Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 4792248, 8 pages
https://doi.org/10.1155/2023/4792248

Research Article

Stability Control of Position Flow Fuzzy Estimation in Swarm Intelligence Aware Privacy Protection

Zhang Yunxiang and Wang Bin

College of Information Science and Electronic Technology, Jiamusi University, Jiamusi 154007, China

Correspondence should be addressed to Wang Bin; wangbin@jmsu.edu.cn

Received 3 October 2022; Revised 27 November 2022; Accepted 13 December 2022; Published 30 January 2023

Academic Editor: Yushu Zhang

The group intelligence perception privacy protection model is a method to achieve the balance between user privacy and service requests through the cooperation between users using location services and has a good perception effect. In order to better protect the location privacy of network users and improve the stability control effect of fuzzy estimation of location flow, this paper designs a stability control method of fuzzy estimation of location flow in group intelligent perception privacy protection. This method uses the group intelligence aware privacy protection model to obtain the user network location coordinates in the group intelligence aware privacy protection. Taking the user's network location coordinates as input, the location flow queue of multiple users in the group intelligence aware privacy protection network is obtained by the Lyapunov multiobjective location flow estimation queue model. After the fuzzy processing of the user location flow queue, the online control mechanism of location flow fuzzy estimation stability under different conditions is established. According to the online control mechanism, a stability control method based on access control and group intelligence aware task allocation is used to realize the stability control of location flow fuzzy estimation in group intelligence aware privacy protection. The experimental results show that the method can obtain 100% of the user location integrity in the group intelligence aware privacy protection, and the target location flow estimation queue is more accurate. It can effectively reduce the number of communication rounds of fuzzy estimation of location flow in the group intelligence aware privacy protection and has better stability control ability.

1. Introduction

Crowdsensing is a new mobile sensing computing paradigm that extends current wireless sensing networks for mobile networks and the Internet of Things [1, 2]. At the same time, crowdsensing is very important to protect the privacy of user activity information during the extension of wireless sensing networks. When users perform network activities, their network locations possess immobility, and crowdsensing privacy protection uses fuzzy estimation to obtain user network locations when sensing user locations. However, when obtaining the user network fuzzy estimated location, it is affected by the network environment and user terminal movement [3–5], resulting in the obtained user location mobility fuzzy estimation results which are not accurate enough. There are many control methods for user location mobility estimation, such as the attribute privacy-preserving location access control method proposed by Tian et al. [6], which calculates a lightweight attribute of user location data based on user network behavior data and proposes a control scheme based on this attribute. However, the method is affected by the large amount of user behavior data in the application process, and the lightweight attributes of the user location it obtains cannot fully describe this data, resulting in poor final control. The modular control method for user location estimation under privacy protection is proposed by Yu et al. The method is based on the modular idea of estimation control for the current location of the user [7], and if the user location changes, the method needs to restart the control algorithm to perform the operation again, which causes more computation steps and slower control efficiency. To solve the above mentioned problems, this paper proposes a stability control method for location flow fuzzy estimation in crowdsensing privacy protection to improve the level of user location flow fuzzy estimation technology.

2. Position Flow Fuzzy Estimation Stability Control Method

2.1. Crowdsensing Privacy Protection Model Construction. The crowdsensing privacy-preserving approach is an approach to achieve a balance between user privacy and service requests through collaboration among users using location services [8]. This approach finds and establishes anonymous groups satisfying k-anonymity mainly for service request initiators through single-hop or multihop communication existing between users' mobile devices, as shown in Figure 1.

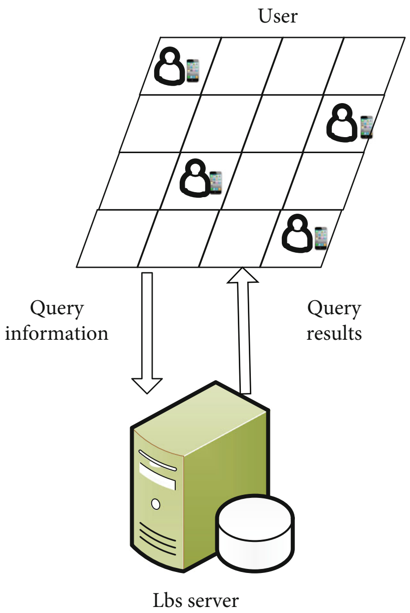

FIGURE 1: Schematic diagram of anonymous group under group intelligence aware privacy protection.

Within an anonymous group under crowdsensing privacy protection, a given user submits integrated query information, or after all users in the group submit query information together, generalization of each user's information is achieved through all collaborating users [9, 10].

Based on the specificity of the two-dimensional properties of location services, the crowdsensing privacy protection model is constructed as follows:

Let $S=\{(p_1,q_1),\cdots,(p_n,q_n)\}$ represent the set of user disturbance position coordinates in the crowdsensing network, where n represents the number of users in the crowdsensing network and then the user location flow fuzzy estimation coordinate expression formula is as follows:

$$A_{\text{acc}}=\left(\frac{\sum_{n1}p_i}{n},\frac{\sum_{n1}q_i}{n}\right). \tag{1}$$

Analyze the sensitivity of formula (1). Let the user location flow coordinate components be Δf_p and Δf_q, respectively, and then, the expression formula of the total sensitivity of the user flow location flow blur estimation is as follows:

$$\Delta f=\Delta f_p+\Delta f_q. \tag{2}$$

The result of formula (2) is the maximum value of the user position flow change in a special case.

Let Δp and Δq represent the variation range of the coordinate components when the user location flows, respectively, r represents the flow radius of the user location, and then, the relationship between Δp, Δq, and r satisfies the following conditions:

$$\begin{cases}\Delta p^2+\Delta q^2\le r^2,\\ \Delta p^2+\Delta q^2>\dfrac{\Delta p^2}{2}+\dfrac{\Delta q^2}{2},\\ \Delta p+\Delta q\le\sqrt{2r}.\end{cases} \tag{3}$$

According to formula (3), formula (1) can be rewritten as

$$A'_{\text{acc}}=\left(\frac{\sum_{n1}p_i}{n}+\text{Laplace}\left(\sqrt{\frac{2r}{\varepsilon}}\right),\frac{\sum_{n1}q_i}{n}+\text{Laplace}\left(\sqrt{\frac{2r}{\varepsilon}}\right)\right). \tag{4}$$

Using formula (4), we can obtain the user location flow coordinates and hide the coordinates to achieve user location privacy protection.

2.2. Lyapunov Multiobjective Location Flow Estimation Queue Model Construction. Based on the user location flow coordinates obtained from formula (4), a multiobjective location flow estimation queue model is established using Lyapunov exponential puissance to obtain the user location estimation queue.

Let t denote the user location mobility slot, divide the user network into K subareas denoted by $L=\{l_1,l_2,\cdots l_k\}$, and within the l_k subarea, the multitarget location mobility estimation task queue is denoted by $R_k(t)$. The maximum boundary of the subregion is $A_k^{\max}$, and the maximum number of tasks in the multitarget flow estimation task queue within this boundary is A_k^t. Then, the expression formula of the $R_k(t)$ change of the multitarget position flow estimation task queue is as follows:

$$R_k(t+1)=\max\left[R_k(t)-B_k(t),0\right]+a_k(t), \tag{5}$$

where $a_k(t)$ represents the user network subarea boundary value, and $B_k(t)$ represents the number of tasks completed in the multitarget location flow estimation queue.

Initializing formula (5) and introducing stability theory, i.e., all multiobjective location flow estimation queues are considered as stable, the constraint of formula (5) is

$$\lim_{T\longrightarrow\infty} \sup \frac{1}{T}\sum_{t=0}^{T-1} E[R_k(t)] < \infty, \forall k \in L. \tag{6}$$

Among them, T represents the user location mobility time slot set, and $E[R_k(t)]$ represents the natural multitarget location mobility estimation task queue logarithm.

Let $\sum_{i=1}^{N} u_{ik} \le B_k$ denote the task budget limit of the multitarget location flow fuzzy estimation task queue in the subregion and establish the virtual queue of the subregion l_k according to the task budget limit of the queue as $Y_k(\mathrm{t})$, and its variation expression formula is as follows:

$$Y_k(t+1) = \max\left[Y_k(t) + \sum_{i=1}^{N} u_{ik} - B_k, 0\right]. \tag{7}$$

To ensure the stability of formula (7), the auxiliary variable γ_k is defined as follows:

$$\gamma_k = \lim_{T\longrightarrow\infty} \frac{E\{\gamma_k(t)\}}{T} \le u_k, \forall k \in L. \tag{8}$$

Substituting formula (8) into formula (7), and based on the results of formula (5) and formula (7), the target location flow estimation queue function is established, and its expression formula is

$$\max \sum_{j=1}^{M}\sum_{k=1}^{K} \overline{V(\gamma_k)} = \lim_{T\longrightarrow\infty} \frac{\sum_{t=0}^{T-1}\sum_{k=1}^{K} E(V(\gamma_k))}{T}. \tag{9}$$

In the above formula, $\overline{V(\gamma_k)}$ represents the profit function under the proportional fairness constraint, and $V(\gamma_k)$ represents the profit function.

The multiple target location flow fuzzy estimation queues within the crowdsensing privacy-preserving network can be obtained using formula (9).

2.3. Online Control Mechanism for Position Flow Fuzzy Estimation Stability.

Based on the multitarget location flow estimation queue within the crowdsensing privacy-preserving network obtained in the previous subsection, the online control mechanism of this location flow estimation queue is designed for its stability control, which is detailed as follows:

Considering the correlation between the distance of the perception task and the user location when using crowdsensing to protect user privacy [11], the user location within the multitarget location flow estimation queue is fuzzy using a two-dimensional Laplace distribution approach, and the two-dimensional Laplace distribution probability density function is expressed as follows.

$$f(p,q) = \frac{\tau^2 e^{-\tau}\sqrt{p^2+q^2}}{2\pi}. \tag{10}$$

In the formula, x and y represent the random variables of the user's estimated queue position, τ represents the coefficient, and e is the natural logarithmic constant.

Due to the $\varepsilon-$ geographic indistinguishability of user-estimated queue locations [12, 13], formula (10) must satisfy the following conditions:

$$e^{-\tau}\sqrt{\frac{p^2+q^2}{e^{-\tau}}}\sqrt{(p+\Delta q)^2+(p+\Delta q)^2} \le e^{\varepsilon}. \tag{11}$$

ε is the privacy protection budget value.

According to formula (11), formula (10) can be rewritten as

$$\begin{aligned} &\tau\left(\sqrt{(p+\Delta p)^2+(q+\Delta q)^2-(p^2+q^2)}\right) \\ &\quad = \tau\left(\sqrt{p^2+q^2+\Delta p^2+\Delta q^2+2\Delta p^* p-2\Delta q^* q}-\sqrt{p^2+q^2}\right) \\ &\quad \le \varepsilon. \end{aligned} \tag{12}$$

Using the Cauchy inequality transformation method, formula (12) can be transformed into

$$\begin{aligned} &\Delta p^2+\Delta q^2+2\Delta p^* p+2\Delta q^* q \\ &\quad \le \Delta p^2+\Delta q^2+\sqrt{\Delta p^{2*}p^2q^2+\Delta q^2p^2q^2} \\ &\quad \le \left(\frac{\varepsilon}{b}\right)^2. \end{aligned} \tag{13}$$

Set the position flow fuzzy estimation stability online control mechanism protection radius to Z, and then, $\sqrt{(\Delta p)^2+(\Delta q)^2} \le Z$, so formula (13) is changed to

$$Z^2+\sqrt{Zp^2+Zq^2} \le \left(\frac{\varepsilon}{b}\right)^2. \tag{14}$$

The above formula is the online control mechanism for the stability of the location flow fuzzy estimation when the location of the user location estimation queue conforms to the $\varepsilon-$ geographic indistinguishability.

When the multitarget location queue is consistent with (ε,δ) geographic indistinguishability [14–16], then

$$\begin{aligned} b &\le \frac{(1/\delta e-1)}{Z}+\sqrt{\frac{\left(1/(\delta e-1)^2\right)+\varepsilon^2}{Z}}, \\ P&\left[\sqrt{x^2+y^2} \ge \frac{\varepsilon^2-Z}{2b^2Z}\right] < \delta. \end{aligned} \tag{15}$$

In the formula, δ denotes the machine accuracy in crowdsensing privacy protection; $P[\cdot]$ denotes the probability function of the user's actual location and ambiguous location.

σ^* is the maximum allowable distance for a given user position distance deviation, which is expressed as

$$\sigma^* = \frac{Z}{(\gamma e - 1)(1/\delta e - 1) + (\gamma e - 1)\sqrt{\left(1/(\delta e - 1)^2\right) + \varepsilon^2}}, \tag{16}$$

where γ denotes the confidence level of the given location fuzzy queue.

In crowdsensing privacy protection process, there will be many identical types of user perception tasks with different locations, so the quantitative relationship between user privacy location and distance aggregation needs to be calculated [17]. Let (φ, η) represent the distance aggregation error, where η represents the confidence level, and φ represents the distance aggregation error, and then, the online control mechanism of the position flow fuzzy estimation stability must meet the following conditions:

$$P[|\tilde{\sigma} - \sigma| \geq \varphi] \leq 1 - \eta. \tag{17}$$

In the formula, $\tilde{\sigma}$ represents the aggregate distance of user location mobility estimation.

When the confidence level η is less than 1, the λ expression formula of the swarm intelligence network sensing task distance error is as follows:

$$\varphi = \frac{\sqrt{\sum_{u=1}^{U} 1/\left[((1/\delta e - 1)/Z) + \left(\left(\sqrt{\left(1/(\delta e - 1)^2\right) + \delta_u^2}\right)/Z\right)\right]^2}}{U\sqrt{1 - \eta}}, \tag{18}$$

where U represents the total number of all types of crowdsensing tasks. It is known from this formula that when the user location privacy protection level is low, then the value of this formula is smaller [18, 19]. When the user mobile location of crowdsensing conflicts with the actual user location, then the user privacy protection level needs to be reduced [20].

2.4. Access Control and Crowdsensing-Based Task Assignment Stability Control Process. Using the result of formula (18) as a reference, the stability control mechanism when the user location meets different geographical indistinguishability can be obtained by using formula (14). Based on this stability control mechanism, the access control and crowdsensing task assignment methods are used to achieve the stability control.

Let $g_i(t)$ and $g_{ij}(t)$ be the access control and task assignment for location mobility fuzzy estimation, respectively, where j denotes the user and i denotes the sensing task type. The objective functions of access control and task assignment are as follows:

$$\begin{aligned} f\left(\mathrm{g}_i(t), \mathrm{g}_{ij}(t)\right) = \max_{\Theta_i(t),\Theta_{ij}(t)} & \zeta \alpha_i(t) \mathrm{g}_i(t) \\ & - \sum_{j \in N} \left\{ \left[\zeta \beta_{ij}(t) d_{ij}(t)\right] g_{ij}(t) \right\} \\ & + \sum_{j \in N} \left\{ \left[Q_{ij}(t)\right] g_{ij}(t) \right\}, \end{aligned} \tag{19}$$

$$g_i(t) = \sum_{j \in N} g_{ij}(t). \tag{20}$$

In the formula, ζ denotes the trade-off factor, $\alpha_i(t)$ and $\beta_{ij}(t)$ denote the stability control coefficient, $Q_{ij}(t)$ denotes the queue length of the sensing task, $d_{ij}(t)$ denotes the distance between user j and sensing task i, and N denotes the number of users in the crowdsensing network.

Set the constraint of Equation (19) as

$$s.t. 0 \leq gi(t) \leq H_i(t), \forall i \in M. \tag{21}$$

In the formula, M denotes the total number of task types; $H_i(t)$ denotes the number of tasks with perceived type i.

For reasons of complexity of the association between $g_i(t)$ and $g_{ij}(t)$ [21–23], assuming that $\Theta_i(t)$ is a known simplified subproblem, formula (19) can be changed to

$$\begin{aligned} f\left(\mathrm{g}_i(t), \mathrm{g}_{ij}(t)\right) = \min & \sum_{j \in N} \left\{ \left[\zeta \beta_{ij}(t) d_{ij}\right] g_{ij}(t) \right\} \\ & + \min \sum_{j \in N} \left\{ \left[Q_{ij}(t)\right] g_{ij}(t) \right\}. \end{aligned} \tag{22}$$

The above formula constraints are as follows:

$$s.t. 0 \leq g_i(t) \leq H_i(t). \tag{23}$$

From Equation (22), it can be seen that the optimal access-controlled crowdsensing task assignment expression is influenced by the number of users and the queue length of the sensing task type and the crowdsensing task weighted distance [24, 25], and therefore, the optimal access-controlled crowdsensing task assignment expression is

$$g_{ij}(t) = \begin{cases} H_i(t), \text{if} j = j_i^*, \\ 0, \text{if otherwise.} \end{cases} \tag{24}$$

In the above equation, j_i^* denotes the task assignment execution algorithm, which is expressed as

$$j_i^* = \arg \min_{j \in N} \left[\zeta \beta_{ij}(t) d_{ij}(t) + Q_{ij}(t)\right]. \tag{25}$$

Substitute formula (25) into (24) and convert formula (19) into

$$f\left(g_i(t), g_{ij}(t)\right) = \max_{gi(t)} g\alpha_i(t)g_i(t) - \zeta\beta_{ij}(t)d_{ij}(t)g_i(t) + Q_{ij}(t)g_i(t). \tag{26}$$

The constraints of the above formula are as in formula (23). According to this formula, the optimal access control expression formula is as follows:

$$g_i(t) = \begin{cases} H_i(t)\zeta\alpha_i(t) > \zeta\beta_{ij}(t)d_{ij}(t) + Q_{ij}(t) \\ 0, \text{otherwise}. \end{cases}, \tag{27}$$

The stability control of location flow fuzzy estimation in crowdsensing privacy protection can be achieved by using formulas ((25)) and ((27)) and based on the online control mechanism for the stability of location flow fuzzy estimation.

3. Experiment Analysis

Using a regional network as the experimental object, we use Python coding tool to obtain the user behavior location information of this network, choose Tianchi open-source dataset (https://tianchi.aliyun.com/dataset/dataDetail?dataId=82714), and then use PyCharm editor to edit the network user behavior location information into math, NumPy, and other format data packets. Based on this packet, we use this paper's method to control the stability of the fuzzy estimation of user location flow in the process of crowdsensing privacy protection in this network.

The completeness of perceived user locations is the basis for achieving stability control of user location fuzzy estimation. The privacy threshold interval of users is set to 0.1-1.0, and the completeness of the method in this paper is tested for the number of perceived user locations of 300 and 600 under this privacy threshold. The results are shown in Figure 2.

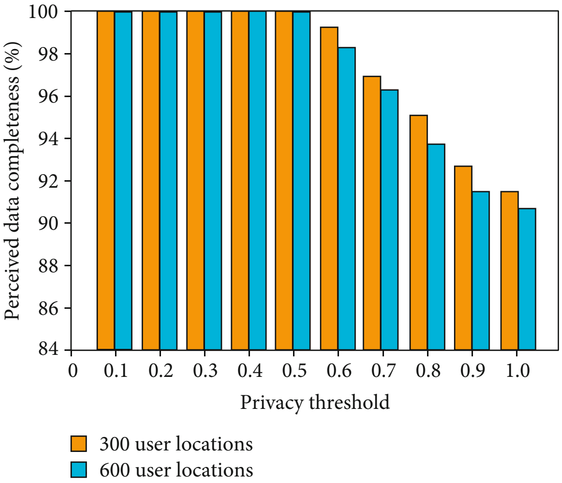

Figure 2: Test results of group intelligence sensing user location completion.

From Figure 2, the lower the threshold of user privacy protection, the higher the integrity value of user location perceived by this method. Before the threshold of user privacy protection is 0.5, the integrity value of user location perceived by this method is 100%, which is not affected by the amount of user location data. After the user privacy protection threshold exceeds 0.5, the perceived user location integrity threshold of this method.

To further verify the ability of the method in this paper to obtain user location data, 20 user location data are used as the experimental object, the user location is obtained using the method in this paper and compared with its actual location for analysis, and the results are shown in Figure 3.

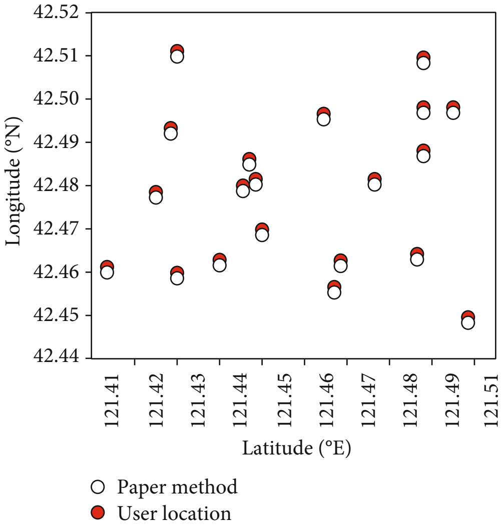

Figure 3: User location data acquisition results.

Analyzing Figure 3, we can see that the longitude and dimensional values of user locations within the crowdsensing network obtained by applying this method match very well with their actual locations, which indicates that this method has a better ability to obtain user location data, and also shows that this method has a better control effect on the fuzzy estimation of user location flow in the privacy protection process of crowdsensing.

A set of network user location latitude data is used as the experimental object to obtain the target location mobility estimation queue using the method in this paper, and the results are shown in Table 1.

Table 1 shows that this paper has conducted 11 comparative analyses from 13 : 02 to 14 : 02 in the afternoon. Among the 11 times of network user location latitude data obtained in this paper, only two results are different from the actual user location latitude, which occurs at 13 : 07 and 13 : 47, but the maximum deviation between the results and the actual user location latitude is only 0.02°N, which is a small value. This shows that the application of this paper can effectively obtain the user network location flow sequence in the

Table 1: Flow estimation queue at target location ($^{\circ}n$).

Time	Actual queue value	Estimated queue value
13 : 02	39.24	39.24
13 : 07	38.56	38.55
13 : 12	37.09	37.09
13 : 17	36.66	36.66
13 : 22	39.11	39.11
13 : 27	39.19	39.19
13 : 32	39.95	39.95
13 : 37	40.13	40.13
13 : 42	40.89	40.89
13 : 47	42.24	42.22
14 : 02	36.65	36.65

crowdsourcing awareness privacy protection process and provides a better data base for the fuzzy estimation control of location flow.

The confidence value of the aggregation distance error is used as a measure of the reasonableness of the online control mechanism of the location flow fuzzy estimation stability set by the method in this paper, the confidence value of the aggregation distance difference is calculated in this paper under different user location flow data volume, and the confidence threshold is set to 0.90. The results are shown in Figure 4.

From Figure 4, it can be seen that the confidence value of the aggregated distance difference of user location mobility data calculated by this method is inversely proportional to the amount of user location mobility data. The confidence value of the aggregated distance difference of user location mobility data shows a slow decreasing trend before 700 sets of user location mobility data. When the user location mobility data exceeds 700 groups, the confidence value of the aggregated distance difference of user location mobility data is balanced and is not affected by the user location mobility data. In the case of different groups of user location mobility data, the confidence values of the aggregated distance difference of user location mobility data calculated by this method are higher than the set threshold, which indicates that the online control mechanism of the stability of location mobility fuzzy estimation set by this method is reasonable and has better control on the stability of location mobility fuzzy estimation.

Using the number of communication rounds of fuzzy estimation of position flow, the stability of fuzzy estimation of position flow controlled by different methods is verified. The results are shown in Figure 5.

It can be seen from Figure 5 that the more location mobility data a user has, the more communication rounds his location mobility fuzzy estimation has. Compared with [6, 7], this method can effectively reduce the number of communication rounds for position mobility estimation of the same user's position mobility data. The maximum difference in the number of communication rounds for location flow fuzzy estimation is about 30, which indicates that the method in this paper can effectively reduce the number of communication rounds for user location flow fuzzy estimation and adjust the control mechanism to make user location flow fuzzy estimation task assignment at each dynamic round. This improves the boundedness and stability of the user location queue, and its application is more effective.

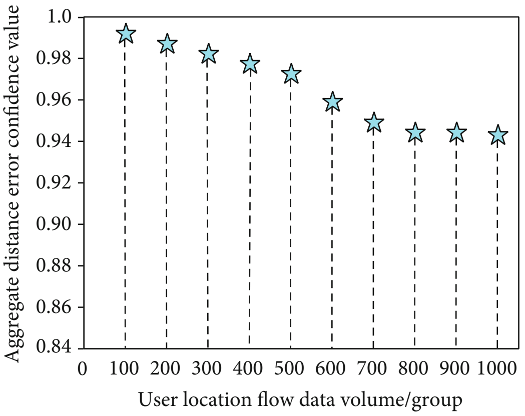

Figure 4: Rationality test results of position flow fuzzy estimation stability online control mechanism.

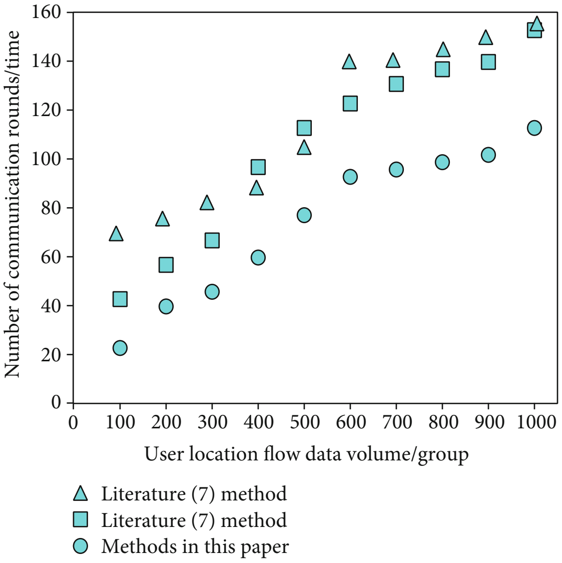

Figure 5: Stability control results of fuzzy estimation of position flow using different methods.

Taking the communication energy consumption in the location flow fuzzy estimation in the public sense privacy protection as an indicator, the stability control effects of different methods on the location flow fuzzy estimation under different user location data are tested, and the results are shown in Figure 6.

It can be seen from Figure 6 that the communication energy consumption in the process of public testing privacy protection is proportional to the user location data. However, under the application of the methods in literature [6] and literature [7], the communication energy consumption in the process of location flow fuzzy estimation is relatively high and fluctuates with the increase of user location data,

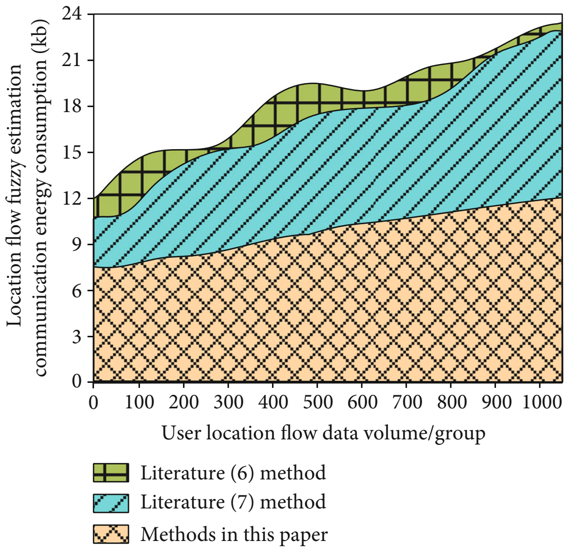

Figure 6: Evaluation of stability control effect of fuzzy estimation of position flow under different control methods.

Table 2: User privacy disclosure probability when different network attackers successfully obtain the proportion of user location data (%).

User location data quantity/piece	Proportion of user location data successfully obtained by network attacker		
	2 : 8	3 : 7	5 : 5
1	5	8	13
2	4	7	12
3	2	5	10
4	0	3	9
5	0	1	6
6	0	0	5
7	0	0	4
8	0	0	3
9	0	0	0
10	0	0	0

indicating that the location flow fuzzy estimation value obtained at this time is not stable. After the application of the method in this paper, the communication energy consumption in the process of fuzzy estimation of location flow is reduced more obviously, and it shows a small and moderate growth trend with the increase of user location data. The results show that the application of this paper reduces the communication energy consumption in the process of location flow fuzzy estimation in the process of public perception privacy protection and can obtain the location flow fuzzy estimation results more quickly and stably.

To verify the application effect of the method in this paper from the perspective of user privacy protection effect, using the user privacy leakage probability as a measure, we test the privacy leakage probability after the application of the method in this paper when the ratio of successful acquisition of user location data by network attackers is 2 : 8, 3 : 7, and 5 : 5, and the results are shown in Table 2.

From Table 2, it can be seen that the higher the ratio of successful acquisition of user location data by network attackers, the higher the probability of user location privacy leakage, and as the user location data gradually increases, the probability of user location privacy leakage gradually decreases for different ratios of successful acquisition of user location data by network attackers. When the proportion of network attackers who successfully obtain user location data is 2 : 8, 3 : 7, and 5 : 5, respectively, and the amount of user location data is 9 and 10, the probability of user location privacy disclosure is 0. This shows that this method can better protect users' location privacy data and reduce the risk of leakage when there are many users in the public test network.

4. Conclusion

In order to better protect the location privacy of network users and improve the stability control effect of location flow fuzzy estimation, this paper introduces the public test privacy protection model into this field, designs a stability control method for location flow fuzzy estimation in public perception privacy protection, and applies this method to the actual location flow fuzzy estimation control process. It is verified that the method has strong user location acquisition capability and user location flow fuzzy queue estimation capability, and the confidence value of the calculated aggregation distance error is accurate. Moreover, the proposed method can effectively realize the stability control of location flow fuzzy estimation in crowdsensing privacy protection, and the application effect is good.

Data Availability

Data is available at https://tianchi.aliyun.com/dataset/dataDetail?dataId=82714.

Disclosure

The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Basic Scientific Research Service Fee Project of Heilongjiang Provincial Undergraduate Universities (2019-KYYWF-1389) and Natural Science Fund of Heilongjiang Province (LH2020F006).

References

[1] C. Tian, H. Xu, T. Lu, R. Jiang, and Y. Kuang, "Semantic and trade-off aware location privacy protection in road networks via improved multi-objective particle swarm optimization," *Access*, vol. 9, pp. 54264–54275, 2021.

[2] R. Alawadhi and T. Hussain, "A method toward privacy protection in context-aware environment," *Procedia Computer Science*, vol. 151, pp. 659–666, 2019.

[3] S. Suzuki, H. Aihara, and K. Takeuchi, "Privacy protection nand flash system with flexible data-lifetime control by in-3-d vertical cell processing," *IEEE Journal of Solid-State Circuits*, vol. 55, no. 10, pp. 2802–2809, 2020.

[4] W. Sun, M. Tang, L. Zhang, Z. Huo, and L. Shu, "A survey of using swarm intelligence algorithms in iot," *Sensors*, vol. 20, no. 5, p. 1420, 2020.

[5] A. N. Shirazi, B. Mozaffari, and S. Soleymani, "Transient stability improvement with neuro-fuzzy control of gupfc in multi machine system," *Journal of Intelligent & Fuzzy Systems*, vol. 37, no. 1, pp. 611–623, 2019.

[6] H. Tian, X. Li, H. Quan, C. C. Chang, and T. Baker, "A lightweight attribute-based access control scheme for intelligent transportation system with full privacy protection," *IEEE Sensors Journal*, vol. 21, 2020.

[7] K. Yu, K. Kashima, and C. Ming, "Modular control under privacy protection: fundamental trade-offs," *Automatica*, vol. 127, no. 4, article 109518, 2021.

[8] A. A. El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, and W. Mazurczyk, "Efficient quantum-based security protocols for information sharing and data protection in 5g networks," *Future Generation Computer Systems*, vol. 100, pp. 893–906, 2019.

[9] W. Wu, H. Zhang, V. Albuquerque, and L. Xu, "Hyper-noise interference privacy protection framework for intelligent medical data-centric networks," *IEEE Network*, vol. 35, 2020.

[10] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain enabled trust-based location privacy protection scheme in vanet," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2034–2048, 2020.

[11] X. Li, B. H. Fireman, J. R. Curtis et al., "Validity of privacy-protecting analytical methods that use only aggregate-level information to conduct multivariable-adjusted analysis in distributed data networks," *American Journal of Epidemiology*, vol. 188, no. 4, pp. 709–723, 2019.

[12] Z. W. Hu and J. Yang, "Trajectory privacy protection based on location semantic perception," *International Journal of Cooperative Information Systems*, vol. 28, no. 3, article 1950006, 2019.

[13] H. Li, L. Pei, D. Liao, M. Zhang, D. Xu, and X. Wang, "Achieving privacy protection for crowdsourcing application in edge-assistant vehicular networking," *Telecommunication Systems*, vol. 75, no. 1, pp. 1–14, 2020.

[14] P. Zhang, M. Durresi, and A. Durresi, "Multi-access edge computing aided mobility for privacy protection in internet of things," *Computing*, vol. 101, no. 7, pp. 729–742, 2019.

[15] C. Qiu, A. C. Squicciarini, C. Pang, N. Wang, and B. Wu, "Location privacy protection in vehicle-based spatial crowdsourcing via geo-indistinguishability," *IEEE Transactions on Mobile Computing*, vol. 21, 2020.

[16] F. Song, T. Ma, Y. Tian, and M. Al-Rodhaan, "A new method of privacy protection: random k-anonymous," *Access*, vol. 7, pp. 75434–75445, 2019.

[17] L. I. Wanjie, X. Zhang, L. I. Xiaohui, G. Cao, and Q. Zhang, "PPDP-PCAO: an efficient high-dimensional data releasing method with differential privacy protection," *IEEE Access*, vol. 7, 2019.

[18] C. Luo, X. Chen, J. Xu, and S. Zhang, "Research on privacy protection of multi source data based on improved gbdt federated ensemble method with different metrics," *Physical Communication*, vol. 49, article 101347, 2021.

[19] L. Du, K. Li, Q. Liu, Z. Wu, and S. Zhang, "Dynamic multi-client searchable symmetric encryption with support for boolean queries," *Information Sciences*, vol. 506, pp. 234–257, 2020.

[20] M. Rodriguez-Garcia, M. Batet, and D. Sánchez, "Utility-preserving privacy protection of nominal data sets via semantic rank swapping," *Information Fusion*, vol. 45, pp. 282–295, 2019.

[21] C. Ju, Q. Gu, G. Wu, and S. Zhang, "Local differential privacy protection of high-dimensional perceptual data by the refined bayes network," *Sensors*, vol. 20, no. 9, p. 2516, 2020.

[22] Q. Wang, J. Zhan, X. Ouyang, and Y. Ren, "Sps and dps: two new grid-based source location privacy protection schemes in wireless sensor networks," *Sensors*, vol. 19, no. 9, p. 2074, 2019.

[23] S. Zhang, X. Li, Z. Tan, T. Peng, and G. Wang, "A caching and spatial k-anonymity driven privacy enhancement scheme in continuous location-based services," *Future Generation Computer Systems*, vol. 94, pp. 40–50, 2019.

[24] A. Chen, G. Lu, H. Xing, Y. Xie, and S. Yuan, "Dynamic and semantic-aware access-control model for privacy preservation in multiple data center environments," *International Journal of Distributed Sensor Networks*, vol. 16, no. 5, 2020.

[25] A. Sultangazin and P. Tabuada, "Symmetries and isomorphisms for privacy in control over the cloud," *IEEE Transactions on Automatic Control*, vol. 66, 2020.