ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 89- 94 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp18.pdf

UNAUTHORIZED USERS RESTRICT TO ACCESS SHARED USERS LOCATING DETAILS FORM SOCIAL MEDIA

K. Vineesha [1], K. Alluraiah [2]
[1] *M.Tech Student,* [2]*Associate professor, Dept. of CSE, SVCE, Tirupathi.*
[1] *vini.kuppam@gmail.com,*
[2] *Alluraiah.k@svcolleges.edu.in,*

ABSTRACT:

Social Media is an application software's where large no of worldwide scattered users are connecting to the network and share the current details to their friends, relatives and community members. Opinions are posted by members on shared messages. Within this entire process, there is no security for individual privacy that is nothing but the lack of freedom to share their private messages to authorized community members. Instead of utilizing it properly, Most of the people misuse this application for fall up the users to do harm and in some cases their especially focus them for a long period of time to make attacks on their properties with proper planning. To overcome these problems, we newly designed an alternative approach which enhances the security of resulting user's location private details from unauthorized user access without losing its originality from the server. Our approach shares the information to specified users, preserve the distance coordinate transformations to all location data shared with the server. It accepts different location queries and makes it as confidential, even if the server wants to see that particular content. We integrate our proposed functionality with modern mobiles and PC'S to test network latency and performance.

Keywords: - Security, location-based social applications, location conversion.

I. INTRODUCTION

Rapid advancements change the life style of humans and smart phone features, devices with effective processing power. In the last few years the utilization of telephones and mobiles are drastically increased compared to earlier days usage is very less. In previous application facilitates the user to recover important content in their present area (e.g., Reason of Findings (ROFS)). All most a lot of Geo-social application are started showing up and supported social media associated between clients those how are near to the topographically nodes in the communication range. Suppose, for example, friends posted their achievements and share their celebration moments with the surrounding area people like friends, relatives, etc. is there in the community meeting individually through online application like e.g., Google Scope and Foursquare. These applications provide a facility to gather their forget friends and relative. Moreover, these apps introduces and create new relation with unanimous persons if their opinions and interests match with each other. It bonds a relative environment one to each other. At the same time some security problems also there with these Geo-social applications. Some people those how harsh the users with some unparliamentarily word posted on the website walls. Based on their current status online apps of user's thief's May theft valuable things by reburying their houses. To server the on-demand requests to the intend applicant, client has to give their area details and these details are misused by gimmicking. Applications provides a lot of information about the area along with timestamp representation is must when a client made a request. With the help of this information supplier allow the user to access the requested services. While this transaction processes required the location details of user by conforming their location details with user then supplier provide their service to the intend user. In this process, only intend client can track their details, but not other people. The application has develop like these to allow only authorized users, but not unauthorized one.

In the same way supplier might know the difference between data and characteristics of clients in the community and a piece of their bio data in social applications. These details are required for verification, allocation the request service purpose, but for personal usage. The application has to take safety precautions to disconcerates on clients' data like personal and official areas, exercises and connections details divert from a supplier point of view. Otherwise, anonymous people can focus on shared information of client's home area, monitoring their activities and behaviours. This information may give to outside persons by getting some profit from them outside one.

II. SCENARIOS AND REQUIREMENTS

Few situations are there to describe the social network context which resulting that users are interact heavy with friends through social media. It clearly imposes that social application required application privacy protection.

A. Geo-social Application Scenarios leverage

Scenario 1: Y and his associates enthusiastically initiate to discover latest things in their city and a latest john and associates are eager about discover to do latest activities in their leaving city and named that program as "Associate referrals" many local businesses offer some funds to this community. At present, John is a downtown person looking to start a new activity in her surrounding area. But other women seek to start an activity provide more discount. Were the discount is high a user shown their interest that and refer more friends get high referral discounts. As a result John finds out and planning to do some other business recommended by her friends and discount is getting by them in their surrounding area. That until she is also gathering there the discount available among others compared to her favourite restaurant in a given location

Scenario 2: We have understandable a problem that arises while processing nearest neighbour queries by applying this technique gives exact results of all real neighbours. By evaluating this technique by using Hilbert curves shows that it determine approximate neighbours only. But if we want to find a real neighbour it requires earlier work is maintained by proxy in between transformation location to actual locations and enhances the processing query performance. It needs Trusted Third Parties to verify the user location privacy details transfer between client and LBSA Servers. LocX fulfil this gap by employing trust third party it does not trust unauthorized users make to their notice. It transfers location details which are not related to actual user location details to mislead the unauthorized users. Our proposed system is under finding to hide the actual neighbours and their favourite resistant details against two attacks based queries

B. System Requirements:

To bring the location preventing feature to already existing social media application following things are required to secure the identities of user as well as location details:

- To provide robust location privacy hides few details like history of locations that a user visited frequently while processing the data from the several server.
- Server maintain some services server confuse for link the user to particular
- If information belongs to the same user services restrict the connection to prevent them from attacks.
- Location data privacy. The servers should not be able to view the content of data stored at a location.
- It maintains location wise data privacy which doesn't allow the server to view the location information details.
- Elasticity and scalability point of view it support circular range and nearest neighbor users queries can access the location data to provide the service to request user.
- In terms of performance it won't compromise any where while computation, bandwidth and network latency to support large scale mobile users.

III. RELATED WORK

A. Prior Work on Privacy in General Location Based Service

We are mainly concentrating on three types of proposals which preserve the location confidentiality. In general, it protects privacy through LBSs approach but it doesn't intensely design for social applications. At Initial stages spatial and temporal Cloaking are there to locate rough locations and time details are send to the server instead of accurate values. It hides the location identities among a bunch of users called K-anonymity and it enhances the privacy. But it disappoints the users expected accurate results and response delay from the server. If attacker made simple attacks on this approach it can't sustain for long period of time and leak the user confidentiality.

Pseudonyms and silent times are alternate methods to complete cloaking. Here subscribers are moving from one place to another place and data transfer will not sustain for long period of time in a regular intervals. Users are disappointed for this type of services. Main intension of this approach is to maintain trusted parties or trusted servers broadcast rough location details to the server in plain text form. We don't trusting any intermediaries or servers in this approach because it is a general solution for tracking the locations. LocX are mainly designed for modern social network application which prevents the location privacy and maintain location coordinates securely. We have understandable a problem that arises while processing nearest neighbour queries by applying this technique gives exact results of all real neighbours. By evaluating this technique by using Hilbert curves shows that it determine approximate neighbours only. But if we want to find a real neighbour it requires earlier work is maintained by proxy in between transformation location to actual locations and enchance's the processing query performance.

B. Prior Work on Privacy in GeoSocial Services

A buddy tracker service is required to find out nearest neighbor friends make them connect to social networking sites. Few modern proposals prove that protecting location privacy is costliest technique for securing two parties communication. To overcome from this, LocX uses symmetric encryption and pseudorandom key generators are inexpensive to serve large scale users.

LocX has to do the prior work for location the user that is Latitude and Longitude which is required to identify a user position and make to coordinate with server by hiding the user's identities. However Latitude and Longitude details are maintained as confidential, in case if two parties are communicating with each other. If system reveal the position details to any one of his friend there may be a chance to leak privacy breaches to the downstream friends. There is a small gap for LocX is that if we share a message to friends will share that message to remaining community members but it maintain individual confidently between the users and friends.

LocX has few goals attain it for fast locating and unlink ability. It provides flexibility to support few features like recommendations, reminders, and others, than just buddy tracking.

C. Anonymous Communication Systems

The system support anonymous users with the help of Tor route them LBSA server these systems, including Tor [34], provide anonymity to users during network activity. One might ask, then, why using Tor to anonymously route data to LBSA servers is not sufficient. This approach seems to provide privacy as the server only sees location data but not the identity of the user behind that data. However, recent research has revealed that hiding the identity of the users alone is not sufficient to protect location privacy. Even if Tor is used, it is possible for an attacker with access to the location data to violate our privacy and unlinkability requirements. For example, using anonymized GPS traces collected by the servers, it has been shown that users' home and office locations, and even user identity can be derived [23], [24], [25], [26]. These approaches are suitable for spatial data outsourcing or data mining scenarios where the data are static and are owned by limited number of users. But they are less suitable for LBSAs, where the data are dynamic and personal, and thus cannot be encrypted under a single secret key. Applying Persona's mechanisms to LBSAs directly would encrypt all location coordinates, making LBSAs unable to process nearest-neighbor queries. But if location is not encrypted, attacks using anonymized GPS traces, mentioned above, can succeed, making Persona insufficient to protect location privacy. Similarly, Adeona is useful for a user to retrieve her own data, but not the data from her friends. Our contributions complement these systems. Some techniques in these papers can help LocX as well, for example,

IV. SYSTEM DESIGN

A. Basic Design

If a user pose different types of query server is in a position to support it on the basis of location data. If a query hits the server, it can able process that request at any particular situation. Server reveal the location coordinates details in the origin plain text for trusted users only. While doing these malicious servers breaks the user's location privacy. To overcome this problem, we introduced a new idea of coordinate transformation. If a user wants to share his secrets to their friends our system allows only them access those details. These secrets include a rotation angle θu, a shift bu, and a symmetric key symmu. The users exchange their secrets via interactions when friends meet in person, or via a separate trusted channel, such as email, phone etc. The secret angle and shift are used by the users to transform all the location coordinates they share with the servers. Similarly, the secret symmetric key is used to encrypt all the location data they store on the servers. These secrets are known only to the friends, and hence only the friends can retrieve and decrypt the data. For example, when a user u wants to store a review r for a restaurant at (x, y), she would use her secrets to transform (x, y) to (x1, y1) and store encrypted review E(r) on the server. When a friend v wants to retrieve u's review for the restaurant at (x, y), she would again transform (x, y) using u's secret (previously shared with v), retrieve E(r), and then decrypt it using u's symmetric key to obtain r. Similarly, v would transform (x, y) according to each of her friends' secrets, obtain their reviews, and read them. We only focus on point queries for now. Figure 1 depicts this basic design.

Limitations.

This basic design has one important limitation: the server can uniquely identify the client devices (for *e.g.*, using the IP address). Using this, the server can associate different transformed coordinates to the same user (using the IP). Sufficient number of such associations can break the transformations (as we show in Section 5). So maintaining unlink ability between different queries is critical. One approach to resolve this limitation is to route all queries through an anonymous routing system like Tor [34]. But simply routing the data through Tor all the time will be inefficient. Especially in the context of recent LBSAs, that adds larger multimedia files (pictures and videos) at each location. So we need to improve this basic design to be both secure and efficient. Fig. 1 A basic design

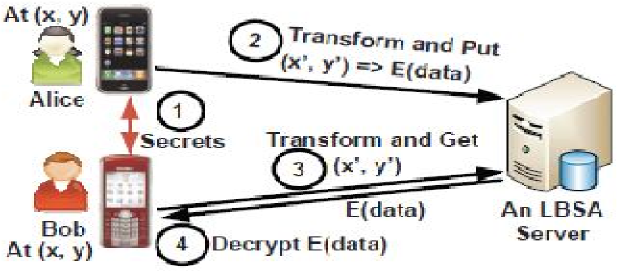


Fig. 1 Basic Design

In the basic design
1) Jhon and James exchange their secrets
2) Jhon stores her review of the restaurant (at (x, y)) on the server under transformed coordinates,
3) James later visits the restaurant and queries for the reviews on transformed coordinates,
4) Decrypts the reviews obtained.

B. Overview of LocX

LocX builds on top of the basic design, and introduces two new mechanisms to overcome its limitations. First, in LocX, we split the mapping between the location and its data into two pairs: a mapping from the transformed *location to an encrypted index* (called **L2I**), and a mapping from the *index to the encrypted location data* (called **I2D**). This splitting helps in making our system efficient. Second, users store and retrieve the L2Is via *untrusted proxies*. This redirection of data via proxies, together with splitting, significantly improves privacy in LocX. For efficiency, I2Ds are not proxied, yet privacy is preserved

1. Decoupling a location from its data:

Location data data(x, y) corresponding to the real world location (x, y) is stored under (x, y) on the server. But in LocX, the location (x, y) is first transformed to (x1, y1), and the location data is encrypted into E(data(x,y)). Then the transformed location is decoupled from the encrypted data using a random index i via two servers as follows:

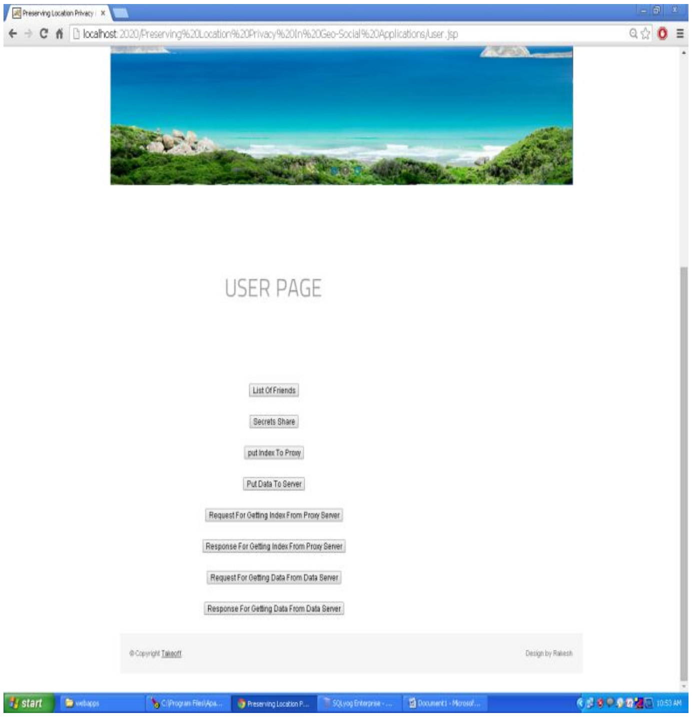
1) AN L2I = [(x1, y1),E(i)],which stores E(i) under the location coordinate (x1, y1), and
2) AN I2D = [i,E(data(x,y))], which stores the encrypted location data E(data(x,y)) under the random index i.

The index is generated using the user's secret random number generator. We refer to the server storing L2Is as the *index server* and the server storing I2D as the *data server*. We describe these two as separate servers for simplicity, but in reality they can be on the same server, and our privacy properties still hold. This separation of location information into two components (L2I and I2D) helps us continue to efficiently run different types of location queries on L2Is and retrieve only relevant I2Ds. Figure 2 depicts the design of LocX.

1) Jhon and James exchange their confidential data, 2) Jhon dynamically creates and L2I and I2D from her review of the restaurant at (x, y)), and stores the L2I on the index server via a proxy.
3) She then stores the I2D on the data server directly, 4) James later visits the restaurant and fetches for L2Is from his friends by sending the transformed coordinates via a proxy,
5) he decrypts the L2I obtained and then queries for the corresponding I2D,
6) finally James decrypts Jhon's review.

2. Proxying L2Is for location privacy:

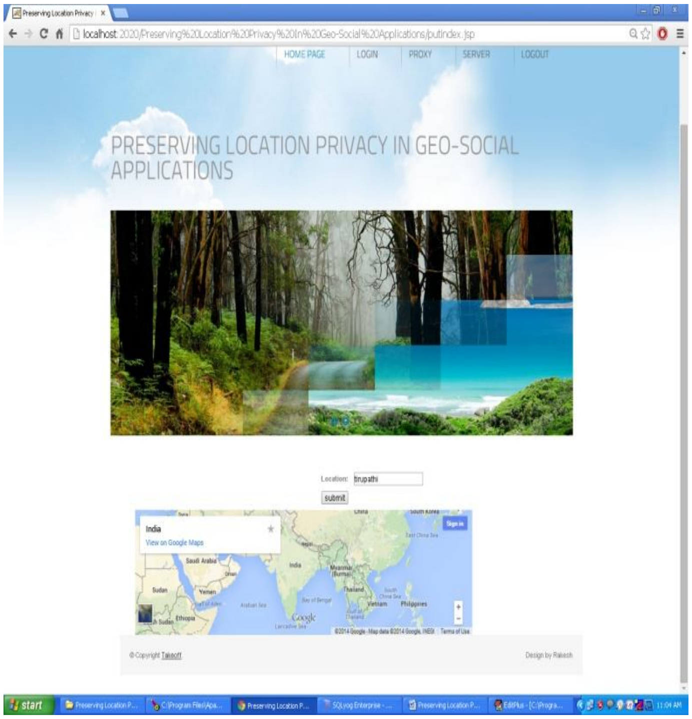
Users store their L2Is on the index server via untrusted proxies. These proxies can be any of the following:
Planet Lab nodes, corporate NATs and email servers in a user's work places, a user's home and office desktops or laptops, or Tor [34] nodes. We only need a one-hop indirection between the user and the index server. These diverse types of proxies provide tremendous flexibility in proxying L2Is, thus a user can store her L2Is via different proxies without restricting herself to a single proxy. Furthermore, compromising these proxies by an attacker does not break users' location privacy, as (a) the proxies also only see transformed location coordinates and hence do not learn the users' real locations, and (b) due to the noise added toL2Is.


localhost:2020/Preserving%20Location%20Privacy%20In%20Geo-Social%20Applications/user.jsp

USER PAGE

List Of Friends
Secrets Share
put Index To Proxy
Put Data To Server
Request For Getting Index From Proxy Server
Response For Getting Index From Proxy Server
Request For Getting Data From Data Server
Response For Getting Data From Data Server
© Copyright Takeoff
Design by Rakesh
start

Fig.2: users service options


localhost:2020/Preserving%20Location%20Privacy%20In%20Geo-Social%20Applications/putindex.jsp

PRESERVING LOCATION PRIVACY IN GEO-SOCIAL APPLICATIONS

Location: tirupathi

Fig.3: shows the user location

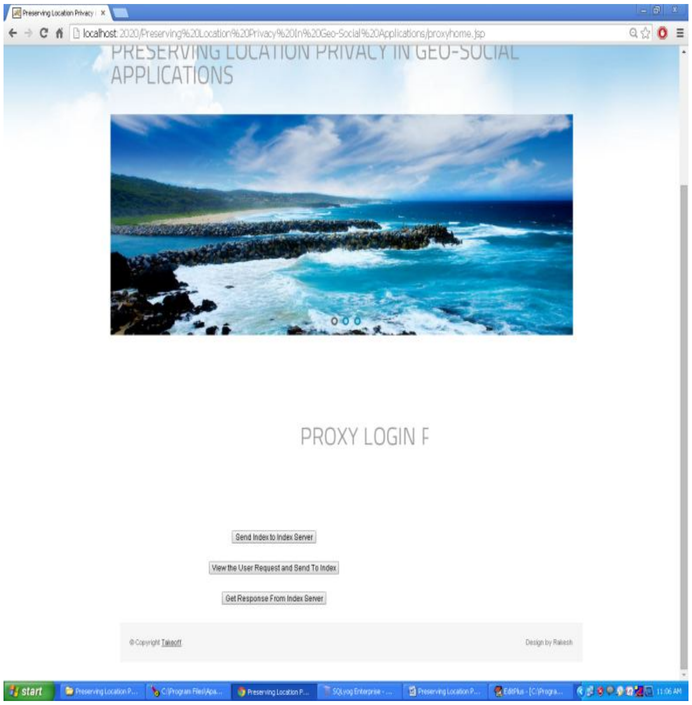

Preserving Location Privacy
localhost:2020/Preserving%20Location%20Privacy%20In%20Geo-Social%20Applications/proxyhome.jsp
PRESERVING LOCATION PRIVACY IN GEO-SOCIAL APPLICATIONS
PROXY LOGIN F
Send Index to Index Server
View the User Request and Send To Index
Get Response From Index Server
© Copyright Takeoff
Design by Rakesh
start

Fig.4: proxy services

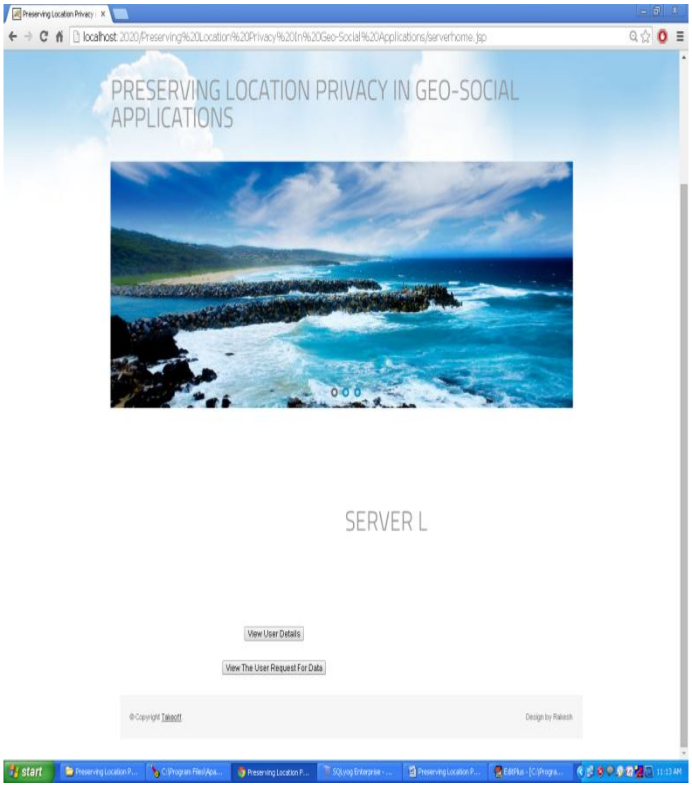

Preserving Location Privacy
localhost:2020/Preserving%20Location%20Privacy%20In%20Geo-Social%20Applications/serverhome.jsp
PRESERVING LOCATION PRIVACY IN GEO-SOCIAL APPLICATIONS
SERVER L
View User Details
View The User Request For Data
© Copyright Takeoff
Design by Rakesh
start

Fig.5: Server Service options

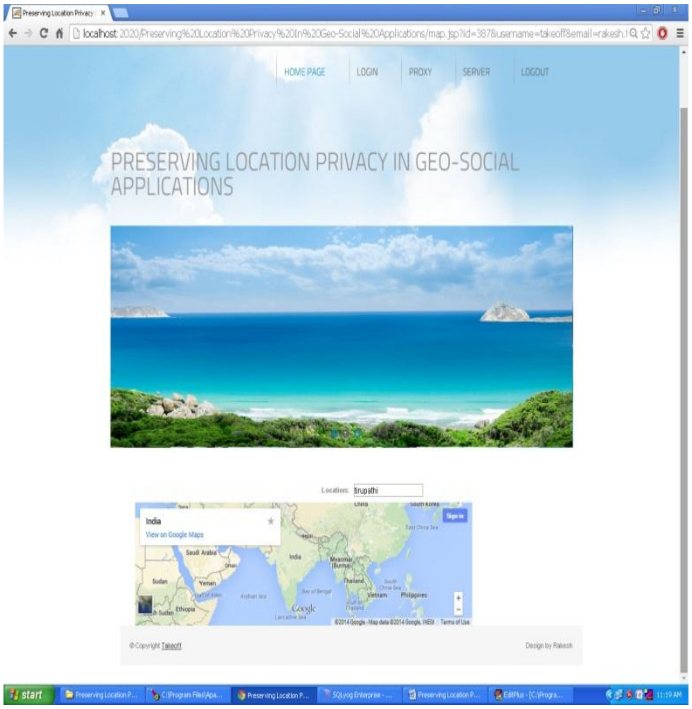

Preserving Location Privacy
localhost:2020/Preserving%20Location%20Privacy%20In%20Geo-Social%20Applications/map.jsp
HOME PAGE
LOGIN
PROXY
SERVER
LOGOUT
PRESERVING LOCATION PRIVACY IN GEO-SOCIAL APPLICATIONS
Location: tirupathi
India
View on Google Maps
Saudi Arabia
India
China
Thailand
Philippines
Google
© Copyright Takeoff
Design by Rakesh
start

Fig.6: user Location

VI. CONCLUSIONS

Our proposed solution resolves the location based attacks by constructing Location Based Social Application which prevents the location identities from unauthorized context. Our solution gives full freedom to the user can share their secret message through secure channels to intend friends. It automatically encrypt's the user location details before transfer it to the server with inexpensive symmetric keys. These keys are handover to authorized users through some secure channel. With the help of this key only users can query and decrypt the data from server securely. By adding LocX plugin to an already existing application few computational and communication overhead are there. LocX is compatible with all mobile version which perform specified operations effectively.

REFERENCES

[1] M. Motani, V. Srinivasan, and P. S. Nuggehalli, "Peoplenet: engineering a wireless virtual social network," in Proc. of MobiCom, 2005.

[2] M. Hendrickson, "The state of location-based social networking," 2008.

[3] P. Mohan, V. N. Padmanabhan, and R. Ramjee, "Nericell: rich monitoring of road and traffic conditions using mobile smartphones," in Proc. of SenSys, 2008.'

[4] G. Ananthanarayanan, V. N. Padmanabhan, L. Ravindranath, and C. A. Thekkath, "Combine: leveraging the power of wireless peers through collaborative downloading," in Proc. of MobiSys, 2007.

[5] M. Siegler, "Foodspotting is a location-based game that will make your mouth water," http://techcrunch.com/2010/03/04/foodspotting/.

[6] http://www.scvngr.com.

[7] B. Schilit, J. Hong, and M. Gruteser, "Wireless location privacy protection,"Computer, vol. 36, no. 12, pp. 135–137, 2003.

[8] F. Grace, "Stalker Victims Should Check For GPS," Feb. 2003,www.cbsnews.com.

[9] DailyNews, "How cell phone helped cops nail key murder suspect secret'pings' that gave bouncer away," Mar. 2006.

[10] "Police: Thieves robbed homes based on facebook, social media sites," WMUR News, September 2010, http://www.wmur.com/r/24943582/detail.html.

[11] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in Proc. of Mobisys, 2003.

[12] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: A privacyaware location-based database server," in ICDE, 2007.

[13] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in Proc. of ICDCS, 2005.