Computers and Artificial Intelligence；Vol.2, No.2; 2025
E-ISSN: 3006 -3728 P-ISSN：3006-371X
DOI: https://doi.org/10.70267/cai.25v2n2.0108
Published by: Zeus Press

A Survey on Truth Discovery in Crowdsensing

Yadong Peng[1*], Tianxi Wang[1], and Qing Lang[2]

[1]*Guizhou University of Finance and Economics, Guiyang, Guizhou, China*

[2]*Guizhou Normal University, Guiyang, Guizhou, China*

**Corresponding author: Yadong Peng.*

Abstract

In recent years, the rapid proliferation of smartphones and wearable devices has significantly propelled the development of crowdsensing. As a prerequisite for ensuring the secure operation of crowdsensing services, data quality has emerged as a critical issue that demands urgent resolution. This paper first introduces the main components and system workflows of crowdsensing, followed by an account of the basic concepts, principles, and key research focuses of truth discovery methods in crowdsensing. By categorizing truth discovery approaches based on modeling paradigms, this study systematically reviews the current research landscape, analyzes and compares existing methods, and constructs a comprehensive framework for their evaluation. Finally, it synthesizes the findings and identifies future challenges for truth discovery in crowdsensing, aligning with the evolving application demands of the field.

Keywords

crowdsensing, data quality, truth discovery, privacy protection

1. Introduction

With the proliferation of highly perceptive intelligent devices, crowdsensing applications have rapidly evolved (Capponi et al., 2019), being widely adopted in fields such as environmental monitoring (Feng et al., 2017), traffic management (Singh et al., 2018), and healthcare (Mehdi et al., 2019). The personal mobility and platform independence of CS enable it to achieve extensive coverage and context awareness. Data quality, a prerequisite for ensuring the secure operation of crowdsensing services, is often constrained by user reliability. The quality of data submitted by users varies widely, with even malicious users providing invalid or fraudulent sensing data (Restuccia et al., 2017). Additionally, due to differences in intelligent device quality, the reliability of sensed data cannot be guaranteed. Such noisy data may cause significant deviations between the sensing results delivered by crowdsensing systems and real-world scenarios, highlighting the urgent need to address data quality issues in crowdsensing.

Researchers have conducted in-depth studies on crowdsensing, focusing on task allocation (Dai et al., 2021; Wang et al., 2023), privacy protection (Kim et al., 2022; Perez & Zeadally, 2022), incentive mechanisms (Cai et al., 2023; Xu et al., 2024), data evaluation (An et al., 2019; Gong & Shroff, 2019), etc. These efforts demonstrate the growing attention to crowdsensing research in recent years. Thus, this paper elaborates on the research status of truth discovery in crowdsensing from the perspective of modeling approaches, aiming to provide valuable references for relevant researchers.

The structure of this paper is as follows: Section 1 introduces the fundamentals of crowdsensing. Section 2 overviews the concepts and research contents of truth discovery in crowdsensing. Section 3 classifies major truth discovery methods based on modeling paradigms, and Section 4 conducts a comparative analysis of existing works. Section 5 summarizes the findings and identifies future research directions, followed by concluding remarks.

2. Related Knowledge

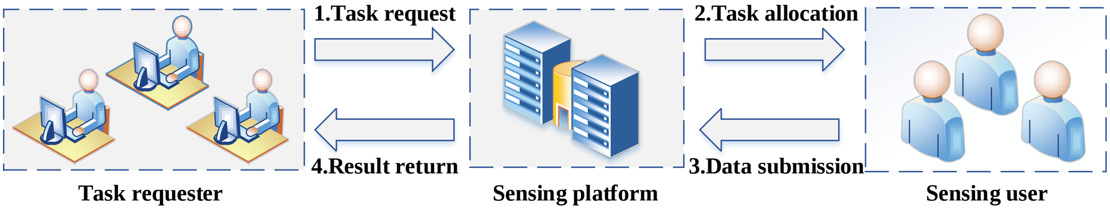
2.1 Crowdsensing

Crowdsensing, which uses intelligent terminals with capabilities such as information collection, environmental perception, and traffic monitoring as carriers (Peng et al., 2024), is an emerging data collection model (Cheng, Ma, Liu, Wu, et al., 2023; Wang et al., 2020) that has attracted extensive research and attention. Compared with traditional sensor networks, crowdsensing offers advantages such as low data collection costs, convenient device maintenance, and scalable system architecture (Z. Wang et al., 2024), fostering the emergence of numerous crowdsensing applications.

A typical crowdsensing architecture is shown in Figure 1. The system architecture comprises a sensing platform, task requesters, and sensing users. The sensing platform receives task requests from service requesters, assigns sensing tasks to users, processes the collected sensing data, and performs other management functions. Upon receiving tasks, users complete them and upload data to the platform, which processes the data and delivers results to task requesters. This entire process enables functions such as data sensing, collection, and information service provision, embodying a service model that integrates data collection, analysis, and extraction of collective intelligence (Ding et al., 2017; Guo et al., 2014).

Crowdsensing can gather massive multi-dimensional heterogeneous data from various locations, effectively addressing large-scale data requirements and providing high-quality, reliable data services. However, with the proliferation of crowdsensing, new challenges have emerged, with insufficient data quality being the primary obstacle that hinders sensing platforms from delivering optimal services. Thus, resolving data conflicts, extracting valid information from collected sensing data, and providing highly reliable and effective sensing task results have become critical issues for advancing this field.

Figure 1: Typical crowdsensing scenarios



2.2 Truth Discovery

The general principle of truth discovery is as follows: if a user frequently provides trustworthy data, a high reliability score will be assigned to them. Meanwhile, if a piece of information is supported by users with high reliability, it has a high probability of being selected as the ground truth.

The truth discovery methods in crowdsensing primarily involve the following concepts: An object refers to an item in a sensing task, corresponding to an entry of sensing data collected by users (Miao et al., 2015). The ground truth denotes the factual information of an object, which is an unknown quantity (Li, Li, Gao, Su, et al., 2014). The truth value is the most reliable value inferred for an object by aggregating sensing data from different users regarding the same object (Li, Li, Gao, Su, et al., 2014). Weight indicates a user's reliability, which is proportional to the quality of their sensing data (Li, Li, Gao, Su, et al., 2014). That is, the closer a user's data is to the ground truth, the greater their weight. Typically, user weights are also unknown quantities.

The crowdsensing platform is opened to all intelligent device users via the Internet, making it difficult to guarantee the work status and motivations of participating users. Furthermore, quality discrepancies among intelligent devices cause collected data to be inaccurate. Typically, data obtained by the sensing platform for the same target object may exhibit inconsistency, meaning these data often contain noise and conflicts. To address this issue, upon receiving sensing data submitted by users, the sensing platform first needs to determine the most credible ground truth of the target object and then provide this result to data requesters. Truth discovery techniques extract the truth value from sensing data provided by multiple users by evaluating the weights of participating users and inferring the real value of the target object (Li et al., 2016). The core idea is to estimate each user's reliability iteratively, estimate the ground truth of the target object by weighted aggregation of user data, until a certain convergence criterion is met—this is essentially an advanced data aggregation method.

3. Comparative Analysis

With the development of truth discovery, a variety of methods have emerged. Classified by modeling approaches, the main truth discovery methods in crowdsensing can be divided into the following three categories.

3.1 Iteration-based Method

Truth Finder is a typical iterative truth discovery framework (Li et al., 2016), which employs Bayesian analysis to iteratively estimate the reliability of data sources and identify the ground truth. It represents one of the most widely used truth discovery frameworks. Based on the iterative paradigm, numerous researchers have conducted studies, as shown in Table 1.

As can be seen, the schemes in the table propose effective solutions to issues such as computational efficiency and sparse data. However, references (Gao et al., 2020; Hu et al., 2024; Liu et al., 2021; Wu et al., 2022) exhibit trust model dependency, assuming that workers and servers are honest but curious. If malicious participants emerge in practical applications, the security of the system may be compromised. References (Gao et al., 2020; Wu et al., 2022) perform poorly in specific application scenarios, such as those involving a large number of participants or extremely unstable network enviro4nments. Additionally, Zheng et al. (2020) assumes that users and cloud servers are honest in the protocol, but in reality, users' malicious behaviors may affect data accuracy and protocol security. Some assumptions in Liu et al. (2024) (e.g., the accuracy of cost and quality information reported by workers) may not hold in practical environments, limiting the model's universality. Although Zhang and Li (2022) optimizes a certain type of truth discovery framework, its applicability to other types of truth discovery algorithms remains unclear and requires further verification.

Table 1: Comparison table of iteration-based truth discovery methods

Literature	Scheme	Advantages
Zheng et al. (2020)	Gradually optimize user weights and data inputs using iterative computation.	Enhances computational efficiency, suitable for large-scale deployment.
Liu et al. (2021)	Iteratively update user weights and aggregate data for sparse data environments.	Particularly addresses sparse data scenarios.
Gao et al. (2020)	Process multidimensional sensing data through iterative algorithms.	Supports real-time data processing.
Wu et al. (2022)	Adopt a dual-server architecture to reduce iteration processes.	Reduces user participation in computational processes.
Hu et al. (2024)	Design multi-round truth discovery mechanisms to balance efficiency and security in iterative processes.	Demonstrates good adaptability to worker dropouts.
Liu et al. (2024)	Iteratively optimize participant selection strategies by combining multi-armed bandits.	Solves the exploration-exploitation dilemma in worker recruitment.
Zhang and Li (2022)	Design defense mechanisms using iterative update strategies to resist poisoning attacks.	Enables better discrimination between normal and malicious data.

3.2 Optimization-based Method

In practical applications, the solutions of optimization-based methods are similar to those of iteration-based methods, with the typical model being CRH (Li, Li, Gao, Zhao, et al., 2014). CRH is a framework for handling data heterogeneity, in which different types of distance functions can be inserted to capture the characteristics of various data types, supporting the estimation of data source reliability across all data types.

In recent years, researchers have proposed new research schemes, as shown in Table 2. Some schemes enhance data accuracy, while others focus on privacy protection, both proposing effective solutions. However, Yan and Yang (2021) assumes that the data quality provided by vehicles at different times is relatively consistent, whereas in reality, sensor performance and environmental factors may cause fluctuations in data quality. The framework in Cheng, Ma, Liu, Li, et al. (2023) verifies reputation values but still lacks effective protection against scenarios where malicious users interfere with sensing data through other means. The effectiveness of Zhou et al. (2022) relies on the accurate modeling of spatial correlation, which may not hold for sensor data in certain environments, thus affecting the reliability of results. P. Wang et al. (2024) improves data collection efficiency through UAVs, but their high usage and maintenance costs may limit broader applications.

Table 2: Comparison table of truth discovery methods based on optimization

Literature	Scheme	Advantages
Yan and Yang (2021)	Optimize the reputation evaluation mechanism for vehicles to better assess and integrate sensing data.	More effective reliability assessment
Cheng, Ma, Liu, Li, et al. (2023)	Introduce a privacy protection mechanism for reputation values to optimize user reliability assessment.	Overcome the limitations of relying solely on data weights
Zhou et al. (2022)	Optimize user privacy protection strategies to reduce the risk of location data leakage.	Balance privacy protection and truth discovery efficiency
P. Wang et al. (2024)	Optimize the incentive mechanism to improve user participation and data quality.	Improve data accuracy and reduce sensing costs

3.3 Probabilistic Graph Model-based Method

Studies based on probabilistic graph models are shown in Table 3. Zhao et al. (2012) specifically models the characteristics of numerical data, enabling more effective handling of real-world data in practical applications. Through a Bayesian approach, the model efficiently addresses small sample sizes and outliers, reducing the impact of extreme values on results. Zhao and Han (2012) features linear time complexity, making it suitable for large-scale datasets. It can incorporate prior knowledge in low-data environments and supports online streaming data processing, adapting to dynamically changing scenarios. Du et al. (2020) considers users' fine-grained reliability across different entity groups, more accurately reflecting their observation capabilities. The contribution value calculation method proposed in Kang et al. (2024) combines data trust and bidding trust, enabling the platform to prioritize high-quality workers and thus improving data collection efficiency and reliability.

However, Zhao et al. (2012) and Zhao and Han (2012) rely on prior knowledge. Although the model can use outputs from other methods as priors, inappropriate prior selection may affect final inference results. Du et al. (2020) assumes fixed clustering of users and tasks, which may fail to adapt to dynamically changing real-world scenarios, limiting its applicability. The ground truth data used in Kang et al. (2024) are obtained from UAVs, which may be difficult to acquire in certain environments, and the high cost of UAVs themselves may restrict their large-scale deployment.

Table 3: Comparison table of truth discovery methods based on probability graph model

Literature	Scheme	Advantages
Zhao et al. (2012)	Optimize the reputation evaluation mechanism for vehicles to better assess and integrate sensing data.	More effective reliability assessment
Zhao and	Introduce a privacy protection mechanism for	Overcome the limitations of relying solely on

Han (2012)	reputation values to optimize user reliability assessment.	data weights
Du et al. (2020)	Optimize user privacy protection strategies to reduce the risk of location data leakage.	Balance privacy protection and truth discovery efficiency
Kang et al. (2024)	Optimize the incentive mechanism to improve user participation and data quality.	Improve data accuracy and reduce sensing costs

4. Future Research Directions and Challenges

4.1 Enhancing Security and Robustness

Develop truth discovery algorithms capable of withstanding attacks from malicious participants to ensure system security and stability across various network environments. This may require introducing more complex trust models to identify and exclude potential malicious behaviors. Therefore, how to effectively detect and defend against malicious activities without increasing system complexity remains a challenge, necessitating the development of smarter trust models and anomaly detection algorithms to address this issue.

4.2 Adaptability to Dynamic Environments

Develop truth discovery algorithms capable of withstanding attacks from malicious participants to ensure system security and stability across various network environments. This may require introducing more complex trust models to identify and exclude potential malicious behaviors. Therefore, how to effectively detect and defend against malicious activities without increasing system complexity remains a challenge, necessitating the development of smarter trust models and anomaly detection algorithms to address this issue.

4.3 Optimizing Cost-effectiveness

On the premise of ensuring data quality, how to reduce the costs of data collection and maintenance is an important research direction. It is necessary to explore how to leverage low-cost technical means to improve data collection efficiency and study how to optimize resource allocation to maximize benefits. Key explorations include: (1) reducing data collection and maintenance costs while ensuring data quality; (2) utilizing low-cost technical means (such as UAVs, IoT devices, etc.) to enhance data collection efficiency.

4.4 Heterogeneous Data Processing

With the continuous development of IoT and big data technologies, data sources are becoming increasingly diversified, posing a challenge of how to effectively process such heterogeneous data. There is a need to develop algorithms capable of handling data of different formats, sources, and qualities, which can effectively fuse data from different sensors, devices, and platforms. Processing heterogeneous data to adapt to diversified data sources is crucial for improving the accuracy of truth discovery.

4.5 Balancing Privacy Protection and Truth Discovery Effciency

Conducting effective truth discovery while protecting user privacy is a complex issue. There is a need to study how to safeguard user privacy and ensure the security of user data during transmission and processing, while still enabling the utilization of user data for effective truth discovery and analysis.

5. Conclusion

This paper systematically reviews the main components and system processes of crowdsensing, and deeply explores the truth discovery methods therein. From a modeling perspective, existing truth discovery methods are classified and analyzed to reveal their principles and research contents. Based on the summary of existing research achievements, this paper compares the advantages and disadvantages of different methods, and points out the shortcomings and challenges in current research. Looking to the future, with the continuous expansion of crowdsensing applications, truth discovery methods urgently need to address challenges in data quality, user reliability, and system scalability. To this end, future research can be dedicated to developing more flexible algorithms and improving data fusion techniques, so as to promote the practical application of crowdsensing in various fields and bring greater value and convenience to society.

References

An, J., Liang, D., Gui, X., Yang, H., Gui, R., & He, X. (2019). Crowdsensing quality control and grading evaluation based on a two-consensus blockchain. *IEEE Internet of Things Journal, 6*(3), 4711-4718. https://doi.org/10.1109/JIOT.2018.2883835

Cai, X., Zhou, L., Li, F., Fu, Y., Zhao, P., Li, C., & Yu, F. R. (2023). An incentive mechanism for vehicular crowdsensing with security protection and data quality assurance. *IEEE Transactions on Vehicular Technology*, *72*(8), 9984-9998. https://doi.org/10.1109/TVT.2023.3262800

Capponi, A., Fiandrino, C., Kantarci, B., Foschini, L., Kliazovich, D., & Bouvry, P. (2019). A survey on mobile crowdsensing systems: Challenges, solutions, and opportunities. *IEEE Communications Surveys and Tutorials, 21*(3), 2419-2465. https://doi.org/10.1109/COMST.2019.2914030

Cheng, Y., Ma, J., Liu, Z., Li, Z., Wu, Y., Dong, C., & Li, R. (2023). A privacy-preserving and reputation-based truth discovery framework in mobile crowdsensing. *IEEE Transactions on Dependable and Secure Computing*, *20*(6), 5293-5311. https://doi.org/10.1109/TDSC.2023.3276976

Cheng, Y., Ma, J., Liu, Z., Wu, Y., Wei, K., & Dong, C. (2023). A lightweight privacy preservation scheme with efficient reputation management for mobile crowdsensing in vehicular networks. *IEEE Transactions on Dependable and Secure Computing, 20*(3), 1771-1788. https://doi.org/10.1109/TDSC.2022.3163752

Dai, C., Wang, X., Liu, K., Qi, D., Lin, W., & Zhou, P. (2021). Stable task assignment for mobile crowdsensing with budget constraint. *IEEE Transactions on Mobile Computing, 20*(12), 3439-3452. https://doi.org/10.1109/TMC.2020.3000234

Ding, S., He, X., & Wang, J. (2017). Multiobjective optimization model for service node selection based on a tradeoff between quality of service and resource consumption in mobile crowd sensing. *IEEE Internet of Things Journal, 4*(1), 258-268. https://doi.org/10.1109/JIOT.2017.2647740

Du, Y., Sun, Y. E., Huang, H., Huang, L., Xu, H., Bao, Y., & Guo, H. (2020). Bayesian co-clustering truth discovery for mobile crowd sensing systems. *IEEE Transactions on Industrial Informatics, 16*(2), 1045-1057. https://doi.org/10.1109/TII.2019.2896287

Feng, C., Wang, W., Tian, Y., Que, X., & Gong, X. (2017). *Estimate air quality based on mobile crowd sensing and big data* [Paper presentation]. 18th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, WoWMoM 2017 - Conference, Macau, China.

Gao, J., Fu, S., Luo, Y., & Xie, T. (2020). *Location privacy-preserving truth discovery in mobile crowd sensing* [Paper presentation]. Proceedings - International Conference on Computer Communications and Networks, ICCCN, Honolulu, HI, USA.

Gong, X., & Shroff, N. B. (2019). Truthful mobile crowdsensing for strategic users with private data quality. *IEEE/ACM Transactions on Networking, 27*(5), 1959-1972. https://doi.org/10.1109/TNET.2019.2934026

Guo, B., Yu, Z., Zhou, X., & Zhang, D. (2014). *From participatory sensing to mobile crowd sensing* [Paper presentation]. 2014 IEEE International Conference on Pervasive Computing and Communication Workshops, PERCOM WORKSHOPS 2014, Budapest, Hungary.

Hu, C., Li, Z., Xu, Y., Zhang, C., Liu, X., He, D., & Zhu, L. (2024). Multiround efficient and secure truth discovery in mobile crowdsensing systems. *IEEE Internet of Things Journal, 11*(10), 17210-17222. https://doi.org/10.1109/JIOT.2024.3359757

Kang, Y., Liu, A., Xiong, N. N., Zhang, S., Wang, T., & Dong, M. (2024). DTD: An intelligent data and bid dual truth discovery scheme for MCS in IIoT. *IEEE Internet of Things Journal*, *11*(2), 2507-2519. https://doi.org/10.1109/JIOT.2023.3292920

Kim, J. W., Edemacu, K., & Jang, B. (2022). Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey. *Journal of Network and Computer Applications, 200*, Article 103315. https://doi.org/10.1016/J.JNCA.2021.103315

Li, Q., Li, Y., Gao, J., Su, L., Zhao, B., Demirbas, M., Fan, W., & Han, J. (2014). A confidence-aware approach for truth discovery on long-tail data. *Proceedings of the VLDB Endowment*, *8*(4), 425-436. https://doi.org/10.14778/2735496.2735505

Li, Q., Li, Y., Gao, J., Zhao, B., Fan, W., & Han, J. (2014). *Resolving conflicts in heterogeneous data by truth discovery and source reliability estimation* [Paper presentation]. Proceedings of the ACM SIGMOD International Conference on Management of Data, New York, NY, United States.

Li, Y., Gao, J., Meng, C., Li, Q., Su, L., Zhao, B., Fan, W., & Han, J. (2016). A survey on truth discovery. *ACM SIGKDD Explorations Newsletter, 17*(2), 1-16. https://doi.org/10.1145/2897350.2897352

Liu, F., Zhu, B., Yuan, S., Li, J., & Xue, K. (2021). *Privacy-preserving truth discovery for sparse data in mobile crowdsensing systems* [Paper presentation]. Proceedings - IEEE Global Communications Conference, GLOBECOM, Madrid, Spain.

Liu, J., Shao, J., Sheng, M., Xu, Y., Taleb, T., & Shiratori, N. (2024). Mobile crowdsensing ecosystem with combinatorial multi-armed bandit-based dynamic truth discovery. *IEEE Transactions on Mobile Computing, 23*(12), 13095-13113. https://doi.org/10.1109/TMC.2024.3428542

Mehdi, M., Schwager, D., Pryss, R., Schlee, W., Reichert, M., & Hauck, F. J. (2019). *Towards automated smart mobile crowdsensing for tinnitus research* [Paper presentation]. Proceedings - IEEE Symposium on Computer-Based Medical Systems, Cordoba, Spain.

Miao, C., Jiang, W., Su, L., Li, Y., Guo, S., Qin, Z., Xiao, H., Gao, J., & Ren, K. (2015). *Cloud-enabled privacy-preserving truth discovery in crowd sensing systems* [Paper presentation]. SenSys 2015 - Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems, New York, NY, United States.

Peng, T., Zhong, W., Wang, G., Zhang, S., Luo, E., & Wang, T. (2024). Spatiotemporal-aware privacy-preserving task matching in mobile crowdsensing. *IEEE Internet of Things Journal*, *11*(2), 2394-2406. https://doi.org/10.1109/JIOT.2023.3292284

Perez, A. J., & Zeadally, S. (2022). Secure and privacy-preserving crowdsensing using smart contracts: Issues and solutions. *Computer Science Review*, *43*, Article 100450. https://doi.org/10.1016/J.COSREV.2021.100450

Restuccia, F., Ghosh, N., Bhattacharjee, S., Das, S. K., & Melodia, T. (2017). Quality of information in mobile crowdsensing: Survey and research challenges. *ACM Transactions on Sensor Networks, 13*(4), 1-43. https://doi.org/10.1145/3139256

Singh, V., Chander, D., Chhaparia, U., & Raman, B. (2018). *Safestreet: An automated road anomaly detection and early-warning system using mobile crowdsensing* [Paper presentation]. 2018 10th International Conference on Communication Systems and Networks, COMSNETS 2018, Bengaluru, India.

Wang, L., Yu, Z., Wu, K., Yang, D., Wang, E., Wang, T., Mei, Y., & Guo, B. (2023). Towards robust task assignment in mobile crowdsensing systems. *IEEE Transactions on Mobile Computing, 22*(7), 4297-4313. https://doi.org/10.1109/TMC.2022.3151190

Wang, P., Li, Z., Guo, B., Long, S., Guo, S., & Cao, J. (2024). A UAV-assisted truth discovery approach with incentive mechanism design in mobile crowd sensing. *IEEE/ACM Transactions on Networking, 32*(2), 1738-1752. https://doi.org/10.1109/TNET.2023.3331059

Wang, Y., Yan, Z., Feng, W., & Liu, S. (2020). Privacy protection in mobile crowd sensing: A survey. *World Wide Web, 23*(1), 421-452. https://doi.org/10.1007/S11280-019-00745-2

Wang, Z., Cao, Y., Jiang, K., Zhou, H., Kang, J., Zhuang, Y., Tian, D., & Leung, V. C. M. (2024). When crowdsensing meets smart cities: A comprehensive survey and new perspectives. *IEEE Communications Surveys and Tutorials*, *27*(2), 1101-1151. https://doi.org/10.1109/COMST.2024.3400121

Wu, H., Wang, L., Cheng, K., Yang, D., Tang, J., & Xue, G. (2022). Privacy-enhanced and practical truth discovery in two-server mobile crowdsensing. *IEEE Transactions on Network Science and Engineering*, *9*(3), 1740-1755. https://doi.org/10.1109/TNSE.2022.3151228

Xu, Y., Xiao, M., Zhu, Y., Wu, J., Zhang, S., & Zhou, J. (2024). Aoi-guaranteed incentive mechanism for mobile crowdsensing with freshness concerns. *IEEE Transactions on Mobile Computing*, *23*(5), 4107-4125. https://doi.org/10.1109/TMC.2023.3285779

Yan, L., & Yang, S. (2021). *Trust-aware truth discovery with long-term vehicle reputation for internet of vehicles crowdsensing* [Paper presentation]. 2021 International Wireless Communications and Mobile Computing, IWCMC 2021, Harbin City, China.

Zhang, H., & Li, M. (2022). *Multi-round data poisoning attack and defense against truth discovery in crowdsensing systems* [Paper presentation]. Proceedings - IEEE International Conference on Mobile Data Management, Paphos, Cyprus.

Zhao, B., & Han, J. (2012, 2012). *A probabilistic model for estimating real-valued truth from conflicting sources* [Paper presentation]. Proc. of QDB, Istanbul, Turkey.

Zhao, B., Rubinstein, B. I. P., Gemmell, J., & Han, J. (2012). A bayesian approach to discovering truth from conflicting sources for data integration. *Proceedings of the VLDB Endowment*, *5*(6), 550-561. https://doi.org/10.14778/2168651.2168656

Zheng, Y., Duan, H., Yuan, X., & Wang, C. (2020). Privacy-aware and efficient mobile crowdsensing with truth discovery. *IEEE Transactions on Dependable and Secure Computing*, *17*(1), 121-133. https://doi.org/10.1109/TDSC.2017.2753245

Zhou, T., Cai, Z., & Su, J. (2022). *Discovering truth in mobile crowdsensing with differential location privacy* [Paper presentation]. Proceedings - IEEE Global Communications Conference, GLOBECOM, Rio de Janeiro, Brazil.

Funding

This work was sponsored by the Key Laboratory Building Program of Blockchain and Fintech of Department of Education of Guizhou Province under Grant QIAN JIAO JI[2023]014.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).