Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **6**, Number **4**, November **2021**

Protecting Location Privacy in Location-based Services with Small Cell Base Stations in Next Generation Cellular Networks

Pei-Qian Liu, Shang-Chen Xie, Zi-Hao Shen, Kun Liu, Hui Wang*

College of Computer Science and Technology
Henan Polytechnic University
Jiaozuo 454000, China
liupeiqian@hpu.edu.cn, xcartoon@126.com, szh@hpu.edu.cn, z3460821471@163.com
*Corresponding Author: wanghui_jsj@hpu.edu.cn

Received August 2021; revised October 2021

Abstract. *Examples of mobile terminals using location-based services are everywhere in daily life, but with that comes the concern about location privacy and fears that sensitive information included falls into lawbreakers. Most existing schemes use GPS technology to access location information first, and then perform operations such as differential privacy on it to protect location privacy. Different from them, we propose a scheme that does not execute any operation on the location information and mobile terminals do not know their location information until the final stage, thus avoiding the risk of location information being leaked during the operation. Owing to the characteristics of abundant small cell base stations in next generation cellular networks, mobile terminals can utilize them to forward requests and get location information. In addition, a method for regional recommendation services is proposed to overcome the drawback of popular contents that are being discontinued due to the over-processing of location information. The simulation results and analysis show that the proposed scheme is feasible and can effectively protect the location privacy of mobile terminals.*
Keywords: Location-based service, Mobile terminal location, Location privacy protection, Regional recommendation service, Next generation cellular network

1. **Introduction.** Along with the rapid evolvement of mobile communication technology, the deployment density of small cell base stations will reach an unprecedented level. The next generation cellular networks have the advantages of ultra-low latency and ultra-high speed, which could further enhance the network experience of mobile terminals and promote the tremendous development of mobile internet. A case in point is the location-based services, which the common system architecture is shown in Figure 1. Mobile terminals can simply send requests with their location information to the location-based service servers to access the candidate results, for instance, COVID-19 patient exposure notification [1]. By correlating the location information of an infected person with the trajectory data of others, it is possible to determine who is a close contact.

However, there is concern about location privacy, because the location information implies some relevant sensitive details, such as the places where are frequently visited. When an attacker intercepts it, the damages caused are likely to outweigh the benefits gained. Therefore, how to protect the location privacy of mobile terminals has attracted considerable attention in academia, and many solutions have been proposed. Generally

speaking, location privacy protection in location-based services is achieved through three types of structures: centralized, distributed, and hybrid [2].

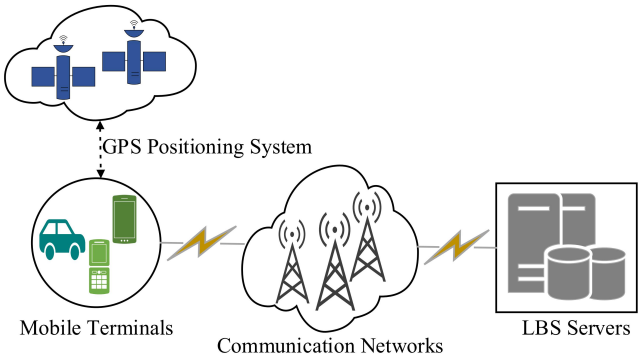

FIGURE 1. The common system architecture

For some of the existing schemes, there are a few drawbacks. (1) It is no guarantee that location information is not attacked internally during the operation of using technologies such as location generalization or K-anonymization for the real location of mobile terminals. In other words, the location information is not protected in the process. (2) Almost all requests need the participation of mobile communication networks, but they ignore the fact that mobile communication networks have the same strength of received signal, which makes the requests delivering among several small cell base stations and could indirectly leak the location information from the clustering perspective [3]. (3) Many location-based service providers are placing their service data on cloud servers like AWS, Azure. Moreover, they use techniques such as attribute-based encryption to protect data. Consequently, it leads many providers to discontinue location-related recommendation services.

To address the above shortcomings, we propose a scheme that relies on mutually curious but trustworthy small cell base stations in next generation cellular networks, which have basic equipment such as computing power, storage capacity and self-powered. The almost equal strength of the transmission signal is not considered as a drawback, with the help of Mitola radio, allowing seamless integration between communication networks and mobile terminals. Mobile terminals can utilize small cell base stations to obtain their location information while performing communication transmissions, thus eliminating the existence of the GPS positioning system. Because the more components involved in location information, the greater the risk of location privacy leakage. Seamless integration implements the ability to send requests to specified small cell base stations, so that mobile terminals can specify which small cell base stations are allowed to execute the forwarding of requests. Furthermore, the development of mobile edge caching and delivery technologies allow for the decentralization of data from remote content providers and reduce the number of interactions with location-based service servers.

Compared with the existing work, the main contributions of this paper are presented as follows:

- The proposed scheme removes the GPS positioning system in the common architecture, gives the mathematical derivation of how to use small cell base stations to obtain mobile terminal location, and proves that the derivation involving homomorphic encryption is also workable in next generation cellular networks.
- In proposed scheme, the location information in requests received by location-based service servers is the location of small cell base stations, not mobile terminals. Such an operation not only skips the step of K-anonymization or generalization of the exact location of mobile terminals, which may lead to the leakage of location information,

but also makes no middleware know the mobile terminal location information, including mobile terminals themselves, during communications. And, with the help of caching and multi-hop, it not only reduces the communication frequency with the location-based service servers, but extends the distance between mobile terminals and the clustering center of small cell base stations.
- We propose a idea that the request time of mobile terminals are recorded and candidate results are cached in small cell base stations, making a regionalized recommendation service algorithm to be presented.
- Simulation experiments under different parameter settings have been organized to evaluate the performance of the proposed scheme. The experimental results show that it costs less computation when getting the mobile terminal location compared to the scheme of Jiang et al. and it performs better than the scheme of Wang et al. and Wei et al. in terms of preventing location information leakage.

The remainder of the paper is organized as follows. In Section 2, we describe the related work. The relevant background knowledge and system framework are presented in Section 3. The proposed scheme and performance evaluation are given in Section 4 and Section 5, respectively. In Section 6, we draw conclusions.

2. **Related work.**

Many state-of-the-art location privacy protection schemes have been proposed by research scholars in location-based services. In this section, we briefly review some works related to our scheme.

From the standpoint of location security, encryption technologies are often applied to protect location information. Based on dynamic searchable encryption, Chen et al. presented an improvement to the VDERS scheme [4]. Only Liu et al. proposed a contact tracking scheme for COVID-19 using zero-knowledge protocol [5]. It not only ensures that all information remain trustworthy but also makes it impossible for government to know the identities and locations of contacts. Using secure multi-party computing, a privacy-preserving scheme for indoor signal strength localization was described by Nieminen and Jarvinen [6]. Jiang et al. presented a solution based on Paillier encryption knowing the location of sensors [7]. And Zeng et al. followed the work of ring signature and constructed a valid deniable authentication to solve the problem of protecting location privacy when devices are connected in edge computing [8].

Mobile terminals could be hidden in cloaked region, making the attacker incapable to accurately locate them. CRAC used heuristic search to find the best cloaked region [9]. In the mix-zone framework, mobile terminals can exchange pseudonyms with each other, avoiding the computation cost which requires extensive encryption [10]. Palanisamy and Liu improved the ability of this framework to resist transition attacks [11]. Meanwhile, K-anonymity is a common privacy-preserving method, using other k-1 positions to assist in cooperation [12]. Natesan and Liu proposed an adaptive learning model for K-anonymity [13]. To meet the geo-indistinguishable need, differential privacy technology is often used [14]. Based on Moore curve, Lian et al. proposed a scheme to find k-nearest neighbor to hide the location on outsourced data [15]. Zhang et al. proposed UGC scheme adopting the caching mechanism, which reduces the number of exposures of location information to LBS servers and minimizes overhead at the same time [16].

3. **Preliminary and system overview.**

This section firstly infers how to get the mobile terminal location through trilateration localization, and then presents the overall system architecture. Finally, the involved components are described in detail.

3.1. **Trilateration localization.** Trilateration localization, a universal location algorithm, could acquire the location information of mobile terminals. Assuming that three anchor points I, J, K are known, and their geographical coordinates are (x_i, y_i), (x_j, y_j), (x_k, y_k) respectively. The distance between the mobile terminal and the anchor point could be measured by communication technology such as time of arrival and DBP [17], supposing that the distances are d_i, d_j, d_k.

According to the Pythagorean theorem, we have Eq.(1).

$$\begin{aligned}(x_i - x)^2 + (y_i - y)^2 &= d_i^2 \\ (x_j - x)^2 + (y_j - y)^2 &= d_j^2 \\ (x_k - x)^2 + (y_k - y)^2 &= d_k^2\end{aligned} \tag{1}$$

Based on Eq.(1), we get the following Eq.(2) and Eq.(3).

$$\begin{aligned}2(x_i - x_k)x + 2(y_i - y_k)y &= d_k^2 - (x_k^2 + y_k^2) - [d_i^2 - (x_i^2 + y_i^2)] \\ 2(x_j - x_k)x + 2(y_j - y_k)y &= d_k^2 - (x_k^2 + y_k^2) - [d_j^2 - (x_j^2 + y_j^2)]\end{aligned} \tag{2}$$

$$\begin{pmatrix}2(x_i - x_k) & 2(y_i - y_k) \\ 2(x_j - x_k) & 2(y_j - y_k)\end{pmatrix}\begin{pmatrix}x \\ y\end{pmatrix} = \begin{pmatrix}d_k^2 - (x_k^2 + y_k^2) - [d_i^2 - (x_i^2 + y_i^2)] \\ d_k^2 - (x_k^2 + y_k^2) - [d_j^2 - (x_j^2 + y_j^2)]\end{pmatrix} \tag{3}$$

Perform the substitution of Eq.(4).

$$\begin{aligned}A &= \begin{pmatrix}x \\ y\end{pmatrix} \\ B &= \begin{pmatrix}2(x_i - x_k) & 2(y_i - y_k) \\ 2(x_j - x_k) & 2(y_j - y_k)\end{pmatrix}^{-1} = \begin{pmatrix}b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2}\end{pmatrix} \\ C &= \begin{pmatrix}l_k - l_i \\ l_k - l_j\end{pmatrix}\end{aligned} \tag{4}$$

Thus, the coordinates of the unknown point are shown in Eq.(5).

$$\begin{pmatrix}x \\ y\end{pmatrix} = A = BC = \begin{pmatrix}b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2}\end{pmatrix}\begin{pmatrix}l_k - l_i \\ l_k - l_j\end{pmatrix} \tag{5}$$

3.2. **Design of system.** The design of system is illustrated in Figure 2, which mainly consists of three parts: mobile terminals, small cell base stations and location-based service servers.

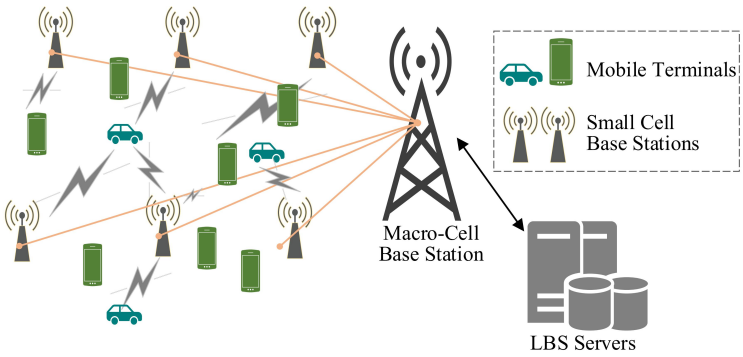

FIGURE 2. The system architecture

Mobile terminal: The mobile terminal request is composed of four segments, the selected small cell base stations, the threshold, the number of hops, and the query content. And, it has the capability to know which small cell base stations are nearby. Based on a strategy, it will select some of them to assist in completing the request. The request that exceeds

the threshold is forwarded to a small cell base station outside a certain number of hops. The query content is the service which it wants to enjoy.

Small cell base station: Due to the achievement of larger communication bandwidth and shorter communication latency in the next generation cellular networks, the deployment density of small cell base stations will be notably dense. Besides inherent equipment, the small cell base station provides a cache area, a table regarding mobile terminal requests and a table concerning adjoining small cell base stations. Candidate results are stored in the cache area. Request table is used to record the received requests and its basic fields are the content of the query, the timestamp, and the number of requests. Neighborhood table has relevant information of neighboring small cell base stations, so that requests could be forwarded to other small cell base stations as soon as possible.

Location-based service server: Most location-based service providers host their service data with existing mature cloud servers, thereby reducing overhead. Mobile terminals send requests to servers which match the corresponding results in relevant databases and return.

4. Proposed scheme.

In this section, we describe the implementation process of the proposed scheme, detail about how to deduce mobile terminal location by using small cell base stations, and then clarify the course of conducting regional recommendation services.

4.1. The process of location privacy protection.

Figure 3 shows the rough architecture diagram of the proposed scheme, which we describe in five steps.

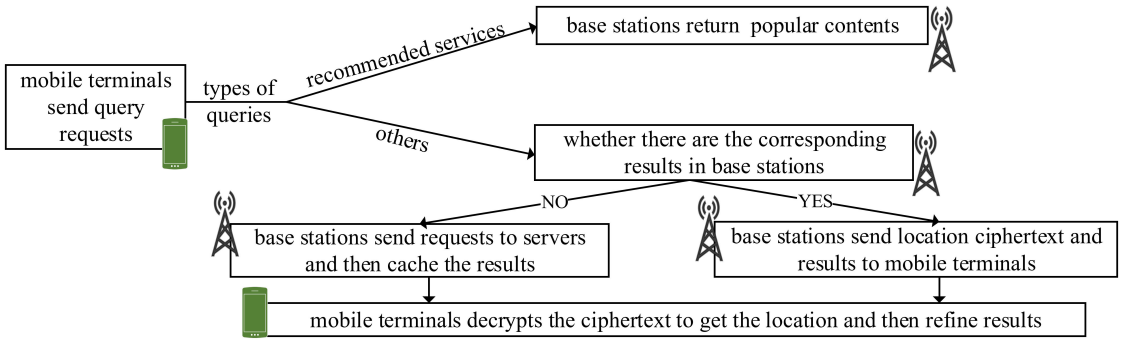

FIGURE 3. The scheme architecture diagram

Step1: Based on the desired type of services, the mobile terminal generates request that does not involve its location information in the corresponding query format and then sends it to small cell base stations selected depending on a selection strategy. That is to say, in the midst of querying, the GPS positioning system in the common architecture is not needed, because the mobile terminal does not need to know its own location at this stage, so that the location can be protected.

Step2: When one selected small cell base station notices that the number of small cell base stations receiving this request exceeds given threshold set in query, it will forward this request to those unselected which are a few hops away from the selected with the help of adjoining small cell base station table and does not record the request in its request table.

Step3: The small cell base station which satisfies both the selected and given threshold conditions will send a notification that it has received successfully to the mobile terminal. The following operation is that it retrieves databases to pinpoint whether there are candidate results or not. This operation not only minimizes the threat of location information exposure by reducing the number of communications with the LBS servers, but also lowers latency. If not find, it will use its own location, namely, the location of small

cell base stations, as the location information for the query and forward the request to location-based service servers. Afterwards, storing the returned results.

Step4: The mobile terminal summarizes the coordinates of those small cell base stations which send a notification, calculates them, and then sends the calculated value to the reciprocal small cell base station. Next, the small cell base station returns the result calculated by multiplying the received value with the value obtained by its own calculation and the candidate results of the query to the mobile terminal. By calculating the forwarded result, the mobile terminal gets its position. The detail of this process is illustrated in Section 4.2.

Step5: The mobile terminal refines the candidate results in accordance with its location to get the desired service. If the request is about regional recommendation services, then the recommended contents are forwarded. The detail of regional recommendation services is presented in Section 4.3.

4.2. **The detail of deducing location.** Hybrid multiplicative homomorphism is one of the homomorphic encryption algorithms, namely, there is an effective algorithm making $xy = D(E(x)y)$ [18].

In practice, we prefer to utilize multilateral localization technique instead of utilizing trilateral localization technique in that the conditions of trilateral localization are difficult to satisfy. Referring to Section 3.1, we get Eq.(6).

$$C = \begin{pmatrix} 2(x_1 - x_n) & 2(y_1 - y_n) \\ 2(x_2 - x_n) & 2(y_2 - y_n) \\ \vdots & \vdots \\ 2(x_{n-1} - x_n) & 2(x_{n-1} - x_n) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} l_n - l_1 \\ l_n - l_2 \\ \vdots \\ l_n - l_n \end{pmatrix} \tag{6}$$

Let:

$$B_1 = \begin{pmatrix} 2(x_1 - x_n) & 2(y_1 - y_n) \\ 2(x_2 - x_n) & 2(y_2 - y_n) \\ \vdots & \vdots \\ 2(x_{n-1} - x_n) & 2(x_{n-1} - x_n) \end{pmatrix} \tag{7}$$

Get:

$$B = \left(B_1^T B_1\right)^{-1} B_1^T = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1n-1} \\ b_{2,1} & b_{2,2} & \cdots & b_{2n-1} \end{pmatrix} \tag{8}$$

$$\begin{aligned} \begin{pmatrix} x \\ y \end{pmatrix} = A = BC &= \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n-1} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n-1} \end{pmatrix} \begin{pmatrix} l_n - l_1 \\ l_n - l_2 \\ \vdots \\ l_n - l_n \end{pmatrix} \\ &= \begin{pmatrix} -b_{1,1}l_1 - b_{1,2}l_2 - \cdots - b_{1,n-1}l_{n-1} + (b_{1,1} + b_{1,2} + \cdots + b_{1,n-1})l_n \\ -b_{2,1}l_1 - b_{2,2}l_2 - \cdots - b_{2,n-1}l_{n-1} + (b_{2,1} + b_{2,2} + \cdots + b_{2,n-1})l_n \end{pmatrix} \end{aligned} \tag{9}$$

All participating small cell base stations encrypt the difference between the distance of the unknown point d_i^2 and coordinates $(x_i^2 + y_i^2)$, namely $l_i = d_i^2 - (x_i^2 + y_i^2)$, and obtain $E(l_i)$. For the first $n-1$ base stations, the mobile terminal sends the respective values and gets the results. For instance, the i^{th} base station sends $-b_{1,i}$,$-b_{2,i}$ and calculates $-b_{1,i}E(l_i)$,$-b_{2,i}E(l_i)$. For the last base station, the summations, $b_{1,1} + b_{1,2} + \cdots + b_{1,n-1}$ and $b_{2,1} + b_{2,2} + \cdots + b_{2,n-1}$ are sent. The mobile terminal decrypts the returned values, sums them, and retrieves its location information.

4.3. **The detail of regional recommendation services.** The regional recommendation services rely on the request table. For the number of requests, it has the independent threshold serving as the standard of the popularity of the regional recommended contents. Request table updates dynamically and periodically removes items which timestamp exceeds the time interval and the number of times is less than the threshold. For item which timestamp exceeds the time interval but the number of times is greater than the threshold, the timestamp is updated to the latest and the number of times is set to zero. Request table is ordered by the number of times, and the regional recommended contents are the results of dissimilar popular requests [19]. The similarity of request R_i and R_j is judged based on Euclidean distance.

$$D_{ij} = \sqrt{w_1(R_1^i - R_1^j)^2 + w_2(R_2^i - R_2^j)^2 + \cdots + w_n(R_n^i - R_n^j)^2} \tag{10}$$

Following the uniform word embedding rule, each request is transformed into a vector of length n, namely $R = R_1, R_2, ..., R_n$. In addition, w_n is the weight of the n^{th} component.

5. **Performance evaluation.** In this section, we evaluate parameters related to the service quality of mobile terminals, discuss why the proposed scheme can protect location privacy, and present comparison results with other existing algorithms in the systematic real-world dataset which follows Zipf distribution as well as $\lambda = 1.05$. The experiments are based on Microsoft Windows 10 operating system with AMD Ryzen 5 CPU and 16GB RAM, implemented in PyCharm IDE with Python. The results are the average of extensive experiments.

5.1. **Impact of parameter variation for performance.** For regional recommendation services, the setting of time interval and the number of threshold in the request table within the small cell base stations have impacts on computation cost for unrelated requests, communication cost of transmitting results, and the coverage ratio of popular contents.

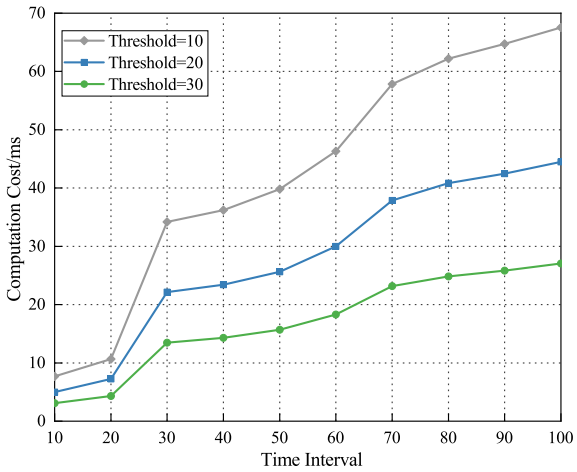

FIGURE 4. The effect on the computation cost

Figure 4 shows the effect on the computation cost. The longer time interval means that the more requests are processed. As a result of that, computation cost is greater. Taking $Threshold = 10$ as an example, it can be seen that the effect of increasing the time interval is more computation cost. In the same time interval, as the threshold increases, the number of requests involved in the calculation decreases, thus reducing computation cost. When the time interval is 20, we know that among the three cases with threshold of 10, 20, and 30, the computation cost is the largest for $Threshold = 10$ and the smallest for $Threshold = 30$.

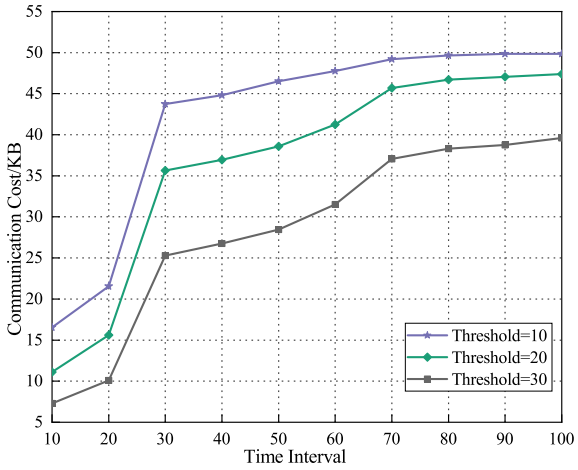

FIGURE 5. The effect on the communication cost

Figure 5 shows the effect on the communication cost. Due to the semantic similarity, there is case where different request contents correspond to the same type of services. What are delivered to mobile terminals is the results of distinct kinds of queries, so it is different between the computation cost in Figure 4 and the communication cost in Figure 5. We can see that communication cost will increase as the time interval increases or threshold value decreases.

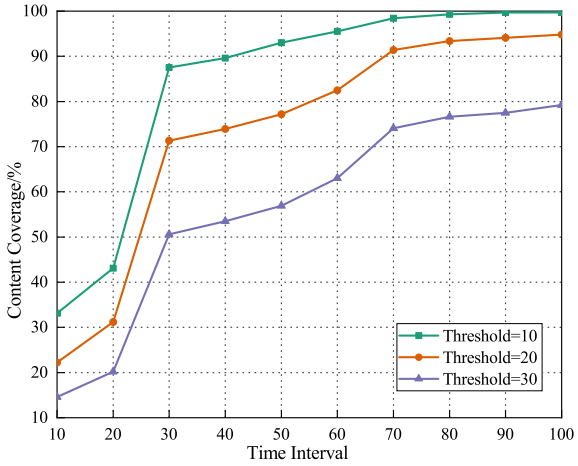

FIGURE 6. The effect on the coverage ratio of popular contents

Figure 6 shows the effect on the content coverage. Long time interval and small threshold indicate that there are more types of available services. Hence, it could result in high content coverage. Under the condition of a given threshold, it can be found that content coverage is only tiny increasing as the time interval becomes longer. In particular, when threshold is 10 and time interval is 80, content coverage is almost close to one hundred percent.

To some extent, the threshold in requests sent by mobile terminals to small cell base stations have already determined the quality of the returned results. As shown in Figure 7, when threshold is one, e.g. only with the help of one small cell base station, the service quality is very poor. Because the location information in this request is from the small cell base station rather than the mobile terminal, thereby their geographic coverage areas only partially overlap, only part of the returned contents is available. Figure 7 also illustrate that the service quality can make great improvement with the increasing of threshold. Although extremely excellent result cannot be achieved ultimately, it is still quite well.

5.2. **Privacy protection analysis.** From mobile terminals' perspective, they does not know their location information until refining the candidate results. As a result, the location information is unknown to mobile terminals and others during the querying operation,

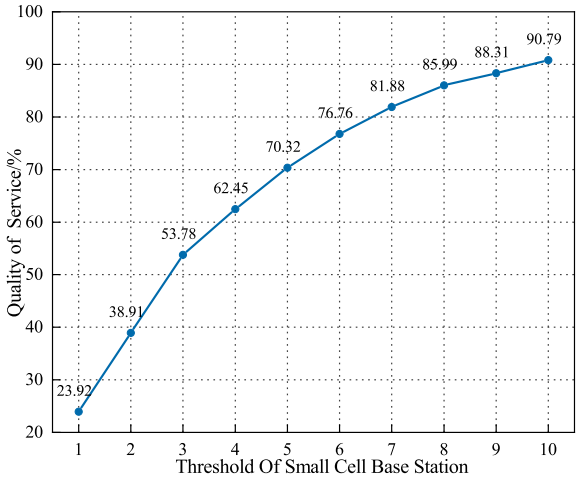

FIGURE 7. The effect on threshold of quality of service

so it is impossible to talk about that the location information will be compromised. Jiang et al. also proposed a similar method to get the locations [7]. But it does not embody the protection of location information, uses Paillier Encryption Scheme, and introduces an attendant edge server.

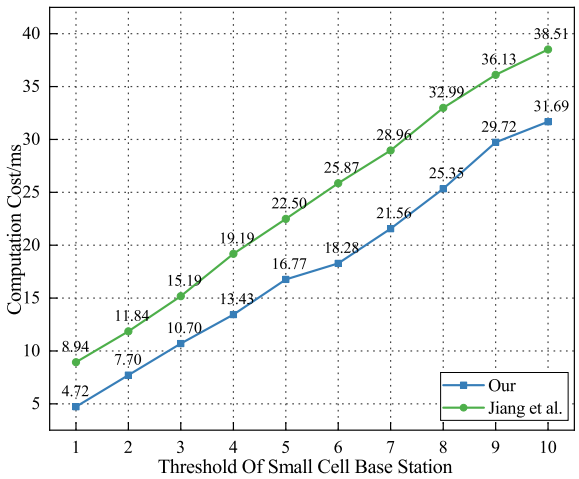

FIGURE 8. Scheme comparison with Jiang et al.'s [7]

It can be known from Figure 8 that the proposed scheme outperforms Jiang et al.'s scheme in terms of the significant computation cost metric when acquiring the location. The main reason is that all transmission contents of Jiang et al.'s scheme are in the form of ciphertext, but only the distance and the final return results of the proposed scheme are in the form of ciphertext. In addition, the introduction of the edge server brings two interactions which are high computation cost.

For small cell base stations, they are honest-but-curious. Supposed that they violate the law of national security and mutually collude, it is also difficult for them to purloin exact location information. Because the critical component difference l_i is encrypted, it is unrealistic to successfully break the homomorphic encryption at short notice.

Mobile terminal can use small cell base stations to get their location, but it is not equivalent to be able to utilize the same requests sent by different small cell base stations to accurately identify the location of mobile terminals in location-based service servers. Additionally, in next generation cellular networks, even under the condition where the location-based service servers are untrustworthy or illegal elements launch an attack against them, the proposed scheme also could protect location privacy by making the clustering center of small cell base stations forwarding the same request away from mobile terminals by the aid of caching and multi-hop.

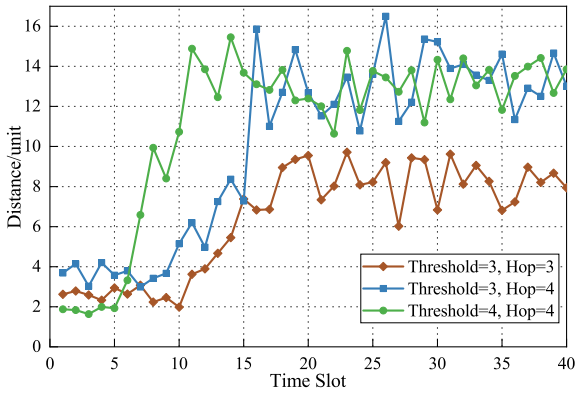

FIGURE 9. Evaluation of distance of different parameters

Figure 9 shows the effect of the threshold and the number of hops on the distance from the clustering center to mobile terminals when the number of selected small cell base stations is 5. At the beginning, the selected small cell base stations will forward the request to the location-based service servers in that the corresponding contents are not cached, resulting in a relatively close distance. However, after a period of time, small cell base stations sending requests are selected by hops, so the distance will become farther, and the larger the hops, the farther the distance will be. As a consequence, the attacker even will analyze to a completely deviated location.

TABLE 1. Performance evaluation of distance of different schemes

Time Slot	Our	Wang et al. [20]	Wei et al. [21]
1	3.268	2.705	0.447
2	3.457	3.446	0.404
3	3.372	2.473	0.761
4	3.539	3.945	0.659
5	4.790	1.593	0.350
6	3.344	2.728	0.502
7	3.974	3.039	0.632
8	3.008	3.545	0.858
9	5.177	1.640	0.551
10	3.298	3.969	0.657
11	3.939	3.774	0.460
12	8.413	2.142	0.847
13	9.965	4.265	0.509
14	10.303	2.771	0.578
15	9.915	2.563	0.490
16	6.540	2.881	0.579
17	10.695	1.200	0.793
18	11.348	2.981	0.604
19	10.685	3.366	0.586
20	12.351	2.148	0.896
21	12.782	2.691	0.907
22	13.221	2.835	0.547
23	13.700	2.188	0.959
24	15.320	3.380	0.505

In the following part, Wang et al.'s scheme and Wei et al.'s scheme are adopted as the comparison, and the strategy of the proposed scheme is that the threshold is set to 3 and the number of hops is set to 4 [20, 21]. Different from the proposed scheme that does

not involve any location information of mobile terminals in the request, both comparison schemes contain the real location. The former takes into account the fact that the signal will switch repeatedly between various small cell base stations and proposes a scheme to find the best small cell base station so that location privacy can be protected. The latter does not take the fact into account but present a scheme to do it from the caching perspective.

Table 1 shows the distance from the clustering center to mobile terminals, we can know from it that proposed scheme is the farthest, and the scheme of Wei et al. which does not take into account the drawback of signal strength is the closest, and the scheme of Wang et al. is in the middle of them. The main novelty that causes this result is the multi-hop mechanism in proposed scheme.

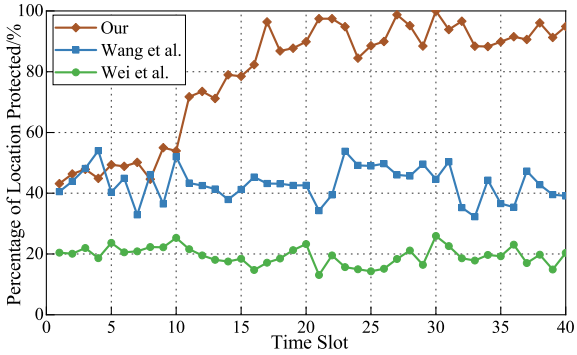

FIGURE 10. Performance comparison of the protected percentage

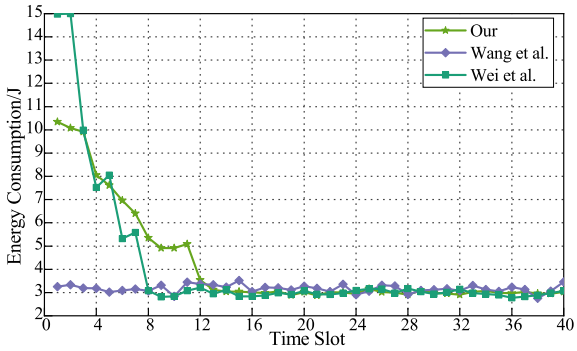

FIGURE 11. Performance comparison of energy consumption

From the perspective of sending the same request to servers for services, Figure 10 shows the extent to which different schemes protect the location privacy of mobile terminals, and Figure 11 reveals the different energy consumption.

Because Wei et al.'s scheme ignores the fact that the signal will switch repeatedly between different small cell base stations in next generation cellular networks, its location privacy protection is the worst. At the same time, a large number of caching operations will be performed in the initial stage, requiring a large amount of energy consumptions. Initially, the location privacy protection level of proposed scheme and Wang et al.'s scheme are similar, but later, due to the advantages of caching and multi-hop, the protection level of proposed scheme becomes better than Wang et al.'s scheme gradually. Ultimately, no matter from protection level or energy consumption, the three schemes will be relatively stable within a range. That is to say, proposed scheme has the best protection level, Wang et al.'s scheme is the second, and Wei et al.'s scheme is the worst, and that energy consumption of them is comparable.

6. **Conclusions.** This paper proposes a scheme using small cell base stations to protect location privacy when mobile terminals enjoy location-based services in the background of next generation cellular networks with huge communication infrastructures. Mobile

terminals use the location of small cell base stations instead of their real locations to complete the queries, by this means not only can the location information be protected from the source, but also can get rid of the GPS positioning system to get location information. Request table and caching make regional recommendation services possible. Experimental results, privacy protection analysis, and comparison schemes confirm that the proposed scheme is feasible and effective.

As shown in the experimental part, the location service quality of the proposed scheme is acceptable to people. However, it is not perfect because it does not reach one hundred percent. Consequently, the study in this direction needs to be strengthened. As a result, we will focus on how to refine candidate results more wholly, improve the quality of service, and construct a more perfect scheme in the future.

REFERENCES

[1] W.J. Bradshaw, E.C. Alley, J.H. Huggins, A.L. Lloyd, and K.M. Esvelt, Bidirectional contact tracing could dramatically improve covid-19 control, *Nature communications*, vol. 12, no. 1, pp. 1–9, 2021.

[2] A. Aloui and O. Kazar, A survey on privacy preservation in location-based mobile business: Research directions, *International Journal of Web Portals(IJWP)*, vol. 13, no. 1, pp. 20–39, 2021.

[3] F. Tariq, M.R. Khandaker, K.K. Wong, M.A. Imran, M. Bennis, and M. Debbah, A speculative study on 6G, *IEEE Wireless Communications*, vol. 27, no. 4, pp. 118–125, 2020.

[4] C.M. Chen, Z. Tie, E.K. Wang, M.K. Khan, S. Kumar, and S. Kumari, Verifiable dynamic ranked search with forward privacy over encrypted cloud data, *Peer-to-Peer Networking and Applications*, vol. 14, pp. 2977–2991, 2021.

[5] J.K. Liu, M.H. Au, T.H. Yuen, C. Zuo, J. Wang, A. Sakzad, X. Luo, and L. Li, Privacy-preserving covid-19 contact tracing app: A zero-knowledge proof approach, *Cryptology ePrint Archive, Report 2020/528*, 2020, https://ia.cr/2020/528.

[6] R. Nieminen and K. Järvinen, Practical privacy-preserving indoor localization based on secure two-party computation, *IEEE Transactions on Mobile Computing*, vol. 20, pp. 2877–2890, 2021.

[7] H. Jiang, H. Wang, Z. Zheng, and Q. Xu, Privacy preserved wireless sensor location protocols based on mobile edge computing, *Computers & Security*, vol. 84, pp. 393–401, 2019.

[8] S. Zeng, H. Zhang, F. Hao, and H. Li, Deniable-based privacy-preserving authentication against location leakage in edge computing, *IEEE Systems Journal*, 2021, https://doi.org/10.1109/JSYST.2021.3049629.

[9] P.S. Saravanan and S. Balasundaram, Protecting privacy in location-based services through location anonymization using cloaking algorithms based on connected components, *Wireless Personal Communications*, vol. 102, pp. 449–471, 2018.

[10] M. Li, H. Zhu, Z. Gao, S. Chen, L. Yu, S. Hu, and K. Ren, All your location are belong to us: Breaking mobile social networks for automated user location tracking, *The Fifteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc'14*, pp. 43-52, 2014.

[11] B. Palanisamy and L. Liu, Attack-resilient mix-zones over road networks: Architecture and algorithms, *IEEE Transactions on Mobile Computing*, vol. 14, pp. 495–508, 2015.

[12] Z. Bao, W. Shi, S. Kumari, Z.Y. Kong, and C.M. Chen, Lockmix: a secure and privacy-preserving mix service for bitcoin anonymity, *International Journal of Information Security*, vol. 19, no. 3, pp. 311–321, 2020.

[13] G. Natesan and J. Liu, An adaptive learning model for k-anonymity location privacy protection, *2015 IEEE 39th Annual Computer Software and Applications Conference*, vol. 3, pp. 10–16, 2015.

[14] Y. Qian, Y. Ma, J. Chen, D. Wu, D. Tian, and K. Hwang, Optimal location privacy preserving and service quality guaranteed task allocation in vehicle-based crowdsensing networks, *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, pp. 4367–4375, 2021.

[15] H. Lian, W. Qiu, D. Yan, Z. Huang, and P. Tang, Efficient and secure k-nearest neighbor query on outsourced data, *Peer-to-Peer Networking and Applications*, vol. 13, pp. 2324–2333, 2020.

[16] S. Zhang, K.K.R. Choo, Q. Liu, and G. Wang, Enhancing privacy through uniform grid and caching in location-based services, *Future Generation Computer Systems*, vol. 86, pp. 881–892, 2018.

[17] C.M. Chen, Y.H. Chen, Y.H. Lin, and H.M. Sun, Eliminating rouge femtocells based on distance bounding protocol and geographic information, *Expert Systems with Applications*, vol. 41, no. 2, pp. 426–433, 2014.

[18] G. Xiang and Z. Cui, The algebra homomorphic encryption scheme based on fermat's little theorem, *2012 international conference on communication systems and network technologies*, pp. 978-981, 2012.

[19] E. Gabrilovich and S. Markovitch, Wikipedia-based semantic interpretation for natural language processing, *ArXiv*, vol. abs/1401.5697, 2009.

[20] W. Wang, S. Ge, and X. Zhou, Location-privacy-aware service migration in mobile edge computing, *2020 IEEE Wireless Communications and Networking Conference(WCNC)*, pp. 1–6, 2020.

[21] X. Wei, J. Liu, Y. Wang, C. Tang, and Y. Hu, Wireless edge caching based on content similarityin dynamic environments, *Journal of Systems Architecture*, vol. 115, 102000, 2021.