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

Yichen Huang

August 19, 2023

Abstract

Crowdsensing using mobile platforms is a technique that employs a vast array of mobile gadgets to gather and process environmental data for a range of applications, revealing both advantages and hurdles in data integrity, privacy, and security. This establishes a cost-effective and easily scalable sensing paradigm. As vehicular networks evolve, many researches delve into the feasibility of integrating vehicles as data collection nodes in the realm of mobile crowdsensing. Nonetheless, there are notable limitations in a sizable chunk of these investigations. To begin with, some have either bypassed conditional privacy measures or have not included protection for the reputation metric. Next, many overlook the complex nature of the vehicular network's multitasking capability, leading to pronounced inefficiency and data storage issues. To address these limitations, we recommend an approach focusing on conditional privacy within a versatile mobile crowdsensing architecture tailored for vehicular systems. This proposed method strikes a balance between supervisory needs and privacy measures, embodying a trait termed as conditional privacy. Moreover, each vehicle is endowed with the ability to simultaneously partake in various data sensing operations. To be precise, the protective measures include safeguarding identity, geographical position, and reputation simultaneously. While the reputation hub refreshes vehicle pseudonyms, it forgoes the need to retain any intrinsic data, such as transient keys or arbitrary figures, thereby lowering the chance of DoS attacks. Consequently, this paves the way for a safer and more viable option in the domain of mobile crowdsensing. Thorough security analysis validates that our strategy complies with essential security benchmarks like precision, conditional privacy assurance, and user verification. Efficiency evaluations suggest our model's potent applicability in the diversified tasks of mobile crowdsensing.

Keywords: Vehicular Networks · Privacy Preserving · Muti-Task · Encryption Algorithm

1 Introduction

With the progression of mobile internet and the proliferation of smart devices with embedded sensors, the concept of mobile crowdsensing (MCS) has gained prominence[5]. MCS, with its ability to sense, accumulate, and process environmental data, is rapidly becoming an essential tool in various domains such as transportation, health, and clinical care. In light of recent advancements, vehicles are now integrated with a myriad of sensors, rendering them aptly suited for inclusion as sensing nodes within mobile crowdsensing frameworks.[2][11] Additionally, vehicular networks bring forth several advantages like high maneuverability, energy efficiency, and straightforward setup and maintenance. This has led to an upsurge in their incorporation in MCS, captivating both scholarly and industrial sectors. In such frameworks, the MCS structure chiefly includes three elements: entities requesting data, a centralized cloud server, and vehicles with sensing capabilities.

These sensor-imbued vehicles have the capacity to perform sensing operations in both urban and rural terrains, positioning them perfectly for applications reliant on mobility.[2] Nevertheless, the inherent openness of vehicular networks makes them susceptible to various threats. For example, vehicle-associated sensors and control systems might be vulnerable to external meddling or unauthorized alterations. Malevolent vehicles equipped with sensors could not just forge or tamper with data, jeopardizing its genuineness and consistency, but might also stealthily acquire sensitive details such as individual identities and geolocations, thereby lowering public trust in such advanced systems. As a countermeasure, trustworthiness often hinges on a reputation metric.[15] [3] This metric, typically overseen by a reputational hub, enables the cloud server to evaluate vehicle reliability based on data accuracy, subsequently relaying its findings to the hub which then updates the vehicle's reputation score.[16] Yet, orchestrating this reputation score grows increasingly intricate when a vehicle partakes in several sensing operations concurrently. Beyond that, while ensuring protection of privacy concerning location and identity does result in added computational and communication burdens, adding reputation score safeguards may further compound system intricacies.

Lately, numerous MCS approaches have integrated the reputation metric to gauge participant reliability. Still, a majority solely focus on safeguarding the vehicle's identity[21] and geolocation[20], overlooking reputation scores[19]. Such gaps permit malicious entities to potentially exploit these scores to infer vehicle paths or even deduce its identity. Additionally, many of the present strategies cater to singular sensing assignments, rendering them unsuitable for multi-task sensing scenarios. When relying on pseudonymous privacy protection techniques, the central server is burdened with the storage of arbitrary numbers for pseudonym updates, amplifying storage demands and making the system prone to denial-of-service (DoS) assaults.

Beyond these challenges, achieving conditional privacy conservation remains pivotal in vehicular infrastructures.[14] On one spectrum, hostile forces might tap into transmissions to extract confidential data, resulting in grave privacy infringements. On the opposite end, there's a need for trustworthy entities to enforce stringent monitoring, for instance, unveiling a vehicle's actual identity when deemed necessary.[18] Thus, vehicular networks

ought to provide conditional privacy measures, harmonizing between safeguarding privacy and fulfilling supervisory necessities. This stringent prerequisite mandates that only the trusted agency should have the privilege to extract genuine identity, geolocation, and reputation data of a vehicle.

To tackle the aforementioned hurdles, the aims of this manuscript are outlined below:

- We introduce a precise, actionable, and implementable mobile sensing strategy that endorses multi-task mobile sensing alongside conditional privacy safeguards for various data types in vehicular systems, emphasizing on privacy of identity, geolocation, and reputation.

- The efficacy of our approach can be gauged through real-world deployments and subsequent evaluations in a server ecosystem, specifically focusing on the temporal and storage overheads during its operational phase.

- Employing techniques such as pseudonym validation, cryptographic signatures, the BCP algorithm, and homomorphic encryption, our strategy's goals are realistic, ensuring conditional privacy for diverse data categories in a multi-task vehicular environment.

- Our proposition is timely and pertinent, addressing the current privacy and security quandaries within vehicular networks, furnishing a robust and pragmatic resolution to the predominant privacy obstacles these systems confront.

- The entire operational cycle, from the deployment phase to the evaluation stage, is designed to adhere to the set project timeframe, assuring timely availability of insights for subsequent interpretation and deductions.

The subsequent sections of this report are structured as follows. Section 2 delves into related academic contributions. Section 3 elucidates the Methodologies and Fundamental concepts underpinning our strategy. Section 4 provides insights into the system's framework, security paradigms, and essential security requisites, while Section 5 delineates our proposed solution. Section 6 encompasses security scrutiny, computational overhead, and communication overhead. The final part, Section 7, concludes the manuscript and stimulates discussion.

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.

Following this, reputation management systems [10][9][13] were introduced. They suggested that instead of updating trust scores solely on individual tasks, one should also determine the weight of recent reputation scores considering reputation feedback reports and vehicles' initial reputation scores. By factoring in the multi-task scenario, these methods offer a refined assessment of the sensing vehicles' reliability.

With the advancement in vehicular sensor technology and the maturity of vehicular network mobile sensing, the need for privacy protection in multi-task settings grows more pressing. Moreover, the integrity and privacy of vehicle reputation scores are paramount. If such data becomes public, ill-intentioned entities could deduce driving behaviors and paths, leading to potential leaks of location and trajectory details, which in turn, puts vehicle owners' privacy at risk. Yet, most of the present vehicular network mobile sensing methods, despite acknowledging the importance of reputation scores, often neglect the safeguarding of these scores.

In the approach presented by [13], a decentralized method grounded in privacy protection for trust management was put forward to mediate the ties between trust and privacy during emergency communication in vehicular networks. This approach utilizes identity-centric encryption to associate a vehicle's identity data with its reputation score and introduces a randomization method based on obfuscation to secure the privacy of the vehicle's reputation score. Nevertheless, the potential risks linked to the interception or modification of reputation scores linger as potential vulnerabilities.

Within the framework of [16], prior to a sensing vehicle conveying its reputation score to the central repository, the score undergoes encryption, making it readable to the reputation center only post-decryption. However, even when encryption, obfuscation, and anonymization tools are deployed, deducing the reputation scores of participants remains feasible. For example, a malevolent actor might analyze the reputation scores across various participants to approximate the actual reputation score of each one.

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 preserv-

ing 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.

Although this design has certain shortcomings, the primary issue is that both cars and reliable third parties demand a lot of storage capacity for holding data. Additionally, if a rogue vehicle transmits incorrect information, pinpointing its identity consumes a considerable period.

In response to above challenges, paper [14] introduced a protocol called ECPP (Efficient Conditional Privacy Preservation). This protocol is designed to attain conditional privacy safeguarding without necessitating excessive storage overhead. The fundamental principle behind the ECPP protocol revolves around creating trusted secure connections through public key certificate exchanges. This ensures protected data transmission and sharing amongst vehicles, all while maintaining user discretion. To bolster this protection of vehicle users' privacy, the ECPP approach integrates attribute-based encryption methods. This ensures conditional access, where only cars that fulfill specific criteria can decrypt and retrieve the shared data.

Moreover, to successfully realize conditional privacy maintenance, vehicles need to regularly acquire fresh anonymous credentials from the trust center. This is crucial since using the same certificates for prolonged durations makes them vulnerable to adversaries who might exploit them to track vehicles, posing a risk to user confidentiality. The primary concept behind the approach in [8] revolves around leveraging identity-based encryption methods and conditional access systems to validate vehicle user identities while also ensuring their privacy.

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 delve into a range of foundational techniques crucial for building the system we're proposing. These techniques encompass both homomorphic encryption, digital signatures and the BCP encryption approach.

3.1 Homomorphic Encryption

The Paillier cryptosystem[17], possessing an additive homomorphic feature, emerges as a predominant encryption technique. Let's consider we possess N data elements encrypted via a uniform public key pk, symbolized as $[m_i]_{pk} \quad (i = 1, 2, \ldots, N)$. This encryption with additive homomorphic properties guarantees that the following relation stays valid:

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

where $D_{sk}()$ represents the decryption procedure associated with the private key sk. Liu[12] has put forth certain enhancements that can serve as tools for managing encrypted information, such as:

- **Secure Less Than (SLT) Protocol:**The SLT protocol is designed to securely determine the relation between two encrypted numbers. Given two encrypted values, say $[x]_{pk}$ and $[y]_{pk}$, the SLT protocol allows one to ascertain an encrypted bit based on whether $x \geq y$ or $x < y$ without revealing any information about x and y. This encrypted bit can be utilized in various cryptographic computations, ensuring the security of data during processing.

- **Secure Equivalent Testing (SEQ) Protocol:**The SEQ protocol, on the other hand, is crafted to determine if two encrypted numbers are equivalent. When presented with two encrypted values $[x]_{pk}$ and $[y]_{pk}$, the SEQ protocol can establish an

encrypted bit that indicates whether the plaintexts of these two numbers are equal (i.e., $x = y$). This is particularly beneficial in scenarios where one needs to compare encrypted data without compromising the confidentiality of the underlying values.

3.2 Digital Signatures

Digital signatures are cryptographic counterparts to handwritten signatures or stamped seals, but much more secure. Their main purpose is to guarantee the authenticity and integrity of a message, transaction, or any digital document. A proper digital signature gives a recipient reason to believe that the message was created by a known sender and that it was not altered in transit.

Given the provided information, the signature generation mechanism can be described as follows:

Key Generation: For the signature scheme, each entity has a pair of cryptographic keys - a private signing key and a public verification key. In the context of the information provided, $x_i \in \mathbb{Z}q$ is the private key used for signing.

Signature Generation:

- Take the encrypted reputation value $[t_i]_{PK_{RC}}$as the message that needs to be signed.
- Compute the cryptographic hash of the message using a cryptographic hash function H. This results in a hash value h, mathematically represented as $h = H\left([t_i]_{PK_{RC}}\right)$.
- The hash value h is then transformed using the private signing key x_i to produce the signature, represented as $\sigma_i = h^{xi}$.

Signature Verification: To verify a signature, the receiver uses the public verification key associated with the sender. They will compute the hash of the received message and compare it to the value derived from the received signature. If both values match, then the signature is valid; otherwise, it's invalid.

This mechanism ensures that even the smallest change in the original document would result in a significantly different signature, making alterations detectable.

3.3 The BCP Encryption Methodology

The BCP encryption[1] is elucidated in the following manner:

KeyGen: Start by selecting two prominent prime numbers p and q. Set n as the product of p and q. Establish g and h as two elements possessing the highest order within the cyclic group G, which is the group of quadratic residues modulo n^2. It's essential to recognize that if we determine h as $g^x \bmod n^2$, where x is chosen from the interval $[1, \lambda(n^2)]$ and $\lambda()$ represents the Euler function, then x tends to be coprime relative to $\mathrm{ord}(G)$. This ensures h has the peak order. The revealed parameters are n, g, and $h = g^x \bmod n^2$, whereas the concealed one is x from $[1, \mathrm{ord}(G)]$.

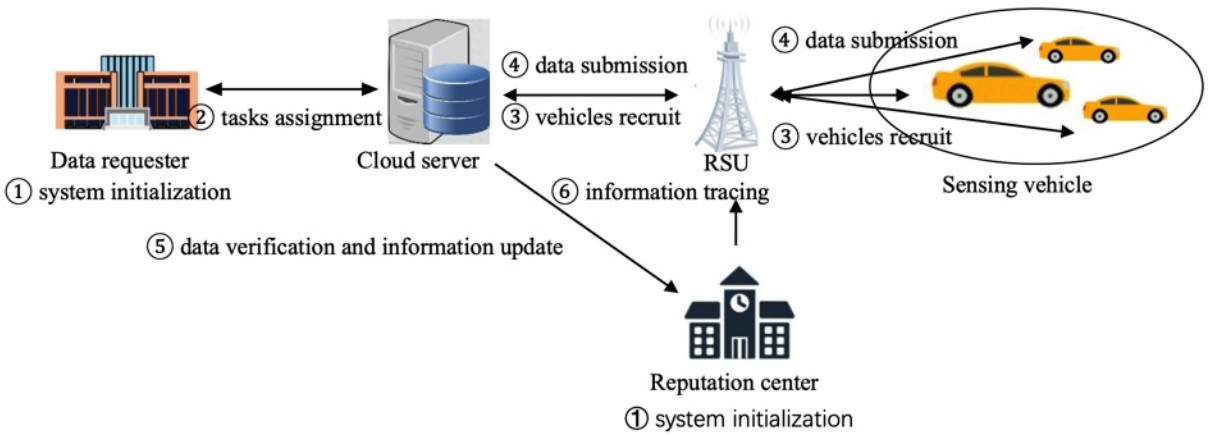

Figure 1: The system model of the multi-task sensing scheme.

Enc: Given a message m from Z_n, opt for a random element r from Z_n^*. The resulting ciphertext, denoted as $[m]$, is derived as $\{h^r(1+mn), g^r\} \bmod n^2$, where its components are represented as (T, T').

Decryption Leveraging Weak Private Key (WDec): By utilizing the confidential key x, the initial message m is retrievable via: $m = L\left(T/\left(T'\right)^x \bmod n^2\right)$, where the function $L(u)$ is described as $(u-1)/n$.

Decryption Employing Robust Private Key (SDec): Any given ciphertext is decryptable employing the robust private key represented as $SK = \lambda(n)$. The process involves:

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

Subsequently, m is deduced from:

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

4 Models and Definitions

In this section, we will present the security model, delineate the system model, and outline the necessary 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 Requester: 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. Additionally, the system evaluates the reliability of vehicles by examining the accuracy of the sensing data they provide, subsequently formulating a feedback report on reputation. Typically, these cloud servers come with strong computational capabilities and ample storage resources.

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: Usually equipped with a variety of sensors, these systems are responsible for gathering and archiving different environmental data. In addition to this, every vehicle sensor system includes an on-board unit (OBU)[4][7], which securely stores sensitive details, encompassing secret keys, user identities, geographical positions, and more.

4.2 Security Model

In this architecture, we operate under the assumption that the data requester, the cloud server, and the Road-Side Units (RSUs) exhibit honest-yet-curious behavior. This means that while they follow the established protocol, they might have the propensity to extract information they shouldn't. For example, within a vehicular network-dependent mobile crowdsensing environment, these entities, though generally honest, may attempt to decipher the locations, identities, and reputational specifics of sensing vehicles. Such a potential breach is termed as an *inference attack*, encompassing location, identity, and reputation inference attacks. Moreover, an ill-intentioned adversary, by eavesdropping on a series of reputation scores tied to a particular sensing vehicle, might infer insights like driving patterns. This attack is dubbed a *reputation linkable attack*.

The reputation center remains wholly trustworthy in this setup. The underlying assumption is that the majority of sensing vehicles are honest participants. However, a small faction of these vehicles may act maliciously, launching the following types of attacks:

- *Data pollution attack*: Malevolent sensing vehicles may deliberately feed inaccurate data, thereby adulterating the collective sensing outcomes.
- *Sybil attack*: These vehicles could either submit redundant data repeatedly or adopt fake personas, with an intention to either inflate their reputational scores or skew the aggregate sensing data.

- *Reputation tamper attack*: Vehicles that have garnered a low reputation might attempt to alter their reputation metrics, paving the way for them to participate in tasks they shouldn't be allowed in.

- *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. In a multi-task environment, should the situation necessitate, the trusted authority has the capability to derive the actual identity, location, and reputation value from the messages exchanged.

- *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 Initialization of Security Parameters, Secure Task Distribution, Vehicle Engagement, Encrypted Data Transmission, Data Integrity and Reputation Assessment, and finally, ecure Information Retrieval. The symbols utilized in the proposed scheme are subsequently encapsulated as follows:

Table 1: Formalized Notations in the Scheme

Notation	Definition
t_i	Reputation of the ith sensing vehicle.
t_0	Minimum reputation required for a sensing task.
m	Substance or content of a sensing task.
$[m]$	Encrypted form of the substance m.
d	Data collected from sensing.
d_0	Benchmark or standard value for the sensing data.
Δd	Maximum permissible error in the sensing data.
PK_{DR}, SK_{DR}	Public and private key pair for the data requester, respectively.
PK_{RC}, SK_{RC}	Public and private key pair for the reputation center, respectively.
(x, y)	Coordinates representing the location of the sensing task.
r	Sensing task's effective radius or coverage area.
TSK	Comprehensive list of all sensing tasks.
RID	Unique identity of a sensing vehicle.
PID	Pseudonym used by the sensing vehicle for anonymity.
T	Tasks in which a sensing vehicle participates.

5.1 Overview of the Proposed Method

For clarity in our exposition, an initial overview of the proposed method is presented. Consider a scenario involving a sensing task within an urban environment. Vehicles equipped with sensing capabilities that wish to partake in this activity need to satisfy both geographical and reputational prerequisites set for the task. For example, if a data requester designates a task and determines a reputational benchmark at t_0, it dictates that the vehicle's reputational score t should meet or exceed t_0. Moreover, the geographical position of the sensing vehicle must be encompassed within a circular region defined by a radius r as given by the task's specifications. Referring to Fig.1, the method integrates the ensuing procedures:

- **Initialization of Security Parameters**. The data requester collaborates with the reputation center to establish system parameters and cryptographic key pairs, optimized for the homomorphic encryption scheme. Subsequently, the reputation center allocates an initial reputation score to each vehicle, transmitting the vehicle's pseudonym and reputation score with the center's digital signature for authentication.

- **Secure Task Distribution**. The data requester securely forwards task specifications, including location constraints and reputation thresholds, to the central cloud server. The server then broadcasts these tasks to potential sensing vehicles via Road-Side Units (RSUs) using encrypted channels.

- **Vehicle Engagement**. Sensing vehicles verify their current geographical coordinates against the task's location criteria. If a match is found, the cloud server securely transmits detailed task instructions to the eligible vehicle.

- **Encrypted Data Transmission**. Vehicles that participate in the sensing task encrypt and send their collected data to the central cloud server through RSUs, ensuring data integrity and confidentiality.

- **Data Integrity and Reputation Assessment**. The central server decrypts and assesses the data quality from each sensing vehicle. Based on this evaluation, a reputation feedback report is generated and securely transmitted to the reputation center. The center then updates the vehicle's pseudonym and reputation score accordingly.

- **Secure Information Retrieval**. Under specific conditions, like detecting a malicious vehicle or responding to a legal request, the reputation center utilizes its master private key to securely retrieve the sensing vehicle's exact location, genuine identity, and current reputation score.

5.2 Details of the scheme proposed from a technical perspective

Step 1: Initialization of Security Parametersm

1.1 **Generation of Key Pair and Initialization of System Parameters**: Using the security parameter κ, we determine two safe primes, p and q, such that $p' = (p-1)/2$ and $q' = (q-1)/2$ stand as prime numbers. Define n as $n = pq$. The cyclic group $\mathbb{G}1$ comprises quadratic residues modulo n^2, where $g1$ holds the highest order. The reputation center and data requester derive secret parameters a and b from the range $[1, \mathrm{ord}\,(\mathbb{G}1)]$. Their key pairs are then formed as $(PKDR = g_1^a, SK_{DR} = a)$ and $(PK_{RC} = g_1^b, SK_{RC} = b)$.

1.2 **Pseudonym Allocation for Vehicles**: In the reputation center's registration phase, the actual identities of sensing vehicles are denoted as RID_i, where i spans from 1 to m. The reputation center designates a cyclic group $\mathbb{G}2$ of order q, with g_2 as its generator. For each vehicle labeled by $RIDi$, a number w_i is chosen randomly from $\mathbb{Z}_q$ along with a confidential value x from $\mathbb{Z}q$. Utilizing ElGamal encryption, the pseudonym $PIDi = \{PID_1, PID_2\}$ is formed, where $PID_1 = {g_2}^{wi}$ and $PID_2 = RID_i \times {h_{pub}}^{wi}$, with $h_{pub} = {g_2}^x$. The reputation center subsequently selects a random number r_i from $[1, \mathrm{n}/4]$, and applies the BCP encryption method to frame the encrypted reputation value $[t_i]_{PK_{RC}} = \{T_i, T_i'\} = \{{PK_{RC}}^{r_i} \times (1+n)^t, {g_1}^{r_i}\}\,(\bmod n^2)$. A corresponding signature for $[t_i]_{PK_{RC}}$, denoted as $\sigma_i = h^{xi}$, is created. Here, x_i from $\mathbb{Z}q$ is the signing key, $h = H\left([t_i]_{PK_{RC}}\right)$, and H is a cryptographic hash function. Lastly, the reputation center releases the system parameters $\{n, g_1, g_2, \mathbb{G}1, \mathbb{G}2, h_{pub}, H, y, PK_{DR}, PK_{RC}\}$ and dispatches $\left\{PID, [t_i]_{PK_{RC}}, \sigma_i\right\}$ to the vehicle identified as RID_i via RSU.

Step 2. Secure Task Distribution

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

$$[d_0]_{PK_{DR}} = \left\{T_{d_0}, T'_{d_0}\right\} = \left\{PK_{DR}^r * (1+n)^{d_0}, g_1^r\right\} \left(\mathrm{mod} n^2\right)$$
$$[\Delta d]_{PK_{DR}} = \{T_{\Delta d}, T'_{\Delta d}\} = \left\{PK_{DR}^r * (1+n)^{\Delta d}, g_1^r\right\} \left(\mathrm{mod} n^2\right)$$

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 $TSK = \{TSK_1, TSK_2 \ldots TSK_n\}$ is constructed, where $TSK_i = \left\{[x_0]_{PK_{Ti}}, [y_0]_{PK_{Ti}}, [r]_{PK_{Ti}}, [t_0]_{PK_{Ti}}, PK_{Ti}\right\}$ for $i = 1, 2, \ldots, n$.

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

Step 3. Vehicle Engagement

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:

$$[x]_{PK_{DR}} = \{T_x, T'_x\} = \{PK_{DR}^r \cdot (1+n)^x, g_1^r\} \left(\mathrm{mod} n^2\right)$$
$$[y]_{PK_{DR}} = \left\{T_y, T'_y\right\} = \{PK_{DR}^r \cdot (1+n)^y, {g_1}^r\} \left(\mathrm{mod} n^2\right)$$

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

3.2 **Vehicle Selection**: Once the cloud server retrieves I_v, it begins a verification process for the pseudonym PID and the signature σ_i to ensure their genuineness. Should the validation fail, the server terminates the interaction with the vehicle. On successful validation, the server evaluates the tasks associated with the vehicle and determines if the vehicle's reputation metric t exceeds the set benchmark t_0. Given a task represented as $TSK_i = \left\{[x_0]_{PK_{Ti}}, [y_0]_{PK_{Ti}}, [r]_{PK_{Ti}}, [t_0]_{PK_{Ti}}\right\}$ from the task set TSK, the

server applies the additive homomorphic property and Secure Less Than Protocol (SLT)[12] to verify if $[t_i]_{PK_{RC}}$ and $[t_0]_{PK_{Ti}}$ conform to:

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

If both the vehicle's location and reputation values are validated as appropriate, the server appends the task identifier i to the vehicle's prevailing task list T.

3.3 **Task Redistribution**: The cloud server employs the proxy re-encryption technique to convert the task data $[m]$ to its final encrypted version $[m]'$ after a thorough analysis of the task list T. Ultimately, the sensor-equipped vehicle will receive $I_c = \{[m]', T\}$.

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, $[d]_{PK_{Ti}}$. In the end, the vehicle forwards $I_v = \{PID, [d]_{PK_{Ti}}, T\}$ to the cloud.

Step 5. Data Integrity and Reputation Assessment

5.1 **Validation of the Multi-task Data**: Once the server in cloud 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, for each vehicle, constructs a feedback report F and transmits $I_c = \{PID, F\}$ to the center overseeing reputation. This is depicted 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 pseudonym of the vehicle undergoes an update to $PID' = \{PID'_1, PID'_2\}$. Here, PID'_1 is defined as $g^{wi'}$, while PID'_2 corresponds to $RID_i \times h_{pub}{}^{\text{wi'}}$. Subsequently, for the vehicle labeled as RID_i, the reputation center sends out $\left\{PID', [t'_i]_{PK_{RC}}, \sigma'_i\right\}$. Following this, the vehicle updates its reputation score and identity.

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, $[t_i]_{PK_{RC}} = \{T_i, T'_{ii}\} = \{PK_{RC}{}^r * (1+n)^t, g_1^r\}$ $(\text{mod} n^2)$. Using the system's master private key, $\lambda(n)$, the reputation center initially computes $T_i^{\lambda(n)} \bmod n^2 = g_1{}^{b*r*\lambda(n)}(1+n)^{t*\lambda(n)} \bmod n^2 = (1 + tn\lambda(n))$. By defining $L(x) = \frac{x-1}{n}$, and then further determine the reputation score as $t = L\left(T_i^{\lambda(n)} \bmod n^2\right) \cdot \lambda(n)^{-1} \bmod n$.

6.3 **Tracing of Location**: In multi-task crowdsensing contexts, to deduce the geographical specifics of sensing vehicles, one might reference $[x]PKDR$. Utilizing the master private key, symbolized as $\lambda(n)$, the reputation center computes $x = L\left(T_i^{\lambda(n)} \bmod n^2\right) * \lambda(n)^{-1} \bmod n$. 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 malicious vehicle $\mathcal{A}$ can intercept the information $I_v = \left\{PID, [t_i]_{PK_{RC}}, \sigma_i, ([x]_{PK_{DR}}, [y]_{PK_{DR}})\right\}$ from those other vehicle, deducing precise location coordinates remains unfeasible. BCP encryption, known for its semantic security under the Decisional Diffie-Hellman 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*: In our design, adversaries might aim to uncover the reporting vehicle's true identity, denoted as RID. While RID is concealed inside PID_i, encryption complexities combined with the absence of the requisite secret key ensure that adversaries cannot access it. 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.

- The reputation center controls the pseudonym of every reporting vehicle, ensuring malicious vehicles are prevented from imitating multiple identities and providing pro-

tection 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

In ourproposed system, computational overhead emerges primarily from exponentiations, multiplications, and select algorithmic executions. Within the initialization phase, the system primarily necessitates the execution of the Miller-Rabin algorithm for secure prime selection, which contributes to the complexity of $O(k^2 \log n)$ where k is the number of iterations and n is the number to be tested. Additionally, exponentiations in spaces G_1 and G_2 are required, contributing to the complexity of $O(\log n)$ each. Multiplications in both spaces add linear time complexity.

Transitioning to the task assignment phase, the system demands eighteen exponentiations and six multiplications in G_1, hence amplifying the computational load. The vehicle recruitment process involves fewer operations but remains significant with six exponentiations and two multiplications in G_1. Lastly, the information tracing operations, although varied, predominantly leverage exponentiations and multiplications in both G_1 and G_2.

In aggregate, the system's computational overhead predominantly scales with the number of exponentiations, as they are the most computationally intensive operations, followed closely by multiplications and specialized algorithms like Miller-Rabin.To elucidate these operations and their associated requirements in the context of our system, a comprehensive summary is provided in Table 2.

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 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

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

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

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

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	$9\mathcal{C}_{BCP} + 4\mathcal{K} + 3\mathcal{S} + \mathcal{P} + \mathcal{H}$

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 over-

head. 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 Roadside 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. Trustworker: 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] Zhiquan 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.