



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

by
Yichen Huang

Supervisor: Nitheesh Murugan Kaliyamurthy

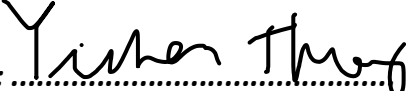
Project submitted as part of the requirements for the
award of MSc Software Engineering and Artificial
Intelligence

November 2023

DECLARATION

I, ...Yichen Huang..... declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

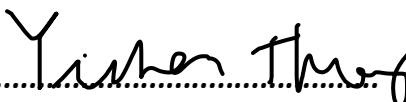
This work has not previously been accepted as part of any other degree submission.

Signed :.....

Date : 7/9/2023.....

FORM OF CONSENT

I Yichen Huang..... hereby consent that my Project, submitted in candidature for the M.Sc. Software Engineering and Artificial Intelligence degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Signed :.....

Date : 7/9/2023.....

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

Yichen Huang

September 7, 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, I recommend an approach focusing on conditional privacy within a versatile mobile crowdsensing architecture tailored for vehicular systems. This 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 the strategy complies with essential security benchmarks like precision, conditional privacy assurance, and user verification. Efficiency evaluations suggest the model's potent applicability in the diversified tasks of mobile crowdsensing.

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

Contents

1	Introduction	3
2	Literature Review	6
2.1	Multi-type Privacy Protection in Vehicular Networks	6
2.2	Multi-task Privacy Protection in Vehicular Networks	7
2.3	Conditional Privacy Preservation in Vehicular Networks	8
2.4	Lightweight and Efficient Privacy Preservation Schemes in Vehicular Networks	9
2.5	Section Conclusion	11
3	Research Methodology	13
3.1	Security Analysis	13
3.2	Efficiency Analysis	13
3.3	Cryptographic Tools and Algorithms	14
3.3.1	Homomorphic Encryption	14
3.3.2	Digital Signatures	14
3.3.3	The BCP Encryption	15
3.4	Section Conclusion	16
4	Design and Implementation	17
4.1	System Model	17
4.2	Security Model	18
4.3	Security Requirements	20
4.4	Multi-task Requirement	21
4.5	Briefing on the scheme	22
4.6	Details of the scheme design	23
4.7	Implementation	27
4.8	Section Conclusion	28
5	Result and Analysis	30
5.1	Security Analysis	30
5.2	Computation Overhead Analysis	32
5.3	Communication Overhead Analysis	34
5.4	Efficiency Analysis	36
5.5	Section Conclusion	38
6	Conclusion and Recommendation	39
7	Reflection	40

1 Introduction

The rapid advancement of mobile internet coupled with the widespread adoption of intelligent devices featuring built-in sensors has elevated the prominence of mobile crowdsensing (MCS)[10]. 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.[5][16] 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.[5] While vehicular networks' innate openness presents opportunities, it equally introduces a range of vulnerabilities. Specifically, sensors and control systems related to vehicles can be exposed to unsolicited interference or illicit modifications. Expanding on this, these networks, given their vast data streams and connected devices, might also be targets for eavesdropping, man-in-the-middle attacks, and malware infiltrations, emphasizing the urgent need for robust security solutions. 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.[20] [7] 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.[21] 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[29] and geolocation[27], overlooking reputation scores[26]. 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. 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. 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 address the multifaceted challenges presented in the realm of vehicular networks within the MCS framework, the field of cryptography has emerged as a promising solution, offering a blend of security, privacy, and efficiency. Cryptography, particularly modern asymmetric cryptographic algorithms, boasts the potential to shield data against unauthorized access while enabling data verification and validation.

Vehicular Ad-Hoc Networks (VANETs) have drawn attention for their ability to foster vehicle-to-vehicle and vehicle-to-infrastructure communications, ensuring real-time data dissemination and acquisition. These networks have also spotlighted the importance of designing cryptographic schemes that prioritize computational efficiency, given the time-sensitive nature of vehicular communications. The delay in data transmission or processing could hinder vehicular operations and safety.

Moreover, as vehicular networks become increasingly intertwined with the broader Internet of Things (IoT) ecosystem, there arises a need for holistic security solutions that cater to the diverse array of devices and communication protocols. The integration of vehicular sensors with other IoT devices, such as traffic lights, roadside cameras, and even pedestrian smartphones, necessitates cryptographic solutions that can seamlessly transition across these platforms.

Furthermore, the dynamic nature of vehicular networks, characterized by the constant movement of vehicles and ever-changing network topologies, presents unique challenges for key distribution and management. Conventional cryptographic solutions may struggle with the real-time demands of vehicular network environments. Therefore, adaptive cryptographic techniques that can evolve with the changing network conditions are of paramount importance.

Lastly, from a user perspective, the preservation of privacy goes beyond just the protection of identity, location, and reputation. With vehicles becoming increasingly "smart" and connected, they are likely to process a plethora of personal data ranging from user preferences in entertainment to their travel patterns and health metrics. The stakes for ensuring data confidentiality and privacy are higher than ever, necessitating cryptographic solutions that adopt a holistic view of user privacy.

To tackle the aforementioned hurdles, The paramount aim of this research is to devise a scheme that not only preserves the privacy of vehicle identity, location, and reputation but also ensures computational and communication efficiency, especially in multi-task scenarios. To navigate toward this encompassing aim, I have delineated the ensuing specific objectives:

- **Literature Review:** Undertake an exhaustive review of pertinent literature to grasp the nuances of existing cryptographic schemes and their deployment in vehicular networks. This review will further discern current challenges and limitations in pre-

serving privacy within multi-task vehicular environments and distill benchmarks and metrics pivotal for evaluating the potency and security of cryptographic endeavors in vehicular networks.

- **Systematic Research Methodology:** Devise a comprehensive research methodology specifically for vehicular network environments, integrating state-of-the-art cryptographic algorithms. This methodological approach will not only guide empirical and theoretical investigations but also ensure the judicious selection and application of cryptographic tools. Through these cryptographic measures, the scheme’s ability to guarantee privacy and security will be reinforced, ensuring the confidentiality, integrity, and authenticity of vehicular data.
- **Security Assurance:** Construct a comprehensive security model that lucidly encapsulates potential adversaries and the multifaceted threats looming over multi-task vehicular networks. This objective also encompasses the rigorous proof of the scheme’s security, ensuring its resilience against the identified adversaries and guaranteeing adherence to requisite security standards.
- **Efficiency Assessment:** Embark on a meticulous analysis of the scheme’s computational and communication overheads, drawing comparisons with extant solutions to underscore its efficiency. This will be complemented by real-world experiments or simulations, which will empirically affirm the theoretical efficiency assertions.
- **Scheme Design:** Elaborate on the intricate architecture of the envisioned cryptographic scheme, spotlighting its diverse components and the interplay amongst them. This objective will further elucidate the cryptographic protocols and tools integral to the scheme, culminating in a methodical procedural guide detailing the spectrum of operations from data encryption to validation within the scheme’s confines.

In the following sections, this report delves into various aspects of privacy protection in vehicular networks. In Section 2, a comprehensive literature review is presented, focusing on different privacy protection paradigms ranging from multi-type and multi-task to conditional and lightweight schemes. The culmination of this review is brought together in the section conclusion. Section 3 outlines the research methodology, detailing the analysis techniques employed and the cryptographic tools and algorithms utilized. This includes a thorough examination of homomorphic encryption, digital signatures, and the BCP encryption method. The design and implementation of the proposed privacy scheme are expounded upon in Section 4. This section provides insights into the system model, security requirements, and a detailed walkthrough of the scheme design, followed by its implementation. Results and comprehensive analyses covering security, computation, communication, and efficiency aspects are discussed in Section 5. Finally, Section 6 provides concluding remarks and recommendations, while Section 7 offers a reflection on the entire research process.

2 Literature Review

The field of vehicular network privacy has witnessed rapid strides, both in terms of challenges encountered and the sophistication of solutions. At the heart of this research progression lies the imperative to strike a balance between rigorous privacy measures and the efficient operation of vehicular networks, especially in intricate multi-task scenarios. The paramount aim of this research is to devise a scheme that not only preserves the privacy of vehicle identity, location, and reputation but also ensures computational and communication efficiency, particularly in multi-task settings. Achieving this delicate equilibrium necessitates a deep understanding of both the past and current state of the art, drawing insights from myriad methodologies and strategies previously proposed.

The literature review stands as a pivotal objective in this research endeavor. It serves as both a compass and foundation, guiding the inquiry by shedding light on the intricate maze of vehicular privacy studies. As I delve into the annals of scholarly works, it becomes evident that while many have treaded this path, only a few have managed to address the multifaceted nature of vehicular privacy challenges holistically. This literature excavation seeks to unearth those seminal works that have not only recognized the multifarious challenges of vehicular privacy but have also proposed innovative solutions, especially in the realms of cryptographic techniques, which play a quintessential role in ensuring the robustness of any privacy-preserving scheme.

In order to fully meet the aforementioned objective, a systematic and comprehensive analysis of existing research paradigms is paramount. The vast landscape of vehicular network privacy is marked by distinct thematic areas, each with its own set of intricacies and nuances. This research, therefore, adopts a structured approach, segmenting the literature review into key thematic pillars that underpin the core challenges and potential solutions in vehicular network privacy preservation.

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. [21] 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. [27] 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 com-

putational 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. [26] 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. [30] 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.

Moving forward, it's pivotal to consider the dynamic nature of vehicular networks. With vehicles constantly entering and exiting these networks, maintaining consistent privacy becomes a challenge. Moreover, with the integration of IoT devices, the volume of data generated and processed in these networks is expected to surge. As such, researchers need to anticipate and address the increased complexity these changes will introduce.

Furthermore, as vehicular networks become more interconnected and their applications diversify, the types of information requiring privacy protection will expand. Beyond just location and sensor data, future vehicular networks might involve more personal data, such as driver profiles, driving habits, and in-car entertainment preferences, further emphasizing the need for robust multi-type privacy protection.

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, along with the evolving nature of vehicular networks, 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, necessitating 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 [11], 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 [15][14][18] 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 [18], 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 [21], 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 preserving privacy, favoring audit and accountability procedures by relevant departments against malicious adversaries.

In paper [24], 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 [19] 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 [13] 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.

2.4 Lightweight and Efficient Privacy Preservation Schemes in Vehicular Networks

As vehicular networks grow in complexity and scale, there is an increasing need for lightweight and efficient privacy preservation schemes. Traditional cryptographic methods, while se-

cure, often come with high computational costs and latency, making them less suitable for the real-time requirements of vehicular networks. This subsection delves into the advancements and methodologies that focus on reducing computational overhead while ensuring robust privacy preservation.

- **Symmetric Cryptography:** Symmetric cryptography, typified by algorithms like AES and ChaCha20, is distinguished by its reliance on a singular key for both encryption and decryption processes [1]. This offers an inherent advantage in terms of efficiency, as managing and distributing a single key is more straightforward than handling a pair of keys, as is the case with asymmetric cryptography. Moreover, symmetric algorithms are known for their resilience against various cryptographic attacks when appropriately implemented. In vehicular networks, where rapid communication is imperative, the expediency of symmetric methods can significantly enhance real-time data exchanges, ensuring both speed and security.
- **Elliptic Curve Cryptography (ECC):** ECC has emerged as a potent alternative to traditional cryptographic methodologies, offering comparable security with considerably shorter key lengths. The reduced key size translates to brisker computations, lesser memory usage, and diminished transmission overhead. In the context of vehicular communication, where bandwidth and computational efficiency are paramount, ECC offers an optimized balance between security and performance. Its lightweight nature makes it particularly suited for vehicular scenarios where real-time communication without significant delay is a necessity.
- **Hash-based Schemes:** Cryptographic hash functions serve as the backbone of hash-based schemes, bestowing them with capabilities to ensure data integrity and provide authentication. The inherent property of hash functions to produce a fixed-size output from variable-size input can be harnessed effectively in vehicular communication. Structures like Merkle trees can be utilized to succinctly verify the contents of voluminous data blocks without the burden of intensive computations. This allows for efficient validation of data integrity in vehicular networks, ensuring that the received data hasn't been tampered with during transit.
- **Aggregation Techniques:** Data aggregation techniques offer a dual advantage: they enhance efficiency and bolster privacy. Instead of inundating the network with raw or individually encrypted data points, vehicles can synthesize data and transmit aggregated insights or summaries [3]. This aggregated data, besides reducing the transmission load, inherently obfuscates individual data points, making it challenging for adversaries to decipher specific vehicle data or patterns, thereby enhancing user privacy.
- **Hardware-based Solutions:** Modern vehicles are increasingly being equipped with sophisticated hardware modules designed for security, such as Trusted Platform Modules (TPMs) or hardware security modules [4]. These on-chip modules can execute

cryptographic operations swiftly, offloading the computational strain from the main system. Furthermore, by isolating cryptographic operations within these secure modules, the system ensures that even if an attacker gains access to the vehicle’s primary computational resources, the encrypted data and cryptographic keys remain impervious to compromise.

- **Privacy-preserving Data Reduction:** Transmitting voluminous data not only strains the network bandwidth but also raises privacy concerns. By employing data reduction techniques like pruning, sampling, and quantization, vehicles can distill the essence of data while discarding superfluous details [8]. This selective transmission inherently boosts privacy, as only a curated or modified version of the data is relayed, making it difficult for potential adversaries to reconstruct the full dataset or discern individual patterns.

In conclusion, the future of vehicular networks hinges on the amalgamation of speed, efficiency, and privacy. Lightweight and efficient privacy preservation schemes play a pivotal role in achieving this trifecta. By moving away from traditional, heavy cryptographic methods and embracing modern, agile techniques, vehicular networks can ensure robust privacy without compromising on performance.

2.5 Section Conclusion

The journey through the annals of vehicular network privacy literature reveals a landscape marked by rapid advancements, innovative methodologies, and evolving challenges. As vehicular networks grow in complexity and intertwine with broader technological ecosystems, the nuances of ensuring privacy while maintaining efficiency become increasingly intricate. Drawing from the comprehensive literature review, several insights emerge that bear profound implications for this research endeavor.

First and foremost, the literature underscores the multifaceted nature of vehicular privacy challenges. Whether it’s the nuances of multi-type privacy protection, the complexities introduced by multi-task scenarios, the delicate balance required for conditional privacy, or the pursuit of lightweight and efficient solutions, each facet presents its own set of challenges and opportunities. These thematic areas, as elucidated in the literature review, form the bedrock upon which this research is anchored.

The paramount aim of this research, as reiterated, is to craft a scheme that seamlessly marries robust privacy preservation with computational and communicative agility, especially in multi-task environments. The literature review, in this regard, serves a dual purpose. On one hand, it offers a repository of knowledge, shedding light on what has been achieved, the methodologies employed, the challenges encountered, and the gaps that remain. On the other hand, it provides a blueprint, charting a clear trajectory that this research can follow, drawing from the collective wisdom of past studies while also carving its niche.

The studies reviewed emphasize the indispensable role of cryptographic techniques in ensuring vehicular privacy. Whether it's the elegance of ECC, the efficiency of symmetric cryptography, the robustness of hash-based schemes, or the agility of hardware-based solutions, the world of cryptography offers a plethora of tools that can be harnessed to achieve the research aim. Moreover, the literature underscores the significance of adopting a holistic approach, one that not only focuses on privacy but also on the broader user experience, computational overhead, real-time requirements, and the dynamic nature of vehicular networks.

In essence, the literature review acts as a lighthouse, illuminating the complexities of the vehicular privacy domain while also highlighting the potential pathways that can be pursued. It accentuates the importance of drawing from diverse methodologies, being open to interdisciplinary solutions, and maintaining a relentless focus on the end goal: a vehicular network privacy scheme that is both robust and efficient.

In conclusion, as this research progresses towards its paramount aim, the literature review stands as a testament to the rich tapestry of scholarly endeavors that have come before. It offers both inspiration and guidance, underscoring the importance of standing on the shoulders of giants while also charting new frontiers. With the insights gleaned from the literature, this research is poised to make a meaningful contribution to the realm of vehicular network privacy, striving to realize a vision where vehicular networks are both private sanctuaries and epitomes of efficiency, especially in intricate multi-task scenarios.

3 Research Methodology

The overarching methodology of this research is meticulously designed to meet the primary objective: to develop a scheme that preserves the privacy of vehicle identity, location, and reputation while ensuring computational and communication efficiency, especially in multi-task scenarios. The methodology is bifurcated into three core segments, each dedicated to a crucial aspect of the research. The following sections delineate the details of each segment.

3.1 Security Analysis

Preliminary Definitions: Before delving into the design of the scheme, it's imperative to establish a robust foundation by articulating key system definitions. This encompasses the architecture of the vehicular network, roles of entities within the network, potential data flows, and operational parameters.

Security Requirements: A clear articulation of security requirements is paramount. This involves stipulating the degree of privacy to be achieved (e.g., anonymity, pseudonymity, unlinkability), potential adversarial models (e.g., passive eavesdroppers, active attackers), and the kind of attacks the system might be susceptible to (e.g., replay, impersonation, Sybil attacks).

Significance of Security Requirements: The rationale for each security requirement is elucidated, underscoring its relevance in ensuring the robustness of the scheme. Each requirement is justified based on real-world scenarios, potential threats, and the overarching need to bolster user trust in vehicular networks.

Post-design Security Analysis: Upon the completion of the scheme's design, a rigorous security analysis is conducted. This analysis evaluates the scheme against the predefined security requirements, ensuring that each stipulated criterion is met. Techniques such as formal security proofs, adversarial modeling, and threat analysis are employed to validate the scheme's resilience against potential attacks.

3.2 Efficiency Analysis

Computational Efficiency: Post the design of the scheme, each step is scrutinized for its computational efficiency. This involves assessing the time complexity of algorithms, the computational overhead introduced by cryptographic operations, and the overall responsiveness of the system, especially in multi-task scenarios.

Communication Efficiency: Parallely, the scheme's communication efficiency is gauged. This entails evaluating the size of messages exchanged, the frequency of communications, and the bandwidth requirements, ensuring the scheme doesn't inundate the network with excessive communication overhead.

Software-based Evaluation: To garner empirical insights into the scheme's efficiency, software-based evaluations are conducted. Tools like MATLAB or Python-based cryptographic libraries can be harnessed to simulate the scheme, measuring its runtime and memory footprints under various scenarios.

Comparison with Existing Schemes: The scheme’s efficiency is juxtaposed with that of established schemes in the literature. This comparative analysis offers insights into the relative advantages of the proposed methodology, showcasing its prowess and potential improvements over traditional methods.

3.3 Cryptographic Tools and Algorithms

In the quest to design a scheme that aligns with the research aim, a suite of cryptographic tools and algorithms is employed. These tools serve as the linchpins, ensuring the robustness, privacy, and efficiency of the scheme.

3.3.1 Homomorphic Encryption

The Paillier cryptosystem[22], possessing an additive homomorphic feature, emerges as a predominant encryption technique. Assuming I have N encrypted data items using a consistent public key pk , denoted as $[m_i]_{pk}$ ($i = 1, 2, \dots, N$). The additive homomorphism attributes of this encryption ensure the ensuing equation remains consistent:

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

where $D_{sk}()$ represents the decryption procedure associated with the private key sk . Liu[17] 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. Assuming that I have a pair of encrypted data, say $[x]_{pk}$ and $[y]_{pk}$, the Secure Less Than Protocol allows one to ascertain an encrypted bit depending on the evaluation of the relation between x and y , specifically if x is either greater than or equal to y or if x is less than 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 a pair of encrypted values $[x]_{pk}$ and $[y]_{pk}$, the Secure Equivalent Testing Protocol able to establish an encrypted data 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.

3.3.2 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 $h = H([t_i]_{PK_{RC}})$.
- The hash value h is then transformed using the private signing key x_i to produce the signature, represented as $\sigma_i = h^{x_i}$.

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.

3.3.3 The BCP Encryption

The BCP encryption technique[2] can be broken down and expanded upon as follows:

Key Generation (KeyGen): [28]The initial phase involves the choice of two significant primes, namely p and q . The value of n is determined by multiplying these primes. Elements g and h are set, with both having maximal order in the cyclic group G . This group is based on quadratic residues relative to n^2 . It's worth noting that if h is computed as $g^x \bmod n^2$, with x belonging to the range $[1, \lambda(n^2)]$, and given that $\lambda()$ symbolizes the Euler function, then x is mutually prime with respect to $\text{ord}(G)$. Thus, ensuring h retains the utmost order. The disclosed parameters are n , g , and $h = g^x \bmod n^2$, while the hidden variable is the range of x within $[1, \text{ord}(G)]$.

Encryption (Enc): For any message m within Z_n , an element r from Z_n^* is selected randomly. Consequently, I can compute $\{h^r(1 + mn), g^r\} \bmod n^2$ to get the ciphertext $[m]$. The components of this result are showcased as (T, T') .

Weak Key-based Decryption (WDec): Leveraging the secret key x , one can retrieve the original message m using: $m = L(T / (T')^x \bmod n^2)$. The function $L(u)$ essentially translates to $(u - 1)/n$.

Strong Key-based Decryption (SDec): This decryption uses a more formidable private key denoted by $SK = \lambda(n)$. The mechanism unfolds as:

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

From the above, the original message m is derived by:

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

In essence, the BCP encryption technique encapsulates multiple phases, each crucial in ensuring secure encryption and decryption processes in different contexts. The emphasis on both weak and strong key-based decryption underscores its flexibility and robustness.

3.4 Section Conclusion

The methodology presented in this research outlines a robust and comprehensive approach tailored to address the complex challenges of vehicular network privacy. Grounded in a tripartite framework, the methodology underscores three pivotal domains: security, efficiency, and the judicious application of cryptographic tools.

The security analysis emphasizes the significance of laying a solid foundation. By defining the system parameters, identifying potential threats, and outlining clear security requirements, the research ensures that the scheme is built upon a bedrock of robust security principles. The post-design analysis further cements this approach, validating the scheme against a spectrum of adversarial models and potential attacks.

The efficiency analysis accentuates the necessity of a scheme that is both computational and communication-efficient. Recognizing the real-time requirements of vehicular networks, the research employs software-based evaluations and comparative analyses to guarantee that the scheme not only stands robust in theory but also excels in practical implementation.

Lastly, the cryptographic segment of the methodology delves deep into the underpinnings of the scheme. By harnessing advanced cryptographic tools and algorithms, such as Homomorphic Encryption, Digital Signatures, and the BCP Encryption technique, the research ensures that the scheme is not only secure but also operationally efficient.

In culmination, the meticulously crafted methodology resoundingly echoes the paramount aim of this research: to conceive a scheme that adeptly preserves the privacy of vehicle identity, location, and reputation, while also ensuring computational and communication efficiency, especially in multi-task scenarios. This methodology guiding the research towards achieving this attainable objective, and further contributes to the evolving tapestry of vehicular network privacy.

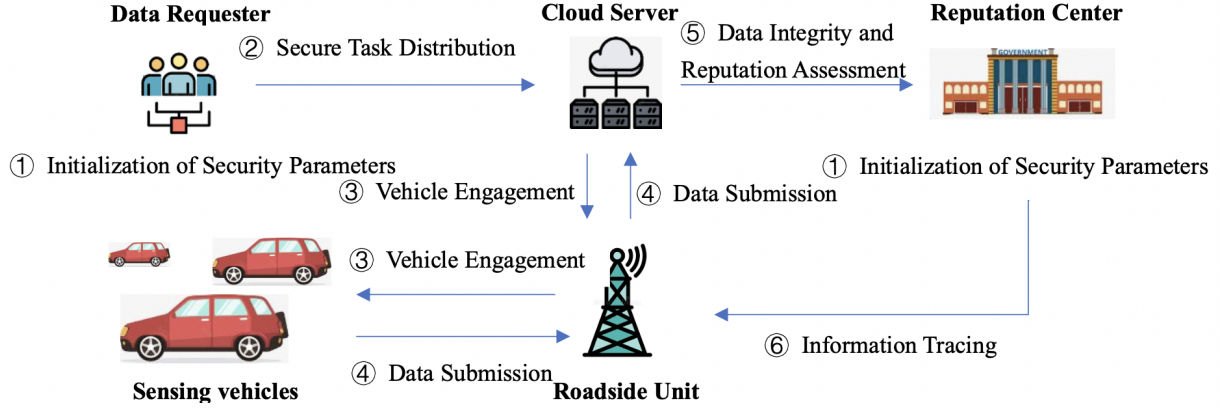


Figure 1: The system model of the multi-task sensing scheme.

4 Design and Implementation

Achieving the paramount aim of this research—to develop a scheme that skillfully preserves the privacy of vehicle identity, location, and reputation, while simultaneously ensuring computational and communication efficiency, particularly in multi-task scenarios—requires a meticulous design approach underpinned by a pragmatic implementation strategy. The design and implementation phase is critical, serving as the bridge between theoretical methodologies and their real-world application, ensuring that the theoretical constructs are translatable to practical vehicular network scenarios.

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. The data requester, while initiating tasks, also has the responsibility to ensure that the delegated tasks align with privacy policies and adhere to real-time requirements. To ensure the authenticity of the data requester, they utilize cryptographic techniques, such as digital signatures, to verify their identity and task legitimacy. The tasks are often categorized based on priority, with urgent tasks like accident alerts or roadblock information requiring immediate attention from the sensing vehicles.

Cloud Server The cloud server primarily serves as a hub for the acquisition, storage, and processing of encrypted sensory data. Furthermore, by scrutinizing the precision of sensing data from vehicles, it gauges their trustworthiness, leading to the generation of reputation feedback reports. In essence, these servers are equipped with significant computational prowess and vast storage capacities. Beyond its role as a data hub, the cloud

server integrates advanced cryptographic tools to ensure data privacy during processing. Homomorphic encryption techniques allow the cloud server to compute on encrypted data without needing to decrypt it, thus ensuring privacy. The cloud server also employs machine learning algorithms to detect anomalies in the received data, filtering out potentially malicious or incorrect data inputs.

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. Trust management is crucial in vehicular networks to prevent malicious vehicles from disseminating false information. The reputation center, with its dynamic scoring system, ensures that only trustworthy vehicles participate in sensing tasks. The use of blockchain technology[25] by some reputation centers provides an immutable record of vehicle behaviors, further enhancing trustworthiness assessments.

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 among sensing vehicles and reputation centers, and also among sensing vehicles and cloud servers. RSUs not only facilitate data transmission but also play a pivotal role in ensuring secure communication in the network. They employ protocols like Vehicle Ad-hoc Networks (VANETs)[23] to securely relay messages across the network. Furthermore, RSUs can cache frequently requested data to reduce latency and improve response times for sensing vehicles and data requesters.

Sensing Vehicle: Often outfitted with an array of sensors, these vehicles primarily focus on capturing diverse environmental metrics and storing this vital information. In addition to this, every vehicle sensor system includes an on-board unit (OBU)[9][12], which securely stores sensitive details, encompassing secret keys, user identities, geographical positions, and more. Sensing vehicles are becoming increasingly sophisticated, with sensors capable of capturing high-resolution images, LiDAR data, and even air quality metrics. However, with the increased granularity of data comes the heightened risk of privacy breaches.

In essence, the vehicular network’s system model represents a synergy of various entities, each playing a crucial role in ensuring efficient data collection while upholding the paramount importance of privacy and security. The intricate interplay between these entities necessitates continuous advancements in cryptographic and vehicular technologies to address the ever-evolving challenges posed by malicious actors and the growing need for real-time data in smart cities.

4.2 Security Model

In this architecture, I 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. A *reputation linkable attack* will occur in this situation.

The reputation center remains wholly trustworthy in this setup. The foundational premise posits that most sensing vehicles operate with integrity. However, a small faction of these vehicles may act maliciously, launching the following types of attacks:

- *Data pollution attack*: The vehicles might deliberately feed inaccurate information, thereby adulterating the collective final outcomes. This is particularly concerning in vehicular networks where accurate data is essential for safe and efficient road operations. For instance, a malicious vehicle could report non-existent traffic jams or road hazards, leading other vehicles to make incorrect navigational decisions. The objective here is often to disrupt the normal flow of operations or to achieve some personal gains, such as rerouting traffic to a less busy route.
- *Sybil attack*: These adversaries 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. In a Sybil attack, one adversary controls multiple nodes in the network, making it appear as if multiple vehicles are providing consistent data. This can severely undermine trust-based systems, as the malicious data may be seen as more reliable due to the perceived consensus among multiple reporting entities.
- *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. By artificially inflating their reputation scores, these vehicles can gain unauthorized access to certain tasks or even manipulate the outcomes of collaborative sensing. This not only undermines the integrity of the reputation system but can also lead to faulty decision-making based on the compromised data they provide.
- *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. Unlike the Sybil attack, where a single adversary pretends to be many, in a collusion attack, multiple adversaries work in unison. Their coordinated effort can make it harder to detect and mitigate the false information they introduce, especially if they strategically spread out their false data submissions to avoid suspicion.

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. While the majority's integrity provides a buffer against malicious intent, it's crucial to recognize that

even a small fraction of malicious nodes can inflict significant harm on the system, especially if they exploit vulnerabilities efficiently. Relying solely on the honesty of the majority can lead to complacency, which is a potential risk in itself. The dynamic nature of vehicular networks, combined with the evolving tactics of adversaries, demands constant vigilance. Implementing proactive security measures, regular system audits, and fostering a culture of security awareness can further bolster the system’s resilience, ensuring not just the integrity of the data but also the safety and efficiency of vehicular operations. It’s a blend of trust in the majority and the readiness to combat the tactics of the minority that will ensure the long-term security of vehicular networks.

4.3 Security Requirements

This scheme takes into account the following security prerequisites:

- *Correctness.* Provided all the participants honestly adhere to the protocol, it will yield accurate outcomes. This implies that the system’s operations and results are consistent with its intentions, and there’s no deviation from the expected behaviors. This correctness is paramount as it builds the foundation of trust and ensures reliability in vehicular communications.
- *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. The conditional aspect of this privacy ensures a balance between security and accountability. In a real-time environment, the trusted authority has the capability to derive the actual reputation value, location, and identity from the messages transmitted, but only under predefined circumstances.
- *Authentication.* It should be impossible for adversaries to tamper with or forge exchanged messages without detection. This ensures that all communication within the network comes from legitimate sources. Authentication acts as a first line of defense against various threats, ensuring that unauthorized entities cannot introduce malicious data or impersonate legitimate nodes within the network.
- *Resistance to other attacks.* The scheme I 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. This multi-faceted resistance is crucial for maintaining the integrity of the vehicular network. By addressing a broad spectrum of potential threats, the system ensures both the confidentiality

of the data and the safety of its operations, even in the face of evolving adversarial tactics.

In conclusion, the security prerequisites outlined in this scheme emphasize a holistic approach to vehicular network security. By ensuring correctness, preserving privacy conditionally, guaranteeing authentication, and building resistance to a multitude of attacks, the system strives to establish a robust, trustworthy, and adaptive environment for vehicular communications.

4.4 Multi-task Requirement

As vehicular networks increasingly become interconnected, the push for a more sophisticated system that caters to multitasking requirements is inevitable. With a multi-task environment, vehicles must handle multiple concurrent tasks without compromising security. This places a heightened emphasis on ensuring a robust security mechanism that is both dynamic and adaptive.

Given the increased complexity of multi-task scenarios, the system needs to address several new security requirements:

Task-based Identity Management: With vehicles undertaking multiple tasks, it becomes crucial to provide task-specific pseudonyms. This ensures that even if an adversary successfully infiltrates one task, the breach doesn't expose the vehicle's involvement in other tasks.

Dynamic Reputation Adjustment: As vehicles are evaluated based on their performance in multiple tasks, a dynamic reputation system that can factor in weights for different tasks becomes vital. A failure in a minor task should not tarnish the reputation as severely as a failure in a critical task.

Concurrency Control: A robust mechanism to handle concurrent operations without causing data integrity issues is crucial. This mechanism should also ensure that while handling multiple tasks, the vehicle's system isn't overwhelmed, which could expose vulnerabilities.

Task Isolation: Each task should be treated in isolation from a security standpoint. Breaching the security parameters of one task shouldn't give an adversary an advantage in another task.

Enhanced Authentication Protocols: Given the multi-tasking environment, there's an increased chance of a Sybil attack where an adversary could impersonate multiple entities. Enhanced authentication protocols that are task-specific can help curb such threats.

The architecture of the vehicular network was elaborated upon, highlighting both the system's integral components and their interdependent functionalities. The model primarily consists of five entities, each with distinct responsibilities ranging from data procurement to ensuring seamless and secure communication. Given the vulnerabilities inherent to such open systems, this research introduced the adversaries, detailing their possible motives and methods of infiltration. The framework anticipates not only these potential threats but also

Table 1: Formalized Notations in the Scheme

Notation	Definition
t_i	Reputation of the i th sensing vehicle.
t_0	Minimum reputation required for a sensing task.
m	Substance or a sensing task's content.
$[m]$	Encrypted form of datae 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	The sensing vehicle's unique identity.
PID	Pseudonym used by the sensing vehicle for anonymity.
T	Tasks in which a sensing vehicle participates.

a myriad of possible real-world attacks. To address these threats, the system incorporates a comprehensive set of security prerequisites. These measures are designed to ensure the accuracy, privacy, authenticity, and overall robustness of the system. As vehicular networks expand in scope and intricacy, the approach aims to strike a balance between flexibility and security, setting the foundation for subsequent multi-task requirements in the ever-evolving environment.

4.5 Briefing on the scheme

In this segment, I initially provide a synopsis of the scheme before delving into its technical specifics. Comprising six stages, the scheme includes Initialization of Security Parameters, Secure Task Distribution, Vehicle Engagement, Encrypted Data Transmission, Data Integrity and Reputation Assessment, and finally, secure Information Retrieval. The symbols utilized in this scheme are subsequently encapsulated in the following table:

For clarity in the exposition, an initial overview of the 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.** During security initialization, pivotal primes are derived from the security parameter, laying the foundation for the cyclic group. The reputation center and data requester develop key pairs from these parameters. To ensure vehicular anonymity, the reputation center allots pseudonyms via ElGamal encryption and couples them with encrypted reputation values crafted using BCP. With shared system parameters, vehicles receive tailored data through RSU, strengthening vehicular communication integrity.
- **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.** Through RSUs, sending vehicles engaged in sensing tasks transmit their encrypted data to the primary cloud server, ensuring the data's authenticity and privacy.
- **Data Integrity and Reputation Assessment.** The central server decrypts and assesses the data quality from each sensing vehicle. The reputation center receives a securely sent reputation feedback report. Subsequently, adjustments are made to the vehicle's score and pseudonym based on the report's findings.
- **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.

4.6 Details of the scheme design

Step 1: Initialization of Security Parameters

- 1.1 **System Initialization and Key Pair Generation:** Given the security measure κ , I select reliable primes p and q . These primes ensure $p' = (p-1)/2$ and $q' = (q-1)/2$ are prime values. I then define n as $n = pq$. Quadratic residues modulo n^2 make up the elements of the cyclic group $\mathbb{G}_1$, where the element g_1 has the maximal order. From the range $[1, \text{ord}(\mathbb{G}_1)]$, secret values a and b are extracted by the reputation center and data requester, respectively. Subsequently, the data requester's key pair is constructed as $(PK_{DR} = g_1^a, SK_{DR} = a)$, and the reputation center's key pair is given by $(PK_{RC} = g_1^b, SK_{RC} = b)$, ensuring a foundation of strong cryptographic security for system interactions.

1.2 Pseudonym Allocation for Vehicles: During the registration phase at the reputation center, sensing vehicles' true identities are represented as RID_i , ranging from 1 to m . A cyclic group $\mathbb{G}_2$ of order q is assigned, having g_2 as its primary generator. For every vehicle identified by RID_i , a number w_i is randomly selected from $\mathbb{Z}_q$, complemented by a secret value x from $\mathbb{Z}_q$. By leveraging El-Gamal encryption, the pseudonym $PID_i = \{PID_1, PID_2\}$ is calculated: specifically, $PID_1 = g_2^{w_i}$ and $PID_2 = RID_i \times h_{pub}^{w_i}$, where $h_{pub} = g_2^x$. Following this, a random value r_i between $[1, n/4]$ is determined and used with the BCP encryption method to create the encrypted reputation value $[t_i]PKRC = \{T_i, T'_i\} = \{PK_{RC}^{r_i} \times (1+n)^t, g_1^{r_i}\} \pmod{n^2}$. A corresponding signature, $\sigma_i = h^{x_i}$, is also generated for $[t_i]PKRC$. In this process, the signing key is x_i from $\mathbb{Z}_q$, with $h = H([t_i]PKRC)$, where H denotes a cryptographic hash function. Concluding the process, system parameters $\{n, g_1, g_2, \mathbb{G}_1, \mathbb{G}_2, h_{pub}, H, y, PK_{DR}, PK_{RC}\}$ are disseminated, and $\{PID, [t_i]PKRC, \sigma_i\}$ is relayed to the vehicle tagged as RID_i through RSU.

Step 2. Secure Task Distribution

2.1 Assignment of Standard Value: Information m is disseminated by the data requester as the sensing task, and the BCP encryption protocol is then used to deduce the ciphertext $[m]$. By adopting proxy re-encryption and harnessing its distinct public key, it formulates 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 partitions whole region to n distinct task sections. Each single section denoted by i , the reputation center commences by generating its key pair, represented as (PK_{Ti}, SK_{Ti}) . Next, the central point coordinates (x_0, y_0) , the threshold t_0 of the reputation value, and the radius r are encrypted using the BCP encryption scheme and private key that corresponds to the specified task, thereby acquiring the ciphertext $[x_0]_{PK_{Ti}}, [y_0]_{PK_{Ti}}, [r]_{PK_{Ti}}, [t_0]_{PK_{Ti}}$. After its initialization, the task TSK_i is appended to the task index TSK by the system. 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 remote server. The cloud server disseminates $I_c = \{PK_{DR}\}$ throughout the crowdsensing area after receiving 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:

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

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

- 3.2 **Vehicle Selection:** Once the remote server retrieves I_v , it begins a verification process for the signature σ_i and the the pseudonym PID 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 . Leveraging the SLT (Secure Less Than Protocol) cited by [17] and the additive homomorphic property, for a task in the task set TSK represented as $TSK_i = \{[x_0]_{PK_{Ti}}, [y_0]_{PK_{Ti}}, [r]_{PK_{Ti}}, [t_0]_{PK_{Ti}}\}$, the server determines whether $[t_i]_{PK_{RC}}$ and $[t_0]_{PK_{Ti}}$ satisfy the prescribed criteria.

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

If both the vehicle's location and reputation values are validated as appropriate, the server appends the task TSK , updating the task list T of the vehicle.

- 3.3 **Task Redistribution:** The task data $[m]$ is transformed into its final encrypted version $[m]'$ by the cloud server using the proxy re-encryption technique after thoroughly analyzing 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 . The ciphertext is created using the BCP encryption method for this data, $[d]_{PK_{Ti}}$. In the end, the vehicle sends $I_v = \{PID, [d]_{PK_{Ti}}, T\}$ to remote server.

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 with $[t'_i]_{PK_{RC}}$. The the vehicle's pseudonym undergoes an update to $PID' = \{PID'_1, PID'_2\}$. Here, PID'_1 is defined as $g^{wi'}$, while PID'_2 corresponds to $RID_i \times h_{pub}^{wi'}$. Subsequently, for the vehicle labeled as RID_i , $\{PID', [t'_i]_{PK_{RC}}, \sigma'_i\}$ is sent out by the reputation center. Following this, all sensing vehicles updates their 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. [28]For instance, $[t_i]_{PK_{RC}} = \{T_i, T'_{ii}\} = \{PK_{RC}^r * (1+n)^t, g_1^r\} \pmod{n^2}$. 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 $L(x) = \frac{x-1}{n}$, and then 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: In multi-task crowdsensing contexts, to deduce the geographical specifics of sensing vehicles, one might reference $[x]PKDR$. Utilizing the master private key, $\{PID', [t'_i]_{PK_{RC}}, \sigma'_i\}$ is sent out by the reputation center. In a similar vein, the center can determine values for y and r to retrieve the sensing vehicle's precise location.

4.7 Implementation

Implementing the design, particularly in a complex vehicular environment, is not a straightforward endeavor. Beyond the theoretical constructs, the real-world application presents its unique challenges. While the design offers a comprehensive blueprint, the intricacies of its actual implementation demand equal attention to ensure the overarching aim is met: preserving vehicle identity, location, and reputation privacy while ensuring computational and communication efficiency, especially in multi-task scenarios.

Practical Considerations: The idealized environment where all entities, like sensing vehicles or RSUs, function flawlessly seldom mirrors the unpredictable nature of real-world scenarios. Sensing vehicles could malfunction, RSUs might experience downtimes, or cloud servers might face overloads. Ensuring redundancy, implementing fail-safe mechanisms, and continuous monitoring are vital.

Scalability Issues: As vehicular networks grow, the number of sensing vehicles and data requesters will increase. The system must be able to handle a surge in data flow without compromising efficiency or security. This requires a modular approach to implementation, ensuring that adding new entities or processing additional tasks doesn't strain the system.

Hardware Constraints: Sensing vehicles, equipped with an array of sensors and an on-board unit (OBU), will have computational limitations. Implementing cryptographic operations, which are computationally intensive, must be balanced against the vehicle's other essential functions.

Network Latency: In a multi-task scenario, where vehicles handle multiple concurrent tasks, network latency could hinder real-time data exchange. Efficient data routing, optimized cryptographic operations, and dedicated communication channels for high-priority tasks can mitigate this.

Interoperability: With a diverse range of vehicles, from various manufacturers, all equipped with different sensors and OBUs, ensuring interoperability is paramount. Implementing standardized protocols and regularly updating them can ensure seamless communication between diverse entities.

Adversarial Adaptability: As the system evolves, so will the tactics employed by adversaries. Continuous threat analysis, routine security audits, and adaptive security protocols will ensure the system remains resilient against evolving threats.

Privacy-Preserving Mechanisms: While cryptographic tools offer a robust line of defense against privacy breaches, they alone might not suffice. Incorporating differential privacy techniques, where noise is added to the data before it's shared, can offer an additional layer of privacy, ensuring that individual vehicle data remains indistinguishable.

User Trust and Acceptance: Beyond technical considerations, user trust is pivotal. Educating users about the system’s privacy-preserving measures, its benefits, and addressing potential concerns proactively can foster trust, ensuring more widespread acceptance and use.

Regulatory Compliance: Different regions might have varied regulations concerning vehicular data collection, storage, and dissemination. Ensuring the system remains compliant with these regulations, while still preserving its core functionalities, is crucial.

Continuous Monitoring and Feedback Loops: Implementing a feedback mechanism, where potential issues or vulnerabilities reported by users or identified by the system itself are addressed promptly, can further bolster the system’s security and efficiency.

In conclusion, while the design of the scheme provides a comprehensive blueprint for achieving the research aim, its implementation in real-world scenarios presents its unique challenges. Addressing these challenges proactively, adapting to the evolving vehicular environment, and ensuring continuous improvements will be pivotal in ensuring the scheme not only preserves vehicular privacy but also remains computationally and communicatively efficient, particularly in multi-task scenarios.

4.8 Section Conclusion

Throughout the *Design and Implementation* section, I delved into the multifaceted intricacies of developing a scheme geared towards preserving the privacy of vehicle identity, location, and reputation while ensuring computational and communication efficiency, especially in complex multi-task scenarios. The research’s primary aim served as the guiding beacon, shaping the contours of the discourse and determining the trajectory of the solutions.

The exploration began with a comprehensive overview of the system model, shedding light on the dynamic interplay between various entities, from sensing vehicles and data requesters to cloud servers and roadside units. Each entity’s role was meticulously delineated, underscoring their collective synergy in achieving the overarching aim.

The security model provided insights into potential threats and vulnerabilities inherent in such open systems. By understanding the potential motives and tactics of adversaries, the framework anticipates a myriad of real-world attacks and is equipped to counteract them. This proactive approach ensures the robustness and resilience of the vehicular networks, with a particular emphasis on privacy and efficiency.

Subsequent discussions on security requirements and the multi-task environment highlighted the scheme’s holistic approach. By ensuring correctness, preserving privacy conditionally, guaranteeing authentication, and building resistance to a multitude of attacks, the system aims to establish a balance between flexibility and security in an ever-evolving vehicular environment.

However, when transitioned into discussing the practicalities of implementation, it became evident that real-world application entails its unique challenges. From addressing scalability issues and hardware constraints to ensuring user trust and regulatory compliance, the path to implementation is strewn with potential pitfalls. Yet, by adopting a

proactive stance, continuously adapting to evolving challenges, and prioritizing the research aim, I can navigate these complexities with finesse.

In essence, the *Design and Implementation* section offers a comprehensive blueprint for achieving my research aim. While the theoretical constructs provide a solid foundation, the real-world application requires adaptability, continuous improvement, and an unwavering commitment to preserving vehicular privacy and ensuring efficiency, especially in multi-task scenarios.

5 Result and Analysis

In the journey to achieve the primary aim of preserving vehicular privacy and ensuring computational and communication efficiency, especially in complex multi-task scenarios, let's transition into the crucial segment of this research: the *Result and Analysis* section. Here, I will delve deep into the practical outcomes and implications of the scheme, dissecting its various facets to understand its robustness, adaptability, and efficiency. Through meticulous analysis, I will examine how well the scheme stands against potential threats, the computational and communicational overhead it introduces, and its overall efficiency in real-world vehicular networks. As I navigate through these evaluations, I'll continually align the findings with the research aim, understanding the successes and potential areas of refinement in this proposal.

5.1 Security Analysis

This section discusses the robustness of the 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. The scheme's correctness attribute is inherently bound to its encryption and decryption mechanics. For a scheme to be correct, the decryption of the encrypted data should yield the original data. Leveraging established cryptographic primitives and protocols, the scheme ensures that, under normal operations, the integrity of the data is maintained. This correctness is vital as it guarantees that the sensed data, once processed, remains a true representation of the original.

Conditional Privacy Maintenance: For this attribute, I 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 ensures that while the malicious vehicle may intercept the information $I_v = \{PID, [t_i]_{PK_{RC}}, \sigma_i, ([x]_{PK_{DR}}, [y]_{PK_{DR}})\}$ 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.

Preserving the confidentiality of a vehicle's location is paramount, especially in urban environments where location data can reveal sensitive information, such as daily routines or frequented places. By ensuring that malicious entities cannot deduce

a vehicle’s exact coordinates even if they intercept transmitted data, the scheme provides robust protection against location-based threats.

- *Identity Confidentiality*: In the 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 $\mathbb{Z}_{n^2}$, the approach ensures identity protection.

The vehicle’s identity is a critical piece of information. Exposure of this identity can lead to various threats, ranging from targeted attacks on the vehicle to misuse of the vehicle’s sensed data. By intertwining the actual identity with pseudonyms and ensuring that only the trusted reputation center can map them back, the scheme offers a robust layer of protection against identity threats.

- *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, the system effectively maintains reputation score confidentiality.

Reputation scores are vital for assessing the reliability and authenticity of a vehicle’s sensed data. Protecting these scores ensures that malicious entities cannot manipulate or misuse them. By ensuring that adversaries cannot view or alter these scores, the scheme upholds the integrity of the multi-task crowdsensing process.

- *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.

While maintaining privacy is crucial, so is the ability to trace back any misinformation or malicious activity to its source. This traceability ensures accountability in the system. By allowing only the trusted reputation center to map pseudonyms back to real identities, the scheme strikes a balance between privacy and accountability.

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. Authentication is the backbone of any secure communication system. By ensuring that only authenticated messages are accepted and processed, the scheme protects against a plethora of threats, such as man-in-the-middle attacks or replay attacks. The incorporation of digital signatures adds an extra layer of validation, ensuring that data not only comes from a legitimate source but also remains unaltered during transmission.

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, the 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.

Inference attacks can be detrimental, as they allow adversaries to deduce sensitive information from seemingly harmless data. By incorporating robust cryptographic techniques, the scheme ensures that adversaries cannot derive any meaningful insights from intercepted data, thereby effectively neutralizing the threat posed by inference attacks.

- In real-world multi-task crowdsensing scenarios, ill-intentioned vehicles might relay incorrect sensing data. The system, by comparing data validity metrics, can discern and reject such misleading data, ensuring data integrity.

Data integrity is crucial to ensure that the crowdsensing process yields meaningful and accurate results. By incorporating mechanisms to validate the authenticity of sensed data, the scheme ensures that malicious or incorrect data is promptly identified and rejected. This validation not only enhances the system’s reliability but also deters malicious vehicles from attempting to pollute the data pool.

- The reputation center controls the pseudonym of every reporting vehicle, ensuring malicious vehicles are prevented from imitating multiple identities and providing protection against Sybil attacks. Furthermore, the system’s cryptographic checks ensure that only vehicles meeting reputation thresholds are verified, offering protection against reputation manipulation attacks.

Sybil attacks, where a malicious entity assumes multiple identities to influence a system, can severely compromise the reliability of sensed data. By ensuring that each vehicle has a unique, centrally controlled pseudonym, the scheme effectively mitigates the threat posed by Sybil attacks. Additionally, by maintaining the integrity of reputation scores and ensuring only vehicles with legitimate scores can participate, the scheme safeguards against reputation manipulation threats.

5.2 Computation Overhead Analysis

In this 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 the 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 3: Computation Overhead Comparison of Sensing Vehicle in this scheme, PACE, and SPOON Schemes[6]

Scheme	Computation Overhead	Runtime (ms)
SPOON [21]	$34T_{pm} + 21T_{pa} + 4T_{bm} + 23T_{exp}$	360.421
PACE [30]	$12T_{gc}$	243.562
this scheme	$6T_{exp} + 2T_{mul}$	43.035

TABLE 2 shows the calculate requirements of each phase in this scheme. Subsequently, I juxtapose the computational load of individual sensing vehicles against other distinguished MCS methodologies [21], [30]. 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 [21]. As evident from TABLE 3, the computational burden per sensing vehicle in this 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 this 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, the methodology exhibits a distinct advantage in reducing the computational overhead for sensing vehicles.

The architecture of vehicular networks and the essence of multi-task crowdsensing introduce unique challenges. Vehicles are perpetually on the move, necessitating a system that's not just secure, but also agile and efficient. As computations mount, delays can ensue, potentially compromising the system's real-time responsiveness. This scheme, with its distinct emphasis on minimizing computational overhead, rises to this challenge. This is manifested in the reduced number of exponentiations, multiplications, and the efficient use of cryptographic primitives like the BCP encryption.

TABLE 2 and TABLE 3 further solidify the efficiency of the system. When compared to other prominent schemes in the domain, the approach consistently showcases reduced computational burdens. This not only bodes well for individual vehicles, conserving their computational resources, but also for the entire network, ensuring swift and seamless data flow and processing.

While the present scheme is promising, the future of vehicular networks and multi-task crowdsensing will bring forth new challenges, especially as technologies like 5G and Edge Computing become more prevalent. There's potential for further optimization, perhaps by integrating machine learning algorithms for predictive task assignments or leveraging quantum-resistant cryptographic algorithms in anticipation of the quantum computing era. Furthermore, as vehicular networks expand, considerations for scalability will become even more crucial, nudging researchers to explore distributed and parallel processing techniques.

The interconnected world of the future, with vehicles communicating with everything from traffic lights to pedestrian devices, will demand even more from security and efficiency standpoints. The current scheme lays a robust foundation, but the journey of refining and evolving it to meet future challenges is an ongoing one. The horizon looks promising, with ample opportunities for innovation and enhancement in the realm of vehicular network security and efficiency.

5.3 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, I will analyze the communication overhead of the described scheme.

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 the scheme is not merely coincidental but is a strategic choice rooted in the inherent advantages of the BCP algorithm.

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

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 this scheme, by leveraging the BCP algorithm's strengths, I 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.

Furthermore, considering the dynamics of vehicular networks, where swift communication is crucial, the BCP algorithm plays a pivotal role in maintaining efficiency. Vehicles on the move cannot afford latency, and with a growing number of vehicles being added to such networks every day, the frequency of message exchanges will only increase. In such scenarios, cryptographic methods that can handle a large volume of data without compromising

on speed or security are indispensable.

Another aspect worth noting is the context of message size in vehicular communication systems. While Table 5 quantifies the communication overhead in terms of different cryptographic components, it’s essential to consider the actual size of these components. For instance, the size of $\mathcal{C}_{BCP}$ is inherently larger than traditional ciphertexts due to the security features it embeds. Therefore, the choice of BCP, while optimizing computational overhead, might increase the data size being transmitted. However, this trade-off is justified by the benefits it brings in terms of batch processing and reduced decryption times, especially when real-time communication is of the essence.

Looking ahead, as vehicular networks become more sophisticated with the integration of technologies like 5G, edge computing, and machine learning, the demands on communication overhead will evolve. The BCP algorithm’s adaptability and robustness make it a promising candidate for future iterations of my scheme. Additionally, researchers could delve deeper into optimizing the BCP algorithm itself, focusing on reducing the size of $\mathcal{C}_{BCP}$ or integrating it with other lightweight cryptographic primitives.

In conclusion, the communication overhead analysis underscores the importance of balancing security with efficiency in vehicular networks. My scheme, by strategically leveraging the BCP algorithm, showcases a pathway to achieve this balance. As vehicular communication systems continue to grow and evolve, so will the cryptographic methods that underpin them, ensuring safer and more efficient vehicular networks for the future.

5.4 Efficiency Analysis

Vehicular crowdsensing networks, characterized by the dynamic nature of vehicles and the sheer volume of data they contribute, stand out as one of the most challenging environments to ensure both security and efficiency. Let’s take a deeper dive into the importance of efficiency within this context.

1. Latency in Real-time Data Transmission:

- *Importance:* In vehicular networks, many applications, such as real-time traffic updates or emergency response systems, rely on immediate data transmission and processing. Any delay can render the data obsolete and might lead to suboptimal or even hazardous decisions.
- *My Approach:* By utilizing the BCP algorithm, I substantially reduce the computational overhead associated with decryption. When a central entity, like a traffic management system, receives data from multiple vehicles, it can leverage the BCP’s batch decryption to swiftly process this data, minimizing latency.

2. Throughput in High Data Inflow Scenarios:

- *Importance:* As more vehicles get equipped with sensors and join the crowdsensing network, the rate of data inflow will exponentially increase. The system must be equipped to handle this inflow without bottlenecks.

- *My Approach:* My scheme’s emphasis on efficient cryptographic operations, especially the batch processing capability of the BCP algorithm, ensures that large volumes of data can be simultaneously processed. This massively parallel processing enhances the system’s throughput, ensuring smooth data flow even during peak times.

3. Balancing Overhead:

- *Importance:* In vehicular communication scenarios, both computational and communication overheads play crucial roles. While computational efficiency ensures swift data processing, communication efficiency ensures that data packets are transmitted without excessive overhead.
- *My Approach:* My scheme, while leveraging the BCP algorithm to minimize computational overhead, does introduce slightly larger ciphertexts. However, this trade-off is strategic. By ensuring swift decryption, especially in batch scenarios, I believe that the benefits in reduced latency and enhanced throughput outweigh the added communication overhead.

4. Scalability in Expanding Networks:

- *Importance:* As urban areas grow and vehicular networks expand, any crowdsensing scheme must be scalable. An approach that works efficiently for a few hundred vehicles might not necessarily scale well for tens of thousands.
- *My Approach:* My scheme’s modular design, combined with efficient cryptographic primitives, ensures scalability. Operations, especially task assignments and vehicle recruitments, are optimized to handle an increasing number of vehicles without compromising on efficiency.

5. Ensuring Reliability and Data Integrity:

- *Importance:* For vehicular crowdsensing data to be useful, it must be reliable. Data integrity ensures that the sensed data, once transmitted and processed, remains a true representation of the original, unaffected by malicious alterations.
- *My Approach:* My scheme incorporates robust authentication mechanisms. By ensuring that only authenticated messages are accepted and processed, I protect against threats like man-in-the-middle attacks. Additionally, my focus on data validation ensures that data remains unaltered during transmission, ensuring its integrity.

In essence, vehicular crowdsensing networks, with their unique challenges, require a balanced approach that emphasizes both security and efficiency. My scheme is a testament to this balance, offering a secure yet efficient framework for the future of vehicular communication.

5.5 Section Conclusion

The analysis section elucidates the robustness and efficiency of the vehicular crowdsensing network scheme. It meticulously examines the security attributes, including correctness, conditional privacy maintenance, and authentication. The scheme’s commitment to preserving sensitive vehicular information, such as location, identity, and reputation score, against potential adversaries is evident. Furthermore, its intrinsic ability to offer a balanced approach between privacy preservation and accountability, via traceability, fortifies the system against potential threats.

In terms of computational overhead, my scheme significantly reduces the burden, especially when juxtaposed with other prevailing schemes. The strategic incorporation of the BCP algorithm, known for its batch decryption capability, streamlines data processing, minimizing latency—a pivotal feature for real-time vehicular applications. This efficient cryptographic choice, though increasing the data transmission size slightly, offers a well-calculated trade-off for enhanced system throughput and reduced computational delays.

The communication overhead analysis underscores the scheme’s prowess in handling vast data inflows, without succumbing to bottlenecks, primarily due to the BCP algorithm’s adaptability. This algorithm not only ensures rapid decryption but also showcases potential for future vehicular network adaptations, as newer technologies become integrated.

Lastly, the efficiency analysis encapsulates the scheme’s holistic approach towards vehicular crowdsensing networks. It emphasizes the importance of real-time data transmission, scalability, and data integrity. The scheme’s modular design ensures its adaptability to ever-growing urban vehicular networks, without compromising data reliability.

In summation, my scheme, through its balanced emphasis on security and efficiency, provides a resilient foundation for future vehicular communication, promising enhanced adaptability and refinement in the face of evolving challenges.

6 Conclusion and Recommendation

In my study, I 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:** My architecture robustly safeguards diverse vehicular information, such as location, identity, and reputation scores. This intricate protection ensures privacy without compromising the necessary traceability, allowing trusted entities to access vital information when deemed essential. Specifically, through advanced cryptographic primitives, the scheme ensures that adversaries cannot gain access to sensitive vehicular information. The dual advantage of this method is the guaranteed confidentiality of data in transit and the provision for authorized entities to trace and retrieve data when mandated, thus striking a balance between privacy and utility.
- **Enhanced Efficiency:** Efficiency remains integral to my design ethos. The scheme, through its computational and communication overhead metrics, elucidates this emphasis. The strategic incorporation of the BCP algorithm, celebrated for its batch decryption capability, not only fortifies security but also notably mitigates computational overhead in multifaceted settings. Beyond the mere numbers, this efficiency translates to real-world benefits, such as reduced latency in data processing and transmission, conservation of vehicular computational resources, and a seamless user experience, especially critical in real-time vehicular applications.
- **Support for Multi-Tasks:** Intrinsically architected for multi-task vehicular networks, my scheme assures secure task distribution and data submission, while concurrently optimizing communication overhead. The BCP algorithm, with its batch processing prowess, ensures scalability even as vehicular nodes proliferate. This feature is particularly beneficial in dynamic vehicular networks where tasks are numerous, diverse, and often concurrent. By facilitating secure multi-tasking, my scheme ensures that vehicles can participate in multiple sensing or computational tasks without compromising on data integrity or privacy, all the while ensuring that the network remains agile and responsive.

In essence, my 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, my 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, I plan to establish verification mechanisms to confirm the integrity and authenticity of these entities.

7 Reflection

Reflecting upon the endeavor to design a vehicular crowdsensing scheme that expertly balances vehicular privacy with computational and communicational efficiency, one is led to ponder both the milestones achieved and the challenges encountered.

The primary aim of this research was unmistakably clear: to devise a scheme that not only prioritizes vehicular privacy in multi-task environments but also ensures a lean computational and communication footprint. Navigating the intricacies of this aim, it became evident that the intersection of privacy and efficiency is a delicate balancing act, often requiring meticulous calibration of cryptographic methods and protocols.

The analysis, as detailed in the preceding sections, reveals that the scheme indeed exhibits a promising blend of robust security and swift efficiency. The integration of the BCP algorithm, with its batch decryption capability, emerged as a cornerstone for computational efficiency. Furthermore, the scheme’s dedication to preserving sensitive vehicular information, from location to identity, underscores the commitment to privacy.

However, reflection isn’t just about acknowledging achievements; it’s also about recognizing areas that beckon further exploration. One such area is the trade-off introduced by the BCP algorithm. While it significantly optimizes decryption times, it introduces slightly larger ciphertexts. This addition, albeit strategic, prompts consideration of whether there are avenues to further optimize this without compromising on the benefits the BCP offers.

Recalling the objectives:

- Understand the vulnerabilities inherent in vehicular crowdsensing networks.
- Develop cryptographic methods that safeguard vehicular privacy.
- Analyze the computational and communication overhead of the scheme.
- Ensure scalability and adaptability of the scheme for future vehicular communication paradigms.

In retrospect, there has been a deep dive into the vulnerabilities, paving the way for a cryptographic approach that inherently respects vehicular privacy. The analysis sections offer a transparent view of the overheads, and the scheme’s modular design suggests scalability. Yet, the rapidly evolving world of vehicular communication, with technologies like 5G, edge computing, and quantum computing on the horizon, will invariably introduce new challenges.

This reflection also brings forth an appreciation for the interconnectedness of the objectives. The understanding of vulnerabilities directly influenced the cryptographic choices, and the emphasis on efficiency naturally led to the dissection of overheads. This interwoven nature of objectives reinforces the idea that in the realm of cybersecurity, every facet, from understanding threats to implementing defenses, is intrinsically linked.

In conclusion, while this research journey has been immensely enlightening, and the scheme lays a strong foundation for vehicular privacy and efficiency, the path ahead is rife with opportunities. The ever-evolving landscape of vehicular communication will continue

to pose challenges, and as a researcher, the endeavor will always be to stay a step ahead, refining and reinventing approaches in pursuit of an even more secure and efficient vehicular future.

References

- [1] G Bertoni, J Daemen, M Peeters, and G Van Assche. The keccak sha-3 submission (2011), submission to nist (round 3), 2014.
- [2] 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.
- [3] Claude Castelluccia, Einar Mykletun, and Gene Tsudik. Efficient aggregation of encrypted data in wireless sensor networks. In *The second annual international conference on mobile and ubiquitous systems: networking and services*, pages 109–117. IEEE, 2005.
- [4] Lin Chen, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi. On security analysis of proof-of-elapsed-time (poet). In *Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, November 5–8, 2017, Proceedings 19*, pages 282–297. Springer, 2017.
- [5] 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.
- [6] Yudan Cheng, Jianfeng Ma, Zhiquan Liu, Yongdong Wu, Kaimin Wei, and Caiqin Dong. A lightweight privacy preservation scheme with efficient reputation management for mobile crowdsensing in vehicular networks. *IEEE Transactions on Dependable and Secure Computing*, 2022.
- [7] 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.
- [8] Wenliang Du and Zhijun Zhan. A practical approach to solve secure multi-party computation problems. In *Proceedings of the 2002 workshop on New security paradigms*, pages 127–135, 2002.
- [9] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, and Alejandro Quintero. Vanet security surveys. *Computer Communications*, 44:1–13, 2014.
- [10] Raghu K Ganti, Fan Ye, and Hui Lei. Mobile crowdsensing: current state and future challenges. *IEEE communications Magazine*, 49(11):32–39, 2011.

- [11] 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.
- [12] 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.
- [13] 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.
- [14] 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.
- [15] 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.
- [16] 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.
- [17] 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.
- [18] 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.
- [19] 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.
- [20] 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.
- [21] 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.

- [22] 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.
- [23] Danda B Rawat, Dimitrie C Popescu, Gongjun Yan, and Stephan Olariu. Enhancing vanet performance by joint adaptation of transmission power and contention window size. *IEEE Transactions on Parallel and Distributed Systems*, 22(9):1528–1535, 2011.
- [24] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of computer security*, 15(1):39–68, 2007.
- [25] Madhusudan Singh and Shiho Kim. Blockchain technology for decentralized autonomous organizations. In *Advances in computers*, volume 115, pages 115–140. Elsevier, 2019.
- [26] 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.
- [27] 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.
- [28] Zhe Xia, Shiyun Liu, Yichen Huang, Hua Shen, and Mingwu Zhang. A multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks. In *International Symposium on Emerging Information Security and Applications*, pages 21–36. Springer, 2022.
- [29] 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.
- [30] 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.