Homomorphic Encryption to Preserve Location Privacy

Maede Ashouri-Talouki and Ahmad Baraani-Dastjerdi

Department of Computer Engineering,
Faculty of Engineering, The University of Isfahan, Isfahan, Iran

{ashoori,ahmadb}@eng.ui.ac.ir

Abstract

Recently user privacy becomes an important security goal in most computer applications especially in context aware services. One of the most popular services in this field is location-based services (LBSs) that deliver the desired data based on the user's location. Although these services make the life easier, they lead to a privacy risk. To get the desired services, a user should disclose her location; so her location privacy is threatened.

In this paper we consider a group of users who wants to use a location-based service while preserving their location privacy. We propose a solution for this scenario and compare it with the previous solution. Analysis of our protocol shows the effectiveness of the proposed approach in terms of computation and communication costs.

Keywords: *Group Privacy, Homomorphic Encryption, Location Privacy*

1. Introduction

Current developments and advancements in mobile communication and internet technology make the Ubiquitous Computing a reality. In ubiquitous computing environments, users receive their desired information according to their current status and context [4] at any time and from anywhere; these services are called context-based services [6]. Location-based services (LBSs) are one of the most popular context-based services that deliver the desired information based on users' current locations [10]. For example a user could ask "where the nearest restaurant to my location is" or "which route goes to the city center from my location".

Because LBSs require users' location to deliver the requested data, users' location privacy are threatened. Hence, users are worried about their location privacy and the usage of their location by LBS providers.

To preserve user location privacy during the use of LBS, a lot of mechanisms are proposed. The most of the current solutions for location privacy protection considered the location privacy of a single user; they do not take care about the location privacy of a group of users. More exactly, current solutions protect the location privacy of an individual user who wants to use a location-based service and do not consider the scenarios in which a group of users wants to use a location-based service [3, 8, 9]. For example, a group of users wants to organize an urgent face to face meeting. They could use a location-based service for finding the nearest meeting point to their current locations. In this scenario, group members aim to protect their location privacy from other group members and from the service provider. Supporting these privacy requirements need special solution to be developed.

This paper considers this grouping scenario and proposes a solution to protect location privacy within the group (from other group members) and from anyone outside the group including the service provider.

The rest of the paper is organized as follows: Section 2 reviews the related work in the context of supporting location privacy in the grouping scenarios. The proposed solution is presented in Section 3. Properties of the proposed solution are discussed in Section 4 and finally the paper is concluded in Section 5.

2. Related Works

There are lots of works available in the field of preserving a user location privacy. According to Solanas's classification [4tubitak], these approaches are categorized in two main classes: 1) methods that are based on a trusted third party (TTP-based), and 2) methods that are free from a TTP (TTP-free).

The TTP-based approaches require a TTP to mediate the communication between a user and an LBS provider. A user sends her location along with the query to the TTP who is responsible for blurring the user's location. Then TTP sends the blurred location and the query to the LBS provider, receives the result from the LBS and sends it back to the user. The main problem with these approaches is that they require the users to trust TTPs. To alleviate this limitation, TTP-free methods are proposed.

In TTP-free methods, users cloak their location without trusting a TTP; these methods are categorized in three sub categories [4tubitak]: 1) collaboration based methods, 2) obfuscation based methods and 3) private information retrieval based methods (PIR-based). In collaboration based method, each user cloaks her location by contacting her peers and collecting their location data. In obfuscation based methods, each user degrades the quality of her location information, i.e., by sending a set of locations instead of sending the exact location. PIR-based methods are totally different from previous approaches; in these methods LBS is encoded such that it can evaluate the location-based queries without knowing users' location.

Although, TTP-free methods solves the drawbacks of TTP-based methods, but there is some problems with these approaches, for example in some of the TTP-free methods, users should trust their peers or the LBS content should be encoded which is not applicable.

All of the above mentioned approaches aim to support a user's location privacy. To the best of our knowledge, there is only one work available in the field of group location privacy proposed by Hashem, et. al., [7]. Hashem, et. al.'s method consists of three steps:

1) Sending the query,
2) Evaluating the query,
3) Finding the meeting point.

In the first step, each user cloaks her location into a rectangle by contacting her peers [hashem07]; then she sends a location-based query along with her cloaked location to the LBS. Also, each user puts attaches an ID to her query that is the same as other members' ID. The query IDs are issued by a group coordinator that is randomly selected at the beginning of the protocol.

In the second step, the LBS provider evaluates the received queries and returns a set of candidate points of interest (POIs). Also, the LBS provider computes and sends the summation of maximum distances and the summation of minimum distances of each POI in the answer set from the query rectangles.

After receiving the answer set, members of the group collaboratively refine the answer set by subtracting their maximum distances from the received summation and adding their exact distances from each POI in the answer set. After doing this by all members, the point with the minimum distance is selected as the meeting point. Hence, without disclosing the exact locations, members find the desired meeting point, so their location privacy is preserved.

Although Hashem et al.'s method protects user location privacy, it suffers from a high communication cost; especially the size of the answer set can be very high.

Our proposed protocol consists of three steps and protects user location privacy with lower communication cost. The first step of the proposed protocol is similar to Hashem, et. al.'s method; in the second step, the LBS computes the desired POIs with a lower computation costs than that of Hashem et al.'s method. Also, the size of the answer set in our protocol is smaller than Hashem, et. al.'s method. Finally, the last step of the proposed protocol is totally different from Hashem, et. al.'s method; it is based on Homomorphic Encryption. The next section describes the proposed protocol in detail.

3. Proposed Protocol

In this section, we will firstly describe the building blocks that are used in the structure of our protocol; then the proposed protocol is presented.

3.1. Building Blocks

We use Homomorphic encryption [2, 5] and the research done by Melchor [1] as the main building blocks of our proposed protocol. Homomorphic encryption is an encryption scheme with three functions named (Gen, Enc, Dec) [2, 5]. Gen Function is responsible for generating a pair of keys (*sk*, *pk*) in public key (PK) scheme. Enc and Dec are the encryption and decryption functions, respectively.

The Encryption function is called Homomorphic if the following two properties hold [2, 5]:

$$Enc_{pk}(x;r).Enc_{pk}(y;r') = Enc_{pk}(x+y;r.r') \qquad (1)$$

$$Enc_{pk}(x;r)^{y} = Enc_{pk}(x.y;r^{y}) \qquad (2),$$

where x and y are the plaintext messages and r and r' are random strings.

The properties of Homomorphic encryption allow the manipulation of the ciphertext and getting a new valid ciphertext without knowing the private key or the corresponding plaintext.

Upon Melchor idea [1], users can construct special masks that upon aggregation, all of the masks will be canceled. In this idea, each user (U_i) arbitrary selects some of the members of the group as her friends and puts them in a special set called BF_i. Then, U_j and each user $\left(U_j\right)$ in BF_i share a unique common secret such that the secret of U_i and U_j is the negative of the shared secret between U_j and U_i, $s_{i,j} = -s_{j,i}$. In this way, aggregating all masks will contain all of the secrets (their positive and negative values) that results in zero value.

We use these two methods and design our protocol structure.

3.2. Our Protocol

This section presents the proposed protocol for protecting location privacy for a group of users; our protocol is based on Homomorphic encryption and Melchor idea [1]. The first step of the proposed protocol is similar to Hashem et al.'s method [7]: each user cloaks her location upon her privacy profile and sends a location-based query along with her cloaked location to the LBS.

In phase 2 of the proposed protocol, the LSB computes the set of candidate answers (A) without computing the summation of maximum and the summation of minimum distances. The LBS evaluates the answer set based on any privacy-preserving group query-processing algorithm [7].

The third step of the proposed protocol is as follows:

One of the members of the group is selected as the group manager (GM); then GM chooses a pair of keys (*sk,pk*) in PK scheme as the group's public/private key. Then, she sends the public key (*pk*) to all members of the group, but the private key (*sk*) is kept secret.

Afterward, each member of the group forms the set BF_i of her friends and shares a unique common secret based on Melchor idea.

Upon receiving the set of candidate answers (A), each member U_i computes her distance to each POI $P_h \in A$ and encrypts this value by the group public key (*pk*), as follows:

$$c_{i,h} = Enc_{pk}(Dist(l_i, P_h), r) \qquad (3)$$

where $Dist(l_i, P_h)$ is the distance from l_i to P_h and l_i is the exact location of U_i.

Sending the value of $c_{i,h}$ to GM, allows her to decrypt it and gets the exact distance of each user U_i to $P_h \in A$. Thus, according to the distance intersection attack [7], GM would learn the exact location of U_i. Preventing this attack, we use Melchor idea [1] to create a mask for $c_{i,h}$ as follows:

Recall that each U_i shares a secret key with her friends in the set BF_i; now she constructs her mask (MSK_i) by computing the summation of all her secrets:

$$MSK_i = \sum_{j \in BF_i} s_{i,j} \qquad (4)$$

Then, U_i encrypts MSK_i with the group public key and computes $w'_{i,h}$ as follows:

$$w'_{i,h} = Enc_{pk}(Dist(l_i, P_h), r).Enc_{pk}(MSK_i, r') \qquad (5)$$

As *Enc* is a Homomorphic function, $w'_{i,h}$ is equal to the encryption of $Dist(l_i, P_h) + MSK_i$ by the public key (*pk*).

For each $P_h \in A$, after receiving the values of $w'_{i,h}$ of all members, GM multiplies them and gets the following according to the homomorphic properties of *Enc* function:

$$\begin{aligned}\prod_{all\ i} w'_{i,h} &= \prod Enc_{pk}(Dist(l_i, P_h) + MSK_i, r.r')\\ &= Enc_{pk}(\sum_{all\ i}(Dist(l_i, P_h) + MSK_i)) \\ &= Enc_{pk}(\sum_{all\ i} Dist(l_i, P_h) + \sum_{all\ i} MSK_i)\end{aligned} \quad (6)$$

Since, each $s_{i,j}$ appears in two forms (positive and negative), the summation of all masks (MSK_i) will be equal to zero; thus GM gets the final result (the summation of all users' distances to each $P_h \in A$) that is encrypted by the group's public key. Now, GM decrypts and broadcasts them to the group. Afterward, the POI with minimum distance is selected as the meeting point.

In the next section the properties of the proposed protocol is discussed.

4. Protocol Analysis

This section talks about privacy properties of the proposed protocol. The first theorem discusses the location privacy protection of each member regarding the GM. The second theorem proves that the location privacy property is preserved even in case of collusion. The third theorem discusses the location privacy property of all group members regarding the LBS.

Theorem 1: Members' location privacy is protected against GM.

Proof: GM receives the value of $w'_{i,h}$ from each user U_i. Upon decryption of $w'_{i,h}$ for all $P_h \in A$, GM would learn the value of $Dist(l_i, P_h) + MSK_i$. To get the exact location of U_i, GM should extract and cancel the mask (MSK_i), but she does not have the required knowledge to learn the value of the mask. Thus, she cannot obtain $Dist(l_i, P_h)$ and consequently user location privacy is preserved.

If GM can successfully collude with at least $|BF_i|-1$ group members, then she can obtain MSK_i and get the desired $Dist(l_i, P_h)$. The probability of collusion is proportional to the cardinality of BF_i; whatever the cardinality of BF_i is increased, the probability of collusion is decreased. The next theorem discusses the location privacy protection in case of collusion:

Theorem 2: The location privacy of the group members is preserved within the group even in case of collusion.

Proof: Each user encrypts her exact distance with group public key and multiplies it with MSK_i (Eq.5). In order to learn the exact distance of U_i, a malicious member should have the group's private key (*sk*) in addition to the knowledge of MSK_i. Since the private key is only known by GM, the malicious member cannot learn it. Moreover, the malicious member must learn MSK_i to successfully decrypt $w'_{i,h}$. To achieve this, the malicious member should collude with at least $|BF_i|-1$ group members. In a collusion of $|BF_i|-1$ malicious members and GM, the exact distances of U_i $\left(Dist(l_i,P_h)\right)$ and consequently her exact location will be revealed. Because U_i forms the set BF_i of her friends, thus it is impractical that all friends of U_i collude against her; the attack probability is very low.

Theorem 3: Location privacy of group members is preserved from the LBS.

Proof: In the first step of the proposed protocol, each member of the group cloaks her location and sends her cloaked area to the LBS, so the user's exact location is protected from the LBS. Eavesdropping on the group's internal communication in the second step cannot reveal any useful information to the LBS because, the LBS does not know the private key of the group and the mask MSK_i of the members.

In real world scenario the LBS only sends the desired POI and nothing else. Thus to apply Hashem et al.'s method, all of the algorithms to process spatial queries in service providers should changed that is not desirable.

Our proposed protocol deals with normal spatial query processors and does not enforce the LBS to do anything more.

Moreover, our protocol is resistant to a collusion of GM and $|BF_i|-1$ malicious members.

In terms of communication cost, our protocol is similar to Hashem et al.'s protocol: there are *2n* messages that are exchanged between group members in the third step. But as it is clear, in the second step, the size of the LBS message in our protocol is less than Hashem et al.'s method. In particular, the size of the result in our proposed protocol is $|p_i|*k$ versus $|p_i|*k+2*l*k$ in Hashem et al.'s protocol, where $|p_i|$ is the size of message containing a single POI (p_i), *k* is the number of POIs in the answer set and l is the size of a message containing the summation of maximum or the minimum distance to the cloaked areas.

Regarding the computation cost, the first step of our protocol reduces the computation cost of the LBS, because there is no need to compute the summation of maximum and minimum distances from each POI in the set of candidate answers to the query rectangles. In the third step, we need more computation than Hashem et al.'s protocol because of encryption and decryption operations. Since the operations of the third step are done in parallel (each member encrypts her distances parallel to other members), the overall computation cost is prorated. Considering *k* as the number of POIs in the answer set, the protocol requires *k* encryption operations and *k* decryption operations in total; consequently the computation complexity of our protocol is *O(k).*

5. Conclusion

This paper talks about an interesting problem called location privacy protection for a group of users. We present a new protocol to preserve the location privacy within the group and from anyone outside the group including the LBS.

The proposed protocol that is based on Homomorphic encryption would simply apply in real world applications without any modification to the algorithm and architecture of the current service providers. Also, the proposed protocol incurs less communication overhead than the previous method. Our protocol preserves members' location privacy in case of collusion of malicious members.

References

[1] C. A. Melchor, B. Ait-Salem and P. Gaborit, "A Collusion-Resistant Distributed Scalar Product Protocol With Application To Privacy-Preserving Computation of Trust", In Proceeding of Eighth IEEE International Symposium on Network Computing and Applications, **(2009)** IEEE Computer Society, Boston, MA, USA.

[2] I. Damgard and M. Jurik, "A generalisation, a simplification and some applications of paillier's probabilistic public-key system", In Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography, **(2001)** London, UK.

[3] J. C'as, "Privacy in Pervasive Computing Environments – A Contradiction in Terms", Journal of IEEE Technology and Society Magazine, vol. 24, no. 1, **(2005)**.

[4] O. Coutand, O. Droegehorn, K. David, P. Nurmi, P. Floréen, R. Kernchen, S. Holtmanns, S. Campadello, T. Kanter, M. Martin, R. van Eijk and R. Guarneri, "Context-aware Group Management in Mobile Environments", In Proceedings of the 14th IST Mobile and Wireless Communication Summit, **(2005)** Dresden, Germany.

[5] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes", In Proceedings of the 17th international conference on Theory and application of cryptographic techniques, **(1999)** Prague, Czech Republic.

[6] S. Campadello, O. Coutand, C. del Rosso, S. Holtmanns, T. Kanter, C. Räck, B. Mrohs and S. Steglich, "Trust and Privacy in Context-Aware Support for Communication in Mobile Groups", Workshop on Context Awareness for Proactive Systems (CAPS), **(2005)** Helsinki, Finland.

[7] T. Hashem, L. Kulik and R. Zhang, "Privacy preserving group nearest neighbor queries", In Proceeding of 13th International Conference on Extending Database Technology, **(2010)** Lausanne, Switzerland.

[8] T. Dumsday, "Group Privacy and Government Surveillance of Religious Services", The Monist, vol. 91, no. 1, **(2008)**.

[9] T. Kuflik, J. Sheidin, S. Jbara, D. Goren-Bar, P. Soffer, O. Stock and M. Zancanaro, "Supporting small groups in the museum by context-aware communication services", In Proceedings of IUI'07, **(2007)** Honolulu, Hawaii, USA.

[10] G. Zhong and U. Hengartner, "A Distributed k-Anonymity Protocol for Location Privacy", In Proceedings of Seventh IEEE International Conference on Pervasive Computing and Communication (PerCom), **(2009)**, Galveston, TX.