© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Indoor Localization Using IPS with User Defined Privacy Preservation

Vishal V, Sanjeev Krishnan R, Kayalvizhi C

Computer Science and Engineering, Dhanalakshmi College of Engineering, Tambaram, Chennai, Tamil Nadu, India

ABSTRACT

Indoor Positioning System (IPS) has played a major part in using navigation inside an enclosed or indoor location. Predominant Smartphone as localization subsystems currently relies on server-side localization processes, allowing the service provider to know the location of a user at all time. Here we propose an algorithm to avoid the other sources from accessing personal data from the user hence avoiding data theft. A key observation is that these incidents typically involve large congregations of individuals, which form durable and stable areas with high density. Since the process of discovering, gathering patterns over large-scale trajectory databases can be quite lengthy, we further develop a set of well thought out techniques to improve the performance.

We have evaluated our framework using a real prototype developed in Android and Hardtop HBase as well as realistic Wi-Fi traces scaling-up to several GBs. We can offer fine-grained localization in approximately four orders of magnitude less energy and number of Messages than competitive approaches.

Keywords : IPS, Security, Navigation, Offline Navigation

I. INTRODUCTION

People spend 80-90 percent of their time in indoor environments,1 including shopping malls, libraries, airports or university campuses. The omni present availability of sensor-rich mobiles has boosted the interest for a variety of indoor location-based services, such as, in-building guidance and navigation, inventory management, marketing and elderly support through Ambient and Assisted Living [1], [2]. To enable such indoor applications in an energy efficient manner and without expensive additional hardware, modern smartphones rely on cloud-based Indoor Positioning Services (IPS), which provide the accurate location (position) of a user upon request. There are numerous IPS, including Skyhook, Google, Indoo.rs, Wifarer, Navizon, IndoorAtlas, ByteLight and our open in-house Anyplace [3] system.2 These systems rely on geolocation databases (DB) containing wireless, magnetic and light signals, upon which users can localize. Particularly, IPS geolocation DB entries act as reference points for requested localization tasks, as explained thoroughly in Section 2. In summary, a smartphone can determine its location at a coarse granularity (i.e., km or hundreds of meters) up to a fine granularity (i.e., 1-2 meters), by comparing against the reference points, either on the service or on the smartphone itself. One fundamental drawback of IPS is that these receive information about the location of a user while servicing them, generating a variety of location privacy concerns (e.g., surveillance or data for unsolicited advertising).3 These concerns don't exist with the satellite based Global Positioning System (GPS), used in outdoor environments, as GPS performs the localization directly on the phone with no location-sensitive information downloaded from any type of service. Although in this work we are mainly concerned with fine-grained Wi-Fi localization scenarios in indoor spaces, our discussion is equally applicable to other types of indoor fingerprints (e.g., magnetic, light, sound) and outdoor scenarios (e.g., cellular).Location tracking is unethical in many respects and can even be illegal if it is carried out without the explicit consent of a user. It can reveal the stores and products of interest in a mall

we've visited, doctors we saw at a hospital, book shelves of interest in a library, artifacts observed in a museum and generally anything else that might publicize our preferences, beliefs and habits. Somebody might claim that telecoms and governments are already tracking smartphone users outdoors, on the premise of public and national safety,4 thus there is no need to care about indoor location privacy either. Clearly, there is a lot of controversy on whether this is right or wrong, which has to do with different cultural, religious, legal and socio-economic dimensions. We feel that location tracking by IPS poses a serious imminent privacy threat, which will have a much greater impact than other existing forms of location tracking discussed in Section 2 (i.e., outdoor GPS tracking or Browser-based location tracking). This holds as IPS can track users at very fine granularity over an extended period of time (i.e., recall that people spend considerable time indoors).

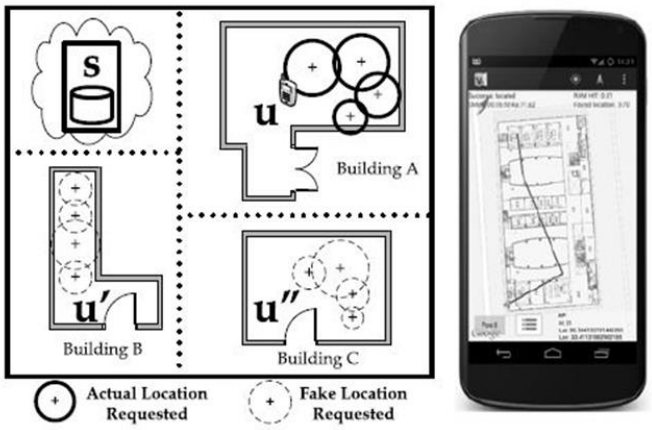


Figure 1: (Left) Indoor localization of user u using the cloud-based IPS s. During the localization, u requests k-1 camouflaged locations using the TVM algorithm, such that s can know the location of u only with probability 1/k. (Right) our TVM prototype implemented in Android OS.

Moreover, IPS are private enterprises that are less controlled, thus they might be tempted to exploit the "big" location data of their customers, by either selling it to advertising companies or by linking it to other sensitive data sources. Additionally, a user cannot know where PS host and operate their data and whether these conform or not to latest legislative efforts and reforms (e.g., EU Data Protection Directive, the US White House Consume Privacy Bill of Rights, U.S.-EU Safe Harbor guidelines, US Do-Not-Track Online Act, etc.) Finally, IPS are attractive targets for hackers, aiming to steal location data and carry out illegal acts (e.g., breaking into houses5). In this paper, we consider that IPS are fundamentally untrusted entities and, as such, develop hybrid techniques that on the one hand exploit the IPS utility, but on the other hand also offer controllable location privacy to the user. Particularly, we tackle the technical challenge of enabling a user u to localize through an IPS s, without allowing s to know where u is. We devise the Temporal Vector Map (TVM) algorithm,6 which guarantees that s can not identify u's location with a probability higher than a user-defined preference pu. InTVM, a user u camouflages its location from s, by requesting a subset of k entries froms, where k is a user-defined constant. To understand the operation of TVM, at a high level, consider the illustration of Fig. 1(left). An arbitrary user moves inside building A, using the TVM smartphone application shown in Fig. 1(right). While u requests reference locations from s pertinent to building A, it also requests reference locations related to arbitrary other buildings B and C. Particularly, u uses a hashing scheme that makes sure that for a given user-preference k ¼ 3, s will not be able to distinguish u's request from requests made by k _ 1 arbitrary other users u0 and u00. Under reasonable assumptions about the scope of IPS, we show that s can know u's location sonly within pu, even while u is moving.

II. METHODS AND MATERIAL

A. Related Work

In this section, we provide background and related work on indoor localization and privacy-preserving data management, upon which our presented techniques are founded. The localization literature is very broad and diverse as it exploits several technologies. GPS is obviously ubiquitously available but has an expensive energy tag and is also negatively affected from the environment (e.g., cloudy days, forests, down town areas, etc.). Besides GPS, the localization community [1] proposed numerous proprietary solutions including: Infrared, Bluetooth, visual or acoustic analysis, laser and LiFi, RFID, Inertial Measurement Units, Ultra-Wide-Band, Sensor Networks, etc.; including their combinations into hybrid systems. Most of these technologies deliver a high level of positioning accuracy; however they require the deployment and calibration of expensive equipment, such as custom transmitters, antennas or beacons, which are dedicated to positioning. This is time consuming and implies high installation costs, while the approaches we discuss operate off-the-

shelf on conventional smartphones and Wireless LANs already deployed in most buildings.

The shelf positioned systems for modern phones are as follows :

i) Global PS (GPS): Uses radio signals from satellites to offer super fine accuracy often less than 1 meter. The localization is carried out on the handheld, thus we consider that there are no privacy concerns with this approach.
ii) Cell DB, Wi-Fi DB or Hybrid Cell/Wi-Fi DB: Use radio signals from mobile Cell Towers, Wi-Fi access points (APs), or their combination, to offer coarse accuracy that is often less than 1,000 and 200 meters, respectively. The given databases have been constructed offline by contributors (e.g., an Android phone by default forwards Wi-Fi AP and Cell Tower data to Google). Subsequently, users can obtain their current location using a query/response to the cloud-based localization service.
iii) Wi-Fi RadioMaps : Is similar to (ii), which stores radio signals from Wi-Fi APs in a database, but at a much higher density. For example, our anyplace [3] and open-source Airplace [7] systems, use a technology that achieved the second highest known accuracy [8], with an average error of 1.96 meters.

Therefore, a more effective way of weighting the K nearest fingerprints is required. In the Weighted-KNN (WKNN) approach, the K nearest neighbours, calculated as in KNN, are assigned a weight equal to:

$$w_i \propto \frac{1}{||V_i - V_u||}.$$

Finally, the user's location is calculated again using a convex combination of those K locations, where in this case the farther locations affect less the calculation than the closer locations.

B. Algorithm Details

In this section, we detail the internal phases of the Temporal Vector Map algorithm, its correctness properties, an example of its operation and further optimizations. The algorithm details have been given below.

Algorithm 1. *Temporal Vector Map*

Input: V_u is the current fingerprint of u; p_u is u's privacy preference; RM is the RadioMap on s
Output: (x, y) is the location of u

▷ **Phase 1: Initial Localization (of u through s)**
———— User-side (u): ————
1: $B_u = createkAB(V_u, p_u)$ ▷ *kAB filter in Algorithm 2*
2: send B_u to s
———— Server-side (s): ————
3: $C_u = kAB\ to\ AP(B_u)$ ▷ Set of Candidate AP MAC identifiers
4: $pRM = filter(RM, C_u)$ ▷ Set of RM rows filtered by C_u
5: send pRM to u
———— User-side (u): ————
6: $(x, y) = localize(V_u, pRM)$ ▷ using WKNN, RBF or SNAP [7]

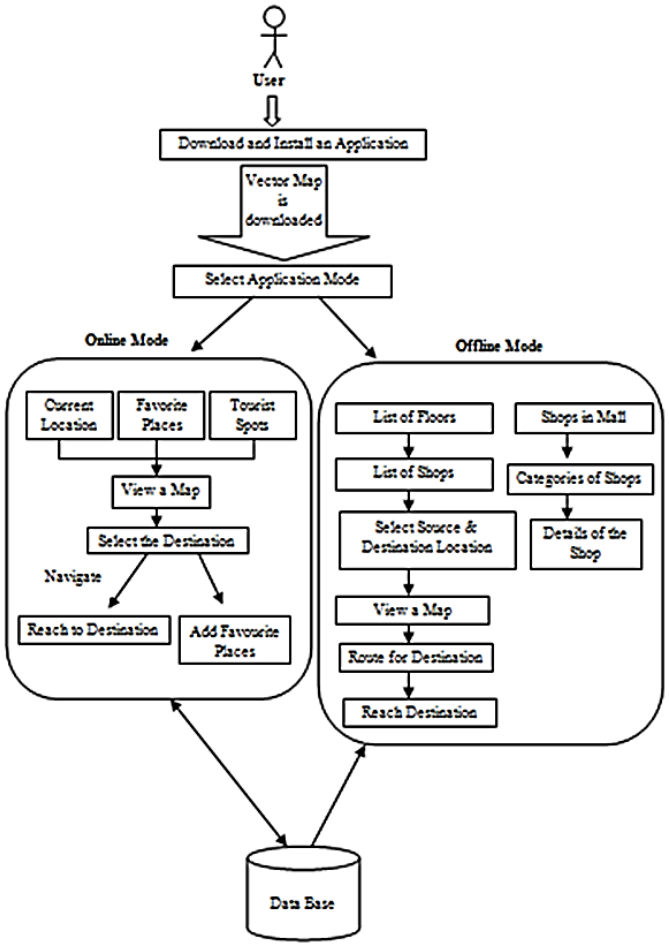
▷ **Phase 2: Subsequent Localization (of u through s)**
———— User-side (u): ————
7: **if** $(canNotBeServed(V_u, pRM))$ **then**
8: $C_u = bestNeighbors(V_u, pRM)$ ▷ Set of APs in Algorithm 3
9: send C_u to s
———— Server-side (s): ————
10: $pRM = filter(RM, C_u)$ ▷ Set of RM rows filtered by C_u
11: send pRM to u
12: **end if**

Algorithm 2. *createkAB*

Input: V_u is the fingerprint of u; p_u is u's privacy preference
Output: B_u *kAB* filter for u

1: *Constants:* h, M, a ▷ # of hash functions, $|AP|$, access point coverage
2: ap_i randomly chosen from V_u ▷ Candidate needed for this localization
3: $k = \frac{1}{a p_u}$ ▷ Equation (2)
4: $b = \lfloor \frac{-h}{\ln(1 - \sqrt[h]{k/M})} \rfloor$ ▷ Equation (4)
5: **for all** h hash functions **do**
6: $B[hash(ap_i) \bmod b] = 1$
7: **end for**

C. System Architecture



D. System Overview

This section formalizes our system model, assumptions and desiderata. Our main symbols are summarized in Table 2.

System Model

Research Goal. Provide continuous localization to a mobile user u that can measure the signal intensity of its surrounding APs, with minimum energy consumption on u, such that a static cloud-based server s can not identify u's location with a probability higher than a user-defined preference pu. We assume a planar area A containing a finite set of ðx; yÞ points (see Fig. 3). We also assume that A is covered by a set of Wi-Fi access points fap1; ap2; . . . ; apM g, each covering a planar points. Area A is not necessarily continuous and can be considered as the joint area of all api 2 AP (i.e., global coverage). Each api has a unique ID (i.e., MAC address) that is publicly broadcasted and passively received by anyone moving in the a points of api. The signal intensity at which the ID of api is received at location ðx; yÞ, is termed the Received Signal Strength of api at ðx; yÞ, having for ease-of-exposition a value in the range ½0::100&. Let a static (cloud-based) positioning service s have constructed beforehand an N _ M table, coined RadioMap (RM), which records the RSS of the api 2 AP broadcasts at specified ðx; yÞ 2 A locations. When an api is not seen at a certain ðx; yÞ the RM records "_1" in its respective cell. Any subset of RM rows will be denoted as partial RadioMap (pRM). A user u localizes through the indoor positioning service s, using the ID and RSS broadcasts of surrounding api 2 AP while moving. This information is termed, hereaf-ter, RSS Vector or Fingerprint (Vu) of u, which changes from location to location and over time. Contrary to RM rows having M attributes, Vu has only M0 < < M attributes.

III. RESULTS AND DISCUSSION

1. The pattern for the existence of such group is saved in a large scale database.
2. The consent of the user is questioned each time the user makes contact with the IPS.
3. To enable such indoor applications in an energy-efficient manner and without expensive additional hardware, modern Smartphone's rely on Indoor Positioning Services (IPS)
4. We can use both online and offline mode in this application.
5. Helps in knowing the user interest with the consent of the user hence allowing him to enhance his experience by giving suggestions of his favorites recently visited.
6. The option to add the favorite's place is available which makes the user aware of the changes in that particular place.
7. We can use both on-line and off-line mode.
8. Calling to particular shop or place is possible since the option is available.

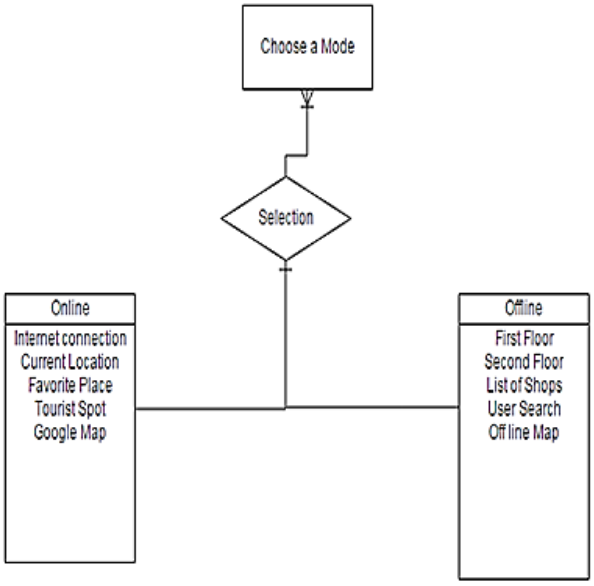
A. TVM Android

Our prototype GUI, built using our in-house Anyplace proj-ect, provides all the functionalities for a user to utilize TVM. The GUI is divided into a visualization interface and a set-tings interface. The visualization interface uses the Android Google MAP API and our proprietary Wi-Fi AP format, which captures multi-dimensional signal strength values collected from nearby AP (i.e., each AP is identified by its network MAC address and its signal strength is measured in dBm). This

allows a user to visualize its location/trace as well as the camouflaged locations/traces in both indoor and outdoor environments. At a high level, our settings interface enables a user to (i) keep a record of fingerprints on local storage and crowdsource them to the server, (ii) configure various privacy, e.g., p_u, and performance preferences, e.g., enable caching, (iii) connect to the positioning service and localize using various TVM, CS or SS methods and (iv) switch between online and offline mode to change between experimentation and real operation.

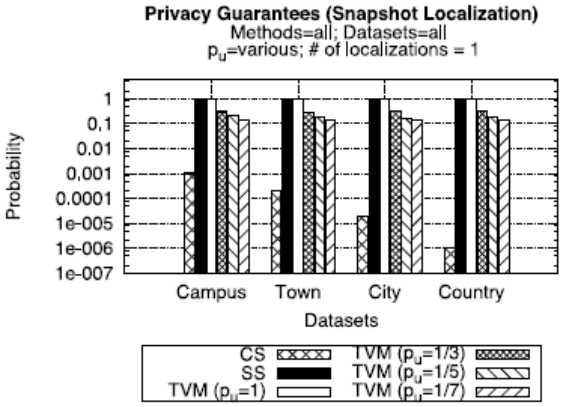
B. E-R Diagrams

- The relation upon the system is structure through a conceptual ER-Diagram, which not only specifics the existential entities but also the standard relations through which the system exists and the cardinalities that are necessary for the system state to continue.
- The Entity Relationship Diagram (ERD) depicts the relationship between the data objects. The ERD is the notation that is used to conduct the date modeling activity the attributes of each data object noted is the ERD can be described resign a data object descriptions.



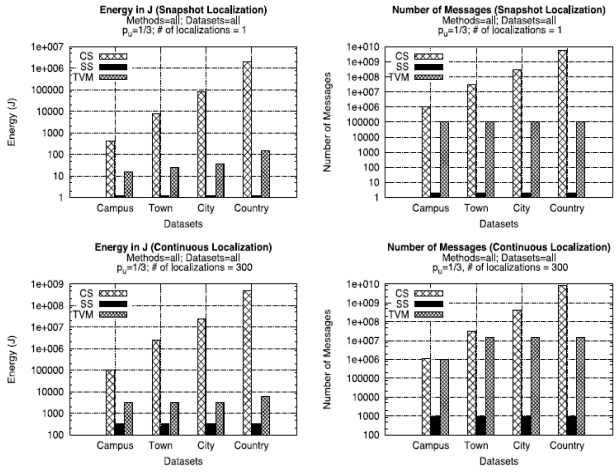
C. Experimental Evaluation

In this section, we describe the details of our experimental methodology: our datasets and our evaluation metrics. We then present the results of our evaluation using five experimental series.



The energy consumed by the CS algorithm includes downloading the RM once and consecutively localizing using the whole RM on the smartphone, rather than utilizing the much smaller pRM. This is the reason why the energy consumption of the CS is higher than TVM, in spite of the fact that their messaging cost is the same for the Cam-pus dataset. TVM and CS have a similar messaging cost for small datasets (e.g., Campus and Town) due to the fact that TVM may end up downloading the whole RM during the 300 localization efforts, just like CS. Notice, that the messaging cost is upper bound by the total size of each dataset, which is equal to the messaging cost of CS. For the large Country dataset, TVM outperforms CS in messaging cost by around two-and-a-half orders of magnitude

D. Privacy Guarantees



IV. CONCLUSION

In the contrast to the previous map applications which lacked the security and efficiency constraints, here we provide enhanced map for interior loactions using temporal vector map and Indoor Positioning Systems. In future, the improvised tracking techniques can be nurtured to increase the power reduction capability while using IPS.

V. REFERENCES

[1] Y. Gu, A. Lo, and I. Niemegeers, "A survey of indoor positioning systems for wireless personal networks," IEEE Commun. Surveys Tuts, vol. 11, no. 1, pp. 13–32, 1st Quarter 2009.

[2] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," IEEE Trans. Syst., Man Cybern., C, Appl. Rev., vol. 37, no. 6, pp. 1067–1080, Nov. 2007.

[3] L. Petrou, G. Larkou, C. Laoudias, D. Zeinalipour-Yazti, and C. G. Panayiotou. (2014). Crowdsourced indoor localization and navi-gation with anyplace, in Proc. 13th Int. Symp. Inf. Process. Sensor Netw., pp. 331–332 [Online]. Available: http://dl.acm.org/ citation.cfm?id=2602339.2602400

[4] B. H. Bloom, "Space/time trade-offs in hash coding with allow-able errors," Commun. ACM, vol. 13, no. 7, pp. 422–426, Jul. 1970.

[5] A. Konstantinidis, G. Chatzimiloudis, C. Laoudias, S. Nicolaou, and D. Zeinalipour-Yazti, "Towards planet-scale localization on smartphones with a partial radiomap," in Proc. 4th ACM Int. Workshop Hot Topics Planet-Scale Meas., 2012, pp. 9–14.

[6] G. Larkou, C. Costa, P. G. Andreou, A. Konstantinidis, and D. Zeinalipour-Yazti, "Managing smartphone testbeds with smartlab," in Proc. 27th Int. Conf. Large Installation Syst. Administra-tion, 2013, pp. 115–132.

[7] C. Laoudias, G. Constantinou, M. Constantinides, S. Nicolaou, D. Zeinalipour-Yazti, and C. G. Panayiotou, "The airplace indoor positioning platform for android smartphones," in Proc. 13th IEEE Int. Conf. Mobile Data Manag., 2012, pp. 312–315.

[8] D. Lymberopoulos, J. Liu, X. Yang, R. R. Choudhury, V. Handziski, and S. Sen, "A realistic evaluation and comparison of indoor location technologies: Experiences and lessons learned," in Proc. 14th Int. Conf. Inf. Process. Sensor Netw., 2015, pp. 178–189.

[9] B. Li, J. Salter, A. G. Dempster, and C. Rizos, "Indoor positioning techniques based on wireless LAN," in Proc. 1st Int. Conf. Wireless Broadband Ultra Wideband Commun., June 2006, pp. 13–16.

[10] L. Sweeney, "K-anonymity: A model for protecting privacy," Int. J. Uncertain. Fuzziness Knowl.-Based Syst., vol. 10, no. 5, pp. 557–570, Oct. 2002.

[11] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. (2002). Hippocratic databases, in Proc. 28th Int. Conf. Very Large Data Bases, pp. 143–154 [Online]. Available: http://dl.acm.org/citation.cfm?id=1287369. 1287383

[12] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communi-cation technique using dummies for location-based services," in Proc. Int. Conf. Pervasive Services, 2005, pp. 88–97.