Simulation of 3D Privacy Preservation and Location Monitoring approach

Rohit Kumar[1], Dr. Sudhir Dawra[2]

[1]*Research Scholar, Sunrise University, Alwar Email-id: mtechrohit@gmail.com*
[2]*Professor, Ideal Institute of Technology, Ghaziabad Email-id: dawra1211@gmail.com*

---***---

Abstract - *Location Monitoring Systems when propel a personal location data to unfaithful server, it may cause a privacy threat to the monitored objects. A 3D privacy preserving location monitoring system for WSN(wireless sensor networks) is used to conserve the privacy of the monitored objects in multi floor-multi section building and to provide the monitoring services to the system users.*

In this system, two location anonymization algorithms, namely, 3D resource-aware and 3D quality-aware algorithms are used. Using these algorithms the system is able to provide high type of quality location monitoring services for system users, whereas preserving personal location privacy. Both of the algorithms uses well established k-anonymity privacy concept to preserve the privacy of monitored objects. By using these algorithms the sensor nodes can present the aggregate information for location of the monitored persons to the containment resolver which after resolving containment sends this information of aggregate location to the server. Each cumulative location is in the form of a 3D monitored area A alongside with the number of objects residing in A, where A comprises at least k number of objects.

The 3D resource-aware algo. minimizes communicational and computational price, whereas the 3D quality-aware algo. is used for maximizing the accurateness of the aggregate locations by minimizing their area of monitoring. For utilizing the aggregate location information to give location monitoring services, here we use a 3D spatial histogram strategy that estimates the distribution of the monitored objects in multi floor-multi section building. So by using blur area of objects we can protect the privacy of the person residing in a Sensitive area.

Key Words: *Location privacy, wireless sensor networks, location monitoring system, aggregate query processing.*

1.INTRODUCTION

In the provisions of system structural design, present spatial cloaking techniques would be classified into centralized, peer-to-peer and distributed looms. In common, the centralized loom suffers from the inside attacks, whereas the distributed loom assumes that movable users converse with the each other throughout base stations is not relevant to the wireless sensor network. Even though the peer-to-peer loom could be concerned to wireless sensor network(WSN), the earlier work using this loom merely spotlight on the hiding a solitary user position with no straight applicability to the sensors-based 3D location monitoring.

Location Tracking Systems (LTS) gather location information silently, without the consent or even the consciousness of individuals. LTSs use a number of varieties of technologies to make record the locations of objects. A Location Tracking System can increase the risks to the security and privacy of individuals.

Our system propsed wireless sensor networks (WSN) by using a privacy-preservation location monitoring system to preserve the privacy of spatial monitored objects and to provide monitoring services. This system uses well established k-anonymity privacy concept. In this method, each sensor make a cloaked area by making blurs its sensing area, where at least k objects are livening. Cumulative location information is reported by each sensor, which make a form of 3D cloaked sensing area, A, beside with the number of objects or persons, N, Situated in Area A. Here a middle tier entity called Containment-Resolver is proposed which accepts the information of aggregate location for monitored objects from the sensor nodes and after resolving containment, sends this resolved information to the server with no. of K-Failures[1].It is noteworthy to take a note on the value of k accomplishes a difference between the firmness of privacy protection and the worth of monitoring services. If a smaller cloaked area reported by the sensors ,it represent a lesser value of k which indicate less privacy preservation as a minor cloaked area is reported by the sensors , therefore it increase monitoring service to that area. In contrast a large value of k decreases the quality of monitored area service but improve the privacy of the objects or persons and obviously privacy protection. By using this system we can avoid the privacy leakage by providing low quality monitoring services for small areas whereas for large areas we will provide a good quality monitoring service so that the rival cannot abuse or track the user[2]. This proposed system also considers the Z co-ordinate for cloaking the area in spatial systems (e.g. Multi-floor Buildings) to preserve the privacy. This also results in high privacy as compare to the privacy provided by the systems that uses the cloaking area shown by only X and Y coordinates (i.e. cloak the area of the same floor only) to

1. Preserve the privacy of monitored objects in multi-floor and multi-section buildings
2. Find out the accuracy of monitoring services provided in 3D space while preserving the privacy of monitored objects.

3. Analyze the location anonymization algorithms in different scenarios like sparse, dense or general environments.
4. Results will be compared with our expected results.
5. Check performance analysis to prove the feasibility of our problem statement.

Current work of privacy preservation in wireless sensor networks cloaks the area of the same floor i.e. area is shown only by X and Y co-ordinates. It doesn't consider the area of different floors means no Z co-ordinate considerations.
In this paper, we presented two main classes or methods for privacy preservation for saving two type of information. First one is data based and second is context based privacy. For saving data based privacy, we focus to aggregate the data sensed by the sensors, so that rival could not collect exact data. On the other hand, for context based privacy we used a blur area known as MBR (Maximum Bounding Rectangle Area). For improve the accuracy we used k- anonymous approach.

2. PROPOSED CONTAINMENT RESOLVER ALGORITHMS

Sensor nodes send aggregate location data found by location anonymization algorithms to a middle tier entity containment resolver[3]. It resolved containment by using containment resolution algorithms and send data to server.

The Containment Resolver is accountable for the gathering aggregate locations details from the sensor nodes and later than resolving containment it sends information to server.

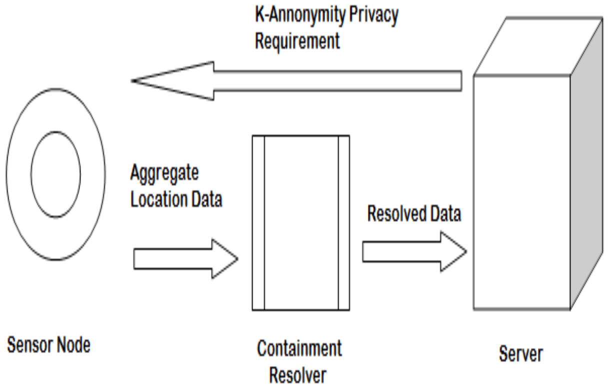


Fig -1: Containment Resolver

2.1 Containment Resolution by Max Object Count

This algorithm find how many times m's sensing area is contained by cloaking area of other sensor nodes and select max object count of m among all object counts.

Algorithm 1
Containment Resolution by Max Object Count

```
1: For Each sensor node m
2: Send aggregate area A and aggregate object count N to the Containment Resolver
3: Containment Resolver randomly redistributes N into aggregate area A or no. of blocks
4:Find how many times m's sensing area is contained by cloaking area of other sensor nodes and object count of m in that aggregate cloaked area.
5: Select max object count for m among all object counts of m.
6: Then find new aggregate object count N for sensor node m.
```

2.2 Containment Resolution by Average Object Count

This algorithm find how many times m's sensing area is contained by cloaking area of other sensor nodes and select average object count of m.

Algorithm 2[4]: Containment Resolution by Average Object Count

```
1: For Each sensor node m
2: Send aggregate area A and aggregate object count N to the Containment Resolver
3: Containment Resolver randomly redistributes N into aggregate area A or no. of blocks
4: Find how many times m's sensing area is contained by cloaking area of other sensor nodes and object count of m in that aggregate cloaked area.
5: Find average object count for sensor node m.
Average object count = Total object count of m in all aggregate areas No. of repetitions of m
6: Then find new aggregate object count N for sensor node m.
```

3. STAGES FOR CURRENT RESEARCH WORK

3.1 First Stage

i. Understanding of object monitoring in Wireless Sensor Networks.
ii. Finding out importance of privacy preservation in object monitoring systems in WSN.
iii. Finding out requirements and need of privacy preservation in object Monitoring systems in WSN.

3.2 Second Stage

iv. Study and understanding of different aspects of privacy preservation in object monitoring systems.
v. Study of location anonymization Algorithms.
vi. Suggested to use Z co-ordinate also instead of using only X & Y co-ordinate to enable the system to work in 3D space.

3.3 Third Stage

vii. Theoretical understanding of Experimental setup, environment and evaluation of system design.
viii. Show the system model in 3 Dimensions. Processing software is used to show the system in 3D. The main advantages of this software are simplicity, open source code, free product, wide documentation on the web and supporting most of the frequently used protocols. For

these reasons processing software is chosen for this project.

ix. Study of existing patches which support random object movement generation patterns and varying mobility speed of objects for JAVA.

3.4 Fourth Stage

x. Implement Algorithm by using JAVA and Processing software.

xi. Experiments and measurements.

3.5 Fifth Stage

xii. Result and graph analysis.

xiii. Closing, Documentation/reports and publications.

4. Architecture Diagram

The paper is mainly concerned to implement an algorithm that preserves privacy of monitored objects in WSN in spatial systems and also makes the system enable to provide monitoring services to system users[5][7].

The application takes input No. of objects, mobility speed of objects and k-anonymity privacy requirement from the user and preserves privacy of monitored objects. In case failed to preserve privacy report K-Failure

The application provides three main utilities:

1) 3D Building structure: This 3D space structure is nothing but the scenario in which we want to apply these algorithms to give the desired output.

2) Processing Software: Which accepts the inputs from server admin or system users and apply all the constraints of privacy preservation using location anonymization algorithms and produce the expected privacy preserved monitoring services in 3D space.

3) Performance Analysis: This gives the output in text file which trace out desired fields of the trace file.

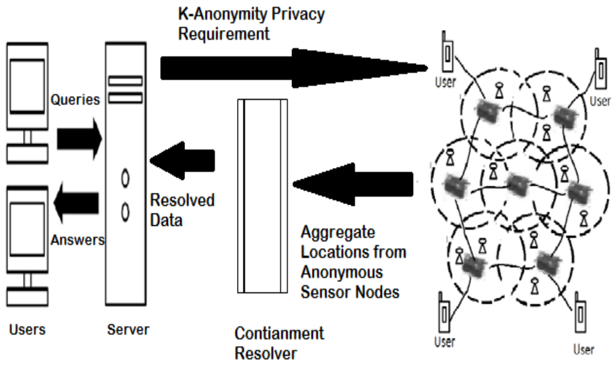


Fig -2: System Architecture

4.1SYSTEM MODULES

1) Sensor nodes.
2) Containment Resolver
3) Server
4) System users
5) Location Anonymization
6) Spatial Histogram

Server

Spatial Histogram is used to calculate the distribution of monitored objects or persons by the server and server is authorized for collecting the location data which is reported by Containment Resolver.

This data is used for answering series queries based on the distribution of objects. Apart from this the k-anonymity level can be changed at any time by the admin. For this he just needs to send a message with a new value of k to the entire sensor node.

System users

The queries can be made by users and authentic admin to the system either to serve or nodes, as shown. For answering these queries the server uses spatial histogram.

Location Anonymization

To preserve personal location privacy, two aggregate location anonymization algorithms, namely, 3D resource- and 3D quality-aware algorithms are used. Both algorithms need the sensor nodes to work together with each other to blur their sensing areas A into cloaked areas, in this way that each cloaked area contains at least k number of persons to comprise a k-anonymous cloaked area A[6]. The resource-aware algorithm targets to minimize communication as well as computational cost, whereas the quality-aware algorithm targets to reduce the size of the cloaked areas A, in order to make the most of the accuracy of the aggregate locations detailed to the Containment Resolver. In the resource-aware algorithm, every sensor node finds a sufficient number of persons or objects, and then it utilizes a greedy approach to get a cloaked area. On the other side, the quality-aware algorithm begins from a cloaked area A, which is calculated by the resource-aware algorithm. Then area A will be periodically refined based on additional communication among the sensor until its area arrives at the minimum possible size. For both of the algo., the sensor node informs its cloaked area A with the number of monitored persons or objects in the area as an aggregate location to the containment resolver. In case failed to preserve the privacy both algorithms reports K-Failure.

Spatial Histogram

Even though this type of system can only identify the aggregate information about the monitored objects or persons, still we can get the monitored services meanwhile answering the aggregate queries for E.g. The number of persons residing in a certain area? For supporting these type of monitoring services, a histogram could be used to analyzes the collected aggregated location information to estimate the distribution of the monitored objects or persons in the system[9]. The estimated distribution is used to answer these aggregate queries.

4.2. System flow diagram

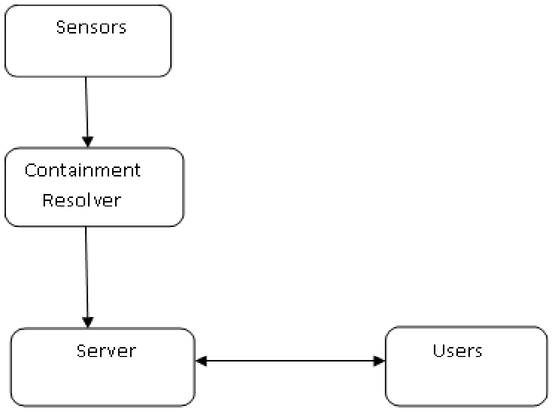


Fig -3: System Flow Diagram[5]

5. P TOOL DESIGN

P-tool is stands for Processing-tool. It was developed by MIT media lab in USA. We select this tool for showing the simulation of our project. As this tool is best tool for showing visual and graphical representation. This tool supports many languages. We use java as a implementation language. This tool is so much ease in use. The tool is available for various Operating Systems like Windows, Linux and Macintosh. We need Processing tool to implement 3D resource aware algorithm and 3 D quality aware algorithm[11].

For the simulation purpose we used Processing tool. Processing is open source tool. The tool is primarily focused for visual or graphical simulations. The work is carried by Ben Fry and Casey Reas. The basic concept of this tool is sketch book. The file created by this tool is known as sketch book. The tool can used many languages like java, android etc. When processing was developed, the first language which supports it was the processing language itself. This language was influence by BASIC and Logo.

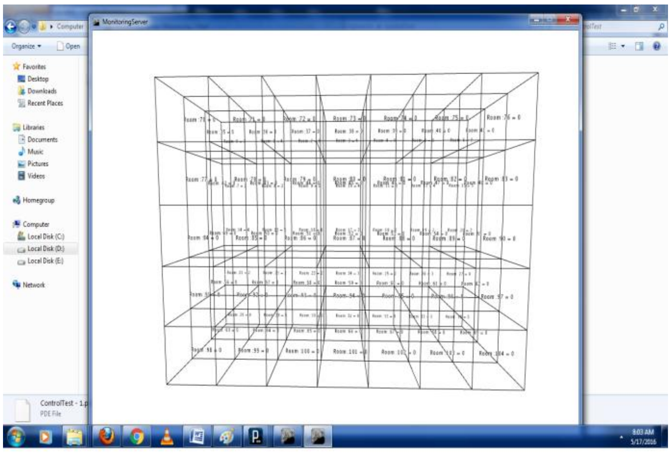


Fig -4: Monitoring the server

To have a keen look over the data, we set up a server, which stores all the information. The log data can be seen on the console window also. The next snapshot also depicted this consol window.

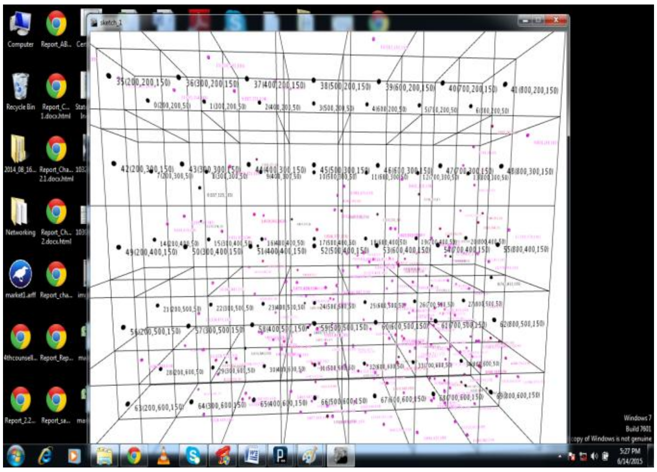
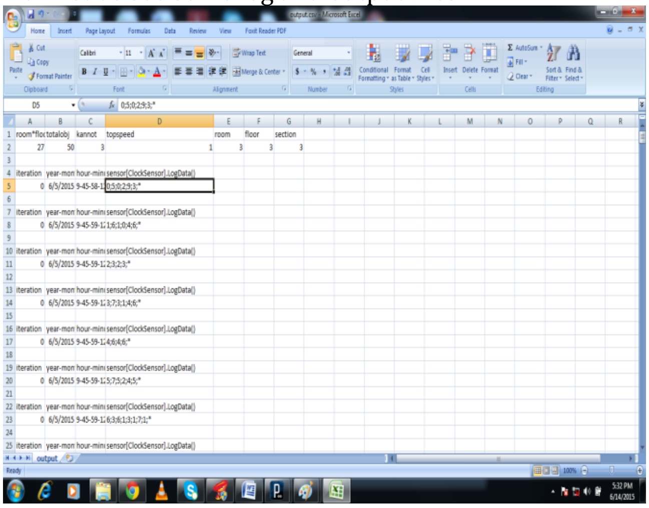


Fig -4: Simulation with co-ordinate

We assume that all the devices attached to the system will work properly without failure. Software and hardware assumptions are expected to be stable.

Now let us see some log and output files

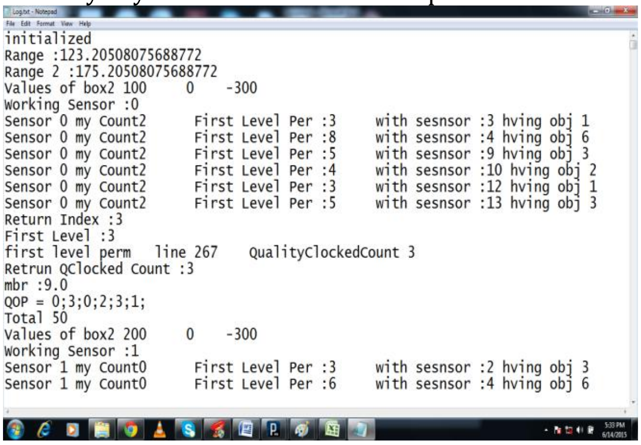


D5 0;5;0;2;9;3;*

	A	B	C	D	E	F	G
1	room*floc	totalobj	kannot	topspeed	room	floor	section
2	27	50	3	1	3	3	3
3							
4	iteration	year-mon	hour-mini	sensor[ClockSensor].LogData()			
5	0	6/5/2015	9-45-58-1	0;5;0;2;9;3;*			
6							
7	iteration	year-mon	hour-mini	sensor[ClockSensor].LogData()			
8	0	6/5/2015	9-45-59-1	1;6;1;0;4;6;*			
9							
10	iteration	year-mon	hour-mini	sensor[ClockSensor].LogData()			
11	0	6/5/2015	9-45-59-1	2;3;2;3;*			
12							
13	iteration	year-mon	hour-mini	sensor[ClockSensor].LogData()			
14	0	6/5/2015	9-45-59-1	3;7;3;1;4;6;*			
15							
16	iteration	year-mon	hour-mini	sensor[ClockSensor].LogData()			
17	0	6/5/2015	9-45-59-1	4;6;4;6;*			
18							
19	iteration	year-mon	hour-mini	sensor[ClockSensor].LogData()			
20	0	6/5/2015	9-45-59-1	5;7;5;2;4;5;*			
21							
22	iteration	year-mon	hour-mini	sensor[ClockSensor].LogData()			
23	0	6/5/2015	9-45-59-1	6;3;6;1;3;1;7;1;*			
24							
25	iteration	year-mon	hour-mini	sensor[ClockSensor].LogData()			

Fig -5: Output.csv

Processing expert and OpenGL are free open source can be used by any one. All class files are depends on each other.



```
initialized
Range :123.20508075688772
Range 2 :175.20508075688772
Values of box2 100     0    -300
Working Sensor :0
Sensor 0 my Count2      First Level Per :3      with sesnsor :3 hving obj 1
Sensor 0 my Count2      First Level Per :8      with sesnsor :4 hving obj 6
Sensor 0 my Count2      First Level Per :5      with sesnsor :9 hving obj 3
Sensor 0 my Count2      First Level Per :4      with sesnsor :10 hving obj 2
Sensor 0 my Count2      First Level Per :3      with sesnsor :12 hving obj 1
Sensor 0 my Count2      First Level Per :5      with sesnsor :13 hving obj 3
Return Index :3
First Level :3
first level perm    line 267    QualityClockedCount 3
Retrun QClocked Count :3
mbr :9.0
QOP = 0;3;0;2;3;1;
Total 50
Values of box2 200     0    -300
Working Sensor :1
Sensor 1 my Count0      First Level Per :3      with sesnsor :2 hving obj 3
Sensor 1 my Count0      First Level Per :6      with sesnsor :4 hving obj 6
```

Fig -6: Log.txt

The system is dependent on Java, Processing-2.0, OpenGL, controlP5 library. As Java, Processing and OpenGL are open source all dependencies must be checked before simulating. Sometimes may be memory size e.g. heap memory for Java when using large no. of objects.

Proposed Algorithms are used in WSN network to preserve the privacy in 3D space. These algorithms will be executed simultaneously in all sensor nodes which find out aggregate location and the containment resolver is used to minimize the containment. Analyze the effect of various containment resolution algorithms in terms of total no. of objects in system and total k-failures.

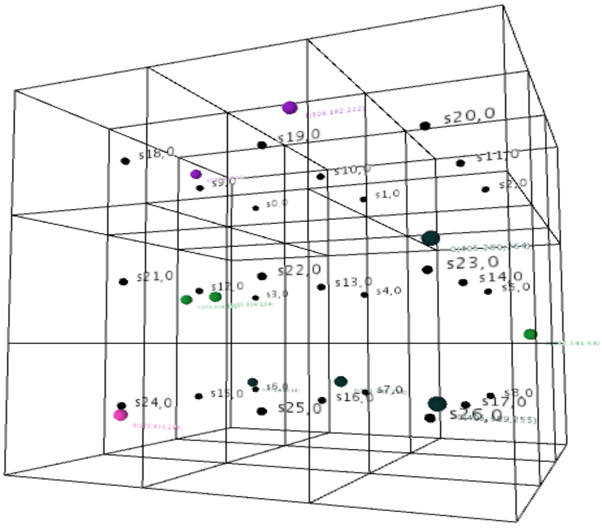


Fig -7: 3D environment

6. CONCLUSIONS

A 3D privacy preserving location monitoring system for wireless sensor networks is used to preserve the privacy of monitored objects in 3D space (e.g. multifloor -multisection building) and to provide the monitoring services to the system users. We used a 3D spatial Histogram method to use aggregate location information for providing location monitoring services, which calculate the distribution of the monitored objects or persons in a multi floor or multi section building. We used this estimated distribution in answering a wide range of queries. The system is shown in 3D.

Since we are considering the X, Y and Z co-ordinate also to show the area which is being cloaked, we can use the system to preserve the privacy of monitoring objects in 3D space which is the new initiative in this area.

Now the system evaluate the performance of 2D privacy-preserving location monitoring system and 3D privacy-preserving location based monitoring system for (WSN) wireless sensor networks used for multi-floor buildings.

Our research work is progressing to implement the system that can be used for buildings having any room sizes.

ACKNOWLEDGEMENT

Authors like to thank Dr. V.K. Agarwal, Chancellor Sunrise University and Dr. Anup Pradhan, Director Research for providing research facilities in Sunrise University Campus.

REFERENCES

[1] C.-Y. Chow, M.F. Mokbel, and X. Liu, “A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks,” IEEE Trans. Mobile Computing, vol. 10, NO 1, Jan 2011.

[2] Hairuo Xie, Lars Kulik, and Egemen Tanin “Privacy-Aware Traffic Monitoring,” IEEE Transactions On Intelligent Transportation Systems, VOL. 11, NO. 1, MARCH 2010.

[3] Marco Gruteser and XUAN LIU “Protecting Privacy in Continuous Location-Tracking Applications”, IEEE SECURITY & PRIVACY , MARCH/APRIL 2004.

[4] Haibo Hu, Jianliang Xu, Senior Member, IEEE, and Dik Lun Lee “PAM: An Efficient and Privacy-Aware Monitoring Framework for Continuously Moving Objects,” IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 22, NO. 3, MARCH 2010.

[5] Jessa Liying Wang and Michael C. Loui “Privacy and Ethical Issues in Location-Based Tracking Systems,” IEEE Conference on Intelligent Transportation, May 2009.

[6] I. Krontiris, F. C. Ferling, T. Dimitriou, “Location Privacy in Urban Sensing Networks: Research Challenges and Directions” IEEE Wireless Communications , Oct. 2010

[7] B. Gedik and L. Liu, “Protecting Location Privacy with Personalized K-Anonymity: Architecture and Algorithms,” IEEE Trans. Mobile Computing, vol. 7, no. 1, pp. 1-18, Jan. 2008.

[8] B. Bamba, L. Liu, P. Pesti, and T. Wang, “Supporting Anonymous Location Queries in Mobile Environments with Privacygrid,” Proc. Int’l Conf. World Wide Web (WWW), 2008.

[9] C.-Y. Chow, M.F. Mokbel, and X. Liu, “A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-Based Services,” Proc. 14th Ann. ACM Int’l Symp. Advances in Geographic Information Systems (GIS), 2006.

[10] H. Kido, Y. Yanagisawa, and T. Satoh, “An Anonymous Communication Technique Using Dummies for Location-Based Services,” Proc. Int’l Conf. Pervasive Services (ICPS), 2005.

[11] M.Gruteser and D. Grunwald, “Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking,” Proc. ACM MobiSys, 2003.