Privacy Assurance in Mobile Sensing Networks: Go Beyond Trusted Servers

Ling Hu Cyrus Shahabi
Computer Science
University of Southern California
{*lingh,shahabi*}*@usc.edu*

***Abstract*—Mobile devices are becoming the largest sensor network around the world. They could be used to collect a large amount of data with little effort and cost which is leading to a promising future for participatory sensing networks or urban sensing. However, privacy concerns of the mobile users are the major inhibitors hindering massive participation. This paper proposes a solution to user privacy preserving problem in a participatory sensing network. Each user is considered as a node in a social network and users are connected through friendship links which are represented as edges on the network. Typically, each user contributes to the participatory system by uploading his/her acquired data to a server. Instead of uploading data to the server directly, we devised a Hot-Potato-Privacy-Protection Algorithm (HP^3) in which data is sent to one of the friends of the user and the friend will choose another friend to deliver the data to the next hop. Hopping goes on until some user-defined threshold is reached, then the last user uploads the data to the server. HP^3 ensures that the probability that the server can make a successful attack on the data owner is no better than $\frac{1}{n}$ where n is the number of mobile users in the system. Therefore, HP^3 protects location privacy as well as data ownership privacy of mobile users. We simulate our approach on some large scale social networks and report some findings in the paper. Experiments show that our system achieves privacy protection for each user against the server with tolerable communication overhead.**

I. Introduction

The total number of mobile users has grown to 3-4 billion in the past ten years. The ubiquity of mobile devices has brought the rapid development of mobile sensing networks. In the last few years, mobile participatory sensing systems [4], [7], [9], [14], [25], [17], [21], [22] have attracted the attention of many researchers. GPS-equipped mobile phones carried by humans or vehicles move around urban areas and collect data along their routes. Contents collected by mobile devices are uploaded to a trusted server which publishes these user-contributed data for different purposes. The data collected by such systems is in fine granularity and high precision, which will greatly improve our knowledge of understanding human behaviors and their interferences with the environment, benefiting many research areas.

Consider an application system as the following: suppose we have built a 3D model of an urban environment such as New York city (like GoogleEarth [1], Microsoft Photosynth [3]) and we want to have a participatory sensing system in which mobile users can upload city images taken with their mobile phones to a server. With these images, the server can texture map urban images onto their target Geo-locations to create a photo-realistic 3D representation. Such systems can recreate the real word with unprecedented details and quality and answer many questions with both temporal and spatial precision. For example, questions like "What does Time Square look like each year on New Year's eve?" or "How did the World Trade center towers appear before the 911 incident?" can be answered in details extracted from user-contributed photos, panoramas, close-ups and videos.

Although the technology advances on mobile devices (GPS, compass, sensors, camera, etc.) and the network improvement on bandwidth (GPRS, 3G, Wi-Fi, WiMAX, etc.) have provided more capabilities to participatory sensing networks, privacy concerns remain as one of the major issues and delays the progress of massive deployment of such systems. Two major privacy concerns are considered here, location privacy and ownership privacy. Location privacy has been studied for location-based services (LBS) [13], [15], [26], [27]. In the scenario of LBS, a user posts queries on a server for points of interest based on his/her current location q and the server returns query results satisfying the query conditions with regard to q. The user may not be willing to disclose the location q and consider it as his/her private information. Similarly, with a user participatory sensing system, data collected by users is tagged with geographical locations (e.g., latitude and longitude) which will disclose information like where the user has been to in the past. Even worse, the server could connect all the locations in the receiving order for a given user to construct the user's trajectory which would reveal more privacy information of the user. The other privacy issue, *ownership privacy*, comes from associating the user and data. With a user participatory system, mobile users may not want to release the ownership information due to safety considerations or political reasons. A mobile user may take a picture secretly of a controversial scene and share it over the Internet. However, the user may not be willing to disclose his/her association with the picture to any party, including the server. As another example, a photo or a video might be taken during a political protest

against the government. Due to the heavy censorship from the government, the photographer may not be willing to reveal his/her connection to the photo or the video because of possible government retaliation. Some TV stations hire reporters all over the world in which case anyone could be a reporter to share pictures or videos that are valuable to some news topic. As most of the spontaneous reporters wish to stay anonymous not only to the public, but also to the TV station who collects these pictures and videos, a privacy protecting system is also required in such scenarios.

In this paper, we study both of these privacy issues and explain in Section II why existing approaches do not solve the problem. Therefore, we propose a Privacy Assurance System for Mobile Sensing Networks (PA-MSN) which employs our original Hot-Potato-Privacy-Protection Algorithm (HP^3) to tackle the problem. Our contributions are summarized as following:

- We define the two privacy issues in participatory sensing networks;
- We propose a framework PA-MSN to address privacy problems and to achieve privacy protection for each user;
- We study two attack models from the server alone and from corrupted mobile users;
- We simulated the system on both synthetic and real network datasets and empirically prove the efficacy of our algorithm and the system.

The rest of the paper is organized as follows. Section II summarizes previous work on urban sensing and location privacy protection and discuss existing solutions and why they do not solve our problem. Our PA-MSN system is proposed in Section III. The Hot-Potato-Privacy-Protection Algorithm (HP^3) is presented in Section IV. We analyze two attack models in Section V, along with experiments and results. We conclude the paper in section VI with directions for future work.

II. Related Work

The idea of using mobile phones as moving sensors to collect data in urban areas has attracted the interest of many researchers [4], [25]. The challenges of such systems are elaborated in [20]. The Mobile Millennium project [25] from UC Berkeley is a state-of-the-art system using GPS-enabled mobile phones to collect en route traffic information and upload to the server in real time. The server processes traffic data, estimates future traffic flows and sends the traffic suggestion and prediction back to mobile users. Similar projects were implemented earlier in CalTel [9] and Nericell [14] which used mobile sensors/smart phones mounted to vehicles to collect traffic information, Wi-Fi access points on the route and road condition. In CycleSense [4], bikers record biking routes during their daily commute in Los Angeles area, along with information on air quality, hazards, traffic conditions, accidents, etc. Bikers trust the server and upload all their data to the server. The server publishes the data on a public website with the mobile phone number removed. In the same research group, similar idea [4] has been applied to other on-going projects on different topics, such as, to watch personal impact on the environment, to explore communities and neighborhoods. Other participatory sensing projects focus on watching petro prices [7], urban air pollution [17], diet, food security, hurricanes and diseases using mobile phones. The main idea behind these projects is to have mobile users participate in and contribute to collecting and monitoring information on various events happening in the urban area. The data collected by such systems are detailed, fine grained and just-in-time with high quality and accuracy which are valuable for academic research as well as to improve real life.

Location privacy has been a popular research topic in the database community, especially in location-based services on spatial database systems [13], [15], [26], [27]. Consider the scenario that Alice is visiting New York city for the first time and she would like to find some restaurants nearby by posting a query on a public server (e.g., Google Maps or Microsoft Virtual Earth) to find k nearest restaurants to her current location using her GPS-enabled mobile phone. The public server is not to be trusted with the user's exact location information. Space cloaking [15], [26], [27] and space-filling curves [13] (Hilbert curve for instance) are the two techniques adopted by most of the solutions for this problem. With space cloaking technique, a trusted anonymizer conceals the exact location of users by converting location points into a cloaked region which contains at least k users. A user is considered to be k-anonymous if her/his identity is indistinguishable from k-1 other users. K-anonymity model was first introduced in [23] and it is adopted in solving problems like privacy-preserving publishing [10] and privacy protection in location-based services. Although the context in participatory sensing networks is different from location-based services, the principle of k-anonymity can be used to address location privacy problems in such scenario as well. In [6], [12], the authors employed k-anonymity by generalizing k users into a tile of the spatial tessellation so that each one of them is indistinguishable from k-1 other users. Huang et al. [8] extended the same idea by using a microaggregation method to find the best coordinates to represent tiles which decreased the data distortion error. However, these approaches cannot solve our problem because our applications need fine-grained data with no distortion. Anonymization approaches will greatly decrease the data quality. Moreover, all the approaches in this category assume a trusted third-party called Anonymization Server (AS). We do not assume the existence of such servers in our system.

Space encoding (encrypting) technique [13] is another school of solutions in location privacy protection. It uses space-filling curves, like Hilbert curve, to transfer multi-dimensional data onto one dimensional space. An un-trusted

party cannot map a Hilbert value to the original location in the original space without knowing the parameters (considered as the encryption key) of the transformation. On the other hand, the mobile users who know the encryption key can easily restore original locations from Hilbert values. However, space encoding method does not solve our problem because in a participatory sensing system, user-contributed contents will be public and accessible to everyone.

Research work on anonymous network communication [19], [24] area shares some similarity with ours. The physical location of a sender is hidden by using some special routing protocols over the network. E.g., Crowds [19] network protects the anonymity of each user by blending that user into all the other users of the system. A user sets up the routing path by sending a message to the server and each user who receives the message flips a coin to decide whether to send the message to the end server or to forward it to the next random user. A virtual path is recomputed to allow dynamic changes in the network. There are two major different between Crowds and our work. In our approach, we do not assume that every user is connected to everyone else. Secondly, at any time, a user can have multiple paths to the server instead of one virtual path and due to the high mobility of sensing networks, no virtual path is maintained in the system.

III. System Architecture

A. System Overview

We propose a Privacy Assurance System in Mobile Sensing Network (PA-MSN) to solve the location and ownership privacy problems. Suppose a group of mobile users move around a city and take pictures/videos en route using their GPS-enabled mobile phones, and upload pictures/videos to a server. Mobile phones function as moving sensors collecting just-in-time on-site data associated with GPS information to support different applications. The third-party server to which all mobile users transmit data may not be trusted or may be compromised by attackers. As a result, the association between mobile users and pictures are compromised and location and ownership privacy information are disclosed. Space cloaking technique is not a preferable solution here because data with more detailed geographical information are needed.

In PA-MSN, mobile users form a social network through social interactions. There are two ways of identifying a friend in the system. Two users can add each other as a friend through personal contact, or any new user to the system can ask the server to provide a list of users that are willing to be added as friends by others. For example, the user could perform a search on the server using some keyword and find people that have some common interests or located in the same region. The server returns a list of subscribers in the system and the user chooses some of them to send friendship request through the server. The system can be modeled as a non-directed graph in which each user is denoted by a node and friendships are represented as edges (links) connecting two nodes. Every node connects to the server because everyone can send data to the server directly. A network with seven mobile users are shown in Figure 1. The blue (solid) edges between mobile users are friendship connections on which data travel. The orange (dotted) edges are the last hops from mobiles users to the server. Data collected by mobile users can be any form, for example, photo images, audio recordings, videos, data collected by sensors of mobile phones, etc. For presentation purpose, we use *image* to generalize user-contributed data for simplicity in the remaining sections of the paper.

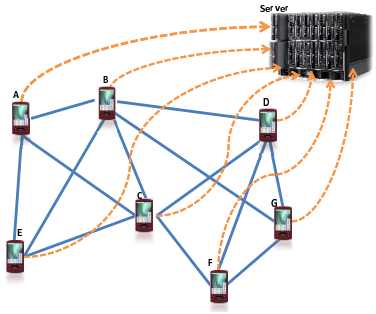

Figure 1. A Simple Network Scenario.

In our system, a mobile user does not send its data directly to the server to avoid disclosing its privacy information. Instead, it sends data to one of its friends chosen randomly and independently. We also devised a scheme which ensures that the last sender of the file is guaranteed not to be the original owner and we will discuss it in Section IV. On the network, a node sends data only to one of its directly connected nodes. Subsequently, that node may transmit the data to another node that it connects to and so on. Each data file is assigned to a random number ρ which ranges from 0 to 1. The value of ρ decreases by some fraction after passing through one node on the network. Whether the current mobile user sends the data to the server depends on the current value of ρ and the hopping threshold τ and different user can choose different τ values. Images are sent to the server when ρ reaches the threshold on that node.

Mobile users correspond with each other using P2P communication and the server is not aware of the data transfers between mobile users. Not only the server, but all the other mobile users are not part of such P2P communications. In other words, each mobile user who receives an image file has no idea about who was the first owner of the image. It could be the last user who sent it, or it could be anyone that can reach the last user.

The privacy protection in PA-MSN is achieved at the cost of the extra communication overhead between mobile users. We show below that such overhead is not a problem on mobile networks because of the dramatic improvement on

the bandwidth of data services. We ran a set of simulation experiments to examine the relation between the hopping threshold τ and the average communication overhead on different network topologies and the results are reported in Section V.

B. For and Against

In this section, We discuss the pros and cons of PA-MSN. The idea of passing images on the mobile network multiple times before uploading them to the server which hosts these user-contributed contents has the advantage of anonymizing the original owner of each image. Therefore, not only the ownership privacy is protected, the location privacy of each participant is preserved as well. Obviously, if an adversary knows that a user has taken an image at some location and has uploaded it to the system, the user's location and his/her ownership of the image are both known to the adversary and nothing can be done here. However, the privacy release of an individual image does not affect other users and all the remaining images contributed by the same user are still safe because no connection can be made between different images taken by the same user.

One might raise the concern on the communication overhead between mobile users. We argue that with the improvement of the bandwidth available for mobile networks as shown in Table I, communication overhead would not be an issue in the future. For example, a photo with the resolution of 1600×1200 taken by a 2-megapixel mobile phone camera is around 200KB (1.6Mb) which can be uploaded in 1 second on a 3G network. A 4 minutes and 30 seconds YouTube video is around 18MB (144Mb) can be uploaded in one minute on a 3G network.

Generations	DownStream	UpStream
GSM (2G)	NA	NA
GPRS (2.5G)	60-80 kbps	20-40 kbps
3G	14Mbps	5.8Mbps
LTE (4G)	100Mbps	50Mbps
UMB (4G)	275Mbps	75Mbps

Table I
EVOLUTION OF BANDWIDTH ON MOBILE NETWORKS [5].

IV. HOT-POTATO-PRIVACY-PROTECTION ALGORITHM

Each node on the network can initiate a process of transmitting data to the server. The image data is encrypted using the server's public key and the encrypted data is D_E. The data passes through a few nodes on the network before it reaches the server and the encryption guarantees that intermediate nodes cannot understand the content, therefore, they cannot perform privacy attacks on the content. The exact path taken by each image is non-deterministic. The first node generates a random number ρ in the range (0,1) and associates ρ with the image. The value of ρ serves as the initial random noise at the first step and it decreases as the image travels along the network path. After passing through a node u_i with k_i edges, ρ decreases by $\frac{1}{k_i}$. Each node on the network runs the HP^3 algorithm independently in the following fashion: it receives data from a friend and passes on the data to another friend v_i chosen by random. The last user sends the data to the server when the value of ρ reaches the hopping threshold τ.

Networks considered in this paper are connected network without self-loops. The server is a super node in the network and the links that connect users to the server are super links (shown as orange (dotted) lines in Figure 1). Mobile users do not use the super node as relay node and they transmit data to the super node only when certain conditions defined in Figure 2 are satisfied. Hence, we omit the super node/edges in a graph representation of a network for simplicity. In the following sections, edges and nodes refer to non-super edges and non-super nodes, unless explicitly specified otherwise.

Privacy is measured by the probability that the server can make a successful attack on the ownership of an image from a user. In the case that users upload data directly to the server, the privacy protection is 0 because the server knows who is the owner of an image with 100% accuracy and there is no privacy protection for the user. When the server does not have any knowledge about the network except the total number of users, the probability that the server succeeds in associating an image to its original owner is $\frac{1}{n}$ (lowerbound). Therefore the privacy protection in such a participatory sensing network is $1 - \frac{1}{n}$. We show in the following that in PA-MSN, the server cannot make an attack on the user privacy with a probability greater than $\frac{1}{n}$ even with the full knowledge of the network.

A. Message routing algorithm

Image transmission paths are partly determined by the two parameters ρ and τ. Each mobile user makes the decision of relaying or submitting the message to the server as the following. When the value of ρ associated with an image reaches the hopping threshold τ, the current mobile user will upload the image to the server. Otherwise, the user decreases the value of ρ and chooses a friend on its friend list to send the message. Communications between friends are secured by some pre-negotiated shared secret between each pair of them.

A pseudo-code of the Hot-Potato-Privacy-Protection Algorithm (HP^3) is shown in Figure 2. HP^3 runs independently on each node in the system. Suppose the algorithm is running on a node with k friends (neighbor nodes). If the node is the initiator, it assigns a random number ρ to the image, encrypts the data using the server's public key and constructs the message m. Subsequently, it randomly chooses a friend node i (line 4) and sends m to i. If the node is a relay node of an image, it first checks if ρ reaches the hopping threshold τ (line 7). If yes, the node uploads the image data $m.D_E$ to the server (line 8). If ρ does not reach the threshold τ, the node decreases ρ by $\frac{1}{k}$, chooses a friend by random out of k-1 friends (excluding the previous node who sent the image to the node to avoid sending messages

back and forth between two users.) and sends m (line 12-14). If the current user only has one friend, it starts over the HP^3 algorithm (line 10).

Hot-Potato-Privacy-Protection Algorithm: (HP^3)
Input: bool initial, ImageData D_E, Message m

```
1)  If (initial)
2)      ρ = Random(0, 1);
3)      m = (D_E, ρ);
4)      i = Random_Integer(1, k);
5)      Send message m to friend[i];
6)  Else
7)      If (m.ρ ≤ τ)
8)        upload m.D_E to server;
9)      Else if (k==1)
10)           HP^3(true, m.D_E, null);
11)         else
12)           m.ρ = m.ρ/k;
13)           i = Random_Integer(1, k-1);
14)           send message m to friend[i];
15) End;
```

Figure 2. Hot-Potato-Privacy-Protection Algorithm (HP^3).

B. Single Point Corruption Avoidance

We assume that most of the mobile users in the system are honest and safe. There are two levels of authentification in PA-MSN: 1) each user needs to subscribe to the server, and 2) the two parties need to verify each other before becoming friends. However, there could be some malicious or compromised mobile users in the system and we propose the following scheme to take care of such cases.

When node corruption happens, compromised nodes can intercept images transferred through them and these images will never reach the server. To address the problem, we enhance the HP^3 with the technique of fragmenting original image into several segments with some redundancy and transporting each segment using the HP^3 algorithm independently. Consequently, each segment follows a different path to the server. If one or a few nodes on the network are malicious, they can merely intercept the segments that happen to pass through them while the remaining parts of the image are still safe. On the server side, different segments of the same image are assembled together to restore the original data. If some segments are missing, the server can still restore the image with the redundant information [1]. The enhanced version of HP^3 algorithm is referred to as HP^{3+} and we study both algorithms in Section V.

V. Experiments

We evaluated our system by using both synthetic and real social network datasets as listed in Table II. SynUniform and SynScaleFree are synthetic datasets each containing 300 nodes. SynUniform has an even node degree distribution and SynScaleFree conforms to a power law degree distribution.

[1]We can use various encoding techniques, such as layered compression [11], to generate the image segments in order to improve the image construction at the server in the presence of missing components. These variations of HP^3 will be studied as part of our future work.

NetScience is a subset of the real world dataset of coauthorship network of scientists working on network theory and experiment [16]. Both NetScience and SynScaleFree are scale-free networks whose node degrees follow a power law (asymptotically) distribution. Scale-free networks are important because some social networks, citation networks and protein networks appear to be scale-free by empirical observation [18]. Figure 3 shows the visualization of the NetScience network generated by IBM Manyeyes online tools [2].

Name	# Nodes	# Edges
SynUniform	300	3640
SynScaleFree	300	1479
NetScience	389	914

Table II
Social Network Datasets.

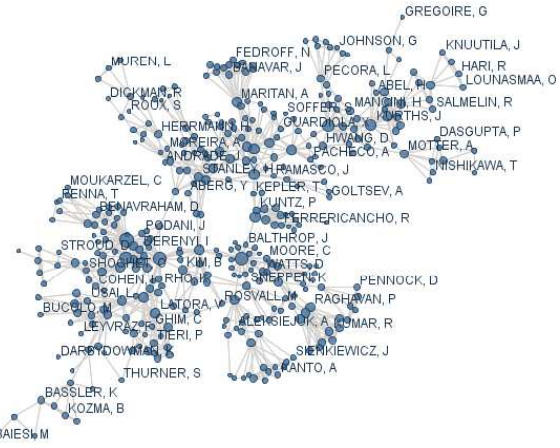

Figure 3. Coauthorship Network of Scientists Working on Network Theory and Experiment (A subset of [16]).

The node degree distributions of the three datasets are shown in Figure 4(a). SynScaleFree shows that the majority of the nodes have degree less than 10 and the number of high degree nodes are fairly small. NetScience exhibits the similar characteristic. In SynUniform, node degrees are evenly distributed across all the nodes shown in the solid blue line.

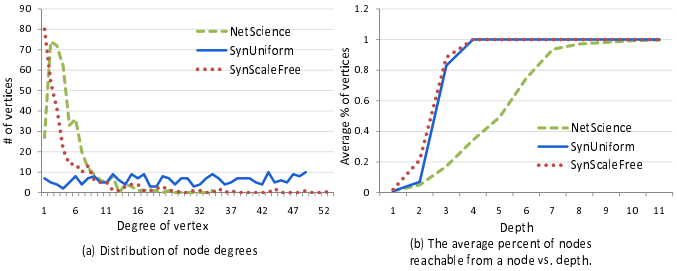

Figure 4. Characteristics of datasets.

A. Discussion on attack models and privacy protection

We first consider the attack model of *ownership privacy attack* from the server side. The server has the knowledge of

the network and the last sender of each image. However, the server is not aware of the number of nodes t (i.e., the number of hops) that the image has passed through. Therefore, it can only estimate the value of t. Figure 4(b) shows the percent of nodes reachable from any node on the network vs. the depth. In SynUniform and SynScaleFree, a node can reach any other node in the network within the depth of 4. In other words, if we construct a minimum spanning tree starting from a random node, the height of the tree is no more than 4. Similarly in NetScience, all the nodes are reachable within the depth of 7. This observation tells us that when the server tries to identify the contributor of an image and tracks backwards from the last sender, it will quickly (in 4 to 7 hops) find that all the users in the network are suspects and the probability for each of them to be the original owner of the data is $\frac{1}{n}$.

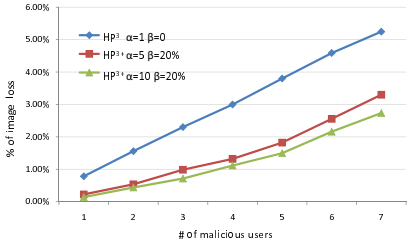

Figure 5. The average percent of image loss vs. number of malicious users.

The second attack model is *malicious mobile users' attack* and we consider the mobile user attackers working independently. As explained in Section IV-B, we enhance the HP^3 algorithm with the technique of splitting each image into several redundant segments and transport each of them separately using the algorithm. Again, each segment is encrypted using the server's public key and no one can decrypt it but the server. When there are malicious nodes in the network, we consider that the malicious node blocks the path and any data transferred via that node is lost. We implement HP^3 and HP^{3+} on NetScience network and the results are shown in Figure 5. We use parity bits to encode redundant data in this set of experiments and as shown in Figure 5, α is the number of segments per image and β is the data redundancy. α=5 and β=20% imply that each image is divided into 5 segments and one of which is the parity data. If any segment is missing, the image can still be restored at the server using the remaining segments [2]. Figure 5 shows the percent of image loss vs. the number of malicious users. HP^{3+} has less image loss than HP^3 with the same number of malicious users. For example, with 4 malicious users in the system, the image loss in HP^3 is 3%. However in HP^{3+}, only 1.3% of image is lost when α is 5 (each image is divided into 5 segments.) and 1.1% loss when α is 10.

[2]We plan to study the impact of redundancy on the quality of image reconstruction using more advanced image compression techniques in our future work.

B. Communication overhead

The relationship between the average number of hops that each image passes through on the network and the hopping threshold τ is studied in Figure 6. Transferring images to intermediate nodes instead of the server directly is considered as extra communication costs and Figure 6 shows the communication overhead versus the hopping threshold τ. When τ is close to 1 ($\lg \tau \to 0$), each user uploads the image to the server without any communication overhead. When τ is close to 0 ($\lg \tau \to -\infty$), each image will hop on the network via infinite number of hops before it reaches the server. Recall that we showed in Figure 4(b) that when the number of hops reaches 4 on SynUniform and SynScaleFree, every user in the network has equal probability to be the original owner. Similar results hold in NetScience when number of hops is 7. Therefore, it is sufficient to set the τ value to around 10^{-5} for SynUniform and SynScaleFree networks and 10^{-6} for NetScience network.

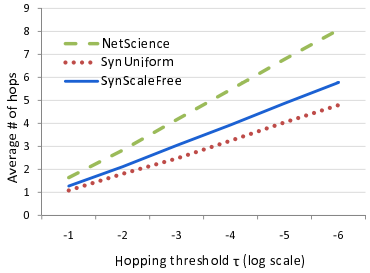

Figure 6. The average number of hops per image vs. hopping threshold τ.

VI. Conclusion

In this paper, we proposed the PA-MSN framework to address the user privacy problem in participatory sensing networks. Specifically, we designed a Hot-Potato-Privacy-Protection Algorithm (HP^3) in which each participant makes use of other users in the network to pass the content before it reaches the server. In such a system, the server cannot identify the association between the content and its contributor, therefore protects the user's privacy without using any trusted server. As the future work, we will study more attack models (for example, conspiracy attack between the server and some malicious users, unlinkability) on PA-MSN to measure the privacy level of the system against different attackers. As most social networks are scale-free networks following power law distribution. We will investigate more on certain behaviors on message propagation over different networks.

VII. Acknowledgement

This research has been funded in part by NSF grants CNS-0831505 (CyberTrust), the NSF Center for Embedded Networked Sensing (CCR-0120778) and in part from the METRANS Transportation Center, under grants from US-DOT and Caltrans. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

The authors would also like to thank Dr. Farnoush Banaei-Kashani for contributing to the earlier discussion of the project and Mr. Grady Laksmono for raising the image breaking idea during a class discussion.

REFERENCES

[1] Google Earth, http://earth.google.com/.

[2] IBM ManyEyes, http://manyeyes.alphaworks.ibm.com/manyeyes/.

[3] Microsoft Live Labs, http://livelabs.com/photosynth/.

[4] Urban Sensing, CycleSense, http://urban.cens.ucla.edu/projects/. *Center for Embedded Networked Sensing (CENS), UCLA*.

[5] Wikipedia, http://en.wikipedia.org/.

[6] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos. Anonysense: privacy-aware people-centric sensing. In *MobiSys*, pages 211–224, New York, NY, USA, 2008. ACM.

[7] Y. Dong, S. S. Kanhere, C. T. Chou, and N. Bulusu. Automatic collection of fuel prices from a network of mobile cameras. In *Proceedings of IEEE DCOSS*, June 2008.

[8] K. L. Huang, S. Kanhere, and W. Hu. Towards privacy-sensitive participatory sensing. In *PerCom*, pages 1 – 6. IEEE International Conference on Pervasive Computing and Communications, 2009.

[9] B. Hull, V. Bychkovsky, Y. Zhang, K. Chen, M. Goraczko, A. Miu, E. Shih, H. Balakrishnan, and S. Madden. Cartel: a distributed mobile sensor computing system. In *SenSys*, pages 125–138, 2006.

[10] R. J. Bayardo Jr. and R. Agrawal. Data Privacy through Optimal k-Anonymization. In *ICDE*, pages 217–228, 2005.

[11] M. Kamran, F. Shi, Y. Xie, and Y. Wang. An efficient layered data compression scheme with constraint analysis. *Mathematics and Computers in Simulation*, 79(4):1216–1232, 2008.

[12] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz. Anonysense: Opportunistic and privacy-preserving context collection. In *Pervasive Computing*, pages 280–297, 2008.

[13] A. Khoshgozaran and C. Shahabi. Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In *SSTD*, pages 239–257, 2007.

[14] P. Mohan, V. N. Padmanabhan, and R. Ramjee. Nericell: rich monitoring of road and traffic conditions using mobile smartphones. In *SenSys*, pages 323–336, 2008.

[15] M. F. Mokbel, C.-Y. Chow, and W. G. Aref. The new casper: Query processing for location services without compromising privacy. In *VLDB*, pages 763–774, 2006.

[16] M. E. J. Newman. Finding community structure in networks using the eigenvectors of matrices. *Preprint physics/0605087*, 2006.

[17] E. Paulos, R. Honicky, and E. Goodman. Sensing atmosphere. In *Workshop on Sensing on Everyday Mobile Phones in Support of Participatory Research*, November 2007.

[18] A. R. and B. A.-L. Statistical mechanics of complex networks. *Review of Modern Physics*, 74:4797, 2002.

[19] M. K. Reiter and A. D. Rubin. Crowds: anonymity for web transactions. *ACM Trans. Inf. Syst. Secur.*, 1(1):66–92, 1998.

[20] K. Shilton, N. Ramanathan, S. Reddy, V. Samanta, J. Burke, D. Estrin, M. Hansen, and M. Srivastava. Participatory design of sensing networks: Strengths and challenges. In *Participatory Design Conference*, 2008.

[21] H. Shirani-Mehr, F. B. Kashani, and C. Shahabi. Efficient viewpoint assignment for urban texture documentation. In *GIS*, page 10, 2009.

[22] H. Shirani-Mehr, F. B. Kashani, and C. Shahabi. Efficient viewpoint selection for urban texture documentation. In *GSN*, 2009.

[23] L. Sweeney. Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):571–588, 2002.

[24] P. F. Syverson, D. M. Goldschlag, and M. G. Reed. Anonymous connections and onion routing. In *IEEE Symposium on Security and Privacy*, pages 44–54, 1997.

[25] Univ. of California Berkeley. http://traffic.berkeley.edu/, 2008-2009.

[26] T. Wang and L. Liu. Privacy-Aware mobile services over road networks. *PVLDB*, 2(1):1042–1053, 2009.

[27] T. Xu and Y. Cai. Location anonymity in continuous location-based services. In *GIS*, page 39, 2007.