2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics

A Privacy-preserving Incentive Framework for the Vehicular Cloud

Abdulrahman Alamer[1], Sultan Basudan[2,1] and Xiaodong Lin[3]

[1]Department of Information Systems, Jazan University, Saudi Arabia
[2]Faculty of Business and Information Technology, University of Ontario Institute of Technology, Canada
[3]Department of Physics and Computer Science, Wilfrid Laurier University, Canada
Email: amalameer@jazanu.edu.sa, sultan.basudan@uoit.net, xlin@wlu.ca

***Abstract*—In this paper, we introduce a promising secure and privacy-preserving incentive mechanism in the vehicular cloud (VC). Such an incentive will convince vehicles with excess sensing data to join in the VC without the risk of privacy disclosure. The proposed scheme uses the Bargain Game theory to model the interactions between a VC server (VCS) and vehicles. With the proposed incentive mechanism, the VCS can select competent vehicles with which to collaborate for the announced task, while the vehicles can earn payment for participation. Further, our mechanism ensures fairness between all participants in terms of reward. We also exploit the signcryption technique to achieve mutual authentication between the VCS and vehicles as well as to prevent the private information of these vehicles from being disclosed. Simulation results are provided to show that the proposed privacy-preserving incentive mechanism is beneficial to both the VCS and vehicles, resulting in a win-win situation.**

***Index Terms*—Vehicular Cloud, Privacy Preservation, Incentive Mechanism**

I. Introduction

A great deal of attention has been recently directed towards the vehicular cloud (VC), which is considered as a promising paradigm that plays a critical role in data generation where a large number of smart vehicles collect various kinds of sensing data with large-volume features [1]. The key point of the VC paradigm is to collect and utilize excess vehicle resources in a dynamic group of vehicles under the vehicle owners' authorization [13]. By using the vehicles' sensing resources, the VC becomes increasingly ideal for its ability to support many applications with more accuracy and useful services compared with other mobile crowdsensing paradigms [2].

While the information that should be collected from vehicles' sensor devices is essential for the success of VC applications, there still exists significant challenges that hinder the rapid development of VCs. The first challenge is to stimulate interest in vehicle owners to utilize their vehicles' sensing data to initiate information exchange with VCs in a dynamic environment. This is because vehicle owners may incur extra operational costs when providing their sensing data to the VC. Thus, they have control over whether they keep sensing data or rent it for economically appealing compensation [13]. This results in the second challenge of selecting vehicles and determining their strategies while ensuring fairness among them. The third challenge concerns the security and privacy preserving issues of the involved vehicles in the VC. For example, the vehicle owners may be concerned about the privacy of their information, such as location during participation.

Although a number of works that use game theory, such as Stackelberg, encourage vehicle owners to share their sensing data in a VC system [3] [4], they still do not adequately consider the problem of how to protect the privacy of the involved vehicles and how to evaluate the vehicles' sensing resources in terms of reward. For instance, exiting works provide fixed monetary rewards for performing a task but with no guarantee of fairness among vehicles.

This means that vehicle that provides a large number of sensing resources will obtain the same compensation as those which provide fewer resources. Vehicle owners may seek to maximize their profit by providing a different number of sensing resources. Due to the fact that there are different sensor devices in a vehicle, each vehicle can be categorized as a different sensing resource according to their application domains [5]. For instance, environmental conditions such as weather status, street images, and traffic conditions can be categorized as different sensing resources that are detected by different sensor devices in the vehicle. The data that are collected by the sensors is totally different from each other in terms of information and social cost. Thus, we cannot merely compensate vehicles that provides a large number of sensing resources in the same way as those which provide fewer resources. Moreover, we cannot provide equal compensation for vehicles that provide their resources in the desired time period with those that are delayed. Schemes that administer a fixed reward cannot penalize vehicles that delay the provision of their resources during the required period. These schemes forfeit fairness and correctness amongst vehicles in terms of reward. This has encouraged us to create a mechanism that is capable of evaluating vehicle resources in order to guarantee fairness and correctness between vehicles.

In this paper, we present a design for a secure and privacy-preserving incentive mechanism to motivate vehicle owners to share their collected sensing resources in the VC without disclosing any privacy-related information. Different from previous works [3] [4], our work builds a secure and privacy-preserving incentive mechanism based on evaluating vehicle

978-1-5386-7975-3/18/$31.00 ©2018 IEEE
DOI 10.1109/Cybermatics_2018.2018.00098

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:48:29 UTC from IEEE Xplore. Restrictions apply.

sensing resources. To be more precise, the main contributions of this paper are as follows:

Firstly, we introduce a vehicular sensing resource evaluation mechanism that is described by our expressive language as a novel approach to guarantee a fairness evaluation for vehicles' sensing resources.

Secondly, by exploiting the Bargain Game model, we propose an incentive mechanism that is compatible with our evaluation mechanism to model the interactions between the VCS and vehicles. A role-based bargain approach, which is more targeted and dynamic, can let the price of the sensing resources be more accurate and result in high welfare for both parties. Thus, the proposed scheme is capable of describing the amount of sensing data provided by each vehicle.

Thirdly, we exploit the signcryption technique to propose a privacy-preserving scheme to prevent the private information of vehicles from being disclosed and to achieve mutual authentication between the VCS and vehicles.

Finally, we conduct a numerical analysis to validate the effectiveness of our privacy-preserving incentive model. The results show that the incentive mechanism works effectively and guarantees fairness among vehicles in terms of rewards. Moreover, the privacy-preserving protocol is much more efficient in terms of computational costs and ciphertext size.

The remainder of this paper is organized as follows. In Section II, we introduce the system and attack model, and identify the design goals followed by a presentation of preliminaries in Section III. In Section IV, we discuss our privacy-preserving incentive mechanism. A security analysis and performance evaluation are described in Section V and VI, respectively. Finally, we draw our conclusions in Section VII.

II. System Model, Attack Model and Design Goals

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

A. System Model

We consider a general VC request system. As shown in Fig.1, the system model consists of a VCS, a roadside unit (RSU) and a number of vehicles $N = \{1, 2, ..., n\}$.

- The VCS is a trusted entity that acts as a task server, which is responsible for announcing a task and recruiting vehicles to achieve this task. It is also responsible for distributing rewards to participating vehicles in return for their resources.
- The RSU acts as a gateway that is responsible for transmitting the messages that come from the VCS to vehicles and those that come from vehicles to the VCS.
- The vehicles act as service providers by completing allocated tasks using their sensor devices. Sensing resources may differ between vehicles because of their different sensor devices.
- The Trusted Authority (TA) is responsible for registering the vehicles and creating accounts to record their reward.

Communication Model. When the VCS seeks available vehicular sensing resources, it will send an announced task that includes some specific requirements towards one of its connected RSUs, as shown in Fig. 1. Once the RSU receives the task from the VCS, it will broadcast it to all vehicles within its communication range. The interested vehicles respond with their parameters to the VCS via the RSU. In turn, the VCS starts bargaining with vehicles and selects those with optimum parameters. The selected vehicles finish the tasks with their sensing resources and receive reward from the VCS.

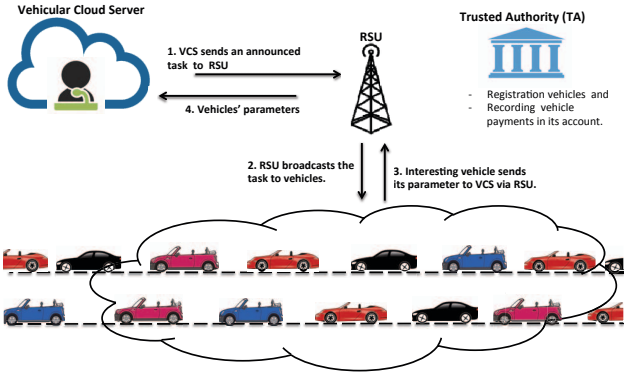

Fig. 1. A Task Announcement Model in the Vehicular Cloud

B. Attack Model

In the system model, the RSU is responsible for establishing communication between the VCS and vehicles, and is considered to be semi-trusted. We consider the case that data generated by vehicles and forwarded to the VCS via RSUs could face a passive attack and reveal private information. Also, a malicious RSU may modify or forge some sensitive information in order to make the VCS accept false results for its own purposes.

C. Design Goals

Our goal is to design an efficient privacy-preserving incentive mechanism that will prevent the above security threats with stimulating the involvement of competent vehicles. The specific objective of this mechanism are as follows.

- **Authentication and Integrity:** This involves the ability to authenticate the message source and its integrity.
- **Confidentiality:** This aspect ensures sensitive information of the message cannot be revealed.
- **Incentive Mechanism:** This involves the design of an incentive mechanism that recruits vehicles without forfeiting fairness in regard to strategies and earned incentives.

III. Preliminaries

A. Bilinear Group

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups with the same prime order q. A mapping $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is an admissible bilinear pairing if ($\hat{e}$) over elliptic curves [6] with the following properties:

- Bilinearity: $\forall P, Q, V \in \mathbb{G}_1$ and $a, b \in Z_q^*$, we have
  - $\hat{e}(P, Q + V) = \hat{e}(P, Q)\hat{e}(P, V)$.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:48:29 UTC from IEEE Xplore. Restrictions apply.

- $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab} = \hat{e}(bP, aQ)$.

- Non-Degeneracy: $\forall P, Q \in \mathbb{G}_1$, where
  - $P \neq 0 \Rightarrow \hat{e}(P, Q) \neq 1 \in \mathbb{G}_2$.
- Computability: $\hat{e}$ is efficiently computable.

B. Complexity Assumptions

We assume the discrete logarithm problem related to our security proposal as follows.

Definition 1: Computational Diffie-Hellman (CDH) Problem. Given $P, aP, bP \in \mathbb{G}_1,\ \forall a, b \in Z_q^*$, compute $abP \in \mathbb{G}_1$ probability within polynomial time.

Definition 2: Decisional Bilinear Diffie-Hellman $(DBDH)$ Problem. Given $P, aP, bP, cP \in \mathbb{G}_1,\ \forall a, b, c \in Z_q^*$ and $f \in \mathbb{G}_2$, decide whether $f = \hat{e}(P, P)^{abc}$.

IV. Proposed Privacy-Preserving Incentive Mechanism

In this section, we present a detailed privacy-preserving incentive mechanism in details, consists of the following parts:

A. System Initialization

The TA initializes the system by generating the bilinear parameters ($\mathbb{G}_1$, $\mathbb{G}_2$, P, $\hat{e}$, q) via the security parameter λ. It then selects $s \in Z_q^*$ as a master private key and computes the corresponding public key $P_{pub} = sP$. P is a generator of $\mathbb{G}_1$. Additional, the TA determines three collision resistant hash functions: $H_1 : \{0,1\}^* \rightarrow Z_q^*$, $H_2 : \mathbb{G}_1 \rightarrow \{0,1\}^n$, $H_3 : \{0,1\}^n \rightarrow \mathbb{G}_1$. The system public parameters are published as $param = (\mathbb{G}_1, \mathbb{G}_2, q, P, \hat{e}, P_{pub}, H_1, H_2, H_3)$.

B. Key Generation

Vehicle i should sends its identity ID_i to the TA to join the system. For protecting each registered vehicle i' ID_i, the TA generates a pseudo identity. The pseudo identity is usually generated from the real identity and a random salt such that $Q_i = H_3(ID_i, salt)$. It is worth noting that the introduction of a random salt is used to prevent the rainbow table attack, which defeat such kind of pseudonym based mechanism for anonymity. In the rainbow table attack, the adversary can create a huge table that contains the mapping of all the real identities and their corresponding pseudonyms. The table is called rainbow table. Whenever a pseudonym is used in a message, the adversary can find out its real identity by searching the table for the pseudonym. Then, TA selects $x_i \rightarrow Z_q^*$ randomly and computes $pk_i = x_i P$ as vehicle i's private and public keys. (pk_i, x_i, Q_i) are sent to vehicle i.

TABLE I
Tracing Table

Identities	Salts	pseudoes
ID_1	$Salt_1$	Q_1
ID_2	$Salt_2$	Q_2
...	...	...
ID_n	$Salt_n$	Q_n

C. Task Announcement

The VCS announces a task T_i attached with its specifications towards one of its connected RSUs. We can exploit the location privacy-aware task recommendation or the privacy-preserving task announcement schemes used in [7], [14] to prevent T_i from any possible attacks [7], [14]. The VCS protects the content of t_i from any adversaries as follows.

$$\alpha_{vc} \leftarrow Signcryp(pk_{vc}, x_{vc}, t_i).$$

The RSU then broadcasts α_{vc} towards all potential participating vehicles within its communication range. If any vehicle i is interested in joining T_i, it will first check whether the message is from the VCS by decrypting α_{vc} as follows.

$$\alpha'_{vc} \leftarrow UnSigncrypt(x_i, \alpha_{vc}).$$

The interested vehicle i will then authenticate itself to the VCS by signcrypting its parameter setup as follows.

- The vehicle i randomly selects $r_i \in Z_q^*$, and
- Computes $L_i = r_i P$.
- Computes $U_i = r_i pk_{vc}$.
- Computes $K_i = H_2(L_i \parallel U_i)$.
- Computes $c_i = K_i \oplus m_i$.
- Computes $h_i = H_3(c_i)$.
- Computes $\sigma_i = (x_i + r_i)h_i$.
- The ciphertext is: $\alpha_i = (L_i, \sigma_i, c_i)$.

The vehicle i then sends the α_i to the VCS via the RSU.

D. Aggregate-Verification

If the RSU receives each ciphertext separately, it has to verify the signature; this will take a long time and may lead to long delays. Consequently, our proposed scheme adopts the aggregation technique that enables the RSU to aggregate all cipheretexts $(\alpha_i)_{i=1}^n$ into one ciphertext (α_{agg}) and simultaneously verify them. Hence the RSU:

- Takes a collection of individual ciphertexts $\alpha_i = (L_i, \sigma_i, c_i)_{i=1}^n$ with their corresponding public keys $(pk_i)_{i=1}^n$.
- Computes the signature aggregation $\sigma_{agg} = \sum_{i=1}^n \sigma_i$.
- Outputs the aggregate ciphertexts $\alpha_{agg} = (L_1 ... L_n, c_1 ... c_n, \sigma_{agg})$.
- Accepts (σ_{agg}) if the following equation is valid.

$$\hat{e}(\sigma_{agg}, P) = \hat{e}(\sum_{i=1}^{n} h_i, pk_i)\hat{e}(\sum_{i=1}^{n} h_i, L_i).$$

If the batch verification is true, the RSU forwards α_{agg} to the VCS in order to complete the unsigncryption step.

E. Data Receiving

The VCS will complete the unsigncrypt as follows.

- Computes $U'_i = x_{vc} L_i$.
- Computes $K'_i = H_2(L_i \parallel U'_i)$.
- Computes $m_i = c_i \oplus K'_i$.

After decrypting all ciphertexts, the VCS will evaluate and choose as the winners vehicles with optimal parameter setup.

- The correctness of our signature scheme is as follows.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:48:29 UTC from IEEE Xplore. Restrictions apply.

$$\begin{aligned}\hat{e}(\sigma_{agg}, P) &= \hat{e}(\sum_{i=1}^{n}(x_i + r_i)h_i, P) \\ &= \hat{e}(\sum_{i=1}^{n}(x_i h_i + r_i h_i), P) \\ &= \hat{e}(\sum_{i=1}^{n} x_i h_i, P)\hat{e}(\sum_{i=1}^{n} r_i h_i, P) \\ &= \hat{e}(\sum_{i=1}^{n} h_i, x_i P)\hat{e}(\sum_{i=1}^{n} h_i, r_i P) \\ &= \hat{e}(\sum_{i=1}^{n} h_i, pk_i)\hat{e}(\sum_{i=1}^{n} h_i, L_i)\end{aligned}$$

- The correctness of $U_i = U_i'$ is as follows.

$$\begin{aligned}U_i &= r_i pk_{vc} \\ &= r_i x_{vc} P \\ &= x_{vc} L_i = U_i'\end{aligned}$$

- The correctness of decryption is as follows.

$$\begin{aligned}m_i' &= c_i \oplus K_i' \\ &= H_2(L_i \parallel U_i) \oplus m_i \oplus H_2(L_i \parallel U_i') \\ &= K_i \oplus m_i \oplus K_i' \\ &= m_i\end{aligned}$$

F. Vehicular Resource Evaluation Mechanism

In this paper, we put forward a vehicular resource evaluation by which the vehicle represents different types of sensing resources. Typically, vehicular ability may differ between different vehicles because of their different sensor devices, which means that a vehicle can provide a variety of sensing resources based on the number of sensor devices it possesses [5]. Thus, the challenge here is how to reveal the diversity of vehicle's valuation in terms of the number of sensing resources that each vehicle can provide. For each announced task, the VCS may need to collect vehicle's sensing data, hence we use $T_i = \{t_s, t_e, L, \Gamma_t\}$ to denote the announced task, where $\Gamma_t = \{\tau_1, \tau_2, ..., \tau_k\}$ denotes k number of sensing tasks required by the VCS. $L = (x_i, y_i)$ denotes the required location through a Global Positioning System (GPS) [8]. t_s and t_e denote the beginning and end of the required time period. Based on variant sensor devices, each vehicle can provide various types of sensing resources. Thus, each vehicle i selects one or a subset of requested tasks $\Gamma_i \subseteq \Gamma_t$ based on its capability. A parameter l_i denotes the number of sensing resources that can be provided by the vehicle i. We use $\lambda_i = \{l_i, \Gamma_i, location_i\}$ to denote the vehicle parameter. Note that it is possible that $\Gamma_i \cap \Gamma_j$ for two vehicles i and j. This interference make the problem NP-complete [9]. Indeed, to express the vehicle's valuation in terms of performance, the VCS performs a penalty (pen_i) for delay time such that a vehicle's valuation for its utility will be loss per unit delay time as shown in Fig. 2. The time delay can be calculated as $d_i = (t_i - t_e)$. The penalty can be calculated as:

$$PN_i = \begin{cases} d_i \cdot pen_i, & if\ t_i > t_e, \\ 0, & elsewhere \end{cases}$$

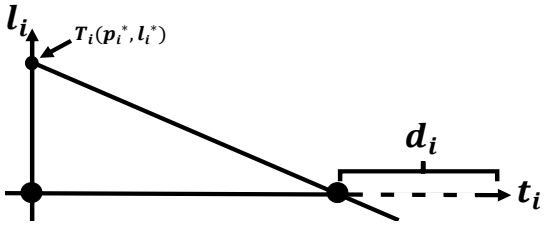

Fig. 2. Valuation Time Delay.

G. Incentive Model

We assume vehicles are selfish, hence each of them intends to provide a number of different sensing resources l_i in one task to maximize its profit. Therefore, we regard these vehicles as non-cooperative game. Additionally, we assume that the VCS has a limited budget B_i for every task to be accomplished. As a result, the VCS needs to distribute the tasks on selected vehicles based on B_i. Consequently, in this paper, we intend to address two fundamental problems, the first of which is how to identify the vehicles that should be selected as winners. The second problem concerns how many sensing resources each winner vehicle should be provided within one task. Given a pool of vehicles N, the VCS aims to pick a set of vehicles with optimal parameters that can cover the budget B_i. Consequently, we utilize the Bargain Game to model the relationship between the VCS and the vehicles. The process for selecting the wining vehicles is as follows.

- **Step 1:** The VCS announces T_i and gives a price p_i, where p_i represents the price per unit sensing resource.
- **Step 2:** Each vehicle i observes p_i and then chooses the number of sensing resources l_i. If p_i is unsatisfied with vehicle i, it would not offer resources such that $l_i = 0$.
- **Step 3:** Vehicle i and the VCS start to bargain over the number of sensing resources l_i that vehicle i can provide.
- **Step 4:** The VCS sorts all vehicles according to their resources such that:

  $$V_1 > ... > V_i > ... > V_n.$$

  Vehicle i with large sensing resources l_i is more valuable and attractive to the VCS.
- **Step 5:** The VCS selects subset S as winners from step 4 until we have ($R \geq B_i$), where $R = \Sigma_{i=1}^{n} l_i$.

Algorithm 1 describes our winner vehicle selection process.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:48:29 UTC from IEEE Xplore. Restrictions apply.

H. Profits Model

Without loss of generality, the VCS has exclusive control over the price p_i making, while each vehicle has exclusive control over offering the number of sensing resources l_i. Hence, it is necessary to make an appropriate resource price p_i to attract various types of vehicles to contribute their data resources to the VC. The VCS's profit function from the sensing resources is formulated as,

$$U_i(p_i, l_i) = R_i(l_i) - p_i l_i \tag{1}$$

where $R_i(l_i)$ represents the VCS's revenue, $(p_i l_i)$ is the vehicle i's reward, such that the VCS rewards every vehicle i based on its l_i. Thus, the vehicle's profit function is formulated as,

$$T_i(p_i, l_i) = p_i l_i - S_i(l_i) \tag{2}$$

where $S_i(l_i)$ denotes the total cost of sensing resources l_i. Each vehicle i has a different total cost $S_i(l_i)$ based on the l_i it provides. The $R_i(l_i)$ and $S_i(l_i)$ are simulated by constant elasticity of substitution (CES) functio [10], as shown below.

$$R_i(l_i) = \frac{l_i^{\gamma}}{\gamma} - PN_i \tag{3}$$

$$S_i(l_i) = \frac{l_i^{\delta}}{\delta} - PN_i \tag{4}$$

where γ and δ are elastic parameters of these two functions. We have $0 \leq \gamma \leq 1$ and $\delta \geq 1$ as convex and concave function. The ultimate goal for each vehicle i is to maximize its profits by finding the optimal l_i^* in response to the p_i given by the VCS. Thus, the optimization problem for vehicle i is formulated as,

$$max_{l_i \geq 0}\ T_i(p_i, l_i) = [p_i l_i - (\frac{l_i^{\delta}}{\delta} - PN_i)] \tag{5}$$

Each vehicle i can improve its utility by deviating from its current strategy to a Nash Equilibrium (NE) [11]. Based on the NE concept, each vehicle i performs its best response strategy, which maximizes its own utility function to achieve maximum profit. In order to achieve the best response strategy $l_i^*(p_i)$ for the vehicle i based on (p_i) given by the VCS, we need to solve equation (5) by taking its first-order derivative, which results in:

$$p_i - l_i^{\delta - 1} = 0 \tag{6}$$

$lim_{l_i \to 0}\ l_i^{\delta-1} = \infty$ and $lim_{l_i \to \infty}\ l_i^{\delta-1} = 0$, representing that the first-order derivative on (5) has a solution. Thus, the best response strategy for a vehicle is formulated as,

$$l_i^* = (p_i^{\frac{1}{\delta - 1}}) \tag{7}$$

The ultimate goal of the VCS is to obtain the largest number of sensing resources with the lowest prices p_i. We assume that the VCS knows vehicle reaction to p_i will be to choose the demand function of the amount of sensing resources $l_i^* = (p_i^{\frac{1}{\delta - 1}})$, so that the VCS can choose its optimal p_i^* to maximize its revenue by expecting a vehicle's best response. Thus, the optimization problem for the VCS is formulated as,

$$max_{p_i \geq 0}\ U_i(p_i, l_i^*) = [(\frac{(p_i^{\frac{1}{\delta-1}})^{\gamma}}{\gamma} - PN_i) - p_i(p_i^{\frac{1}{\delta-1}})] \tag{8}$$

We then take the first-order derivative of equation (8), which results in:

$$\delta = \frac{(p_i^{\frac{\gamma-1}{\delta-1}})}{p_i} \tag{9}$$

The best response strategy for the VCS is by solving the equation (9) to obtain p_i^*. Thus, $(p_i^*, l_i^*(p_i^*))$ is a NE outcome of our Bargain Game mode.

Algorithm 1 Algorithm Vehicle Recruiting

Data: N, T_i p_i.
Output: S, p_i^*, l_i^*, U_i^*, and T_i^*
$S = \emptyset$
Sort vehicles according to l_i
$V_1 > ... > V_i > ... > V_n$
for $k = 2 : N$ **do**
Calculate $p_i^*(k-1)$, $l_i^*(k-1)$, $T_i^*(k-1)$ and $U_i^*(k-1)$;
end for
Define $max = U_i^*(1)$, $max = T_i^*(1)$ and $max_{int} = 2$
for $j = 1 : N$ **do**
if $l_j = 0$; Then
$U_i(p_i, 0) = 0$;
else if $(U^*(j), T^*(j)) \geq max$, and $(R \leq B)$
$l_j = 1$;
Add $l_j \to R$; and $j \to S$;
$N = j + 1$;
end if
end for
Return set of winners $S = \{V_1, ..., V_n\}$

V. Security Analysis

In this section, we briefly summarize the security properties of our proposed privacy-preserving incentive mechanism.

- *Security and Privacy Preservation.* The proposed scheme guarantees the confidentiality and integrity of a message under to CDH problem. Thus, an adversary cannot decrypt and modify any message without knowing the receiver's private key and r_i, which is randomly chosen from the sender and used to calculate L_i and U_i.
- *Mutual Authentication.* In the proposed scheme, only a registered vehicle i can sign a message by calculating σ_i using its private key. The VCS verifies σ_i under the $DBDH$ and establishes mutual authentication by computing U_i' using its private key. Thus, mutual authentication between the VCS and vehicles can be achieved.
- *Anonymity.* In our scheme, each vehicle i uses its pseudo identity Q_i that is generated from its real identity during the registration processes. Thus, no one can reveal the real identity of vehicle i during the transmission process.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:48:29 UTC from IEEE Xplore. Restrictions apply.

VI. Performance Evaluation

A. Performance of Privacy-preserving

In this section, we demonstrate the performance of the proposed privacy-preserving protocol in terms of computational cost and communication overhead. We count the number of complicated cryptographic operations, including scalar multiplication in $\mathbb{G}_1$, $\mathbb{G}_2$ exponentiation and computation cost pairing $\hat{e}$. We denote P_1, P_2 and P_3 , the point multiplication in $\mathbb{G}_1$, exponentiation in $\mathbb{G}_2$ and pairing $\hat{e}$. The computation is conducted by using a notebook with Intel Core i5-4200U CPU @2.29GHz and 4.00GB memory. We use MIRACL library 5.6.1 curve with Tate pairing to implement number-theoretic based methods of cryptography [12]. To ensure the security of the proposed scheme, the parameter q is approximately 160 bits. The running time is displayed in Table II.

We also analyze the communication overhead of our scheme from two aspects: vehicle-to-RSU communication and RSU-to-VCS communication. When a vehicle i sends its resource, it needs to send the encrypted report α_i to the RSU, which is $320 + 256$ bits, if we assume the binary length of $\mathbb{G}_1$ is 160 bits and z_q^* is 256 bits. The RSU aggregates $(\alpha_i)_i^n = 1$ and sends σ_{agg}, which is $[n(160 + 256) + 160]$ bits. The binary length of the encrypted message between the RSU and VCS increases linearly with the growth of n.

TABLE II
Computational Overhead

Phases	Operations	Run Time (ms)
Setup	$2P_1$	1.2
Vehicle's report sending	$3P_1$	1.8
Verification	$3P_3$	13.5
Receiving report	P_1	0.6

B. Effectiveness Analysis of Incentive Mechanism

In this section, we conduct a numerical analysis of the proposed incentive mechanism. The expression of $(p_i^*, l_i^*(p_i^*))$ is the NE outcome of our Bargain Game mode. We examine the utility of both the VCS and the vehicles. The VCS's utility is calculated by subtracting $(R(l^*))$ from the reward (p^*l^*) while the vehicle utility is calculated by subtracting (p^*l^*) from its cost $(S(l^*))$. $R(l^*)$ and $S(l^*)$ are simulated by using two parameters γ and δ. Thus, in Fig. 4 and Fig. 5, we examine the VCS and vehicle utility in terms of increasing (δ) ascently. We set three fixed values (γ) to be $0.9, 0.5$ and 0.2. As shown in Fig. 4, by increasing (δ), the VCS's utility also increases while the vehicle's utility decreases as seen in Fig. 5. Thus, we deduce that increasing (δ) has a positive influence on the VCS's utility and a negative influence on the vehicle's utility. We also examine the VCS and vehicle utilities in terms of increasing (γ) ascently. We fix (δ) in three values: $10, 5$ and 2. As in Fig. 6 and Fig. 7, by increasing (γ), the utility of both the VCS and vehicles is decreased. Thus, (γ) value can negatively influence the VCS and vehicle utilities. In addition, Fig. 7 shows that the vehicle utility can also influenced by the order of the three fixed values of (δ) $(10, 5$ and $2)$.

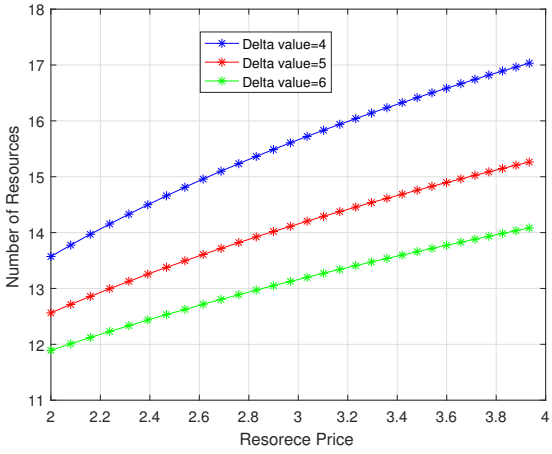

Fig. 3. Relationship Between Price p^* and Sensing Resource l^*

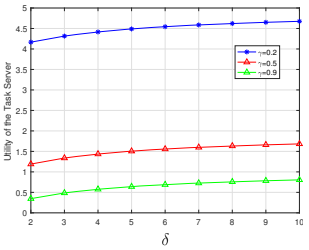

Fig. 4. Utility of VCS

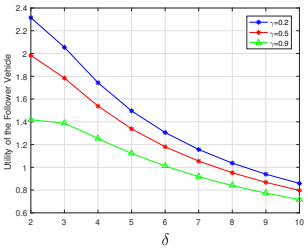

Fig. 5. Utility of Vehicle

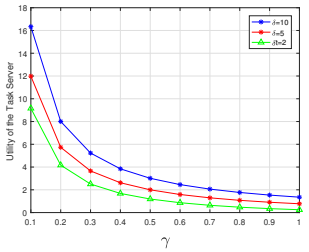

Fig. 6. Utility of VCS

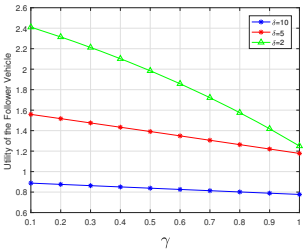

Fig. 7. Utility of Vehicle

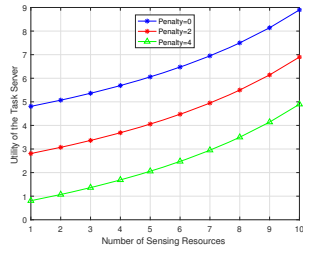

Fig. 8. Utility of VCS

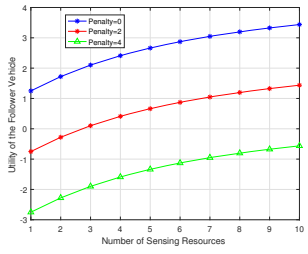

Fig. 9. Utility of Vehicle

Accordingly, we infer that the (γ) and (δ) make our incentive model more reasonable and fair in order to satisfy the VCS and vehicles during the bargaining process. This guarantees that every rational vehicle will bargain with a large number

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:48:29 UTC from IEEE Xplore. Restrictions apply.

of resources l_i to maximize its revenue. In contrast, the VCS should offer optimal (p^*) to motivate vehicles into joining the task. Fig. 3 shows the relationship between (p^*) and (l^*).

In Fig. 8 and Fig. 9, we show the impact of the penalty on the utilities of the VCS and the vehicles. We set three penalty values (Penalty = 0, Penalty = 2 and Penalty = 4). Increasing the number of resources results in an increase in the utilities of both the VCS and the vehicles. As a result, our Bargain Game model can result in a win-win outcome. However, for lazy vehicles, we can see that as shown in Fig. 9 and Fig. 8 with Penalty = 2 and Penalty = 4, the vehicle's utility decreases. This guarantees that every rational vehicle will take the time requirements into consideration.

By summarizing the above results, our proposed incentive mechanism works effectively and can guarantee fairness amongst vehicles. Since it compensates each vehicle based on the number of its resources and penalizes any vehicle that delays submitting its result in the desired time period.

VII. Conclusion

In this paper, we propose a novel privacy-preserving incentive mechanism in the VC. The proposed incentive mechanism can select optimal vehicles. We also describe a vehicular resource evaluation mechanism that enables the VCS to calculate vehicles' rewards based on their resources and penalize lazy vehicles. Through performance analysis, we demonstrate the effectiveness of the proposed incentive mechanism in terms of the utilities of the VCS and vehicles. In addition, the proposed privacy-preserving protocol meets security requirements with more efficiency regarding computational cost and communication overhead. In future work, the truthful social cost and privacy issues related to guaranteeing the availability of the incentive mechanism will be considered.

References

[1] 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 Transactions on Parallel and Distributed Systems, vol. 23, no. 11, pp. 2067–2080, 2012.

[2] A. Alamer, Y. Deng, G. Wei, and X. Lin, "Collaborative Security in Vehicular Cloud Computing: A Game Theoretic View," IEEE Network, vol. 32, no. 3, pp. 72 - 77, May/June 2018.

[3] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to smartphones: incentive mechanism design for mobile phone sensing," Proc. ACM MobiCom, pp. 173–184, 2012.

[4] ——, "Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones," Biological Cybernetics, vol. 24, no. 3, pp. 1732–1744, 2016.

[5] S. Abdelhamid, H. S. Hassanein, and G. Takahara, "Vehicle as a mobile sensor," Procedia Computer Science, vol. 34, pp. 286–295, 2014.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM journal on computing, vol. 32, no. 3, pp. 586–615, 2003.

[7] A. Alamer, Y. Deng, and X. Lin, "Secure and privacy-preserving task announcement in vehicular cloud," Proc. the 9th International Conference on Wireless Communications and Signal Processing, (WCSP 2017), Nanjing, China, October, 2017.

[8] A. Rai, K. K. Chintalapudi, V. N. Padmanabhan, and R. Sen, "Zee: Zeroeffort crowdsourcing for indoor localization," Proc. the 18th annual international conference on Mobile computing and networking, pp. 293–304, 2012.

[9] H. Jin, L. Su, B. Ding, K. Nahrstedt, and N. Borisov, "Enabling privacyp-reserving incentives for mobile crowd sensing systems," Proc. the 36th International Conference on Distributed Computing Systems (ICDCS), pp. 344-353, 2016.

[10] Chan, Nathan W and Gillingham, Kenneth, "The microeconomic theory of the rebound effect and its welfare implications," Journal of the Association of Environmental and Resource Economists, pp. 133-159, 2015.

[11] Gibbons, A primer in game theory. Harvester Wheatsheaf, 1992.

[12] M. Scott, "Efficient implementation of cryptographic pairings," [Online], Available: http://www. pairing-conference. org/2007/invited/Scott slide. pdf, 2007.

[13] Q. Kong, R. Lu, H. Zhu, A. Alamer and X. Lin, "A Secure and Privacy-Preserving Incentive Framework for Vehicular Cloud on the Road," Proc. IEEE Global Communications Conference (GLOBECOM), Washington, DC, pp. 1-6, 2016.

[14] A. Alamer, J. Ni, X. Lin and X. Shen, "Location privacy-aware task recommendation for spatial crowdsourcing," Proc. the 9th International Conference on Wireless Communications and Signal Processing, (WCSP 2017), Nanjing, China, October, 2017.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:48:29 UTC from IEEE Xplore. Restrictions apply.