

Project Proposal: A Multi-task Mobile Crowdsensing Scheme with Conditional Privacy Preserving for Vehicle Networks

Yichen Huang(2200440)

April 18, 2023

Contents

1	Introduction	1
1.1	Background and Hypothesis	2
1.2	Research Problem	2
1.3	Significance	3
1.4	Scope and Limitations:	3
1.5	Section Conclusion	3
2	Literature Review	4
2.1	Privacy Protection in Mobile Crowdsensing for Vehicular Networks	4
2.2	Reputation Management in Multi-Task Mobile Crowdsensing	4
2.3	Conditional Privacy Preserving in Mobile Crowdsensing for Vehicular Networks	4
2.4	Section Conclusion	5
3	Methodology	5
3.1	Research Design	5
3.2	Research Strategies	6
3.3	Security Analysis	7
3.4	Data Testing and Security Requirements	7
3.5	Section Conclusion	8
4	Expected Outcomes and Contributions	8
4.1	Expected Outcomes	8
4.2	Contributions	9
4.3	Section Conclusion	10
5	Schedule and Plan	10
6	Evaluation and Conclusion	10

1 Introduction

Mobile crowdsensing is a method that involves a group of users and their sensing devices to perform sensing tasks. This approach is highly flexible, scalable, and cost-effective. With the development of vehicle networks, researchers have explored the use of vehicles as sensing units for mobile crowdsensing. However, many studies in this field have certain limitations. Firstly, they tend to prioritize either privacy preservation or supervision, but not both. Secondly, they often focus on a single sensing task and do not consider the management of users' reputations across multiple tasks. To overcome these limitations, we propose a multi-task mobile crowdsensing scheme that offers conditional privacy preservation for vehicle networks. Our scheme harmonizes the requirements for privacy preservation and supervision, thereby achieving conditional privacy preservation. It also allows each vehicle to participate in multiple sensing tasks simultaneously. Our privacy protection measures cover identity

privacy, location privacy, and reputation privacy at the same time. In addition, the reputation center does not need to store any internal information when updating vehicles' pseudonyms, minimizing the risks of Denial-of-Service attacks. As a result, our proposed scheme offers a more secure and practical solution for mobile crowdsensing. Security analyses demonstrate that our scheme meets the desirable security requirements, including correctness, conditional privacy preservation, and authentication. Efficiency analyses show that our scheme can be applied efficiently in multi-task mobile crowdsensing.

1.1 Background and Hypothesis

Mobile crowdsensing [1](MCS) has become a popular method for data collection and analysis in various applications, including transportation, medical treatment, and healthcare. MCS involves recruiting a group of users and utilizing their sensing devices to accomplish a sensing task. With the development of mobile Internet and the widespread deployment of intelligent devices with sensors, the concept of MCS has become more prevalent. However, MCS faces various challenges, including privacy concerns, security threats, and the management of users' reputations across multiple tasks.

Vehicular networks are an ideal platform for MCS, as they enjoy many advantages, such as high mobility, low energy consumption, and convenient installation and maintenance. In vehicular networks, vehicles can serve as sensor nodes for MCS, and researchers have investigated how to use vehicles as the sensing units for MCS. However, the openness of vehicular networks makes them vulnerable to various attacks, and the majority of existing schemes can only achieve privacy preservation or supervision, but not both. Moreover, they mainly consider a single sensing task and overlook the management of users' reputations across multiple tasks.

Hypothesis: We propose a multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks to overcome the limitations of existing schemes. Our proposed scheme harmonizes the requirements for privacy preservation and supervision, achieving a property called conditional privacy preserving. Each vehicle can participate in multiple sensing tasks at the same time, and privacy protection covers identity privacy, location privacy, and reputation privacy simultaneously. Our scheme provides a more secure and practical solution for mobile crowdsensing, achieving the desirable security requirements, such as correctness, conditional privacy preserving, and authentication.[2]

Moreover, our proposed scheme uses a reputation value to evaluate the trustworthiness of the vehicles, which is often issued and managed by a reputation center. When updating the pseudonyms of the sensing vehicles, our proposed scheme does not require the reputation center to store any internal information, such as random numbers or ephemeral keys, reducing the risks of DoS attacks and storage overheads. Our proposed scheme can be used efficiently in multi-task mobile crowdsensing, achieving conditional privacy preserving for identity, location, and reputation value simultaneously, and providing a practical and secure solution for vehicular networks.

In conclusion, our proposed multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks can overcome the limitations of existing schemes, achieve desirable security requirements, and provide a practical and secure solution for MCS in vehicular networks.

1.2 Research Problem

Mobile crowdsensing (MCS) is a powerful technique that has gained widespread use in various fields, including transportation, medical treatment, and healthcare. However, MCS faces various security and privacy challenges, especially in vehicular networks, where the openness of the network makes it vulnerable to attacks. The majority of existing MCS schemes for vehicular networks can only achieve privacy preservation or supervision, but not both, and they mainly consider a single sensing task, overlooking the management of users' reputations across multiple tasks. Moreover, achieving privacy protection in location and identity already causes large overheads in communication and computing. If the reputation value is also protected, the system may become even more complex. Therefore, there is a need for a multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks that can harmonize the requirements for privacy preservation and supervision and enable each vehicle to participate in multiple sensing tasks simultaneously.

The research problem addressed in this proposal is how to develop a multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks that can provide a more secure and practical solution for MCS, while achieving desirable security requirements, such as correctness, conditional privacy preserving, and authentication. This scheme should also address the challenges of reputation management in vehicular networks and reduce the risks of DoS attacks and storage overheads. This research problem is significant because it addresses the limitations of existing MCS schemes for vehicular networks and provides a more comprehensive and efficient solution for multi-task mobile crowdsensing with conditional privacy preserving.

1.3 Significance

The proposed multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks is significant for several reasons.

- First, the scheme addresses the limitations of existing MCS schemes for vehicular networks, which can only achieve privacy preservation or supervision, but not both, and they mainly consider a single sensing task, overlooking the management of users' reputations across multiple tasks. Our proposed scheme achieves conditional privacy preserving for identity, location, and reputation value simultaneously, harmonizing the requirements for privacy preservation and supervision, and enabling each vehicle to participate in multiple sensing tasks simultaneously.
- Second, our proposed scheme provides a more secure and practical solution for MCS in vehicular networks. Reputation value is used to evaluate the trustworthiness of the vehicles, and our scheme does not require the reputation center to store any internal information, such as random numbers or ephemeral keys, reducing the risks of DoS attacks and storage overheads.
- Third, our proposed scheme achieves desirable security requirements, such as correctness, conditional privacy preserving, and authentication. Security analyses prove that our scheme can provide a secure and efficient solution for multi-task mobile crowdsensing in vehicular networks.
- Finally, the proposed scheme has practical applications in various fields, including transportation, medical treatment, and healthcare. The ability to collect and analyze information about the surrounding environment can provide valuable insights and improve the efficiency and effectiveness of various applications.

In conclusion, the proposed multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks is significant because it addresses the limitations of existing MCS schemes, provides a more secure and practical solution for MCS in vehicular networks, achieves desirable security requirements, and has practical applications in various fields.

1.4 Scope and Limitations:

The proposed multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks has a specific scope and limitations that need to be considered.

Firstly, our proposed scheme focuses on mobile crowdsensing in vehicular networks, where vehicles serve as sensor nodes. The proposed scheme aims to address the limitations of existing MCS schemes, achieve conditional privacy preserving for identity, location, and reputation value, and provide a more secure and practical solution for multi-task sensing in vehicular networks.

Secondly, the proposed scheme considers the reputation value to evaluate the trustworthiness of the vehicles, which is often issued and managed by a reputation center. The proposed scheme reduces the risks of DoS attacks and storage overheads by not requiring the reputation center to store any internal information when updating the pseudonyms of the sensing vehicles.

However, there are some limitations to the proposed scheme. Firstly, the proposed scheme requires a trusted authority to perform effective supervision, which may not always be possible in some scenarios. Secondly, achieving privacy protection in location and identity already causes large overheads in communication and computing, and if the reputation value is also protected, the system may become even more complex. Therefore, the proposed scheme may not be suitable for all scenarios, especially those with limited computing and communication resources.

In conclusion, the proposed multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks has a specific scope and limitations that need to be considered. The proposed scheme focuses on mobile crowdsensing in vehicular networks, aims to address the limitations of existing MCS schemes, and provides a more secure and practical solution for multi-task sensing. However, the proposed scheme may not be suitable for all scenarios and requires a trusted authority to perform effective supervision.

1.5 Section Conclusion

In this proposal, we have presented a research problem, significance, and scope of a proposed multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks. We identified the limitations of existing MCS schemes for vehicular networks and highlighted the need for a more comprehensive and efficient solution for multi-task mobile crowdsensing with conditional privacy preserving. Our proposed scheme achieves

conditional privacy preserving for identity, location, and reputation value simultaneously, harmonizing the requirements for privacy preservation and supervision and enabling each vehicle to participate in multiple sensing tasks simultaneously.

We have shown that our proposed scheme provides a more secure and practical solution for MCS in vehicular networks by reducing the risks of DoS attacks and storage overheads. Moreover, we have demonstrated that our proposed scheme achieves desirable security requirements, such as correctness, conditional privacy preserving, and authentication.

Finally, we acknowledge that our proposed scheme has limitations, such as requiring a trusted authority to perform effective supervision and being unsuitable for all scenarios, especially those with limited computing and communication resources.

In conclusion, the proposed multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks has significant potential in various fields, including transportation, medical treatment, and healthcare. Our proposed scheme provides a more comprehensive and efficient solution for multi-task mobile crowdsensing with conditional privacy preserving in vehicular networks, and it has practical applications in various fields.

2 Literature Review

2.1 Privacy Protection in Mobile Crowdsensing for Vehicular Networks

Many existing schemes have focused on achieving privacy protection in mobile crowdsensing based on vehicular networks, with particular emphasis on identity and location privacy. For instance, Ni et al. [3] utilized matrices to record sensing areas and tasks, and randomized matrix multiplication to obtain matching of sensing tasks. Wang et al. [4] proposed an area obfuscation mechanism that combined ϵ -differential privacy with δ -distortion privacy in sparse mobile crowdsensing to address privacy protection for vehicle location. Sun et al. [5] used homomorphic encryption for privacy protection, while Zhao et al. [6] employed zero-knowledge proofs to ensure statistics privacy. However, these schemes often suffer from heavy communication and computation overheads, which limit their practical applicability in real-world scenarios.

2.2 Reputation Management in Multi-Task Mobile Crowdsensing

In order to assess the trustworthiness of sensing vehicles, many researchers have proposed using reputation value as a metric. Reputation value is often used to determine the qualification of a vehicle to participate in sensing tasks, and some schemes have even incorporated real-time updates of reputation value, such as at the end of each sensing task. However, these reputation management schemes have typically not considered the multi-task environment [7]. Additionally, some schemes have suggested that reputation value should not only be updated for a single task, but also take into account the reputation feedback report and the vehicle's original reputation value when calculating the weight of the new reputation value [8]. Nevertheless, existing literature has shown limited consideration for protecting the reputation values of vehicles, which can potentially be leaked and used by adversaries to infer the trajectory and driving patterns of the vehicles. For example, Liu [8] proposed a reputation management scheme where reputation values are used to collect high-quality sensor data, but this information is susceptible to interception or tampering. Although some schemes, such as the one proposed by Ni et al. [3], suggest transmitting and storing reputation values in a threshold fashion, the protection is limited and reputation values can still be inferred by adversaries. Hash-based approaches, such as the one proposed by Zhang et al. [9], provide lightweight privacy preserving for reputation values, but are still vulnerable to attacks due to the deterministic nature of hash functions.

2.3 Conditional Privacy Preserving in Mobile Crowdsensing for Vehicular Networks

Conditional privacy preserving is another important requirement in mobile crowdsensing for vehicular networks. Raya [10] proposed a conditional privacy preserving authentication scheme with anonymous certificates, where vehicles' on-board units (OBUs) are pre-loaded with public/private key pairs and corresponding certificates to protect their identities. However, this scheme has drawbacks, including the need for large storage space for data storage by both vehicles and the trusted third party, and the long recovery time for a malicious vehicle's identity after sending a faulty message. To address these limitations, Lu et al. [11] proposed a modified conditional privacy preserving authentication scheme using anonymous certificates, where vehicles obtain temporary anonymous certificates when passing by a roadside unit (RSU). However, this approach still requires frequent requests for new

anonymous certificates to achieve conditional privacy preserving, as the adversary can trace a vehicle if the same certificate is used for a long period. Zhang et al. [12] presented a novel conditional privacy preserving authentication scheme leveraging pseudonyms and ID-based signatures in order to protect entities' privacy [13]. Nevertheless, existing schemes have not fully addressed the need for conditional privacy preserving, and there is a gap in the literature in terms of integrating reputation management and multi-task considerations into the privacy protection framework for mobile crowdsensing in vehicular networks.

2.4 Section Conclusion

In summary, existing literature in the field of mobile crowdsensing for vehicular networks has made significant contributions in terms of privacy protection, reputation management, and conditional privacy preserving. However, there are still several gaps that need to be addressed. These include the heavy communication and computation overheads of existing privacy protection schemes, the lack of consideration for multi-task environments in reputation management schemes, the vulnerability of reputation values to interception and tampering, and the frequent requests for new anonymous certificates in conditional privacy preserving schemes. Additionally, there is a need for further research on integrating reputation management and multi-task considerations into the privacy protection framework for mobile crowdsensing in vehicular networks.

Furthermore, there is a lack of literature that provides new theoretical insights or develops new models as conceptual frameworks for research in this field. Most existing schemes are based on traditional cryptographic techniques, such as homomorphic encryption, zero-knowledge proofs, and hash-based approaches, but there may be opportunities to explore new approaches or frameworks that can better address the challenges of privacy protection, reputation management, and conditional privacy preserving in mobile crowdsensing for vehicular networks.

Lastly, while some existing literature claims that their proposed research will contribute to the literature, there is a need for empirical evidence and validation to support these claims. It is important to conduct rigorous evaluation and validation of proposed schemes to demonstrate their effectiveness, efficiency, and real-world applicability. This can be achieved through simulations, experiments, or real-world deployments to validate the proposed frameworks and their contributions to the literature.

In conclusion, the literature review serves as a critical component of research in mobile crowdsensing for vehicular networks, providing a comprehensive overview of the existing literature, identifying gaps and limitations, and highlighting the need for further research. It acknowledges the contributions of previous works, demonstrates the researcher's knowledge and understanding of the research problem and related theoretical and research issues, and sets the stage for the proposed research by providing new insights, developing conceptual frameworks, and validating the significance and potential contributions of the proposed research to the literature.

3 Methodology

3.1 Research Design

The proposed system model, as depicted in Fig. 2, consists of five entities: data requester, cloud server, reputation center, roadside unit, and sensing vehicle.

Data requester: The data requester can be a management department, a service department, or an authorized individual. It assigns sensing tasks to obtain valuable information, such as road conditions, weather data, congestion levels, etc.

Cloud server: The cloud server collects, stores, and processes the encrypted sensing data. It also evaluates the trustworthiness of sensing vehicles based on the accuracy of their submitted data and generates reputation feedback reports. The cloud server typically has strong storage and computing capabilities.

Reputation center: The reputation center is responsible for verifying, storing, and distributing reputation values and pseudonyms to each sensing vehicle. It also updates the reputation values of the vehicles based on the reputation feedback reports.

Roadside Unit (RSU): The RSU is deployed on both sides of the road and is responsible for data transmission. It provides data transmission services between cloud servers and sensing vehicles, as well as between reputation centers and sensing vehicles.

Sensing vehicle: The sensing vehicle is equipped with various sensors that collect and store environmental data. Each sensing vehicle also has an on-board unit (OBU) that stores secret information, such as secret keys, identities, and locations.

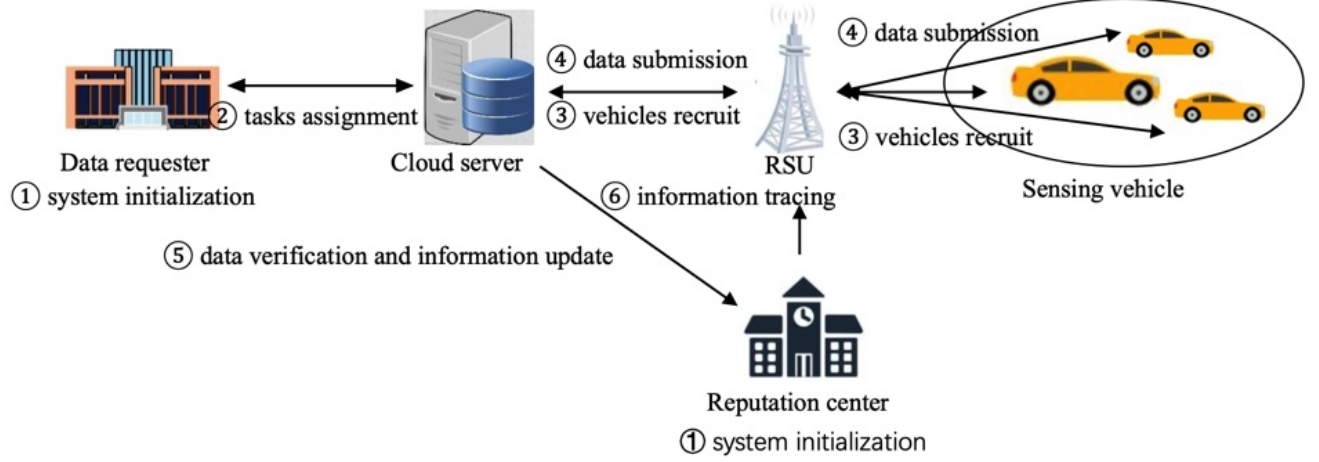


Figure 1: System architecture of the proposed scheme.

The proposed system model involves these entities working together to enable secure and reliable data collection and reputation management in the urban sensing system.

3.2 Research Strategies

Design and Development of Secure Data Collection Mechanism: In this research strategy, we will focus on designing and developing a robust and secure data collection mechanism that ensures the integrity and authenticity of the collected data. This will involve using advanced encryption techniques, such as symmetric or asymmetric encryption, to protect the data during transmission and storage. Data integrity and authenticity checks, such as digital signatures or message authentication codes (MACs), will be implemented to detect and prevent data tampering or spoofing. Moreover, secure communication protocols, such as Transport Layer Security (TLS), will be utilized to establish secure channels between the data requester, sensing vehicles, roadside units, cloud server, and reputation center, ensuring end-to-end data security.

Reputation Management Algorithm Design: In this research strategy, we will develop an effective reputation management algorithm that accurately evaluates the trustworthiness of sensing vehicles based on their submitted data. This algorithm will consider various factors, such as data accuracy, consistency, and reliability, to generate reputation feedback reports for each sensing vehicle. Machine learning techniques, such as supervised or unsupervised learning, may be employed to train the reputation management algorithm using historical data. The algorithm will be designed to adaptively update the reputation values of sensing vehicles based on the feedback reports from the cloud server and reputation center, ensuring accurate and dynamic reputation assessment.

Pseudonym Management and Privacy Preservation: In this research strategy, we will design and implement a pseudonym management mechanism that protects the privacy of sensing vehicles. This mechanism will generate and distribute pseudonyms to each vehicle to prevent the linking of their real identities with the collected data, ensuring anonymity. Pseudonyms will be securely stored in the on-board unit (OBU) of sensing vehicles and will be used for data submission to the cloud server and reputation center. Privacy preservation techniques, such as data anonymization, will be employed to further protect the privacy of the collected data. Differential privacy, which adds statistical noise to the data, can also be used to achieve a balance between data utility and privacy.

Communication and Networking Protocol Design: In this research strategy, we will design efficient communication and networking protocols for data transmission between the entities in the system, including the cloud server, reputation center, roadside units, and sensing vehicles. These protocols will ensure secure and reliable data transmission, authentication of entities, and efficient utilization of communication resources. For instance, secure communication protocols, such as Secure Socket Layer (SSL) or Internet Protocol Security (IPsec), will be used to establish secure channels for data transmission. Authentication mechanisms, such as digital certificates or public key infrastructure (PKI), will be employed to verify the identities of entities before data transmission. Moreover, optimized communication protocols, such as lightweight protocols or multicast protocols, will be designed

to reduce communication overhead and improve system efficiency.

Performance Evaluation and Security Analysis: In this research strategy, we will conduct comprehensive performance evaluation and security analysis of the proposed system. Performance evaluation will involve conducting simulations or experiments to measure the efficiency and effectiveness of the data collection mechanism, reputation management algorithm, and pseudonym management mechanism. Performance metrics, such as data accuracy, data delivery ratio, system throughput, and system response time, will be used to assess the system performance. Security analysis will involve identifying potential vulnerabilities and threats to the system, such as data tampering, data spoofing, identity theft, and replay attacks, and proposing appropriate countermeasures to mitigate these risks. Security evaluation metrics, such as confidentiality, integrity, availability, and authenticity, will be used to assess the system security.

By pursuing these detailed research strategies, we aim to develop a robust and secure urban sensing system that ensures the security, privacy, and reliability of data collection and reputation management. The proposed system will contribute to the advancement of smart city technologies and enable

3.3 Security Analysis

In our proposed urban sensing system, we assume that the data requester, the cloud server, and the roadside units (RSUs) are honest-but-curious entities. This means that while they will follow the protocol, they may attempt to obtain information beyond their authorized access. For example, in a mobile crowdsensing environment based on vehicular networks, these entities may try to infer the location, identity, and reputation information of the sensing vehicles, which can be referred to as inference attacks. These inference attacks can include location inference attacks, identity inference attacks, and reputation inference attacks. Additionally, if a malicious adversary intercepts a series of reputation values for the same sensing vehicle, they may be able to infer other information, such as the driving mode of the vehicle, which is known as a reputation linkable attack.

We also assume that the reputation center in our system is fully trusted. However, we acknowledge that there may be a minority of dishonest sensing vehicles that may attempt to carry out various attacks. These attacks can include data pollution attacks, where malicious sensing vehicles submit false sensing data in order to pollute the overall sensing results. Another type of attack is the Sybil attack, where malicious sensing vehicles may submit the same data multiple times or use fake identities to manipulate their reputation and obtain a higher reputation score or disrupt the sensing results. Lastly, malicious sensing vehicles with low reputation values may attempt reputation tamper attacks, where they tamper with their own reputation values in order to participate in sensing tasks for which they are not authorized.

To mitigate these potential attacks, our research will focus on developing robust mechanisms and algorithms that can detect and prevent data pollution, Sybil, and reputation tamper attacks. We will also design secure communication protocols and pseudonym management mechanisms to protect the privacy and anonymity of sensing vehicles, and ensure that only authorized entities have access to sensitive information. Moreover, we will conduct thorough security analysis to identify and address potential vulnerabilities in the system, and evaluate the performance of our proposed system using various metrics to ensure its efficiency and effectiveness.

By addressing these potential attacks and implementing appropriate countermeasures, our proposed system aims to ensure the security, privacy, and reliability of data collection and reputation management in the urban sensing environment. This will contribute to the advancement of smart city technologies and enable trustworthy and efficient urban sensing applications.

3.4 Data Testing and Security Requirements

Correctness: It is essential that the protocol generates correct outputs when all participants execute it honestly. This means that the data collected from sensing vehicles should be accurately processed and analyzed to generate reliable results. Any deviation from the correct execution of the protocol may result in inaccurate or misleading data, which can affect the overall trustworthiness of the system.

Conditional Privacy Preservation: Privacy protection is enforced on the identity, location, and reputation values of sensing vehicles to prevent adversaries from gaining unauthorized access to this information. Identity privacy ensures that the real identity of sensing vehicles cannot be extracted by adversaries during communication with other entities. Location privacy ensures that malicious adversaries cannot learn about the precise locations of sensing vehicles through messages. Reputation value privacy ensures that the reputation values of vehicles are not exposed or linked. However, the trusted authority may have the capability to extract the real identity, location, and reputation value from the exchanged messages in a multi-task environment when necessary. This conditional

privacy preservation approach ensures that sensitive information is protected from unauthorized access, while still allowing for necessary access by trusted entities.

Authentication: To ensure the integrity and authenticity of the exchanged messages, it is imperative that the messages cannot be tampered or fabricated by adversaries without being detected. This requires the use of authentication mechanisms, such as digital signatures or message authentication codes, to verify the integrity of the messages. Any attempt to tamper with or forge messages should be detected and rejected by the system to prevent unauthorized modifications to the data or communications.

Resistance to Other Attacks: The proposed scheme should be able to withstand various attacks that may occur in real-world applications. These attacks may include inference attacks, reputation linkable attacks, data pollution attacks, Sybil attacks, and reputation tamper attacks, among others. Inference attacks involve adversaries trying to learn sensitive information, such as location, identity, or reputation, from the data collected by sensing vehicles. Reputation linkable attacks involve adversaries trying to link reputation values to other information to infer additional information. Data pollution attacks involve malicious sensing vehicles submitting false or misleading data to pollute the overall sensing results. Sybil attacks involve malicious sensing vehicles submitting multiple fake identities to manipulate reputation scores. Reputation tamper attacks involve malicious sensing vehicles tampering with reputation values to participate in unauthorized sensing tasks. The proposed scheme should have robust mechanisms and algorithms to detect, prevent, and mitigate these types of attacks to ensure the overall security and reliability of the system.

In summary, our proposed scheme includes security requirements such as correctness, conditional privacy preservation, authentication, and resistance to various attacks. Through the implementation of these security measures, we aim to create a secure and trustworthy environment for data collection and processing in urban sensing applications.

3.5 Section Conclusion

In conclusion, our proposed methodology for data testing and security in urban sensing applications involves the design of a secure protocol, development of algorithms and mechanisms to implement the security requirements, simulation and evaluation of the scheme’s performance, and fine-tuning and optimization based on the results. Through the implementation of this methodology, we aim to create a secure and trustworthy environment for data collection and processing, ensuring the integrity, privacy, and authenticity of the data exchanged among the entities involved. The proposed methodology can be further refined and customized based on the specific requirements and characteristics of the urban sensing applications, and can serve as a foundation for building secure and reliable data testing and security solutions in urban sensing domains.

4 Expected Outcomes and Contributions

4.1 Expected Outcomes

Enhanced Security: The proposed scheme is expected to provide a high level of security by ensuring correct outputs when all participants execute the protocol honestly. The mechanisms for conditional privacy preservation, such as identity privacy, location privacy, and reputation value privacy, are expected to effectively protect the sensitive information of sensing vehicles from adversaries. This means that adversaries will not be able to extract the real identity of sensing vehicles during communication with other entities, and the locations of sensing vehicles will not be revealed through messages. The reputation values of vehicles will also be kept confidential and not exposed or linked. However, the trusted authority will still have the ability to extract the real identity, location, and reputation value from the exchanged messages in a multi-task environment when necessary. The authentication mechanisms are expected to prevent tampering or fabrication of exchanged messages by adversaries without detection, ensuring the integrity and authenticity of the data.

Improved Privacy Preservation: The proposed scheme aims to enhance privacy preservation in urban sensing applications by protecting the identity, location, and reputation value of sensing vehicles from unauthorized extraction by adversaries. The privacy preservation mechanisms are expected to effectively prevent adversaries from learning about the real identity of sensing vehicles, protecting the privacy of the individuals and vehicles involved in the sensing network. The reputation value privacy mechanisms are expected to ensure that reputation values of vehicles are not exposed or linked, preventing potential inference attacks or reputation linkable attacks. However, the trusted authority will still have the capability to access the real reputation values from the exchanged messages when necessary, ensuring the balance between privacy and functionality.

Reliable Data Testing: The proposed scheme includes robust algorithms and mechanisms for detecting and mitigating potential data integrity issues, such as data pollution and reputation linkable attacks. The anomaly detection techniques are expected to accurately identify abnormal data points and outliers, improving the accuracy and trustworthiness of the collected data. The reputation management mechanisms are expected to ensure that reputation values of vehicles are accurately maintained and not tampered with, contributing to the reliability of the data used for decision-making and analysis. By effectively detecting and addressing data integrity issues, the proposed scheme aims to provide reliable and trustworthy data for urban sensing applications, enhancing the quality and effectiveness of the data testing process.

High Performance and Scalability: The proposed scheme aims to be efficient and scalable, minimizing the computational overhead and communication cost. The developed algorithms and mechanisms will be optimized for performance, allowing for real-time data testing and processing in large-scale urban sensing applications. The simulation and evaluation results will provide insights into the performance of the proposed scheme in realistic urban sensing scenarios, and further fine-tuning and optimization will be performed to ensure high performance and scalability of the system. The goal is to develop a practical and scalable solution that can be implemented in real-world urban sensing environments without significant performance degradation.

Real-world Applicability: The proposed scheme is designed to be adaptable and customizable based on the specific requirements and characteristics of different urban sensing domains. This ensures its applicability in real-world scenarios, where different urban sensing applications may have unique data testing and security requirements. The developed methodology can serve as a foundation for building secure and reliable data testing and security solutions in various urban sensing applications, such as traffic monitoring, environmental sensing, and smart city applications. The successful implementation of the proposed scheme is expected to contribute to the advancement of urban sensing technologies and applications, making a positive impact on real-world urban environments by providing enhanced security, improved privacy preservation, reliable data testing, and high performance.

4.2 Contributions

The proposed multi-task mobile crowdsensing scheme with conditional privacy preservation for vehicular networks makes several contributions to the field of urban sensing and privacy preservation:

- **Comprehensive Privacy Preservation:** The proposed scheme addresses the privacy concerns of identity, location, and reputation value simultaneously, providing a comprehensive solution for preserving the sensitive information of sensing vehicles. The conditional privacy preservation property ensures that the real identity of sensing vehicles is not revealed during communication, protecting the privacy of individuals and vehicles involved in the sensing network. The location privacy mechanisms prevent adversaries from tracking the movements of sensing vehicles, adding an additional layer of privacy protection. The reputation value privacy mechanisms ensure that reputation values of vehicles are not exposed or linked, preventing potential inference attacks or reputation linkable attacks. This comprehensive approach to privacy preservation contributes to enhancing the security and trustworthiness of the proposed scheme in urban sensing applications.
- **Multi-Task Capability:** The proposed scheme allows each sensing vehicle to participate in several sensing tasks simultaneously, providing a flexible and efficient solution for multi-task mobile crowdsensing. This capability enables sensing vehicles to contribute to multiple sensing applications concurrently, maximizing the utilization of resources and improving the efficiency of data collection. This multi-task capability contributes to the scalability and adaptability of the proposed scheme, making it suitable for diverse urban sensing scenarios with varying requirements and characteristics.
- **Resilience to Denial-of-Service (DoS) Attacks:** The proposed scheme reduces the risks of DoS attacks by eliminating the need for the reputation center to store any internal status, such as random numbers and ephemeral keys, when updating the pseudonyms of sensing vehicles. This design choice makes the scheme more resilient to DoS attacks that could potentially disrupt the operation of the system. The robustness against DoS attacks enhances the security and reliability of the proposed scheme, ensuring that it can operate effectively in real-world urban sensing environments.
- **Theoretical Analysis and Efficiency:** The proposed scheme has undergone theoretical analyses to demonstrate its security and efficiency. The weaknesses in existing schemes have been addressed, and the proposed scheme has been shown to be efficient for multi-task mobile crowdsensing. This theoretical analysis provides a solid foundation for the proposed scheme, validating its effectiveness in achieving the desired security and privacy preservation goals.

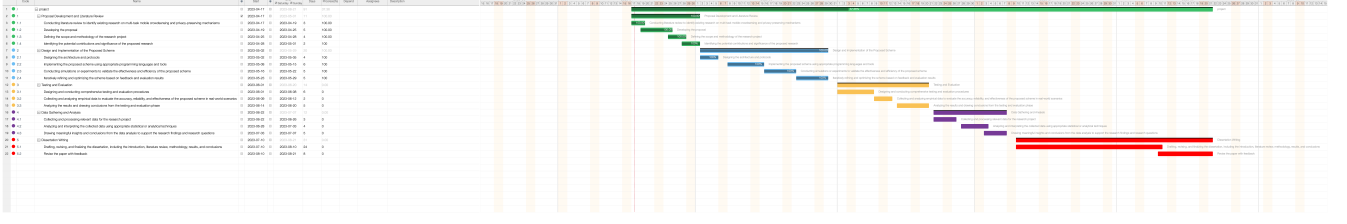


Figure 2: GANTT chart

- **Future Research Directions:** The proposed scheme identifies potential future research directions, such as considering a more severe security model, removing the assumption that the data requester, cloud server, and RSUs are honest-but-curious, and providing verification mechanisms for these entities. This identification of future research directions contributes to the advancement of the field and opens up opportunities for further exploration and improvement of the proposed scheme.

4.3 Section Conclusion

In conclusion, the proposed multi-task mobile crowdsensing scheme with conditional privacy preservation for vehicular networks makes significant contributions to the field of urban sensing and privacy preservation. The comprehensive privacy preservation, multi-task capability, resilience to DoS attacks, theoretical analysis, and identification of future research directions highlight the significance and potential impact of the proposed scheme in advancing the state-of-the-art in urban sensing technologies and applications.

5 Schedule and Plan

The research project is divided into several phases, with the official commencement around May, although preliminary work and groundwork will have been undertaken prior to that through the proposal development stage. This approach ensures that the development phase is already underway, allowing for efficient data gathering and analysis during the dedicated timeline allocated for the dissertation.

The timeline for the proposed research project is outlined in a GANTT chart, as shown in Figure 2. The chart provides a visual representation of the planned activities and their respective durations. The timeline is designed to ensure smooth progress and completion of the project within the designated timeframe.

6 Evaluation and Conclusion

To evaluate the effectiveness and performance of the proposed multi-task mobile crowdsensing scheme with conditional privacy preservation for vehicular networks, we will conduct extensive experiments and simulations in a realistic urban sensing environment. We will use performance metrics such as privacy preservation level, system overhead, communication latency, and resource utilization to measure the performance of the scheme.

We will compare the proposed scheme with existing schemes in the literature to assess its superiority in terms of privacy preservation, efficiency, and resilience against attacks. We will also evaluate the scalability and adaptability of the proposed scheme by varying the number of sensing vehicles, the number of tasks, and the density of the urban environment in our experiments.

Furthermore, we will conduct comprehensive security analysis to identify potential vulnerabilities or weaknesses in the proposed scheme. We will assess the robustness of the scheme against various types of attacks, including identity disclosure attacks, location tracking attacks, reputation inference attacks, and DoS attacks. We will also assess the performance of the proposed scheme under different traffic loads and network conditions to evaluate its stability and reliability.

In this proposal, we have presented a multi-task mobile crowdsensing scheme with conditional privacy preservation for vehicular networks. The proposed scheme addresses the privacy concerns of identity, location, and reputation value simultaneously, while allowing each sensing vehicle to participate in multiple sensing tasks efficiently. The scheme is designed to be resilient to DoS attacks and has been theoretically analyzed to demonstrate its security and efficiency.

The proposed scheme contributes to the field of urban sensing and privacy preservation by providing a comprehensive privacy preservation solution, multi-task capability, and resilience to attacks. It identifies future research directions for further improvement and advancement of the scheme.

Through extensive evaluation and simulations in a realistic urban sensing environment, we aim to validate the effectiveness and performance of the proposed scheme. The results of our evaluation will provide insights into the strengths and weaknesses of the scheme and guide potential improvements in its design and implementation.

In conclusion, the proposed multi-task mobile crowdsensing scheme with conditional privacy preservation for vehicular networks shows great promise in addressing the privacy concerns and efficiency challenges in urban sensing applications. It has the potential to contribute to the advancement of the field and provide a secure and efficient solution for multi-task mobile crowdsensing in vehicular networks.

References

- [1] R. K. Ganti, F. Ye, and H. Lei, “Mobile crowdsensing: Current state and future challenges,” *IEEE Communications Magazine*, vol. 49, no. 11, pp. 32–39, 2011.
- [2] X. Chen, S. Xu, J. Han, H. Fu, X. Pi, C. Joe-Wong, Y. Li, L. Zhang, H. Y. Noh, and P. Zhang, “Pas: Prediction-based actuation system for city-scale ridesharing vehicular mobile crowdsensing,” *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3719–3734, 2020.
- [3] J. Ni, K. Zhang, Q. Xia, X. Lin, and X. S. Shen, “Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing,” *IEEE Transactions on Mobile Computing*, vol. 19, no. 6, pp. 1317–1331, 2019.
- [4] L. Wang, D. Zhang, D. Yang, B. Y. Lim, X. Han, and X. Ma, “Sparse mobile crowdsensing with differential and distortion location privacy,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2735–2749, 2020.
- [5] G. Sun, S. Sun, H. Yu, and M. Guizani, “Toward incentivizing fog- based privacy-preserving mobile crowdsensing in the Internet of Vehicles,” *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4128–4142, 2019.
- [6] Zhao, S. Tang, X. Liu, and X. Zhang, “Pace: Privacy-preserving and quality-aware incentive mechanism for mobile crowdsensing,” *IEEE Transactions on Mobile Computing*, vol. 20, no. 5, pp. 1924–1939, 2020.
- [7] S. Gao, X. Chen, J. Zhu, X. Dong, and J. Ma, “Trustworker: A trustworthy and privacy-preserving worker selection scheme for blockchain-based crowdsensing,” *IEEE Transactions on Services Computing*, 2021.
- [8] Z. Liu, F. Huang, J. Weng, K. Cao, Y. Miao, J. Guo, and Y. Wu, “Btmpp: Balancing trust management and privacy preservation for emergency message dissemination in vehicular networks,” *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5386–5407, 2021.
- [9] Z. Liu, J. Ma, J. Weng, F. Huang, Y. Wu, L. Wei, and Y. Li, “Lppte: A lightweight privacy-preserving trust evaluation scheme for facilitating distributed data fusion in cooperative vehicular safety applications,” *Information Fusion*, vol. 73, pp. 144–156, 2021.
- [10] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.
- [11] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,” in *Proc. 27th Conf. IEEE INFOCOM*, Apr. 2008, pp. 1903–1911.
- [12] Zhang, L. Zhu, C. Xu, K. Sharif, K. Ding, X. Liu, X. Du, and M. Guizani, “Tppr: A trust-based and privacy-preserving platoon recommendation scheme in VANET,” *IEEE Transactions on Services Computing*, 2019.
- [13] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,” in *Proc. 27th Conf. IEEE INFOCOM*, Apr. 2008, pp. 1903–1911.