

An Implementable Scheme for Enhanced Efficiency and Multi-Type Information Privacy in Multi-Task Vehicular Networks

Yichen Huang

August 15, 2023

Abstract

Mobile crowdsensing is a method that utilizes widespread mobile devices to collect and analyze data from their environment for various applications, presenting both opportunities and challenges in privacy, security, and data quality. This provides a flexible and scalable sensing model with minimal deployment expenses. With the progression of vehicle networks, numerous studies have explored the potential of using vehicles as sensing units in the context of mobile crowdsensing. However, a significant portion of these studies exhibit certain constraints. First, either they have not considered conditional privacy preserving, or the protection has not covered the reputation value. Secondly, they do not consider the multi-tasking vehicular network environment, resulting in more serious efficiency and storage overhead problems. In order to overcome these constraints, we suggest a conditional privacy preservation approach within a multi-task mobile crowdsensing framework for vehicular networks. Our suggested approach harmonizes the need for privacy preservation and supervision, thereby realizing a characteristic known as conditional privacy preservation. Furthermore, each vehicle has the capability to engage in numerous sensing tasks concurrently. Specifically, privacy safeguards encompass identity, location, and reputation privacy all at once. The reputation center, while updating the pseudonyms of vehicles, doesn't necessitate the storage of any internal data (for instance, ephemeral keys or random numbers), thus mitigating the potential for Denial-of-Service (DoS) attacks. As a result, it offers a more secure and feasible solution for mobile crowdsensing. Security evaluations confirm that our approach meets the desired security prerequisites, such as accuracy, conditional privacy preservation, and authentication. Efficiency assessments indicate that our approach can be effectively implemented in multi-task mobile crowdsensing.

Keywords: Vehicular Networks · Privacy Preserving · Reputation Management · Encryption Algorithm

1 Introduction

As mobile internet evolves and intelligent devices with sensors become increasingly prevalent, the notion of mobile crowdsensing (MCS) has emerged[5]. MCS, with its capacity to perceive, gather, and analyze environmental data, has become a highly sought-after technique applied in diverse fields such as transportation, healthcare, and medical treatment. Recently, vehicles have been enhanced with more sensors, making them smarter and naturally suitable as sensor nodes in mobile crowdsensing.[2][11] Furthermore, vehicular networks offer numerous benefits, including high mobility, low energy usage, and easy installation and maintenance. Consequently, their application in MCS has garnered increasing interest from both academia and industry. In these networks, the MCS architecture primarily comprises three components: data requesters, a cloud server, and sensing vehicles.

These sensing vehicles can execute sensing tasks while traversing rural and urban areas, making them ideal for mobility-dependent applications.[2] However, the open nature of vehicular networks exposes them to a variety of attacks. For instance, vehicle sensors and controllers could be manipulated or tampered with by adversaries. Malicious sensing vehicles can not only falsify and alter data, compromising its authenticity and integrity, but also pilfer sensitive information such as identity and location, thereby reducing user acceptance of this emerging technology. To mitigate this, a reputation value is often employed to assess the trustworthiness of vehicles.[15] [3] Typically, this value is issued and managed by a reputation center: the cloud server assesses vehicle trustworthiness based on the accuracy of the sensing data and sends a feedback report to the reputation center, which then updates the vehicle's reputation value accordingly.[16] However, managing the reputation value becomes more challenging when the sensing vehicle participates in multiple sensing tasks simultaneously. Additionally, ensuring privacy protection in terms of location and identity already incurs significant communication and computing overheads. If reputation value protection is also implemented, the system may become even more complex.

In recent times, many MCS schemes have utilized reputation value to assess participant trustworthiness. However, most of these schemes only consider privacy protection for the vehicle's identity[21] and location[20], neglecting the reputation value[19]. This oversight allows malicious adversaries to potentially use the reputation value to deduce the vehicle's trajectory or even its identity. Furthermore, most existing schemes only consider a single sensing task and are not applicable to multi-task sensing. In existing privacy protection schemes based on pseudonyms, the cloud server needs to store random numbers when updating pseudonyms, leading to significant storage overheads and making the system susceptible to denial-of-service (DoS) attacks.

In addition to these issues, conditional privacy preservation is a critical requirement in vehicular networks.[14] On one side, adversaries may intercept communications to extract sensitive information, leading to serious privacy breaches. On the other side, a trusted authority needs to conduct effective supervision, such as extracting the real identity of a vehicle when necessary.[18] Therefore, conditional privacy preservation should be provided to balance privacy preservation and supervision requirements in vehicular networks. This

strict requirement stipulates that the trusted authority must be the only entity capable of extracting the real identity, location, and reputation value of a vehicle.

To address the above challenges, The objectives of this report are summarized as follows:

- This report will propose a specific, tangible, and executable mobile sensing scheme that supports multi-task mobile sensing and conditional privacy protection of multiple information types in vehicular networks, with a focus on identity, location, and reputation privacy of vehicles.
- The scheme's performance will be measurable through deployment and testing in a server environment, where the time and storage overhead during execution will be quantified.
- By leveraging pseudonym authentication, signature technologies, the BCP algorithm, and homomorphic encryption, the scheme's objectives are achievable, providing conditional privacy protection for various information types in a multi-task vehicular network setting.
- The scheme is relevant as it addresses the prevailing security and privacy concerns in vehicular networks, offering a more secure and practical solution to the primary privacy challenges these networks currently face.
- The entire process, from deployment and testing to evaluation of the scheme, is time-bound to be completed within the specified project timeline, ensuring the availability of results for analysis and conclusion.

The rest of the paper is organized as follows. Section 2 reviews some related works. Section 3 describes some Methodologies and Preliminaries that will be used in our proposed scheme. Section 4 describes the system model, security model, and security requirements, and Section 5 presents our proposed scheme. Section 6 provides security analysis, calculation overhead and communication overhead analysis. Finally, conclusion and discussion are included in Section 7.

2 Related Works

As an ever-evolving field of research, privacy preservation in vehicular networks poses significant challenges due to its multi-type, multi-task nature, and the increasing need for conditional privacy protection. The evolving literature provides various approaches to tackle these concerns. This section provides a comprehensive review of key studies and methods that have significantly contributed to addressing these issues.

2.1 Multi-type Privacy Protection in Vehicular Networks

Present research on vehicular networks' mobile sensing primarily focuses on diverse aspects, with significant attention devoted to privacy protection across multiple types of information.

One of the fundamental types is location privacy. For instance, Ni et al. [16] proposed a matrix-based approach, where each column in the matrix represents a sensing area, and each row corresponds to a sensing task. By leveraging random matrix multiplication, the matching of sensing tasks with sensing areas is achieved, consequently providing location privacy protection. However, this approach is computationally intensive, necessitating the exploration of more efficient matrix multiplication algorithms or alternative methods for location information encryption.

In another study focusing on location privacy, Wang et al. [20] introduced a method integrating ϵ -differential privacy and δ -distortion privacy. This method first applies differential privacy to vehicle locations, and then maps these locations and sensing tasks to a high-dimensional space subject to distortion. While this method effectively reduces computational overhead and preserves sensing result accuracy, it too involves a certain degree of communication and computational costs.

In terms of sensor data privacy, another type, Sun et al. [19] proposed a privacy-preserving method employing homomorphic encryption. This method sends encrypted sensing tasks and results to the cloud, where the computations are performed. The advantage of this approach is its effectiveness in data privacy protection and its ability to offload computations to cloud services, making it suitable for modern vehicular networks.

Lastly, focusing on the privacy of statistical data in mobile sensing, Zhao et al. [22] used a zero-knowledge proof technique to prove the satisfaction of specific conditions by vehicles without compromising personal privacy. Despite its effectiveness in preserving individual privacy and enabling statistical analysis, this method also has limitations. It requires substantial computational and communication resources, and is restricted to specific mobile sensing tasks, not being adaptable to other types of sensing tasks or multitasking mobile sensing.

In conclusion, while significant strides have been made in the field of privacy protection in vehicular networks, there still exist two primary challenges. The first pertains to achieving simultaneous privacy protection across multiple types of information, including location, identity, and sensing data. The second revolves around the need to reduce computational costs and overhead associated with communication processes in a multi-tasking environment. These challenges highlight the need for further research and innovation in multi-type privacy protection in vehicular networks.

2.2 Multi-task Privacy Protection in Vehicular Networks

In the field of vehicular network mobile sensing, evaluating vehicular reputation in a multi-task environment effectively deters malicious vehicles from infiltrating the network. However, the multi-task environment introduces fresh challenges to privacy preservation, ne-

cessitating exploration of innovative methods and techniques.

In related studies, many researchers have proposed the use of reputation scores to assess the trustworthiness of sensing vehicles and determine their eligibility for participation in sensing tasks. For instance, in scheme [6], a reputation center uses reputation scores based on a worker’s historical performance to evaluate their trustworthiness and select the most suitable workers to complete tasks. This scheme, however, is only applicable to simple single-task environments and doesn’t account for scenarios where each sensing vehicle might perform multiple tasks simultaneously.

Subsequently, reputation management schemes [10][9][13] were proposed, arguing that trust scores should not merely be updated based on individual tasks but should also calculate the weight of new reputation values based on reputation feedback reports and original reputation values of vehicles. These schemes, taking into account the multi-task environment, provide a more accurate evaluation of the trustworthiness of sensing vehicles.

As vehicular sensor equipment and vehicular network mobile sensing mature, privacy protection in a multi-task environment becomes increasingly important. Additionally, vehicle reputation values themselves also need protection. If this information is leaked, malicious adversaries could use it to infer driving patterns and trajectories, leading to location and trajectory information leakage and threatening the privacy of vehicle owners. However, existing vehicular network mobile sensing schemes, though considering the application of reputation values, overlook the privacy protection of these reputation values.

In scheme [13], a distributed privacy protection-based trust management mechanism was proposed to balance the relationship between trust and privacy in vehicular network emergency message transmission. The scheme uses identity-based encryption to bind the vehicle’s identity information with its reputation value and employs an obfuscation-based randomization technique to protect vehicle reputation value privacy. However, the possible interception and tampering of reputation values remain a potential security issue.

In scheme [16], before the sensing vehicle reports its reputation value to the reputation center, it encrypts its reputation value, and the reputation center can only view the reputation value after decryption. Yet, even with the application of encryption, obfuscation, and anonymization technologies, it is still possible to infer participants’ reputation values. For instance, a malicious adversary can compare the reputation values of multiple participants to deduce each participant’s true reputation value.

Consequently, privacy protection across multiple sources must incorporate the privacy protection of reputation values, as well as ensuring the efficiency of reputation management in a multi-task environment. Hence, the urgent need for research and development geared towards overcoming these challenges in multi-task vehicular networks.

2.3 Conditional Privacy Preservation in Vehicular Networks

In a vehicular network environment with multiple sources and tasks, conditional privacy protection can facilitate the sharing and access control of public information while preserving privacy, favoring audit and accountability procedures by relevant departments against malicious adversaries.

In paper [18], the authors proposed a method for implementing conditional privacy protection in vehicular network mobile sensing, utilizing obfuscation and encryption techniques. Specifically, each vehicle generates an anonymous certificate, using it to encrypt its communication. The public/private key pairs and corresponding certificates involved in encryption/decryption are preloaded into the vehicle's OBU to protect identity privacy. For information that needs to be public (such as road condition information), vehicles can use group signature technology to protect conditional privacy. Only group members meeting certain conditions can decrypt and access this information.

However, this scheme has certain drawbacks. First, both vehicles and trusted third parties require substantial storage space to store data. Second, when a malicious vehicle sends erroneous messages, it takes a significant amount of time to recover its identity.

Addressing these limitations, paper [14] proposed a protocol named ECPP (Efficient Conditional Privacy Preservation), aiming to achieve conditional privacy protection without requiring substantial additional storage space. The core idea of the ECPP protocol is to establish secure trust relationships by exchanging public key certificates and to allow secure communication and information sharing between vehicles while protecting user privacy. To further safeguard vehicle user privacy, the ECPP protocol employs attribute-based encryption techniques to implement conditional access control, where only vehicles meeting certain conditions can decrypt and access the information.

Furthermore, for the implementation of conditional privacy protection, each vehicle must frequently request new anonymous certificates from the reputation center because if certificates are used for extended periods, adversaries can use them to track vehicles, thereby threatening user privacy. The core idea of scheme [8] is to use identity-based encryption technology and conditional access control mechanisms to achieve vehicle user identity verification and privacy protection.

Upon reviewing the strengths and weaknesses of existing schemes, it is evident that establishing a reputation center for managing vehicle privacy information can help minimize the amount of data that sensing vehicles need to store. Additionally, sensing vehicles can prevent identity information leakage or interception by malicious adversaries by registering under pseudonyms.

However, conditional privacy protection is indispensable in vehicular network mobile sensing schemes. Existing conditional privacy protection schemes often require storage of a large number of public and private key pairs in multi-task environments, undoubtedly increasing storage and audit pressures. Therefore, how to achieve efficient conditional privacy protection in a multi-task environment is a critical problem that needs to be addressed by this study.

In conclusion, privacy preservation in vehicular networks is a multi-faceted problem that requires sophisticated solutions addressing a myriad of challenges simultaneously. From multi-type information privacy preservation to multi-task privacy protection, and finally to conditional privacy preservation, the existing literature offers a plethora of approaches,

each with its unique advantages and disadvantages. However, each of these schemes faces limitations in practical applications, primarily due to the increased computational and storage requirements, along with potential vulnerabilities that could be exploited by malicious entities. Therefore, future research in this field should focus on developing more efficient, robust, and comprehensive privacy-preserving solutions, capable of dealing with the growing complexity of vehicular network environments. The goal is to strike a balance between preserving privacy and maintaining the operability of vehicular networks, all while minimizing resource consumption.

3 Preliminaries and Methodologies

In this section, we discuss several foundational methodologies essential to the construction of our proposed system. These include homomorphic encryption and the BCP encryption scheme.

3.1 Homomorphic Encryption

The Paillier cryptosystem[17], possessing the additive homomorphic property, is one of the most prevalent encryption schemes. Let's consider N encrypted data under the identical public key pk , which are expressed as $[m_i]_{pk}$ ($i = 1, 2, \dots, N$). It is guaranteed by additive homomorphic encryption that the equation below invariably stands true

$$D_{sk} \left(\prod_{i=1}^N [m_i]_{pk} \right) = \sum_{i=1}^N m_i$$

where $D_{sk}()$ signifies the decryption algorithm linked with the private key sk . Certain extensions have been suggested by Liu[12] that could be employed as a toolkit for handling encrypted data, such as the *Secure Less Than* Protocol (SLT) and *Secure Equivalent Testing* Protocol (SEQ). Given two encrypted values $[x]_{pk}$ and $[y]_{pk}$, the SLT protocol can derive a bit in an encrypted format, depending on whether $x \geq y$ or $x < y$. Similarly, the SEQ protocol can obtain a bit in the encrypted format, depending on whether the plaintext of the two encrypted data is identical (i.e., $x = y$).

3.2 The BCP Encryption Scheme

The BCP encryption scheme[1] operates as detailed below:

KeyGen: Initiate with two substantial primes p, q , and $n = pq$. Define g and h as two elements with the utmost order in G , wherein G is the cyclic group of quadratic residues modulo n^2 . It's important to note that if h is calculated as $g^x \bmod n^2$, with $x \in [1, \lambda(n^2)]$ and $\lambda()$ being the Euler function, then x is likely to be coprime with $\text{ord}(G)$, leading to h being of maximal order. The public parameters are n, g and $h = g^x \bmod n^2$, with the hidden value being $x \in [1, \text{ord}(G)]$

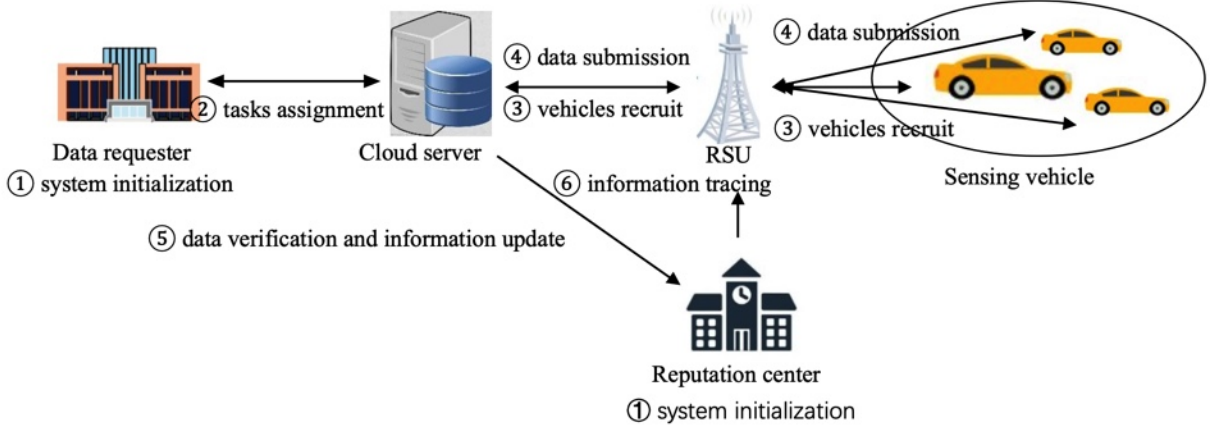


Figure 1: The system architecture of proposed scheme.

Enc: If given a message $m \in Z_n$, select a random number r from Z_n^* . The ciphertext is calculated as $[m] = (T, T') = \{h^r(1 + mn), g^r\} \bmod n^2$.

Decryption Using Weak Private Key (WDec): Using the secret key x , the original message m can be recovered in the following manner: $m = L(T / (T')^x \bmod n^2)$, where $L(u) = (u - 1)/n$.

Decryption Utilizing Strong Private Key (SDec): Any ciphertext can be decrypted with the strong private key $SK = \lambda(n)$ via the calculation:

$$T^{\lambda(n)} \bmod n^2 = g^{xr\lambda(n)}(1 + mn\lambda(n)) \bmod n^2 = 1 + mn\lambda(n)$$

Following this, m can be restored as:

$$m = L(T^{\lambda(n)} \bmod n^2) \cdot \lambda(n)^{-1} \bmod n$$

4 Models and Definitions

This section will describe the system model, security model, and security requirements. By providing an in-depth examination of these three components, this section aims to give readers a solid foundation for understanding the core concepts of our research, setting the stage for the further discussions and analyses to follow.

4.1 System Model

Fig.1 illustrates the system model, which is composed of five distinct entities: the data requester, the cloud server, the reputation center, the roadside unit, and the sensing vehicle.

Data Requestor: This could be an administrative body, a service provider, or an individual with proper authorization. They are responsible for delegating sensing tasks with the objective of procuring valuable data such as road conditions, weather updates, traffic congestion levels, and more.

Cloud Server: Its role is to gather, retain, and compute the encrypted data gathered through sensing. Furthermore, it assesses the trustworthiness of vehicles based on the precision of their provided sensing data and creates a reputation feedback report. These cloud servers are generally equipped with robust storage and computational capacities.

Reputation Center: Its job is to authenticate, save, and disseminate reputation values and pseudonyms to each vehicle involved in sensing. It also revises the reputation scores of vehicles in line with the reputation feedback reports.

Roadside Unit (RSU): This unit is stationed on either side of the roadway, accountable for data transmission. To be precise, the RSU facilitates data transfer services between cloud servers and sensing vehicles, and also between reputation centers and sensing vehicles.

Sensing Vehicle: It is typically fitted with diverse sensors, tasked with the collection and storage of varied environmental data. Each sensing vehicle also possesses an on-board unit OBU[4][7] capable of holding confidential information such as secret keys, identities, locations, and so forth.

4.2 Security Model

In this system, the data requester, the cloud server, and the Road-Side Units (RSUs) are presumed to be honest-yet-curious. That is to say, they adhere to the given protocol but may seek to gain unauthorized information. For instance, in a mobile crowdsensing setting reliant on vehicular networks, these honest-yet-curious entities might aim to deduce the sensing vehicles' location, identity, and reputation details, known as an *inference attack* (comprising location inference attack, identity inference attack, and reputation inference attack). Additionally, a malicious adversary could deduce extra information, such as the vehicle's driving pattern, by intercepting a sequence of reputation scores linked to the same sensing vehicle. This type of attack is referred to as a *reputation linkable attack*.

The reputation center is considered to be completely trusted. It's assumed that most sensing vehicles act honestly, while a minority of deceptive vehicles could instigate the subsequent attacks:

- *Data pollution attack:* Malicious sensing vehicles might provide false data, leading to the contamination of the sensing results.
- *Sybil attack:* Malicious sensing vehicles might repeatedly submit identical data or employ counterfeit identities with the goal to amass a greater reputation or distort the sensing results.
- *Reputation tamper attack:* Sensing vehicles with a low reputation might manipulate their reputation score, enabling them to take part in sensing tasks they are otherwise unauthorized to perform.

- *Collusion attack*: A group of malicious vehicles may collaborate to reinforce false information or compromise the integrity of the network, leading to a potentially harmful influence on decision-making processes.

The assumption of an honest majority allows for the system to be resistant to these attacks, but awareness and active defense measures should still be considered.

4.3 Security Requirements

This proposed scheme takes into account the following security prerequisites:

- *Correctness*. Provided all the participants honestly adhere to the protocol, it will yield accurate outcomes.
- *Conditional privacy preservation*. Privacy safeguards are in place for identity, location, and reputation value to keep them away from adversaries. However, when required, this information can be accessed by a trusted authority. Specifically, identity privacy ensures that a sensing vehicle’s actual identity remains concealed from adversaries during communication with other entities. Location privacy implies that malicious entities can’t discover the sensing vehicles’ whereabouts via messages. Reputation value privacy sees to it that the reputation values of vehicles are neither revealed nor linked. However, in a multi-task environment, if needed, the trusted authority can extract the real identity, location, and reputation value from the communicated messages.
- *Authentication*. It should be impossible for adversaries to tamper with or forge exchanged messages without detection.
- *Resistance to other attacks*. The scheme we propose is designed to resist a variety of real-world attacks, such as inference attacks, reputation linkable attacks, data pollution attacks, Sybil attacks, and reputation tamper attacks.

5 Scheme Design

In this segment, we initially provide a synopsis of the proposed scheme before delving into its technical specifics. Comprising six stages, the proposed scheme includes system initialization, task allotment, vehicle recruitment, submission of data, verification of data and information update, and finally, information tracing. The symbols utilized in the proposed scheme are subsequently encapsulated as follows:

5.1 An Outline of the Proposed Scheme

In order to simplify the presentation, we initially provide a brief outline of the suggested scheme. Let’s consider a sensing task set up in an urban area. Sensing vehicles interested

Table 1: Formalized Notations Utilized in the Proposed Scheme

Notation	Definition
t_i	the reputation value of the i th sensing vehicle
t_0	the reputation threshold for the sensing task
m	the substance of a sensing task
$[m]$	the m 's encrypted form.
d	data gathered through sensing
d_0	standard value of the sensing data
Δd	error threshold of the sensing data
PK_{DR}, SK_{DR}	key pair of the data requester
PK_{RC}, SK_{RC}	key pair of the reputation center
x, y	coordinates of the sensing task
r	radius of the sensing task
$TSK.$	the list of sensing tasks
RID	actual identity of a sensing vehicle
PID	sensing vehicle's pseudonym
T	the list of tasks a sensing vehicle is involved in

in participating in this task must meet the location and reputation requirements of the task. To illustrate, suppose the data requester sets a task and establishes the reputation threshold at t_0 . This implies that the reputation value t of the sensing vehicle should be equal to or more than t_0 . Additionally, the sensing vehicle's position should fall within a circle with radius r specified by the sensing task. As depicted in Fig.1, the following steps are incorporated in the proposed scheme:

- **System Initialization.** The data requester and the reputation center generate system parameters and key pairs for the homomorphic encryption scheme. The reputation center initializes the reputation score for each vehicle, then dispatches each vehicle's pseudonym and reputation value to the respective sensing vehicle. All these messages are signed by the reputation center prior to transmission.
- **Task Allocation.** The data requester delegates a sensing task to the cloud server, complete with the location requirement and reputation threshold for this sensing task. The cloud server subsequently broadcasts this task to the sensing vehicles via RSUs.
- **Recruitment of Vehicles.** Each sensing vehicle validates whether its current position falls within the task's effective area. If the validation is positive, the cloud server dispatches the corresponding task to the sensing vehicle.
- **Submission of Data.** The sensing vehicles relay the sensing data to the cloud server via RSUs.

- **Verification of Data and Updating of Information.** The cloud server checks the authenticity of the sensing data provided by each sensing vehicle, creates a reputation feedback report and forwards it to the reputation center. The reputation center, in turn, updates the pseudonym and reputation value of the sensing vehicle.
- **Information Tracing.** When necessary, for instance when a vehicle is identified as malicious and court requires the vehicle's information, the reputation center uses a master private key to access the location, identity, and reputation information of the sensing vehicle.

5.2 Details of the scheme proposed from a technical perspective

Step 1: Initializing the system

- 1.1 **Key pair generation and system parameters initialization:** Based on a given security parameter κ , we select two safe primes p, q in a way that $p' = (p - 1)/2$ and $q' = (q - 1)/2$ are also primes. Let $n = pq$ and $\mathbb{G}_1$ represents the cyclic group of quadratic residues modulo n^2 , with g_1 having the maximal order in it. The reputation center and the data requester pick secret parameters a, b from the range $[1, \text{ord}(\mathbb{G}_1)]$ and generate their key pairs as $(PK_{DR} = g_1^a, SK_{DR} = a)$ and $(PK_{RC} = g_1^b, SK_{RC} = b)$.
- 1.2 **Assignment of vehicle's pseudonym:** During the registration phase initiated by the reputation center, the actual identities of the sensing vehicles are represented as RID_i for $i = 1, 2, \dots, m$. The reputation center selects a cyclic group $\mathbb{G}_2$ of order q , with g_2 being its generator. For each vehicle identified by RID_i , the reputation center randomly selects a number w_i from $\mathbb{Z}_q$ and a secret value x from $\mathbb{Z}_q$. The pseudonym $PID_i = \{PID_1, PID_2\}$ is generated using ElGamal encryption, where $PID_1 = g_2^{w_i}$, $PID_2 = RID_i \cdot h_{pub}^{w_i}$ and $h_{pub} = g_2^x$. Subsequently, the reputation center picks a random number r_i from the range $[1, n/4]$, and employs the BCP encryption algorithm to create the ciphertext for the reputation value $[t_i] PKRC = \{T_i, T'_i\} = \{PK_{RC}^{r_i} \cdot (1 + n)^t, g_1^{r_i}\} \pmod{n^2}$. Then, a signature for $[t_i] PKRC$ is generated as $\sigma_i = h^{x_i}$, where $x_i \in \mathbb{Z}_q$ is the key for signing, $h = H([t_i] PKRC)$ and H is a cryptographic hash function. The reputation center discloses the system parameter $\{n, g_1, g_2, \mathbb{G}_1, \mathbb{G}_2, h_{pub}, H, y, PK_{DR}, PK_{RC}\}$ and sends $\{PID, [t_i] PKRC, \sigma_i\}$ to the vehicle identified by RID_i through RSU.

Step 2. Distribution of Tasks

- 2.1 **Assignment of Standard Values:** The sensor task data m is released by the data requester who subsequently employs proxy re-encryption to determine the initial ciphertext $[m]$. Utilizing its own public key along with the BCP encryption algorithm,

it generates ciphertexts $[d_0]_{PK_{DR}}$ and $[\Delta d]_{PK_{DR}}$, wherein

$$\begin{aligned} [d_0]_{PK_{DR}} &= \{T_{d_0}, T'_{d_0}\} = \{PK_{DR}^r * (1+n)^{d_0}, g_1^r\} \pmod{n^2} \\ [\Delta d]_{PK_{DR}} &= \{T_{\Delta d}, T'_{\Delta d}\} = \{PK_{DR}^r * (1+n)^{\Delta d}, g_1^r\} \pmod{n^2} \end{aligned}$$

2.2 Construction of Task Index: The data requester segregates the entire region into n task segments. For block number i , the reputation center firstly initiates the key pair (PK_{Ti}, SK_{Ti}) of that task block. Next, the central point coordinates (x_0, y_0) , the radius r , and the reputation threshold t_0 are encrypted using the corresponding private key and BCP encryption algorithm, thereby acquiring the ciphertext $[x_0]_{PK_{Ti}}, [y_0]_{PK_{Ti}}, [r]_{PK_{Ti}}, [t_0]_{PK_{Ti}}$. The data requester adds the task TSK_i to the task index TSK after its initialization. Lastly, the task index $TSK = \{TSK_1, TSK_2 \dots TSK_n\}$ is constructed, where $TSK_i = \{[x_0]_{PK_{Ti}}, [y_0]_{PK_{Ti}}, [r]_{PK_{Ti}}, [t_0]_{PK_{Ti}}, PK_{Ti}\}$ for $i = 1, 2, \dots, n$.

2.3 Task Broadcasting: Once task initialization is complete for all tasks, the data requester transmits $I_d = \{[m], [d_0]_{PK_{DR}}, [\Delta d]_{PK_{DR}}, TSK, PK_{DR}\}$ to the cloud server. The cloud server broadcasts $I_c = \{PK_{DR}\}$ within the crowdsensing region upon receipt of I_d .

Step 3. Enrolling Vehicles

3.1 Matching Location: The vehicle equipped with sensors retrieves I_c , determines its present position coordinates as (x, y) , and then employs the public key of the data requester along with the BCP encryption technique to compute the encrypted coordinates: $([x]_{PK_{DR}}, [y]_{PK_{DR}})$. It's defined as:

$$\begin{aligned} [x]_{PK_{DR}} &= \{T_x, T'_x\} = \{PK_{DR}^r \cdot (1+n)^x, g_1^r\} \pmod{n^2} \\ [y]_{PK_{DR}} &= \{T_y, T'_y\} = \{PK_{DR}^r \cdot (1+n)^y, g_1^r\} \pmod{n^2} \end{aligned}$$

Subsequently, the sensing vehicle transmits $I_v = \{PID, [t_i]_{PK_{RC}}, \sigma_i, ([x]_{PK_{DR}}, [y]_{PK_{DR}})\}$ to the remote server.

3.2 Choosing a Vehicle: On obtaining I_v , the cloud server initiates a check on the pseudonym PID and the signature σ_i to confirm their authenticity. If they are not authenticated, the server ends its communication with the vehicle. If authenticated, the server ascertains the tasks the vehicle engages in and checks if the vehicle's reputation score t surpasses the threshold t_0 . For a task denoted as $TSK_i = \{[x_0]_{PK_{Ti}}, [y_0]_{PK_{Ti}}, [r]_{PK_{Ti}}, [t_0]_{PK_{Ti}}\}$ within the task list TSK , the server leverages the additive homomorphic feature and Secure Less Than Protocol (SLT)[12] to see if $[t_i]_{PK_{RC}}$ and $[t_0]_{PK_{Ti}}$ adhere to:

$$\begin{cases} t_i \geq t_0 \\ (x - x_0)^2 + (y - y_0)^2 \leq r^2 \end{cases}$$

In cases where the vehicle's position and reputation scores are deemed valid, the server includes the task's sequence number i into the vehicle's existing task list T .

- 3.3 Task Re-allocation:** Post the screening of the task list T , the cloud server utilizes the proxy re-encryption method to transform the task message $[m]$ into its conclusive encrypted form $[m]'$. In the end, $I_c = \{[m]', T\}$ is dispatched to the vehicle equipped with sensors.

Step 4. Submitting the Data

Upon receiving the ciphertext $[m]'$, the vehicle involved in sensing deciphers it, leading to the acquisition of task details m . This vehicle then initiates the specified sensing task, producing data d . It employs the BCP encryption method to create the ciphertext for this data, $[d]_{PK_{T_i}}$. In the end, the vehicle forwards $I_v = \{PID, [d]_{PK_{T_i}}, T\}$ to the server in the cloud.

Step 5. Authentication of Data and Updating Information

- 5.1 Validation of the Sensing Data:** Once the cloud server receives I_v , it begins by confirming the legitimacy of the vehicle's pseudonym. After a successful validation, it evaluates d' and Δd using $[d']_{PK_\Sigma}$ and $[\Delta d]_{PK_{DR}}$. To elaborate, the server initially computes:

$$[d']_{PK_\Sigma} = \begin{cases} [d - d_0]_{PK_\Sigma} & d \geq d_0 \\ [d_0 - d]_{PK_\Sigma} & d < d_0 \end{cases}$$

Post this, d' and Δd are assessed using $[d']_{PK_\Sigma}$ and $[\Delta d]_{PK_{DR}}$. If the condition $d' \leq \Delta d$ is met, the data is deemed valid. If not, the server declines the sensing data.

- 5.2 Creation of Reputation Feedback:** Depending on the outcome from the sensing data's verification, the cloud server formulates a feedback report F for every vehicle and forwards $I_c = \{PID, F\}$ to the reputation center. This is represented as:

$$F = \begin{cases} 1 & d' \leq \Delta d \\ 0 & d' > \Delta d \end{cases}$$

- 5.3 Reputation and Pseudonym Refreshment:** Initially, the reputation center checks the authenticity of the PID. If found authentic, the reputation score of every vehicle is updated. The center then evaluates the change Δt in the vehicle's reputation score and proceeds to update the score as:

$$[t'_i]_{PK_{RC}} = \begin{cases} [t_i + \Delta t]_{PK_{RC}} = [t_i]_{PK_{RC}} * [\Delta t]_{PK_{RC}} \\ [t_i - \Delta t]_{PK_{RC}} = [t_i]_{PK_{RC}} * [\Delta t]_{PK_{RC}}^{n-1} \end{cases}$$

Subsequently, a signature σ'_i is produced for $[t'_i]_{PK_{RC}}$. The vehicle's pseudonym is then renewed as $PID' = \{PID'_1, PID'_2\}$, where $PID'_1 = g^{wit}$, $PID'_2 = RID_i \times$

h_{pub}^{wi} . The final step involves the reputation center dispatching $\{PID', [t'_i]_{PK_{RC}}, \sigma'_i\}$ to the vehicle identified as RID_i . The vehicle then refreshes its identity and reputation score.

Step 6: Tracing Information

- 6.1 **Tracing of Identity:** The genuine identity of the vehicle, denoted by RID , is concealed within $PID_i = \{PID_1, PID_2\}$. Here, $PID_1 = g_2^{wi}$ and $PID_2 = RID_i \cdot h_{pub}^{wi}$ with $h_{pub} = g_2^x$. By employing the system's private key, the reputation center has the capability to calculate g_2^{wi*x} and deduce the real identity, $RID_i = PID_2 \cdot g_2^{-wi*x} = RID_i \cdot h_{pub}^{wi} \cdot g_2^{-wi*x}$, of the vehicle that provides the sensing data.
- 6.2 **Tracing of Reputation Value:** In the context of multi-task crowdsensing, one can track the reputation score of sensing vehicles. For instance, $[t_i]_{PK_{RC}} = \{T_i, T'_i\} = \{PK_{RC}^r * (1+n)^t, g_1^r\} \pmod{n^2}$. Using the system's master private key, $\lambda(n)$, the reputation center initially computes $T_i^{\lambda(n)} \pmod{n^2} = g_1^{b*r*\lambda(n)}(1+n)^{t*\lambda(n)} \pmod{n^2} = (1+tn\lambda(n))$. By defining $L(x) = \frac{x-1}{n}$, the center can further determine the reputation score as $t = L\left(T_i^{\lambda(n)} \pmod{n^2}\right) \cdot \lambda(n)^{-1} \pmod{n}$.
- 6.3 **Tracing of Location:** When aiming to uncover the location details of sensing vehicles in multi-task crowdsensing scenarios, consider $[x]_{PK_{DR}}$ for illustration. With the master private key, $\lambda(n)$, the reputation center is able to derive $x = L\left(T_i^{\lambda(n)} \pmod{n^2}\right) * \lambda(n)^{-1} \pmod{n}$. In a similar vein, the center can determine values for y and r to retrieve the sensing vehicle's precise location.

6 Analysis

6.1 Security Analysis

This section discusses the robustness of our suggested approach, focusing on its achievement of essential security attributes like correctness, conditional privacy maintenance, and authentication.

Correctness: A comprehensive proof of this attribute is not provided due to space constraints. Broadly, it is evident that encryption can be properly decrypted and valid signatures can be confirmed. Consequently, when all involved entities act sincerely, the system yields accurate results.

Conditional Privacy Maintenance: For this attribute, we argue that specific sensitive details of any vehicle, including its location, identity, and reputation score, remain shielded from potential adversaries. Nevertheless, the trusted entity can access this information when deemed necessary.

- *Location Confidentiality:* The scheme proposed ensures that while the adversary $\mathcal{A}$ can intercept the message $I_v = \{PID, [t_i]_{PK_{RC}}, \sigma_i, ([x]_{PK_{DR}}, [y]_{PK_{DR}})\}$ from the

reporting vehicle, deducing the precise location coordinates remains unfeasible. BCP encryption, known for its semantic security under the DDH assumption over $\mathbb{Z}_{n^2}$, encrypts location data. Thus, adversaries cannot ascertain the vehicle’s position. Furthermore, while the cloud server might match vehicles based on their location for task assignments, adversaries remain ignorant of exact vehicle locations, ensuring location confidentiality.

- *Identity Confidentiality:* Within our scheme, adversaries may aspire to determine the genuine identity RID of the reporting vehicle. Although the actual identity RID is wrapped within PID_i , it remains inaccessible for adversaries due to encryption intricacies and lack of the necessary secret key. Leveraging the DDH presumption over $\mathbb{Z}_{n^2}$, our approach ensures identity protection.
- *Reputation Score Confidentiality:* Potential adversaries might aim to discern the reputation score of the reporting vehicle. Even though they might intercept related ciphertexts, the actual reputation value remains hidden, courtesy of BCP encryption’s semantic security. Thus, our system effectively maintains reputation score confidentiality.
- *Traceability:* The true identity RID is embedded within the pseudonym, but system private keys allow the reputation center to decipher the real vehicle identity. Similarly, trusted entities can discern location and reputation scores, ensuring the system’s traceability.

Authentication: In the scheme, senders digitally sign all messages. Receivers, on their end, accept messages only post successful signature validation. With digital signature security, it becomes infeasible for adversaries to alter or fabricate messages unnoticed. Therefore, the approach satisfactorily accomplishes authentication.

Defence Against Other Threats: The approach has been designed to defend against multiple threats, such as inference, reputation linkage, data manipulation, Sybil, and reputation manipulation attacks.

- With the discussed protections, our system effectively thwarts adversaries like data requesters and cloud servers from location, identity, or reputation inference attacks. Additionally, the randomized encryption of reputation values equips the scheme with defenses against reputation linkage attacks.
- In real-world multi-task crowdsensing scenarios, ill-intentioned vehicles might relay incorrect sensing data. Our system, by comparing data validity metrics, can discern and reject such misleading data, ensuring data integrity.
- As the pseudonym of each reporting vehicle is regulated by the reputation center, malicious vehicles cannot simulate multiple identities, ensuring defense against Sybil attacks. Furthermore, the system’s cryptographic checks ensure that only vehicles meeting reputation thresholds are verified, offering protection against reputation manipulation attacks.

6.2 Computation Overhead Analysis

During the initialization of the system, two large secure primes are first chosen. This selection can be achieved using the Miller-Rabin algorithm, which only needs to be run a single time. Following this, both the data requester and the reputation center calculate a key pair, each involving an exponentiation in G_1 . Subsequently, the reputation center formulates both an ElGamal ciphertext and a BCP ciphertext. The ElGamal ciphertext needs two exponentiations and a multiplication in G_2 , whereas the BCP ciphertext demands three exponentiations and a multiplication in G_1 . Moving to the task assignment phase, the data requester produces six BCP ciphertexts, necessitating eighteen exponentiations and six multiplications in G_1 . During the vehicle recruitment process, the sensing vehicle formulates two BCP ciphertexts, which involve six exponentiations and two multiplications in G_1 . For information tracing, tracing of identity requires an exponentiation and a multiplication in G_2 . When tracing reputation value, there's a need for an exponentiation and a multiplication in G_1 . For tracing of location, three exponentiations and equal multiplications in G_1 are needed. Owing to the efficient computation of these operations, the scheme proposed is notably efficient for practical applications.

Table 2: Summary of Operations and Their Requirements

Phase/Process	Operation	Requirement
Initialization	Secure primes selection	1 Miller-Rabin algorithm
	Key pair calculation	1 Exponentiation in G_1
	ElGamal ciphertext	2 exponentiations, 1 multiplication in G_2
	BCP ciphertext	3 exponentiations, 1 multiplication in G_1
Task Assignment	BCP ciphertexts	18 exponentiations, 6 multiplications in G_1
Vehicle Recruitment	BCP ciphertexts	6 exponentiations, 2 multiplications in G_1
Information Tracing	Identity tracing	1 exponentiation, 1 multiplication in G_2
	Reputation value tracing	1 exponentiation, 1 multiplication in G_1
	Location tracing	3 exponentiations, 3 multiplications in G_1

Table 3: Computation Overhead Comparison of Sensing Vehicle in our scheme, PACE, and SPOON Schemes

Scheme	Computation Overhead	Runtime (ms)
SPOON [16]	$34T_{pm} + 21T_{pa} + 4T_{bm} + 23T_{exp}$	353.581
PACE [22]	$12T_{gc}$	240
our scheme	$6T_{exp} + 2T_{mul}$	43.035

TABLE 2 shows the calculate requirements of each phase in our scheme. Subsequently, we juxtapose the computational load of individual sensing vehicles against other distinguished MCS methodologies [16], [22]. Let w symbolize the count of sensing vehicles engaged in sensing assignments. To ensure a balanced comparison, only the task distribution and data submission phases are taken into account for the SPOON approach [16].

As evident from TABLE 3, the computational burden per sensing vehicle in our scheme is notably lower than its counterparts when $w = 1$. In the context of the SPOON approach, T_{pm} , T_{pa} , T_{bm} , and T_{exp} denote the durations for operations such as point multiplication, point addition, bilinear mapping, and exponentiation, respectively. Meanwhile, T_{gc} stands for the Commitment generation duration in the PACE scheme.

In our proposed framework, it is noteworthy that vehicles engaged in sensing are only required to compute the BCP ciphertext of their current position during the 'Enrolling Vehicles' phase (Step 3). Consequently, when juxtaposed with alternative schemes, our methodology exhibits a distinct advantage in reducing the computational overhead for sensing vehicles.

6.3 Communication Overhead Analysis

Communication overhead is a crucial factor in determining the efficiency of a cryptographic scheme, especially in multi-task environments where multiple entities are involved and frequent data exchanges occur. Here, we will analyze the communication overhead of the described scheme.

Table 4: Symbols and Descriptions Utilized in Communication Overhead Analysis

Symbol	Description
$\mathcal{C}_{BCP}$	Size of a BCP ciphertext
$\mathcal{P}$	Size of a plaintext message
$\mathcal{S}$	Size of a signature
$\mathcal{H}$	Size of a hash output
$\mathcal{K}$	Size of a public/private key

Table 5: Communication Costs for Different Steps

Step	Communication Cost
Initializing the system	$2\mathcal{K} + \mathcal{C}_{BCP} + \mathcal{S}$
Distribution of Tasks	$2\mathcal{C}_{BCP} + n\mathcal{K}$
Enrolling Vehicles	$2\mathcal{C}_{BCP} + \mathcal{K} + \mathcal{S}$
Submitting the Data	$\mathcal{P} + \mathcal{C}_{BCP}$
Authentication of Data and Updating Information	$\mathcal{C}_{BCP} + \mathcal{S} + \mathcal{H}$
Tracing Information	$2\mathcal{C}_{BCP} + \mathcal{K}$
Total Communication Overhead	$9\mathcal{C}_{BCP} + 4\mathcal{K} + 3\mathcal{S} + \mathcal{P} + \mathcal{H}$

From Table 5, it's evident that the most recurring component in the communication cost is the BCP ciphertext, $\mathcal{C}_{BCP}$. The prominence of $\mathcal{C}_{BCP}$ in our scheme is not merely coincidental but is a strategic choice rooted in the inherent advantages of the BCP algorithm.

The BCP algorithm, as highlighted in numerous studies, offers a unique capability: it allows for the decryption of ciphertexts encrypted by a set of weak private keys using a strong private key in a batch processing manner. This batch decryption capability is particularly advantageous in multi-task environments. Instead of decrypting each ciphertext individually, which would be computationally intensive and time-consuming, the BCP algorithm facilitates the decryption of multiple ciphertexts simultaneously, leading to a significant reduction in computational overhead.

In multi-task environments, where numerous entities are involved, and data exchanges are frequent, the ability to batch process decryption becomes invaluable. For instance, consider a scenario where a central entity needs to decrypt messages from multiple senders. Traditional cryptographic schemes would require the central entity to decrypt each message individually. However, with the BCP algorithm, if these messages are encrypted using weak private keys, the central entity can leverage its strong private key to decrypt them in batches, thereby reducing the time and resources required.

In our proposed scheme, by leveraging the BCP algorithm’s strengths, we aim to strike a balance between robust security and optimized efficiency. The choice of BCP is strategic, ensuring that as the system scales and the number of tasks increases, the communication overhead does not grow prohibitively.

7 Conclusion

In our study, we introduced a novel scheme tailored for multi-task vehicular networks, addressing key challenges of efficiency and multi-faceted information privacy. The scheme offers:

- **Multi-Type Privacy Protection:** It robustly safeguards various vehicular information, including location, identity, and reputation scores. While ensuring privacy, the scheme’s traceability allows trusted entities to access vital information when necessary.
- **Enhanced Efficiency:** Our scheme emphasizes efficiency, as demonstrated by its computational and communication overhead metrics. The integration of the BCP algorithm, renowned for batch decryption, notably diminishes computational overhead, particularly in multi-task settings.
- **Support for Multi-Tasks:** Designed for multi-task vehicular networks, our scheme ensures secure task distribution and submission while optimizing communication overhead. The BCP algorithm’s batch processing capability ensures scalability and efficiency as task numbers increase.

In essence, our scheme merges strong security with optimal efficiency, positioning it as a viable solution for modern multi-task vehicular networks. As these networks grow in complexity, our scheme will be pivotal in facilitating secure, seamless interactions, data

sharing, and task execution, all while preserving privacy and resource optimization. Future research will delve into a stringent security framework, challenging the assumption of honest-but-curious behavior among entities like data requesters, cloud servers, and Road-side Units (RSUs). Additionally, we plan to establish verification mechanisms to confirm the integrity and authenticity of these entities.

References

- [1] Emmanuel Bresson, Dario Catalano, and David Pointcheval. A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 37–54. Springer, 2003.
- [2] Xinlei Chen, Susu Xu, Jun Han, Haohao Fu, Xidong Pi, Carlee Joe-Wong, Yong Li, Lin Zhang, Hae Young Noh, and Pei Zhang. Pas: Prediction-based actuation system for city-scale ridesharing vehicular mobile crowdsensing. *IEEE Internet of Things Journal*, 7(5):3719–3734, 2020.
- [3] Minghui Dai, Zhou Su, Qichao Xu, Yuntao Wang, and Ning Lu. A trust-driven contract incentive scheme for mobile crowd-sensing networks. *IEEE Transactions on Vehicular Technology*, 71(2):1794–1806, 2021.
- [4] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, and Alejandro Quintero. Vanet security surveys. *Computer Communications*, 44:1–13, 2014.
- [5] Raghu K Ganti, Fan Ye, and Hui Lei. Mobile crowdsensing: current state and future challenges. *IEEE communications Magazine*, 49(11):32–39, 2011.
- [6] Sheng Gao, Xiuhua Chen, Jianming Zhu, Xuewen Dong, and Jianfeng Ma. Trust-worker: A trustworthy and privacy-preserving worker selection scheme for blockchain-based crowdsensing. *IEEE Transactions on Services Computing*, 15(6):3577–3590, 2021.
- [7] Gilles Guette and Olivier Heen. A tpm-based architecture for improved security and anonymity in vehicular ad hoc networks. In *2009 IEEE Vehicular Networking Conference (VNC)*, pages 1–7. IEEE, 2009.
- [8] Debiao He, Sherali Zeadally, Baowen Xu, and Xinyi Huang. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Transactions on Information Forensics and Security*, 10(12):2681–2691, 2015.
- [9] Hao Hu, Rongxing Lu, Cheng Huang, and Zonghua Zhang. Tripsense: A trust-based vehicular platoon crowdsensing scheme with privacy preservation in vanets. *Sensors*, 16(6):803, 2016.

- [10] Hao Hu, Rongxing Lu, Zonghua Zhang, and Jun Shao. Replace: A reliable trust-based platoon service recommendation scheme in vanet. *IEEE Transactions on Vehicular Technology*, 66(2):1786–1797, 2016.
- [11] Cheng Huang, Rongxing Lu, and Kim-Kwang Raymond Choo. Vehicular fog computing: architecture, use case, and security and forensic challenges. *IEEE Communications Magazine*, 55(11):105–111, 2017.
- [12] Ximeng Liu, Robert H Deng, Kim-Kwang Raymond Choo, and Jian Weng. An efficient privacy-preserving outsourced calculation toolkit with multiple keys. *IEEE Transactions on Information Forensics and Security*, 11(11):2401–2414, 2016.
- [13] Zhiqian Liu, Feiran Huang, Jian Weng, Kun Cao, Yinbin Miao, Jingjing Guo, and Yongdong Wu. Btmpp: Balancing trust management and privacy preservation for emergency message dissemination in vehicular networks. *IEEE Internet of Things Journal*, 8(7):5386–5407, 2020.
- [14] Rongxing Lu, Xiaodong Lin, Haojin Zhu, P-H Ho, and Xuemin Shen. Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications. In *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pages 1229–1237. IEEE, 2008.
- [15] Lichuan Ma, Xuefeng Liu, Qingqi Pei, and Yong Xiang. Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing. *IEEE Transactions on Services Computing*, 12(5):786–799, 2018.
- [16] Jianbing Ni, Kuan Zhang, Qi Xia, Xiaodong Lin, and Xuemin Sherman Shen. Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing. *IEEE Transactions on Mobile Computing*, 19(6):1317–1331, 2019.
- [17] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *International conference on the theory and applications of cryptographic techniques*, pages 223–238. Springer, 1999.
- [18] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of computer security*, 15(1):39–68, 2007.
- [19] Gang Sun, Siyu Sun, Hongfang Yu, and Mohsen Guizani. Toward incentivizing fog-based privacy-preserving mobile crowdsensing in the internet of vehicles. *IEEE Internet of Things Journal*, 7(5):4128–4142, 2019.
- [20] Leye Wang, Daqing Zhang, Dingqi Yang, Brian Y Lim, Xiao Han, and Xiaojuan Ma. Sparse mobile crowdsensing with differential and distortion location privacy. *IEEE Transactions on Information Forensics and Security*, 15:2735–2749, 2020.

- [21] Chuan Zhang, Liehuang Zhu, Chang Xu, Kashif Sharif, Kai Ding, Ximeng Liu, Xiaojiang Du, and Mohsen Guizani. Tppr: A trust-based and privacy-preserving platoon recommendation scheme in vanet. *IEEE Transactions on Services Computing*, 15(2):806–818, 2019.
- [22] Bowen Zhao, Shaohua Tang, Ximeng Liu, and Xinglin Zhang. Pace: Privacy-preserving and quality-aware incentive mechanism for mobile crowdsensing. *IEEE Transactions on Mobile Computing*, 20(5):1924–1939, 2020.