International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Location Privacy and Safety Recommendations in GSN

Kiran Nagale[1], Amruta Amune[2]

[1]Department of Computer Engineering, G. H. Raisoni Collage of Engineering and Management, Ahmednagar University of Pune, India

[2]Professor, Department of Computer Engineering, G. H. Raisoni Collage of Engineering and Management, Ahmednagar, University of Pune, India

Abstract: ***Online Social Networks have become a rich source of information wherein users of all ages readily provide their personal information. Using various GeoSocial applications, millions of people interact with their surroundings through their friends and their recommendations, without adequate privacy protection, these systems can be easily misused. Applications like targeted advertisement, personalized recommendations can be provided by the GeoSocial network with the help of the personal information aggregated by the user's visit at a venue. This may lead the user towards a significant risk, if their personal information is somehow leaked or sold. In this paper we provide novel approach of building LCPs of current users in a secured way and also proving its location correctness where users can modify LCPs in a predefined manner only. This paper securely and privately extract, model and embed public safety information into user experiences.***

Keywords: Location-based social applications, Location privacy, GSN

1. Introduction

Using GeoSocial Networks (GSNs) users explore for restaurants, nightlife spots, outlets and different places of interests around their vicinity. The recommendations made by their friends through GSN help user to find a correct place to hang out. The GSN applications like Foursquare, Yelp supply vital private information about their user's locations, check-ins made by them at various venues, their recommendations about the venue visited etc. Using these recommendations, the GSN applications provide venue based, location targeted advertisement to their user and helps manifold increase in the venue owner's business. Without adequate security measures, the user's information can be misused or can be sold. But if the access to this user's personal information is restricted by the GSN provider to the venue owner then it hampers their business. In this paper, we introduce a Security Wall, a suite of mechanisms which create Location Centric Profiles (LCP) of the users in a secured manner. These LCPs provide true assurance of the user's presence at the specified venue or location of the site owner. In the proposed Security Wall framework, the colocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server. The users can change their location privacy levels and also decide whether and when to accept the location proof requests. The objective of this paper is to discuss the privacy issues raised by location based services (LBS) and the challenges of implementing privacy-preserving location-aware systems.

2. Literature Survey

In "PROFILr : Toward Preserving Privacy and Functionality in Geosocial Networks" [1], Bogdan Carbunar, Mahmudur Rahman, Jamie Ballesteros, Naphtali Rishe, introduced the *Location Centric Profile (LCP)* aggregates which are created using the user profiles present at a given location. The GSN hosts a system with a client application wherein both the users and the venue owners or businesses (restaurants, yoga classes, cafeteria etc) register themselves with unique user id. The system stores information of both the registered venues and the registered subscribers with an associated geographic location. When a user visits a registered venue, they are encouraged to write their reviews about the venue, specify their location which is done by check-in at the specified venue. There is a new paradigm of business between the GSN providers and the venue owners which provide targeted advertisement to the users when they visit a specified venue or location. User profiles are created based upon the information provided by the user.

In "Preserving Location Privacy in GeoSocial Applications" [2] Krishna P.N. Puttaswamy et al., target the plethora of geosocial applications with the assumption that the servers that store the geosocial data can be attacked and hence cannot be trusted. In [2] their design goal is to provide limited access to a user's location information to his social environment in geosocial applications.
They proposed *LocX* which provides location privacy using secure user specific, distance preserving coordinate transformations to all location data shared with the server. Therefore by providing location privacy, a user's friends can query about his/her location data. The user's friends provide the user's secrets which can apply for the same transformation. The architecture in [2], describes the fact that location coordinate are sent to the server in plain text. So they proposed *coordinate transformation* which handles the privacy issue. In "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System" [3] Zhichao Zhu and Guohong Cao, put forward an architecture called *A Privacy-Preserving LocAtion proof Updating System (APPLAUS)*. The bluetooth enabled mobile devices colocated at a location generate location proofs for updating the location proof server. The architecture contains following entities:

Location Proof Server, Prover, Witness, Certificate Authority and Verifier. The mobile devices use the randomly changed pseudonyms to protect the source location privacy from each other. The locations proofs can be queried to the server by an authorized verifier. The location proof requests are broadcasts by the Prover node using Bluetooth. The locations proofs send by the Prover node are stored as pseudonyms on the location proof server. The Certificate Authority generates the public/private keys.

In "Locanyms: Towards Privacy-Preserving Location-Based Services" [4] Sebastein Gambs, Marc-Olivier Killijian, Matthieu Roy and Moussa Traore, defined *Location Based Services (LBS)* as a service whose input is the current location of a user and whose output depend on the given input. They proposed *locanym*, which is a pseudonym linked to a particular location and can be used for creating privacy preserving LBS. This locanym can be used for privacy-preserving location based services. They proposed the framework for solving the Secure Positioning Verification problem by a technique which contains two entities the Prover and the group of Verifiers. The Prover proves his location position by interacting with the group of verifiers. For this it uses the *Distance-bounding Protocol (DBP)* and the *Received Signal Strength Indicator* (RSSI). Using above two mechanisms the authors in [4] ensure unlikability, accountability and sovereignty with privacy for creating *LBS*.

In "Lockr: Better privacy for social networks" [5] Amin Tootoonchian, Stefan Saroiu, Yashar Ganjali and Alec Wolman describe that a user's social networking information is provided least amount of privacy by the current online social networking sites. Their proposed system architecture for designing *Lockr* ensures privacy to both centralized and decentralized online content sharing system. It can be done in following three steps. Firstly, there is a clear separation between the services the OSNs provide and the social networking content. This helps the user to decide or control which OSN can store their social information, which third party can be given access to it. Secondly, the proposed system Lockr provides access to the social data only through digitally signed social relationships and this data can't be reused by OSN for any other purpose. Finally, using a social relationship key the messages are encrypted. The relationship between two strangers is verified by a common friend using this key.

In "Safebook: Feasibility of transitive cooperation for privacy on a decentralized social network" [6] Leucio Antonio, Cutillo Refik Molva and Thorsten Strufe focused on the Online Social Network (OSN) services like Facebook, MySpace and LinkedIn etc provide a centralized architecture for storing a user's online social information. They observed that this centralized architecture is not suitable for providing security to the user's social data. They proposed a new decentralized mechanism called *Safebook.* The two important pillars in this architecture are: 1) instead of having a centralized storage provider, the architecture uses peer-to-peer system thus there is no centralized entity control over the users data and 2) provides trust management and privacy for communication of user with OSN services.

3. Proposed System

Without privacy people may be reluctant to use geosocial networks; without user information the provider and venues canno t support applications and have no incentive to participate. The personal social information can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linkable to a specific individual. Therefore, computing Location Centric Profiles (LCPs) which ensure user's location privacy and correctness of user's participation at a specific venue needs to be devised.

We introduce the concept of LCP which addresses the security concerns related to user data i.e. user profiles. These are created using two methods: 1) based upon the users visit to a certain location or 2) through a collection of co-located users. The proposed framework creates profiles of users who are present at a venue while maintaining privacy with ability to prove correctness whether the said user or users are actually present at the specified venue. Correctness can be proved in two ways: a) *Location Correctness* and b) *LCP Correctness*. Using Location Correctness; users who are present at a specified venue can only add the LCPs. Using LCP Correctness; the users can update their LCPs only in a predefined way.

We introduce Security Wall, a privacy preserving algorithm for computing safety snapshots of co-located mobile devices as well as geosocial network users. It is an application built on PROFILR. Security Wall uses the context of users, in terms of their location, time, other people present, to build a *safety* representation. Quantifying the safety of a user based on her current context can be further used to provide safe walking directions and context-aware smartphone authentication protocols (i.e., more complex authentication protocols in unsafe locations). Security Wall combines information collected from social sites with census and historical crime databases as well as context collected by the users' mobile devices.

We introduce the creation of user profiles based on their current location or venue. It creates and stores profiles at venues. These profiles are based on present user's profiles ensuring participant's privacy and correctness. Correctness of user's data can be verified in two ways. Firstly, *correctness of location* - where users can only add to LCPs of venue where they are located to avoid fake check-ins. Secondly, *LCP Correctness* – only through a predefined manner a user can modify LCPs. It relies on Benaloh's homomorphic cryptosystem and zero knowledge proofs which provide creation of true and accurate LCPs. The project also proposes a distributed framework using mobile devices which aggregate the co-located user's profiles. Fig.1 shows system architecture for Security Wall.

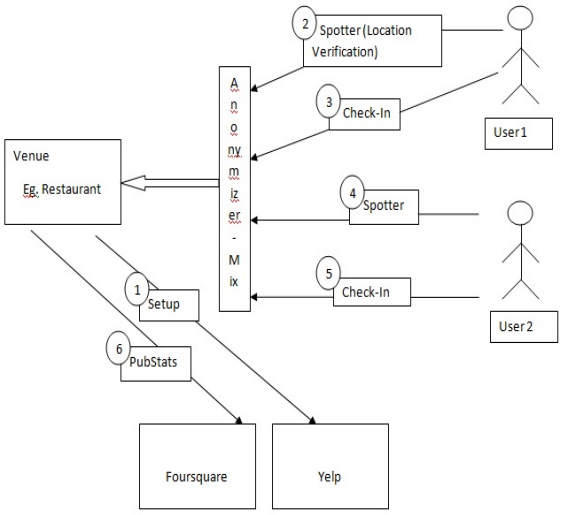


Figure 1: Security Wall Architecture

1) **Setup:** Generate the public and private key and sharing them between the sender and receiver.
2) **Spoter:** The user's location and current time are used. We can initialize the MAC and IP address to identify the user location. User location is depending on where user gives the Check-in in GeoSocial network.
3) **Check-In:** This executes only when previous run of spotter executes successfully. It uses previous random MAC and IP address. Depend on the user location user give the check-in.
4) **Pubstats:** It shares to reconstruct the private key and publish the result.

Let *K* denote the level of privacy which needs to be provided to the user at any location. We define a private LCP solution to be a set of functions. P P(*k*) = {*Setup, Spotter, CheckIn, PubStats*}. At each venue *Setup* is run to collect statistics about user's check-ins. User runs *Spotter* so as to prove his physical presence at the venue. If *Spotter* generates error then verification is failed otherwise user verification is proved. Between the user and the venue *Check-In* is run, only after Spotter is successful, so that user's profile information can be collected. PubStats publishes the collected user's profiles.

During a check-in by a user *U* at venue *V*, the Spoter protocol with *SPOTRv* is executed. During this the Venue *V* verifies *U*'s physical presence using a challenge/response protocol between *SPOTRv* and the user device. If successful the Spoter sends a secret key created by the Benaloh cryptosystem to *U*. During each venue visit by user *U*, his profile is updated with the set *Sh* of shares of secret key send to him so far.

User *U* executes *CheckIn* in conjunction with *SPOTRv* and sends his secret key and receives the encrypted counter sets. During *CheckIn*, user *U* increments the counter according to his range and re-encrypts all the counters and gives the resulting set to *SPOTRv*. Now *U* and *SPOTRv* execute the zero knowledge protocol to verify that exactly one counter has been incremented by user *U*. The latest encrypted counter set sent by user *U* is stored by *SPOTRv*. Now all the *K* users complete their *CheckIn* procedure, *SPOTRv* executes *PubStats* to generate private key to decrypt all the encrypted counters and publish the tally.

LCP

$PU = \{pU1, pU2, .., pUd\}$
Where,
P - User's Profile
d - dimensions (e.g., age, gender, home city, etc).
LCP(L) is the set $\{LCP1, LCP2, .., LCPd\}$,
L - Location ,μ - Set of Users.
LCPi denotes the aggregate statistics over the i^{th} dimension of profiles of users from μ.

Private LCP Solution
$PP(k) = \{Setup, Spotter, Check\ In, PubStats\}$

Homomorphic Cryptosystems:
KG(l) (Key Generation):
l - an odd integer, is a system parameter.
primes - *p* and *q* such that $l|(p-1)$ and $gcd(l, (p-1)/l) = 1$ and $gcd(l, q-1) = 1$.
Let $n = pq$. Select $y \in Z^*_n$, such that
$y^{(p-1)(q-1)/l} \bmod n \_= 1$.
n and *y* are the public key and *p* and *q* are the private key.
• *E(u,m)*:
Encrypt message $m \in Z^*_l$, using a randomly chosen value $u \in Z^*_n$
Output $y^m u^l \bmod n$.
• *D(z)*:
Decrypt ciphertext *z*. Let $z = y^m u^l \bmod n$.
If $z^{(p-1)(q-1)/l} = 1$, then return $m = 0$. O.w. for $i = 1..l$, compute $s_i = y^{-l} z \bmod n$. If $s_i = 1$, return $m = i$.

Annonymizer Algorithm :

```
function random ASR(k, Amin, IDnow(X,Y))
int random = new Random(10);
if (random>rnd)
{
 Adds the grid-area which has the highest QoS into S until the total users in S is not less than k;
 break;
}
else
{
 Adds the grid-area into S by randomly until the total users in S is not less than K;
 break;
}
if (random > rnd)
{
 Adds the grid-area which has the highest QoS into S until the total square measure of S is not less than Amin;
 break;
}
else
{
 Adds the grid-area into S randomly until the total square measure of S is not less than Amin;
 break;
}
```

Security Wall iSafe Algorithm:

```
1. Object implementation iSafe;
2. neighbor[] N;
3. double CI, SI;
4. double V;
5. BigInteger R;
```

6. BigInteger[] shares;
7. BigInteger[] NShares;
8. int BWC;
9. int TBlk;
10. Method1 int safetyDecision(Epoch _T)
11. B := getCurrentBlock();
12. PCIB := S.getPCI(B, _T);
13. if (PCIB! = −1)
 then return (CI _ PCIB);
 else return cas();
 if end
14. Method2 int cas()
15. N := discoverNeighbors();
16. if (N.size < NThr) then return − 1;
 BWCSUP := multiPartySum(0)− BWC;
 TBlkSUP := multiPartySum(1)− TBlk;
 return(V _ BWCSUP/TBlkSUP);
17. end

Module Structure

Module 1:
In Module first following details are includes:
1. Different users are register at venue as server through GPS and login it.
2. User on/off the GPS.
3. User Scan the WiFi Access point details and show on screen.
4. User gets the latitude and longitude of user location through GPS.

Module 2:
In Module second following details are includes:
1. User gets the list of different locations which are nearby location (Spotter).
2. User gives the Check-in.
3. Encrypt/Decrypt the details given by user.
4. Anonymizer verifies checkin indistinguishability (CI-IND).

Module 3:
In Module third following details are includes:
Use of iSafe to visualize safety levels of checkin location.

4. Prototype Implementation

The prototype has two software components: client and server. The client is implemented in JAVA on Android Developer Phone 2 , which is equipped with 528 MHz chipset, 512 MB ROM, 192 MBRAM, Bluetooth, and GPS module, and running Google Android OS. It can communicate with the server anytime through wireless data service. The server is implemented on a p4 2.1 GHz 3 GB RAM laptop. It stores the uploaded location proof records and manages corresponding indices using MySQL. We can use android phones to communicate with each other to test our solution.

5. Result Analysis

We can evaluate the performance of our application on the basis of various parameters like CPU utilization, key size and power consumption. The CPU utilization of the client code allows one to monitor the CPU usage of all the processes running on the mobile. The CPU utilization is near around 0.5 percent when the application is in standby; it indicates that listening to incoming inquiries requires very low computation. When communicating with another device and with the server the CPU utilization is around 3 and 5 percent, respectively, due to different communication interfaces. Due to heavy computations like encryption/decryption, location proof packet generation, authentication the CPU utilization reaches highest level of 10 percent.

The key size used for encryption/decryption determines the number of bits involved in the key to provide strong security. But this leads to heavy computations which increases the power consumption of the mobile. Hence we use Benaloh's cryptosystem which provides better security as well as short key length than RSA cryptosystem. The power consumption of the mobile device increase due to use of large size keys. As implementation uses short the key length, the power consumption is reduced. The figure below shows power consumption under different WiFi status and different communication distance.

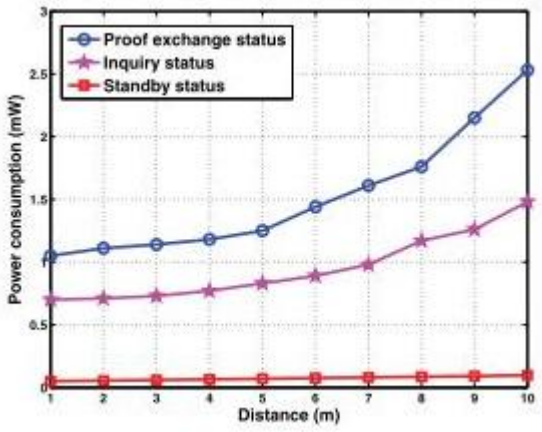
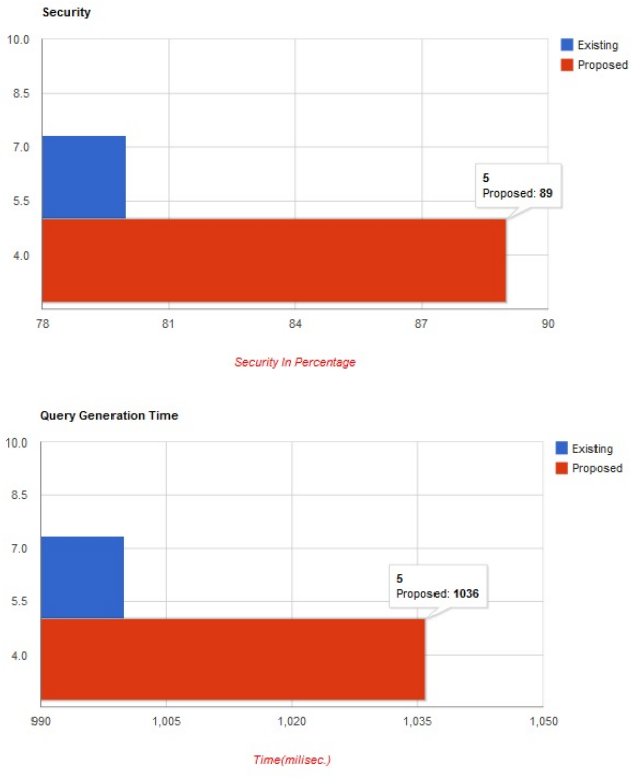


Figure 2: Power consumption under different WiFi status and different communication distance.



6. Acknowledgment

This is a great pleasure & immense satisfaction to express my deepest sense of gratitude & thanks to everyone who has directly or indirectly helped me in completing my work successfully. I express my gratitude towards project Prof. Amruta Amune, Bhivarabai Sawant, Department of Computer Engineering G.H.Raisoni College of Engineering & Management, Ahmednagar, who guided & encouraged me in completing the this work in scheduled time. I would like to thanks our Principal, for allowing me to pursue my project in this institute.

References

[1] Bogdan Carbunar, Mahmudur Rahman, Jaime Ballesteros, Naphtali Rishe, and Athanasios V. Vasilakos "PROFIL$_r$: Toward Preserving Privacy and Functionality in Geosocial Networks", in IEEE transactions, vol. 9, No. 4, April 2014.

[2] Krishna P.N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel and Ben Y. Zhao, "Preserving Location Privacy in Geosocial Applications", in *IEEE Transactions*, January 2014.

[3] Zhichao Zhu and Guoh1ong Cao, "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System", in *IEEE Transactions*, January 2013.

[4] Marc-Olivier Killijian, Matthieu Roy, Moussa Traore, "Locanyms: Towards Privacy-Preserving Location-Based Services", by Sebastien Gambs, in *ACM*, May 2012.

[5] A. Tootoonchian, S. Saroiu, Y. Ganjali, and A. Wolman, "Lockr: Better privacy for social networks", in *ACM*, December 2009.

[6] A. Cutillo, R. Molva, and T. Strufe, "Safebook: Feasibility of transitive cooperation for privacy on a decentralized social network", in *IEEE Transaction*, Jun. 2009.

[7] B. Krishnamurthy and C. E. Wills and Craig E. Wills, "On the leakage of personally identifiable information via online social networks", in *ACM*, August 2009.

[8] R. Dingledine, N. Mathewson, and P. F. Syverson, Tor: The second generation onion router" in *ACM*, August 2004.

[9] M. Rahman, N. Rishe, and S. S. Iyengar, "Towards safe cities: A mobile and social networking approach", J. Ballesteros, B. Carbunar, in *IEEE Transaction*, Nov. 2013.

[10] D. Freni, C. Ruiz Vicente, S. Mascetti, C. Bettini, and C. S. Jensen, "Preserving location and absence privacy in geo-social networks", in *ACM CIKM, October* 2010.

[11] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SLAM J. Comput.*, vol. 18, no. 1, pp. 186-208, 1989.

[12] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, and S. Barocas, "Adnostic: Privacy preserving targeted advertising," in *Proc. Network Distrib. Syst. Security (NDSS) Symp.*, 2010, pp. 1-3.

[13] S. Mascetti, D. Freni, C. Bettini, X. Sean Wang, and S. Jajodia, "Privacy in geo-social networks: Proximity notification with untrusted service providers and curious buddies," *VLDB J.*, vol. 20, no. 4, pp. 541-566, Aug. 2011.

[14] K. P. N. Puttaswamy and B. Y. Zhao, "Preserving privacy in location - based mobile social applications," in *Proc. 11th Workshop Mobile Comput. Syst. Appl.*, New York, NY, USA, 2010, pp. 1-6.

[15] M. Wernke, F. Durr, and K. Rothermel, "PShare: Position sharing for location privacy based on multi-secret sharing," in *Proc. PerCom*, 2012, pp. 153-161.

Author Profile

Kiran Nagale received the B.E degree 2013 Information Technology from PREC, Savitribai Phule Pune University, Maharashtra, India. She is currently pursuing M.E. under Savitribai Phule Pune University, Maharashtra, India.

Amruta Amune received the M.E degree 2012 Computer from MIT,Pune,University, Pune, India. She is working as Professor in G. H. Raisoni College of Engineering & Management, Ahmednagar, University of Pune, India.