isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 3 ,Apr,2016 ,ISSN_NO: 2321-3337

INDOOR LOCALIZATION USING INDOOR POSITIONING SYSTEM WITH USER DEFINED PRIVACY PRESERVATION

Ayswariya.D[1], Esther Rani.R[2],Mr.Yoganand.S[3]

Student, Dept. of Computer Science and Engineering, Agni College of Technology, India.[1,2]
Asst. Professor, Dept. of Computer Science and Engineering, Agni College of Technology, India. [3]

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. This also helps in consuming less energy than traditional systems. 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 system 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*—* **Indoor, localization, Smart phones, trajectory, fine grained, privacy, Android.**

1. INTRODUCTION

Our project has been based on mobile computing techniques and the algorithm used in this project is known as Indoor Positioning System (IPS). 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. This also helps in consuming less energy than traditional systems. 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.

People spend most of their time in indoor environments, including shopping malls, libraries, airports or university campuses. To enable such indoor applications in an energy efficient manner and without expensive additional hardware, modern smart phones rely on cloud-based Indoor Positioning Services(IPS), which provide the accurate location (position) of a user upon request. There are numerous IPS ,including Google Indoors, Navizon, Indoor Atlas. These systems rely on geolocation databases (DB) containing wireless, magnetic and light signals, upon which users can localize. In summary, a smart phone 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 smart phone itself. One fundamental drawback of IPS is that while servicing them these receive information about the location of a user, generating a variety of location privacy concerns (e.g., surveillance or data for unsolicited advertising).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).

In many respects, Tracking of locations is unethical 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, bookshelves of interest in a library, artifacts observed in a museum and generally anything else that might publicize our preferences, beliefs and habits. Clearly, there is a lot of controversy on whether this is right or wrong. 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. This holds as IPS can track users at very fine granularity over an extended period of time.

2. BACKGROUND AND RELATED WORK

In this part, we discuss background and related work on indoor localization and privacy-preserving data management, upon which our presented techniques are founded. Several technologies are available in localization literature. GPS is obviously ubiquitously available but has an expensive energy tag and is also negatively affected from the environment (e.g., cloudy days, forests, downtown areas, etc.). Besides GPS, the localization community 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. A high level of positioning accuracy is provided by most of these technologies, 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 smart phones and Wireless LANs already deployed in most buildings.

2.1 Privacy-Preserving Data Management

Location Privacy typically refers to the scenario where a data owner wants to publish data or allow spatial querying in its moving object database. To achieve privacy-preservation, the data owner must first "sanitize" the given dataset, such that no one can associate a particular record with the corresponding data subject or infer the sensitive information of any data subject. Privacy-preserving techniques for location services are based on some of the following concepts: (i) sanitized locations;(ii) spatial cloaking; (iii) space transformations; and (iv) k-anonymity.

3 SYSTEM OVERVIEW:

Software design sits at the technical kernel of the software engineering process and is applied regardless of the development paradigm and area of application. Design is the first step in the development phase for any engineered product or system. The designer's goal is to produce a model or representation of an entity that will later be built. Beginning, once system requirement have been specified and analyzed, system design is the first of the three technical activities -design, code and test that is required to build and verify software.

3.1 System Design

Goal. With minimum energy consumption on *u*, Provide continuous localization to a mobile user *u* that can measure the signal intensity of its surrounding APs, such that a static cloud-based server *s* cannot identify *u*'s location with a probability higher than a user-defined preference *pu*.

We are assuming a planar area A containing a finite set of (x, y) points and that A is covered by a set of Wi-Fi access points {ap1, ap2, . . . ,apM}, each covering a planar points. Area A is not necessarily continuous and can be considered as the joint area of all apiϵ AP (i.e., global coverage). Each api has a unique ID i.e., MAC address, that is publicly broadcasted and passively received by any one moving in the a points of api. The signal intensity at which the ID of api is received at location (x, y), is termed the Received Signal Strength of api at (x, y).

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 belongs to AP broadcasts at specified (x, y) ϵ locations. When an api is not seen at a certain (x, y) 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 ϵ AP while moving. This information is termed, here after, 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 M′<< M attributes.

We assume s to be a static (cloud-based) server of infiniteresources, similar to popular positioning and mapping services(e.g., Google Maps), where the user can only communicatewith s over the web. Given that s is fundamentallyuntrusted, we are interested in enabling a user u to localizethrough a server s without allowing *s* to know where *u* is.

3.2System Architecture

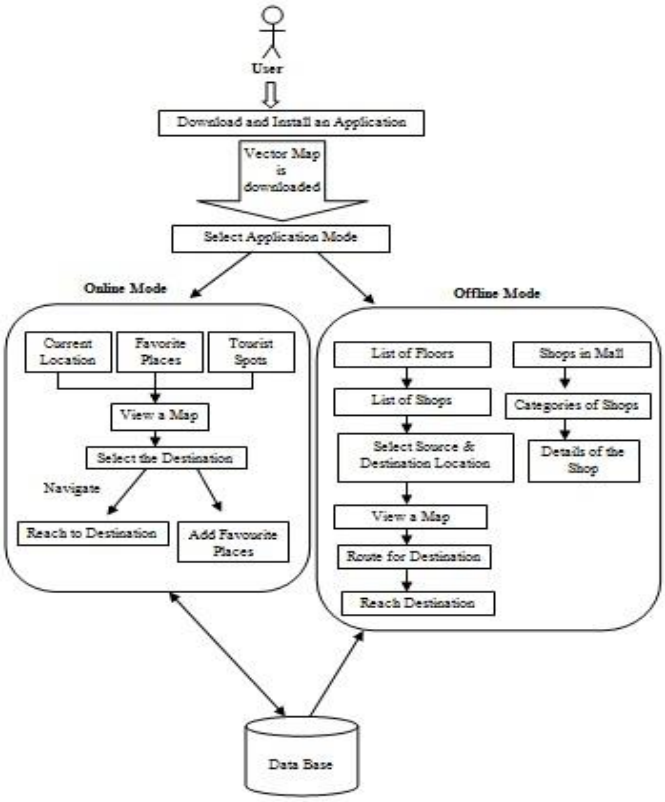

Fig 1 System Architecture

4 THE TVM ALGORITHM

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.

Algorithm 1. Temporal Vector Map

Input: Vu is the current fingerprint of *u*; *pu* 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):————————

Volume: 4, Issue: 3,Special Issue: 3 ,Apr,2016 ,ISSN_NO: 2321-3337

1: Bu ═*createkAB*(Vu,pu)
-›kAB filter in Algorithm 2
2: send Bu to s
————————Server-side (s):————————
3: Cu ═kAB to P(Bu)
-›Set of Candidate AP MACidentifiers
4: pRM═filter(RM,Cu)
-› Set of RM rows filtered byCu
5: send pRM to u
————————User-side (u):————————
6: (x, y) =localize(Vu,pRM)
-› using WKNN, RBF or SNAP
Phase 2: Subsequent Localization (of u through s)
————————User-side (u):————————
7: if (canNotBeServed(Vu,pRM)) then
8: Cu =bestNeighbors(Vu,pRM)
-› Set of APs in Algorithm3
9: send Cu to s
————————Server-side (s):————————
10: pRM=filter(RM,Cu)
-› Set of RM rows filteredby Cu
11: send pRM to u
12: end if
————————User-side (u):————————
13: (x, y) =localize(Vu,pRM)
-› using WKNN, RBF or SNAP

4.1 Outline

Algorithm 1 outlines the high-level steps of our proposed TVM algorithm for answering initial and subsequent localization queries of some user u through the service s. In phase 1, u generates a k-Anonymity Bloom filter Bu using the createkAB routine in Line 1, presented in Algorithm 2. The given filter Bu, sent to s, guarantees that s cannot identify u's location with a probability higher than pu. Upon reception, s uses Bu in Line 3, to find the set of possible matching AP identifiers Cu. In Line 4, s uses Cu to identify a partial RadioMap (pRM),which is sent to u. Using pRM, u is able to localize with known fingerprint-based algorithms such as WKNN,RBF or SNAP [7] in Line 6. In phase 2, for the subsequent localization tasks, u identifies whether it can be served from its prior pRM state in Line 7 (e.g., if a user only moved by a few meters). If this is not the case, u initiates the bestNeighbor routine in Line 8, presented in Algorithm 3. This routine generates a new set Cu, which maintains the privacy guarantees when sent to s. Upon reception, s uses the new Cu to identify the corresponding pRM in Line 10 and send it to u to complete localization.

Algorithm 2.createkAB

Input: Vu is the fingerprint of u; pu is u's privacy preference

Output: Bu kAB filter for u

1: Constants: h, M, a -› # of hash functions, ⎪AP⎪, access pointcoverage

2: api randomly chosen from Vu

-› Candidate needed forthis localization

3: k = 1/(a*pu) -›Equation (2)

4: b = b [-h/ln(1-h√k/M)] -› Equation (4)

5: for all h hash functions do

6: B[hash(api) mod b] = 1

7: end for

5. TVM Android

Our prototype GUI, built using our in-house anyplace project, provides all the functionalities for a user to utilize TVM. The GUI is divided into a visualization interface and a settings 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.

6 .IPS

Ips-Indoor Positioning System

An indoor positioning system (ips) is a system to locate objects or people inside a building using radio waves, magnetic fields, acoustic signals, or other sensory information collected by mobile devices. There are several commercial systems on the market, but there is no standard for an IPS system. IPS systems use different technologies, including distance measurement to nearby anchor nodes (nodes with known positions, eg- Wi-Fi access points), magnetic positioning, dead reckoning. They either actively locate mobile devices and tags or provide ambient location or environmental context for devices to get sensed. The localized nature of an IPS has resulted in design fragmentation, with systems making use of various optical, radio, or even acoustic technologies.

7. EXPERIMENTAL EVALUATION

In this section, we describe the details of our experimental methodology: our datasets.

7.1 Datasets

As a foundation for generating large-scale realistic Radio-Maps to carry out our trace-driven experimentation, we used the following real data:

CSUCY Data. Data is collected in a typical building at the Computer Science (CS) department of the University of Cyprus using three Android devices. In particular, it consists of 45,000 reference fingerprints taken from ~120 Wi-Fi APs installed in the four

floors of the CS and neighboring buildings. On average, 10.6 APs are detected per location. We collected our data by walking over a path that consists of 2,900 locations. The CSUCY data has a size of 2.6 MBs.

KIOSUCY Data. Data is collected inside a typical office environment at the KIOS Research Center, University of Cyprus using three different Android devices. In particular, it consists of 105 fingerprints from 10 Wi-Fi APs. The KIOSUCY data has a size of 0.14 MBs.

Crawdad Data. Data obtained from the Crawdad online archive that include fingerprints from four areas in the United States: the University of Dartmouth, a building in Kirkland Washington DC, and two buildings in Seattle. In particular, it consists of fingerprints from 6,807 distinct locations from ~1,293 APs. The Crawdad data has a size of ~17 MBs.

8.CONCLUSION

In future, the improvised tracking techniques can be nurtured to increases the power reduction capability while using IPS.In this paper, we propose a complete algorithmic frame work, coined Temporal Vector Map, for enabling a user to localize without letting the service know where the user is.

Our algorithm encapsulates a number of innovative internal components for snapshot and continuous localization. We provide an analytical study for both the performance and the privacy guarantees provided by our approach and present a real prototype system consisting of a big-databack-end and a smart phone front-end. Using. Our results indicate that TVM can offer fine grained localization in approximately four orders of magnitude less energy and number of messages than competitive approaches. In the future, we aim to carry out a field study, investigate server-side optimizations that will further boost the performance of TVM, and also investigate the applicability of the TVM framework to more generalized sensor measurements.

REFERENCES

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

[2] H. Liu, H. Darabi, P. Banerjee, and J. Liu, “Survey of wirelessindoor 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). Crowd sourced indoor localization and navigation with anyplace, in Proc. 13th Int. Symp. Inf. Process. Sensor Netw., pp. 331–332 [Online].

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

[5] G. Larkou, C. Costa, P. G. Andreou, A. Konstantinidis, and D.Zeinalipour-Yazti, “Managing smart phone test beds with smart lab,” in Proc. 27th Int. Conf. Large Installation Syst. Administration,2013, pp. 115–132.

[6] C. Laoudias, G. Constantinou, M. Constantinides, S. Nicolaou, D.Zeinalipour-Yazti, and C. G. Panayiotou, "The air place indoor positioning platform for android smart phones," in Proc. 13th IEEEInt. Conf. Mobile Data Manag., 2012, pp. 312–315.

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

[8] M. L. Yiu, C. S. Jensen, X. Huang, and H. Lu, "Spacetwist: Managingthe trade-offs among location privacy, query performance, and query accuracy in mobile services," in Proc. 24th IEEE Int.Conf. Data Eng., 2008, pp. 366–375.