Theory and Practice of Science and Technology
2025, VOL. 6, NO. 1, 64-67
DOI: 10.47297/taposatWSP2633-456913.20250601

Privacy Protection Method Based on Group Collaboration Caching and Virtual Location

Hui Wang, Bianti Wang, Zihao Shen*, Peiqian Liu, Kun Liu

Henan Polytechnic University, Jiaozuo 454000, China

ABSTRACT
Privacy protection in location-based services has been one of the most pressing issues in recent years. When users use LBS technology, their location data may be leaked. To address these issues, this article proposes a LBS privacy protection scheme based on collaborative caching. This scheme ensures service quality while preventing the leakage of user location information through untrusted communication channels and LSPs.

KEYWORDS
Trajectory privacy protection; Virtual location; Collaborative Neighbor Caching

1 Introduction

With the popularization of wireless communication, mobile devices, and positioning technology, location-based services (LBSs) provide abundant resources and diverse services in fields such as entertainment, commerce, healthcare, work, and emergency response. However, in order to enjoy the convenience brought by LBS, mobile users must disclose their actual location and points of interest (POIs) to location-based service providers (LSPs). LSP can find and respond to the required POIs based on the location information of mobile users, but such disclosure may lead to privacy breaches. On the basis of comprehensive consideration of various aspects of existing work, this paper proposes a new location privacy protection scheme GCCV to protect the user privacy of LBS.

2 GCCV scheme

In this section, the working process of GCCV is described. The query user must first generate the modified location through Algorithm 1. In this way, users can use the modified coordinates to send and receive location related information.

2.1 Generate modification location

To protect location privacy from malicious attackers, query the location where the user generated modifications in their vicinity. The process of generating modified locations and requesting queries is shown in Table 1.

Table 1 Modify location and request query area generation

Input:R
Output:$Fr=(fx,fy)$
1:The user intends to query a range with radius R centered on(t_x,t_y)
2:The user selects a security parameterα, where: $\alpha_{min}\leqslant\alpha\leqslant$R.
3:With the user-selected parameterα, Calculate the reach range $R'=R-\alpha$Where:$R\geqslant R'$
4:Construct another virtual circle with (t_x,t_y)as the center and R' as the radius.Then, select any random location F_r in R'.
5:if$\alpha\geqslant R/2$
6:$R''=2R-R/2$
7:else
8:$R''=2R$
9:End if
10:Prepare a query area centered around$F_r$with a radius ofR''
11:End it

The actual location of the user remains hidden from neighbors, eavesdroppers, and untrusted LSPS. Ideally, the modified location should be some distance from the actual location of the user.The longer the distance, the more privacy.

In addition, choosing different modification locations while moving F_r prevents the intelligent adversary from knowing the user's trajectory. Each time the user makes a new request, it selects a different α and changes the location. Figure 1 shows how users are protected when using continuous LBS.

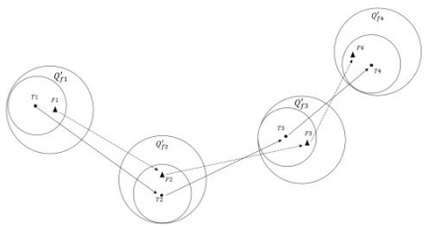

Figure 1 Trajectory privacy protection under continuous requests

2.2 Group cooperation

Each user has a unique group identifier that prevents tracking and identification in the proposed GCCV. This article assumes that there are enough users in a region for group collaboration. In the request phase, the user prepares a collaboration request for nearby neighbors.In Table 2, the process of finding neighbors and obtaining request information is described.

Table 2 Primary group (AGO) formation

Input:$F_r=(f_x,f_y),R^{''}$
Output: Query location information(P_x,P_Y)
1:A query user broadcasts their request to N neighbors.
2:for$i \leftarrow$ 1toNdo
3:$D_i=\sqrt{(N_{x_i}-d_x)^2+(N_{y_i}-d_y)^2}$
4:if$D_i \leqslant R^{''}$:
5:$D_{N_i} \leftarrow$Cooperative neighbor
6:endif
7:endfor
8:$\gamma=\frac{2\pi}{n}$ Where: n is the number of points selected on the circle.
9:The user evenly splits the query radius with γg and sends it to selected collaborating neighbors.
10:Agent$\leftarrow$ min(D_i)
11:Return Query location information(P_x,P_Y)
12:Finish

After the partners receive the request from their respective agents, they check the requested information in their respective caches. If the information is available, they respond to their respective agents in the format {POLName, longitude, latitude}. The agent then matches the multiple cached information results received by the cooperating neighbor and prepares a response list containing POLs information for thequery user.

2.3 Virtual location generation algorithm

In the proposed GCCV scheme, an untrusted LSP is associated when the requested information is not available in the neighbor's cache.The user generates $k-1$virtual location build service queries based on the dummy location generation algorithm and sends them to the agent.

The LBS server divides the request query area into I×J cells.$cell_{i,j}$ Representing cells in row i and column j, i= 1,2,..., I, j= 1, 2,..., J.$cell_{i,j}$ The position can be expressed as$r_{i,j}$where$r_{i,j}=(x_{i,j},y_{i,j})$, Be at $cell_{i,j}$ Inside a randomly selected location.$cell_{i,j}$The service request probability is$q_{i,j}$, service u in$cell_{i,j}$ The service semantics is $e_{(i,j),u}$.Service request probability$q_{i,j}$Indicates that the user initiates the request in the request area $cell_{i,j}$ The probability of the request.$e_{(i,j),u}$ Indicates that the user$cell_{i,j}$ The probability of initiating service type u among all requested service types. The vehicle user uses the dummy position selection algorithm to generate the dummy position.

$$H=-\sum_{i=0}^{k-1} p_{i,u}\log_2 p_{i,u} \tag{1}$$

where：

$$p_{i,u}=\frac{q_i e_{i,u}}{\sum_{i=0}^{k-1} q_i e_{i,u}} \tag{2}$$

Upon receipt, the LBS server retrieves the database and returns the service result to the agent.By collaborating with the query user, the agent also anonymously obtains POIs information from the LSP.

3 Experiment and analysis

In this section, the performance of GCCV is analyzed from the perspective of safety and effectiveness.In addition, the performance of this method is compared with some existing methods based on cache or virtual location.

All experiments were run on an Intel-Core I 53.4ghz machine with 8GB of memory.

3.1 Location-related attacks

The theoretical premise of LCA as shown in Figure 2 is that there is a spatiotemporal correlation between locations, and each anonymous region or location set should contain the actual location of a vehicle user.

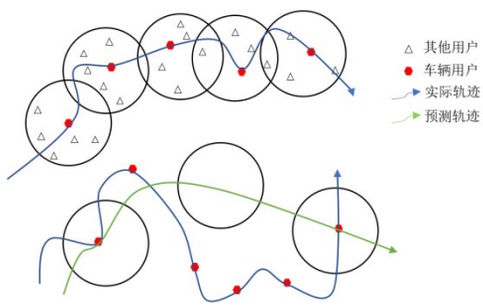

Figure 2 Resistance to location-related attacks (LCA)

In GCCV, since the virtual location set sent to the LBS server may not contain the actual location of the vehicle user, the spatiotemporal correlation of the location information received by the LBS server is guaranteed. So it's hard to get trajectories.

3.2 Impact of query radius

Figure 3 shows the impact of computation time and communication overhead at different query radii.For this case, this article considers POIs=2000, Subgroupsize=2, NeighborsN=200, and variation R. The calculation time of DPP scheme and UGC scheme is higher than that of GCCV scheme.This is mainly due to the addition of shaded areas depending on the actual location of the user.The higher the hiding area, the more time it takes to search for POIs information.

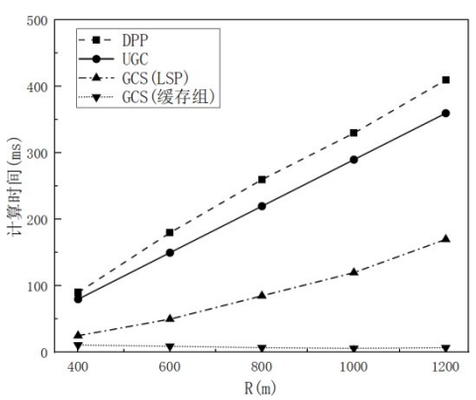

Figure 3(a) Computation time and communication cost with query radius

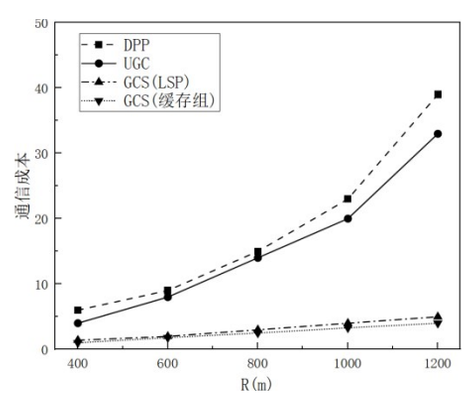

Figure 3(b) Comparison of communication cost under different query radius

4 Finish

In this study, a new GCCV scheme is proposed, which can not only guarantee the quality of [14] certificate query service, but also effectively protect the location privacy of users to avoid malicious attacks by LSPS.In this paper, caching technology and virtual location generation strategy are used to achieve this goal. The simulation results show that compared with other location privacy protection schemes, the proposed GCCV scheme has a good effect in terms of security and utility.In the future, this paper plans to further expand the proposed group collaboration scheme, using the smallest communication cost to protect the user's location privacy in a differential privacy way. At the same time, this paper also plans to incorporate users' content and trajectory privacy into continuous LBS applications to further improve the level of user privacy protection.

About the Author

*Corresponding Author: Zihao Shen.

References

[1] JIANG H, LI J, ZHAO P, et al. Location Privacy-preserving Mechanisms in Location-based Services: A Comprehensive Survey[J/OL]. Acm Computing Surveys, 2021, 54(1): 4.

[2] QIU S, PI D, WANG Y, et al. Novel trajectory privacy protection method against prediction attacks[J/OL]. Expert Systems with Applications, 2023, 213: 118870.

[3] ALMARSHOUD M S, AL-BAYATTI A H, KIRAZ M S. Location privacy in VANETs: Provably secure anonymous key exchange protocol based on self-blindable signatures[J/OL]. Vehicular Communications, 2022, 36: 100490.

[4] NISHA N, NATGUNANATHAN I, XIANG Y. An Enhanced Location Scattering Based Privacy Protection Scheme[J/OL]. IEEE Access, 2022, 10: 21250-21263.

[5] LI T, HE X, JIANG S, et al. A survey of privacy-preserving offloading methods in mobile-edge computing[J/OL]. Journal of Network and Computer Applications, 2022, 203: 103395.

[6] MONTORI F, GIGLI L, SCIULLO L, et al. LA-MQTT: Location-aware Publish-subscribe Communications for the Internet of Things[J/OL]. ACM Transactions on Internet of Things, 2022, 3(3): 20:1-20:28.

[7] XU Y, XIAO M, LIU A, et al. Edge Resource Prediction and Auction for Distributed Spatial Crowdsourcing With Differential Privacy[J/OL]. IEEE Internet of Things Journal, 2022, 9(17): 15554-15569.

[8] RAZAQ M M, RAHIM S, TAK B, et al. Fragmented Task Scheduling for Load-Balanced Fog Computing Based on Q-Learning[J/OL]. Wireless Communications and Mobile Computing, 2022, 2022: e4218696.

[9] NISHA N, NATGUNANATHAN I, XIANG Y. An Enhanced Location Scattering Based Privacy Protection Scheme[J/OL]. IEEE Access, 2022, 10: 21250-21263.

[10] LIU S, WANG J H, WANG J, et al. Achieving User-Defined Location Privacy Preservation Using a P2P System[J/OL]. IEEE Access, 2020, 8: 45895-45912.

[11] NIU B, LI Q, ZHU X, et al. Achieving k-anonymity in privacy-aware location-based services[C/OL]//IEEE INFOCOM 2014 - IEEE Conference on Computer Communications. 2014: 754-762.

[12] ZHANG S, WANG G, BHUIYAN M Z A, et al. A Dual Privacy Preserving Scheme in Continuous Location-Based Services[J/OL]. IEEE Internet of Things Journal, 2018, 5(5): 4191-4200.

[13] Enhancing privacy through uniform grid and caching in location-based services[J/OL]. Future Generation Computer Systems, 2018, 86: 881-892.

[14] NISHA N, NATGUNANATHAN I, GAO S, et al. A novel privacy protection scheme for location-based services using collaborative caching[J/OL]. Computer Networks, 2022, 213: 109107.

[15] HUANG Q, XU X, CHEN H, et al. A Vehicle Trajectory Privacy Preservation Method Based on Caching and Dummy Locations in the Internet of Vehicles[J/OL]. Sensors, 2022, 22(12): 4423.