IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 7, 2018, accepted April 10, 2018, date of publication April 17, 2018, date of current version May 24, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2827365

Achieving Secure and Privacy-Preserving Incentive in Vehicular Cloud Advertisement Dissemination

QINGLEI KONG[1], (Student Member, IEEE), RONGXING LU[2], (Senior Member, IEEE), HUI ZHU[3], (Member, IEEE), AND MAODE MA[1], (Senior Member, IEEE)

[1]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798
[2]Faculty of Computer Science, University of New Brunswick, Fredericton, NB E3B 5A3, Canada
[3]School of Cyber Engineering, Xidian University, Xi'an 710071, China

Corresponding author: Qinglei Kong (qlkong@ntu.edu.sg)

This work was supported in part by MOE Tier 1, Singapore, under Grant M4011450, in part by the Project Development of NTU/NXP Smart Mobility Test-Bed under Grant S15-1105-RF-LLF, in part by NBIF Start-Up under Grant Rif 2017-012, and in part by URF under Grant 124419.

ABSTRACT The recent research trend of extending cloud computing to vehicles by leveraging under-utilized on-board capabilities [also known as vehicular cloud (VC)] is unsurprising, partly due to the increasing popularity of intelligent vehicles (with on-board computing equipment) and cloud computing. However, VC deployment is still challenging: how to securely verify responding vehicles, how to recruit competent vehicles, and how to achieve privacy preservation, are among the remaining research challenges. In this paper, we propose a secure and privacy-preserving incentive mechanism under the vehicular advertisement dissemination setting, which enables vehicles to opportunistically perform on-demand advertisement dissemination tasks and (financially) benefit from the completed task. Specifically, the road side unit (RSU) representing the advertisement dissemination server first announces a dissemination task, and performs the privacy-preserving access control of the responding vehicles. Then the RSU selects the participating vehicles among a pool of verified competent vehicles, and acknowledges the participation of selected vehicles with a secure secret sharing scheme; meanwhile, the selected vehicles performs the dissemination task with incentives. Finally, we prove the security of the proposed scheme in terms of secure access control and privacy preservation, and demonstrate its efficiency via simulation results (i.e., improves the amount of advertisement dissemination and brings incentives to participating vehicles).

INDEX TERMS Advertisement dissemination, incentive mechanism, privacy preservation, vehicular cloud.

I. INTRODUCTION

With the rapid development of the automotive industry as well as the information and communications technologies (ICT), intelligent vehicles are increasingly commonplace. Intelligent vehicles are equipped with various on-board devices (e.g., on-board computers, radio transceivers, storage equipment, and sensors), such that they can act as service providers; meanwhile, the concept of vehicular cloud (VC) is proposed to leverage the under-utilized on-board resources [1], [2]. Among all the promising applications provided by VC [3]–[5], vehicular advertisement dissemination is especially attractive, in which the road side unit (RSU) sends out commercial advertisements via vehicle-to-RSU (V2R) communication, and the receiving vehicles propagate the digital advertisements towards neighboring vehicles along with their moving trajectories [6]–[8]. Meanwhile, as the disseminated advertisements are normally relevant to merchants like garages and gas stations, which can help to maintain the normal operations of vehicles and further improve the traffic safety and driving experience.

Distinguished from the strong capability of the traditional cloud architecture [2], [9], whose resources are controlled by the cloud provider, VC is opportunistically and temporarily formulated by coordinating the distributive and limited residue resources in vehicles and roadside infrastructures [4]. In terms of advertisement dissemination, the propagating frequency and coverage of one vehicle is limited, and multiple vehicles are required to achieve the publicity effect. During

the vehicular advertisement dissemination process, the propagating operation would cost the on-board storage, transmission bandwidth, and energy resources. However, most of the service providing vehicles are privately owned and maintained, these (independent and selfish) vehicles are unlikely to avail their spare resources to the VC advertisement dissemination without any sort of compensation [10], and incentives are required to compensate for the resource consumption. In VC, a few incentive schemes are designed to stimulate the participation of service providers. A temporarily formulated VC data center application for airports is proposed in [11], where vehicles contribute their excess on-board capabilities with incentives. A hierarchical cloud architecture in vehicular networks is designed in [3], and the proposed scheme formulates a game-theoretical based strategy to achieve the resource coordination among vehicles. However, none of the existing scheme considers the problem of both developing an incentive mechanism to stimulate the participation of vehicles, while guaranteeing the fairness (in terms of task and incentive allocation) among the participating vehicles.

Another problem relates to the security and privacy preservation of the involved vehicles. On one hand, due to the lack of advertisement dissemination standardization, different softwares need to be installed for different advertisement dissemination systems, i.e., competence of vehicles need to be verified for each dissemination process [12]. On the other hand, the privacy of the participating vehicles should also be protected from other vehicles, since the vehicle's real identity and configuration setup could possibly be disclosed [13]. Without privacy preservation, vehicles are reluctant to involve in an announced task even offered with attractive incentives. Various anonymity schemes are proposed to hide the real-identities of vehicles [14], [15], however, in the proposed incentive mechanism, the real identities still needs to be learnt by the server for the incentive recording.

To address the above-mentioned challenges, we propose a secure and privacy-preserving incentive mechanism for VC. We deploy the proposed scheme in an advertisement dissemination setting, in which a road side unit (RSU) dynamically recruits vehicles for dissemination tasks. We regard the contributions of this paper to be three-fold:

1) We exploit an efficient single-attribute access control protocol to identify competent vehicles for advertisement dissemination tasks (registration and installation of the required software), while preserving the identity and configuration privacy of the responding vehicles. Meanwhile, a privacy-preserving secret sharing scheme is also developed to acknowledge participation of selected vehicles.
2) We devise an incentive mechanism to stimulate the competent participating vehicles, determine the dissemination strategy (when a unique Nash Equilibrium is achieved), and calculate the payment of the selected vehicles.
3) Detailed security analysis are performed to achieve the security goals of secure access control, privacy preservation and data integrity. Meanwhile, we compare the performance of the proposed incentive mechanism with the fixed price strategy, which greatly increases the amount of advertisement dissemination.

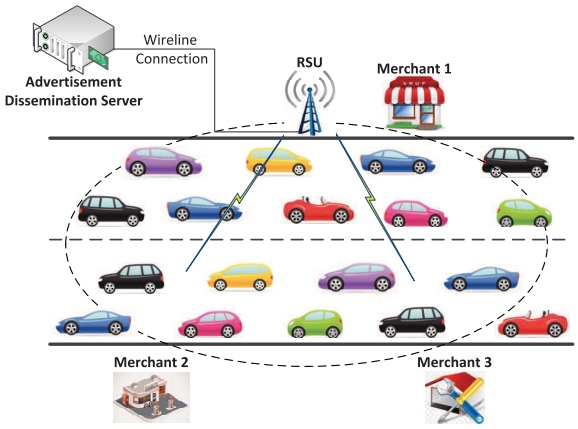

FIGURE 1. A vehicular cloud (VC) advertisement dissemination model.

The rest of this paper is structured as follows. We introduce our system model, present our security requirements, and identify our design goals in Section II. Then we present our proposed privacy preserving incentive scheme in Section III. The security analysis and performance evaluations are shown in Sections IV and V, respectively. Related work is described in Section VI, and we conclude the paper in Section VII.

II. SYSTEM MODEL, SECURITY REQUIREMENTS, AND DESIGN GOALS

In this section, we introduce the system model, present the security requirements, and identify the design goals.

A. SYSTEM MODEL

As shown in Fig. 1, we present the architecture of the proposed VC advertisement dissemination system. Analogous to the digital version of traditional static billboards, vehicles broadcasts advertisements encapsulated in beacon data towards neighboring vehicles in vehicular ad hoc networks (VANETs) [16]. In this paper, the proposed system model consists of three entities: an advertisement dissemination server (ADS), RSUs, and vehicles.

- *ADS* is owned and maintained by a commercial advertisement company [17]; meanwhile, it specifies dissemination details (i.e., mechants, coverage, duration, and frequency), and it forwards advertisement content and specifications to relevant RSUs. Due to contractual agreement with the RSU vendors (e.g. municipal traffic management centers), it can communicate securely with RSUs via wired links. The server also maintains an account for each registered vehicle to record the incentives earned from joining in the dissemination tasks, and the incentives can also be exploited to pay for

traffic-related expenses (e.g. highway toll fees, parking fees, and speeding fines).

- Each *RSU* is deployed along the street, and acts as in interface between the ADS and vehicles. After receiving an advertisement dissemination task, the RSU selects competent vehicles, assigns dissemination tasks towards selected vehicles, and delivers advertisements to vehicles [18].
- *Vehicles* are equipped with on-board computers and radio transceivers, such that a dynamically moving vehicle with under-utilized capability can actually participate in the VC advertisement dissemination system as a service provider through propagating advertisements to other vehicles. Meanwhile, vehicles are responsible for disseminating the commercial advertisements with the some existing algorithms [19], [20], along their moving trajectory and further increase the effect of publicity.

Communication Model: The the vehicle-to-RSU (V2R) and vehicle-to-vehicle (V2V) communications are realized through the IEEE 802.11p Wireless Access for Vehicular Environment (WAVE) standard [21], which is a short to medium range communication technology operating at 5.9 GHz band. The connection between the RSU and the ADS is realized through secure wired link with high bandwidth and low transmission delay.

B. SECURITY REQUIREMENTS

Security is critical for the successful operation of the proposed secure incentive mechanism in VC. In the security model, we consider the advertisement server is fully trusted and tamper-proof. Since the RSUs are deployed and managed by the municipal traffic management centers (in most cases), the RSUs are also considered to be fully trusted. As the participating vehicles are independently owned and maintained, they are considered to be honest-but-curious. That is, the vehicles will correctly execute the defined dissemination process, but they are interested in learning the identities of other vehicles. In addition, we assume there exists an adversary, which may launch some active attacks to modify data transmission. Specifically, in the proposed scheme, we take three security requirements into consideration.

1) ACCESS CONTROL

Since there is no standardization, different software may be installed for different advertisement dissemination systems. The access control of a responding vehicle guarantees the installation of the required software and the registration of the vehicle.

2) PRIVACY PRESERVATION

To protect each responding vehicle from revealing its personally identifiable information, the private information of one vehicle should be protected from the rest of vehicles. In the proposed incentive mechanism, the identity, configuration setup, and dissemination strategy of each involved vehicle, should not be learnt by any other vehicle.

3) DATA INTEGRITY

The proposed scheme should be able to verify that each received message has not been modified during data transmission, even if an adversary modifies the data transmission, the malicious behavior should be detected by the receivers. In this way, the security requirement of data integrity could be satisfied.

C. DESIGN GOALS

In the proposed scheme, our design goal is to develop a secure and privacy-preserving incentive mechanism in VC under the advertisement dissemination setting. Specifically, the following three goals should be achieved:

The proposed scheme should achieve the above security requirements. If the proposed scheme does not take the defined security requirements into consideration, the eligibility of the recruited vehicles could not be guaranteed, private information (including identities, configurations, and strategies) of the selected vehicles could be threatened, and the data integrity of data transmission could be violated. Then the advertisement dissemination system cannot function properly.

The proposed scheme should guarantee the fairness of the strategies and incentives. RSU should guarantee the fairness of the dissemination strategy and incentive distribution among the participating vehicles. Meanwhile, the proposed scheme should maximize the amount of advertisement dissemination. In addition, the ADS should be able to accurately record the incentive distributed to each participating vehicle.

The proposed scheme should achieve high efficiency in computation complexity. Computation efficiency should be achieved in the proposed incentive mechanism, i.e., both RSUs and participating vehicles need to perform minimum computation operation during the advertisement dissemination process.

III. PROPOSED INCENTIVE MECHANISM FOR VEHICULAR CLOUD

In this section, we present the proposed incentive mechanism under an advertisement dissemination setting, and we mainly focus on the interaction between one RSU and a group of vehicles. Before the description of the proposed scheme, we first revisit the concept of the bilinear pairing technique, which serves as the basis of our proposed incentive mechanism.

A. BILINEAR PAIRINGS

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative groups with the same prime order q. The bilinear map e: $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ has the following properties:

1) Bilinearity: $\forall g, h \in \mathbb{G}$, and $\forall a, b \in \mathbb{Z}_q^*$, we can derive $e(g^a, h^b) = e(g, h)^{ab}$;

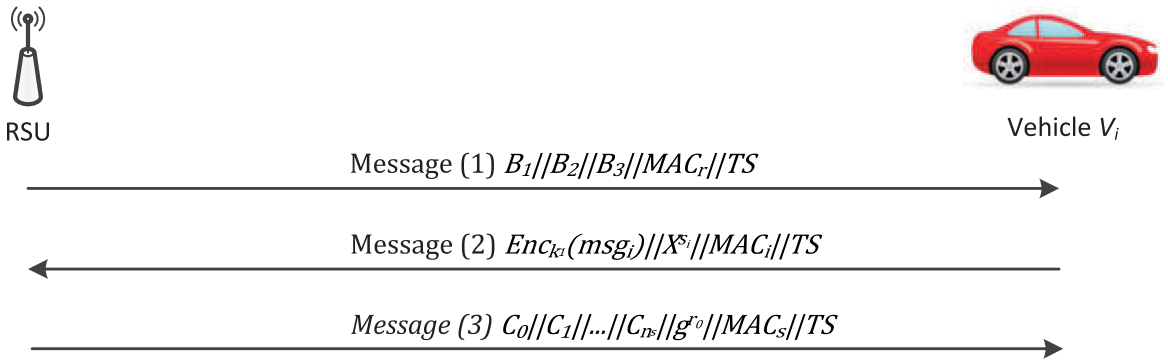

FIGURE 2. Message flow of the proposed privacy preserving incentive mechanism.

2) Nondegeneracy: There exist $g \in \mathbb{G}$ and $h \in \mathbb{G}$, satisfy the condition that $e(g, h) \neq 1_{\mathbb{G}_T}$.

3) Computable: $\forall g, h \in \mathbb{G}$, there is an efficient algorithm to compute $e(g, h)$.

Definition 1: A bilinear parameter generator $\mathcal{G}en$ denotes a probabilistic algorithm that takes a parameter related to κ as the input, and gives a 5-tuple $(q, g, \mathbb{G}, \mathbb{G}_T, e)$ as the output, where q is κ-bit prime, $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups with order q, $g \in \mathbb{G}$ is a generator, and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is non-degenerated and computable bilinear map.

B. SYSTEM INITIALIZATION

In the system initialization phase, the ADS, which functions as the trusted authority (TA), will bootstrap the entire system. TA first generates a five-tuple bilinear parameter $(q, g, \mathbb{G}, \mathbb{G}_T, e)$ by running $\mathcal{G}en(\kappa)$. It also selects a secure encryption algorithm $\mathcal{E}nc(\cdot)$, and one secure cryptographic hash functions, $H(\cdot) : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$. Then, TA selects two random numbers $(a, x) \in \mathbb{Z}_q^*$, chooses two random elements $(g_1, g_2) \in \mathbb{G}$, and computes $A = g^a$, $b = H(a)$, and $X = e(g, g)^x$. Finally, TA keeps the master key (a, b, x) in confidential, and publishes the system parameter $params = (q, g, \mathbb{G}, \mathbb{G}_T, e, H, g_1, g_2, A, X)$.

During the registration of each vehicle V_i with identity VID_i, the TA first checks its on-board computer configuration (memory, processor, etc.). If V_i satisfies the basic configurations, the ADS installs the advertisement dissemination software on V_i's on-board computer. Then the TA computes $(t_{i1}, t_{i2}) \in \mathbb{Z}_q^*$, where $t_{i1} = H(VID_i \| b \| 1)$ and $t_{i2} = H(VID_i \| b \| 2)$; meanwhile, the TA calculates the access control key ak_i, which is denoted as $ak_i = (g^{x+at_{i1}}, g^{t_{i1}}, g^{t_{i2}}, g_1^{t_{i1}} g_2^{t_{i2}})$, and securely delivers ak_i towards V_i.

C. COMPETENT VEHICLE ACCESS CONTROL

When the RSU receives an advertisement content with dissemination specifications from the ADS, the RSU first generates an access control vector to verify the competence of the responding vehicles [22]. The RSU selects a random number $r \in \mathbb{Z}_q^*$ to compute the value $e(g, g)^{x \cdot r}$ and the access control vector (B_1, B_2, B_3):

$$B_1 = g^r, \quad B_2 = A^r \cdot g_1^{-r}, \; B_3 = g_2^{-r}. \tag{1}$$

Then the RSU generates the message authentication code $MAC_r = H(B_1 \| B_2 \| B_3 \| TS)$, where TS is the current timestamp. The RSU broadcasts the dissemination task with the access control vector $B_1 \| B_2 \| B_3 \| MAC_r \| TS$ towards all the vehicles under its coverage (see *message (1)* in Fig. 2).

After receiving $B_1 \| B_2 \| B_3 \| MAC_r \| TS$, V_i first verifies the correctness of MAC_r, by computing $MAC_r \stackrel{?}{=} H(B_1 \| B_2 \| B_3 \| TS)$. If it verifies to be correct, V_i (which has the required software installed and intends to participate in the dissemination task) recovers the value $e(g, g)^{x \cdot r}$ with its access control key ak_i, which is

$$\begin{aligned} &\frac{e(B_1, g^{x+at_{i1}})}{e(B_2, g^{t_{i1}}) \cdot e(B_3, g^{t_{i2}}) \cdot e(B_1, g_1^{t_{i1}} g_2^{t_{i2}})} \\ &= \frac{e(g^r, g^{x+at_{i1}})}{e(g^{ar} g_1^{-r}, g^{t_{i1}}) \cdot e(g_2^{-r}, g^{t_{i2}}) \cdot e(g^r, g_1^{t_{i1}} g_2^{t_{i2}})} \\ &= \frac{e(g^r, g^x) \cdot e(g^r, g^{at_{i1}})}{e(g^{ar}, g^{t_{i1}}) \cdot e(g_1^{-r}, g^{t_{i1}}) \cdot e(g_2^{-r}, g^{t_{i2}}) \cdot e(g^r, g_1^{t_{i1}} g_2^{t_{i2}})} \\ &= e(g, g)^{x \cdot r}. \end{aligned} \tag{2}$$

Meanwhile, V_i determines the unit dissemination cost c_i based on the dissemination task and configurations, estimates the maximal dissemination capability M_i^{max} based on the current on-board computer usage, and formulates the message $msg_i = VID_i \| M_i^{max} \| c_i$. V_i also selects a random number $s_i \in \mathbb{Z}_q^*$, and computes $(X^{s_i}, k_i = H((e(g, g)^{x \cdot r})^{s_i} \| TS))$. In addition, V_i encrypts Msg_i with k_i and generates the message authentication code $MAC_i = H(msg_i \| X^{s_i} \| TS)$. Finally, V_i delivers $\mathcal{E}nc_{k_i}(msg_i) \| X^{s_i} \| MAC_i \| TS$ towards the RSU (see *message (2)* in Fig. 2).

After receiving $\mathcal{E}nc_{k_i}(msg_i) \| X^{s_i} \| MAC_i \| TS$, the RSU first obtains the message Msg_i with the private key k_i, where k_i is derived as $k_i = H((X^{s_i})^r \| TS)$. Then the RSU verifies the correctness of MAC_i by checking whether $MAC_i \stackrel{?}{=} H(msg_i \| X^{s_i} \| TS)$. If it verifies to be correct, V_i is verified to be installed with the required software.

D. INCENTIVE-BASED VEHICLE SELECTION

In this subsection, we first introduce the dissemination strategy of each participating vehicle, then we describe the competent vehicle selection process, which is the strategy of the RSU.

Given one dissemination task, the total reward announced by the RSU is denoted as $\mathcal{R}$, which is determined by the ADS according to the dissemination specifications (coverage, frequency, duration, etc.) [23]. To expand the disseminating range and increase the effect of publicity, multiple vehicles are recruited for one dissemination task. We also assume that there exist n verified responding vehicles, and n_s out of n vehicles are selected for the dissemination task. Since the participating vehicles are selfish and independently owned, each vehicle aims to maximize its utility. The optimization problem of $V_i, i = 1, \ldots, n$ is formulated as:

$$\begin{aligned} &max_{m_i}\ U_i(m_i) = \frac{m_i}{\sum_{l=1}^{n} m_l}\mathcal{R} - c_i m_i, \\ &s.t.\ (1)\ U_i \geq U_{th-min}, \\ &\quad (2)\ M_i^{max} \geq m_i \geq M_{th-min}, \end{aligned} \tag{3}$$

where $U_i(\cdot)$ denotes the utility of V_i, the dissemination strategy of V_i is m_i, and $\sum_{l=1}^{n} m_l$ represents the sum of the advertisement dissemination strategies of all the n selected vehicles. In Eq. (3), the first constraint indicates the minimum utility of V_i, i.e., the minimum profit U_{th-min} earned by V_i in the announced dissemination task. The second constraint restricts the maximum and minimum value of m_i, i.e., m_i should be less than the maximum dissemination capability M_i^{max} and higher than the minimum threshold M_{th-min}.

Let $\mathcal{M}$ denote the dissemination strategy space of all the participating vehicles, each vehicle determines its own strategy $m_i \in \mathcal{M}$. Let $\vec{m} = (m_1, m_2, \ldots, m_n) \in \mathcal{M}$ be the strategy vector of all the selected vehicles. To obtain the value of $\vec{m}$, we first introduce the definition of **Nash Equilibrium (NE)** within our application scenario.

Definition 2: A given dissemination strategy vector $\mathcal{M}^{NE} = (m_1^{NE}, m_2^{NE}, \ldots, m_n^{NE})$ is said to be a **Nash Equilibrium (NE)**, if it satisfies the following condition: $\forall i \in \{1, \ldots, n\}$, $U_i(m_i^{NE}, \mathcal{M}_{-i}^{NE}(m_i^{NE})) \geq U_i(m_i, \mathcal{M}_{-i}^{NE}(m_i))$.
where $\mathcal{M}_{-i}^{NE}(m_i)$ denotes the dissemination strategies of all the participating vehicles besides V_i when the dissemination strategy of V_i is m_i and an NE is achieved.

In order to derive the value of m_i^{NE}, we also prove the existence and uniqueness of NE. The existence of NE guarantees that all the participating vehicles are able to find their dissemination schemes, where no vehicle is able to improve its utility by unilaterally deviating from the derived strategy.

Theorem 1: There exists at least one NE in the advertisement dissemination task among the participating vehicles, if $\mathcal{M}$ is a non-empty, convex, and compact subset of some Euclidean space R^n and $U_i(m_i)$ is continuous in $\vec{m}$ and quasi-concave in m_i [24].

Proof: For each vehicle V_i, its strategy space is bounded by a minimum value M_{th-min} and a maximum value M_i^{max}. Thus, it is obvious that the dissemination strategy vector $\vec{m}$ is a non-empty, convex, and compact subset of the space R^n. According to its definition in Eq. (3), $U_i(m_i)$ is continuous in $\mathcal{M}$. Then we take the secondary-order derivative of $U_i(m_i)$ with respect to m_i to prove the concaveness of m_i, which is shown as following:

$$\frac{\partial^2 U_i}{\partial m_i^2} = \frac{-2m_i}{(m_i + \mathcal{M}_{-i})^3}\mathcal{R} < 0. \tag{4}$$

Since $U_i(m_i)$ is a strictly concave function in m_i, $U_i(m_i)$ must be a quasi-concave function in m_i. Thus, the existence of NE can be proved.

In addition, we prove the uniqueness of NE: the uniqueness of NE ensures that each selected vehicle can achieve only one dissemination strategy vector when a unique NE is achieved.

Theorem 2: There exists a unique NE in the advertisement dissemination task among the participating vehicles.

Proof: To prove the uniqueness of NE, we define the concept of the best response strategy (see *Definition* 3) [25].

Definition 3: Given the dissemination strategy $\mathcal{M}_{-i}$, if m_i^* maximizes $U_i(m_i, \mathcal{M}_{-i})$ over all possible values of m_i, then the value of m_i^* is viewed as the best response strategy.

Based on the concept of NE, each vehicle is performing its best response strategy when an NE is achieved [26]. To determine the best response strategy m_i^* of V_i, we take the first-order derivative of $U_i(m_i)$ with respect to m_i : $\frac{\partial U_i}{\partial m_i}$. Since U_i is a concave function with respect to m_i and $\partial^2 U_i/\partial m_i^2 < 0$, $\partial U_i/\partial m_i$ is a strictly decreasing function with respect to m_i. Then, the best response strategy of m_i can be derived as:

$$m_i^* = \begin{cases} M_i^{max}, & \partial U_i/\partial m_i > 0, \\ m_i^*, & \partial U_i/\partial m_i = 0, \\ M_{th-min}, & \partial U_i/\partial m_i < 0. \end{cases} \tag{5}$$

Thus, we can guarantee that there exists only one best response strategy m_i^* (as shown in Eq. (5)), and the uniqueness of the NE can be proved.

To derive the optimal value of m_i, we formulate the Lagrangian dual function of Eq. (3), which is

$$\begin{aligned} L_i(m_i, \lambda_i, \mu_i, \xi_i) = {} & U_i(m_i) + \lambda_i(U_i - U_{th-min}) \\ & + \mu_i(M_i^{max} - m_i) + \xi_i(m_i - M_{th-min}), \end{aligned} \tag{6}$$

where $\lambda_i, \mu_i, \xi_i, \forall i$ are the dual variables introduced. Given a fixed $\mathcal{M}_{-i}$, we differentiate L_i with m_i and apply the Karush-Kuhn-Tucker (KKT) condition [27]. Thus, the optimal dissemination strategy can be obtained as follows:

$$m_i^* = [\sqrt{\frac{(1+\lambda_i)\mathcal{M}_{-i}\mathcal{R}}{(1+\lambda_i)c_i + \mu_i - \xi_i}} - \mathcal{M}_{-i}]^+, \tag{7}$$

where $[x]^+ = max(0, x)$. The dual variables are updated with the following sub-gradient method:

$$\begin{aligned} \lambda_i(t+1) &= [\lambda_i(t) + \eta(U_i(m_i(t)) - U_{th-min})]^+ \\ \mu_i(t+1) &= [\mu_i(t) + \eta((M_i^{max} - m_i(t))]^+ \\ \xi_i(t+1) &= [\xi_i(t) + \eta(m_i(t) - M_{th-min})]^+, \end{aligned} \tag{8}$$

where η is the step size and t is the iteration index.

For the RSU, its utility function U_R is formulated as $U_R = \sum_{i=1}^{n} \alpha^n M_i$. Since the introduced computation complexity increase with the number of participating vehicles, we introduce a parameter $\alpha \in (0, 1)$ to denote the complexity of R_j. According to the expression of dissemination strategy m_i^* in Eq. (7), the value of m_i^* decreases with the increase of c_i. Therefore, we sort the verified competent vehicles from the lowest to the highest and label them 1 to n, which is denoted as $(\vec{c} = (c_1, \ldots, c_n))$. The participating vehicle selection and dissemination strategy calculation process of the RSU is shown in Algorithm 1.

Algorithm 1 VehicleSelection(n,$\vec{c}$,$\vec{M}^{max}$,M_{th-min},α)

Data:n,$\vec{c}$,$\vec{M}^{max}$,M_{th-min},α
Output:n_s, $\mathcal{R}^*$, U_R^*, $\vec{M}^*$

```
max_N = 0, max_U = 0, U_R(1) = 0
for n_s = 2 : n do
  for i = 1 : n_s do
    Calculates m_i^NE(n) using Eq. (7)(8):
  end for
  Calculates U_R(n_s) = Σ_{i=1}^{n_s} α^{n_s} m_i^NE(i);
  if U_R(n_s) > max_U then
    max_N = n_s, max_U = U_R(n_s)
  end if
end for
n_s = max_N, U_R(n_s) = max_U
```

E. SELECTED VEHICLES ANNOUNCEMENT

When the set of n_s participating vehicles is determined, the RSU acknowledges the participation of the selected vehicles with privacy preservation. The RSU selects two random variables $r_0 \in \mathbb{Z}_q^*$ and $y \in \mathbb{Z}_q^*$, and performs the following computation process

$$\begin{aligned}&\prod_{i=1}^{n_s}(y - k_i) + r_0 \\ &= y^{n_s} + \sum_{i=1}^{n_s}(-1)k_i y^{n_s-1} + \ldots + (-1)^{n_s}\prod_{i=1}^{n_s} k_i + r_0 \\ &= c_{n_s} y^{N_p} + c_{n_s-1} y^{n_s-1} + \ldots + c_0 \end{aligned} \tag{9}$$

Then R_j calculates the values $C_l = g^{c_l}, l = 0, 1, \ldots, n_s$, generates the corresponding message authentication code $MAC_s = H_1(C_0 \| C_1 \| \ldots \| C_{n_s} \| g^{r_0} \| TS)$, and publishes $C_0 \| C_1 \| \ldots \| C_{n_s} \| g^{r_0} \| MAC_s \| TS$ (see *message (3)* in Fig. 2).

After receiving $C_0 \| C_1 \| \ldots \| C_{n_s} \| g^{r_0} \| MAC_s \| TS$, V_i first verifies the correctness of MAC_s by checking $MAC_s \stackrel{?}{=} H_1(C_0 \| C_1 \| \ldots \| C_{n_s} \| g^{r_0} \| TS)$. If it verifies to be correct, it calculates whether

$$\prod_{l=0}^{n_s} C_l^{(k_i)^l} \stackrel{?}{=} g^{r_0} \tag{10}$$

If the above equation verifies to be equal, V_i learns itself to be selected for the dissemination process. Otherwise, V_i is not selected for the dissemination task.

Correctness Analysis: To validate the correctness of Eq. (10), we perform the following computation process:

$$\begin{aligned}\prod_{l=0}^{n_s} C_l^{(k_i)^l} &= (g^{c_{n_s}})^{(k_i)^{n_s}} \cdot (g^{c_{n_s-1}})^{(k_i)^{n_s-1}} \cdots g^{c_0} \\ &= g^{k_i^{n_s}} \cdot g^{\sum_{z=1}^{n_s}(-1)k_z k_i^{n_s-1}} \cdots g^{\prod_{z=1}^{n_s}(-1)^{n_s} k_z + r_0} \\ &= g^{\prod_{z=1}^{n_s}(k_i - k_z) + r_0} = g^{r_0}. \end{aligned} \tag{11}$$

Upon the completion of the advertisement dissemination task, the participating vehicles complete the task first and obtain their payments after the dissemination duration, similar to the incentive mechanism proposed in [28].

IV. SECURITY ANALYSIS

In the section, we analyze the security properties of the proposed secure and privacy-preserving incentive mechanism. To be more specific, we are concerned with the following three aspects: how does the proposed incentive scheme achieve access control, how does the proposed incentive mechanism achieve privacy preservation, and how does the proposed incentive mechanism guarantee data integrity.

A. THE PROPOSED SECURE INCENTIVE MECHANISM CAN ACHIEVE THE ACCESS CONTROL OF RESPONDING VEHICLES

To achieve the access control of responding vehicles, the proposed scheme exploits a single attribute encryption technique proposed in [29], which is demonstrated to be secure in the spirit of cipher plaintext attack indistinguishability. Given $(B_1 = g^r, B_2 = A^r \cdot g_1^{-r}, B_3 = g_2^{-r})$, only registered vehicles (with the access control key ak_i) can recover the value $e(g, g)^{x \cdot r}$, due to the unforgeable on $e(g, g)^{x \cdot r}$ of the exploited attribute encryption technique. Thus, in the proposed incentive mechanism, the security goal of access control can be achieved, which guarantees the registration and software installation of the verified vehicles.

B. THE PROPOSED SECURE INCENTIVE SCHEME CAN ACHIEVE THE PRIVACY PRESERVATION OF RESPONDING VEHICLES

During the access control phase, to achieve privacy preservation of the responding vehicles, the identity and configuration setup are encrypted by the session key k_i, which is established between V_i and the RSU with the Diffie-Hellman key exchange protocol and it prevents privacy disclosure of a responding vehicle towards any other entity besides the RSU. During the selected vehicles acknowledgement phase, the RSU generates a set of values according to the session keys shared with the verified responding vehicles. Since k_i is only shared between the RSU and V_i, the proposed scheme achieves the acknowledgement of the selected responding vehicles with privacy preservation. Due to the hardness of the discrete logarithm algorithm, given C_j, it is difficult to obtain the value of c_j, and further recover the value of $k_i, i = 1, \ldots, n$. Thus, the proposed incentive

mechanism achieves the privacy preservation of the responding vehicles.

C. THE PROPOSED SECURE INCENTIVE SCHEME CAN PROTECT DATA INTEGRITY OF DATA TRANSMISSION

During the task announcement phase, to protect the data integrity of the access control vector $B_1\|B_2\|B_3$, a message authentication code MAC_r is attached in Fig. 2 (*message (1)*). Furthermore, in Fig. 2 (*message (2)*), a message authentication code MAC_i is also generated to protect the data integrity of Msg_i. In addition, the data integrity of $C_0\|C_1\|\ldots\|C_n\|g^{r_0}$ is preserved by a message authentication code MAC_s in Fig. 2 (*message (3)*). Thus, the data integrity of all the messages are guaranteed in the proposed scheme.

Based on the above security analysis, we conclude that the proposed incentive mechanism can achieve the security goals of access control, privacy preservation and data integrity.

V. PERFORMANCE EVALUATIONS

In this section, we evaluate the performance of the proposed secure incentive scheme under the VC advertisement dissemination setting. Specifically, we evaluate and compare the computation overheads introduced towards the RSU and each vehicle; meanwhile, we analyze and compare the numerical performance of the proposed incentive scheme in terms of the amount of dissemination.

A. COMPUTATION COMPLEXITY

We analyze the computation complexity introduced by the proposed scheme. During the access control phase, the RSU performs 4 exponentiation operations in $\mathbb{G}$ and 1 exponentiation operation in $\mathbb{G}_T$. We denote the exponentiation operations in $\mathbb{G}$ and $\mathbb{G}_T$ as $T_{e,1}$ and $T_{e,2}$, respectively; meanwhile, a single bilinear pairing operation in $\mathbb{G}$ is represented as T_b. In comparison of the exponentiation and bilinear pairing operations, other operations are considered to be negligible. Then each responding vehicle performs 4 bilinear pairing operations to generate the verification vector, conducts 2 exponentiation operations in $\mathbb{G}_T$ to generate the response message. When there exist n responding vehicles, the computational overhead introduced to the RSU is calculated as $(n+1)*T_{e,2}$ after receiving the response messages. During the secure acknowledgement phase, if n_s out of n vehicles are selected for participation, the RSU performs (n_s+2) exponentiation operations in $\mathbb{G}_T$ to generate the vector; meanwhile, each vehicle conducts (n_s+1) exponentiation operations in $\mathbb{G}_T$ for verification. Therefore, when n_s out of n vehicles are selected for participation, the total computational overhead of each vehicle and RSU are $T_v = 4*T_b+(n_s+1)*T_{e,1}+2*T_{e,2}$ and $T_r = (n_s+6)*T_{e,1}+(n+1)*T_{e,2}$.

To identify the efficiency of the proposed scheme, we compare the access control and secure acknowledgement scheme with the group signature technique [30] exploited in [31]. Each vehicle consumes 9 exponentiation operations in $\mathbb{G}$, 3 bilinear pairing operations, and 3 exponentiation operations in $\mathbb{G}_T$, in order to generate an access control vector. Then the RSU performs 8 exponentiation operations in $\mathbb{G}$, 4 bilinear pairing operations, and 4 exponentiation operations in $\mathbb{G}_T$ to verify the competence of the received vector. Meanwhile, we keep the selected vehicles announcement phase in our proposed scheme. Thus, the computational overhead in the compared scheme of each vehicle and RSU are $T_v^{'} = 3*T_b+(n_s+10)*T_{e,1}+3*T_{e,2}$ and $T_r^{'} = 4*n*T_b+(8*n+n_s+2)*T_{e,1}+4*n*T_{e,2}$.

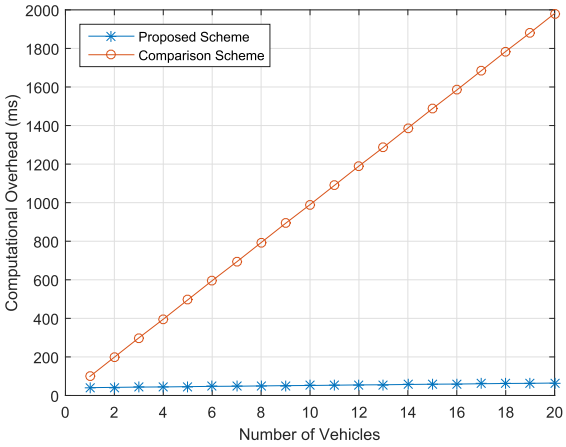

FIGURE 3. Comparison of the computational delay of the RSU.

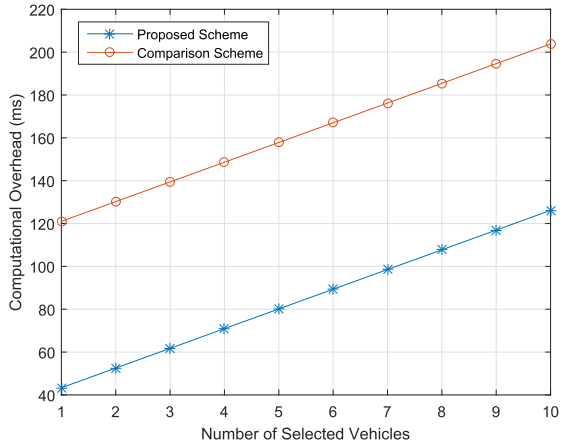

FIGURE 4. Comparison of the computational delay of the vehicle.

We test the latency with Java Pairing-Based Library Type-A pairing [32] 1,000 times, while the experiment environment setup is based on a personal computer with one dual-processor Intel Core 3.40 GHz CPU with 8.00 GB RAM. The computational costs are denoted as $T_{e,1} = 9.20\ ms$, $T_{e,2} = 0.75\ ms$, and $T_b = 5.86\ ms$. In Fig. 3 and Fig. 4, we compare the computational overheads introduced towards the RSU and each vehicle in terms of the proposed scheme and the scheme in comparison. As shown in Fig. 3 and Fig. 4, the proposed scheme greatly improves the computational overhead.

B. NUMERICAL ANALYSIS OF INCENTIVE MECHANISM

For the proposed incentive mechanism, we compare the proposed incentive mechanism with the fixed price scheme.

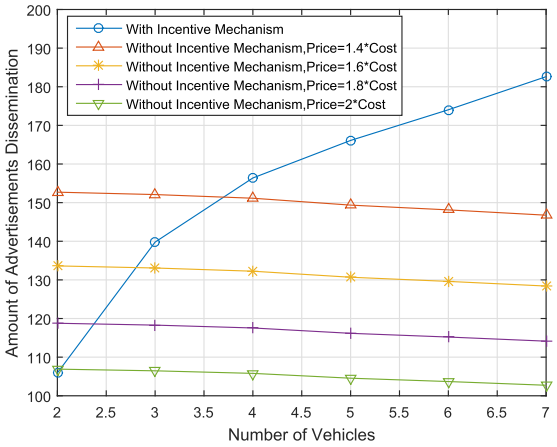

FIGURE 5. Comparison of the dissemination with fixed reward strategy.

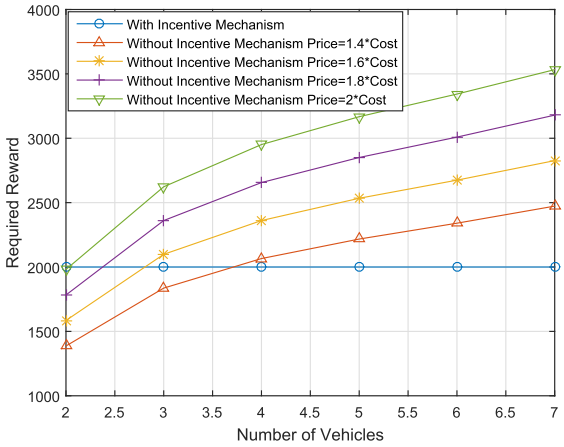

FIGURE 6. Comparison of reward with fixed amount of dissemination.

In the fixed price scheme, the unit dissemination price is fixed. To be more specific, the unit dissemination price is defined to be p, the value of m_i is calculated is $m_i = \mathcal{R}/(p * n_s)$. The utility of V_i, $\forall i$ in the fixed price strategy is calculated as $U_i^f = (p - c_i) * m_i$, i.e., the amount of advertisement dissemination multiplies price minus the amount of advertisement dissemination multiplies cost. Meanwhile, the utility function of the RSU is also expressed as $U_r^f = \sum_{i=1}^{n_s} \alpha^{n_s} * m_i$.

In Fig. 5, we compare the amount of advertisements dissemination achieved by the proposed scheme with that in the fixed price strategy with the number of participating vehicles, when the value of the reward $\mathcal{R}$ is set to be 2000 and the average value of the unit cost c_i, $\forall i$ is set to be 10. We assume that the unit dissemination price in the fixed price strategy p_i is set to be 1.4 to 2.0 times of the unit cost c_i. When the number of vehicles is small, the total amount of dissemination achieved by the proposed scheme, is less than the fixed reward strategy when p_i is set to be 1.4 times of c_i. This is because, when $\mathcal{R} = 2000$, the amount of dissemination achieved in the fixed strategy is higher than the total amount of dissemination achieved by the proposed scheme. However, in the proposed incentive mechanism, the total amount of dissemination increases with respect to the increase of the number of vehicles. In Fig. 6, given the fixed amount of advertisement dissemination, we compare the reward $\mathcal{R}$ required to achieve the given amount of advertisement dissemination with respect to the increase of the number of vehicles, when the price of dissemination p_i is set to be 1.4 to 2.0 times of c_i.

Fig. 5 and Fig. 6 show that the proposed incentive mechanism can disseminate more advertisements than the fixed reward strategy when the price of the computation is higher than 1.6 times of the cost, which is highly plausible that the vehicles are likely to earn more from joining the dissemination task and their prices are usually set to be more than twice their costs.

Fig. 7 examines the utility of the RSU with respect to the increase of the number of vehicles, when the value of α ranges from 0.85 to 1. As shown in Fig. 7, the optimal

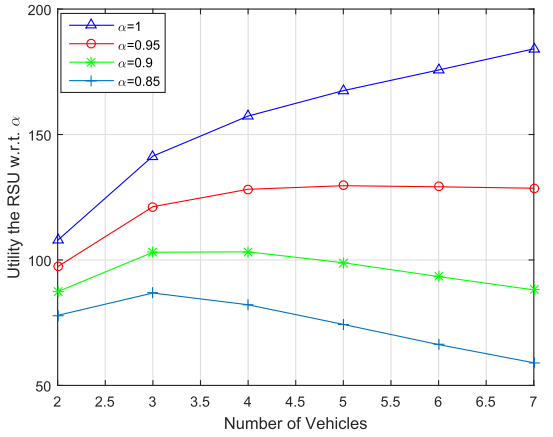

FIGURE 7. Utility of RSU with number of vehicle under different α.

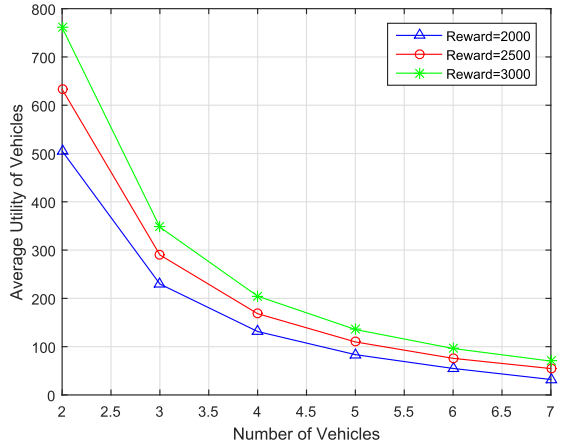

FIGURE 8. Utility of vehicle with number of vehicle.

number of the participating vehicles are 7, 5, 4, and 3, when the corresponding value of α are set to be 1, 0.95, 0.9, and 0.85, respectively.

Fig. 8 to Fig. 10 show the performance of the proposed incentive scheme from the perspective of vehicles. Fig. 8 shows the average utility one vehicle earned from

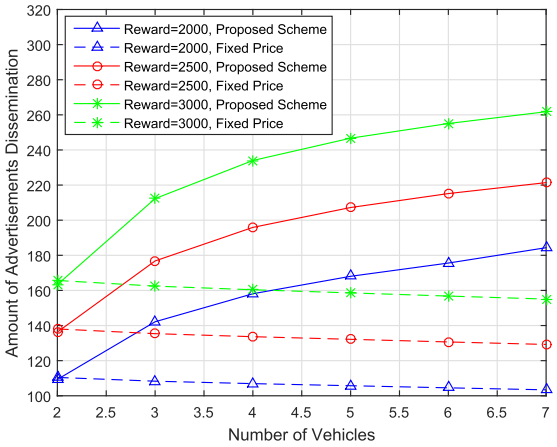

FIGURE 9. Amount of dissemination with number of vehicle.

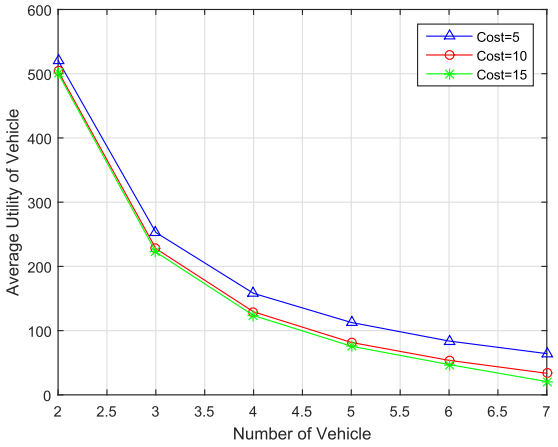

FIGURE 10. Utility of vehicle with number of vehicles.

participating in the dissemination task, when the average dissemination cost of each involved vehicle is set to be 10. Meanwhile, the value of the reward $\mathcal{R}$ is set to be $2,000$, $2,500$, and $3,000$, respectively, and p_i is set to be twice the cost c_i in the fixed reward strategy. Fig. 9 compares the total amount of advertisement dissemination of the vehicles in the proposed incentive scheme with that in the fixed reward scheme, under the same average utility of the participating vehicles in Fig. 8. That is, to earn the same utility achieved in Fig. 8, the amount of advertisements can be disseminated in the fixed reward strategy, when the fixed dissemination price is set to be 1.4 to 2.0 times the cost. The amount of dissemination in the fixed reward strategy decreases with the number of vehicles, this is because the average utility of each selected vehicle decreases, as shown in Fig. 8.

Fig. 10 shows the average utility of the involved vehicles, when the average cost of dissemination is set to be 5, 10, and 15, respectively. Fig. 11 compares the total amount of advertisements disseminated by the vehicles in the proposed incentive mechanism with that in the fixed price strategy, where we set the reward to be $2,000$, and the price are set to be twice the cost. The amount of dissemination done by the vehicles decreases with the average cost of dissemination in both the proposed incentive mechanism and the fixed reward strategy.

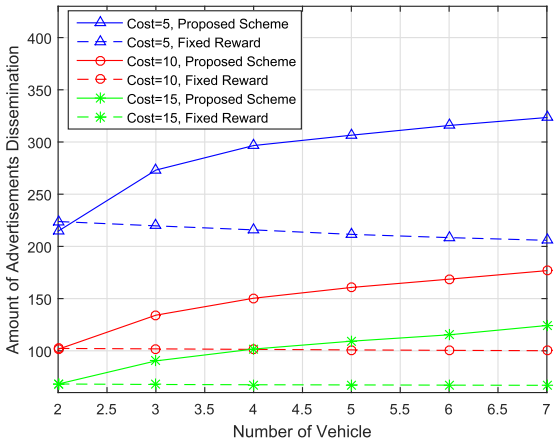

FIGURE 11. Amount of dissemination with number of vehicles.

VI. RELATED WORK

In this section, we briefly review some works tightly related to our work, in the aspects of incentive mechanism, access control in vehicular networks.

A. INCENTIVE MECHANISMS

In cloud computing, service providers (e.g., Microsoft, Amazon, etc.) are offering cloud hosting user applications under a utility pricing model, and the most commonly utilized scheme is the pay-as-you-go pricing mode, where users pay the per-unit resource (e.g.,a virtual machine) per-unit time (e.g.,an hour) [2], [9]. Jain *et al.* [9] have introduced a flexible pricing and resource allocation approach for tasks on cloud systems, in which each cloud user submits a task with an utility function that indicate its willingness to pay as a function of completion time. Prasad and Rao [2] have proposed a resource procurement method in cloud, which can not only automatically select a suitable cloud vendor, but also dynamically price for the uploaded services. In [33], a game-theoretic model of behavior for online question and answer forums has been proposed. In order to encourage participation, the asker provided incentives for early responders as well as user who submits the final answer. However, in a cloud computing environment, the service providers are fixed. This is somewhat different from our dynamically changing VC scenario, where the number of service providers (i.e. vehicles) adapts to the opportunistically changing surrounding environment and the completion of a task requires the collaboration of multiple vehicles. In VCs [11], vehicles are encouraged to rent their spare resources to the parking cloud data center, since vehicles located in parking lots for a relatively long period of time. Free parking, shopping coupons, or virtual credits for other relevant services would then be allocated to participating vehicles as compensation. A secure architecture was presented to encourage the participation of under-utilized

vehicles to participate in traffic management by issuing them traffic tokens, which can be used to pay for service from the cloud [10]. Under the advertisement dissemination setting, the authors have presented a secure incentive framework which stimulates for vehicular advertisement system in [6], and the proposed scheme exploits the receipts of advertisement receivers as the incentive for the ad forwarding vehicles. Li *et al.* [34] proposed an incentive-centered architecture to encourage cooperative vehicles to involve in advertisement dissemination, and propose a cash-in algorithm to advocate vehicular nodes to join in forwarding ad packets. However, none of the above works consider the problem of how to stimulate vehicles to join in and collaboratively conduct a task, and distribute the payments to the vehicles with fairness.

B. SECURE ACCESS CONTROL IN VCS

In VCs, an attacker could provide or access the same resources as their targets; meanwhile, the VC is vulnerable to risks associated with both vehicular networks and cloud computing, and it is challenging to distinguish an attacker from a normal service provider or user [13]. A few novel secure and privacy preserving access control schemes have been designed in vehicular networks [30], [35]–[38]. To distinguish malicious attackers from legitimate nodes in VANETs, a secure scheme has been proposed to verify the identities of the users prior to the access to the network [35]. A secure and privacy-preserving scheme with the group and identity-based signature has been proposed in [30], where the security goals of authentication and anonymity can be achieved. However, the computational overheads introduced by the group signature schemes are high, which may not be applicable to applications with intermittent connection and stringent delay requirement. To support the differentiated access control requirement, a privacy-preserving authentication and access control scheme has been proposed in [36]. However, the proposed scheme is designed for the service request application, which cannot be applied to our vehicle selection scenario. In [37], an indistinguishable credential scheme has been proposed, which enables a user to retrieve and utilize credentials for navigation service. However, the proposed scheme faces the problem of scalability and is not adaptive to the scenario when vehicles are recruited on-demand.

However, none of these studies considers both the privacy-preserving verification and incentive-based competent vehicles selection. A secure and privacy-preserving incentive framework between vehicles is proposed in [31], the mutual verification between vehicles is realized through the group signature technique; meanwhile, both the incentives of the task announcing vehicle and selected participating vehicles need to be maximized. In our work, we combine a secure access control scheme for the competent vehicles and a privacy-preserving incentive mechanism between the RSU and vehicles is designed, in order to stimulate the participation of disseminating vehicles.

VII. CONCLUSION

In this paper, we have proposed a secure and privacy-preserving incentive mechanism for VC advertisement dissemination, where an RSU verifies the responding vehicles with an access control scheme, selects participating vehicles for the dissemination task with an incentive mechanism, and acknowledges the selected vehicles for their participation with a secret sharing scheme. Security analysis proved that our proposed scheme achieves secure service provider access control, privacy preservation and data integrity protection. We also demonstrated the practicality of the scheme through simulations, i.e., it reduced the computational overhead and improves the amount of dissemination with fairness. Future research includes deploying the proposed scheme in a real-world setting, the NTU-NXP smart mobility Testbed project, with the aims of validating and refining the scheme.

REFERENCES

[1] S. Olariu, T. Hristov, and G. Yan, "The next paradigm shift: From vehicular networks to vehicular clouds," in *Mobile Ad Hoc Networking Mobile Ad Hoc Networking: Cutting Edge Directions*, 2nd ed. Hoboken, NJ, USA: Wiley, 2013.

[2] A. S. Prasad and S. Rao, "A mechanism design approach to resource procurement in cloud computing," *IEEE Trans. Comput.*, vol. 63, no. 1, pp. 17–30, Jan. 2014.

[3] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud-based vehicular networks with efficient resource management," *IEEE Netw.*, vol. 27, no. 5, pp. 48–55, Sep./Oct. 2013.

[4] E. Lee, E.-K. Lee, M. Gerla, and S. Y. Oh, "Vehicular cloud networking: Architecture and design principles," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 148–155, Feb. 2014.

[5] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *J. Netw. Comput. Appl.*, vol. 40, pp. 325–344, Apr. 2014.

[6] S. B. Lee, J. S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2715–2728, Jul. 2012.

[7] J. Qin, H. Zhu, Y. Zhu, L. Lu, G. Xue, and M. Li, "POST: Exploiting dynamic sociality for mobile advertising in vehicular networks," in *Proc. IEEE INFOCOM*, May 2014, pp. 1761–1769.

[8] H. Zheng and J. Wu, "Optimizing roadside advertisement dissemination in vehicular cyber-physical systems," in *Proc. 35th IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Columbus, OH, USA, Jun./Jul. 2015, pp. 41–50.

[9] N. Jain, I. Menache, J. Naor, and J. Yaniv, "A truthful mechanism for value-based scheduling in cloud computing," *Theory Comput. Syst.*, vol. 54, no. 3, pp. 388–406, 2014.

[10] K. Lim, I. M. Abumuhfouz, and D. Manivannan, "Secure incentive-based architecture for vehicular cloud," in *Proc. Int. Conf. Ad-Hoc Netw. Wireless*, Athens, Greece, Jun./Jul. 2015, pp. 361–374.

[11] S. Arif, S. Olariu, J. Wang, G. Yan, W. Yang, and I. Khalil, "Datacenter at the airport: Reasoning about time-dependent parking lot occupancy," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 11, pp. 2067–2080, Nov. 2012.

[12] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017.

[13] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 284–294, Mar. 2013.

[14] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[15] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, Sep. 2010.

[16] X. Li *et al.*, "On-road ads delivery scheduling and bandwidth allocation in vehicular CPS," in *Proc. INFOCOM*, Apr. 2013, pp. 2571–2579.

[17] Y. Lim and S. Ahn, "Design of commercial ads dissemination system in vehicular environments," *IETE Techn. Rev.*, vol. 29, no. 3, pp. 248–256, 2012.
[18] D. Baby, R. D. Sabareesh, R. A. K. Saravanaguru, and A. Thangavelu, "VCR: Vehicular cloud for road side scenarios," in *Advances in Computing and Information Technology*. Berlin, Germany: Springer-Verlag, 2013, pp. 541–552.
[19] M. Sardari, F. Hendessi, and F. Fekri, "Infocast: A new paradigm for collaborative content distribution from roadside units to vehicular networks," in *Proc. 6th Annu. IEEE Commun. Soc. Conf. Sens., Mesh Ad Hoc Commun. Netw. (SECON)*, Rome, Italy, Jun. 2009, pp. 1–9.
[20] N. Cenerario, T. Delot, and S. Ilarri, "A content-based dissemination protocol for VANETs: Exploiting the encounter probability," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 771–782, Sep. 2011.
[21] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.
[22] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 3, pp. 614–624, Mar. 2013.
[23] S.-G. Sim and H. Lee. (Dec. 22, 2017). *Input Price Discrimination, Advertisement Efforts, and Welfare*. [Online]. Available: https://ssrn.com/abstract=2633111
[24] L. Cong, L. Zhao, K. Yang, H. Zhang, and G. Zhang, "A Stackelberg game for resource allocation in multiuser cooperative transmission networks," *Wireless Commun. Mobile Comput.*, vol. 11, no. 1, pp. 129–141, 2011.
[25] R. D. Yates, "A framework for uplink power control in cellular radio systems," *IEEE J. Sel. Areas Commun.*, vol. 13, no. 7, pp. 1341–1347, Sep. 1995.
[26] P. Zhou, W. Yuan, W. Liu, and W. Cheng, "Joint power and rate control in cognitive radio networks: A game-theoretical approach," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Beijing, China, May 2008, pp. 3296–3301.
[27] Z.-Q. Luo and W. Yu, "An introduction to convex optimization for communications and signal processing," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 8, pp. 1426–1438, Aug. 2006.
[28] M. M. E. A. Mahmoud and X. Shen, "FESCIM: Fair, efficient, and secure cooperation incentive mechanism for multihop cellular networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 5, pp. 753–766, May 2012.
[29] R. Lu, X. Lin, X. Liang, and X. S. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in *Proc. 5th ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS)*, Beijing, China, Apr. 2010, pp. 282–292.
[30] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[31] Q. Kong, R. Lu, H. Zhu, A. Alamer, and X. Lin, "A secure and privacy-preserving incentive framework for vehicular cloud on the road," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Washington, DC, USA, Dec. 2016, pp. 1–6.
[32] A. D. Caro and V. Iovino, "JPBC: Java pairing based cryptography," in *Proc. 16th IEEE Symp. Comput. Commun. (ISCC)*, Corfu Island, Greece, Jun./Jul. 2011, pp. 850–855.
[33] S. Jain, Y. Chen, and D. C. Parkes, "Designing incentives for online question-and-answer forums," *Games Econ. Behavior*, vol. 86, pp. 458–474, Jul. 2014.
[34] Z. Li, C. Liu, and C. Chigan, "On secure VANET-based ad dissemination with pragmatic cost and effect control," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 124–135, Mar. 2013.
[35] A. Daeinabi and A. G. Rahbar, "Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks," *Multimedia Tools Appl.*, vol. 66, no. 2, pp. 325–338, Sep. 2013.
[36] L.-Y. Yeh, Y.-C. Chen, and J.-L. Huang, "PAACP: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks," *Comput. Commun.*, vol. 34, no. 3, pp. 447–456, 2011.
[37] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "VSPN: VANET-based secure and privacy-preserving navigation," *IEEE Trans. Comput.*, vol. 63, no. 2, pp. 510–524, Feb. 2014.
[38] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, "LESPP: Lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication," *Computing*, vol. 98, no. 7, pp. 685–708, 2016.

QINGLEI KONG (S'15) received the B.Eng. degree in communication engineering from the Harbin Institute of Technology, Harbin, China, in 2012, and the M.Eng. degree in electronic and information engineering from the Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, China, in 2015. She is currently pursuing the Ph.D. degree with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. Her research interests include wireless communications, VANET, and game theory.

RONGXING LU (SM'15) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Canada, in 2012. He was a Post-Doctoral Fellow with the University of Waterloo from 2012 to 2013. He was an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from 2013 to 2016. He has been an Assistant Professor with the Faculty of Computer Science, University of New Brunswick (UNB), Canada, since 2016. He has published extensively in his areas of expertise (with over 11 100 citations and H-index 51 from Google Scholar as of 2018). His research interests include applied cryptography, privacy enhancing technologies, and IoT-big data security and privacy. He was a recipient of the most prestigious Governor Generals Gold Medal, the 8th IEEE Communications Society Asia Pacific Outstanding Young Researcher Award in 2013, and eight best (student) paper awards from some reputable journals and conferences. He was also a recipient of the Excellence in Teaching Award, from 2016 to 2017, FCS, and UNB. He currently serves as the Vice-Chair (Publication) of the IEEE ComSoc Communications and Information Security Technical Committee.

HUI ZHU (M'13) received the M.Sc. degree from Wuhan University, Wuhan, China, in 2005, and the Ph.D. degree from Xidian University, Xi'an, China, in 2009. From 2010 to 2014, he was an Associate Professor with the School of Telecommunications Engineering, Xidian University. Since 2015, he has been with the School of Cyber Engineering, Xidian University, as an Associate Professor. His research interests are in the areas of applied cryptography, and cyber security and privacy.

MAODE MA (SM'09) received the B.E. degree from Tsinghua University, Beijing, China, in 1982, the M.E. degree from Tianjin University, Tianjin, China, in 1991, and the Ph.D. degree from The Hong Kong University of Science and Technology, Hong Kong, in 1999. He is currently an Associate Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. He has authored or co-authored about 200 international academic publications, including over 80 journal papers, over 140 conference papers and/or book chapters, and three academic books. His research interests are wireless networking and wireless network security. He is a member of a few technical committees in the IEEE Communication Society. He has been a member of the technical program committees for over 100 international conferences. He has been a general chair, a technical symposium chair, a tutorial chair, a publication chair, a publicity chair, and a session chair for over 50 international conferences. He serves as an Editor-in-Chief/Associate Editor for six international journals.