IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 10, December 2014.
www.ijiset.com
ISSN 2348 – 7968

Privacy and Content Protection Using Centroid Localization Algorithm

Suresh.G[1] , Arulselvam.R[2], Ramachandiran.R[3]

[1,2]PG Student, Dept. of MCA, Sri Manakula Vinayagar Engineering College, Puducherry

[3]Assistant Professor,Dept.of MCA, Sri Manakula Vinayagar Engineering College, Puducherry

ABSTRACT

In this paper we present a solution to one of the location-based query problems. This problem is defined as follows: (i) a user wants to query a database of location data, known as Points Of Interest (POIs), and does not want to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, does not want to simply distribute its data to all users. The location server desires to have some control over its data, since the data is its asset. We propose a major enhancement upon previous solutions by introducing a two stage approach, where the first step is based on Oblivious Transfer and the second step is based on Private Information Retrieval, to achieve a secure solution for both parties. The solution we present is efficient and practical in many scenarios. We implement our solution on a desktop machine and a mobile device to assess the efficiency of our protocol. We also introduce a security model and analyse the security in the context of our protocol. Finally, we highlight a security weakness of our previous work and present a solution to overcome it.

Index Terms -

INTRODUCTION

ALOCATION based service (LBS) is an information, entertainment and utility service generally accessible by mobile devices such as, mobile phones, GPS devices, pocket PCs, and operating through a mobile network. ALBS can offer many services to the users based on the geographical position of their mobile device. The services provided by LBS are typically based on a point of interest database. By retrieving the Points Of Interest (POIs) from the database server, the user can get answers to various location based queries, which include but are not limited to - discovering the nearest ATM machine, gas station, hospital, or police station. To solve the localization problem, it is natural to consider placing sensors manually or equipping each sensor with a GPS receiver. However, due to the large scale nature of sensor networks, those two methods become either inefficient or costly, so researchers propose to use a variety of localization approaches for sensor network localization. And when GPS (Global Positioning System) is used, it is hard to get accurate location information because of the reception rate varying according to place. These approaches can be classified as range-based and range-free. Firstly, the range based approach uses an absolute node-to-node distance or angle between neighbouring sensors to estimate locations. Common techniques for distance or angle estimation include received signal strength indicator (RSSI), time of arrival (TOA), time difference of arrival (TDOA), and angle of arrival (AOA). The approaches typically have higher location accuracy but require additional hardware to measure distances or angles. Secondly, the range-free approach does not need the distance or angle information for localization, and depends only on connectivity of the network and the contents of received messages.

Related Work

Issues in Wireless Sensor Networks

Wireless sensor networks provide the means to link the physical world to the digital world. The mass production of integrated, low-cost sensor nodes will allow the technology to cross over into a myriad of domains. In the future, applications of wireless sensor networks will appear in areas we never dreamed. Listed below are just a few places where sensor networks can and will be deployed.

- Earthquake monitoring
- Environmental monitoring
- Factory automation
- Home and office controls
- Inventory monitoring
- Medicine
- Security

Although still in its infancy, wireless sensor network applications are beginning to emerge. A recent study on Great Duck Island in Maine used sensor networks to perform monitoring tasks without the intrusive presence of humans.

Weighted Centroid Localization Algorithm

In the algorithm, mobile anchor node confronts the right to decide the location of the centred through weighted factor to reflect. The use of weighted factor reflected the intrinsic relationship between them. We embody this relationship through the formula of the weighted factor:

$X=(X1/d1+ X2/d2+ X3/d3)/(1/d1+1/d2+1/d3)$

$Y=(Y1/d1+ Y2/d2+ Y3/d3)/(1/d1+1/d2+1/d3)$.

Weighted Centroid Localization Algorithm process:

① The mobile anchor node periodically sends its own information.

② Unknown node received information, only records the same location of the mobile anchor node average RSSI.

③ Unknown node received over threshold m in the position information then RSSI value in accordance with the smallest sort of mobile anchor node location. And to establish the mapping between RSSI value and the distance from unknown node to the mobile anchor node. The establishment of three sets:

Mobile anchor node_set = {a1, a2, … , am};

Distance_set = {d1, d2, … , dm};

Mobile anchor node position_set = {(X1, Y1), (X2, Y2), … , (Xm, Ym)};

④ RSSI value with the first few large location of mobile anchor node of the calculation:

Based on the preceding analysis, In the mobile anchor node_set Select RSSI value of large node location then the composition of the triangle set. This is very important.

Triangle_set = {(a1, a2, a3), (a1, a2, a4), … (a1, a3, a4), (a1, a3, a5) … };

⑤ n location of mobile anchor nodes can be composed of C_n^3 triangles. The use formula ① calculates C_n^3 coordinate.

⑥ Calculates the mean value(X,Y) of C_n^3 coordinate. The (X, Y) is Unknown node coordinate.

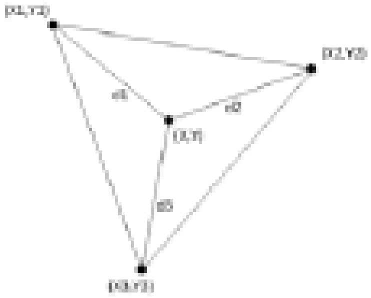


Fig. 1. Scheme of the adaptive weighted centroid localization algorithm

Our Contributions

In this paper, we propose a novel protocol for location based a query that has major performance improvements with respect to the approach by Ghinitat. Like such protocol, our protocol is organized according to two stages. In the first stage, the user privately determines his/her location within a public grid, using oblivious transfer. This data contains both the ID and associated symmetric key for the block of data in the private grid. In the second stage, the user executes a communicational efficient PIR [11], to retrieve the appropriate block in the private grid. This block is decrypted using the symmetric key obtained in the previous stage. Our protocol thus provides protection for both the user and the server. The user is protected because the server is unable to determine his/her location. Similarly, the server's data is protected since a malicious user can only decrypt the block of data obtained by PIR with the encryption key acquired in the previous stage. In other words, users cannot gain any more data than what they have paid for. We remark that this paper is an enhancement of a previous work. In particular, the following contributions are made.

1) Redesigned the key structure

2) Added a formal security model

3) Implemented the solution on both a mobile device and desktop machine

As with our previous work, the implementation demonstrates the efficiency and practicality of our approach.

Localized Approximation Method

Inertia Information

Inertia information indicates how long a moving object has moved from its current position. For actual utilization of the information, accordingly, it needs to be transformed to the navigation coordinate system.

Inertial coordinate system

In this coordinate system, the origin is the centre of earth, and axis X and Y are positioned on the equator regardless of the earth's rotation, and axis Z coincides with the earth's rotation axis.

Global coordinate system

In this coordinate system, the origin is the centre of earth, axis X is the point where the longitude intersects the equator, axis Z is the axis running toward the North Pole, and axis Z is the direction turning 90 counter clockwise from axis X.

Navigation coordinate system

In this coordinate system, the origin is the centre of the moving object, and axis X, Y and Z are north, east and down, respectively.

PROTOCOL MODEL

Before describing our protocol we introduce the system model, which defines the major entities and their roles. The description of the protocol model begins with the notations and system parameters of our solution.

Notations

Let x ← y be the assignment of the value of variable y to variable x and E ←v be the transfer of the variable v to entity E. Denote the El Gamal encryption of message m as E(m, y) = A = (A1,A2) = (gr, gmyr), where g is a generator of group G, y is the public key of the form y = gx, and r is chosen at random. This will be used as a basis for constructing an adaptive oblivious transfer scheme. Note that A is a vector, while A1, A2 are elements of the vector. The cyclic group G0 is a multiplicative subgroup of the finite field Fp, where p is a large prime number and q is a prime that divides (p − 1).

System Model

The system model consists of three types of entities (see Fig. 1): the set of users1 who wish to access location data U, a mobile service provider SP, and a location server LS. From the point of view of a user, the SP and LS will compose a server, which will serve both functions. The user does not need to be concerned with the specifics of the communication.

The users in our model use some location-based service provided by the location server LS. For example, what is the nearest ATM or restaurant? The purpose of the mobile service provider SP is to establish and maintain the communication between the location server and the user. The location server LS owns a set of POI records ri for 1 ≤ ri ≤ ρ. Each record describes a POI, giving GPS coordinates to its location (xgps, ygps), and a description or name about what is at the location.

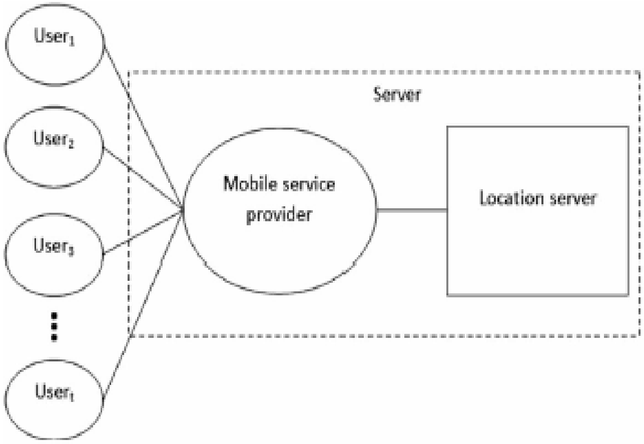


Fig.2.System model.

PROTOCOL DESCRIPTION

We now describe our protocol. We first give a protocol summary to contextualise the proposed solution and then describe the solution's protocol in more detail.

Protocol Summary

The ultimate goal of our protocol is to obtain a set (block) of POI records from the LS, which are close to the user's position, without compromising the privacy of the user or the data stored at the server. We achieve this by applying a two stage approach shown in Fig. 2. The first stage is based on a two-dimensional oblivious transfer and the second stage is based on a communication ally efficient PIR. The oblivious transfer based protocol is used by the user to obtain the cell ID, where the user is located, and the corresponding symmetric key. The knowledge of the cell ID and the symmetric key is then used in the PIR based protocol to obtain and decrypt the location data.

The user determines his/her location within a publicly generated grid *P* by using his/her GPS coordinates and forms an oblivious transfer query2. The minimum dimensions of the public grid are defined by the server and are made available to all users of the system. This public grid superimposes

ISSN 2348 – 7968

over the privately partitioned grid generated by the location server's POI records, such that for each cell *Qi,j* in the server's partition there is at least one *Pi,j* cell from the public grid. This is illustrated in Fig.3.

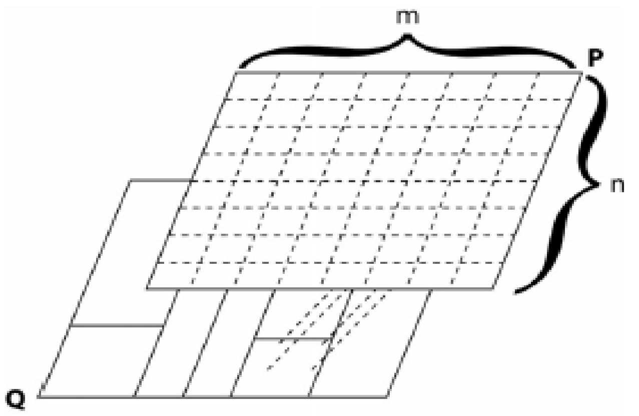


Fig.3. Public grid superimposed over the private grid

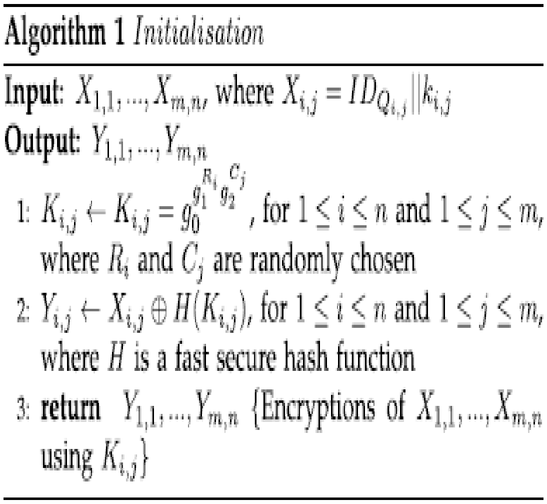
Oblivious Transfer Phase

The purpose of this protocol is for the user to obtain one and only one record from the cell in the public grid P, shown in Fig. 4. We achieve this by constructing a 2-dimensional oblivious transfer, based on the ElGamal oblivious transfer [2], using adaptive oblivious transfer proposed by Naor et al. The public grid P, known by both parties, has m columns and n rows. Each cell in P contains a symmetric key ki,j and a cell id in grid Q or (IDQi,j , ki,j), which can be represented by a stream of bits Xi,j. The user determines his/her i, j coordinates in the public grid which is used to acquire the data from the cell within the grid. The protocol is initialised by the server by generating m×n keys of the form

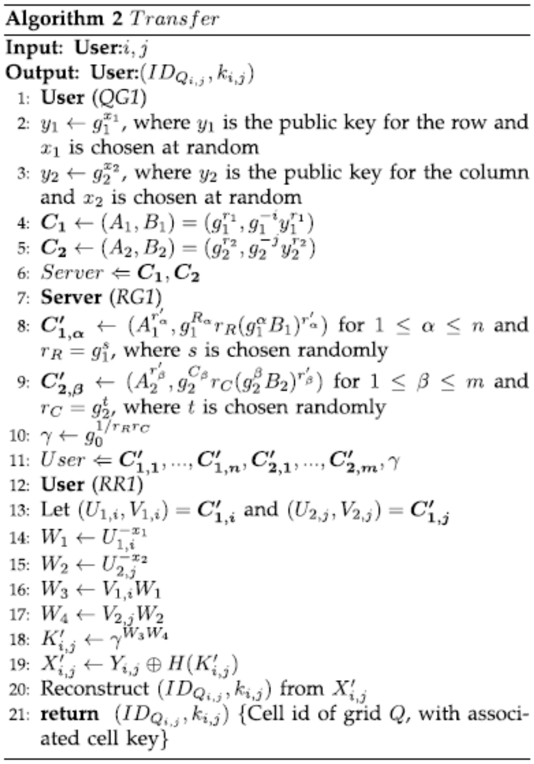
Theorem 1 (Correctness). Assume that the user and server follow Algorithms 1 and 2 correctly. Let Xi,j be the bit string encoding the pair (IDQi,j , ki,j) and let X_i, j the bit string generated by Algorithm 2 X_i, j = Yi,j⨁H(Ki,j). Then X_i,j = Xi,j. Proof. We begin this proof by showing that Ki,j = K_i,j, where K_ i,j is the key obtained by the user according to the Algorithm 2.

$$\begin{aligned} W_3 &= V_{1,i}W_1 \\ &= g_1^{R_i} r_R (g_1^{\alpha} g_1^{-i} y_1^{r_1})^{r_1'} U_{1,i}^{-x_1} \\ &= g_1^{R_i} r_R (y_1^{r_1 r_1'}) U_{1,i}^{-x_1} \end{aligned}$$

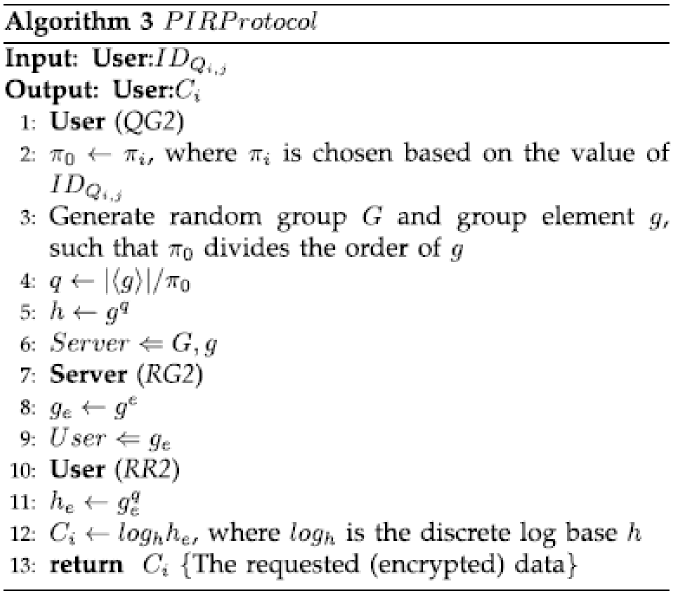
$$\begin{aligned} &= g_1^{R_i} r_R (g_1^{x r_1 r_1'})(g_1^{r_1 r_1'})^{-x_1} \\ &= g_1^{R_i} r_R (g_1^{x r_1 r_1'})(g_1^{-(x r_1 r_1')}) \\ &= g_1^{R_i} r_R \ (mod\ q) \end{aligned}$$



```
Algorithm 1 Initialisation
Input: $X_{1,1}, ..., X_{m,n}$, where $X_{i,j} = ID_{Q_{i,j}} || k_{i,j}$
Output: $Y_{1,1}, ..., Y_{m,n}$
  $K_{i,j} \leftarrow K_{i,j} = g_0^{g_1^{R_i} g_2^{C_j}}$ , for $1 \leq i \leq n$ and $1 \leq j \leq m$,
    where $R_i$ and $C_j$ are randomly chosen
  $Y_{i,j} \leftarrow X_{i,j} \oplus H(K_{i,j})$, for $1 \leq i \leq n$ and $1 \leq j \leq m$,
    where $H$ is a fast secure hash function
  return $Y_{1,1}, ..., Y_{m,n}$ {Encryptions of $X_{1,1}, ..., X_{m,n}$
    using $K_{i,j}$}
```



```
Algorithm 2 Transfer
Input: User:$i, j$
Output: User:$(ID_{Q_{i,j}}, k_{i,j})$
  User (QG1)
  $y_1 \leftarrow g_1^{x_1}$, where $y_1$ is the public key for the row and
    $x_1$ is chosen at random
  $y_2 \leftarrow g_2^{x_2}$, where $y_2$ is the public key for the column
    and $x_2$ is chosen at random
  $\boldsymbol{C_1} \leftarrow (A_1, B_1) = (g_1^{r_1}, g_1^{-i} y_1^{r_1})$
  $\boldsymbol{C_2} \leftarrow (A_2, B_2) = (g_2^{r_2}, g_2^{-j} y_2^{r_2})$
  $Server \Leftarrow \boldsymbol{C_1}, \boldsymbol{C_2}$
  Server (RG1)
  $\boldsymbol{C'_{1,\alpha}} \leftarrow (A_1^{r'_\alpha}, g_1^{R_\alpha} r_R (g_1^{\alpha} B_1)^{r'_\alpha})$ for $1 \leq \alpha \leq n$ and
    $r_R = g_1^{s}$, where $s$ is chosen randomly
  $\boldsymbol{C'_{2,\beta}} \leftarrow (A_2^{r'_\beta}, g_2^{C_\beta} r_C (g_2^{\beta} B_2)^{r'_\beta})$ for $1 \leq \beta \leq m$ and
    $r_C = g_2^{t}$, where $t$ is chosen randomly
  $\gamma \leftarrow g_0^{1/r_R r_C}$
  $User \Leftarrow \boldsymbol{C'_{1,1}}, ..., \boldsymbol{C'_{1,n}}, \boldsymbol{C'_{2,1}}, ..., \boldsymbol{C'_{2,m}}, \gamma$
  User (RR1)
  Let $(U_{1,i}, V_{1,i}) = \boldsymbol{C'_{1,i}}$ and $(U_{2,j}, V_{2,j}) = \boldsymbol{C'_{1,j}}$
  $W_1 \leftarrow U_{1,i}^{-x_1}$
  $W_2 \leftarrow U_{2,j}^{-x_2}$
  $W_3 \leftarrow V_{1,i} W_1$
  $W_4 \leftarrow V_{2,j} W_2$
  $K'_{i,j} \leftarrow \gamma^{W_3 W_4}$
  $X'_{i,j} \leftarrow Y_{i,j} \oplus H(K'_{i,j})$
  Reconstruct $(ID_{Q_{i,j}}, k_{i,j})$ from $X'_{i,j}$
  return $(ID_{Q_{i,j}}, k_{i,j})$ {Cell id of grid $Q$, with associated cell key}
```



```
Algorithm 3 $PIRProtocol$
Input: User:$ID_{Q_{i,j}}$
Output: User:$C_i$
User ($QG2$)
    $\pi_0 \leftarrow \pi_i$, where $\pi_i$ is chosen based on the value of $ID_{Q_{i,j}}$
    Generate random group $G$ and group element $g$, such that $\pi_0$ divides the order of $g$
    $q \leftarrow |\langle g \rangle| / \pi_0$
    $h \leftarrow g^q$
    $Server \Leftarrow G, g$
Server ($RG2$)
    $g_e \leftarrow g^e$
    $User \Leftarrow g_e$
User ($RR2$)
    $h_e \leftarrow g_e^q$
    $C_i \leftarrow log_h h_e$, where $log_h$ is the discrete log base $h$
    return $C_i$ {The requested (encrypted) data}
```

This proves Ki,j = K_ i,j. Since ⊕ is self inverse and given that Yi,j = Xi,j⊕H(Ki,j), it follows that Xi,j = Yi,j⊕ H(Ki,j). Using knowledge of K_ i,j, the user can compute Xi,j, which is the same as X_ i,j as desired. This completes the proof.

SECURITY ANALYSIS

In this section, we analyse the security of the client and the server. While the client does not want to give up the privacy of his/her location, the server does not want to disclose other records to the client. This would not make much business sense in a variety of applications.

Client's Security

Fundamentally, the information that is most valuable to the user is his/her location. This location is mapped to a cell Pi,j. In both phases of our protocol, the oblivious transfer based protocol and the private information retrieval based protocol, the server must not be able to distinguish two queries of the client from each other. We will now describe both cases separately.

Theorem3. Assume that the ElGamal encryption scheme is semantically secure and the Gentry-Ramzan PIR has client security, our protocol has client security, i.e., the server cannot distinguish any two queries of the client from each other.

Server's Security

Intuitively, the server's security requires that the client can retrieve one record only in each query to the server, and the server must not disclose other records to the client in the response. Our protocol achieves the server's security in the oblivious transfer phase, which is built on the Naor-Pinkas oblivious transfer protocol

Theorem4. Assume that the discrete logarithm is hard and the Naor-Pinkas protocol is a secure oblivious transfer protocol, our protocol has server security.

PERFORMANCE ANALYSIS

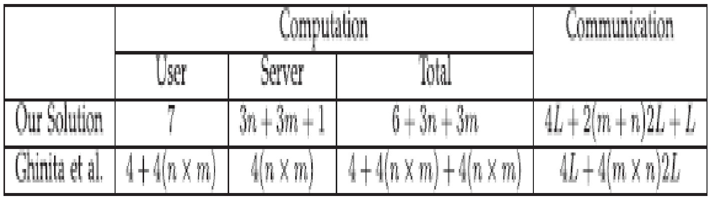
We now analyse the performance of our solution and show that it is very practical. The performance analysis consists of the computation analysis and the communication analysis. We supplement this analysis with a comparison with the protocol

Computation

Since the most expensive operation in our protocol is the modular exponentiation, we focus on minimising the number of times it is required. We assume that some components can be precomputed, and hence we only consider the computations needed at runtime. Furthermore, we reduce the number of exponentiations required by the PIR protocol to the number of multiplications that are required. This will make the computational comparison between our solution and the solution of Ghinita

TABLE 1

Stage 1 Performance Analysis Summary



	Computation			Communication
	User	Server	Total	
Our Solution	7	$3n+3m+1$	$6+3n+3m$	$4L+2(m+n)2L+L$
Ghinita et al.	$4+4(n \times m)$	$4(n \times m)$	$4+4(n \times m)+4(n \times m)$	$4L+4(m \times n)2L$

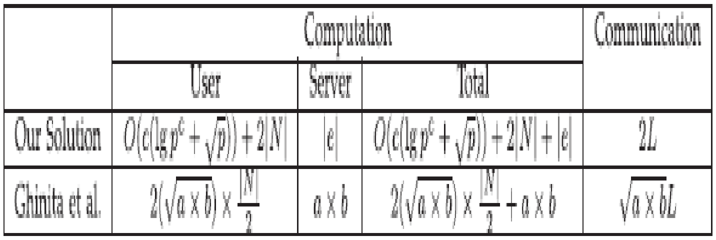
Communication

Since we require the discrete logarithm to be intractable for security reasons, we set q_ to be 1024 bits, which makes p roughly 1025 bits. Since q_ and p are about the same size we set a common L as 1024 bits for analysis. In our proposed solution, the user needs 4L communications, while the server requires 2(m + n)2L + L communications in the oblivious transfer protocol. In the PIR protocol, the user and server exchange one group element each.

EXPERIMENTAL EVALUATION

We implemented our location based query solution on a platform consisting of: a desktop machine, running the server software of our protocols; and a mobile phone, running the client software of our protocols.

TABLE 2
Stage 2 Performance Analysis Summary



	Computation			Communication
	User	Server	Total	
Our Solution	$O(c(\lg p^c+\sqrt{p}))+2\|N\|$	$\|e\|$	$O(c(\lg p^c+\sqrt{p}))+2\|N\|+\|e\|$	$2L$
Ghinita et al.	$2(\sqrt{a \times b}) \times \frac{\|N\|}{2}$	$a \times b$	$2(\sqrt{a \times b}) \times \frac{\|N\|}{2}+a \times b$	$\sqrt{a \times b}L$

CONCLUSION

In this paper we have presented a location based query solution that employs two protocols that enables a user to privately determine and acquire location data. The first step is for a user to privately determine his/her location using oblivious transfer on a public grid. The second step involves a private information retrieval interaction that retrieves the record with high communication efficiency. If there are many opportunities available for sensor initialization, however, the new method may increase errors resulting from the synchronization of each sensor and the reliability level tends to depend on the type of sensor. Furthermore, for high reliability, reference objects need to be entered into map data in advance. Despite these shortcomings, however, if the reliability level is set based on empirical or experimental data, we can build a positioning system of high reliability at a relatively low cost compared to network size.

References

1. Ssu, K.F., Ou, C.H., Jiau, H.C.: Localization with mobile anchor points in wireless sensor networks. IEEE Trans. on Vehicular Technology 54(3), 1187–1197 (2005)

2. Hu, L., Evans, D.: Localization for mobile sensor networks. In: Proc. of ACM MobiCom (2004)

3. Song, C.W., Ma, J.L., Lee, J.H., Chung, K.Y., Rim, K.W.: Localization Accuracy Improved Methods Based on Adaptive Weighted Centroid Localization Algorithm in Wireless Sensor Networks. International Journal of Computer Science and Information Security 8(8), 284–288 (2010)

4. Laurendeau, C., Barbeau, M.: Centroid localization of uncooperative nodes in wireless networks using a relative span weighting method. EURASIP J. Wirel. Commun. Netw. (2010)

5. Nagpal, R., Shrobe, H.E., Bachrach, J.: Organizing a global coordinate system from local information on an ad hoc sensor network. In: Zhao, F., Guibas, L.J. (eds.) IPSN 2003. LNCS, vol. 2634, pp. 333–348. Springer, Heidelberg (2003)

6. Niculescu, D., Nath, B.: DV based positioning in ad hoc networks. Journal of Telecommunication Systems 22(4), 267–280 (2003)

7. Kim, Y.C., Kim, Y.J., Chang, J.W.: Distributed Grid Scheme using S-GRID for Location Information Management of a Large Number of Moving Objects. Journal of Korea Spatial Information System Society 10(4), 11–19 (2008)

8. Lee, Y.K., Jung, Y.J., Ryu, K.H.: Design and Implementation of a System for Environmental Monitoring Sensor Network. In: Proc. Conf. APWeb/WAIM Workshop on Data- Base Management and Application over Networks, pp. 223–228 (2008)

9. Hammad, M.A., Aref, W.G., Elmagarmid, A.K.: Stream window join: Tracking moving objects in sensor network databases. In: SSDBM (2003)

10. Niculescu, D., Nath, B.: Position and orientation in ad hoc networks. Ad hoc Networks 2(2), 133–151 (2002)

11. Chen, Y., Pan, Q., Liang, Y., Hu, Z.: AWCL: Adaptive weighted centroid target localization algorithm based on RSSI in WSN. Proc. IEEE ICCSIT 9, 9–11 (2010)

12. Wang, J., Urriza, P., Han, Y., Cabrić, D.: Performance analysis of weighted centroid algorithm for primary user localization in cognitive radio networks. In: Proc. ACSSC, Pacific Grove, pp. 7–10 (2010)