the V_{ci} requested for. Next, V_{ci} sends content requests $R(DT_i)$ to V_p(s) respectively.

C. Content Forwarding

- **Signing**

When selected V_{pj} receives the $R(DT_i)$ sent by V_{ci}, it selects the most appropriate piece of content DT_{ij} in its CSBs. In order to enable the receiver to verify if the content has been tampered with, V_{pj} generates the fake identity as pseudo-ID PID_j to make a digital signature with the content DT_{ij}. Then V_{pj} sends it to V_{ci}. The operations conducted by V_{pj} are as following:

1) After V_{pj} receives request $R(DT_i)$, V_{pj} picks the suitable content DT_{ij}.
2) V_{pj} generates pseudo-ID $PID_j = \{PID_j^1, PID_j^2\}$, where $PID_j^1 = r_j \cdot P$, $PID_j^2 = RID_j \oplus h(r_j \cdot P_{pub})$. $r_j \in Z_q^*$ is a random number selected by V_{pj}.
3) Then V_{pj} gets the current timestamp T_j, calculates the signing key $sk_j = s_{TA} \cdot H_1(PID_j^1||PID_j^2||T_j) \bmod q$.
4) V_{pj} chooses a number $d_j \in Z_q^*$ randomly, calculates the signature: $\delta_j = sk_j + H_2(PID_j^1||PID_j^2||DT_{ij}||T_j) \cdot d_j \bmod q$.
5) Next, V_{pj} calculates $D_j = d_j \cdot P$.
6) Finally, V_{pj} sends the quintuple $\nabla = \{PID_j, DT_{ij}, \delta_j, D_j, T_j\}$ to V_{ci}.

- **Verification**

When V_{ci} receives the $\nabla = \{PID_j, DT_{ij}, \delta_j, D_j, T_j\}$, V_{ci} checks the signature δ_j to ensure that the signed content has not been manipulated which to guarantee the integrity of DT_{ij}.

At this time, V_{ci} may receive content from more than one vehicle simultaneously. There are a lot of information pile up, may result in crowding, thereby reducing the vehicle's efficiency. To avoid this situation, the signatures received by V_{ci} can be verified one by one or batch verified. The details are described as following:

1) Single Verification
   a) For V_{ci}, considering whether the content received is fresh enough or not to refrain from replay attacks, there is a pre-set lag time ΔT which V_{ci} can tolerate. Supposing the time to receive the signature is T_{ci}, V_{ci} checks whether the inequality $\Delta T + T_j \geq T_{ci}$ is true or not. If the answer is yes, V_{ci} continues this process. Or else, V_{ci} rejects it.
   b) V_{ci} calculates $H_j^1 = H_1(PID_j^1||PID_j^2||T_j)$ and $H_j^2 = H_2(PID_j^1||PID_j^2||DT_{ij}||T_j)$.
   c) Then V_{ci} checks whether the equation (1) is holds or not. If it is true, V_{ci} considers the verification have passed.

$$\delta_j \cdot P = H_j^1 \cdot P_{pub} + H_j^2 \cdot D_j \tag{1}$$

On account of $s_{TA} \cdot P = P_{pub}$ and $d_j \cdot P = D_j$, the reasoning process (2) of equation (1) is as following :

$$\begin{aligned} \delta_j \cdot P &= \left(sk_j + H_2(PID_j^1||PID_j^2||DT_{ij}||T_j) \cdot d_j\right) \cdot P \\ &= \left(s_{TA} \cdot H_1(PID_j^1||PID_j^2||T_j)\right. \\ &\quad \left. + H_2(PID_j^1||PID_j^2||DT_{ij}||T_j) \cdot d_j\right) \cdot P \\ &= H_j^1 \cdot s_{TA} \cdot P + H_j^2 \cdot d_j \cdot P \\ &= H_j^1 \cdot P_{pub} + H_j^2 \cdot D_j \end{aligned} \tag{2}$$

2) Batch Verification Within a certain period of time, we suppose that V_{ci} receives a large amount of signatures $\delta_1, \delta_2 ..... \delta_n$, included in $\{PID_1, DT_{i1}, \delta_1, D_1, T_1\}$, $\{PID_2, DT_{i2}, \delta_2, D_2, T_2\}$ $.....\{PID_n, DT_{in}, \delta_n, D_n, T_n\}$ sent by $V_1, V_2 ..... V_n$. V_{ci} completes batch verification for many signatures simultaneously. The execution process is as below which is similar to single verification:
   a) The verifier V_{ci} uses the timestamp T_j to check the freshness of ∇s. If one or more ∇s is not new enough, V_{ci} discards it. Otherwise, V_{ci} continues the verification.
   b) Here we use small exponential test to avoid signature redundancy and obfuscation attacks [17]. V_{ci} randomly produces a vector l, this vector represents $\{l_1, l_2 ..... l_n\}$. Every value in this vector is random, the range is between 1 and 2^t. Note that, even if it's just one of n signatures is wrong, V_{ci} can check it out. Furthermore, t is a very small integer which takes little computation overhead.
   c) V_{ci} verifies equation (3). If equation (3) is correct, the contents received are considered to be legitimate and haven't been modified. The reasoning process of equation (3) is similar to (2) in single verification.

$$\left(\sum_{i=1}^{n} l_i \cdot \delta_i\right) \cdot P = \left(\sum_{i=1}^{n} l_i \cdot H_i^1\right) \cdot P_{pub} + \sum_{i=1}^{n} l_i \cdot H_i^2 \cdot D_i \tag{3}$$

If appropriate result is not obtained in the alternative vehicles selection and similarity screening, or the user doesn't want to request content from proxy vehicles, the user can choose to request content from CS via 5G-BS directly.

V. Security Proof

A. Security Model

First, we introduce the elliptic curve computable discrete logarithm (ECCDL) problem.

Definition 1. ***(ECCDL problem)*** *Given an element $\Omega \in Z_q^*$. The computation goal of the ECCDL problem is $\omega \in Z_q^*$, which is unknown and can satisfy that $\omega \cdot P = \Omega$. This goal is impossible to achieve.*

Definition 2. *The signature algorithm of the proposed scheme is secure under the adaptive chosen message attack if any probabilistic polynomial time adversary $\mathcal{A}$ cannot forge a legal signature message with a non-negligible probability.*

The security of the proposed scheme is defined by the game between the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$. $\mathcal{A}$ can perform some queries on $\mathcal{C}$, and $\mathcal{C}$ will respond as following.

1) $Setup - Oracle$: When $\mathcal{A}$ executes this query, $\mathcal{C}$ selects a random number $x \in Z_q^*$ as the system's private key and calculates system parameters. Then, $\mathcal{C}$ returns system parameters to $\mathcal{A}$.
2) $H_1 - Oracle$: $\mathcal{C}$ randomly generates a number $n \in Z_q^*$ when $\mathcal{A}$ carries out the query with the message m. And then, $\mathcal{C}$ stores tuple (m, n) in the list L_{H_1}, which is initialized empty. Finally, $\mathcal{C}$ gives the n to $\mathcal{A}$ as the return value.
3) $H_2 - Oracle$: $\mathcal{C}$ randomly generates a number $n \in Z_q^*$ when $\mathcal{A}$ carries out the query with the message m. And then, $\mathcal{C}$ stores tuple (m, n) in the list L_{H_2}, which is initialized empty. Finally, $\mathcal{C}$ gives the n to $\mathcal{A}$ as the return value.
4) $Extract - Oracle$: $\mathcal{C}$ generates private key and stores it in the list L_E, which is initialized empty, when $\mathcal{A}$ carries out the query with user's pseudo-ID PID_j.
5) $Sign - Oracle$: When $\mathcal{A}$ carries out the query with the content DT_{ij}, $\mathcal{C}$ randomly produces a tuple (DT_{ij}, D_j, δ_j) and gives it to $\mathcal{A}$.

We use the symbol Σ to represent the proposed scheme. $\mathcal{A}$ can break the proposed scheme if it can forge a legal login message. The advantage of $\mathcal{A}$ attacking the security of the authentication for the proposed scheme Σ can be defined as $Adv_{\Sigma}^{\mathcal{A}}(Auth)$.

B. Security Proof

In this subsection, we prove that the proposed scheme is able to provide the security of the authentication. That is to say, the adversary $\mathcal{A}$ can not forge a legal signature message with a negligible probability ϵ. We suppose the two hash functions (H_1 and H_2) in the scheme are two random oracles.

Theorem 1. *R and S represent the number of times that $\mathcal{A}$ executes the queries in the random and the sign oracle. If $\mathcal{A}$ is able to breach the authentication of the proposed scheme, then $\mathcal{C}$ will solve the ECCDL problem with a probability less than $120686RT/\epsilon$ during the time period T, where $\epsilon \geq 10(R + S)(S + 1)/q$.*

$Proof$: Suppose the adversary $\mathcal{A}$ can forge legitimate signature message with a non-negligible probability ϵ. Then we will show how the challenger $\mathcal{C}$ can use a non-negligible probability to solve the ECCDL problem. We deduce an implicit contradiction from the hypothesis.

For the ECCDL problem, there is a random instance (P, aP) in G_q. If $\mathcal{C}$ could solve the problem, it means that $\mathcal{C}$ will calculate a which is unknown. Moreover, the challenger $\mathcal{C}$ is able to settle the ECCDL problem by carrying out the following queries from adversary $\mathcal{A}$.

1) $Setup$: After setting the security parameter k as input, $\mathcal{C}$ selects a random number s_{TA}, which represents its private key. Next, $\mathcal{C}$ calculates $P_{pub} = s_{TA} \cdot P$, where P_{pub} is the system public key. Finally, $\mathcal{C}$ sends $\{P, P_{pub}, q, h, H_1, H_2\}$ to $\mathcal{A}$.
2) $H_1 - query$: After receiving the query with the tuple (PID_j^1, PID_j^2, T_j) from $\mathcal{A}$, $\mathcal{C}$ checks if the list L_{H_1} has $(PID_j^1, PID_j^2, T_j, H_j^1)$. If it exists, $\mathcal{C}$ returns H_j^1 to $\mathcal{A}$. Otherwise, $\mathcal{C}$ randomly generates a number $H_j^1 \in Z_q^*$, inserts the tuple $(PID_j^1, PID_j^2, T_j, H_j^1)$ into L_{H_1}. Finally, $\mathcal{C}$ gives the H_j^1 to $\mathcal{A}$.
3) $H_2 - query$: After receiving the query with the tuple $(PID_j^1, PID_j^2, DT_{ij}, T_j)$ from $\mathcal{A}$, $\mathcal{C}$ checks if the

list L_{H_2} has $(PID_j^1, PID_j^2, DT_{ij}, T_j, H_j^2)$. If it exists, $\mathcal{C}$ returns H_j^2 to $\mathcal{A}$. Otherwise, $\mathcal{C}$ randomly generates a number $H_j^2 \in Z_q^*$, inserts the tuple $(PID_j^1, PID_j^2, DT_{ij}, T_j, H_j^2)$ into L_{H_2}. Finally, $\mathcal{C}$ gives the H_j^2 to $\mathcal{A}$.

4) $Extract-query$: After receiving the query with user's pseudo-ID PID_j form $\mathcal{A}$, $\mathcal{C}$ selects a random number $d_j \in Z_q^*$, calculates $D_j = d_j \cdot P$ and checks if the list L_E has $(PID_j^1, PID_j^2, T_j, sk_j)$. If it exists, $\mathcal{C}$ returns sk_j to $\mathcal{A}$. Otherwise, $\mathcal{C}$ calculates $sk_j = s_{TA} \cdot h(PID_j^1||PID_j^2||T_j) mod\ q$ and stores the new tuple in L_E. Finally, $\mathcal{C}$ gives sk_j to $\mathcal{A}$ as the return value.
5) $Sign-query$: After receiving the query on the content DT_{ij} with user's pseudo-ID PID_j form $\mathcal{A}$, $\mathcal{C}$ checks if the list L_{H_1} has $(PID_j^1, PID_j^2, T_j, H_j^1)$ firstly. $\mathcal{C}$ extracts H_j^1 from the tuple. Then, $\mathcal{C}$ chooses two random numbers d_j and H_j^2. Besides, $\mathcal{C}$ chooses two random numbers x_j and y_j again. Otherwise, $\mathcal{C}$ calculates $D_j = H_j^{2^{-1}} x_j \cdot P - Q$ and $\delta_j = y_j$ and sends (DT_{ij}, D_j, σ_j) to $\mathcal{A}$, where $H_j^2 = H_2(PID_j^1||PID_j^2||DT_{ij}||T_j)$.
6) $Analysis$: According to Forking lemma [41], if $\mathcal{A}$ can forge two legitimate signatures $(D_j, \delta_j{}' = sk_j + d_j \cdot H_j^2 mod\ q)$ and $(D_j{}', \sigma_j{}' = sk_j + d_j \cdot H_j^2{}' mod\ q)$, where $H_j^2 \neq H_j^2{}'$, $\mathcal{C}$ will gain sk_j form the two signatures by computing.

$$\begin{aligned} &\frac{(H_j^2{}'\delta_j - H_j^2\delta_j{}')}{H_j^2{}' - H_j^2} mod q \\ &= \frac{H_j^2{}' H_j^2 d_j + H_j^2{}' sk_j - H_j^2 H_j^2{}' d_j - H_j^2 sk_j}{H_j^2{}' - H_j^2} mod q \\ &= sk_j \end{aligned} \tag{4}$$

Accroding to the above, we can draw a conclusion that $\mathcal{C}$ can solve the ECCDL problem with a probability less than $120686RT/\epsilon$ during the period T, where $\epsilon \geq 10(R+S)(S+1)/q$. However, it contradicts with the difficulty of solving the ECCDL problem. So the proposed scheme is secure against adaptive chosen message attack in the random oracle model.

C. Security Analysis

In this subsection, we will analyze the security of the proposed scheme under the above security proof.

- **Message Authentication**

According to the above proof, no any polynomial probability time adversary $\mathcal{A}$ can forge a legal signature. Therefore, the receiver can check the integrity of message received from other vehicles by computing $\delta_j P = H_j^1 P_{pub} + H_j^2 D_j$.

- **Identity Anonymity**

Because the vehicle adopts a pseudo-ID during the interaction, the real identity is hidden in the pseudo-ID such as $PID_j^1 = r_j \cdot P, PID_j^2 = RID_j \oplus h(r_j \cdot P_{pub})$. The system private key is secret and r_j is random which will not be got by $\mathcal{A}$. Therefore, the proposed scheme provides identity anonymity.

- **Identity Traceability**

When a vehicle uses an anonymous identity PID_j to send error message or illegal information, TA can use s_{TA} to extract the real identity by computing $RID_j = PID_j^2 \oplus h(s_{TA} \cdot PID_j^1)$. Therefore, the proposed scheme supports identity tracking.

- **Un-linkability**

Each time the vehicle makes a signature, it generates a pseudo-ID to send content. Pseudo-ID is updated frequently. In addition, dynamic random number is added to the signature, such as $\delta_j = sk_j + d_j \cdot H_2(PID_j^1||PID_j^2||DT_{ij}||T_j)$. Therefore, it is very hard for an adversary to link multiple messages from the same vehicle.

- **Resistance to Modify Attack**

Because the signature of each message contains the system private key and the dynamic random number, the adversary cannot obtain the system private key and the random number. The adversary cannot tamper with the message. Otherwise, the recipient's authentication of the signature is not valid. Thus, the proposed scheme can withstand the modify attack.

- **Resistance to Replay Attack**

A timestamp is embedded in the signature of each message, and the signature cannot be tampered with. The receiver of the message can check for replay attacks by validating the signature. Thus, the proposed scheme can withstand the replay attack.

- **Resistance to Impersonation Attack**

On the basis of the security proof mentioned above, we know that there is no any probabilistic polynomial time adversary $\mathcal{A}$ can forge a legitimate signature message if it doesn't has the system private key. Thus, the proposed scheme can also resist impersonation attack.

- **Resistance to Password Guess Attack**

During the registration phase, the user's real identity RID_i and password PW_i are issued by TA, so there will be no disclosure. TPD authenticates the two parameters holding by user. After authentication, the user can obtain the right to control the vehicle. Thus avoiding the illegal users from obtaining the control rights of vehicles.

D. Security Comparison

Let L1, L2, L3, L4, L5 and L6 represent the message authentication, the conditional privacy preservation, the un-linkability, the resistance to replay attack, the resistance to modify attack resistance and the resistance to password guess attack respectively. TABLE II shows the security comparison with several related schemes, which indicates that the proposed scheme has a good performance in terms of security.

TABLE II
SECURITY COMPARISON

	L1	L2	L3	L4	L5	L6
Zhong's scheme [42]	✓	✓	✓	✓	×	×
Azees's scheme [43]	✓	✓	✓	✓	✓	×
Assar's scheme [44]	✓	✓	✓	✓	✓	×
Li's scheme [45]	✓	✓	✓	✓	✓	×
Our scheme	✓	✓	✓	✓	✓	✓

✓: The security requirement is satisfied.
× : The security requirement is not satisfied.

VI. PERFORMANCE ANALYSIS

Hereinafter, we analyze the performance of the proposed scheme, then compare it to four recent message authentication schemes based vehicular networks [42], [43], [44], [45]. We illustrate that the proposed scheme is effective and feasible from the two aspects of computation overhead and communication delay. It's worth noting that since the backgrounds are not exactly the same, the main body we need to sign in the proposed scheme is called content DT_{ij}. The main body for the other four schemes need to be signed is called message M_i, they are the same essentially. In the proposed scheme, it is not limited to signing message, what needs to be delivered reliably can be any type of content the users want.

The cryptographic operations of privacy preservation authentication schemes came up by Zhong et al. [42] in 2019 and Azees et al. [43] in 2017 are based on bilinear pairing. The other two schemes [44], [45] to be compared are the same as the one we proposed, which are based on elliptic curve for cryptographic operations.

The bilinear pairing : $\bar{E} : G_1 \times G_1 \rightarrow G_T$ can reach the secure level of 80 bits. $\bar{P}$ is the generator of the additive group G_1. G_1 has order $\bar{P}$ on the super singular elliptic curve $\bar{E} : y^2 = x^3 + x$ mod $\bar{p}$ which $\bar{p}$ is a large prime number with 512 bits, and $\bar{q}$ should be a 160 bit Solinas prime number. With regard to the proposed scheme, the elliptic curve $E : y^2 = x^3 + ax + b$ (mod p) is used, $a, b \in Z_q^*$. An additive group G is generated from the elliptic curve with a generator P, and the order is q, where p, q are both 160-bit prime number.

The cryptography library used in the experiment is MIRACL [19]. The execution time for operations involved was measured by us before. These data have been used in the authentication schemes which have been published [17], [46]. For the same operation, due to the characteristics of CPU, the time it takes to execute multiple times is not the same even in the same environment. In order to eliminate the deviation and compare as fairly as possible, the execution time of operations involved are measured separately. We quantify the total overhead based on this result to make a fair comparison. The hardware platform is as the same as the one in Cui's scheme [17].

We define all the execution time of related operations as following:

1) T_{bp} : The execution time of carrying out a bilinear pairing operation $\bar{e}(P, Q)$, where $P, Q \in G_1$.
2) T_{bp-sm} : The execution time of carrying out a scale multiplication operation $\bar{x} \cdot \bar{P}$ that is connected with bilinear pairing, where $\bar{P} \in G_1$, $\bar{x} \in Z_{\bar{q}}^*$.
3) T_{bp-pa} : The execution time of carrying out a point addition operation $\bar{P} + \bar{Q}$ that is also connected with bilinear pairing, where $\bar{P}, \bar{Q} \in G_1$.
4) T_{mtp} : The execution time of carrying out a MapToPoint operation.
5) T_{ec-sm} : The execution time of carrying out a scale multiplication operation $x \cdot P$ that is connected with elliptic curve, where $P \in G$, $x \in Z_q^*$.
6) T_{ec-pa} : The execution time of carrying out a point addition operation $P + Q$ that is also connected with elliptic curve, where $P, Q \in G$.
7) T_h : The execution time of carrying out a secure one-way hash function operation.

The execution time for all operations mentioned above are listed in TABLE III.

TABLE III
EXECUTION TIME

Operation	Time(ms)
T_{bp}	5.0860
T_{bp-sm}	0.6940
T_{bp-pa}	0.0018
T_{mtp}	0.0992
T_{ec-sm}	0.3218
T_{ec-pa}	0.0024
T_h	0.0010

A. Computation Overhead

We analyze operations involved in the following three steps of all schemes [42], [43], [44], [45] and list them in the TABLE IV (Assuming that n represents the number of batch verification messages).

1) SSM : Signing a single message.
2) VSM : Verifying a single message.
3) BVMM : Batch verifying for multiple messages.

Next, we conduct detailed analysis of Zhong's scheme [42] and the proposed scheme, the analysis process of other three schemes can be obtained in the same way [43], [44], [45].

Zhong's scheme takes advantage of bilinear pairing to ensure message integrity. First, for the step of signing a single message, figuring out the parameters R_i and T_i is necessary to generate a signature σ_i for the message. So three scale multiplication operations, two point addition operations, one MapToPoint operation and one secure one-way hash function operation are required. The total computation overhead of this step is $3T_{bp-sm}$ + $2T_{bp-pa}$ + $1T_{mtp}$ + $1T_h$ $\approx$ 2.1858 ms. Then, three bilinear pairing operations, two scale multiplication operations, one point addition operation, two MapToPoint operations and one secure one-way hash function operation is needed to verify a single message. So this step takes $3T_{bp}$ + $2T_{bp-sm}$ + $1T_{bp-pa}$ + $2T_{mtp}$ + $1T_h$ $\approx$ 16.8472 ms. Finally, for batch verification in [42], there are three bilinear pairing operations, 2n scale multiplication operations, (4n-3) point addition operations, (n+1) MapToPoint operations and 2n secure one-way hash function operations to achieve it. Consequently, the execution time for this step is $3T_{bp}$ + 2n

TABLE IV
COMPARISON OF COMPUTATION OVERHEAD

	SSM	VSM	BVMM
Zhong's scheme [42]	$3T_{bp-sm}$ + $2T_{bp-pa}$ + $1T_{mtp}$ + $1T_h$	$3T_{bp}$ + $2T_{bp-sm}$ + $1T_{bp-pa}$ + $2T_{mtp}$ + $1T_h$	$3T_{bp}$ + 2n T_{bp-sm} + (4n-3) T_{bp-pa} + (n+1) T_{mtp} + 2n T_h
Azees's scheme [43]	$4T_{bp-sm}$ + $2T_h$	$2T_{bp}$ + $5T_{bp-sm}$ + $2T_{bp-pa}$	(n+1) T_{bp} + 5n T_{bp-sm} + 2n T_{bp-pa}
Asaar's scheme [44]	$7T_{ec-sm}$ + $6T_h$	$12T_{ec-sm}$ + $8T_{ec-pa}$ + $8T_h$	(4n+10) T_{ec-sm} + (6n+2)T_{ec-pa} + (6n+2) T_h
Li's scheme [45]	$1T_{ec-sm}$ + $2T_h$	$4T_{ec-sm}$ + $1T_{ec-pa}$ + $2T_h$	(2n+2) T_{ec-sm} + n T_{ec-pa} + 2n T_h
Our scheme	$3T_{ec-sm}$ + $3T_h$	$3T_{ec-sm}$ + $1T_{ec-pa}$ + $2T_h$	(n+2) T_{ec-sm} + (n-1) T_{ec-pa} + 2n T_h

T_{bp-sm} + (4n-3) T_{bp-pa} + (n+1) T_{mtp} + 2n T_h $\approx$ 1.4964 n + 15.3518 ms.

For the scheme we proposed, we first generate the pseudo-ID PID_j by using the real identity RID_j and the system public key P_{pub}. Then we get the current timestamp T_j to make the signing key sk_j, and finally we get the signature σ_j of a single content DT_{ij}. This step requires three scale multiplication operations and three secure one-way hash function operations, which will take $3T_{ec-sm}$ + $3T_h$ $\approx$ 0.9684 ms. And then, three scale multiplication operations, one point addition operation and two secure one-way hash function operations are indispensable for verifying a single content, which will consume $3T_{ec-sm}$ + $1T_{ec-pa}$ + $2T_h$ $\approx$ 0.9698 ms. Finally, for batch verification, the total operations required are (n+2) scale multiplication operations, (n-1) point addition operations and 2n secure one-way hash function operations, that is (n+2) T_{ec-sm} + (n-1) T_{ec-pa} + 2n T_h $\approx$ 0.3262 n + 0.6412 ms.

The computation overhead results for all schemes to complete the three steps are shown in TABLE V. Fig. 5 shows the computation overhead of signing a single message and verifying a single message. It can be clearly seen that the proposed scheme is far lower than Zhong's scheme [42], Azees's scheme [43] and Assar's scheme [44] in the computation overhead of SSM and VSM. For Li's scheme [45], we are less than it when verifying a single message. However, since the generation of pseudo-ID is left to TA, this part of the computation overhead is saved in Li's scheme [45]. In the proposed scheme, each time the content is sent, the vehicle generates a pseudo-ID to ensure identity privacy.

For the computation overhead of batch verification, we assume that the number of messages that participating in the batch authentication is n. In TABLE IV, we have listed the number of all operations required in batch verification for each scheme. Similarly, we put the execution time of each operation in TABLE III into TABLE IV. The results are shown in TABLE V which are five linear functions. As the number of messages increases, the computation overhead of batch verification are shown in the Fig. 6. Obviously, the linear function of our scheme is at the bottom. Therefore, our scheme has the lowest computation overhead.

B. Communication Delay

Due to the length of $\bar{p}$ is 64 bytes, the length of q is 20 bytes, so the length of additive group G_1 is of 64 $\times$ 2 = 128 bytes, and the length of G is 20 $\times$ 2 = 40 bytes. The size of

TABLE V
COMPARISON OF COMPUTATION OVERHEAD TIME

	SSM (ms)	VSM (ms)	BVMM (ms)
Zhong's scheme [42]	2.1858	16.8472	1.4964 n + 15.3518
Azees's scheme [43]	2.7780	13.6456	8.5596 n + 5.0860
Asaar's scheme [44]	2.2586	3.8888	1.3076 n + 3.2248
Li's scheme [45]	0.3238	1.2916	0.6480 n + 0.6436
Our scheme	0.9684	0.9698	0.3262 n + 0.6412

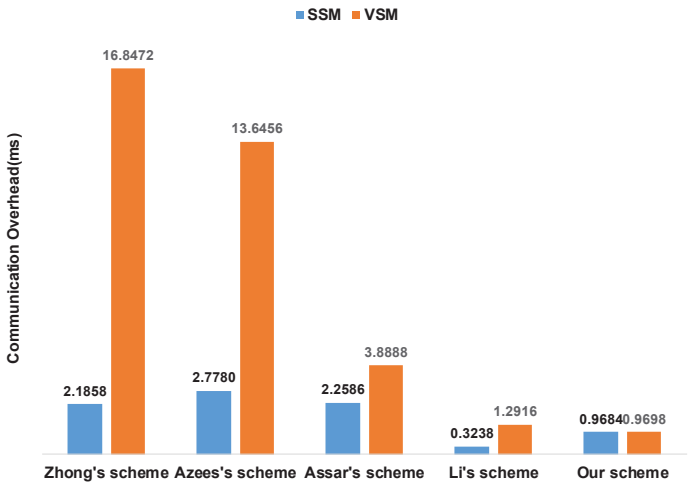


Fig. 5. Computation overhead of SSM and VSM

the element belonging to the closure Z_q^* is 20 bytes. The size of the element output by the secure one-way hash function is 20 bytes. The size of obtained timestamp is 4 bytes. Hence, $|G_1|$ = 128 bytes, $|G|$ = 40 bytes, $|H|$ = 20 bytes, $|Z_q^*|$ = 20 bytes, $|T_i|$ = 4 bytes. The communication delay we consider is the size of the signature sent by the vehicles.

In Zhong's scheme [42], the size of signature $\{PID_i, m_i, vpk_i, t_i, \sigma_i\}$ is 128 $\times$ 2 + 4 + 128 + 4 + 128 + 128 = 644 bytes, which σ_i including $\{R_i, T_i\}$. The t_i is a timestamp, $PID_{i,1}, PID_{i,2}, vpk_i, R_i, T_i$ are all $\in$ G_1 and PID_i consists of three parts $PID_{i,1}, PID_{i,2}, VP_i$, VP_i denotes the valid period of PID_i, here we treat its length as the same as the timestamp. Similarly, the communication delay of the other three is calculated as following: In Azees's scheme, the signature to be sent

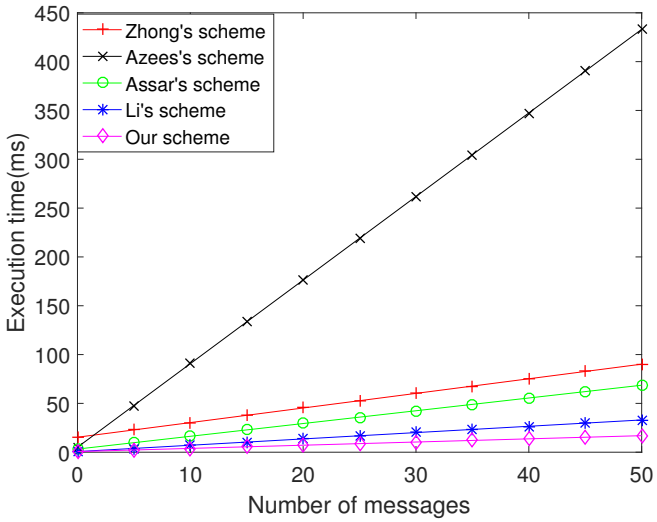


Fig. 6. Computation overhead of BVMM

$\{sig, Y_k, Cert_k\}$ is 128 × 6 + 3 × 20 + 20 = 848 bytes, where $Cert_k = (Y_k||E_i||DID_{ui}||\gamma_u||\gamma_v||c||\lambda||\sigma_1||\sigma_2)$. c is a hash result, $sig, E_i, DID_{ui}, \gamma_u, \gamma_v, Y_k \in G_1$, $\lambda, \sigma_1, \sigma_2 \in Z_q^*$. The third scheme is Asaar's scheme, double signature was taken due to the presence of proxy vehicles. The signature to be sent is $\{PID_i, T_i, m_i, R_i, W_i, s_{i,1}, s_{i,2}\}$, $\{b, PID_p, PID_i, W_i, T_i, \sigma_1, \sigma_2, R_p, s_p\}$. The size of the first tuple is 40 + 20 + 4 + 40 + 40 + 20 + 20 = 184 bytes. $PID_i = \{PID_{i,1}, PID_{i,2}\}$ where $PID_{i,1} \in G$, $PID_{i,2} \in Z_q^*$, T_i is a timestamp, $R_i, W_i \in G$, $s_{i,1}, s_{i,2} \in Z_q^*$. For the second tuple, b is a flag bit that indicates whether the batch verification results are valid or not, only takes 1 byte. The size of PID_p is same as PID_i, they are both 60 bytes, $W_i, R_p \in G$, T_i is a timestamp, $\sigma_1, \sigma_2, s_p \in Z_q^*$. The size is 1 + 60 × 2 + 40 × 2 + 4 + 20 × 3 = 265 bytes. So the total size is 184 + 265 = 449 bytes. In Li's scheme [45], the information which vehicle broadcasts is $\{M_i, PID_{i,l}, PK_{i,l}, R_i, T_i, sig_i\}$, where $PID_{i,l} \in Z_q^*$, $PK_{i,l}, R_i, sig_i \in G$, T_i is a timestamp, so the communication delay is 20 + 40 × 3 + 4 = 144 bytes.

Next, we analyze the communication delay of the proposed scheme. The size of quintuple $\nabla = \{PID_j, DT_{ij}, \delta_j, D_j, T_j\}$ is 40 + 20 + 20 + 40 + 4 = 124 bytes, $PID_j = \{PID_{j,1}, PID_{j,2}\}$ where $PID_{i,1} \in G$, $PID_{i,2} \in Z_q^*$, $\delta_j \in Z_q^*$, $D_j \in G$ and T_i is a timestamp.

Communication delay for all schemes are shown in TABLE VI. Similar to the computation overhead, our communication delay is significantly better than other four schemes [42], [43], [44], [45].

TABLE VI
SIZE OF COMMUNICATION DELAY

Scheme	Sending a message	Sending n messages
Zhong's scheme [42]	644 bytes	644 n bytes
Azees's scheme [43]	848 bytes	848 n bytes
Asaar's scheme [44]	449 bytes	449 n bytes
Li's scheme [45]	144 bytes	144 n bytes
Our scheme	124 bytes	124 n bytes

VII. CONCLUSION

In vehicular networks, the rapid movement of vehicles makes the communication opportunities between vehicles last for a very short duration. With the increase in the diversification of users' content services, the security and efficiency of content sharing have turned into two of the most important issues. Therefore, we introduce an elliptic curve-based message authentication scheme into the content sharing process. We adopt the mode of separating content from evaluation, so that the vehicle can obtain the evaluation arrays of adjacent vehicles without acquiring the specific content details. Simultaneously, we take into account the mobility and computing power of vehicles. Further, the security analysis shows that the proposed scheme meets the security requirements in vehicular networks. We also prove that it achieves a better performance.

In the future, we plan to consider improving the security of content sharing by using an in-group dual authentication mechanism to construct a more secure and efficient content sharing mechanism for 5G-enabled vehicular networks.

REFERENCES

[1] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in vanets," *IEEE transactions on vehicular technology*, vol. 66, no. 4, pp. 3235–3248, 2015.

[2] C. Lai, R. Lu, D. Zheng, and X. S. Shen, "Security and privacy challenges in 5g-enabled vehicular networks," *IEEE Network*, vol. 34, no. 2, pp. 37–45, 2020.

[3] X. Cheng, R. Zhang, and L. Yang, "Wireless toward the era of intelligent vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 188–202, 2018.

[4] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1621–1632, 2018.

[5] C. Lai, M. Zhang, J. Cao, and D. Zheng, "Spir: A secure and privacy-preserving incentive scheme for reliable real-time map updates," *IEEE Internet of Things Journal*, 2019.

[6] A. Yang, J. Weng, N. Cheng, J. Ni, X. Lin, and X. Shen, "Deqos attack: Degrading quality of service in vanets and its mitigation," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4834–4845, 2019.

[7] J. Cheng, G. Yuan, M. Zhou, S. Gao, C. Liu, and H. Duan, "A fluid mechanics-based data flow model to estimate vanet capacity," *IEEE Transactions on Intelligent Transportation Systems*, 2019.

[8] X. Cheng, R. Zhang, S. Chen, J. Li, L. Yang, and H. Zhang, "5g enabled vehicular communications and networking," *China Communications*, vol. 15, no. 7, pp. iii–vi, 2018.

[9] K. S. V. Prasad, E. Hossain, and V. K. Bhargava, "Energy efficiency in massive mimo-based 5g networks: Opportunities and challenges," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 86–94, 2017.

[10] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson, "5g mmwave positioning for vehicular networks," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 80–86, 2017.

[11] J. Cheng, G. Yuan, M. Zhou, S. Gao, C. Liu, H. Duan, and Q. Zeng, "Accessibility analysis and modeling for iov in an urban scene," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4246–4256, 2020.

[12] N. Magaia, Z. Sheng, P. R. Pereira, and M. Correia, "Repsys: A robust and distributed incentive scheme for collaborative caching and dissemination in content-centric cellular-based vehicular delay-tolerant networks," *IEEE Wireless Communications*, vol. 25, no. 3, pp. 65–71, 2018.

[13] T. Van Mierlo, "The 1% rule in four digital health social networks: an observational study," *Journal of medical Internet research*, vol. 16, no. 2, p. e33, 2014.

[14] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "Pa-crt: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[15] M. H. Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5g-enabled vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 7868–7881, 2016.

[16] B. Bellalta, E. Belyaev, M. Jonsson, and A. Vinel, "Performance evaluation of ieee 802.11 p-enabled vehicular video surveillance system," *IEEE Communications Letters*, vol. 18, no. 4, pp. 708–711, 2014.

[17] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "Rsma: Reputation system-based lightweight message authentication framework and protocol for 5g-enabled vehicular networks," *IEEE Internet of Things Journal*, 2019.

[18] J. Chen, G. Mao, C. Li, and D. Zhang, "A topological approach to secure message dissemination in vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, 2019.

[19] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39–68, 2007.

[20] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*. IEEE, 2008, pp. 1229–1237.

[21] A. Wasef, Y. Jiang, and X. Shen, "Ecmv: efficient certificate management scheme for vehicular networks," in *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*. IEEE, 2008, pp. 1–5.

[22] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on vehicular technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[23] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in vanets," *Computer Communications*, vol. 71, pp. 50–60, 2015.

[24] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 907–919, 2013.

[25] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*. IEEE, 2008, pp. 246–250.

[26] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.

[27] Y. Liu, L. Wang, and H.-H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3697–3710, 2014.

[28] M. Gerla, C. Wu, G. Pau, and X. Zhu, "Content distribution in vanets," *Vehicular Communications*, vol. 1, no. 1, pp. 3–12, 2014.

[29] B. Xu, A. Ouksel, and O. Wolfson, "Opportunistic resource exchange in inter-vehicle ad-hoc networks," in *IEEE International Conference on Mobile Data Management, 2004. Proceedings. 2004*. IEEE, 2004, pp. 4–12.

[30] J. Zhang, Q. Zhang, and W. Jia, "Vc-mac: A cooperative mac protocol in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 3, pp. 1561–1571, 2008.

[31] C. Cheng, J. Lee, T. Jiang, and T. Takagi, "Security analysis and improvements on two homomorphic authentication schemes for network coding," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 993–1002, 2016.

[32] T. Wang, L. Song, Z. Han, and B. Jiao, "Dynamic popular content distribution in vehicular networks using coalition formation games," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 538–547, 2013.

[33] M. Xing, J. He, and L. Cai, "Utility maximization for multimedia data dissemination in large-scale vanets," *IEEE Transactions on Mobile Computing*, vol. 16, no. 4, pp. 1188–1198, 2016.

[34] D. D. Van, Q. Ai, Q. Liu, and D.-T. Huynh, "Efficient caching strategy in content-centric networking for vehicular ad-hoc network applications," *IET Intelligent Transport Systems*, vol. 12, no. 7, pp. 703–711, 2018.

[35] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in internet of vehicles: A review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, 2015.

[36] X. Cheng, C. Chen, W. Zhang, and Y. Yang, "5g-enabled cooperative intelligent vehicular (5genciv) framework: When benz meets marconi," *IEEE Intelligent Systems*, vol. 32, no. 3, pp. 53–59, 2017.

[37] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen, "Sirc: A secure incentive scheme for reliable cooperative downloading in highway vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 6, pp. 1559–1574, 2016.

[38] Q.-T. Ngo, O. Berder, and P. Scalart, "Minimum euclidean distance based precoders for mimo systems using rectangular qam modulations," *IEEE transactions on signal processing*, vol. 60, no. 3, pp. 1527–1533, 2011.

[39] I. Dokmanic, R. Parhizkar, J. Ranieri, and M. Vetterli, "Euclidean distance matrices: essential theory, algorithms, and applications," *IEEE Signal Processing Magazine*, vol. 32, no. 6, pp. 12–30, 2015.

[40] H. Sheng, J. Xiao, Y. Cheng, Q. Ni, and S. Wang, "Short-term solar power forecasting based on weighted gaussian process regression," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 1, pp. 300–308, 2017.

[41] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of cryptology*, vol. 13, no. 3, pp. 361–396, 2000.

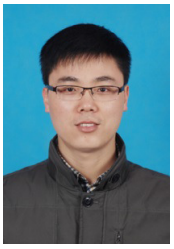
[42] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in vanet," *Information Sciences*, vol. 476, pp. 211–221, 2019.

[43] M. Azees, P. Vijayakumar, and L. J. Deboarh, "Eaap: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[44] M. R. Asaar, M. Salmasizadeh, W. Susilo, and A. Majidi, "A secure and efficient authentication technique for vehicular ad-hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5409–5423, 2018.

[45] J. Li, K.-K. R. Choo, W. Zhang, S. Kumari, J. J. Rodrigues, M. K. Khan, and D. Hogrefe, "Epa-cppa: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *Vehicular Communications*, vol. 13, pp. 104–113, 2018.

[46] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, "Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 2241–2250, 2017.

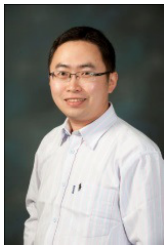


Jie Cui was born in Henan Province, China, in 1980. He received his Ph.D. degree in University of Science and Technology of China in 2012. He is currently a professor and Ph.D. supervisor of the School of Computer Science and Technology at Anhui University. His current research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). He has over 100 scientific publications in reputable journals (e.g. IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network and Service Management, IEEE Transactions on Emerging Topics in Computing, IEEE Transactions on Circuits and Systems and IEEE Internet of Things Journal), academic books and international conferences.

Jiayi Chen is now a research student in the School of Computer Science and Technology, Anhui University. Her research focuses on the security of vehicular networks.

Hong Zhong was born in Anhui Province, China, in 1965. She received her PhD degree in computer science from University of Science and Technology of China in 2005. She is currently a professor and Ph.D. supervisor of the School of Computer Science and Technology at Anhui University. Her research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). She has over 140 scientific publications in reputable journals (e.g. IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network and Service Management, IEEE Transactions on Big Data and IEEE Internet of Things Journal), academic books and international conferences.

Jing Zhang is currently a PhD student in the School of Computer Science and Technology, Anhui University, Hefei, China. Her research interests include vehicular ad hoc network, IoT security and applied cryptography. She has over 10 scientific publications in reputable journals (e.g. IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, Information Sciences, Science China Information Sciences and Vehicular Communications) and international conferences.



Lu Liu is the Professor of Informatics and Head of Department of Informatics in the University of Leicester, UK. Prof Liu received the Ph.D. degree from University of Surrey, UK and MSc in Data Communication Systems from Brunel University, UK. Prof Liu's research interests are in areas of cloud computing, service computing, computer networks and peer-to-peer networking. He is a Fellow of British Computer Society (BCS).