EAI/Springer Innovations in Communication and Computing

Sara Paiva *Editor*

Precision Positioning with Commercial Smartphones in Urban Environments

EAI
RESEARCH MEETS INNOVATION

Springer

EAI/Springer Innovations in Communication and Computing

Series Editor

Imrich Chlamtac, European Alliance for Innovation, Ghent, Belgium

Editor's Note

The impact of information technologies is creating a new world yet not fully understood. The extent and speed of economic, life style and social changes already perceived in everyday life is hard to estimate without understanding the technological driving forces behind it. This series presents contributed volumes featuring the latest research and development in the various information engineering technologies that play a key role in this process.

The range of topics, focusing primarily on communications and computing engineering include, but are not limited to, wireless networks; mobile communication; design and learning; gaming; interaction; e-health and pervasive healthcare; energy management; smart grids; internet of things; cognitive radio networks; computation; cloud computing; ubiquitous connectivity, and in mode general smart living, smart cities, Internet of Things and more. The series publishes a combination of expanded papers selected from hosted and sponsored European Alliance for Innovation (EAI) conferences that present cutting edge, global research as well as provide new perspectives on traditional related engineering fields. This content, complemented with open calls for contribution of book titles and individual chapters, together maintain Springer's and EAI's high standards of academic excellence. The audience for the books consists of researchers, industry professionals, advanced level students as well as practitioners in related fields of activity include information and communication specialists, security experts, economists, urban planners, doctors, and in general representatives in all those walks of life affected ad contributing to the information revolution.

Indexing: This series is indexed in Scopus, Ei Compendex, and zbMATH.

About EAI

EAI is a grassroots member organization initiated through cooperation between businesses, public, private and government organizations to address the global challenges of Europe's future competitiveness and link the European Research community with its counterparts around the globe. EAI reaches out to hundreds of thousands of individual subscribers on all continents and collaborates with an institutional member base including Fortune 500 companies, government organizations, and educational institutions, provide a free research and innovation platform.

Through its open free membership model EAI promotes a new research and innovation culture based on collaboration, connectivity and recognition of excellence by community.

More information about this series at http://www.springer.com/series/15427

Sara Paiva
Editor

Precision Positioning with Commercial Smartphones in Urban Environments

Springer

EAI
RESEARCH MEETS INNOVATION

Editor
Sara Paiva
Instituto Politécnico de Viana do Castelo
Viana do Castelo, Portugal

ISSN 2522-8595 ISSN 2522-8609 (electronic)
EAI/Springer Innovations in Communication and Computing
ISBN 978-3-030-71287-7 ISBN 978-3-030-71288-4 (eBook)
https://doi.org/10.1007/978-3-030-71288-4

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This book intends to provide an insight about recent trends, solutions, and approaches to real-life scenarios, where urban mobility is challenged by the lack of precision of the Global Positioning Systems, paving the way for new approaches that can provide location and context-aware secure services and solutions to citizens.

The book is organized in seven chapters. The first and second chapters address security issues and mitigation strategies. The first chapter proposes various spoofing detection techniques to be applied on mobile devices, using location and context information. Authors test the techniques on Android apps and study the effects of the detection parameters in order to achieve a desired trade-off between false-alarm and misdetection probabilities. The second chapter uses a crowd-sensing approach to inform the user of public transports location when the bus is unable to communicate its position. The proposed solution also addresses security issues to identify and deal with malicious attacks. The third chapter refers to location-based services (LBS), infrastructures and systems, and also outlines open research issues in provisioning of LBSs. The fourth chapter provides a comprehensive survey of Proximity-Based Social Networking (PSBN) and a new model of categorization of PSBN is presented as well as its thorough evaluation based on several important criteria. Chapter "Satellite Navigation" has the key objective to explain both the global and regional level satellite navigation system and its technology and application. Chapter "Bluetooth Low Energy (BLE) Beacon-Based Micro-positioning for Pedestrians Using Smartphones in Urban Environments" presents a Bluetooth Low Energy (BLE) beacon-based system for positioning in urban environment using smartphones, mainly intended for pedestrians. Finally, Chapter "Legal Issues and the Need to Engineer Positioning Systems for Protection of Privacy and Personal Security" discusses regulations that guide systems that make use of location data so they are in compliance with law, ethics, and social values.

This book attracted contributors from all over the world, and I would like to thank all authors that have contributed to this book. Also, a word of appreciation to all reviewers for their review work and to all those who made this book become a reality.

Viana do Castelo, Portugal Sara Paiva

Contents

Context-Based Detection of GNSS Position Spoofing for Smartphones

Francesco Formaggio, Silvia Ceccato, Nicola Laurenti, and Stefano Tomasin

In this chapter, following the trace of [1], we delve into three solutions to let smartphones detect GNSS spoofing attacks. The first, and most simple, foresees the analysis of the visible satellites and the corresponding navigation message, checking both its integrity and its correctness. The second approach, first introduced in [2], makes use of the network connectivity of the smartphone, which provides alternative location information, in order to verify the consistency of the global navigation satellite system (GNSS) measurements. Finally, with the third approach we process the smartphone inertial measurements unit (IMU) data with a Kalman filter (KF) to derive a suitable spoofing detection mechanism.

1 Literature Background

The *spoofing* attack is a well known threat, where a malicious entity forges fake GNSS signals in order to trick a victim receiver into computing the desired false position and/or time. An extensive literature has been produced on spoofing detection for various use cases [3–17].

Spoofing detection in vehicular applications is investigated in [6], where a mobile device is used for comparing the absolute value of linear and angular acceleration with those obtained from GNSS. This approach avoids the calibration of inertial measurements units (IMU) and is invariant to manipulations of the device initial orientation. The automotive scenario is also the target application of [7], wherein the

F. Formaggio · S. Ceccato · N. Laurenti · S. Tomasin (✉)
Department of Information Engineering, University of Padova, Padova, Italy
e-mail: francesco.formaggio@dei.unipd.it; silvia.ceccato@dei.unipd.it; nicola.laurenti@dei.unipd.it; stefano.tomasin@dei.unipd.it

S. Paiva (ed.), *Precision Positioning with Commercial Smartphones in Urban Environments*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-71288-4_1

proposed solution integrates data from GNSS, IMU, and the odometer. Differently from [10] and [6], the comparison metric is position rather than acceleration, and the detection statistics are obtained as the norm of the difference between position vectors (from GNSS and from IMU or odometer). The novelty in this approach is the idea of performing GNSS-based sensor calibration at fixed time intervals only when the GNSS signal is considered authentic.

Note that it is generally believed to be impractical for an attacker to spoof a vehicle position without the end user detecting the inconsistency with the surrounding environment. However, in [11] the adversary aims at luring a victim receiver to a specific location, while maintaining the consistency between outside environment and Google Maps' trajectory. The spoofing optimization algorithm searches for areas of the map that are topologically similar to the road shape in the user real location. The spoofing signal then induces a jump to the user location, eventually driving it to the selected fake position through a path that mimics on the map the user actual trajectory, making it hard for the receiver to notice the attack.

In aviation, the authors of [10] identify high frequency acceleration components as a suitable source of randomness for authentication purposes, similarly to [8]. The work targets an attacker with imperfect information on the precise aircraft acceleration and develops a spoofing detection algorithm based on decoupling IMU and GNSS positioning, providing a direct comparison of the acceleration for an unlimited time window.

Other anti-spoofing techniques include cryptographic mechanisms applied to the navigation message [12, 13], spreading code encryption [14], signal quality monitoring techniques [15, 16], and physical-layer authentication schemes [17, 18].

Only in recent years the interest in anti-spoofing techniques has been extended to mobile devices applications. As location-based services (LBS) are now deeply integrated in billions of people everyday life, the security of positioning in mobile phones has become a concern. The most popular application of LBS is navigation: traffic monitoring, vehicle management, and road information are just some of the services that exploit positioning information in smartphones, offering guidance in unfamiliar environments and improving the overall traveling experience. LBS have also spurred the development of taxi sharing platforms, (e.g., Uber and Lyft) that have become a competitive alternative to other services, thanks to features such as real time monitoring for both providers and customers. Several other fields now benefit from LBS, such as emergency and disaster management, insurance and financial applications, and production process support. Home banking, financial transactions, mobile based transportation, goods delivery, and access control based on location proximity are just some examples of services readily accessible from our mobile device that could be compromised by spoofing attacks. Indeed, in [1] evidence is provided that even modern smartphones are vulnerable to such security threats. Table 1 (from [1]) shows the time needed to obtain a fix for various smartphones models, under three spoofing attacks:

Exp. 1 Spoofing from the correct position (Padova, Italy) to the fake position (New York, USA).

Table 1 Navigation data spoofing: Experiment results, from [1]

	Time to fix			
Smartphone	Exp. 1	Exp. 2	Exp. 3	Exp. 4
Apple iPhone 5	< 30 s	< 60 s	No fix	No fix
Apple iPhone 6s	< 120 s	< 30 s	No fix	No fix
Apple iPhone SE	< 60 s	< 60 s	No fix	No fix
Asus Nexus 7	< 120 s	< 30 s	No fix	No fix
Asus Zefone 2	< 30 s	< 180 s	< 30 s	No fix
Google Pixel	< 30 s	< 60 s	< 30 s	No fix
HTC one M9	< 60 s	No fix	No fix	No fix
Huawei Honor 8	< 30 s	< 30 s	< 30 s	< 30 s
Huawei Honor 9	< 30 s	< 30 s	< 120 s	< 120 s
Huawei p8 lite	< 60 s	< 180 s	No fix	No fix
Huawei p10 lite	< 30 s	< 120 s	No fix	No fix
LG Nexus 5	< 30 s	< 30 s	No fix	No fix
LG Nexus 5x	< 30 s	< 60 s	No fix	No fix
LG G6	< 30 s	< 60 s	< 60 s	No fix
LG G3	< 120 s	< 120 s	No fix	No fix
Motorola Moto G	< 30 s	< 30 s	No fix	No fix
OnePlus 2	< 60 s	< 120 s	No fix	No fix
OnePlus 5	< 60 s	< 120 s	No fix	No fix
Samsung S6 Edge	< 30 s	< 30 s	< 30 s	< 30 s
Samsung S6	< 30 s	< 60 s	< 60 s	< 240 s
Samsung S7 Edge	< 60 s	< 120 s	< 60 s	< 30 s
Xiaomi Mi 4c	< 60 s	< 120 s	No fix	No fix
Xiaomi Mi5	< 30 s	< 30 s	No fix	No fix
Xiaomi Mi6	< 120 s	No fix	No fix	No fix
Xiaomi Redmi Note 4x	< 60 s	< 120 s	< 30 s	No fix

Exp. 2 Spoofing from the Empire State Building to Canberra, Australia. In the spoofed signal navigation data were erased, except for the telemetry word, the handover word, and the time indicators. Old navigation data was used by the smartphone.

Exp. 3 Spoofing from the Empire State Building to the New York airport. In the spoofed signal all navigation data erased. Old navigation data was used by the smartphone.

Exp. 4 Spoofing from the Empire State Building to Canberra, Australia. In the spoofed signal all navigation data erased and all stored data in smartphone was erased.

See [2] for more details on the experiments.

2 Visible Satellites and Navigation Message

In this Section we present a client-server (CS) architecture designed to detect specific spoofing attacks. This CS architecture was also implemented in the form of an Android application (APP). In the context of GNSS spoofing, the client, or user, is also the victim receiver, subject to the attacker's GNSS signals. The server instead is an external application, which we assume authentic and capable of reliable communication with the user.

2.1 Attack Model

We consider spoofing attacks, wherein an attacker generates false GNSS signals and sends them to the victim receiver with the intention to induce a position estimation that does not correspond to the true user's position.

The attacker chooses a fake position and the set of satellites, visible from the fake position, that he intends to spoof. We then distinguish two attacks.

1. The attacker does not *null* the legitimate signals received by the user, while instead he transmits a higher power spoofing signal. Note that nulling is theoretically feasible, since for every time and every position it is possible to predict the exact shape of any legitimate GNSS signal; therefore, the attacker could send these signals with inverse polarity and cancel them at the victim receiver. However, nulling requires the exact computation of the carrier phase at each time instant, which is a demanding task, corroborating the significance of this first attack model.
2. In this case, the attacker tampers also with the navigation message, modifying its content or even completely deleting all information. This might not seem a clever attack, since predicting the navigation message is not as difficult as the carrier phase estimation problem for nulling. However, in [1] it is shown that nowadays smartphones obtain positioning information even from GNSS signals with incorrect or missing navigation message. Moreover, the attacker might want to simply disrupt or destructively interfere with the GNSS services, making the navigation message manipulation its very objective.

2.2 Client-Server Architecture

The proposed CS architecture is shown in Fig. 1, where, as previously mentioned, the client represents the victim receiver, subject to the two attacks described in Sect. 2.1.

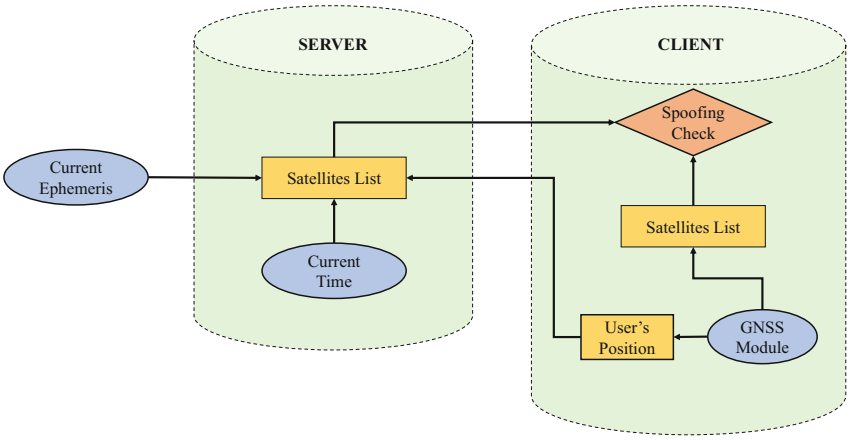


Fig. 1 CS architecture of the proposed spoofing detection strategy. The client queries the server sending the computed position, and the server answers with a list of visible satellites, for which the spoofing check is performed

The spoofing detection procedure starts with the GNSS module at the client side, which provides an estimation of the user's position. The client then queries the server by sending the estimated position itself.

The server keeps an updated version of ephemeris data, which are typically stored in institutional websites, such as [19] for GPS. Indeed, in Fig. 1 the current ephemeris block is placed outside the server, because it represents already existing information and the server needs only to retrieve it. With current ephemeris, current time (also available at the server), and user's position, the server builds a list of satellites that are visible from the client's position and sends it back to the client itself. The list contains the satellites' identifiers (IDs), which uniquely identify each satellite by its spreading code number, and the satellite's positions (azimuth and elevation). Note that the server does not use any GNSS module to build the list, therefore it is not subject to GNSS spoofing and the information sent to the user is assumed authentic.

At the client's side, another satellite list is produced, equivalent to the one at the server, but this time the IDs and positions of satellites are computed directly by the GNSS module, thus being prone to forgery. Indeed, the spoofing check consists in comparing the satellite list produced by the client and the one coming from the server, as shown in Fig. 1.

2.3 Spoofing Check

The spoofing detection at the client includes two checks against the two attacks of Sect. 2.1.

The first check needs actually only the satellites' IDs retrieved by the client through the GNSS module. Retrieving this information does not require the decoding of the navigation message, since spreading codes are known, and the visible IDs are available right after acquisition.

Let S_u and S_s be the set of IDs retrieved by the user and the server, respectively. Then the first spoofing check output is the Boolean results of the following expression

$$S_u \subseteq S_s. \tag{1}$$

The spoofing check reports no spoofing when the user sees only satellites that are supposed to be in view from his position. Otherwise, a flag is raised, meaning that there might be an ongoing spoofing attack. Note that we use the subset operator rather than equality, because even in nominal conditions some satellites may not be in view due to physical obstacles, e.g., buildings or trees.

The spoofing check (1) is designed to tackle attack 1 of Sect. 2.1. If the attacker does not null the legitimate signal (as discussed in the previous section), the user may be able to acquire also the legitimate satellites, even if tracking and position estimation are performed based on the more powerful spoofed satellites. Therefore, this spoofing check detects attacks inducing a fake position for which the visible satellites are different from those in view from the user true positions. If the true and fake positions are close enough to yield the same set of visible satellites, the attack goes undetected.

However, time also plays an important role, the satellites in view changes over time, therefore the acquired satellites may be inconsistent with the time/position spoofed by the attacker. Indeed, *time spoofing* is also an important attack to smartphones, since system level applications may rely on the GNSS time output and temporal inconsistencies can cause software failures (see [1]). Moreover, tampering with the navigation message (attack 2) can also result in such timing difference, triggering spoofing detection.

As previously mentioned, (1) can be evaluated without looking at the navigation message, and the attack 2 of Sect. 2.1 can easily go undetected if induced position and time satisfy the satellite visibility constraints. Therefore, to address navigation message tampering we compare the azimuth and elevation angles of the two satellites' lists.

The second check procedure works as follows. For every ID in S_u, retrieve its corresponding element in the server's list. If such element does not exist, the first spoofing check detects spoofing. Otherwise, compare the satellite's coordinates in the two lists. If the difference is above a suitable threshold, raise a spoofing warning, otherwise declare that no spoofing attack is occurring. Note that when comparing the satellites' coordinates, the threshold is needed whenever (as often occurs) communications and data processing of the CS architecture introduce a random delay. Indeed, even in nominal conditions, azimuth and elevation computed by client and server will not be the same due to the different computation instants. A timestamp sent by the user would solve the problem, but, at the same time, would pave the way for time spoofing attacks.

Unlike satellites' IDs, both azimuth and elevation can only be computed after decoding of the navigation message, therefore, attack 2 is immediately revealed when the navigation message is absent or corrupted in the specific fields used to compute the satellite position.

2.3.1 Stand-Alone Navigation Message Checks

Following the trace of the second proposed spoofing check, other integrity inspections aimed at verifying the compliance of the navigation message fields can be considered.

Some compliance check do not require the CS architecture, and can be performed offline. For example, navigation message specifications, are publicly available (e.g., see [20]), and some verification functions can be hard coded in the smartphone's software. Examples of compliance checks are:

- the *week number* filed must be equal for all satellites currently in view;
- the *issue of data clock* (IODC) and the *issue of data ephemeris* (IODE) are always between 0 and 1023.

2.3.2 Remark

The proposed spoofing checks are specific against the considered attacks, while more sophisticated attacks, e.g., a combination of GNSS spoofing and server hijacking, may go undetected. However, when a user can rely on such CS architecture and on the stand-alone techniques, the attacker's degrees of freedom are significantly reduced. Also, this approach assumes that the user has access to the server via a network connection, which is quite reasonable, given the smartphone-oriented use case.

2.4 Android Implementation

The architecture of Fig. 1 has been implemented, whereas the client is an Android APP running on the user smartphone, and the server is a desktop application.

Figure 2 shows two screenshots of the Android APP. In Fig. 2a the client has just acquired data from the GNSS module and the APP displays the list of visible satellites together with information on the decoded navigation message. At this stage, the APP shows the client's satellite list of Fig. 1.

Then, by tapping on the `Analyze` button, the client queries the server, which promptly answers with its own satellite list, and the spoofing checks is performed. This corresponds to Fig. 2b, where in the first half of the screen the two satellite lists are shown. The experiment has been carried out in nominal conditions, i.e., without

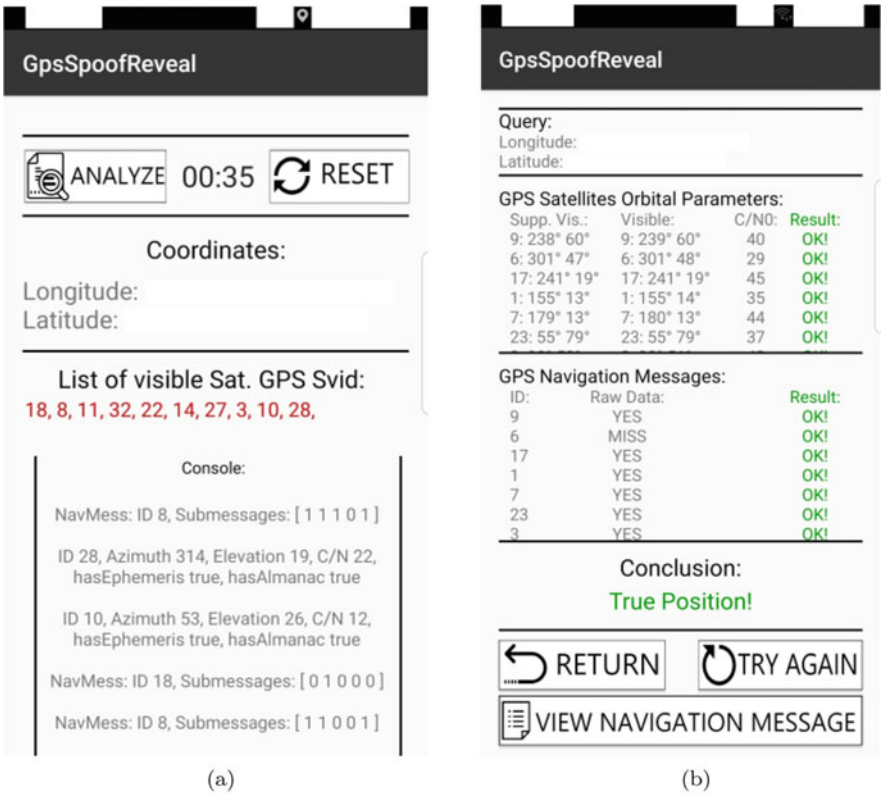


Fig. 2 Screenshots of the developed APP: data acquisition and spoofing checks with the data received from the server. (**a**) Acquisition of satellites at the client. (**b**) Spoofing checks on the visible satellites

spoofing, and the results show that all azimuth and elevation values differ at most by one degree, providing a design direction for the spoofing check threshold.

3 Network Connectivity

In this Section we report a novel technique that checks the consistency between the position estimates obtained by GNSS and the cellular network, summarizing our work [2]. For the latter estimate we propose two distinct solutions: one is based on the position of the base stations (BSs) (see Sect. 3.1) and the other directly on the smartphone position estimated by the cellular network (see Sect. 3.2). Both these solutions assume that the user has access to the network, and rely also on its security.

We have also implemented the proposed techniques in an Android APP and tested its effectiveness in detecting spoofing attacks.

3.1 BS-Position-Based Solution

A first simple solution to detect a spoofing attack is checking the consistency between the GNSS position and the region covered by the serving cell, as identified by the BS connected to the smartphone. With this technique we need to know: the position reported by the GNSS, the position of the serving BS, and its coverage area. We observe that the BS position is available since the second generation of cellular networks, i.e., with the global system for mobile communications (GSM); still, here we focus on a forth generation network, and Android application programming interface (API). By using the `TelephonyManager` class we obtain the cell ID and the location area code (LAC), that provide a unique identification of the BS in the network.

About the BS position, it can be easily retrieved by open databases available on Internet, such as OpenCellId [21] or Mozilla Location Service [22]. Note that a secure implementation of this solution would require secure communication with these servers and the assurance that the stored data are correct. As a proof of concept, the OpenCellId has been used in [2].

A third needed information is the coverage area. This is the most problematic data, which is not provided by available databases with good precision. For example, CellMapper [23] provides an approximated estimate of the coverage area, as shown in Fig. 3. Due the absence of the accurate coverage area, only qualitative information is obtained. A second option would be to model cells as Voronoi regions around each BS. Thus, by using the information on the BS position provided by OpenCellId, we can obtain the coverage information. Still, this procedure is based on a relevant assumption, and again it is hard to determine the resulting false-alarm and misdetection probabilities of spoofing detection.

Although this approach is very qualitative, it can protect against strong attacks to which current smartphones are subject, where the fake position is set thousands of kilometers from the true position (see [1, experiment 1]).

3.2 Network-Provided Position

A second, more accurate spoofing detection procedure checks the consistency between the position provided by the GNSS device and that provided by the cellular network. Indeed, from the 3rd generation of cellular systems, the network estimates the user position by exploiting directly the cellular signals, without resorting to the user GNSS device. In particular, we use the Android class `LocationManager`, which reports the position as given by the network provider, denoted network position (NP). By default, the NP is obtained by processing signals of WiFi access points nearby to the user. At the time of writing this Chapter, there is no clear distinction between the NP obtained only from cellular network signals and that obtained also from WiFi signals, in the Android documentation. However,

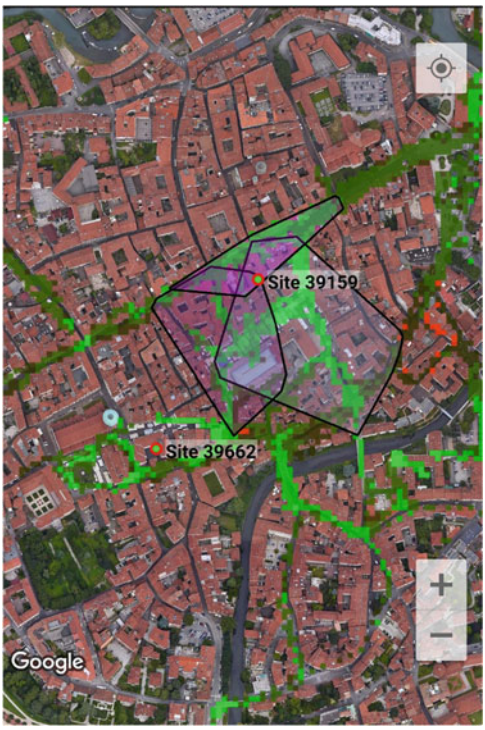


Fig. 3 Base stations and estimated coverage area. Screenshot from [23]

it is always possible to force the NP to rely only on the cellular network, by switching off the WiFi module. If in the future it will be possible to distinguish position estimations obtained from different signals (cellular network, WiFi, ...) the technique presented in this section can be easily extended to these richer scenarios.

In [2] an analysis of this spoofing detection technique has been carried out, exploiting the accuracy provided by the Android APIs on both GNSS position (GP) and NP estimates. In particular, starting from the two hypotheses

$$\begin{cases} \mathcal{H}_0 & \text{the GNSS module works correctly,} \\ \mathcal{H}_1 & \text{the GNSS module is under spoofing,} \end{cases} \tag{2}$$

the generalized likelihood ratio test (GLRT) has been derived, assuming a Gaussian distribution of the positions under hypothesis $\mathcal{H}_0$, i, l.

$$\hat{\mathcal{H}} = \begin{cases} \mathcal{H}_0 & \text{if } ||\hat{\boldsymbol{g}} - \hat{\boldsymbol{n}}|| < \gamma \\ \mathcal{H}_1 & \text{if } ||\hat{\boldsymbol{g}} - \hat{\boldsymbol{n}}|| \geq \gamma, \end{cases} \tag{3}$$

where γ is a threshold to be set for the desired false alarm probability, and $\hat{\boldsymbol{g}}$ and $\hat{\boldsymbol{n}}$ are the GP and NP, respectively.

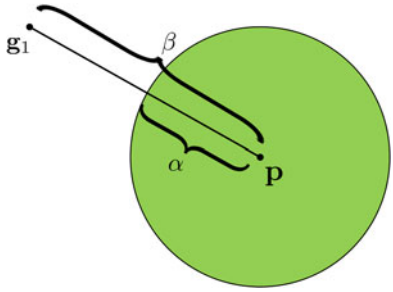


Fig. 4 α attack scenario, under hypothesis $\mathcal{H}_1$

When assuming specific attacks, the likelihood ratio test can be performed, which provides a more effective detection. In [2] two kinds of attacks have been considered: the α attack and the border spoofing attacks.

The α attack induces a fake position that is at least at distance α from the true one. In this scenario the measurement model under the two hypotheses is then

$$\mathcal{H}_0: \quad \hat{\boldsymbol{g}} = \boldsymbol{g}_0 + \xi_G e^{j\theta_G}, \quad \hat{\boldsymbol{n}} = \boldsymbol{p} + \xi_N e^{j\theta_N}, \tag{4a}$$

$$\mathcal{H}_1: \quad \hat{\boldsymbol{g}} = \boldsymbol{g}_1 + \xi_G e^{j\theta_G}, \quad \hat{\boldsymbol{n}} = \boldsymbol{p} + \xi_N e^{j\theta_N}, \tag{4b}$$

where $\boldsymbol{g}_0$ and $\boldsymbol{g}_1$ are the spoofed positions under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively, $\boldsymbol{p}$ is the true position, and the other parameters model the estimation errors. Note that it can also be $\boldsymbol{g}_0 = \boldsymbol{p}$ in the absence of spoofing. Due to the constraint on the distance of the spoofed position with respect to the correct one we have

$$||\boldsymbol{p} - \boldsymbol{g}_1|| \geq \alpha. \tag{5}$$

Figure 4 shows the α attack scenario under hypothesis $\mathcal{H}_1$, where β is the attack distance such that $\beta \geq \alpha$.

With the border spoofing attack the attacker aims at inducing a position that is beyond a known border, or inside a specific region in space. For example, this attack is meaningful against location-based services, where a service is granted only if the user is in a specific area, and the attacker wants to induce a position inside the specific area, in order to get access to the service. In [2] the specific area border is approximated as piece-wise linear, and the line closer to the correct position has known angular coefficient m and intercept q. The resulting scenario is shown in Fig. 5, where d_1 and d_2 are the distances from the border of $\boldsymbol{p}$ and $\boldsymbol{g}$, respectively. In this case, the measurement model is

$$\mathcal{H}_0: \quad \hat{\boldsymbol{g}} = \boldsymbol{p} + \xi_G e^{j\theta_G}, \quad \hat{\boldsymbol{n}} = \boldsymbol{p} + \xi_N e^{j\theta_N}, \tag{6a}$$

$$\mathcal{H}_1: \quad \hat{\boldsymbol{g}} = \boldsymbol{g} + \xi_G e^{j\theta_G}, \quad \hat{\boldsymbol{n}} = \boldsymbol{p} + \xi_N e^{j\theta_N}, \tag{6b}$$

where $\boldsymbol{g}$ is the spoofed position under $\mathcal{H}_1$.

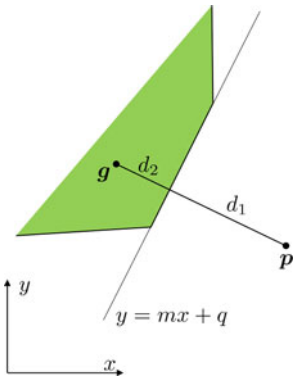


Fig. 5 Border spoofing scenario

While for a generic spoofing attack the GLRT uses the simple expression reported in (3), for both the α and the border spoofing attack we can provide specific defences requiring the following additional steps. First, the unknowns quantities $(\boldsymbol{p}, \boldsymbol{g}_0, \boldsymbol{g}_1)$ of (4), and $(\boldsymbol{p}, \boldsymbol{g})$ of (6), are estimated via a maximum likelihood approach, using the NP and GP measurements, as detailed in [2]. Then, the likelihood function can be computed as

$$\mathcal{L}(\hat{\boldsymbol{g}}, \hat{\boldsymbol{n}}) = \frac{p(\hat{\boldsymbol{g}}|\mathcal{H}_0)\, p(\hat{\boldsymbol{n}}|\mathcal{H}_0)}{p(\hat{\boldsymbol{g}}|\mathcal{H}_1)\, p(\hat{\boldsymbol{n}}|\mathcal{H}_1)}, \tag{7}$$

where the conditional probability density function $p(\cdot|\cdot)$ are derived from the measurement models (4) and (6), and computed using the estimated parameters. Finally, the detection test for both the α and the border spoofing attack is

$$\hat{\mathcal{H}} = \begin{cases} \mathcal{H}_0 & \text{if } \mathcal{L}(\hat{\boldsymbol{g}}, \hat{\boldsymbol{n}}) \geq \gamma', \\ \mathcal{H}_1 & \text{if } \mathcal{L}(\hat{\boldsymbol{g}}, \hat{\boldsymbol{n}}) < \gamma', \end{cases} \tag{8}$$

where for each value of the threshold γ' we obtain different performance in terms of false alarm and misdetection probability, i.e., the detection error tradeoff (DET).

3.3 Numerical Results

The idea of comparing the network-provided position with the GNSS position has been tested through an Android APP. An example of screenshot of the APP, under a spoofing attack is shown in Fig. 6: the two positions are shown, and a traffic light (showing red in this case) indicates that a spoofing attack has been detected. We recall that the two positions in Fig. 6 are the NP and the GP described in Sect. 3.2, and the underlying spoofing detection strategy follows the GLRT in (3), where the

Fig. 6 Screenshot taken from our APP, under a spoofing attack

threshold γ can be set by the user or it can be designed and hard coded, upon offline testing, in order to meet a certain false-alarm probability.

The false position in Fig. 6 is set to Lat. 40.7484404°, Long. −73.9878441°, i.e., the Empire State Building in New York City, USA. Note that this is the same setting of [1, Exp. 1]. Clearly our solution is able to detect the spoofing attacks where the fake position is far away from the correct one, a situation that remains undetected in nowadays smartphones, as shown in Table 1.

By collecting data from a measurement campaign, the APP has been tested and the DET curve of Fig. 7 shows the misdetection probability as a function of the false-alarm probability. The attack in this case is simulated by adding an offset δ to the GNSS position measurements. Both the GLRT test for a generic attack (continuous lines) and the test for α attack with $\alpha = 100$ m (dashed lines) have been performed. The continuous lines correspond to test (3) and, again, bigger δ means better detection performance. The detection test used for the α attack is, instead, given by (8). Note that in this case performance obtained with the two tests is almost identical.

Simulations have also been conducted to test specific α and border attack. For both attacks the detection test is given by (8), where however $\tilde{\boldsymbol{\theta}}$ changes with the attack, as seen in Figs. 4 and 5. Figure 8 shows the DET for α attack, $\alpha = 100$ m, $\boldsymbol{g}_0 = \boldsymbol{p}$, and different values of β. We observe that as the distance of the fake position from the correct position increases, the spoofing detection mechanism is

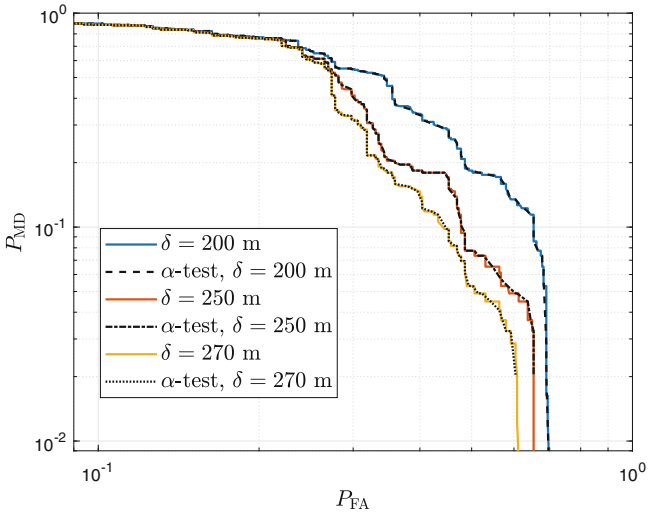


Fig. 7 DET on data from the measurement campaign, from [2]

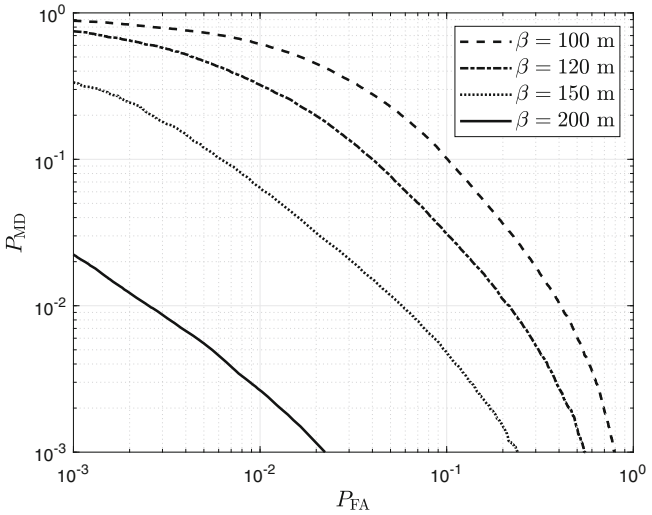


Fig. 8 DET for α attack and different values of β

more effective. For the border attack, Fig. 9 shows the DET for $d_2 = 0$ m and different values of d_1. Also in this case we observe that performance improves for attacks of more remote positions.

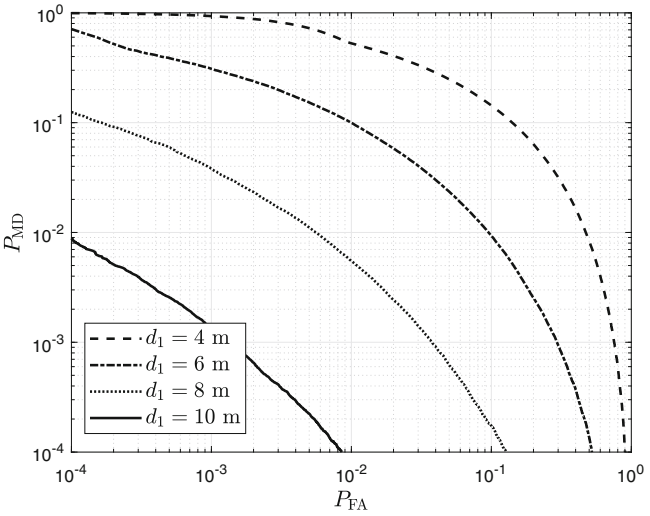


Fig. 9 DET for border attack, $d_2 = 0$ m and different d_1

4 IMU Data

This section tackles the use of opportunity data collected from integrated IMU for anti-spoofing purposes. This mechanism is well known in safety critical applications such as aviation, where several works have investigated the security improvement provided by high precision sensors, [8, 9]. Since raw GNSS measurements are now available to Android smartphones applications [24], several works are focusing on integrating GNSS and IMU measurements in mobile devices, not only for performance improvement, but also for security enhancement. In [25] a comparison of the performance improvement in the position, velocity, and time (PVT) between loosely and tightly coupled GNSS/IMU is carried out and compared to a system solely relying on GNSS. The result highlights how the tightly-coupled implementation boosts performance. Some relevant implementation issues are pointed out, such as the critical time synchronization between inertial-sensor measurements and GNSS chip set, the problem of data latency, and the management of different sampling frequencies. The authors of [26] and [10] perform quality assessment of measurements taken with IMU and GNSS chip sets in different mobile phone models. They point out how even measurements from low-cost IMUs of mobiles provide useful data for navigation integration. The performance of low-cost accelerometers for anti-spoofing in aviation is reviewed in [10], where high-frequency acceleration components are identified as a suitable source of randomness for authentication purposes, similarly to [8]. The work targets an attacker with imperfect information on the precise aircraft acceleration and develops a spoofing detection algorithm based on the decoupling of IMU and GNSS acceleration, allowing a direct comparison of acceleration for an unlimited

time window. The proposed detection algorithm is reviewed in different application scenarios such as railways and automotive, wherein is found to be less effective due to the lower intensity of high frequency components in the acceleration process. Spoofing detection in vehicular applications is investigated in [6], where a mobile device is used for comparing the absolute value of linear and angular acceleration with those obtained from the GNSS solution. This approach avoids the calibration of IMU and is invariant to manipulations to the device initial orientation. The automotive scenario is also the target application of [7], wherein the proposed solution integrates data from GNSS, IMU, and odometer. Differently from [10] and [6], the comparison domain is position and not acceleration, and the detection statistics are obtained as the norm of the difference between position vectors (from GNSS and from IMU/odometer). The novelty in this approach is the idea of performing GNSS based sensor calibration at fixed time intervals only if the spoofing detection algorithm confirms that the GNSS solution is authentic.

Several works in the literature have investigated the problem of anti-spoofing via integration and comparison with IMU data. The abundance of recent works on this idea confirms the interest of the community towards this topic.

4.1 Inertial Measurement Units

An IMU is usually composed by a combination of multiple accelerometers and gyroscopes that measure the force acting on them (and thus the resulting linear acceleration) and it angular velocity, respectively [27]. Some IMUs also integrate a magnetometer that measures the Earth magnetic field.

The general problem of navigation through sensor fusion, i.e., the integration of multiple positioning sources to obtain a more accurate and robust PVT solution, deals with data transformation between different coordinate frames. Following the approach of [28]:

Body frame, b: is the reference frame for IMU outputs. Its origin is located in the center of the accelerometer triad and the axes are generally aligned to the IMU case.

Navigation frame, n: is the target local geographical frame, where we want to measure the device PVT. In order to integrate the inertial IMU measurements we need to know the position and orientation of the b-frame with respect to the n-frame.

Inertial frame, i: is stationary with respect to the Earth. It has the origin in its center and the axis aligned with the stars;

Earth frame, e: rotates with the Earth (origin in the Earth center and axis fixed with respect to the Earth).

As reported in [28] the IMU outputs acceleration and angular velocity of the body frame relative to the inertial frame, with measurements that are expressed in the body frame (i.e., with the body frame as reference basis).

4.1.1 Gyroscope Measurements

The gyroscope measures the angular velocity of the body frame relative to the inertial frame, $\boldsymbol{\omega}_{\text{ib}}^{(\text{b})}$, where superscript (b) indicates that the vector is expressed through coordinates in the b-frame. For navigation purposes we are interested in the angular velocity of the sensor relative to the navigation frame expressed in the b-frame

$$\boldsymbol{\omega}_{\text{nb}}^{(\text{b})}(t) = \boldsymbol{\omega}_{\text{ib}}^{(\text{b})}(t) - R^{(\text{bn})}(t)(\boldsymbol{\omega}_{\text{en}}^{(\text{n})}(t) + \boldsymbol{\omega}_{\text{ie}}^{(\text{n})}), \tag{9}$$

where $R^{(\text{bn})}$ is the rotation matrix from the n-frame to the b-frame, $\boldsymbol{\omega}_{(\text{ie})}^{(\text{n})}$ (in rad/s) is the angular velocity of the earth frame relative to the inertial frame, and $\boldsymbol{\omega}_{\text{en}}^{(\text{n})}$ is the angular velocity of the n-frame relative to the e-frame.

In low grade applications it is customary to make the simplifying assumption that the n-frame is stationary with respect to the Earth, thus $\boldsymbol{\omega}_{\text{en}}^{(\text{n})} = 0$. Moreover, since $|\boldsymbol{\omega}_{\text{ie}}^{(\text{n})}| \approx 7.29 \cdot 10^{-5}$ rad/s, this contribution can also be assumed negligible. For ease of notation, from (9), we define the time varying vector $\boldsymbol{\omega}(t)$ as

$$\boldsymbol{\omega}(t) \triangleq \boldsymbol{\omega}_{\text{ib}}^{(\text{b})} \approx \boldsymbol{\omega}_{\text{nb}}^{(\text{b})}. \tag{10}$$

4.1.2 Accelerometer Measurements

The accelerometer measures the force acting on the sensor and computes the *specific* force, that is

$$\boldsymbol{a}_{\text{i}}^{(\text{b})}(t) = R^{(\text{bn})}(t)(\boldsymbol{a}_{\text{i}}^{(\text{n})}(t) - \boldsymbol{g}^{(\text{n})}), \tag{11}$$

where $\boldsymbol{g}^{(\text{n})}$ is the gravitational acceleration and $\boldsymbol{a}_{\text{i}}^{(\text{n})}(t)$ is the acceleration of the device relative to the i-frame. For navigation purposes we are interested in $\boldsymbol{a}_{\text{n}}^{(\text{n})}$, the acceleration of the device relative to the n-frame. The relationship between $\boldsymbol{a}_{\text{n}}^{(\text{n})}$ and $\boldsymbol{a}_{\text{i}}^{(\text{n})}$ is [28]

$$\boldsymbol{a}_{\text{i}}^{(\text{n})}(t) = \boldsymbol{a}_{\text{n}}^{(\text{n})}(t) + 2\boldsymbol{\omega}_{\text{ei}}^{(\text{n})} \times \boldsymbol{v}(t) + \boldsymbol{\omega}_{\text{ei}}^{(\text{n})} \times \boldsymbol{\omega}_{\text{ei}}^{(\text{n})} \times \boldsymbol{p}(t), \tag{12}$$

where $\boldsymbol{p}$ and $\boldsymbol{v}$ are the position and velocity of the device relative to the navigation frame.

In (12) the angular velocity of the Earth is assumed constant and the navigation frame is fixed to the Earth frame, which is reasonable when the travelled distance is negligible with respect to the Earth radius. This formulation is derived by using the relation between rotating coordinate frames. The last term of the sum represents the centrifugal acceleration, while the second is the Coriolis acceleration. The former is typically absorbed in the gravity vector and has a magnitude of around $3.39 \cdot$

$10^{-2}\mathrm{m}/s^2$ while the latter depends on the velocity of the object on which the IMU is mounted, and has a magnitude in the order of 10^{-3} for a speed of 120 km/h.

In order to simplify the model we assume these two terms to be negligible and we define the time varying vector

$$\boldsymbol{a}(t) \triangleq \boldsymbol{a}_{\mathrm{n}}^{(\mathrm{n})}(t) \approx \boldsymbol{a}_{\mathrm{i}}^{(\mathrm{n})}(t). \tag{13}$$

The physical relationships between $\boldsymbol{a}$, $\boldsymbol{p}$, and $\boldsymbol{v}$ are

$$\boldsymbol{v}(t) = \frac{\partial \boldsymbol{p}(t)}{\partial t}, \quad \boldsymbol{a}(t) = \frac{\partial \boldsymbol{v}(t)}{\partial t}. \tag{14}$$

4.1.3 Representation of Orientation

The acceleration $a(t)$ is not directly measured by the IMU. Indeed, the measured acceleration $a_b(t)$ is expressed with respect to the body frame rather than the navigation frame. In order to express $a(t)$ as a function of $a_b(t)$, a rotation of the former has to be performed and the entity and direction of this rotation is given by the orientation of the navigation frame with respect to the body frame.

Orientation can be parametrized in different ways. We consider unit quaternions, one of the most widely used orientation parametrization in estimation problems [28]. Unit quaternions are a 4-dimensional representation of orientation:

$$\mathbf{q} = (q_0, q_1, q_2, q_3)^T = \begin{pmatrix} q_0 \\ \mathbf{q_v} \end{pmatrix}, \ \mathbf{q_v} \in \mathbb{R}^3, \ ||\mathbf{q}||_2 = 1. \tag{15}$$

A rotation of a vector in $\mathbb{R}^3$ is a change of its direction while its length remains constant. The rotation of $\mathbf{x_a}$ into $\mathbf{x_b}$ can be expressed with unit quaternions as:

$$\mathbf{x_b} = \mathbf{q^{ba}} \odot \mathbf{x_a} \odot (\mathbf{q^{ba}})^c, \tag{16}$$

where the $\odot$ represents quaternion multiplication, that can be expressed in matrix form (see [28] for the derivation).

Rotations in $\mathbb{R}^3$ form the special orthogonal group, $SO(3)$, that is a matrix *Lie group*. As reported in [28], this allows to represent an orientation deviation with an exponential map over rotation vectors. An orientation with respect to the navigation frame, $\mathbf{q_t^{nb}}$ is thus represented in terms of a linearization point ($\tilde{\mathbf{q}}_\mathbf{t}^{\mathbf{nb}}$) and an orientation deviation parametrized by a rotation vector, $\boldsymbol{\eta_t}$, expressed in the body frame as

$$\mathbf{q_t^{nb}} = \exp\left(\frac{\bar{\boldsymbol{\eta}}_t}{2}\right) \odot \tilde{\mathbf{q}}_\mathbf{t}^{\mathbf{nb}}, \tag{17}$$

where $\bar{\boldsymbol{\eta}}_t = (0, \boldsymbol{\eta}_t{}^T)^T$, and $\boldsymbol{\eta_t} = \mathbf{n}\boldsymbol{\alpha}$ is a rotation vector, parametrized by a unit vector, $\mathbf{n}$ and rotation Euler angles $\boldsymbol{\alpha}$. The exponential operation is defined as

$$\exp(\bar{\eta}) = \cos||\eta||_2 + \frac{\bar{\eta}}{||\bar{\eta}||}\sin||\eta||_2. \tag{18}$$

In our case we are interested in expressing the orientation in time as a function of the angular velocity and the initial orientation. Therefore, (17) will be used, where the reference orientation $\tilde{\mathbf{q}}_{\mathbf{t}}^{\mathbf{nb}}$ is the initial orientation at time t_0, and the rotation vector is represented by the angle displacement, i.e., the time integral of the angular speed

$$\mathbf{q}^{\mathbf{nb}}(t) = \exp\left(\frac{\bar{\eta}(t)}{2}\right) \odot \tilde{\mathbf{q}}^{\mathbf{nb}}(t_0), \tag{19}$$

with

$$\eta(t) = \int_{t_0}^{t} \boldsymbol{\omega}(t)dt. \tag{20}$$

The acceleration in the navigation frame can thus be expressed in the following way with respect to the acceleration in the body frame and the relative orientation of the two coordinate frames

$$\mathbf{a}^{\mathbf{n}}(t) = \mathbf{q}^{\mathbf{nb}}(t) \odot \mathbf{a}^{\mathbf{b}}(t) \odot (\mathbf{q}^{\mathbf{nb}}(t))^{c}. \tag{21}$$

4.2 Measurement Error Models

Data from gyroscopes and accelerometers are corrupted by measurement noise. By collecting data from a stationary IMU standing on a flat surface the gyroscope is expected to measure only the earth rotation, while the accelerometers should measure the resulting acceleration that accounts for gravity and the centrifugal force. Over some tens of seconds the data seem to fit well a Gaussian distribution with non-zero mean.

4.2.1 Gyroscope

In general the noise can be divided into two distinct contributions: a slowly time varying bias $\boldsymbol{\delta}_{\omega,t}$ and a white noise component $\boldsymbol{e}_{\omega,t} \sim \mathcal{N}(0, \Sigma_\omega)$, with Σ_ω a 3×3 diagonal matrix. The subscript t denotes discrete time samples. Therefore, the measures can be written as

$$\boldsymbol{y}_{\omega,t} = \boldsymbol{\omega}(nT_\omega) + \delta_{\omega,t} + e_{\omega,t}, \tag{22}$$

where T_ω is the sampling period of the gyroscope.

There are two main approaches to model the bias, which is considered either constant or slowly time-varying in the time interval of the measurements. In the latter case, the bias is modeled as a random walk

$$\boldsymbol{\delta}_{\omega,t+1} = \alpha \boldsymbol{\delta}_{\omega,t} + \boldsymbol{e}_{\delta_{\omega,t},t}, \tag{23}$$

with $\alpha \in (0, 1)$, $\boldsymbol{e}_{\delta_{\omega,t},t} \sim \mathcal{N}\left(0, \Sigma_{\delta_{\omega,t}}\right)$ and $\Sigma_{\delta_{\omega,t}}$ 3×3 diagonal.

This model fits well the experimental data and can be verified by the means of the Allan variance.

4.2.2 Accelerometer

For the accelerometer the same observations of the gyroscope hold, and the noise has two contributions: a bias that is slowly time varying and a white noise. The measurement model for the accelerometer is:

$$\boldsymbol{y}_{a,t} = \boldsymbol{a}_{\mathrm{i}}^{(\mathrm{b})}(t) + \boldsymbol{\delta}_{a,t} + \boldsymbol{e}_{a,t}, \tag{24}$$

where T_a is the sampling period of the accelerometer, and $\boldsymbol{e}_{a,t} \sim \mathcal{N}\left(0, \Sigma_{\delta_{a,t}}\right)$, with again $\Sigma_{\delta_{a,t}}$ a 3×3 diagonal matrix.

4.2.3 GNSS Module

The lower level output of the GNSS module are the pseudorange measurements $\rho_t^{(s)}$ and carrier phase measurements $\phi_t^{(s)}$, where the superscript s denotes the number of satellites in view. From the raw measurements and the ephemeris data we can compute PVT.

GNSS measurements are corrupted by additive noise, i.e.,

$$\boldsymbol{y}_{p,t} = \boldsymbol{p}(nT_p) + \boldsymbol{e}_{p,t}, \tag{25}$$

where T_p is the sampling period of the GNSS module. A reasonable model for the additive error process is a Gauss-Markov process defined as follows

$$\boldsymbol{e}_{p,t+1} = \exp(-\beta T_p)\boldsymbol{e}_{p,t} + \nu_t, \tag{26}$$

where β is a parameter describing the correlation between successive samples, $\nu_t \sim \mathcal{N}\left(0, \Sigma_p\right)$. Parameters β, T_p, and Σ_p are tabulated in [29, 30].

4.3 Extended Kalman Filter

The KF is an efficient approach to evaluate the state of a complex system, governed by known laws and described by noisy measurements. In our problem, the system under exam is a moving object and the laws that describe its state (position, velocity, and time) are the physics laws of motion. The available measurements can be used for state evaluation according to a known measurement model (described in Sect. 4.2). The KF approach is based on the assumption that the noise corrupting both the measurements and the state estimate is Gaussian and that the equations describing the evolution of both the state and the measurements are linear. As the motion of an accelerating object cannot be represented by linear equations (since the object position is part of the state variables), it is customary to adopt the extended Kalman filter (EKF) instead. The EKF exploits a linearization of the non-linear equations that describe the state and measurement evolution through the Jacobian of non-linear functions. While the KF provides an optimal estimate, the EKF uses approximation and therefore it is not optimal. The EKF can be used to estimate the PVT of a moving object through the iterative repetition of two steps:

time update: the motion model is used to "predict" the state of the next time step;
measurement update: the predicted state estimate is updated according to the current measurement and the measurement model.

One of the most common implementations of EKF integrating GNSS and IMU uses the measurements from the former in the measurement update step, while the measurements from the latter are used in the time update step to predict the next state value. A complete derivation of the EKF equations and matrices can be found in [28].

4.4 Innovation Testing

Innovation testing is a spoofing detection approach that exploits the EKF designed for sensor fusion and navigation. Typically, such EKF have position, velocity, and orientation as state, and IMU and GNSS as measurements.

The innovation step (which is part of the measurement update step), in any linear KF (a similar expression holds for EKF), is

$$\boldsymbol{i}_k = \boldsymbol{z}_k - H\hat{\boldsymbol{x}}_{k|k-1}, \tag{27}$$

where $\hat{\boldsymbol{x}}_{k|k-1}$ is a prediction of the current state. The covariance matrix of $\boldsymbol{i}$ is known [31] and denoted by P_k. Then, by normalizing $\boldsymbol{i}_k$ by its covariance matrix, we obtain the test statistic

$$\beta_k = \boldsymbol{i}_k^t P_k \boldsymbol{i}_k, \tag{28}$$

which can be shown to be Chi-squared distributed with as many degree of freedom as the dimension of the measurement vector $\boldsymbol{z}$ [31].

Innovation testing for anti-spoofing leverages the fact that under spoofing, the state prediction derived from the IMU measurements are likely to disagree with the GNSS measurements (arbitrarily forged by the attacker). Therefore under attack $\boldsymbol{x}_{k|\hat{k}-1}$ is no longer a good prediction of the state, causing the absolute value of the innovation to increase. Then, under spoofing β_k is no longer Chi-squared distributed and the spoofing detection is performed, in the framework of binary hypothesis testing (see also (2)), according to

$$\hat{\mathcal{H}} = \begin{cases} \mathcal{H}_0 & \beta_k \sim \chi^2 \\ \mathcal{H}_1 & \beta_k \not\sim \chi^2. \end{cases} \tag{29}$$

Innovation testing is common in the literature, especially in aviation scenarios [4, 9].

In order to evaluate the results of innovation testing on a simple, analytic scenario, let us simulate a spoofing attack by designing a legitimate trajectory (LT), i.e., the trajectory that the user physically follows, and a spoofing trajectory (ST), i.e., the trajectory that the spoofer induces to the user. The corresponding IMU and GNSS measurements have been generated according to the measurement model described in Sect. 4.2. Let us recall that under $\mathcal{H}_0$ both GNSS and IMU follow the LT, while under $\mathcal{H}_1$ the GNSS module follows the ST.

The ST initially matches the LT, but then diverges by an angle θ. This is done by fixing 3 waypoints for the ST, $\boldsymbol{w}_1$, $\boldsymbol{w}_2$, and $\boldsymbol{w}_3$, such that

$$\boldsymbol{w}_1 = [0, 0, 0]^t, \tag{30}$$

$$\boldsymbol{w}_2 = [10, 3, 0]^t, \tag{31}$$

$$\boldsymbol{w}_3 = \boldsymbol{w}_2 + R_\theta \boldsymbol{w}_2, \tag{32}$$

where R_θ is a rotation matrix that rotates any vector by an angle θ in the (x, y) plane. We then create a temporal axis by fixing a time of arrival at each waypoint and specifying a trajectory sampling time. A cubic interpolation generates the intermediate points between waypoints using the time axis as interpolation query. Velocity and acceleration profiles are computed by numerical derivation of position vector.

Using the same time axis, we specify also an orientation profile, i.e., a quaternion for each time instant describing the orientation of the body frame with respect to the navigation frame. From the orientation profile we compute the angular velocity in the body frame at each time instant, such that

$$\omega_t^{\mathrm{b}} = \left(\boldsymbol{q}_t^{(\mathrm{nb})}\right)^{\mathrm{c}} \odot \boldsymbol{q}_{t+1}^{(\mathrm{nb})}. \tag{33}$$

From angular velocity, acceleration and position profiles we can generate GNSS and IMU measurements.

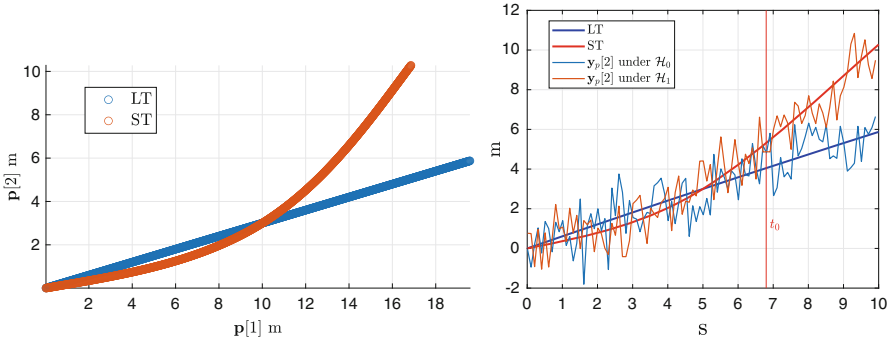


Fig. 10 Simulation scenario. (**a**) Scatter plot of $\boldsymbol{p}[1]$ and $\boldsymbol{p}[2]$ of the spoofed and authentic trajectory. $\theta = \pi/6$. (**b**) $\boldsymbol{p}[2]$ of the spoofed and authentic trajectory, versus time. Thinner lines are the corresponding measurements

Figure 10 shows the LT and the ST. Figure 10b shows a 2D scatter plot of $\boldsymbol{p}$, where divergence between LT and ST starts at point $(10, 3)$ and $\theta = \pi/6$. Before diverging, the two trajectories are not exactly the same because of the cubic interpolation that avoids singularities in later numerical derivations. Figure 10b shows the same trajectories (only the second component of each 3D position vector) as function of time together with the corresponding GNSS measurements, where the velocity absolute value is constant.

4.4.1 Analytical Results

We expect that the test statistic β(coinciding with the normalized innovation) is Chi-squared distributed with 3 degrees of freedom under $\mathcal{H}_0$, since the measurement vector of the EKF is 3-dimensional. Hence we have

$$\beta \sim \chi^2_3, \quad p(\beta|\mathcal{H}_0) = \frac{1}{2^{3/2}\Gamma(3/2)}\beta^{3/2-1}e^{-\beta/2}, \tag{34}$$

where $\Gamma(\cdot)$ is the well-known gamma function. Figure 11a shows $\hat{p}(\beta_k|\mathcal{H}_0)$ together with $p(\beta|\mathcal{H}_0)$ and we can see how the two distributions match, as expected. Then we apply the EKF on the ST and Fig. 11b shows how in this case the innovation test is not chi-squared distributed and hence spoofing detection can be performed.

The measurement frequency was set to 100 Hz for the IMU and 10 Hz for GNSS. A window of 1 s worth of innovation values was used for detection purposes, with varying the test instant t_0 and the trajectory angle θ. The DET curves were derived through Monte Carlo simulations, by collecting the statistics of the normalized innovation at different time instants, both in the authentic and spoofing case. The

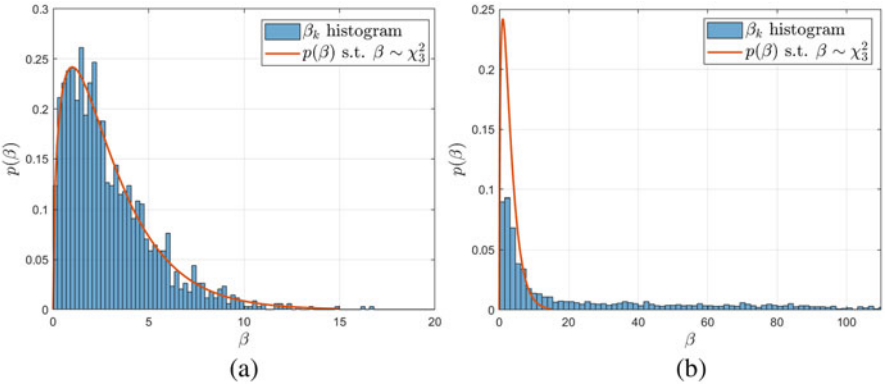


Fig. 11 Histogram plots of β_k under a LT and ST, i.e., under $\mathcal{H}_0$ and $\mathcal{H}_1$. (**a**) Histogram plot of $\beta_k|\mathcal{H}_0$. (**b**) Histogram plot of $\beta_k|\mathcal{H}_1$

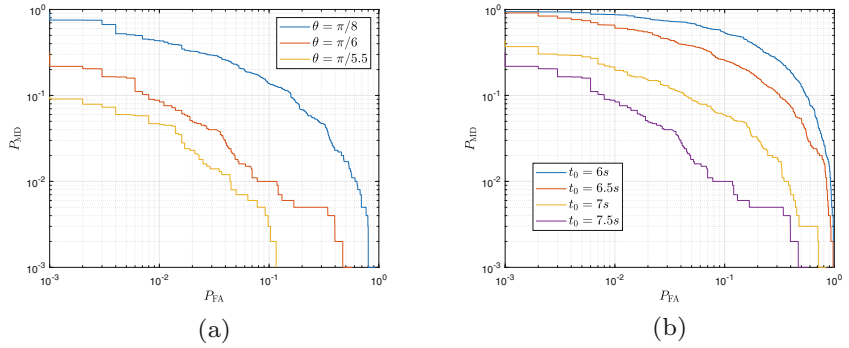


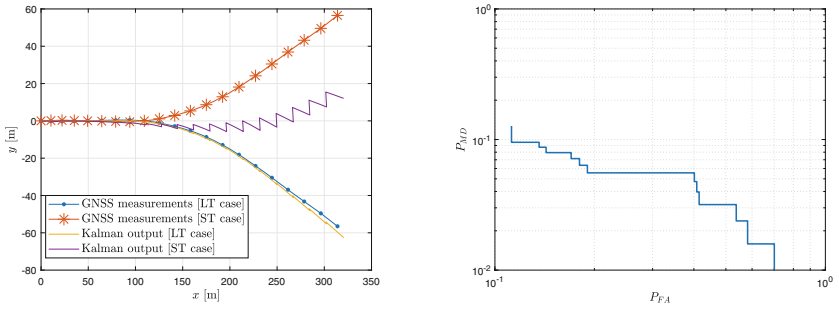
Fig. 12 DET curves for spoofing detection with the EKF. (**a**) DET curves for different θ ($t_0 = 7.5$s). (**b**) DET curves for different t_0 ($\theta = \pi/6$)

results are reported in Fig. 12. It is noticeable that, as expected, the more the two trajectories diverge, the more effective is the spoofing detection.

4.4.2 Testing on Real World Data

In the following some results are presented from the processing of measurements gathered from a Novatel sensor [32].

Figure 13a shows part of the LT and ST used for this experiment. The LT is taken directly from the available GNSS measurements, while the ST was obtained from the LT, such that the two trajectories diverge symmetrically. In both scenarios the IMU measurements are the same.



(a) (b)

Fig. 13 Experimental scenario and innovation testing performance. (**a**) LT and ST example with data from [32]. In both cases it is shown the position as estimated by the KF. (**b**) DET resulting from the application of innovation testing the scenario of Fig. 13a

The spoofing detection experiment was performed by feeding the EKF with the two trajectories and the IMU measurements. Figure 13a shows the position estimates of the EKF in both cases, making it possible to see the effect of measurement inconsistencies in the spoofing case. Figure 13b shows, instead, the DET resulting from innovation testing. False alarm and misdetection probabilities are estimated from 10 different portions of trajectory that are similar to the LT in Fig. 13a, for a total of 4×10^4 IMU samples and 210 GNSS samples.

4.4.3 Testing on a Software Receiver

In the following we evaluate the performance of innovation testing by exploiting the GNSS software receiver built by the University of Padova. The innovation testing module has as input the position computed by the PVT module and generates acceleration and gyroscope noisy measurements, according to the model in Sect. 4.2. The GNSS signal that is fed as input to the software receiver is generated with the c++ signal generator built by the University of Padova.

For both the nominal and the spoofing scenarios, 150 s worth of GNSS signal were generated. This time in the nominal scenario the receiver is stationary, therefore the IMU records only Gaussian noise. In the spoofing scenario the attacker is assumed to fake a stationary position, while the receiver is actually moving with constant acceleration. Indeed, the GNSS module computes a stationary position in the spoofing scenario, while the IMU measures a constant acceleration of 3 m/s^2 in magnitude.

Performance in terms of DET is shown in Fig. 14. The results are in the same order of magnitude of those in Fig. 13b.

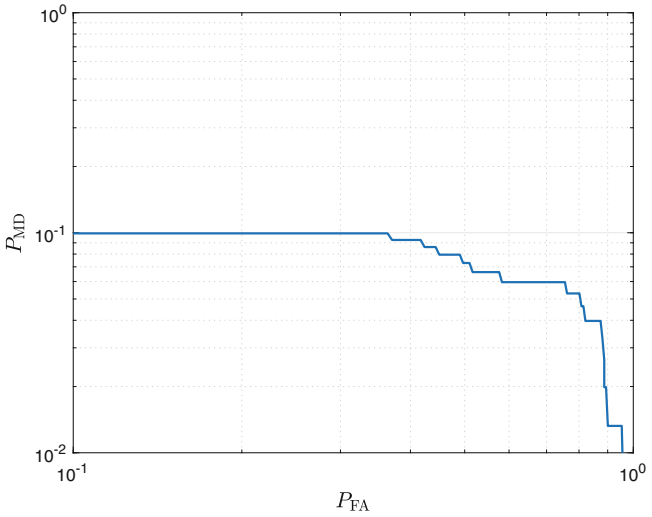


Fig. 14 DET resulting from innovation spoofing applied to the scenario described in Sect. 4.4.3

5 Conclusions

We have proposed various spoofing detection techniques to be applied on smartphones, using context information coming from other components, such as the cellular network or the IMU, or through consistency-checks of the received signals. All these techniques have been tested in APPs developed in Android and effects of the detection parameters have been studied in order to achieve a desired trade-off between false-alarm and misdetection probabilities. We have also shown the effectiveness of these defence strategies against various attacks previously reported in the literature.

Acknowledgments The authors gratefully acknowledge the contributions of Amedeo Pachera and Giovanni Carollo for developing the apps, and Marco Ceccato for his support with some simulations.

References

1. Ceccato, S., Formaggio, F., Caparra, G., Laurenti, N., Tomasin, S.: Exploiting side-information for resilient GNSS positioning in mobile phones. In: Proc. 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), pp. 1515–1524 (Jun 2018)
2. Formaggio, F., Ceccato, S., Basana, F., Laurenti, N., Tomasin, S.: GNSS spoofing detection techniques by cellular network cross-check in smartphones. In: Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019), pp. 3904–3916, Miami, Florida (September 2019)

3. Qiao, Y., Zhang, Y., Du, X.: A vision-based gps-spoofing detection method for small uavs. In: 2017 13th International Conference on Computational Intelligence and Security (CIS), pp. 312–316 (Dec 2017)
4. Kerns, A.J., Shepard, D.P., Bhatti, J.A., Humphreys, T.E.: Unmanned aircraft capture and control via gps spoofing. J. Field Rob. **31**, 617–636 (2014)
5. Kwon, C., Liu, W., Hwang, I.: Analysis and design of stealthy cyber attacks on unmanned aerial systems. J. Aerosp. Inf. Syst. **11**, 525–539 (2014)
6. Curran, J.T., Broumendan, A.: On the use of low-cost IMUs for GNSS spoofing detection in vehicular applications. In: International Technical Symposium on Navigation and Timing (ITSNT) 2017, Toulouse, France (2017)
7. Broumandan, A.. Lachapelle, G.: Spoofing detection using gnss/ins/odometer coupling for vehicular navigation. Sensors (Apr 2018)
8. Tanil, C., Khanafseh, S., Pervan, B.: Impact of wind gusts on detectability of GPS spoofing attacks using RAIM with INS coupling. In: Proc. ION Conference, pp. 674–686 (April 2015)
9. Tanil, C., Khanafseh, S., Pervan, B.: An INS monitor against GNSS spoofing attacks during GBAS and SBAS-assisted aircraft landing approaches. In: Proc. 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2016), pp. 2981–2990, Portland, Oregon (Sept. 2016)
10. Lo, S., Chen, Y.H., Reid, T., Perkins, A., Walter, T., Enge, P.: Keynote: The benefits of low cost accelerometers for gnss anti-spoofing. In: ION 2017 Pacific PNT Meeting (2016)
11. Zeng (Curtis), K., Liu, S., Shu, Y., Wang, D., Li, H., Dou, Y., Wang, G., Yang, Y.: All your GPS are belong to us: Towards stealthy manipulation of road navigation systems. In: 27th USENIX Security Symposium (USENIX Security 18), pp. 1527–1544. USENIX Association, Baltimore, MD (2018)
12. Fernández-Hernández, I., Rijmen, V., Seco-Granados, G., Simon, J., Rodríguez, I., David Calle, J.: A navigation message authentication proposal for the galileo open service. Navig. J. Inst. Navig. **63**(1), 85–102 (2016)
13. Caparra, G., Sturaro, S., Laurenti, N., Wullems, C., Ioannides, R.T.: A novel navigation message authentication scheme for gnss open service. In: Proc. ION GNSS, pp. 2938–2947 (2016)
14. Caparra, G., Curran, J.T.: On the achievable equivalent security of GNSS ranging code encryption. In: Proc. 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), pp. 956–966. IEEE (2018)
15. Jahromi, A.J., Broumandan, A., Daneshmand, S., Lachapelle, G., Ioannides, R.T.: Galileo signal authenticity verification using signal quality monitoring methods. In: Proc. 2016 International Conference on Localization and GNSS (ICL-GNSS), pp. 1–8. IEEE (2016)
16. Pagot, J.-B., Thevenon, P., Julien, O., Amarillo-Fernandez, F., Maillard, D.: Signal quality monitoring for new gnss signals. In: Proc. ION GNSS 2016, 29th International Technical Meeting of the Satellite Division of the Institute of Navigation, pp. pp–1750 (2016)
17. Formaggio, F., Tomasin, S., Caparra, G., Ceccato, S., Laurenti, N.: Authentication of galileo GNSS signal by superimposed signature with artificial noise. In: Proc. 2018 26th European Signal Processing Conference (EUSIPCO), pp. 2573–2577. IEEE (2018)
18. Formaggio, F., Tomasin, S.: Authentication of satellite navigation signals by wiretap coding and artificial noise. EURASIP J. Wirel. Commun. Netw. **2019**(1), 98 (2019)
19. ftp://cddis.gsfc.nasa.gov/. Last accessed: 9/12/2019
20. https://www.gps.gov/technical/icwg/. Last accessed: 9/12/2019
21. Opencellid: https://www.opencellid.org
22. Mozilla Location Service: https://location.services.mozilla.com/
23. cellmapper: https://www.cellmapper.net
24. GSA: Using GNSS raw measurements on android devices, Jan 2018
25. Falco, G., Pini, M., Marucco, G.: Loose and tight gnss/ins integrations: Comparison of performance assessed in real urban scenario. Sensors (Jan 2017)
26. Gikas, V., Perakis, H.: Rigorous performance evaluation of smartphone GNSS/IMU sensors for ITS applications. Sensors (Aug 2016)

27. Starlino: A guide To using IMU (accelerometer and gyroscope devices) in embedded applications. https://www.starlino.com/imu_guide.html, [Posted: 29 December 2009]
28. Kok, M., Hol, J.D., Schön, T.B.: Using inertial sensors for position and orientation estimation. Foundations and Trends in Signal Processing, vol. 11, pp. 1–153 (2017). https://doi.org/10.1561/2000000094
29. Niu, X., Chen, Q., Zhang, Q., Zhang, H., Niu, J., Chen, K., Shi, C., Liu, J.: Using Allan variance to analyze the error characteristics of GNSS positioning. GPS Solutions **18**(2), 231–242 (2014)
30. Rankin, J.: GPS and differential gps: an error model for sensor simulation. In: Position Location and Navigation Symposium, pp. 260–260 (1994)
31. Liu, Y., Li, S., Fu, Q., Liu, Z.: Impact assessment of gnss spoofing attacks on ins/gnss integrated navigation system. Sensors (2018)
32. Novatel: Product home page. Available at https://docs.novatel.com/OEM7/Content/Home.htm

Using a Crowd-Sensing Strategy to Support Public Transport Tracking

Fábio Rodrigues de la Rocha and Michelle Wangham

1 Introduction

Urban mobility is currently a major issue due to problems such as traffic congestion, parking availability and commuting times. As the cities' infrastructures no longer support the increasing number of vehicles [4] and improvements require major investments, the future outlook is not encouraging. The importance of studying urban mobility becomes clear when we realize that half of humanity lives in cities today. According to the United Nations, this number will reach 60% by 2030 [17].[1] However, in many countries the scenario is even worse. In Brazil, this number will reach 89.9% and in Japan 93.3% by 2030. Due to its importance, urban mobility is in the list of 17 Sustainable Development Goals (SDGs) to be implemented by all countries up to 2030.

An alternative to mitigate this problem is an efficient public transport system. This system also offers a reduction in air pollution [10] as well as number and severity of car accidents [16]. A key to an efficient public transport system is an online tracking system. Commercial systems usually implement online tracking system through a dedicated embedded system composed of a small computer with

[1] https://www.worldometers.info/world-population.

F. R. de la Rocha (✉)
Federal University of Santa Catarina, Araranguá, SC, Brazil

M. Wangham
University of Vale do Itajaí, Florianópolis, SC, Brazil
e-mail: wangham@univali.br

S. Paiva (ed.), *Precision Positioning with Commercial Smartphones in Urban Environments*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-71288-4_2

a proprietary software, a Global Positioning System (GPS) to capture its location, and a mobile data communication radio (such as GPRS/GSM, CDMA, 3G, 4G, 5G, etc.) to send data.

Online tracking systems for public transport have some technical issues to be investigated and improved. These systems, called Automatic Vehicle Location (AVL) [9], provide real-time data that enables the improvement of public transport systems reliability. Data from AVL also allows the development of mobile applications, by which customers have access to routes, bus stops, times, etc. However, there are financial and technical issues that make online tracking systems difficult to develop. The financial issue is mainly for small businesses because of the high cost of deploying servers, network infrastructure, and dedicated hardware to equip the bus fleets. Technical issues reach both small and large companies and are related to GPS-based online tracking and mobile data communication. The state of the art of vehicle tracking systems and some technical issues are presented in [15]. Among them, there is the well-known "urban canyon problem", where the GPS is unable to find a location due to tall buildings that block the line of sight of satellites [23]. Other issues are associated with non-functional mobile data communication caused by network infrastructures (dead zones, overcrowded radio channels, topography, etc.) [18].Whenever a problem occurs, the bus current location is unknown for both the company and customers (which only see the last updated location and may assume the bus is broken). Besides, all predictions based on current bus location are affected and subject to error or inaccuracy [7, 20]. As a result, the system loses quality and passenger interest.

The aim of this paper is to improve the availability of online tracking systems for public transport. We do this by a solution that uses a crowd-sensing strategy along with smartphones [13] and low cost hardware to provide a real or approximate bus location. In a crowd-sensing strategy, customers use their mobile devices sensors (Bluetooth, accelerometer, compass, GPS) to capture data of interest and submit it to a server where it is processed to extract information [1, 11, 14]. A Crowd-sensing strategy is useful for online tracking applications as it presents financial advantages for the transportation company that does not have to deal with the sensors nor the communication infrastructure between the sensors and a cloud server. However, as it relies on customers to help locate buses, it also opens a security breach where malicious users can corrupt the system (man-in-the-middle or impersonating attacks). Therefore, this paper (1) analyzes and solves the security aspect on the exchanging messages between peers; (2) presents a Bluetooth Low Energy (BLE) data dissemination protocol to transfer data between a bus and multiple mobile applications without relying on connection nor pairing; (3) validates a solution through a prototype integrated with a commercial vehicular scanner; (4) presents evaluations on functionality and performance.

The paper is organized as follows. Section 2 analyzes some related works and compares them with the proposed solution. The proposed solution and the developed prototype are described in Sects. 3 and 4. The prototype evaluation is discussed in Sect. 5. Finally, Sect. 6 presents the concluding remarks as well as future work suggestions.

2 Related Work

In [22], the authors present a crowd-sensing system for bus tracking which is maintained by customers with no direct support from the transport company. Customers use a mobile application which detects when they are inside a bus (using traces from the GPS and the accelerometer) and sends its location to a server. There might be a misdetection if the user is inside or nearby a bus. There is no citation on how multi-user locations are managed and whether there is any authentication mechanism to avoid fake locations from malicious users. In [25] users use a mobile application that detects the mobile network provider in the area and uses this information to determine the location instead of a GPS. By keeping the GPS turned off, the battery consumption is significantly reduced. The application automatically detects when the user is inside the bus using the audio signature of the bus ticket machine. Therefore, the solution cannot be applied to other types of buses. Data is submitted to a server using the user's mobile data connection. As in [22], there is no citation on how multi-user locations are managed and whether there is any authentication mechanism. Again, there is no support from the transport company.

Reference [8] shows a system based on mobile applications where users evaluate the bus conditions (full/empty, ripped seats, non-functional lights, etc.) and also automatically send their current location to a server using their data connection. As in the last two related works, there is no citation on how multi-user locations are managed and whether there is any authentication mechanism.

Other related work [6] presents a wireless sensor network in a bus. There are different sensors (location, tire pressure, etc.). All sensors send data to the bus driver's smartphone which works as a gateway collecting and sending data to a server. The bus tracking system is subject to failures if the driver's smartphone is unable to send data. In [19], a low cost embedded system inside a bus is used to send a location to a server. Data is available to customers using a web application or SMS messages. There is no participation of customers and thus location failures can happen if the embedded system is unable to locate the bus or to send data.

In [12], a simple tracking system for poor cities in underdeveloped countries that are unable to afford the costs of a GPS in each bus is described. In the proposed system, bus stops are intelligent, consisting of a cheap microcontroller, an RFID reader module, and a mobile data communication module. Buses, on the other hand, have an affordable passive RFID tag that is detected when they pass the bus stop, where the information is submitted to a server using the mobile data communication. In this system, the bus current position is only known at bus stops and needs to be interpolated through algorithms to other points along the way. Malicious users can clone RFID tags to corrupt the location system. In [20], an embedded system inside a bus is used to capture the location and computes the arrival time at each bus stop along the way. The results are posted in a web server. There is no customer participation and so failures can occur if the embedded system is unable to send data.

In a previous work [5], a crowd-sensing system is used by customers to assist with the bus location (whenever the bus is unable to send its own location). Customer's mobile apps need to perform IEEE 802.11 (WiFi) connections on each bus to capture their data, therefore disturbing data communications. The embedded system also uses an On-Board Diagnostic (ODB) scanner module (connected by wires) to extract the vehicle telemetry. As seen in previous works, there is no citation on how multi-user locations are managed and whether there is any authentication mechanism. Besides, failures can happen if the bus cannot obtain its GPS location.

This section presented articles with location unavailability issues where the bus location depends on a single entity (embedded system/bus driver) or multiple entities (crowd-sensing customers). The latter offers advantages in case of failure, since other entities can provide a location. However, there are security issues (attacks by malicious users) and challenges to merge collaborative locations.

Our solution uses a crowd-sensing system to deal with the location unavailability issue. In the ideal scenario, the driver's mobile application submits the bus location to the cloud server. In case of failure, the nearby collaborative customers detect messages from the buses and propagate them to the cloud server.

3 Proposed Solution

The solution described in this paper is based on the use of smartphones for both the bus driver and customers (passengers). Because of this, it is not necessary to design and implement a complex dedicated embedded device that would result in higher costs for the public transport company. All necessary components to develop an online tracking system are available in a smartphone such as the GPS unit, the mobile communication module, BLE, WiFi, and others. The use of smartphones allows customers to automatically assist with locating buses at no cost to the bus company. Another advantage of using smartphones, is that software development is centered on mobile applications. This enables a great flexibility of programming languages, component libraries, and frameworks. Whenever an updated mobile app version is available, the update process takes place easily. In addition to smartphones, the only hardware element is Bus Broadcasting Device (BBD), a simple and inexpensive embedded system on the bus that broadcasts information.

The advantage of crowd-sensing strategy for the transport company is that it encourages users to participate. The user can track the buses locations and make smart decisions about his trips. Furthermore, transport companies can provide a rewarding mechanism where users receive financial compensation or discounts on trips if they are willing to collaborate with the system [24]. On the other hand, users need to install a mobile application which uses storage space on the smartphone. Also, when running the application it consumes the user's data plan and increases the battery usage. This paper does not address the business model related to the buses' online tracking system.

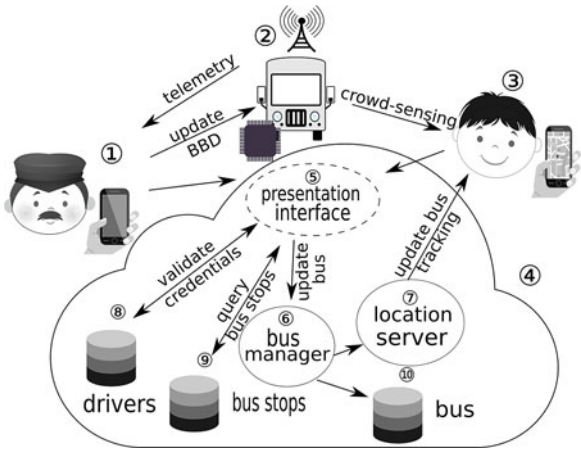


Fig. 1 Proposed solution overview

3.1 Overview

Figure 1 presents an overview of the proposed system architecture with its four entities: ① the driver, ② the BBD, ③ the customer, and ④ the cloud application server.

3.2 Bus Driver

The bus driver uses the Bus Driver Mobile Application (BDMA) that automatically feeds the cloud application server with the bus information. As a safety procedure, the BDMA runs without interaction from the bus driver. The app performed actions are: validation of the bus driver credentials; capture of the bus telemetry using a bluetooth ODB scanner; localization of the bus using the smarphone's GPS; update of the cloud application server with location and telemetry data; and update of the BBD with the current location.

3.3 Bus Broadcasting Devices

BBD is a low cost device capable of receiving information from the BDMA. It propagates these information to all nearby customers. The exchanged information between the BBD and the mobile apps use BLE instead of the mobile data network.

Each BBD is assigned to a bus and broadcasts a beacon composed of (1) an unique mac-address, (2) the bus name, (3) its current location, and a (4) status flag. The status flag represents the result of the last attempt performed by the BDMA to update

the cloud application server (success/failure) as well as the working status of its GPS (operational/non-operational). After receiving the beacon, the customers know if the bus is unable to update the bus location on the cloud application server. In this case, the nearby customers can provide assistance submitting its location to the cloud application server.

3.4 Customers

Customers use the Customers Mobile Application (CMA) with two distinct functions. The first captures and presents all buses on a map in real-time. The second function is to act proactively using the crowd-sensing strategy to assist in locating the buses. In both cases, all communications use the customer's mobile data plan.

The CMA can automatically detect and submit nearby bus locations to the cloud application server. In a multi-customer scenario, a vast sensing area is created. This helps tracking buses when they are unable to locate themselves. Figure 2 presents a fragment of an area of a city with buses and customers. Some of these customers are within the scope of the beacon signal (hatched areas) and are able to obtain information from one or more buses (a customer can even be inside a bus). These customers may assist in locating these buses. BDMA is the main app responsible for informing the location of the bus. Whenever the BDMA is unable to update the cloud server (problems with GPRS/GSM or the inability to obtain the location of GPS), the client application, using its own data connection, will send the location. Mobile application customers have different mobile operators, which in turn have different coverages according to the location. Therefore, some customers may experience internet access problems, while others can still assist locating the buses.

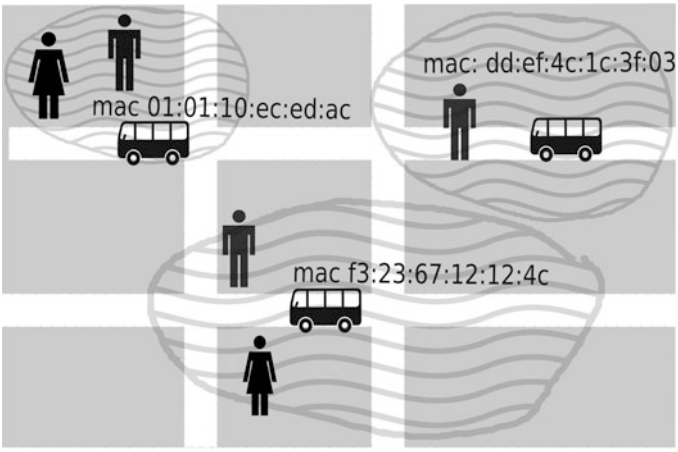


Fig. 2 Nearby customers capturing the beacon from buses

3.5 Cloud-Based Application Server

The cloud application server shown in Fig. 1 is maintained by the transport company and is responsible for receiving and handling requests from both apps (① BDMA and ③ CMA). The BDMA accesses the cloud application server ⑤ to validate the driver's credentials using ⑧ the driver's database, and it also gets the ⑨ bus stop list. Whenever a bus update is required (such as location or telemetry info), the ⑥ bus manager component performs this task by accessing the ⑩ bus database. The CMA submits a nearby bus location to the cloud application server and captures the bus stop list from the same server. The bus manager ⑥ is the internal software component that receives the updates. Each time a new location is received and processed, the component triggers the ⑦ location server to update all currently connected CMA.

3.6 Message Exchanges and Security Issues

As the tracking system relies on collaborative users to deliver messages, it is necessary to prevent malicious customers from corrupting the system. There are four possible scenarios for exchanging messages. In scenario 1, shown in Fig. 3, the bus (BDMA) is capable of obtaining its GPS location and sending data over the mobile data network. In this case, it directly submits its location to the cloud application server, which will be responsible for updating the customer apps with the current bus location. Scenario 1 has a direct connection between the BDMA and the cloud application server and employs Transport Layer Security (TLS) to provide a secure channel and authentication.

The security on the remaining scenarios is enforced by digital signatures based on asymmetric cryptography [21] (e.g: RSA 2048 bits). The mechanism creates a pair of keys (public and private) for each BBD. The private key is stored at the BBD and

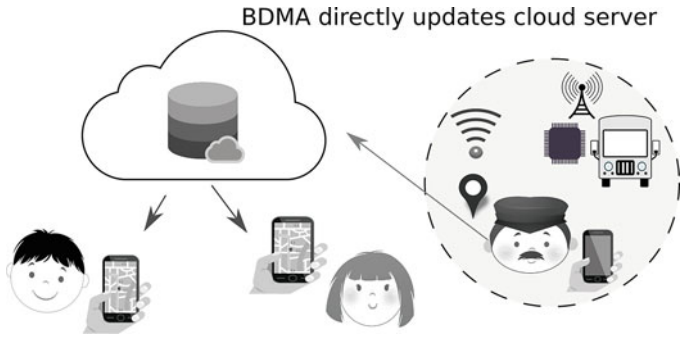


Fig. 3 Message exchange in scenario 1

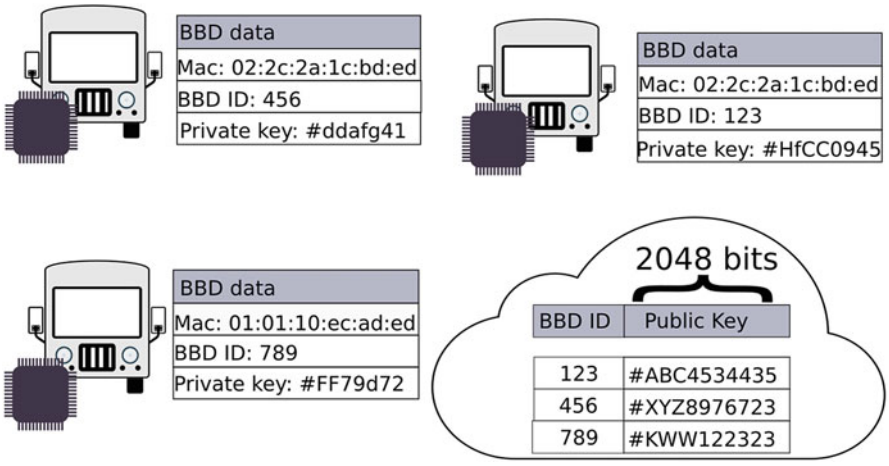


Fig. 4 Message authentication based on asymmetric cryptography

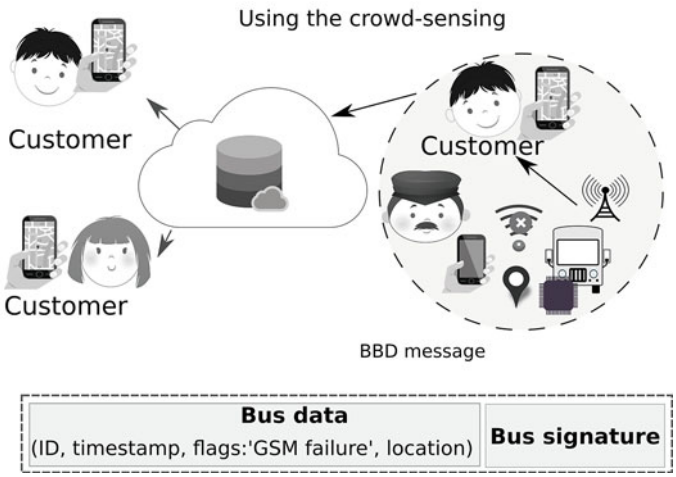


Fig. 5 Message exchange in scenario 2

the public key is stored on the cloud application server Fig. 4. The private key cannot be read nor extracted from the BBD which is assumed to be a secure hardware.

In scenario 2 (Fig. 5), the BDMA can obtain its GPS location, but cannot send the information through the mobile data network, forcing data to be sent using the crowd-sensing feature. In this scenario, a customer using the CMA receives the beacon of a nearby bus (BBD broadcast). The beacon message has fields such as flags, timestamp, BBD ID, and a signature. The BBD indicates that the update failed through the use of flags. In this case, the CMA sends the message to the server using its own data connection.

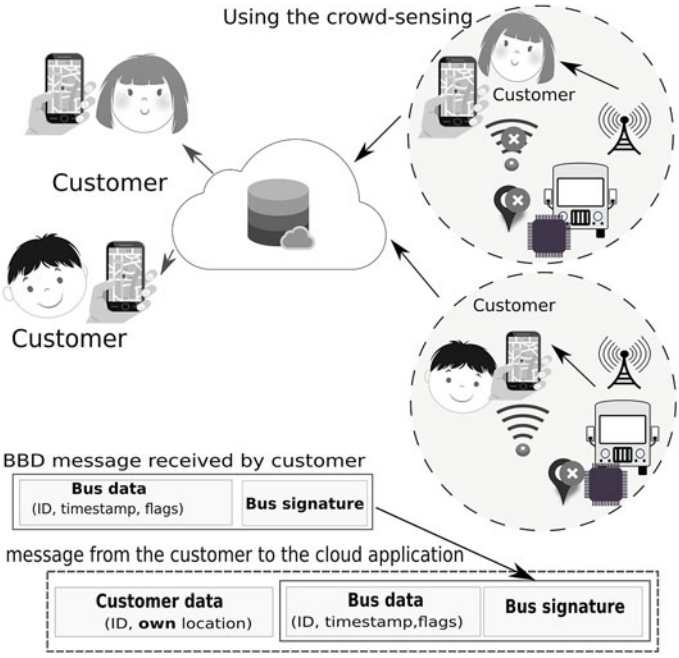


Fig. 6 Message exchange in scenarios 3 and 4

Finally, Fig. 6 shows scenarios 3 and 4. In scenario 3, the BDMA can communicate with the server, but it can not obtain its GPS location and in scenario 4, the BDMA has neither communication nor location capability. In either case, CMA get messages broadcasted by the BBD, identify the problem using the flags and send the message to the cloud application server.

Whenever the BDMA is unable to update the cloud application server (scenarios 2–4), it switches to the crowd-sensing mode by instructing the BBD of the failure type and it uploads its timestamp and GPS location, if available (scenario 2). The BBD receives the message and applies a hash function (e.g: SHA3-224) to produce a digest. The digest is encrypted using the private key kept at the BBD and concatenated to the original message, resulting in a signed message (Fig. 7). The signed message is broadcasted to collaborative customers which will capture and propagate it to the cloud application server using their own data connection

At the cloud application server the signed message is splitted in two parts, the original message and the encrypted digest. The same hash function (SHA3-224) is applied to the original message to produce a digest. On the encrypted digest is applied a public key to produce a plain digest and both digests are compared. The message is authentic and accepted if the digests are equal, otherwise it is discarded.

In scenarios 2,3 and 4, where a malicious customer can capture, modify and transmit the message, the cloud application server is able to detect the problem and discard the message. The malicious customer can also capture, store and send a

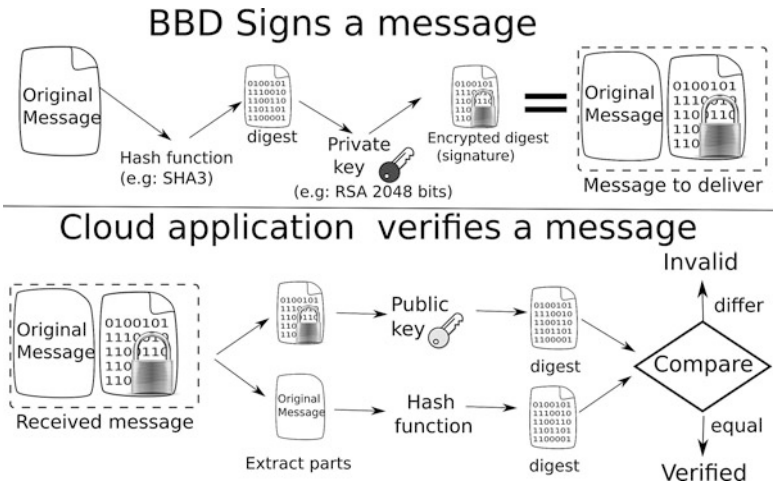


Fig. 7 Signing and verifying messages

message later when the bus is at another location in an attempt to cheat the location system, leading to an error. In this case, the cloud application server will discard the message because, although genuine, it has an old timestamp.

Finally, a malicious customer can also impersonate a bus by creating a beacon and trying to trick legitimate customers into propagating their messages. In this case, even if the legitimate customer propagates the message, it will be identified as a bogus message due to the fake signature, and it will not be accepted by the cloud application server.

3.7 Multiple Locations

On a real situation the cloud application server will receive k messages from BBDs and customers targeting a bus location. On the cloud application server, the received information is stored on a list ordered by the message's timestamp and only keeps the last messages which fit inside the time-window Δt. Messages can be labeled trusted or untrusted according to their origin. Whenever a message is received directly from a BDMA or from a customer and authenticated it is assumed as trusted. On the other hand, messages from scenarios 3 & 4 are untrusted as they may contain fake locations.

3.7.1 Trusted Locations

Figure 8a shows the case where there are 5 messages on a list, 1 directly from a BDMA and 4 from customers. Customers 5, 12 and 1 sent their own locations as they

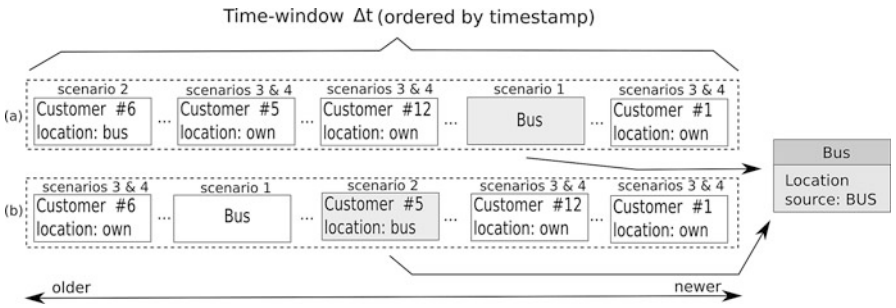


Fig. 8 Location submissions with at least one trusted location

are acting as in scenario 3 & 4. Customer 6 is action as in scenario 2 (authenticated message) and finally the bus driver acts as scenario 1. Both scenarios 1 and 2 are trusted as they possess an authenticated message. However, as the timestamp of the bus driver's message is earlier, its location is chosen to represent the current bus location. In (b) both the bus driver and the customer 5 are trusted and as the customer has the earlier timestamp, therefore its location is chosen.

3.7.2 Untrusted Locations

A special situation happens when the location list possesses only locations from customers acting as in scenarios 3 & 4. As in this cases customers submit their own locations, they cannot be trusted and every customer may present a different but near location for the same bus. Two questions arise: (1) how to detect if one/some customers are delivering malicious locations (e.g: a bus presented as in a far away location), and (2) how to combine all customers locations into a single one.

There is no easy answer for the first question as malicious customers can collude by sending fake but near/equal locations for a bus. Our solution uses a best-effort **acceptance test** which tries to prevent malicious customers from mislocating the bus without promising success. The acceptance test may employ different algorithms and for illustration purposes, we employ a K-means algorithm [3] as follows. All N customers' submitted locations within a time-window (e.g: 60 s) are grouped in K clusters. Using the Algorithm 1, near locations are assigned to the same data set. The number K was chosen to be a function of N, such as, $K = \lceil \log_2 N \rceil$. Finally, The data set with more elements is chosen to represent the approximate bus location and their locations are computed by the **combining algorithm** to result in a single location.

Within a time window Δt (Fig. 9), e customers submit their locations to the cloud application server. The average bus location (avg_{Lat}, avg_{Lon}) is computed using the combining Algorithm 2, which uses the location of each customer C_i ($1 \leq i \leq e$) to define the average geographical point. The combining Algorithm can be summarized in three steps: (1) converts all geolocations to radians and then to

Algorithm 1 Acceptance test

```
1: custLoc(1, .., N) submitted locations from N customers
2: K ← ⌈log2 N⌉ number of centroids
3: centLoc(1, .., K) K centroid locations
4: function CHOOSELOCATIONS(N, K, custLoc, centLoc)
5:     // Create random locations for Centroids
6:     centLoc ← initRandomLocations(K)
7:     repeat
8:         // Assign each customer location to a set own by closest centroid
9:         clusterSet ← empty
10:        for i ← 1, N do
11:            closest ← findClosestCentroid(custLoc(i), centLoc)
12:            clusterSet[closest] ← clusterSet[closest] ∪ custLoc(i)
13:        end for
14:        // Re-calculate each centroid's location
15:        oldcentLoc ← centLoc
16:        centLoc ← newMeanLocation(clusterSet)
17:    until convergence (oldcentLoc,centLoc)
18:    return elementsFromBiggerSet();
19: end function
```

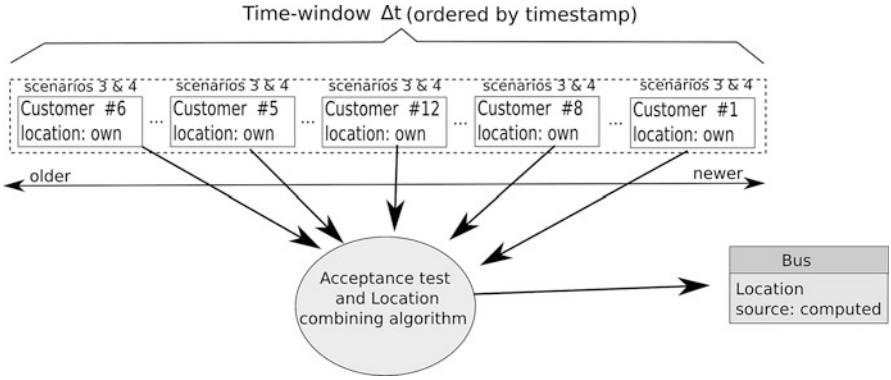


Fig. 9 Location submissions with only own locations

Cartesian locations ($cartesianX$,$cartesianY$,$cartesianZ$); (2) sums all resulting locations; and (3) converts the result back to geolocation (latitude, longitude).

In Step 2, all locations sent by customers within the time window are equally treated. For example, a location sent by a customer at the very beginning of a time window has the same weight as the most recent location sent by another customer. The combining algorithm creates a weighted average location where the timestamp is accounted to create a weighted value. Figure 10 presents a scenario where a single bus moves from right to left with 4 customers nearby. At time t_1, customer C_1 detects the bus and sends its location with a timestamp (already shown converted into a Cartesian location) $(x_1, y_1, z_1), t_1$. At time t_2, the bus is already at another position and customer C_2 detects and sends its location $(x_2, y_2, z_2), t_2$. At time

Algorithm 2 Combining geolocations

$sumX \leftarrow 0\ sumY \leftarrow 0\ sumZ \leftarrow 0\ W_{total} \leftarrow 0$
for all i such that $1 \leq i \leq e$ **do**
  // Step 1- Converts to rad and then to cartesians
  $lat \leftarrow latitude[i] \times (\pi/180)$
  $long \leftarrow longitude[i] \times (\pi/180)$
  $cartesianX \leftarrow \cos(lat) * \cos(long)$
  $cartesianY \leftarrow \cos(lat) * \sin(long)$
  $cartesianZ \leftarrow \sin(lat)$
  // Step 2 - Sums all locations
  $sumX \leftarrow sumX + cartesianX \times W[i]$
  $sumY \leftarrow sumX + cartesianY \times W[i]$
  $sumZ \leftarrow sumX + cartesianZ \times W[i]$
  $W_{total} \leftarrow W_{total} + W[i]$
end for
// Computes the GeoMidpoint
$X_M \leftarrow sumX/W_{total}$
$Y_Y \leftarrow sumY/W_{total}$
$Z_M \leftarrow sumZ/W_{total}$
// Step 3 - Converts back to degrees
$avg_{Lon} \leftarrow atan2(Y_Y, X_M)$
$hyp \leftarrow \sqrt{X_M * X_M + Y_Y * Y_Y}$
$avg_{Lat} \leftarrow atan2(Z_M, hyp)$
$avg_{Lon} \leftarrow avg_{Lon} \times (180/\pi)$
$avg_{Lat} \leftarrow avg_{Lat} \times (180/\pi)$

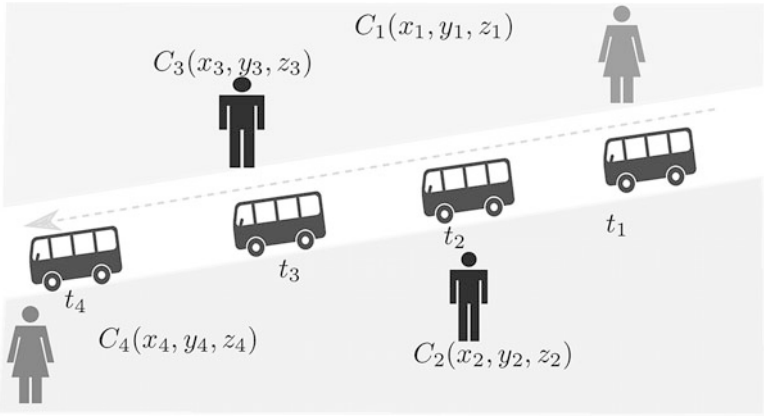


Fig. 10 Bus been detected by customers as it moves

t_3, both customers C_2 and C_3 detect and send their locations. Finally, at time t_4, customer C_4 detects and sends its location.

Lets assume W_i is the weight (or contribution) of customer C_i to the resulting weighted location. W_i is low if the customer's location was submitted at beginning of the time window and high if submitted at end. Assuming the time window Δt

Table 1 Summarizing the events

Time	Event	Inside the time window
t_1	C_1 detects bus	$(x_1, y_1, z_1$ at $t_1)$
t_2	C_2 detects bus	$(x_1, y_1, z_1$ at $t_1)$
		$(x_2, y_2, z_2$ at $t_2)$
t_3	C_3 detects bus	$(x_1, y_1, z_1$ at $t_1)$
	C_2 detects bus	$(x_2, y_2, z_2$ at $t_3)$
		$(x_3, y_3, z_3$ at $t_3)$
t_4	C_4 detects bus	$(x_1, y_1, z_1$ at $t_1)$
		$(x_2, y_2, z_2$ at $t_3)$
		$(x_3, y_3, z_3$ at $t_3)$
		$(x_4, y_4, z_4$ at $t_4)$

covers $[t_1, t_4]$, W_1 at t_1 values 1, at time t_2 values 2 and so forth. Table 1 summarizes the data. After computing the new locations (x_M, y_M, z_M), the coordinates are converted back to latitude and longitude.

4 Implementation

The BBD needs to communicate with ordinary smartphones and, therefore, it was necessary to choose a compatible communication technology. Nowadays, most smartphones are BLE capable, which is a Bluetooth low power extension that allows to send and receive messages from other BLE devices without disturbing the regular WiFi communication.

One such device is called iBeacon and basically its function is to periodically broadcast a message with a token (identification). If a smartphone detects an iBeacon broadcast, it can take an action such as showing the token or running a specific application in response. Besides detecting a token, smartphones can also connect to the iBeacon and extract some information. Examples of ordinary iBeacon devices are temperature sensors, smart body scale, car tire pressure sensors, etc.

BLE devices can be classified as Peripheral or Central. A Peripheral device is an information server device (such as a temperature sensor). It periodically broadcasts its message (advertise). Within this advertise, there is some information about *services* and *characteristics* that are available, as well as the manufacturer's information, *mac-address*, device name, etc.

A BLE device has multiple *services* and each *service* can have multiple *characteristics*. A smartphone is a Central *device* that scans the BLE network and detects all advertise *packets* within a time window. It can connect to a device identified by its *mac-address* and perform operations such as reading/writing on a *characteristic* that belongs to a *service*. Thus a smartphone is able to read the temperature of a sensor by periodically sending read operations.

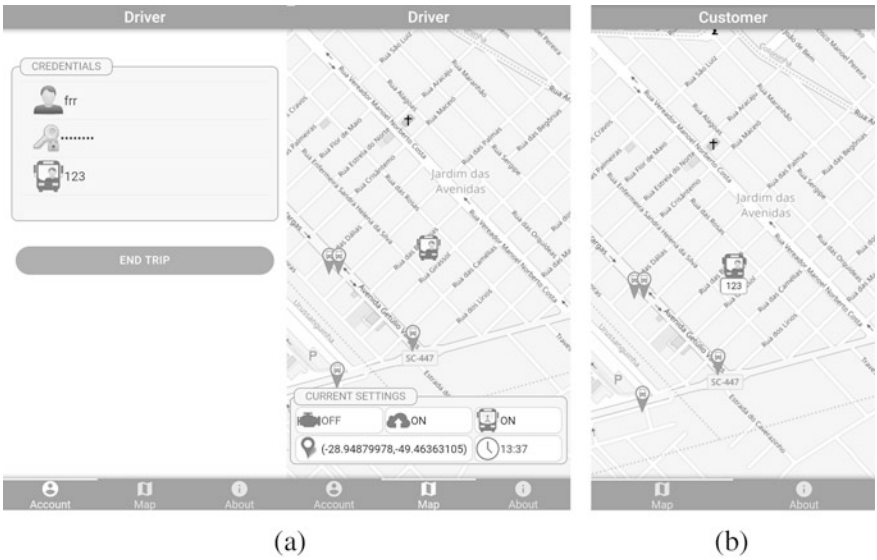


Fig. 11 Screenshots from both mobile apps. (**a**) BDMA application. (**b**) CMA application

4.1 Mobile Apps

In software development for mobile applications, we used Cordova hybrid framework, which uses JavaScript, HTML, and CSS to create apps for Android and iOS without the learning curve of each of these specific platforms. The result is a mobile application ready for publication in Apple Store (iOS) or Play Store (Android). Using plug-ins, Cordova gains access to the native resources of a smartphone (GPS, Bluetooth, WiFi, camera, etc.). Also, there are frameworks and libraries with easy to use resources such as user interface, push notifications, online maps, etc.

Figure 11 shows screenshots of the mobile apps. In (a) the BDMA app is shown with two screens: the driver's sign-in credentials and the map/status (Telemetry status, GPS location, server status and BBD update status). In (b) is shown the CMA with a map, nearby buses and bus stops.

Internally, the application server implements a RESTful Application Programming Interface (API) to support requests from mobile applications. The server also uses WebSockets to reduce latency and allows customers' applications to be notified whenever a bus location is updated.

4.2 BBD Implementation

The embedded device BBD can be programmed using any BLE capable device. We have tested ESP32 and Raspberry Pi Zero W as both are BLE capable and low

cost devices. Raspberry Pi Zero W is a more powerful device in terms of CPU and memory. Also, it hosts a full operating system and libraries which are convenient for software development/testing. On the other hand, ESP32 from Espressif is a simpler microcontroller with only 520KiB of RAM, 4 MiB of Flash memory and can be programmed using Arduino environment. In our implementation the ESP32 device was chosen due to its lower cost.

The public-key cryptography was implemented in software. However, recently Espressif release the new SoC ESP32-S2 with security features embedded in hardware such as secure boot, encrypted flashing code, cryptographic accelerator and support for digital signature which keeps the private key secure.

The initial test with the BLE revealed drawbacks with many failed attempts when trying to connect the CMA to the BBD. Additionally, many successful attempts required a variable time to establish the connection. Furthermore, a BLE device typically supports up to four simultaneous connections that limits the actual intended scenario with multiple CMA connecting and capturing data from the BBD.

4.2.1 Data Dissemination Protocol

To address this drawback, a bus data dissemination protocol has been developed where the customers' applications do not need to establish a connection with the bus to access its data. In this protocol, the CMA captures the advertise packets transmitted via broadcast and, inside these packets, lies the useful bus data. However, the BBD data amount needed to broadcast (BBD ID, location, message type, timestamp, digital signature, etc.) does not fit in a single advertise packet. As a result, the dissemination protocol breaks the original message into a set of enumerated fragments, which are transmitted one at a time inside the advertising packet every 200ms. The cycle restarts after the last fragment has been transmitted.

Fragments are received by one or more CMA, stored and reassembled without these fragments having to be received (correctly) in an ascending order. In this protocol, since there is no connection between the two peers, the initially reported problem no longer exists and the possible number of CMA receiving the data is no longer a concern. As long as the BDMA does not update the BBD with a new message, the BBD continues to cyclically transmit the fragments of the last received message. When a fragment of a new message is received by the CMA, all the previously stored fragments are discarded as they will never be retransmitted.

4.2.2 Telemetry

Besides its location, the bus sends telemetry information (engine temperature, fuel consumption, battery level, Rotations per Minute (RPM), vehicle speed, fuel injector status, engine air temperature, etc.). This information is important to prematurely diagnose problems and analyze bus driver behavior. The BDMA is able

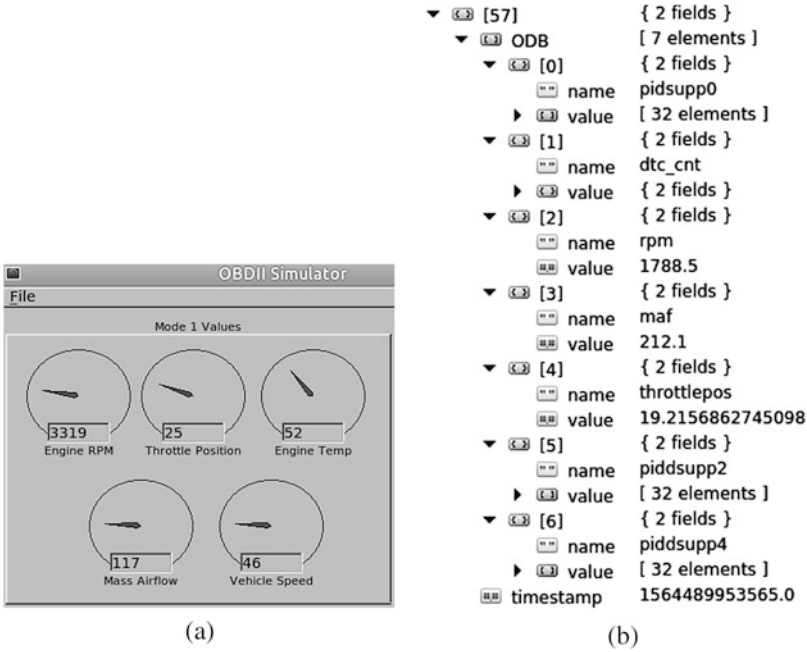


Fig. 12 Telemetry data on the simulator and on the cloud application. (**a**) ODB scanner simulator. (**b**) Telemetry on the cloud server

to communicate with a commercial bluetooth ODB scanner, send commands and capture values from the vehicle's computer.

The BDMA app needs to capture vehicular telemetry from an ODB device and send to the cloud application. During the software development an ODB simulator was used to test/debug the communication between the BDMA and the ODB device. The simulator software transforms a personal computer into a Bluetooth scanner and allows the mobile application to pair, send and capture commands just like a real ODB device. Vehicle sensor values can be easily modified using the simulator graphical interface and check if the change has been captured at the mobile application and also at the cloud application. The simulator is shown in Fig. 12a where the user can set the Engine RPM, Speed, Temperature, Throttle position, etc. The simulated values were captured by the BDMA and sent to the cloud application for storage in MongoDB [2]. In (b) is show a fragment of the ODB data extracted from the MongoDB using a visual interface (Robo 3T[2]). After the mobile development was finished the BDMA app was successfully tested on a real commercial ODB bluetooth scanner.

[2] https://robomongo.org/.

4.3 Cloud Server

The cloud-based application has been implemented using NodeJS due to its ability to stand a high demand from concurrent customers and also by its rich ecosystem of the open source libraries and the tools available. In addition, both NodeJS and Cordova (used to deploy mobile applications) are based on JavaScript, which reduces the learning curve of different computer languages and also allows code sharing. Our implementations uses Amazon AWS as a cloud hosting provider.

5 Evaluations and Tests

This section presents the functional evaluations of the tracking system and the dissemination protocol. Furthermore, it shows the measures of the BDMA bandwidth and as well as the app battery consumption.

5.1 GPS Traces Evaluation

The BDMA captures GPS data and uploads it to the cloud-based application where it is kept in a location history. For testing purposes, the cloud server's API was extended to accept a **`GET/location`** request and return an array with the stored locations.

For this test scenario, a car was used to move around the city approximately at 50 km/h with an Android smartphone (Samsung Galaxy A10) running the BDMA with a 3G/4G data connection. A Web application was developed to present the city map, send the **`GET`** request, capture the location history and plot the locations as a continuous line connecting the GPS locations. The result is shown in Fig. 13.

During a test, the car was driven to a parking lot inside a building where the GPS is non-functional (the urban canyon problem) and left after 5 min to continue a trip. The GPS traces showed a jump from the parking lot entrance to a different location (approximately 600 m away from the car's real position). The behavior can be explained as the default Android settings use other location sources (such as the mobile antennas) when the GPS is unavailable to create an estimated location. After changing the Android settings to use GPS as the only location source, no more mislocations were detected. The test was repeated and the final result is shown in Fig. 13. This time the plot presents the locations before and after the parking lot as the smartphone was unable to send new locations when inside.

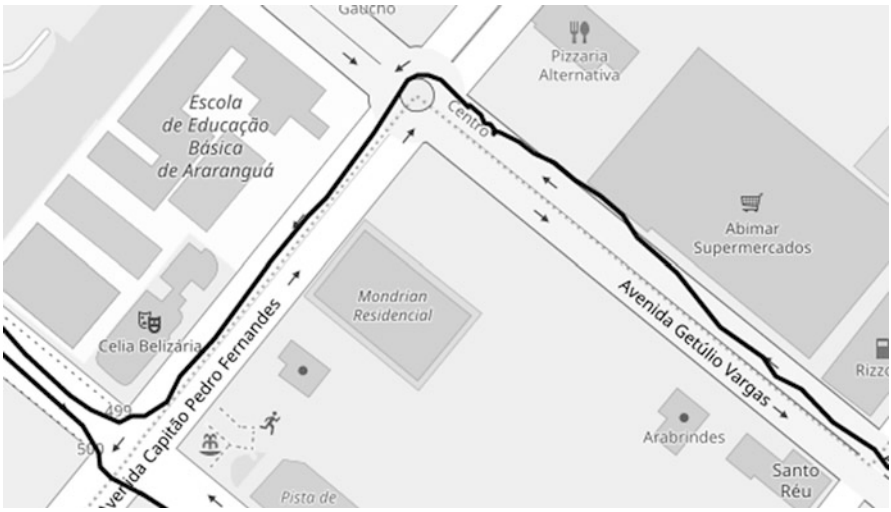


Fig. 13 GPS traces in a test scenario

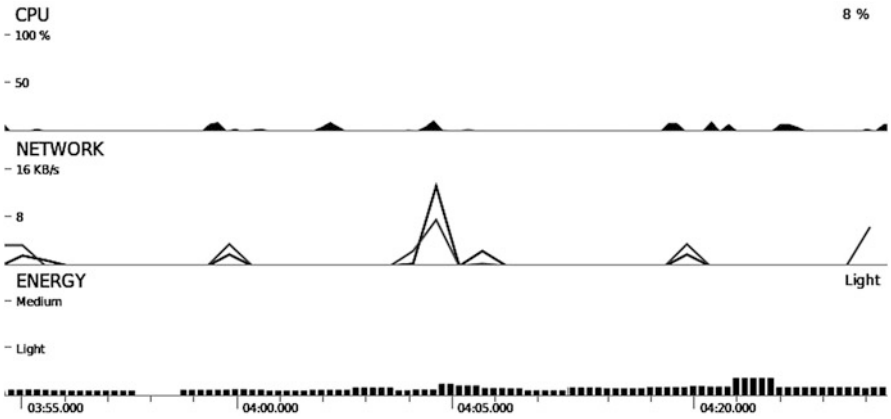


Fig. 14 Fragment showing the evaluations on the Android Studio

5.2 Performance Evaluations

Android Studio is the official development environment for the development of Android applications. Among others resources, it has an evaluation tool that transfers and runs an Android Application Pack (`apk`) on the smartphone. The application sends back data that is presented in Android Studio as a set of graphics for CPU, network and energy usage (Fig. 14). Each graph shows the behavior of the application as time passes (x-axis) with values on the y axis.

5.2.1 CPU Evaluation

The application's CPU usage spikes due to the periodic behavior of the application that transmits telemetry and the current location every 5 s to the cloud server. Most CPU spikes occur periodically every 5 s due to the capture location `GPS` and network activity. The CPU spikes that occurred outside this period are due to the switching between application screens and the design process that consumes CPU resources to render the interface. General CPU usage is generally 4% with a maximum peak of 12%.

5.2.2 Network Evaluation

In many regions, mobile data can be both limited and expensive. Therefore, it is necessary to analyze the bandwidth use of the `BDMA` application. At first, the application validates the driver's credentials on the cloud server and *downloads* static data and map. After the initial stage, the only network activities are due to telemetry and location which are periodic, in addition to updates to the map service. Telemetry from the `ODB` scanner is composed of 368 bytes and transmitted every 20 s. On the other hand, the location consists of 115 bytes and is transmitted every 5 s.

The application performs **`POST`** operations on the cloud server and uses basic authentication. The process is repeated for each data transmission. Unfortunately, as requests use the *https* protocol, there is a *overhead* in each submission. On average, the bandwidth usage (sending and receiving) is less than 6KiB/s. Although the current use of bandwidth is small, there is an opportunity for significant reduction, avoiding the *https* protocol and replacing it, for example, with *websockets*).

5.2.3 Energy Evaluation

An Android application presents a variable use of energy according to user interaction. The main aspects that lead to greater energy use are the user interface (screen rendering), `GPS` and network.

For example, if the user selects a screen with static information (menu **About**), energy use is low due to the screen. If the user selects a screen with a map, the energy will increase due to the amount of CPU required to render the map, download and store the streets in *cache*. According to Android Studio the general energy use of the test application is classified as light.

5.3 Functional Evaluation of Data Dissemination Protocol

The message broadcast system has been initially evaluated in a testbed composed by 5 ESP32 development kits. Each of these kits represents a `BBD` and receive

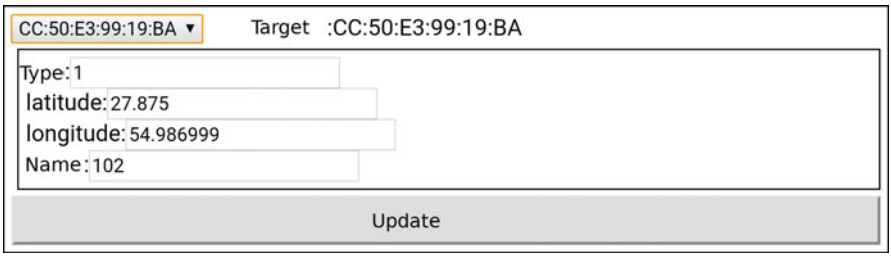


Fig. 15 Application to update BBD during tests

ID	Type	Name	Latitude	Longitude	Timestamp
A4:CF:12:02:CB:A2	1	103	26.45600128173828	54.88800048828125	2019-05-27, 10:25 AM
30:AE:A4:03:47:BE	1	101	28.12299919128418	54.474998474121094	2019-05-27, 10:23 AM
30:AE:A4:0B:09:0E	1	100	28.546998977661133	55.47100067138672	2019-05-27, 10:22 AM
CC:50:E3:99:19:BA	1	102	27.875	54.98699951171875	2019-05-27, 10:24 AM
30:AE:A4:0C:D6:52	1	104	27.12299919128418	55.12300109863281	2019-05-27, 10:26 AM

Fig. 16 Customer mobile application showing the buses nearby

messages from the BDMA, break the messages into fragments, and send them via *broadcast*. For evaluation purposes, another mobile application has been developed to create/update dummy coordinates for each bus (Fig. 15).

In this application, it is possible to select the target bus (by its *mac-address*), adjust the bus location (latitude and longitude) and send data to a specific bus. By using this application, locations were sent to each BBD and the correct results were seen on the CMA (Fig. 16). The CMA does not show repeated messages, even though they are being periodically resubmitted by the BBDs. The test was repeated 20 times with 100% of success.

6 Conclusion

In this paper, we presented a solution to mitigate the unavailability of bus location data in public transport tracking by providing a real or approximate location whenever a bus is unable to report its position. Our solution uses a crowd-sensing strategy along with mobile applications and addresses security issues to identify and deal with malicious customer attacks. Also, we developed a data dissemination protocol to transfer information between customers and buses via BLE without a prior connection or handshaking mechanism. Finally, we dealt with the cost-

effective problem by providing a solution based on low-cost hardware elements and open source software. As a future work, we intend to evaluate our proposal through a simulated environment and measure a quality benefit for users.

References

1. An, J., Gui, X., Wang, Z., Yang, J., He, X.: A crowdsourcing assignment model based on mobile crowd sensing in the internet of things. IEEE Internet Things J. **2**(5), 358–369 (oct 2015)
2. Banker, K.: MongoDB in Action. Manning Publications, Greenwich, CT, USA (2011)
3. Berkeley, C., Macqueen, J.: Some methods for classification and analysis of multivariate observations. Statistics **1**, 281–297 (1967)
4. David, S., Bill, E., Tim, L., Jim, B.: 2015 Urban Mobility Scorecard. Tech. rep., Published jointly by The Texas A&M Transportation Institute and INRIX (2015)
5. de la Rocha, F.R., Tramontin, R.: Improving public transport location by using a collaborative mobile system. In: CLEI 2018 - WLATAC (Oct 2018)
6. Deans, C.: The design of an intelligent urban transportation system in Jamaica based on the Internet of Things. In: SoutheastCon (2015)
7. Fan, W., Gurmu, Z.: Dynamic travel time prediction models for buses using only GPS data. Int. J. Transp. Sci. Technol. **4**(4), 353–366 (2015)
8. Farkas, K., Feher, G., Benczur, A., Sidlo, C.: Crowdsending based public transport information service in smart cities. IEEE Commun. Mag. **53**(8), 158–165 (Aug 2015)
9. Ferreira, M., Fernandes, R., Conceição, H., Gomes, P., d'Orey, P.M., Moreira-Matias, L., Gama, J.a., Lima, F., Damas, L.: Vehicular sensing: Emergence of a massive urban scanner. In: Martins, F., Lopes, L., Paulino, H. (eds.) Sensor Systems and Software, pp. 1–14. Springer, Berlin, Heidelberg (2012)
10. Flagan, R.C., Seinfeld, J.H.: Engineering: Fundamentals of Air Pollution Engineering (Dover Civil and Mechanical Engineering). Dover Publications (2012)
11. Guo, B., Chen, C., Zhang, D., Yu, Z., Chin, A.: Mobile crowd sensing and computing: when participatory sensing meets participatory social media. IEEE Commun. Mag. **54**(2), 131–137 (2016)
12. Haleem, S.L.A., Samsudeen, S.N.: Real time bus tracking and scheduling system using wireless sensor and mobile technology. J. Inf. Syst. Inf. Technol. **1**(1), 18–23 (2016)
13. Kamilaris, A., Pitsillides, A.: Mobile phone computing and the internet of things: A survey. IEEE Internet Things J. **3**(6), 885–898 (dec 2016)
14. Khan, W.Z., Xiang, Y., Aalsalem, M.Y., Arshad, Q.: Mobile phone sensing systems: A survey. IEEE Commun. Surv. Tutor. **15**(1), 402–427 (2013)
15. Moreira-Matias, L., Mendes-Moreira, J., de Sousa, J.F., Gama, J.: Improving mass transit operations by using AVL-based systems: A survey. IEEE Trans. Intell. Transp. Syst. **16**(4), 1636–1653 (Aug 2015)
16. Morency, P., Strauss, J., Pépin, F., Tessier, F., Grondines, J.: Traveling by bus instead of car on urban major roads: Safety benefits for vehicle occupants, pedestrians, and cyclists. J. Urban Health **95**, 196–207 (2018)
17. ONU: Sustainable Cities: Why They Matter (2016), https://www.un.org/sustainabledevelopment/wp-content/uploads/2016/08/16-00055K_Why-it-Matters_Goal-11Cities2p.pdf
18. Pardeshi, A., Dantara, K.: Maximum efficiency of mobile cellphones in shadow zone. IOSR J. Electr. Electron. Eng. (IOSR-JEEE) (2015)
19. Sarraf, J., Priyadarshini, I., Pattnaik, P.K.: Real time bus monitoring system. In: Advances in Intelligent Systems and Computing, pp. 551–557. Springer India (2016)

20. Shriram, S., Bagavathi Sivakumar, P., Anantha Narayanan, V.: The smart bus for a smart city - A real-time implementation. In: 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1–6 (Nov 2016)
21. Stallings, W.: Cryptography and Network Security: Principles and Practice, sixth edn. Prentice Hall Press, Upper Saddle River, NJ, USA (2013)
22. Thiagarajan, A., Biagioni, J., Gerlich, T., Eriksson, J.: Cooperative transit tracking using smartphones. In: 8th ACM Conference on Embedded Networked Sensor Systems. ACM Press (2010)
23. Vanegas, F., Gaston, K.J., Roberts, J., Gonzalez, F.: A framework for UAV navigation and exploration in GPS-denied environments. In: 2019 IEEE Aerospace Conference. IEEE (Mar 2019)
24. Zhang, X., Yang, Z., Sun, W., Liu, Y., Tang, S., Xing, K., Mao, X.: Incentives for mobile crowd sensing: A survey. IEEE Commun. Surv. Tutor. **18**(1), 54–67 (2016)
25. Zhou, P., Zheng, Y., Li, M.: How long to wait? Predicting bus arrival time with mobile phone based participatory sensing. IEEE Trans. Mobile Comput. **13**(6), 1228–1241 (2014)

Location-Based Services for Smart Living in Urban Areas

Pampa Sadhukhan, Nandini Mukherjee, and Pradip K. Das

1 Introduction

The dramatic growth in wireless communication technologies and mobile platform along with the increasing demand of the mobile subscribers to access various location-related information, services and also applications anywhere anytime has led to the development of a new genre of mobile services that would be able to provide useful information and services based on the current location of the mobile subscribers. This set of mobile services is called location-Based Services (LBSs). Example of such services include 911 emergency services [1], services for locating the nearest object of interest like Automatic Teller Machine (ATM), petrol pump, medical centre etc., in urban areas, mobile tour guides, vehicle tracking system and so on. Apart from these, several other applications such as Dark Sky used for obtaining accurate down-to-minute weather forecast for the present location of user, Uber ride app enabling a user to book some cab and obtain pick up service from his/her current location, Gas Buddy app helping to find out real-time fuel prices at the nearby gas stations and so on have significant usage in urban people's daily life. The wide applicability of the LBSs in several aspects of modern-day living which include transport, healthcare, leisure activities, business etc., is the main driving force behind drawing significant attention from not only the researchers but also the mobile network operators as well as the service providers in designing such services for smart living in the urban areas. Since LBSs require the knowledge of position information of the users to provide them appropriate information and

P. Sadhukhan (✉)
School of Mobile Computing and Communication, Jadavpur University, Kolkata, India
e-mail: pampa.sadhukhan@ieee.org

N. Mukherjee · P. K. Das
Department of Computer Science and Engineering (CSE), Jadavpur University, Kolkata, India

S. Paiva (ed.), *Precision Positioning with Commercial Smartphones in Urban Environments*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-71288-4_3

services, localization or positioning technology is an integral part of the systems that provide such services. Apart from the positioning technology, LBS infrastructures also incorporate several other components such as mobile devices including any commercial smart phone, communication network as well as the application and content providers. On the other hand, the very poor signal strength of the global positioning system (GPS) and also the cellular network within the buildings (that constitutes indoor areas) necessitates for designing alternative positioning techniques or localization systems to provide accurate position information in such areas [2]. Thus, various promising solutions to provide accurate position information in the indoor areas based on wireless technologies like Wireless Fidelity (Wi-Fi), Bluetooth, Zigbee, Radio Frequency Identification (RFID) etc., have been proposed in literature over the past few decades [2]. Thus, the precise positioning of the user is the most important criteria for designing the LBS systems. Apart from the positioning or localization technologies, other components of an LBS system or infrastructure are the mobile devices, communication network and the services as well as content providers. This chapter, at first, provides a detailed ***definition of the LBSs*** and also states ***its importance in today's World.*** Then, it provides a ***state-of-the-art review of the various LBS Infrastructures and systems*** proposed in the literature since its origin in 1996. A brief description about the ***architecture of an LBS infrastructure*** and the data flow among its components is subsequently given in this chapter. Finally, it outlines some **important research issues** in the **provisioning of LBSs** in the urban environments.

2 Location Based Services and Its Importance

Location-Based Services (LBSs) are designed to provide useful information and services based on the current location of the user. Several other definitions of LBSs that are available in the literature and the one made by the Global System for Mobile (GSM) [3] association, are presented below.

- "Information services accessible with mobile devices through the mobile network and utilizing the ability to make use of the location of the mobile device" (Virrantaus et al., 2001 [4]).
- "The provision of geographically orientated data and information services to users across mobile telecommunication networks" (Shiode et al., 2004 [5]).
- According to the GSM Association, LBSs aim to add value to the services based on the current location of the target by filtering out unnecessary data.

Examples of such services include providing a list of nearby point of interest such as Automatic Teller Machine (ATM), Medical Centre and so on, showing the position of some target on a map, or automatic activation of the service when the target enters or leaves certain predefined region.

Based on the aforementioned definitions, most of the LBSs can be realized nowadays as data or messaging services that can be provided via the *wireless*

application protocol (WAP) [6], *general packet radio service* (GPRS) [7] or *short message service* (SMS). LBSs can also be applied in the area of location based routing or selective routing, which determines the route of telephone calls or data based on the current location of the user. Thus, the geographical position of mobile devices must be determined accurately and consistently to support LBSs. From the perspective of research, LBSs have been generally considered a special subset of context-aware services. Context-aware services enable automatic provisioning of information and services according to the current context of the user. The context of the user typically consists of a set of user-specific parameters including his/her location, the characteristics of the access device and interface, the interest of the user and so on. Thus, the location being a part of the context information, LBSs are a part of the context-aware services.

The commercial LBSs are typically revenue-generating services that offer value to a mobile subscriber based on their current location. A certain type of commercial LBSs consist of finder service that, on request, delivers to users a list of nearby points of interest, such as restaurant or gas station [8]. Another type of commercial LBSs are generally based around a "push" model, in which selected data is presented to the mobile subscriber [8]. For example, the user can receive a special offer provided by a shop inside a market complex when he/she approaches its vicinity. Another very obvious and reasonable application of LBSs is the provisioning of emergency services, which require estimating the location of an emergency caller accurately if the call is received from a mobile subscriber [9]. In addition to commercial LBSs and emergency services, various other applications of LBSs include location-sensitive billing, pedestrian navigation, asset tracking, fleet management, smart transportation systems and so on.

3 State-of-the-Art Review of LBS Infrastructures and Systems

This section provides a brief review of various LBS infrastructures and systems proposed in the literature for provisioning of LBSs in the ubiquitous environment. At first, the existing LBS infrastructures are reviewed briefly in Sect. 3.1. Then Sect. 3.2 briefly discusses the existing LBS systems proposed providing services in ubiquitous environment.

3.1 LBS Infrastructures Proposed in Literature

Several infrastructures for delivering LBSs proposed in the literature over the past few decades are studied in this subsection. Their usefulness and limitations are also presented. Authors in [10] present an architecture based on open source technologies

for the development of Location-Based Services (LBSs). Their proposed architecture SAGESS (Spatial Application Generic Environment System Standards) enables LBS developers to offer services for heterogeneous portable devices utilizing a wide category of developing environments based on different technologies. The authors also describe a methodology, Spatial Application Generic Environment (SAGE), for developing LBS applications that are OS independent. The SAGESS architecture and the SAGE development methodology offer considerable advantages to LBS application developer and content provider by providing the facilities with higher contents compared to any other existing LBS application and by reducing the LBS development cost. However, the authors present only a study on how to deploy a prototype LBS application on SAGESS architecture. No real implementation using the toolkit for SAGE development has been provided in [10]. In [11], the authors have discussed several technical issues associated with the provisioning of LBSs through the existing wireless network architecture. For providing services through a secure and reliable wireless network, the authors have proposed some modifications to the current wireless network infrastructure. Their proposed architecture contains a Geo-location Server (GLS) that gathers information required to estimate the location of the user and contains a Geo-Location Database (GLDB) for storing the geo-related information concerning geographic objects, which enables users to visualize geographic information based on their location. The authors have also presented several application scenarios based on emergency situations, context-awareness and also the user's navigation to demonstrate the feasibility of their proposed architecture. They have also shown that such an LBS infrastructure could enable the user to access the location-dependent information rapidly in a changing environment. However, their proposed infrastructure cannot provide solution to some real-world implementation related problems like lack of scalability in dynamic data collection and also the standardization of interfaces between additional equipment. Moreover, their proposed LBS Infrastructure does not take into account the location estimation and service provisioning via wireless access networks like Bluetooth or Wi-Fi-based network applicable in indoor areas.

The researchers in [12] have presented a classification of Location-Based Services based on whether the user is willing to invoke the services and data objects are mobile or stationary. They have also described the potentially useful services belonging to each category of LBS as specified by them, emphasizing on the requirements of query-processing needed to implement that service. Although some of the services illustrated by the authors can be realized by existing commercial DBMS and GIS, the implementation of other services presented in the paper requires special data structure and query-processing algorithms. The authors in [12] have also pointed out several issues associated with query-processing as these are not supported by existing DBMS. Moreover, the introduction of a new data type, namely, the trajectory in [12] imposes new functional requirements on GIS and DBMS in terms of memory, indexing and query-processing time. The authors in [13] have initially studied the feasibility of the current wireless network infrastructure to support LBSs that deliver the location-sensitive real time message to the mobiles in a target region based on the assumption that each mobile is equipped with

self-geolocation capability. In order to offer a service that enables geographically targeted message delivery called geocasting, the wireless network has to provide geolocation information of the mobile devices to an application service provider (ASP) through which the service is offered. Here the main challenge to the wireless network and ASP is keeping track of the location information of the devices for maintaining a certain quality of service (QoS) for the LBSs as the QoS depends on the geolocation update frequency. The authors in [13] have presented several geolocation updating schemes to minimize the frequency of updating while satisfying the QoS of the application services since the geolocation update made by the mobile user consumes battery power, radio resources and increases signaling overhead in the network. The authors have presented two LBSs, namely location-based traffic report service (LBS-TR) and location-based navigation service (LBS-NS) with a description of how to adjust the operational parameters such as geolocation update frequency, resolution of geolocation to satisfy the QoS of abovementioned LBSs while reducing the signaling overhead. A metadata-based infrastructure needed for providing semantics aware LBSs in the smart environments is proposed by the researcher in [14]. This semantic-aware LBS infrastructure incorporates both ontological spatial and geometric representation. It also uses graph-based and knowledge-based navigation algorithms for delivering the services.

In our earlier works [15–18], we have proposed an LBS infrastructure that is able to provide services to heterogeneous mobile devices in ubiquitous environment using either wireless communication technologies like Bluetooth, Wi-Fi or the Internet connection. Our proposed LBS infrastructure comprises several base stations (BS) each of which is Bluetooth-enabled as well as Wi-Fi-enabled and one (central BS) among these BSs have global IP in order to make the services available anywhere over the Internet connection. Moreover, LBS-Middleware is deployed on each BS in order to advertise the services to the mobile users as well as enable the devices with limited resources (like computing capability, memory etc.) to consume the services in a secured fashion [16–18]. Our proposed LBS-Middleware acquires the features of generalized middleware such as interoperability, portability, scalability and so on. It can also dynamically deploy the client application onto the devices in order to reduce the memory consumption and make devices adaptable to new services it discovers whenever it reaches a new location as described in [19]. Apart from GPS-based positioning, a time-of arrival (ToA) based localization scheme, modified geometry-assisted location estimation (MGALE) proposed in our earlier work [20], can be integrated into our proposed LBS infrastructure to address the technical challenges associated with the replacement of all existing cellular handsets with GPS-equipped handsets as well as the problem of limited availability of signals in dense urban areas. Furthermore, a hybrid mobility management scheme based on integrating mobile IP and session initiation protocol (SIP) has been proposed in our earlier work [21] to address the user mobility issues and to enable the users to invoke the services in an uninterrupted fashion through our proposed LBS infrastructure.

3.2 Provisioning of LBSs in Ubiquitous Environment

Many approaches for delivering LBS to mobile users in a ubiquitous environment have been proposed by the researchers over the past few decades. From the literature survey, it has been noted that almost half of the LBS systems rely on GPS for providing services outdoor while the majority of them utilize wireless technologies like WLAN, Infrared, Radio-frequency identification (RFID), Bluetooth, Zigbee etc., for providing services indoor. Due to variations in indoor and outdoor positioning techniques used in the urban environments, various LBSs provisioning systems proposed in the literature for such environments can be divided into three categories. These are (1) indoor location-based services and tracking systems, (2) outdoor location-based services and navigation system and (3) Integrated indoor and outdoor location-based services. In the following sections, these three categories are discussed.

3.2.1 Indoor LBS and Location Tracking System

In this section, some existing systems and approaches that can provide LBSs and navigation services in indoor environments like shopping mall, airports and university department buildings are reviewed along with their advantages and limitations. To explicitly determine a user's position in an indoor environment, wireless technologies such as Infrared, RFID, WLAN, Bluetooth, Zigbee are exploited. Active Badge developed by researchers in [22] uses infrared technology for indoor localization. They encounter two major problems created by lack of line-of sight and short-range signal transmission.

SpotON proposed in [23] attempts to determine three-dimensional location of an object by using RFID based signal strength measurements. In this system, several object location tags were built and their locations were determined by homogeneous sensor nodes without having any central control. Several other LBS systems presented in [24, 25] rely on RFID technology, whereas the researchers in [26] utilize Zigbee for indoor localization. However, most of the mobile devices do not come with technologies like RFID and Zigbee.

Authors in [27] propose an approach that uses triangulation methods on the nodes in a local wireless network, e.g., a network formed by Wi-Fi or Bluetooth, to provide sufficiently accurate location estimation in an indoor area. However, this approach consumes large amount of power and also requires high network bandwidth, which are not always readily available. The LBS systems proposed in [28–30] uses Wi-Fi technology for location estimation and provisioning of services to the user. However, accurate position estimation of the devices using WLAN or Wi-Fi technology, mandates the use of some sophisticated positioning algorithms like fingerprint techniques or some model-based techniques that find out the relation between the measured signal strength at some receiving point from a transmitter and the separating distance between them [31]. On the other hand, the experimental

results provided in [32], shows that the Bluetooth-based personal area networks (PANs) can maintain almost equal bandwidth and also a fixed level of energy efficiency while those for the IEEE 802.11-based PANs decrease sharply with an increasing number of PANs. The wireless technology Wi-Fi is mainly compliant with IEEE 802.11b whereas, Bluetooth is low-cost as it operates in the license-free domain, consumes less power compared to other wireless technologies and comes with almost every mobile device. Thus, in the remaining part of this section, Bluetooth-based indoor localization and the navigation systems have mainly been focused.

The authors in [33, 34] present Bluetooth based system providing LBSs in indoor environment. In [33], authors demonstrate a context-aware system developed using Java for the purpose of providing appropriate information about every art to the museum visitors while they come near to that art to view it. Their proposed system consists of three types of software entities: (1) mobile application that runs on a Bluetooth-enabled device, (2) Museum Information Point (MIP) that provides information about the arts over Bluetooth connectivity upon a request from a mobile client and (3) central data server that stores information about various arts located within the museum in its database and provides those art related information to the MIPs. The major limitation of this LBS provisioning system is that only those devices having support for Java API for Bluetooth Wireless Technology (JABWT) [35] can communicate with the MIPs via the preinstalled client application running on those devices to access art related information.

On the other hand, the authors in [34] have presented a Bluetooth based LBS system called SBIL, to determine the position of the mobile users in the indoor areas by using the Received Signal Strength (RSS) measurements combined with an algorithm Minimum Mean Square Error (MMSE) described in [36]. In SBIL, various location dependent services are provided from the server to the mobile users via Bluetooth beacons, which are also used to track the mobile user's location. In order to access and navigate the services in uninterrupted way, the mobile client in SBIL system need to remain connected to at least four beacons all the time. Thus, it mandates the deployment of a high density of Bluetooth beacons and also the extended battery life of the mobile devices for proper functioning of SBIL.

The researchers in [37] have presented an approach to provide location-aware web-based content to Java-enabled mobile devices where the localization system is separated from the content access mechanism. In their proposed system, the positioning system incorporates several different localization technologies like Bluetooth, GPS, and WLAN, in order to enable the mobile user to select the most suitable localization technology interface from among the various available radio localization technologies based on the environment he/she is residing in. Although the above-mentioned approach supports multiple radio localization technologies, the authors have evaluated the performance of their proposed system using Bluetooth technology only and have not provided any solution to the technical issues associated with switching between different localization techniques while the user is on the move. The researchers in [38] have proposed a Map/INS/Wi-Fi integrated system that applies the cascaded Particle/Kalman filter framework structure for

delivering indoor location-based service (LBS) applications. The proposed system integrates two-dimensional indoor map information with the measurements from an inertial measurement unit (IMU) and also the received signal strength indicator (RSSI) value for estimating a location in the indoor areas.

3.2.2 Outdoor LBS and Navigation System

Most of the LBS and navigation systems that deliver location-related information and services in an outdoor environment are based on GPS-based positioning. A web-based mobility tracking and analysis system is presented in [39]. The proposed system collects and processes both cellular network-based position data such as BS id as well as GPS-based positions data to create the mobility profiles of cell phone users. However, cellular network-based position data leads to inaccurate mobility paths since the BS id always gives coarse location estimation. A GPS-based location tracking system that collects the positional co-ordinates from the integrated GPS receiver of the mobile device and determines the semantic location of the user with the help of GIS software, is proposed in [40]. However, such tracking system brings some privacy issues and security concerns as revealing location information and the possibility of editing tracked data may pose risks to an innocent person. Although in terms of accuracy, GPS is the most viable solution to positioning in an outdoor environment, the high prices of the GPS receiver along with the practical infeasibility of replacing all existing handsets with GPS-equipped handsets have deferred the researchers and telecom operators to accept it as the most viable positioning solution in an outdoor environment. Only a few LBS systems working in outdoor environments utilize the cellular ID-based positioning as the location estimation done by this positioning technique lacks accuracy. Some methods based on network-based localization technique in an outdoor environment have been investigated in detail in [41]. Lack of accuracy, loss of privacy of the user in case of cellular network-based location estimation and also the increased complexity of the Base Station (BS) in case of Angle-of-Arrival (AoA) and multipath analysis-based location estimation have primarily been cited as the main deterrents in using these approaches.

A hybrid location estimation scheme that combines the GPS-based positioning with the position estimate provided by the 3G network, has been proposed in [42]. The proposed scheme uses the signals received from the Base Stations of 3G network if the GPS receiver of the mobile device could not obtain signals from at least four satellites since four Time-of Arrival (ToA) measurements are essential for 3D position estimate of the device. The researchers in [43] have integrated GPS-based positioning with the GSM Cell-ID-based localization for providing proactive LBSs to the mobile users. The integrated positioning scheme aims to reduce the power consumption made by continuous invocation of the GPS-based location sensing and also introduce several strategies for extending the lifetime of the battery. However, the above two proposed hybrid localization schemes would not be effective to provide LBSs in dense built-up areas and metropolitan city areas as

the signal strength of both GPS and cellular network like GSM and 3G/4G are very poor. On the other hand, an application of mobile mapping and LBSs for health care is proposed and developed by integrating remotely sensed satellite data with the geographical information system (GIS) and web GIS technologies [44]. The proposed application can provide the emergency medical services through web GIS technology and also provides medical facilities in a GIS environment for various mobile clients to find suitable facility using network analysis.

3.2.3 LBS Platforms Integrating Indoor Localization and Outdoor Localization

A generic integrated platform involving several positioning technologies such as GPS, WLAN etc., and allowing various types of mobile devices to access LBSs through different communication protocols like HTTP, WAP and SMS in both indoor as well as outdoor environments, has been proposed in [45]. The researchers in [45], have discussed about the prototype implementation of proposed LBS platform, but no experimental results in order to evaluate its performances are given there. In [46], the authors have presented mobile location-aware information system that is capable of delivering location-dependent information to the mobile users while they are roaming around. Their proposed system provides support for administration of the content, navigation of the user as well as runtime management of the user sessions. In addition to these, their proposed system behaves like a large-scale system having large number of simultaneous user-sessions. However, the authors have not provided any experimental result to demonstrate its effectiveness in offering services to the users simultaneously at the scale of hundred as claimed by the authors. Moreover, the architecture of their proposed system lacks the communication interface between the integrated platform proposed by them and the mobile device willing to invoke the LBSs.

On the other hand, the researchers in [47–49] have proposed LBS systems to enable the users to invoke the services in ubiquitous environment. These systems combine GPS-based positioning with other indoor positioning technologies such as RFID, Wi-Fi etc., for determining the user's location anywhere as well as to provide him/her location aware information and services accordingly. However, these LBS systems do not have service-advertising facility and cannot manage the user mobility. A distributed architecture to provide the LBSs available on the local web server via some local access point (AP) is presented in [50]. However, the proposed system remains silent about how the connections between the local AP and various types of mobile terminals are set up and also how the invocation of services by the user continues when the mobile terminal goes out of the communication range of the local AP. The LBS Infrastructure proposed in [51] integrates the WLAN environment with 3G network to provide services anywhere. But the LBSs provided by such system can be consumed by only those devices that have proper API support for processing the messages compliant with XML-based Simple Object Access Protocol (SOAP) [52]. A similar drawback, i.e., the devices that do not

have proper API support for processing of SOAP messages are unable to consume services, is found in the work done in [53]. In [54], the authors have presented an LBS-middleware named as Middleware for Location Cost Optimization (MILCO) that attempts to reduce the consumption of network resources needed to carry out location requests. This Middleware uses most suitable localization technique for each location request to meet desired quality of service (QoS) as demanded by the user while minimizing the use of network resources. Although MILCO reduces the consumption of network resources as compared to the observed time difference-of arrival (OTDOA) and assisted GPS (A-GPS)/OTDOA coupling as shown by the experimental results, it lacks the advertising facility of location-based information services and cannot facilitate the users to consume those services in an optimal way.

The authors in [55] have investigated suitable sensors and location techniques that can be utilized in the pedestrian navigation system for continuous position determination of pedestrians. They have presented the design of a pedestrian navigation system, which integrates several suitable location sensors and incorporates different location methods in order to enable a continuous positioning of the pedestrian. However, their proposed system lacks appropriate mechanism for seamless transition between positioning in indoor area and outdoor area.

A seamless indoor/outdoor positioning scheme, which integrates GPS-based localization for outdoor environment with Wi-Fi based localization for indoor areas, is proposed in [56]. The proposed technique uses received signal strength (RSS) based fingerprint technique for indoor localization [69, 70] and also adopts some method to carry out seamless handoff between Wi-Fi-based positioning and GPS-based positioning. However, this integrated positioning scheme consumes significant battery power due to the continuous searches for available Wi-Fi APs as well as GPS signal in a continuous fashion. In [57], the researchers have presented a prototype implementation of a LBS infrastructure that have the service advertising facility and also helps the heterogeneous mobile devices to access the services. Although the proposed LBS infrastructure can deliver customable user interfaces (UIs) required to consume the services on the heterogeneous mobile platforms, but only those devices having proper compiler support to run the UIs can invoke the services effectively. A reasonable way to address the above-mentioned issue is the dynamic deployment of appropriate platform independent client application required to consume a certain LBS and also runnable on the heterogeneous mobile platforms onto the mobile device willing to invoke that service, as demonstrated by the LBS middleware proposed in our earlier work [19]. Moreover, our proposed middleware based LBS system integrating Bluetooth, Wi-Fi and GPS based positioning, can provide services anywhere over the Bluetooth, Wi-Fi or Internet connection [16–18].

Apart from the above mentioned LBS systems, several other existing LBS applications in various domains like social networks, fitness monitoring and healthcare, transport, assistive technology etc., are briefly reviewed in [58]. The authors in [59] aims to identify the public bus stops in urban areas and also to characterize their waiting time which is of much significance to the public transportation system, by analyzing the GPS-based position traces of the public bus. An LBS-based dilemma

zone warning system to assist the drivers to take appropriate action during yellow interval at the signalized intersections to ensure road safety, has been proposed in [60]. Moreover, location-based real-time application to avoid collisions for on-road vehicles and to locate some suitable nearest parking spot in urban areas have been proposed in [61] and [62] respectively. An application of location-based social network to detect the functional regions in urban areas based on the co-occurrence patterns of point of interest (POI) types, is presented in [63]. Another set of LBS applications designed for remote health monitoring have been proposed in the literature to support the dementia patients and their caregivers in wandering event [64] and also in detecting emergency situation along with reporting of fall detection [65].

4 Basic Architecture of an LBS Infrastructure

The LBS Infrastructure is a compounded system consisting of four components, viz., mobile devices, communication network, service and content providers and positioning technologies as shown in Fig. 1. The intersection among these four components of LBS system is also shown in Fig. 1.

On the other hand, Fig. 2 illustrates the data flow between the different components of the LBS Infrastructure where a user can invoke services provided

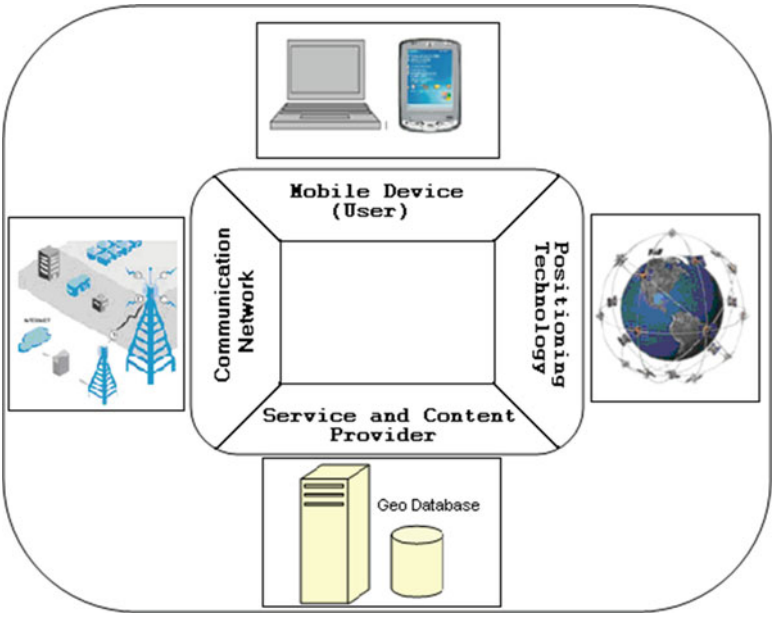


Fig. 1 Basic components of an LBS infrastructure and intersection among these components

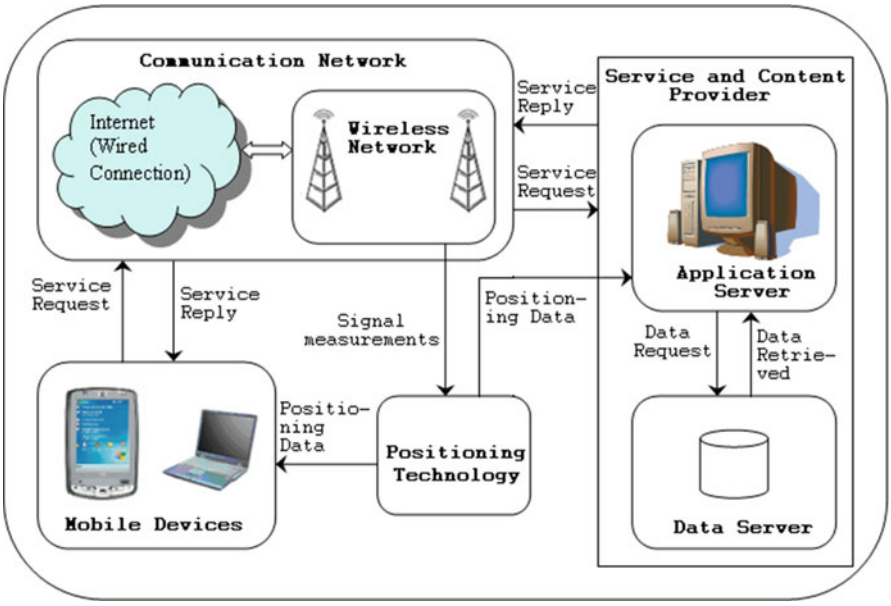


Fig. 2 Data flow between the different components of an LBS infrastructure

by the service provider from his/her mobile device having optional positioning technology through the communication network. In general, mobile user needs to send the service request to the application server where LBSs are deployed through the communication network based on wireless technologies like Bluetooth, Wi-Fi or 3G/4G. The position of the device can be estimated via terminal-based positioning if the device itself has either built-in positioning technology like GPS or the capability to calculate its position using signals received from the base stations.

(BSs); otherwise, the position of the device is estimated by invoking the location service that utilizes some network-based localization technique and the signal measurement from the network BSs. Based on the position of the device, the application server retrieves the required information from geographic information system (GIS) or geo database and sends back the service result to the user through the communication network.

5 Open Research Issues in Provisioning of LBSs

Since determining the user's position is mandatory for providing LBSs, thus location estimation or positioning is an aspect of research in provisioning of LBSs. Apart from positioning, other important aspects of LBS research are data modelling, preserving location privacy, enabling advertisement of services and their discovery

by the users and also addressing device heterogeneity, the constraint of resources within the devices as well as the mobility of user. These open research issues in provisioning of LBSs are pointed out below.

- Positioning—although GPS-based positioning can provide accurate location information in outdoor areas, replacing all existing devices with the GPS-enabled devices increases their cost and size. Even though various indoor positioning systems have been devised and proposed in the literature over the past few decades to overcome the limitations of the GPS-based positioning in such areas, *switching between the indoor and outdoor positioning schemes in an uninterrupted way* is essential for provisioning of the LBSs in urban areas. On the other hand, the accuracy of 5G-based positioning is expected to be less than 1 m in the urban as well as indoor areas and the same for suburban areas is expected to be less than 2 m [66, 67]. But there are several technical challenges to 5G-based positioning. Among these, major issues are the optimal combination of the cmWave based positioning with mmWave based positioning in 5G technology, designing some low-cost highly accurate algorithm through data fusion of multiple sources like inertial sensors, cameras, Bluetooth etc., through cooperative positioning, mitigating the effect of multipath reflections/NLoS propagation [68]. Thus, *designing a positioning solution to provide accurate location estimation anywhere in the urban environments* still remains a major research issue.
- Data Modelling—the effective modelling of the LBS data such as location data as well as other context information of the users is an important requirement in the field of LBS research. The research on this aspect aims to provide some solution on how to represent, use and store this type of LBS data.
- Privacy and Security—preserving the location privacy of the LBS user, i.e., not revealing the user's location to any third party is a crucial requirement from the user's perspective. On the other hand, enabling the user to consume the services in a secured fashion in order to reduce the consumption of network bandwidth and other resources is another important requirement from the perspective of the service provider. Thus, privacy and security are two major issues in the field of LBS research.
- Service advertisement and discovery—the advertisement of the services by the LBS system to the users as well as their discovery by the client application running at the user's devices are also two important research issues in this area.
- Device heterogeneity—the continuous evolution of mobile platforms and wireless communication technologies has created the proliferation of heterogeneous mobile devices into the market. Thus, providing LBSs to the heterogeneous devices is another important consideration.
- Constraint of resources—as majority of the mobile devices have limited resources like computing capability, memory, screen size and so on, the deployment of any computationally intensive LBS application onto such resource constraint devices is a significant research issue.
- User mobility—The user mobility hinders the uninterrupted flow of information and services to the mobile users. So, it creates uncertainty in the area of providing

LBSs. The convergence of different wireless communication technologies such as Bluetooth, Wi-Fi, 4G/5G cellular and so on has enabled the mobile users to select some appropriate wireless interface to invoke a specific LBS from his/her device when roaming around the public places like airport, shopping mall, university campus etc. In this regard, the major challenge is how to provide services in the uninterrupted way to the mobile users while they are switching between different networks through either single or multiple wireless interfaces available on their devices.

References

1. http://transition.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html
2. Liu, H., Darabi, H., Banerjee, P., Liu, J.: Survey of wireless indoor positioning techniques and systems. IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. **37**(6), 1067–1080 (2007)
3. Eberspächer, J., Bettstetter, C., Vögel, H.-J., Hartmann, C.: GSM: Architecture, Protocols and Services, 3rd edn. Wiley (2009)
4. Virrantaus, K., Markkula, J., Garmash, A., Terziyan, Y.V.: Developing GIS supported location-based services. In: Proceeding of WGIS'2001 First International Workshop on Web Geographical Information Systems, Kyoto, Japan, pp. 423–432 (2001)
5. Shiode, N., Li, C., Batty, M., Longley, P., Maguire, D.: The impact and penetration of location based services. In: Karimi, H.A., Hammad, A. (eds.) Telegeoinformatics: Location Based Computing and Services, vol. 2004, pp. 349–366. CRC Press (2004)
6. Mann, S., Sbili, S.: The Wireless Application Protocol (WAP): A Wiley Tech Brief. Wiley (2002)
7. Heine, G., Sagkob, H.: GPRS: Gateway to Third Generation Mobile Networks. Artech House (2003)
8. Küpper, A.: Location-Based Services: Fundamentals and Operation. Wiley (2005)
9. Junglas, I.A., Watson, R.T.: Location-based services. Evaluating user perceptions of location-tracking and location-awareness services. Commun. ACM. **51**(3), 65–69 (2008)
10. Mabrouk, M.: OpenGIS Location Services (OpenLS): Core Services, Open Geospatial Consortium Inc. Document Number, OGC 07-074, Sept 2008. http://www.opengeospatial.org/standards/ols
11. Hand, A., Cardiff, J., Magee, P., Doody, J.: An architecture and development methodology for location-based services. Electron. Commer. Res. Appl. **5**(3), 201–208 (2006)
12. Beaubrun, R., Moulin, B., Jaben, N.: An architecture for delivering location-based services. Int. J. Comput. Sci. Network Secur. **7**(7), 160–166 (2007)
13. Gratsias, K., Frentzos, E., Delis, V., Theodorias, Y.: Towards a taxonomy of location based services. In: The Proceedings of W2GIS, LNCS, Vol. 3833, pp. 19–30 (2005)
14. Kolomvatsos, K., Papataxiarhis, V., Tsetsos, V.: Semantic location based services for smart spaces. In: Sicilia, M.A., Lytras, M.D. (eds.) Metadata and Semantics. Springer, Boston, MA (2009)
15. Sadhukhan, P., Das, P.K.: Location-aware services in mobile environments. In: Proceeding of the 4th Asian International Conference on Mobile Computing, pp. 152–156 (2006)
16. Sadhukhan, P., Sen, R., Chatterjee, N., Das, A., Das, P.K.: A middleware-based approach to mobile web services. In: Proceeding of the Fifth Asian International Mobile Computing Conference (AMOC'07), 3–6 Jan 2007, Kolkata, India, pp. 167–175
17. Sadhukhan, P., Chatterjee, N., Das, A., Das, P.K.: A scalable location-based services infrastructure combining GPS and bluetooth based positioning for providing services in ubiquitous

environment. In: Proceedings of Fourth IEEE International Conference on Internet Multimedia Systems Architecture and Application (IMSAA-10), 15–17 Dec 2010, Bangalore, India, pp. 93–98
18. Das, S., Sadhukhan, P.: Performance evaluation of a LBS system delivering location-based services using wireless local area network. In: Proceedings of IEEE International Conference on 2014 Applications and Innovations in Mobile Computing (AIMOC'14), 27 Feb–1 Mar 2014, Kolkata, India, pp. 85–90
19. Sadhukhan, P., Sen, R., Das, P.K.: A middleware based approach to dynamically deploy location based services onto heterogeneous mobile devices using Bluetooth in indoor environment. In: Chang, C.C., Vasilakos, T., Das, P., Kim, T., Kang, B.H., Khurram Khan, M. (eds.) Advanced Communication and Networking. ACN 2010. Communications in Computer and Information Science, vol. 77, pp. 9–22. Springer, Berlin, Heidelberg (2010)
20. Sadhukhan, P., Das, P.K.: MGALE: a modified geometry-assisted location estimation algorithm reducing location estimation error in 2D case under NLOS environments. In: Fuller, R., Koutsoukos, X.D. (eds.) Mobile Entity Localization and Tracking in GPS-less Environments. MELT 2009. Lecture Notes in Computer Science, vol. 5801, pp. 1–18. Springer, Berlin, Heidelberg (2009)
21. Sadhukhan, P., Das, P.K., Saha, S.: Hybrid mobility management schemes integrating mobile IP and SIP for seamless invocation of services in all-IP network. Telecommun. Syst. **52**(4), 2027–2046 (2013)
22. Want, R., Hopper, A., Falcão, V., Gibbons, J.: The active badge location system. ACM Trans. Inf. Syst. **10**(1), 91–102 (1992)
23. Hightower, J., Vakili, C., Borriello, C., Want, R.: Design and calibration of the SpotON AD-Hoc location sensing system. UW CSE 01-08-?? University of Washington, Seattle, WA (2001)
24. Bahl, P., Padmanabhan, V.N.: Radar: an in-building RF-based user location and tracking system. In: Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings INFOCOM 2000, vol. 2, pp. 775–784 (2000)
25. Lu X., Jin G., Park M.: An indoor localization mechanism using active RFID Tag. In: Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 5–7 June 2006
26. Ohta Y., Sugano M., Kawazoe T., Murata M.: Indoor localization system using RSSI measurement of wireless sensor network based on zigbee standard. In: Proceedings of Wireless Sensor Network (2006)
27. Priyantha, N.B., Chakraborty, A., Balakrishnan, H.: The cricket location-support system. In: Proceeding of MOBICOM 2000, ACM Press, Boston, MA, pp. 32–43 (2000)
28. http://newsroom.cisco.com/dlls/partners/news/2006/prprod05-02.htmls
29. Di Flora, C., Hermersdorf, M.: A practical implementation of indoor location-based services using simple Wi-Fi positioning. J. Locat. Based Serv. **2**(2), 87–111 (2008)
30. Castro, P., Chiu, P., Kremenek, T., Muntz, R.: A probabilistic room location service for wireless networked environments. In: Proceedings of UbiComp 2001, LNCS, vol. 2201, pp. 18–34. Springer, Heidelberg (2001)
31. Banerjee, S., Agarwal, S., Kamel, K., Kochut, A., Kommareddy, C., Nadeem, T., Thakkar, P., Trinh, B., Youssef, A., Youssef, M., Larsen, R.L., Udaya Shankar, A., Agrawala, A.: Rover: scalable location-aware computing. J. IEEE Comput. **35**(10), 46–53 (2002)
32. Johansson, P., Kapoor, R., Kazantzidis, M., Gerla, M.: Personal area networks: Bluetooth or IEEE 802.11? Int. J. Wireless Inf. Networks. **9**(2), 89–103 (2002)
33. Cano, J.-C., Manzoni, P., Toh, C.K.: Ubiqmuseum: a Bluetooth and Java based context-aware system for ubiquitous computing. In: Wireless Personal Communications, vol. 38, pp. 187–202, Springer (2006)
34. Subramanian, S.P., Sommer, J., Schmitt, S., Rosenstiel, W.: SBIL: scalable indoor localization and navigation service. In: Proceedings of Third International Conference on Wireless Communications and Sensor Networks (WCSN), pp. 27–30 (2007)
35. JABWT: Java APIs for Bluetooth. http://www.jcp.org/en/jsr/detail?id=82

36. An, X., Wang, J., Venkatesha Prasad, R., Neimegeers, I.G.M.M.: OPT: online personal tracking system for context-awareness in wireless personal network. In: Proceedings of the 2nd international workshop on Multi-hop ad hoc networks: from theory to reality (REALMAN'06), pp. 119–121, ACM (2006)
37. Zafeirropoulos, A., Papaioannou, I., Solidikis, E., Konstantinou, N., Stathopoulos, P., Mitrou, N.: Exploiting Bluetooth for deploying indoor LBS over localization infrastructure independent architecture. Int. J. Comput. Aided Eng. Technol. **2**(2), 145–163 (2010)
38. Yu, C., Lan, H., Gu, F., Yu, F., El-Sheimy, N.: A Map/INS/Wi-Fi integrated system for indoor location-based service applications. Sensors. **17**, 1272 (2017). https://doi.org/10.3390/s17061272
39. Bayir, M.A., Demirbas, M., Cosar, A.: Track me! a web-based location tracking and analysis system for smart phone users. In: Proceedings of 24th International Symposium on Computer and Information Sciences (ISCIS 2009), pp. 117–122 (2009)
40. Michael, K., Mcnamee, A., Michael, M.G., Tootell, H.: Location-based intelligence-modeling behavior in humans using GPS. In: The Proceedings of IEEE International Symposium on Technology and Society, Queens, NY, pp. 1–8 (2006)
41. Steinfield, C.: The development of location based services in mobile commerce. In: Elife After the dot.com Bust. Springer, Berlin
42. He, L., Deng, Z., Huang, J.: Location based services combined with GPS and 3G wireless networks. In: Proceedings of IEEE International Conference on Service Operations and Logistics, and Informatics, vol. 1, pp. 542–545 (2008)
43. Deblauwe, N., Ruppel, P.: Combining GPS and GSM Cell-ID positioning for Proactive Location-based Services. In: Proceedings of Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous 2007), pp. 1–7 (2007)
44. Rao, K., Jhorman, P., Raju, P.L.N.: Application of mobile mapping and location based services for Dehradun Health Services K. Mob. Comput., 2(2) (2013)
45. Spanoudakis, M., Batistakis, A., Priggouris, I., Ioannidis, A., Hadjiefthymiades, S., Merakos, L.: Extensible platform for location based services provisioning. In: Proceeding of Fourth International Conference on Web Information Systems Engineering Workshops, pp. 1–8 (2003)
46. Savidis, A., Zidianakis, M., Kazepis, N., Dubulakis, S., Graminos, D., Stephanidis, C.: An integrated platform for management of mobile location-aware information systems. In: Proceedings of 6th International Conference on Pervasive Computing, Sydney, Australia, 19–22 May 2008, LNCS, vol. 5013, pp. 128–145
47. Xia, Y., Bae, H.Y.: General platform of location based services in ubiquitous environment. In: Proceedings of IEEE International Conference on Multimedia and Ubiquitous Engineering (MUE 2007), pp. 791–795 (2007)
48. Fang, L., Xialei, L., Fuling, B.: A framework for autonomous LBS in wireless pervasive computing environments. In: Proceedings of the 9th International Conference on Advanced Communication Technology, vol. 3, pp. 1715–1720 (2007)
49. Martin, S., Cristobal, E.S., Gil, R., Castro, M., Diaz, G., Peire, J.: A context-aware application based on ubiquitous location. In: Proceedings of Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM 2008), pp. 83–88 (2008)
50. Steele, R., Khankan, K., Dillon, T.: Mobile web services discovery and invocation through auto-generation of abstract multimodal interface. In: Proceeding of Third International Conference on Information Technology: Coding and Computing (ITCC'05), vol. 2, pp. 35–41 (2005)
51. Park, G.C., Kim, S.S., Bae, B.T., Kim, Y.S., Kang, B.H.: An automated WSDL generation and enhanced SOAP message processing system for mobile web services. In: Proceedings of the Third International Conference on Information Technology New Generations (ITNG'06), IEEE (2006)
52. SOAP. http://www.w3.org/TR/soap/
53. Aalto, L., Nicklas, G., Korhonen, J., Ojala, T.: Bluetooth and WAP push based location-aware mobile advertising system. In: Proceedings of Second International Conference on Mobile

Systems, Applications and Services, Boston, MA, pp. 49–58 (2004)
54. Martin-Escalona, I., Barcelo-Arroyo, F.: QoS-driven middleware for optimum provisioning of location based services. In: Proceedings of Second IEEE International Conference on Communication Systems Software and Middleware, 7–12 Jan 2007, Bangalore, India, pp. 1–6
55. Retscher, Günther. "Pedestrian navigation systems and location-based services. IET Digital Library, pp. 359–363 (2004)
56. Hansen, R., Wind, R., Jensen, C.S., Thomson, B.: Seamless indoor/outdoor positioning handover for location-based services in streams pin. In: Proceedings of the 10th IEEE International Conference on Mobile Data Management: Systems, Services and Middleware, pp. 267–272 (2009)
57. Hodes, T.D., Katz, R.H.: Composable ad hoc location-based services for heterogeneous mobile clients. Wirel. Netw. **5**, 411–427 (1999)
58. Huang, H., Gartner, G., Krispc, J.M., Raubald, M., Weghe, N.V.: Location based services: ongoing evolution and research agenda. J. Locat. Based Serv. **12**(2), 63–93 (2018). https://doi.org/10.1080/17489725.2018.1508763
59. Mandal, R., Agarwal, N., Das, P., Pathak, S., Rathi, H., Nandi, S., Saha, S.: A system for stoppage pattern extraction from public bus GPS traces in developing regions. In: Proceedings of the Third ACM SIGSPATIAL International Workshop on Mobile Geographic Information Systems, pp. 72–75 (2014)
60. Li, Y., Wang, J., Zhang, L.: LBS-based dilemma zone warning system at signalized intersection. In: Gartner, G., Huang, H. (eds.) Progress in Location-Based Services 2014, pp. 223–237. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-11879-6_16
61. Pal, M.K., Debabhuti, N., Sadhukhan, P., Sharma, P.: A novel real-time collision avoidance system for on-road vehicles. In: 2018 Fourth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Kolkata, India, 22–23 Nov 2018, pp. 141–146. https://doi.org/10.1109/ICRCICN.2018.8718724
62. Sadhukhan, P., Talukder, A.: Automated real-time parking management for smart cities. In: Kundu, S., et al. (eds.) Proceedings of the 2nd International Conference on Communication, Devices and Computing, Lecture Notes in Electrical Engineering 602, pp. 655–667. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-0829-5_61
63. Gao, S., Janowicz, K., Couclelis, H.: Extracting urban functional regions from points of interest and human activities on location-based social networks. Trans. GIS. **21**(3), 446–467 (2017). https://doi.org/10.1111/tgis.2017.21.issue-3
64. Horta, E.T., Lopes, I.C., Rodrigues, J.J.P.C.: Ubiquitous MHealth approach for biofeedback monitoring with falls detection techniques and falls prevention methodologies. In: Adibi, S. (ed.) Mobile Health. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-12817-7_3
65. Herrera, E.P.: Location-based technologies for supporting elderly pedestrian in 'getting lost' events. Disabil. Rehabil. Assist. Technol. **12**(4), 315–323. https://doi.org/10.1080/17483107.2016.1181799
66. Forum, G.: 5G New Wave—towards future societies in the 2020S. Future-Networks-2020-InDesign-PDF.pdf (5gamericas.org).
67. Witrisal, K., Meissner, P., Leitinger, E., Shen, Y., Gustafson, C., Tufvesson, F., Haneda, K., Dardari, D., Molisch, A., Conti, A., Win, M.Z.: High-accuracy localization for assisted living: 5G systems will turn multipath channels from foe to friend. IEEE Signal Process. Mag. **33**(2), 59–70 (2016)
68. Wymeersch, H., Seco-Granados, G., Destino, G., Dardari, D., Tufvesson, F.: 5G mmWave positioning for vehicular networks. IEEE Wirel. Commun. **24**(6), 80–86 (2017). https://doi.org/10.1109/MWC.2017.1600374
69. He, S., Chan, S.-G.: Wi-Fi fingerprint-based indoor positioning: recent advances and comparisons. IEEE Commun. Surveys Tutorials. **18**(1), 466–490 (2016)
70. Sadhukhan, P.: Performance analysis of clustering-based fingerprinting localization systems. Wirel. Netw. **25**(5), 2497–2510 (2019)

Proximity Based Social Networking in Urban Environments: Applications, Architectures and Frameworks

Asslinah Mocktoolah Ramtohul and Kavi Kumar Khedo

1 Introduction

An impressive growth of online social networking (OSN) is observed during the recent years and has flourished as never before in human history. On the other side of the world of technology, smart phones have been noted to be another success story in this new era. According to eMarketer [1], 1.75 billion people own a smart phone. This significant penetration of smart phones, together with the rapid emergence of social networking resulted in new consumer behavior and expectations. Large web online social networking sites ~~have~~ adapted to this new transition and social networking was stretched to mobile phones known as Mobile Social Networking (MSN) [2]. Popular online social networking sites such as Facebook and Twitter were not left behind and mobile applications have been introduced for their users [3, 59]. An important field of application of MSN has been highlighted by Kayastha et al. [4] known as Proximity-based social networking. These services take advantages of the additional features of smart phones such as the GPS and Wi-Fi to discover friends around or make new connections with physical proximate mobile users [5].

Proximity-based social networking (PBSN) refers to the social interaction of mobile users which takes into consideration location information primarily using geo-proximity as a main filter to determine who is discoverable on the network. The main activity on these networks known as "check-in", allows the users to share their real and current geographical location automatically in their posts. While studies has emphasized on how people are becoming more and more anti-social by using online social networking services and face-to-face interactions are decreasing [6], PBSN

A. M. Ramtohul (✉) · K. K. Khedo
Faculty of Information, Communication and Digital Technologies, University of Mauritius, Le Réduit, Mauritius
e-mail: k.khedo@uom.ac.mu

S. Paiva (ed.), *Precision Positioning with Commercial Smartphones in Urban Environments*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-71288-4_4

on the other side changes this perception of social networking. Cranshaw et al. [7] and Zhang et al. [8] endorse this fact by stating that PBSN as compared to OSN enables tangible personal social interactions blurring the distinction between online and offline social networks while OSN contributes to the isolation of people in the physical world. These statements illustrate that internet communication no longer has a negative impact on individuals as PBSN allows physical communications therefore decreasing level of loneliness.

PBSN services are practical to users allowing them to meet up with their friends in the surroundings or initiate new friendships with people around having similar attributes [9]. These networks have helped users to select restaurants or stores which have good reviews from friends. Therefore, this shows that PBSN is not only useful to users but it is equally important to promote businesses. Moreover, PBSN enable users to select routes based on the traffic information and set reminders at a specific place, for example, when a user reaches a grocery store, a reminder can be set so that the user remembers what he is supposed to buy based on his location.

1.1 Overview of Proximity Based Social Networking (PBSN)

The emergence of new technologies such as GPS, Bluetooth, Wi-Fi and broadband cellular networks has nurtured a new trend in social networking by offering location-based or proximity-based services to users. Proximity based services can be classified according to their functionalities and depending on how location information is being used. Three main types of location based services have been identified in existing literatures namely position awareness, location tracking and sporadic queries.

1. Position awareness also known as triggered PBSN services or simply push services, allow the location discovery of users, e.g. users can receive notifications about events taking place in their surroundings based on their current locations [10].
2. Location tracking applications, on the other side, track the locations of users using a GPS-enabled device by continuously pinpointing to the coordinates (longitude and latitude) and deriving the course direction of the users [11, 12].
3. Sporadic queries refer to services in which the user initiates the transfer of his location information to a service provider, e.g. a user can request the PBSN application to search for nearby hotels or restaurants based on his interests such as food tastes [13].

Generally, different components of the PBSN system work together and communicate with each other to offer the numerous services to mobile users. The main components of a PBSN system are the network infrastructure, service and application provider, data and content provider, positioning technology and mobile devices as illustrated in Fig. 1.

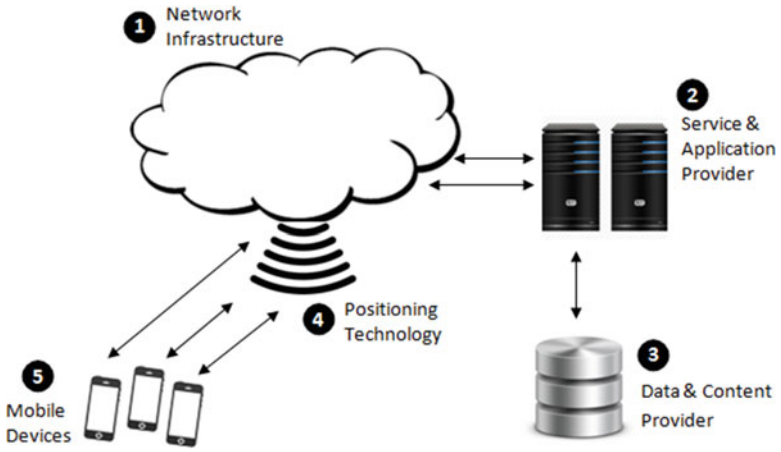


Fig. 1 PBSN components

1. **Network Infrastructure**
   The network infrastructure of a PBSN system refers to a wireless network using technologies such as Bluetooth, Wi-Fi or cellular networks to allow transfer of data between the service provider and the mobile users [4].
2. **Service and Application Provider**
   The service and application provider acts as a middleware between the data and content provider and the network infrastructure [14]. It will take the requests from clients through the wireless network and fetches the geographic information from the data content provider.
3. **Data and Content Provider**
   The content provider takes requests from clients, then processes and delivers the data to the users since service providers will not usually retain all information requested by users [15].
4. **Positioning Technology**
   The positioning feature provides the core services of PBSN system allowing the localization of mobile devices in the network by using different techniques such as GPS localization.
5. **User's Mobile Device**
   Any portable devices equip with proper communication technologies that allow reception of data from content providers and allow transfer of data to other users in the network.

1.2 Chapter Plan

In this chapter, a meticulous introduction to PBSN is presented outlining the different main components. The remainder of the study is organized as follows. In Sect. 2, the real-world PBSN application Foursquare is presented. Section 3 outlines an extensive categorization of the PBSN applications followed by a discussion of evaluation criteria used to measure PBSN systems in Sect. 4. Innovative PBSN applications in Urban Environments is presented in Sect. 5. Section 6 focuses on the different research challenges of PBSN before the concluding remarks in Sect. 5.

2 A PBSN Application: Foursquare City Guide

Foursquare City Guide, commonly known as Foursquare, is one of the most popular PBSN application, with more than 50 million monthly active users and around 105 million venues around the world have been mapped on the application [16]. Users check-in to a place on Foursquare when they are located there physically and inform other users in the network about their locations. Users are further encouraged to check-in at different places, by providing an innovative game-like service where the users are awarded for multiple check-ins by receiving points or badges. The user with the most number of check-ins at a particular place becomes the mayor of that place and may receive virtual and tangible rewards such as vouchers or free drinks. Foursquare adopted its own location detection technology: Pilgrim by using GPS and users' past check-in histories [17]. The Pilgrim technology refers to a decision-making engine, which determines the next destination of a user, where a user usually stops to hang out or the places he might be interested. It also recognizes when a user arrives in a new city and provides location recommendations of restaurants, bars or other places of interests.

2.1 Features of Foursquare

The main features of Foursquare relate to Check-ins, Tips, To-Dos, Things Done, Gaming and Venue Categorization as illustrated in Fig. 2. Check-ins are carried out in physical locations known as venues by the Foursquare users to share their locations. Users may also post tips about any venues to share information concerning any aspect positively or negatively, for example posting a good review on a specific meal in a restaurant or complaining about the service. Tips are also used to provide suggestions about the possible activities of that venue. The To-Do List feature allows the user to keep a list of the interesting places he may want to visit while the Things Done mark the items as done. Foursquare additionally employs gaming elements such as points, badges or mayorships to further attract users and to motivate them to use the check-in service at their most. A set of

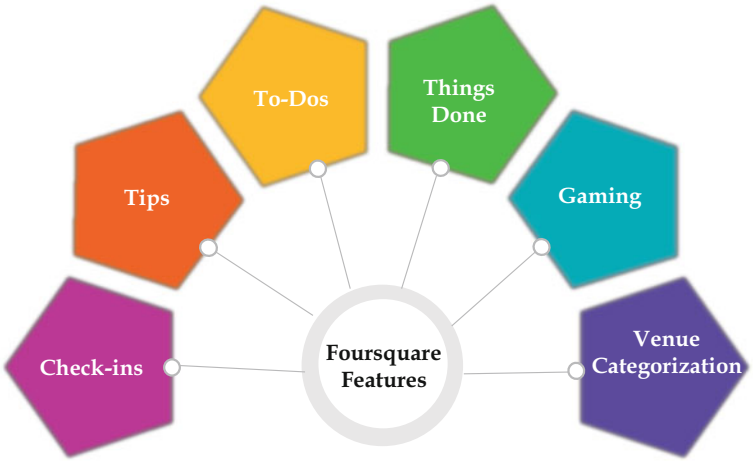


Fig. 2 Foursquare features

venue categories is maintained by Foursquare which allows users to search any locations according to their interests. The eight pre-defined venue categories are Arts & Entertainment, Colleges & Universities, Food, Great Outdoors, Nightlife Spots, Travel Spots, Shops, Home, Work and Others.

2.2 Foursquare Architecture

Foursquare relies on a client-server architecture and stores all the locations of the users in its database even if the users do not manually check-in to a particular location. The GPS in their mobile devices enable Foursquare to record their location histories. Based on this data, Foursquare cross-check which other users in the network that are located in the same place or in nearby locations. Suggestions can be sent to the proximity users to connect based on their tracked locations by Foursquare. As reported by Chen [18], the architecture of Foursquare comprises of five components as depicted in Fig. 3.

The Foursquare App refers to the client application on the mobile device of the user. The Foursquare App Server is the main component, which provides all the interfaces needed by the client server including the check-in service and third party applications. The Data Server allows the data storage using MongoDB and PostgreSQL while the Foursquare Offline Data Analysis system supports the data analysis and statistics of the users' check-in data. The Foursquare App Server, Data Server and the Offline Data Analysis system are deployed on Amazon Elastic Compute Cloud (Amazon EC2). On the other side, the map service provider used by Foursquare is Google maps, which allows the map contents to be visible on the Foursquare applications.

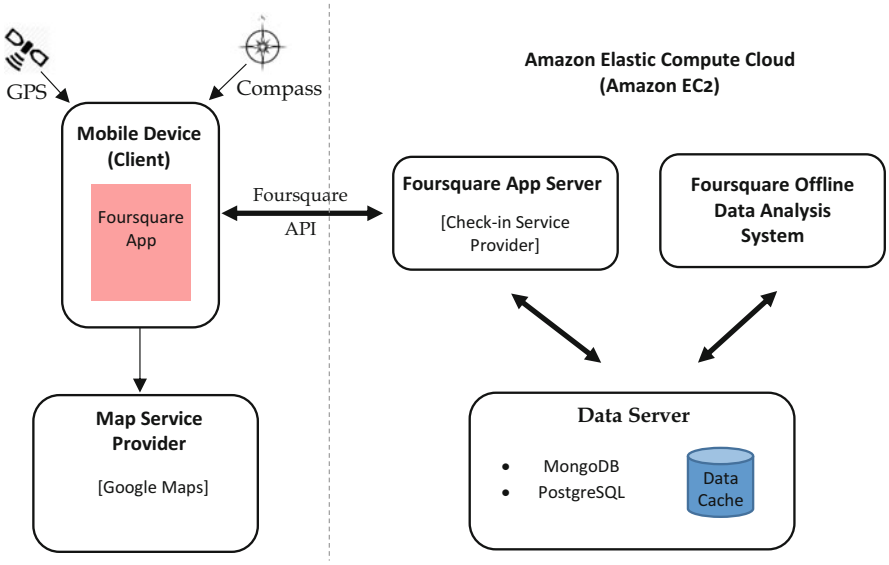


Fig. 3 The Foursquare architecture (Adapted from [18])

2.3 Uses of Foursquare

Other than sharing locations with Foursquare by check-in to different venues, Foursquare allows users to meet up with their friends or simply to find out where their friends are hanging out. Many users employ Foursquare as an entertainment purpose to win points, badges by checking-in and ultimately being the mayor of a particular venue by having the most number of check-ins in that location. Business also makes use of Foursquare to improve their services by working on the tips provided by their customers. Additionally, tips are exploited by the business, who are also Foursquare users, to promote any products or brands. It has also been noted that Foursquare can be used as an important feature in urban computing to carry out different research studies. For instance, the user activities in urban environments can be inferred by using the check-ins of the users in Foursquare [19]. Similarly, the popularity of locations in cities can be inferred from the analyzed Foursquare data and the users' movement pattern in the city streets can also be observed [20]. A recent study by Quercia and Saez [21] showed that location data from the Foursquare application can be used for crowdsourcing the land use of urban environments. With these data, the physical changes in a neighborhood is possible which can help to monitor the socio-economic deprivation of that neighborhood.

3 Categorization of PBSN Applications

Different types of mobile applications have emerged during the recent years helping people to locate each other and based on the location of users as a primary feature, different services are offered to them. Several attempts have been made in the past to give an overview of the different categories of PBSN applications. In light of the rapid adoption of smartphones and social media over the past years, new categories of PBSN applications have emerged providing users with more services. Hence, in this research, a new model of categorization has been derived based on four different criteria namely location, object, purpose and trajectory. Figure 4 illustrates the categorization proposed in this study:

The description of the categorization model is illustrated in Table 1 outlining the four categories:

The below sections give a detailed overview of the four categories of PBSN applications. For each category, around three sub-classes have been defined according to their application areas.

3.1 Categorization by Locations (Where)

In this category of PBSN applications, the responses of the applications are based on the changes of locations. The location information can be retrieved directly from the applications on a mobile device if location services are turned on, e.g. Location Services in iPhone allow some applications such as Maps and Camera to determine the user's location automatically using cellular data, Wi-Fi, GPS and Bluetooth [22]. The Where class of PBSN can be further be classified into several sub-classes as below:

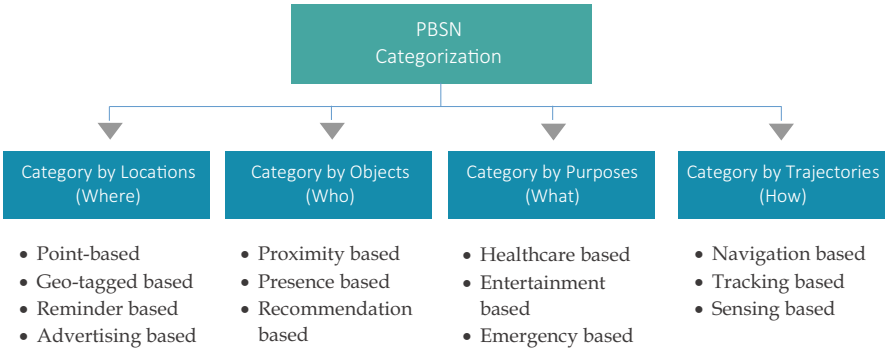


Fig. 4 PBSN categorization

Table 1 Description of categorization model of PBSN applications

Categories	Description	Example
Categorization by locations (where)	This category refers to applications where the location of users is the basis under which services are proposed to users	Check-in at a place
Categorization by objects (who)	It revolves around mostly the people in question such as discovery and recommendation algorithms which are integrated in PBSN applications to give further services to users in proximity	Friend finder applications
Categorization by purposes (what)	This category offers services in different application areas such as in health care, entertainment and emergency by taking into account the user's locations	Health care applications or location-based games
Categorization by trajectories (how)	This type of application refers to the different locations of a user in motion providing services	Road guide, tracking or fleet asset management

3.1.1 Point-Location Based

In this category, users can share their location using check-in posts allowing their friends to know where they are. Checking-in as outlined by Gao et al. [23] refers to an online activity which reveals the user's location with the help of social media acting as an interaction between the user and the real world. Facebook Places and Swarm (originated from Foursquare), categorized as point-location based applications, allow users to share their locations by checking-in to a particular place [24, 25].

3.1.2 Geo-Tagged Based

Bao et al. [26] introduced geo tagging services facilitating users to add a location label to different media contents such as text, photos or videos. For example in Facebook, if location services are enabled on a smartphone, the location is automatically shared when the user posts a status, clicks a picture or records a video and shares it on the timeline. Users can then view all the places they visited where photos were taken on a digital map. The same scenario applies for photo-sharing OSN Flickr [27] where photos uploaded from mobile phones having geographical data can be displayed on a map according to the location the pictures were taken. Color [28], a similar PBSN application, allows creation of photo and video albums with users located within 150 ft at social events such as parties or weddings.

3.1.3 Reminder Based

The services provided by this class of PBSN correspond to leaving self-reminders or notifications for friends at specific locations and when users are identified at the specific places, in other words, push notifications are sent by the applications installed on their mobile devices based on their locations. Some uses of such applications as outlined by Puttaswamy and Zhao [9] may correspond to leaving reminders for different events such as an updated location or time of a party, sending a shopping list when the user, his friends or family are near a grocery store. In addition, these applications can be also helpful when users want to keep a track of their running habits by setting reminders at specific points of their running tracks. Some applications such as Geobells are configurable such that notifications can be set either when arriving at a place or else whilst exiting [29]. The reminders can be viewed on a map and then swiped off once completed.

3.1.4 Advertising Based

Location-based advertising (LBA) applications correspond to adverts reaching customers directly when they are close to the advertisers' locations notifying users of the different sales going on or more interestingly on the new products based on the user's earlier collected tastes [30]. Early LBA applications, known as SMS-oriented, correspond to users receiving SMS adverts based on their locations suggesting them to visit a nearby local store or restaurant [31]. LBA services can be push-based where advertisements are sent based on the known vicinity of the users or pull-based LBA referred to as on-demand services. Customers make a request to receive some information and ultimately, they receive commercial messages, for example, finding the closest ATM machine [32].

3.2 Categorization by Objects (Who)

This category takes into consideration the responses based on the proximity changes of the objects, where in PBSN, the objects refer to the users. The below sections illustrate how these applications collect information from individual users and provide services such as discovery and facilitate interactions of groups of people in proximity.

3.2.1 Proximity Based

Proximity based applications use geo-proximity as a principal filter to determine users who are discoverable in the social network and enable physically proximate travelling users to interact with each other through their mobile devices.

Crocker [33] further identified three stages for connecting to this type of network namely the proximity network, where the nearby anonymous users can only be discovered, the elastic network and finally the social network. In the elastic network stage, users can interact with other people in the proximity network and build relationships with them without sharing too much information. Once a trust has been built, they enter the final stage, the social network, where the user's details are revealed, and stronger relationships are built. Yu and Han [34] focused on discovering groups of people who are most likely to share information by applying the CPMd algorithm for detecting the communities, for example Proxxi [35].

3.2.2 Presence-Based

Presence-based social networks applications focus on connecting users present in a certain place for a definite period of time such as a concert, wedding or sport event [33]. Users can discover each other within the time span they are in the proximity network and also have the choice to continue their friendship even afterwards. LoKast [36], short for "local-casting", is an example of such type of PBSN application and allows users to connect with group mediums starting around specific activities or events and then discover other users. They can then communicate with each other, share photos and videos thus enjoying their experiences around activities and events using their smartphones or other mobile devices. This type of PBSN application can be greatly used in business meetings to share useful information or reactions to live events happening.

3.2.3 Recommendation Based

Friend-finder applications help users to make new friendships but only if those users are in the same location or in nearby surroundings [33]. The recommended friends are based mostly by what they shared on their profiles and based on a matching algorithm these new relations are created. However, Burcea and Jacobsen [37] presented another view of such application where a user being notified when a member of his family or a friend is located in the surroundings. This algorithm is such that each user has a unique identifier MIN (Mobile Identification Number) associated with his mobile phone and if a user subscribes to the service, a corresponding location constraint such as MIN_1 or MIN_2 is created. Therefore, when two users are found in the same locality, the location constraint will be matched and thus notifications will be sent to each user.

3.3 Categorization by Purpose (What)

This categorization refers to what types of services that can be offered to users by using their location information where the responses are based on the purposes of the applications. These types of applications are designed for specific application areas such as healthcare, entertainment and emergency as detailed in the sections below.

3.3.1 Healthcare Based

Online social networking sites such as Facebook and Yelp are a common platform used for sharing health problems and seek health advices [38]. This was confirmed by a study carried out by Scanfeld et al. [39] who considered social networking sites such as Twitter as a medium for the informal sharing of health information and advices. However, Boulos [40] outlined that the users' needs are related to where they are and location information should be taken into consideration when advices about health information are given. CAALYX [41] is a user health monitoring platform which is used to closely monitor the health of elder people and try to help them in when they are in need. The autonomy and self-confidence of these people is increased by wearing a light device which can measure the vital signs, detect their falls and communicate in real time with their care provider in case of an emergency. A future work of CAALYX is to develop a geo-reminder system, which can help Alzheimer's patients with their short memory problems.

3.3.2 Entertainment Based

Entertainment features are usually embedded in popular PBSN applications such as Foursquare where there are virtual and tangible rewards when users check in. Points, badges or even mayorships can be won as virtual rewards for the check-ins recorded. When a user has the maximum number of check-ins at a particular venue for a certain period of time, the user becomes the Mayor of that location. Tangible rewards will correspond to some discounts at a coffee shop or free drinks or snacks at restaurants for users having significant number of points or for the mayor of that place [42].

Mobile Location Based Gaming (MLBG) is another growing trend among location-based services linking different games with new technologies such as GPS, Bluetooth, Wi-Fi and image recognition on smartphones [15] thus further bridging the gap between the physical and digital world. Sensors are used in the games applications to capture information about the gamers' current context and also their location which is used to deliver a gaming experience which changes according to their position, to what they are doing or even feeling. BotFighters [43] and PokemonGo [44] are popular location based gaming applications where the

locations of the gamers are used to provide interesting features in the games such as finding objects in the real world with reference to photos uploaded or locating friends using positioning techniques [45]. It is also known that Angry Birds will also include location-based features in the near future where locations such as coffee shops, bars, etc. will convert into playing grounds and players can compete with one another on a unique leader board tied to each location [46].

3.3.3 Emergency Based

Location information can be integrated into emergency-based applications to assist them in difficult situations. Twitter was used as an emergency service by De Longueville et al. [47] by analyzing the spatio-temporal dynamics of tweets activities during a major forest fire event in France in July 2009. The authors argued that the information gathered for this incident can support emergency planning, risk assessment and damage assessment activities in the future. Gomide et al. [48] analysed how the Dengue epidemic spreading in Brazil from 2009 to 2011 was reflected on Twitter, in other words, the tweets of users referring to Dengue were evaluated taking into consideration both time and location dimensions. They asserted the fact that Twitter can be used to predict Dengue epidemics spatially and temporally by means of clustering. Help me [49] is a specialized emergency GPS application based on location services where users can seek help from nearby smartphone users in crisis situations when there is no Internet connection.

3.4 Categorization by Trajectories (How)

In this category, the responses are based not only on the current locations but also the previous and future ones so as to offer users better services based on their routes. The below sub-classes give a better idea about these services.

3.4.1 Navigation Based

New interactive applications for social navigation have been emerged with the rising trend of embedded technologies such as GPS navigation and broadband internet access on mobile devices. Social Navigation Network [50], a framework for PBSN focusing on navigation where not only recommendations on where to go are given but also on how to get at a particular place. Users can mark locations on a map suggesting them two types of routes: walking or driving. On top of that, using the marked locations, users can indicate recommendations for not only locations to go, but also locations not to go by giving different ranks to locations. Onstar [51], an automatic vehicle location service, use the vehicle's GPS receivers together with the mapping guide to offer services in selected cars. Directions or other types of

assistance can be asked to a live OnStar representative by pressing the Onstar built-in button in the GM vehicle and if the vehicle is involved in an accident, the latter immediately contacts the driver to determine the help needed and then summons local emergency services as required.

Gaonkar et al. [52] introduced an alert-based location application to help and guide lost users. Since, internet maps will not help much in small areas such as a university camp, these location-aware alerts can help by enabling the user to view the pre-recorded walking directions from his current position to the desired location to find the way to their destination, for example their classroom.

3.4.2 Tracking Based

Popular applications such as Facebook, Twitter, Google and Foursquare use passive location tracking mainly for data mining purposes so as to improve their services [53] e.g. Google is known to track daily movements of users on a map to improve its search results. Many commercial applications such as Geofency [54] and Placeme [55] monitor the users' daily activities such as working hours, client visits, etc. Placeme allows a calendar view where a history of the locations visited can be viewed and notes can be added to each location. These tracking services can also be used to help preventing thefts of valuable items and to locate people such as lost children or pets. Some trucking companies used such applications to locate their trucks and in addition, to check the contents inside delivery trucks using an onboard wireless LAN. They claim that efficiency and customer service can be enhanced by making last minute delivery changes, which are based on truck invention and location. Route optimization for deliveries can be further improved by combining tracking with navigation services.

3.4.3 Sensing Based

Mobile location sensing allows not only collection of users' information but can provide location based services such as recognizing different activities of the users such as walking, running or driving or classifying several sounds associated with a particular context or activity such as using an ATM machine or being in a particular coffee shop [56]. Furthermore, combining the accelerometer data and location details from the GPS, the application can recognize the mode of transportation of a user, such as using a bike or car or taking a bus or the subway.

Personal sensing systems such as CenceMe [57] allows to predict the user's behavior including sitting, standing, using mobile phone, running, climbing, etc. by making use of human activity algorithms. The sensing presence can be added into online social networking applications such as Facebook, MySpace and IM such as Skype allowing for new levels of connections and implicit communication between friends in these networks. In addition, the CenceMe system also provides users with health related services by estimating the exposure to ultraviolet light and noise and

the number of steps taken to calculate distance travelled and number of calories burned. CitySense [58] relies on same protocols but the most popular places are sensed based on the number of check-ins. The popular places are noted on Google maps and thus are identified as the most happening places of the day or night. Over time, the preferences of the user can also be learnt, e.g. where the person likes to go or recommend people with similar tastes or even displays where a user's friends are.

3.5 Discussion

Based on the categorization model presented, Table 2 outlines a summary of the different categories discussed. The main features of each category are defined along with some examples of existing systems in which the features are applied. A short description on how the applications retrieve the locations of the users is also included.

4 PBSN System Evaluation

The efficiency of current PBSN systems has been measured against a set of criteria such as architecture, security and communication protocols. The different evaluation criteria that are used to evaluate PBSN systems are described below.

4.1 Architecture and Framework

There are different types of architectures for PBSN applications such as client-server, distributed, peer-to-peer (P2P) and cloud computing. However, distributed and P2P architectures are mostly used in such systems due to the absence of a fixed Internet connection. In a distributed architecture, servers and clients communicate with each other through a middleware providing and receiving services from each other [74]. A P2P architecture is more appropriate for such systems since the services are mostly intended for mobile users. Each peer may act as a server and a client in the absence of a centralized server and can be a source of information for some peers while at the same time retrieving information from others.

Based on the above-mentioned architectures, several frameworks have been designed and implemented for PBSN applications such as AllJoyn [75], HumHub [76], Elgg [77] and Anahita [78]. These help developers to design and implement such systems easily in which locations of users are automatically retrieved. The developers then have just to customize their applications according to their needs and requirements. Figure 5 presents the architecture of the AllJoyn framework.

Table 2 Categorization of PBSN applications

Categorization	Application areas	Features	Existing systems	Localization
Category by locations (where)	Point-based	– Push notifications are sent to users when they are located at particular places – Users can check-in using their mobile devices having GPS/Wi-Fi/Cellular Networks – Reviews, recommendations and comments from other users are obtained when users check in	– Swarm [25] – Facebook [3] – Twitter Twitter [59]	GPS in smart phones or tablets are used by these applications to retrieve the exact location of users
	Geo-tagged based	– Location label are embedded to media contents such as pictures or videos when posted online – Photos can be viewed on a digital map in the geographic context as created	– C-IMAGE [60] – Flickr [27] – Color Network Computing [28]	The geo tags can be added explicitly by the user or the tagging can occur passively when content is posted
	Reminder based	– Notifications or alerts can be set at a particular place so as when users are located nearby, the application reminds them of the action to be taken – Edge or the radius of the geo-fence can be specified defining how close the user is	– SmartNotify [60] – Task Trigger [61] – Geobells [29]	The app monitors the GPS information collected by the smart phone to trigger the alert when the user arrives at or leaves a destination
	Advertising based	– Advertisements are sent to customers based on their locations – On demand services or pull based allow users to opt for these advertisements	– Messiah [62] – Foursquare [63]	Different types of advertisements are sent to users based on their real-time location such as geo-aware ads, geo-fencing ads and geo-conquesting ads

(continued)

Table 2 (continued)

Categorization	Application areas	Features	Existing systems	Localization
Category by objects (who)	Proximity based	– Use geo-proximity to detect nearby friends – Allows meeting up and chatting with friends in same surroundings	– Foursquare [63] – Proxxi [35]	GPS or Bluetooth of mobile devices cross-check the position of a user with the locations of friends in proximity
	Presence-based	– When attending events such as a concert, business meeting or wedding, users can be in communication with each other through the application as a group – Information, photos and videos can be shared with each other	– iGroups [64] – Lokast [36] – Color [28]	The localization protocol ensures that only the persons within the location range are eligible for the service
	Recommendation-based	– Analyse and discover the social relationships between users in proximity to give location based recommendations – The suggestions are based on different other criteria as well such as interests or friends but focus remains on proximity	– Foursquare [63] – The Scoop [65] – Alike [66]	The profiles of mobile users are compared with other proximate users and recommendations are sent based on their matched profiles
Category by purposes (what)	Healthcare based	– Health advices can be given based on user's locations – Monitors health of patients taking into consideration their locations so as to alert required persons	– Caalyx [41]	The location information is taken into consideration when a user is in trouble and notices are sent to other people so as to locate him and help him
	Entertainment based	– Integrate current location information in gaming services – The exact location of the users is used as a feature in the games	– Geocaching [67] – BotFighters [43] – PokemonGo [44]	GPS of the mobile device tracks the location of the users

	Emergency based	– Can send current address, GPS coordinates and emergency message – This application can be for great help for elder people who live and travel alone	– Help Me [49] – OPLITOP [68] – SANA [69]	Spatio-temporal information of users is taken into consideration for such applications
Category by trajectories (how)	Navigation based	– Locations can be marked on a map to produce routes for users to follow – Telematic services or automatic vehicle location services are part of this categorization of PBSN	– GeoLife [70] – Social Navigation Network [50] – Onstar [51]	The locations are not retrieved at only one place but along routes, therefore a constant trace of the locations is taken
	Tracking based	– Locations of users are constantly retrieved from users even when they are not using the applications – Can be used in asset and fleet management	– PlaceMe [55] – Geofency [54] – PowerSpy [71]	Tracking devices using GPS can be integrated either in the mobile devices or in the vehicles and messages sent to the respective personals
	Sensing based	– Sensing occurs through ubiquitous devices for different activities of users and even for different sounds	– SenseDcity [72] – AndroSensor [73] – CitySense [58]	Different sensors on smartphones, such as accelerometer, digital compass, gyroscope, microphone, and camera are used together with GPS to retrieve locations and activities of users

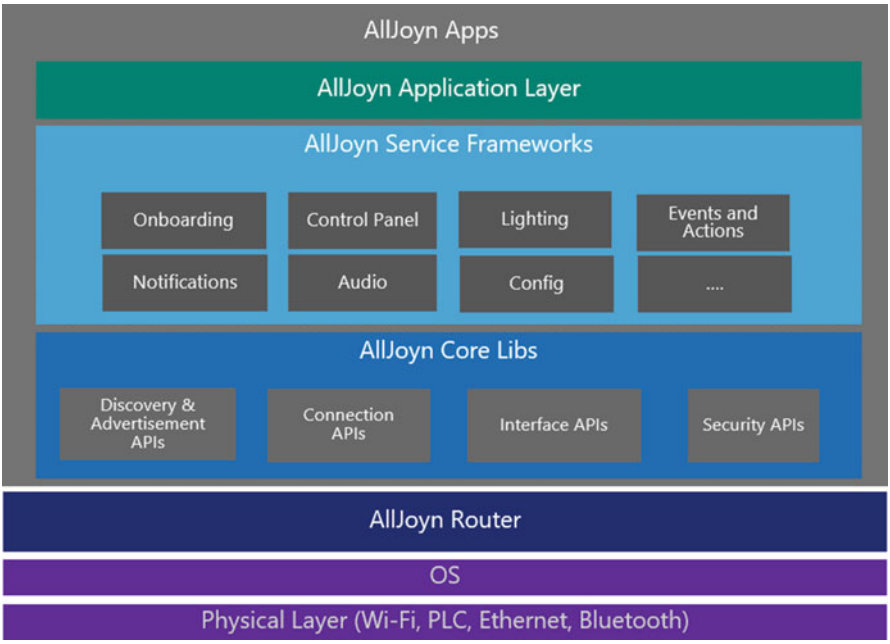


Fig. 5 AllJoyn framework [75]

4.2 Discovery Protocols

The discovery protocol is used firstly to access the users' attributes, then a proximity calculation is carried out based on the users' social coordinates. If the proximity between two users reaches a specific threshold, they can then discover each other. Eagle and Pentland [79] introduced BlueAware, a Mobile Information Device Profile (MIDP) 2.0 application, based on a central server device discovery and profile matching in which Bluetooth is used as the proximity detection protocol. MobiClique [80] is based on the same idea but however does not depend on a centralized server or even infrastructure connectivity but is mainly based on opportunistic connections between devices in proximity. When two mobile users are located near to each other and if their profiles are similar, both users are notified and then they can choose to have an exchange which can be a simple friendship or content distribution over an ad hoc network. The neighborhood discovery procedure depends on the radio technology of the device being used such as Bluetooth device discovery or WiFi SSID.

4.3 Profile Matching

Profile matching refers to the comparison of profiles and based on similar profiles, that is, two or more users having some attributes in common, these matched profiles can be used for recommendation purposes. Different profile matching algorithms were designed for PBSN systems but most of the recent ones focus on offering a secure profile-matching algorithm so that users do not have to compromise on the data shared on their profiles. Zhang et al. [8] proposed a fine-grained private matching protocol which enables finer differentiation among users having different levels of interest for the same attribute. Zhu et al. [81] designed a novel Privacy Preserving and Fairness-aware Friend Matching protocol in which the matching of profiles takes place only if the interests of both participants are common ensuring that no other extra information can be accessed from the protocol except the information that the user reveals.

4.4 Communication Protocols

Popular PBSN applications such as Foursquare rely on trusted cloud services allowing users to share their locations and communicate with each other in proximity. Recently, location based services have switched to Device to Device (D2D) communication using local-range technologies such as Bluetooth, WLAN and infrared known as Near LBS. Systems such as LoKast [36] and AllJoyn [82] also apply D2D communication in their implementations enabling accurate detection of nearby devices. D2D communication not only results in precise nearby devices detection but also enables excellent ad hoc communication and sharing. In ad hoc networks, the distance between devices are used to establish connection with each other and the peer-to-peer relationship based on proximity is used to continuously restructure the network into multiple clusters. In this model of ad hoc mobility, no fixed infrastructure is important to support communication.

4.5 Recommendation Algorithms

Recommender systems are known to be a success in OSN helping users to connect to friends whom they may know or simply connecting to new friends based on similar interests. The two most popular algorithms for recommender systems are content-based filtering and collaborative filtering [83]. While OSN has been concentrating on friend recommendations and tag recommendations only, PBSN considers location recommendations also [84]. Bao et al. [85] presented a location-based and preference-aware recommender system to facilitate the travel of users not only in their surrounding areas but also in a new city. Two models were proposed in

the system: online modeling where the personal preferences are learnt automatically based on the users' location histories and the social opinions and secondly, the offline modeling part where the location histories are extracted. Khalid et al. [86] proposed a novel cloud based recommendation framework which recommends venues at a finer granularity to address several issues such as data sparseness, cold-start and scalability.

4.6 Location Prediction

Location prediction is different from a location recommender system such that location prediction forecasts the next location that the users had been before or based on their location patterns. On the other hand, location recommendation focuses on recommending a new location to the user that the user had never been before. Location prediction can be applied on different applications such as mobile marketing, traffic planning and disaster relief [84]. Mahmud et al. [87] introduced a hierarchical ensemble algorithm using a combination of statistical and heuristics classifications for predicting the home or primary locations of Twitter users by considering their tweets and analyzing their tweet behavior. In addition to predict locations, the framework by Do and Gatica-Perez [88] forecasts also the applications that users will use in the next 10 min by using the contextual information extracted from the sensors of their smartphones. Their framework was based on a generic model comprising of commonly used prediction algorithms such as Least-Square Linear Regression, Logistic Regression, Random Forest, Markov Models and the Blending Model.

4.7 Security and Privacy

There are several threats associated with sharing of personal information online, however, PBSN users are more skeptical to share their locations on these applications as they are present physically and therefore the danger is greater. The users can be stalked, threatened or even sexually assaulted. Many commercial PBSN such as Foursquare, Lokast etc. employed different initiatives to help protect users' privacy by allowing the users to control the sharing of their information, for example by choosing the audience with whom they share their posts. However, it is clearly mentioned in their policies that once information has been shared these are no longer safe and third parties can have access [130].

Different privacy protection schemes have been introduced such as the use of anonymous identifiers or cryptographic keys when users in proximity communicate with each other [89, 90]. The data transferred is protected and can be received by only the persons having the shared keys. Others have adopted location-obfuscating techniques by hiding the exact locations of the users while some employed

encryption methods to protect the personal and location information of users [91]. These security measures allow users to have more trust in the applications and attract a larger number of users.

4.8 Overall Evaluation of PBSN Systems

A list of popular PBSN systems as from year 2005 is compared based on the above-mentioned criteria and details about how these criteria are used in each system are presented outlining the different techniques employed.

Based on the evaluation of the PBSN systems, it is observed that the centralized architecture is not commonly used, instead most of the systems employ the Client-Server and Peer-to-Peer architecture. Most of the PBSN systems makes use of cryptographic schemes to secure the data in the systems while some promote the use of secure identifiers. The most commonly used communication protocol refers to Bluetooth and GPS (Table 3).

5 Innovative PBSN Applications in Urban Environments

Urban environments have employed the implementation of intelligent infrastructure and advanced technologies to improve the services of the cities. Moreover, the vision of smart cities has been influenced by the widespread adoption of smartphones in such a way that GPS data is exploited to provide the citizens modern services. It has been observed that urban environments have adopted PBSN applications to facilitate the daily activities of the citizens or to attract tourists during their journey in the city. The different areas of the innovative popular PBSN applications are described below:

5.1 Collective Sensing Applications

Smartphones are no longer regarded as devices to communicate with each other but provide an extension of the users' personalities and a database of their interests. The embedded sensors in the mobile devices have allowed new advancements by retrieving data about people and their environments. Novel applications have emerged by using these features such that proximity and light sensors can be used to retrieve the context of the users while the accelerometer data can estimate the physical movements of the users [101]. As reported by Li et al. [102], it is possible to determine the activity of a person by continuously collecting audio from the phone's microphone. Furthermore, if the data of the accelerometer and the location estimates are combined, the mode of transport can be deduced [103]. Based on

Table 3 Evaluation of PBSN systems

Existing systems	Security and privacy	Communication protocols	Recommendation algorithms	Profile matching	Location prediction	Discovery protocols	Architecture	Frameworks
Identity Server [90]	Anonymous identifier (AID) using cryptographic hash function SHA-1	Bluetooth AID sharing service	N/A	Anonymous exchange of social networks	N/A	Discovery is based on AID generated	Peer-to-peer architecture	Restlet framework
MobiShare [92]	Two different servers are used to store users' information	Mobile cellular networks (3G/4G)	N/A	Based on profiles and distance of the users	N/A	Based on the public key of user and its threshold distance	Client-server architecture	JoyentCloud and Linode
Facebook Places [3]	Users control the audience to share their posts	Wi-Fi, Cellular Networks, GPS	Based on the check-ins and distance in km	Based on interests and places visited by users	Previous visit patterns	Location is automatically shared if location services are on	Client server	N/A
Foursquare [63]	Information is self-controlled by users	Wi-Fi, Cellular Networks, GPS	Push notifications Reviews or comments	Based on users' tastes and locations visited	Previous pattern visits and distance	Based on users' tastes	Client server	Scala/lift web framework
Place-Its [93]	Computation is done on the client's device	GPS, GSM and Bluetooth radio technologies	N/A	N/A	N/A	Set reminders are generated based on locations	Distributed architecture	Symbian Series 60 platform

EnCore [89]	Unique encounter ID and associated shared key using encryption/authentication codes	Bluetooth	A record of strangers' devices is kept to send recommendations	Based on shared attributes	N/A	Based on known friends, matched profiles or previously encountered devices	Peer-to-peer architecture	SDDR protocol
GeoSocialDB [94]	Privacy aware query processing is provided for recommendation queries	Users communicate by geo-tagged messages	Based on spatial and social preferences	N/A	N/A	Based on range distance	Distributed architecture	GeoSocialDB framework
E-SmallTalker [95]	One-way hashing of Bloom filters	Bluetooth	Based on common topics of users	Exchange of Bloom filters by the Content exchange components	N/A	Using the Bluetooth Service Discovery Protocol (SDP)	Distributed architecture	N/A
BlueAware [79]	No privacy measures employed	Bluetooth	N/A	Different weights are set on attributes	N/A	Using Bluetooth identifier (BTID) and timestamps	Centralised architecture	
OmniSuggest [86]	N/A	GPS	Hyperlink Induced Topic Search (HITS) approach	Using preferred venues	N/A	N/A	Hybrid cloud computing architecture	OmniSuggest

(continued)

Table 3 (continued)

Existing systems	Security and privacy	Communication protocols	Recommendation algorithms	Profile matching	Location prediction	Discovery protocols	Architecture	Frameworks
Bao et al. [85]	N/A	Data collected from Foursquare	Top-k ranked locations based on an offline and online modeling	Using a weighted category hierarchy-WCH	N/A	User's preferences are learned from their location history	Distributed architecture	N/A
Micro-Blog [52]	Users can control their own privacy preferences	Wireless networks such as Wi-Fi, cellular and GPS	N/A	Matching algorithm applied on micro blogs	N/A	Using a persistent TCP session locate users on map	Client Server architecture	Micro-Blog
CenceMe [57]	Users can control their privacy settings	Embedded sensors, Bluetooth, GPS	N/A	N/A	Based on user patterns	Based on previous visits	Threaded architecture	Java Micro Edition (JME)
MobiClique [80]	Entity's authentication support	Bluetooth connectivity	N/A	Syntactic pattern-matching	N/A	Depends on the radio technology used	Distributed architecture	Facebook API
Tribler [96]	Secure identifiers (PermIDs) using elliptic-curve cryptography	File Transfer Protocol (FTP) service	User-item rating matrix and standard collaborative filtering techniques	Using the Peer Similarity Evaluator module	N/A	Controlled by the BitTorrent protocol using Buddycast	Peer-to-peer system	BitTorrent

Existing systems	Security and privacy	Communication protocols	Recommendation algorithms	Profile matching	Location prediction	Discovery protocols	Architecture	Frameworks
Mobilis Group [97]	N/A	eXtensible Messaging and Presence Protocol	Based on current location and group memberships	N/A	N/A	The XMPP Service Discovery extension	Centralized architecture	Mobilis
Road Speak [98]	Asymmetric cryptographic key pair (using PKI)	Using 3G-based cellular over a voice communication system	N/A	Based on time, location and interests	N/A	Based on groups and location	Centralized system	Vehicular Social Networks (VSN)
VENETA [99]	Commutative encryption scheme	Bluetooth	Based on mutual friends	Based on age and gender	N/A	Based on matched friends	Decentralize architecture	Java microedition
Clements et al. [100]	N/A	Geo-tagged photos retrieved from Flickr	Based on preferences of landmarks	Gaussian kernel convolution	Based on travel behavior	N/A	Centralised architecture	Flicker API

the collective sensing features, different classes of applications have been emerged in urban environments such as monitoring real-time traffic including braking and honking [104]. Additionally, the road conditions such as potholes or bumps can also be detected by using the embedded sensors such as accelerometer, microphone and GPS as described by Nericell [105]. Environment pollution monitoring such as EcoSensor is also possible with PBSN applications allowing the monitoring of air pollution through mobile sensors [106] and the NoiseTube project, which is used to monitor noise pollution by using microphones in the mobile phones to measure the noise level in the current location.

5.2 Mobile Guide

PBSN applications can be used as mobile guides in the city streets as a replacement to traditional maps and paper guides. The geo-positioning features of the smartphone in addition to its portability allows the mobile guide PBSN applications to provide real-time information to visitors and are easier to reach tourists. Furthermore, the mobile guide applications offer search features, pull and push notifications to the users based on their locations and also reviews and recommendations by previous users [107]. As outlined by [108], learning about new cultures and history of the cities is one of the main reason of travelling and PBSN mobile guide applications engage visitors in an entertaining way to learn about the places they are currently visiting. Pica et al. [109] proposed the GeoGuide application which allows the overlaying of images, sounds and videos to allow visitors discover and learn the history of buildings or even view the landforms of the cities before the existence of the current infrastructures.

5.3 Assistive Technology

Urban cities have witnessed a rapidly changing population where the distance between family members is increasing resulting into a higher degree of isolation among older people. To improve the living conditions of this group of population, different assistive technologies have been introduced to support them in their daily life and to provide care facilities [110]. While these solutions can be expensive and require large computational cost, PBSN applications, inspired by human cognition, can offer the assistance by making use of the retrieved context data. Similarly, assistive services can be provided to visually impaired persons to facilitate their pedestrian experience in the city streets [111]. The proposed system provides guidance in real-time and is responsible for obstacle detection as well as interaction facilities with the users.

5.4 Crowdsourcing

Crowdsourcing applications allow users to contribute to complex problem solving in a transparent manner by making use of the multi-sensing capabilities of the smartphones [112]. The PBSN crowdsourcing applications are known to be more beneficial by using the temporal dimension in addition to the location coordinates. As outlined by [113], these innovative applications were helpful in emergencies such as finding a lost child in the city or a disaster relief. To find the child, several pictures have been uploaded by visitors in that area during a certain timeframe and by using data analytics, the police looked out for the lost child by using the uploaded pictures. For the second case, an infrastructure in a city was damaged and no way was available to assess the damage using the remaining infrastructure. To help reconstruct the disaster site, citizens shared its pictures, which were helpful in speeding up the rescue efforts in a more effective way.

6 Research Challenges

Numerous PBSN systems have been designed or implemented in different application areas to help people in their daily lives. However, it is noticed that there are still many issues and challenges involving these applications. The main challenges of PBSN platforms are described below.

6.1 Security and Privacy

Popular PBSN applications are known to provide self-controlled privacy settings for users to protect their information online. However as outlined by Chang et al. [114], hiding information does not really mean that a flawless privacy protection is provided since locations of users can be deduced from different sources, e.g. based on friendships of users and moreover, when users are tagged on friends' posts, locations are automatically exposed. A study carried out by Krishnamurthy and Wills [115], showed that leakage of personally identified information (PII) of users is occurring in many OSN sites to third parties aggregation servers. TaintDroid [116] was implemented to study the behavior of 30 such third-party applications and the study concluded that two-thirds of the applications examined exhibit suspicious handling of sensitive data, and that 15 of the 30 applications reported users' locations to other advertising servers. Several attempts such as encryption and cryptography approaches have been proposed to further protect location information but it is also known that many attacks can be made on such encryption protocols to decrypt and have access to the information such as spoofing attack or man-in-the-

middle attack. In addition, securing data in a peer-to-peer environment is even more challenging in the absence of a centralized server for communication.

6.2 Anonymous Profile Matching

Many studies on profile matching of PBSN have based their algorithms on fine-grained privacy protocols to primarily secure the privacy of the users and in addition to present them with finer detailed profiles that are matched on different levels of their interests. Since in this case, the privacy of users is related to both the privacy of their profile information and the results of their profile matching, therefore anonymous profile matching should be done. Liang et al. [117] addressed this challenge by introducing two protocols with full anonymity namely the Comparison-based Profile Matching (eCPM) and the Predicate-based Profile Matching (iPPM). These two protocols enabled users to anonymously request messages and respond to the requests without disclosing any personal information. However, in the current system, partial information about the user is revealed. Deep investigation and further research is needed in this area so as to improve the matching algorithms by integrating full anonymity measures and in addition, users should be aware of the information that is being used for this feature.

6.3 Trust Management

Trust between users in online social networking sites following a centralized architecture, is based mostly on the real life social relationships such as college friends, family members or even colleagues. For PBSN services, the level of trust between the users will be different since people communicate with each other without any prior interactions before. Since communication will be based on a peer-to-peer architecture, trust management will be more challenging because of an absence of a central server and in addition the mobility of the users. As outlined by Cho et al. [118], defining and managing trust in mobile ad hoc networks, the interactions between the composite cognitive, social, information and communication networks must be considered. MobiTrust [102] is a novel trust management model for PBSN where it is based on a fully decentralized and self-managed system. The computation of trust is based on three functional factors such as user profile similarity, reputation and history of friends. Trust management plays an imperative role in defining the success of PBSN applications where both the location and identity of users have to be protected. Further works must be done to establish trust relationships among the users and also between the users and the system.

6.4 Data Analytics

Location based services are the new trend in social networking and the market is currently expanding to meet its customers' needs and to further improve its services, the business models are concentrating deeply on data analytics. Several platforms are used to monitor social media and some of them focus on the analysis of location-based social data, e.g. or the Foursquare Merchant Dashboard [63]. The data analyzed can be used in several areas such as for advertisements and marketing purposes and also to study the usage patterns of users for example, the platform KitLocate [119] uses data to forecast the user's next actions. However, it should be noted as for other research challenges outlined, data analytics also raises a privacy issue for users as the information are usually publicly available on the Internet.

6.5 Analysis of Topological Characteristics of Social Networks

Due to the popularity and huge acceptance of PBSN applications, it is vital to further study the statistics and dynamics of these networks to better design the future applications or to improve the existing ones. Analyzing the topological characteristics of such networks is challenging since it involves crawling large graphs of data and highly dynamic ones. In addition, it becomes more challenging since the networks change quickly over time through the addition of new edges, therefore changing the underlying social structure. As future directions, studies should be carried out to understand the content patterns of these networks and to derive new algorithms for discovering people, recommendations and advertising based on the preferences of the users.

6.6 Link Prediction Problem

A common computational problem with the social network is the link prediction problem. Many studies have been carried out to improve the current link prediction services by analyzing user mobility patterns. For instance, Liben-Nowell and Kleinberg [120] studied an array of measures such as graph distance, common neighbours, etc. that can help to lead to the most accurate link predictions. Scellato et al. [121] argued that effective link prediction on location-based services is possible by focusing on the friends-of-friends and on the place of friends of a user. However, when there are millions of users, these are quite sparse, therefore designing an accurate and efficient prediction algorithm is quite challenging. Gao and Liu [84] outlined that the best way to combine PBSN services with location prediction efficiently is still an open research problem. Therefore, further investigation is required so as to improve the link prediction problem using geometric data

together with spatial-temporal data. As outlined by Bliss et al. [122], the prediction algorithms should be designed in such a way so as to prevent decay of links over time and deducing the inconsistencies in flow rates.

6.7 Privacy Context Based Communication

Different types of context-based services have been implemented making use of the location information and daily activities of users ranging from discovering nearby friends applications to sharing recommendations or content and gaming applications. While offering several benefits to users, at the same time, these applications expose users' to different risks. EnCore allows secure event-based communications, but in spite of the strong security and privacy guarantee, different types of attacks can take place, e.g. attackers can act as peers and participate in the communication [89]. Other ways that the security of EnCore can be bypassed consist of attackers tracking a device if it remains in continuous communication with another device over Bluetooth or if users have shared some explicit information such as nicknames, attackers are able to link the communication or posts shared. Other challenges of communication in context aware services as outlined by Li et al. [123] include of a quick discovering method, efficient channel allocation, power control and interference management.

6.8 Adaptabilities

Adaptability is one of the fundamental characteristic of wireless services and mobile applications in the current trend of PBSN. It refers to the ability how the PBSN applications gracefully abide with changes in circumstances. Context information is normally used to provide adaptability in the mobile network [124]. The adaptation provides a proximity based selection of services, automatic reconfiguration in the settings of the application or of the contextual information and also a set of actions during a context change. From previous studies, it is noticed that designing such algorithms can be quite challenging to ensure adaptability in PBSN applications since the network is quite large and very dynamic [125]. Adaptive applications need to match the main three domains: user preferences, device capabilities, and application requirements. Much research must be done in this area to better support PBSN systems. Matching approaches in PBSN applications must be based on semantics so as they are able to adapt to different situations.

7 Conclusion

In this chapter, a comprehensive review of PBSN was carried out outlining the different types and components of PBSN systems. An innovative categorization model of PBSN applications has been presented namely Categorization by Locations, Categorization by Objects, Categorization by Purposes and Categorization by Trajectories. Each category has been further classified into sub-classes and examples of each has been provided after providing a systematic discussion. A thorough evaluation of PBSN is done based on important criteria such as security and privacy, discovery protocols and architectures. It is observed that even though PBSN is a novel application in the social networking area, several new aspects have been emerged in addition to the features of OSN applications since location is taken into consideration. For instance, the architecture is different since the mobility of the users have to be considered in addition to the computation cost and battery life of the mobile devices. The development and evaluation of these proximity applications are subjected to a new direction in the field of social computing giving rise to innovative research directions. We have observed that location privacy is very crucial for these applications and static privacy as provided for OSN applications cannot be applied in PBSN but the dynamic situations of the users should be considered. This survey is concluded with a discussion of research challenges in Proximity Based Social Networks. The research challenges will be helpful in the design of future PBSN applications so that important features such privacy-preserving techniques, communication and adaptabilities are taken into consideration. This detailed study on PBSN applications will also support future researches in the implementation of new algorithms for PBSN frameworks.

References

1. eMarketer: Smartphone users worldwide will total 1.75 billion in 2014. http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536#sthash.T8j1GPPN.dpuf (2014). Accessed 21 Mar 2019
2. Ziv, N.D., Mulloth, B.: An exploration on mobile social networking: Dodgeball as a case in point. In: Mobile Business'. ICMB'06. International Conference on, pp. 21–21. IEEE (2006)
3. Facebook. https://www.facebook.com (2020). Accessed 10 Jan 2020
4. Kayastha, N., Niyato, D., Wang, P., Hossain, E.: Applications, architectures, and protocol design issues for mobile social networks: a survey. Proc. IEEE. **99**(12), 2130–2158 (2011)
5. Niu, B., Zhang, T., Zhu, X., Li, H., Lu, Z.: Priority-aware private matching schemes for proximity-based mobile social networks. Technical Report, Submitted on 31st January 2014, Cornell University Library (2014)
6. The Australian Psychological Society Ltd: The social and psychological impact of online social networking, APS National Psychology Week Survey (2010)
7. Cranshaw, J., Toch, E., Hong, J., Kittur, A., Sadeh, N.: Bridging the gap between physical location and online social networks. In: Proceedings of the 12th ACM international conference on Ubiquitous computing, Copenhagen, Denmark, pp. 119–128. ACM (2010)

8. Zhang, R., Zhang, Y., Sun, J., Yan, G.: Fine-grained private matching for proximity-based mobile social networking. In: 2012 Proceedings IEEE INFOCOM, Orlando, FL, pp. 1969–1977. IEEE (2012)
9. Puttaswamy, K.P., Zhao, B.Y.: Preserving privacy in location-based mobile social applications. In: Proceedings of the 11th Workshop on Mobile Computing Systems & Applications, Annapolis, MD, pp. 1–6. ACM (2010)
10. Asghar, D., Zubair, M., Ahmad, D.: A review of location technologies for wireless mobile location-based services. J. Am. Sci. **10**(7), 110–118 (2014)
11. Lee, S., Tewolde, G., Kwon, J.: Design and implementation of vehicle tracking system using GPS/GSM/GPRS technology and smartphone application. In: 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, South Korea, pp. 353–358. IEEE (2014)
12. Sultana, S., Enayet, A., Mouri, I.J.: A smart, location based time and attendance tracking system using android application. Int. J. Comput. Sci. Eng. Inf. Technol. **5**(1), 1–5 (2015)
13. Moheshkumar, G., Padmapriya, G.: Survey on location-based services. Innov. Int. J. Appl. Res. **5**(1) (2017)
14. Abulleif, T., Al-Dossary, A.: Location based services (LBS). In: Proceedings of the 3rd National GIS Symposium in Saudi Arabia, Khobar, Saudi Arabia, (2008)
15. Buczkowski A.: Location-based services. Available from http://geoawesomeness.com/knowledge-base/location-based-services/ (2012). Accessed 20 Mar 2020
16. Foursquare Statistics: 99Firms. https://99firms.com/blog/foursquare-statistics/#gref (2020). Accessed 10 June 2020
17. Crook, J.: Techcrunch. https://techcrunch.com/2017/03/01/foursquare-launches-pilgrim-sdk-to-let-developers-leverage-location/ (2017). Accessed 10 June 2020
18. Chen, R.: Ubiquitous positioning and mobile location-based services in smart phones. IGI Global, Hershey, PA (2012)
19. Noulas, A., Mascolo, C., Frias-Martinez, E.: Exploiting foursquare and cellular data to infer user activity in urban environments. In: 2013 IEEE 14th International Conference on Mobile Data Management, vol. 1, pp. 167–176. IEEE (2013)
20. Li, Y., Steiner, M., Wang, L., Zhang, Z.L.,, Bao, J.: Exploring venue popularity in foursquare. In: 2013 Proceedings IEEE INFOCOM, pp. 3357–3362. IEEE (2013)
21. Quercia, D., Saez, D.: Mining urban deprivation from foursquare: implicit crowdsourcing of city land use. IEEE Pervasive Comput. **13**(2), 30–36 (2014)
22. Apple Support: About privacy and Location Services using iOS 8 on iPhone, iPad, and iPod touch. https://support.apple.com/en-us/HT203033 (2019). Accessed 30 Apr 2019
23. Gao, H., Tang, J., Liu, H.: Exploring social-historical ties on location-based social networks. In: Proceedings of the 6th International AAAI Conference on Weblogs and Social Media (2012)
24. Matt, H.: Who, What, When, and Now...Where. https://www.facebook.com/notes/facebook/who-what-when-and-nowwhere/418175202130 (2016). Accessed 2 May 2018
25. The Foursquare Blog. http://blog.foursquare.com/post/87012827988/more-on-swarm-and-the-future-of-foursquare (2014). Accessed 2 May 2018
26. Bao, J., Zheng, Y., Wilkie, D., Mokbel, M.F.: A survey on recommendations in location-based social networks. In: ACM Transaction on Intelligent Systems and Technology, pp. 1–30 (2014)
27. Flickr. https://www.flickr.com/ (2020). Accessed 3 Mar 2020
28. Diana, A.: Information week network computing. Color Labs Offers Location-Based Photo Sharing App. http://www.networkcomputing.com/networking/color-labs-offers-location-based-photo-sharing-app/d/d-id/1096818? (2011). Accessed 17 June 2018
29. Geobells: Location based reminders, improved. http://geobells.com/ (2014). Accessed 16 June 2018
30. Bauer, C., Strauss, C.: Location-based advertising on mobile devices. Manag. Rev. Q. **66**(3), 159–194 (2016)
31. Drossos, D., Giaglis, G.M., Lekakos, G., Kokkinaki, F., Stavraki, M.G.: Determinants of effective SMS advertising: an experimental study. J. Interact. Advert. **7**(2), 16–27 (2007)

32. Xu, H., Oh, L.B., Teo, H.H.: Perceived effectiveness of text vs. multimedia location-based advertising messaging. Int. J. Mob. Commun. **7**(2), 154–177 (2009)
33. Crocker, P.: Proximity-based mobile social networking: outlook and analysis. Gigaom Pro. http://percolatorla.com/wp-content/uploads/2014/05/Industry.pdf (2013). Accessed 11 May 2018
34. Yu, N., Han, Q.: Context-aware community construction in proximity-based mobile networks. Mob. Inf. Syst. **2015**, 402705 (2015)
35. Proxxi: Proxxi, A Proximity-Based Social App. http://coenraets.org/blog/2014/01/proxxi-a-proximity-based-social-app/ (2014). Accessed 17 June 2019
36. LoKast. http://www.lokast.com/lokast-app/ (2018). Accessed 22 May 2018
37. Burcea, I., Jacobsen, H.A.: L-ToPSS–push-oriented location-based services. In: International Workshop on Technologies for E-Services, Berlin, Heidelberg, pp. 131–142. Springer (2003)
38. Knowledge@Wharton: The experts vs. the amateurs: a tug of war over the future of media. http://knowledge.wharton.upenn.edu/article.cfm?articleid=1921 (2019). Accessed 30 Apr 2019
39. Scanfeld, D., Scanfeld, V., Larson, E.L.: Dissemination of health information through social networks: twitter and antibiotics. Am. J. Infect. Control. **38**(3), 182–188 (2010)
40. Boulos, M.N.: Location-based health information services: a new paradigm in personalised information delivery. Int. J. Health Geogr. **2**(1), 2 (2003)
41. Boulos, M.N.K., Rocha, A., Martins, A., Vicente, M.E., Bolz, A., Feld, R., Tchoudovski, I., Braecklein, M., Nelson, J., Laighin, G.Ó., Sdogati, C.: CAALYX: a new generation of location-based services in healthcare. Int. J. Health Geogr. **6**, 9 (2007)
42. Carbunar, B., Potharaju, R.: You unlocked the mt. everest badge on foursquare! countering location fraud in geosocial networks. In: 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS), Las Vegas, NV, pp. 182–190. IEEE (2012)
43. BotFighters: BotFighters. http://www.botfighters.com/ (2017). Accessed 10 June 2017
44. PokemonGo: PokemonGo. https://www.pokemon.com/us/app/pokemon-go/ (2017). Accessed 23 July 2017
45. Steinfield, C.: The development of location based services in mobile commerce. In: E-life after the Dot Com Bust, Physica, Heidelberg, pp. 177–197. Springer (2004)
46. Schramm, M.: Angry Birds creators plan new game, location-based platform. Engadget. http://www.engadget.com/2011/06/15/angry-birds-creators-plan-new-game-location-based-platform/ (2011). Accessed 20 Apr 2020
47. De Longueville, B., Smith, R.S., Luraschi, G.: Omg, from here, I can see the flames!: a use case of mining location based social networks to acquire spatio-temporal data on forest fires. In: Proceedings of the 2009 International Workshop on Location Based Social Networks, Seattle, Washington, pp. 73–80. ACM (2009)
48. Gomide, J., Veloso, A., Meira Jr, W., Almeida, V., Benevenuto, F., Ferraz, F., Teixeira, M. Dengue surveillance based on a computational model of spatio-temporal locality of Twitter. In: Proceedings of the 3rd International Web Science Conference, Koblenz, Germany, p. 3. ACM (2011)
49. Mokryn, O., Karmi, D., Elkayam, A., Teller, T.: Help me: opportunistic smart rescue application and system. In: The 11th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), Ayia Napa, Cyprus, pp. 98–105. IEEE (2012)
50. Karimi, H.A., Zimmerman, B., Ozcelik, A., Roongpiboonsopit, D.: SoNavNet: a framework for social navigation networks. In: Proceedings of the 2009 International Workshop on Location Based Social Networks, Seattle, Washington, pp. 81–87. ACM (2009)
51. Navigation OnStar. https://www.onstar.com/us/en/services/navigation.html (2019). Accessed 12 June 2019
52. Gaonkar, S., Li, J., Choudhury, R.R., Cox, L., Schmidt, A.: Micro-blog: sharing and querying content through mobile phones and social participation. In: Proceedings of the 6th international conference on Mobile systems, applications, and services, Breckenridge, CO, pp. 174–186. ACM (2008)

53. Torchia, B.: Passive-location tracking in iOS: why it happens and how to stop it. http://getorchard.com/blog/location-tracking-app-ios/ (2014). Accessed 20 June 2015
54. Geofency. http://www.geofency.com/ (2019). Accessed 20 June 2019
55. PlaceMe. https://www.placemeapp.com/placeme/ (2019). Accessed 20 June 2019
56. Rachuri, K.K., Hossmann, T., Mascolo, C., Holden, S.: Beyond location check-ins: Exploring physical and soft sensing to augment social check-in apps. In: 2015 IEEE International Conference on Pervasive Computing and Communications (PerCom), St. Louis, MO, pp. 123–130. IEEE (2015)
57. Miluzzo, E., Lane, N.D., Eisenman, S.B., Campbell, A.T.: CenceMe—injecting sensing presence into social networking applications. In: Smart Sensing and Context, Berlin Heidelberg, pp. 1–28. Springer (2007)
58. Schonfeld, E.: Location-tracking startup sense networks emerges from stealth to answer the question: where is everybody? http://techcrunch.com/2008/06/09/location-tracking-startup-sense-networks-emerges-from-stealth-to-answer-the-question-where-is-everybody/ (2008). Accessed 20 June 2019
59. Getting started with twitter via your mobile phone. https://support.twitter.com/articles/14589-how-to-add-your-phone-via-sms. Accessed 21 Mar 2019
60. Li, L., Katangur, A.K., Karuturi, N.N.: SmartNotify: an intelligent location based notification system using users' activities and points of interests. Int. J. Adv. Pervasive Ubiquitous Comput. **10**(1), 37–50 (2018)
61. Patil, P., Sawant, K., Desai, S., Shinde, A., Bhelande, M.M.: Task trigger: reminder application based on location. Int. Res. J. Eng. Technol. **05**(03), 3282–3285 (2018)
62. Hadiwardoyo, S.A., Patra, S., Calafate, C.T., Cano, J.C., Manzoni, P.: An intelligent transportation system application for smartphones based on vehicle position advertising and route sharing in vehicular Ad-Hoc networks. J. Comput. Sci. Technol. **33**(2), 249–262 (2018)
63. Foursquare.: Available from https://foursquare.com/ (2018). Accessed 20 Apr 2018
64. iGroups: Apple's new iPhone social app in development. Patently Apple. http://www.patentlyapple.com/patently-apple/2010/03/igroups-apples-new-iphone-social-app-in-development.html (2010). Accessed 17 June 2019
65. The Scoop. https://itunes.apple.com/us/app/scoop-nytimes-guide-to-nyc/id374981318?mt=8 (2019). Accessed 20 June 2019
66. Buczkowski A.: Alike App—location-based recommends of nearby venues that are just like your favorites. http://geoawesomeness.com/alike-app-location-based-recommends-of-nearby-venues-that-are-just-like-your-favorites/ (2012). Accessed 20 Mar 2020
67. Geocaching. https://www.geocaching.com/play/ (2020). Accessed 20 Mar 2020
68. Jetiyanuwat, T., Kositwutisopon, T., Tanthawatkul, P., Viriyasitavat, W.: OPLITOP: A localized broacast media. In: 2014 Third ICT International Student Project Conference (ICT-ISPC), Nakhon Pathom, Thailand, pp. 151–154. IEEE (2014)
69. Hwang, T., Jeong, J.P., Lee, E. SANA: safety-aware navigation app for pedestrian protection in vehicular networks. In: 2014 International Conference on Information and Communication Technology Convergence (ICTC), Busan, South Korea, pp. 947–953. IEEE (2014)
70. Zheng, Y., Xie, X., Ma, W.Y.: GeoLife: a collaborative social networking service among user, location and trajectory. IEEE Data Eng. Bull. **33**(2), 32–39 (2010)
71. Michalevsky, Y., Schulman, A., Veerapandian, G.A., Boneh, D., Nakibly, G.: PowerSpy: location tracking using mobile device power analysis. In: Proceedings of the 24th USENIX Conference on Security Symposium, Washington, DC, pp. 785–800. USENIX (2015)
72. Ghosh, S., Dutta, J., Roy, S.: SenseDcity: a participatory sensing based approach. In: Proceedings of the Workshop Program of the 19th International Conference on Distributed Computing and Networking, Varanasi, India, p. 16. ACM (2018)
73. AndroSensor: AndroSensor. https://play.google.com/store/apps/details?id=com.fivasim.androsensor&hl=en/ (2018). Accessed 20 May 2018
74. Chow, C.Y., Mokbel, M.F.: Privacy in location-based services: a system architecture perspective. Sigspatial Special. **1**(2), 23–27 (2009)

75. AllSeen Alliance: Overview for oneM2M. http://ftp.onem2m.org/Meetings/TP/2014%20meetings/20140922_TP13_Phoenix/TP-2014-0496R02-Overview_for_oneM2M.PDF (2014). Accessed 1 June 2020
76. HumHub. https://www.humhub.org (2020). Accessed 18 Apr 2020
77. Elgg. https://elgg.org (2020). Accessed 18 Apr 2020
78. Anahita: Anahita—open source social networking platform and framework. http://www.getanahita.com/ (2020). Accessed 18 Apr 2020
79. Eagle, N., Pentland, A.: Social serendipity: mobilizing social software. IEEE Pervasive Comput. **4**(2), 28–34 (2005)
80. Pietilainen, A.K., Oliver, E., LeBrun, J., Varghese, G., Diot, C.: MobiClique: middleware for mobile social networking. In: Proceedings of the 2nd ACM workshop on Online social networks, Barcelona, Spain, pp. 49–54. ACM (2009)
81. Zhu, H., Du, S., Li, M., Gao, Z.: Fairness-aware and privacy-preserving friend matching protocol in mobile social networks. IEEE Trans. Emerg. Top. Comput. **1**(1), 192–200 (2013)
82. AllJoyn: Open Connectivity Foundation. https://openconnectivity.org/developer/reference-implementation/alljoyn/ (2020). Accessed 18 Apr 2020
83. He, J., Chu, W.W.: A social network-based recommender system (SNRS). In: Data mining for social network data, pp. 47–74. Springer, Boston, MA (2010)
84. Gao, H., Liu, H.: Data analysis on location-based social networks. In: Mobile Social Networking, pp. 165–194. Springer, New York (2014)
85. Bao, J., Zheng, Y., Mokbel, M.F.: Location-based and preference-aware recommendation using sparse geo-social networking data. In: Proceedings of the 20th international conference on advances in geographic information systems, Redondo Beach, CA, pp. 199–208. ACM (2012)
86. Khalid, O., Khan, M.U.S., Khan, S.U., Zomaya, A.Y.: Omnisuggest: a ubiquitous cloud-based context-aware recommendation system for Mobile Social Networks. IEEE Trans. Serv. Comput. **7**(3), 401–414 (2014)
87. Mahmud, J., Nichols, J., Drews, C.: Home location identification of twitter users. ACM Trans. Intell. Syst. Technol. **5**(3), 47 (2014)
88. Do, T.M.T., Gatica-Perez, D.: Where and what: Using smartphones to predict next locations and applications in daily life. In: Pervasive and Mobile Computing, vol. 12, pp. 79–91. Elsevier (2014)
89. Aditya, P., Erdélyi, V., Lentz, M., Shi, E., Bhattacharjee, B., Druschel, P.: Encore: private, context-based communication for mobile social apps. In: Proceedings of the 12th annual international conference on Mobile systems, applications, and services, Bretton Woods, NH, pp. 135–148. ACM (2014)
90. Beach, A., Gartrell, M., Han, R.: Solutions to security and privacy issues in mobile social networking. In: 2009 International Conference on Computational Science and Engineering, Vancouver, Canada, vol. 4, pp. 1036–1042. IEEE (2009)
91. Li, M., Zhu, H., Gao, Z., Chen, S., Yu, L., Hu, S., Ren, K.: All your location are belong to us: Breaking mobile social networks for automated user location tracking. In: Proceedings of the 15th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Philadelphia, PA, pp. 43–52. ACM (2014a)
92. Wei, W., Xu, F., Li, Q.: Mobishare: Flexible privacy-preserving location sharing in mobile online social networks. In: 2012 Proceedings IEEE INFOCOM, Orlando, FL, pp. 2616–2620. IEEE (2012)
93. Sohn, T., Li, K.A., Lee, G., Smith, I., Scott, J., Griswold, W.G.: Place-its: a study of location-based reminders on mobile phones. In: International Conference on Ubiquitous Computing, Berlin, Heidelberg, pp. 232–250. Springer (2005)
94. Chow, C.Y., Bao, J., Mokbel, M.F.: Towards location-based social networking services. In: Proceedings of the 2nd ACM SIGSPATIAL International Workshop on Location Based Social Networks, San Jose, CA, pp. 31–38. ACM (2010)

95. Champion, A.C., Yang, Z., Zhang, B., Dai, J., Xuan, D., Li, D.: E-SmallTalker: a distributed mobile system for social networking in physical proximity. IEEE Trans Parallel Distrib Syst. **24**(8), 1535–1545 (2013). https://doi.org/10.1109/TPDS.2012.251.
96. Pouwelse, J.A., Garbacki, P., Wang, J., Bakker, A., Yang, J., Iosup, A., Epema, D.H., Reinders, M., Van Steen, M.R., Sips, H.J.: TRIBLER: a social-based peer-to-peer system. Concurr. Comput. Pract. E. **20**(2), 127–138 (2008)
97. Lubke, R., Schuster, D., Schill, A.: Mobilisgroups: Location-based group formation in mobile social networkss. In: IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Seattle, WA, pp. 502–507. IEEE (2011)
98. Smaldone, S., Han, L., Shankar, P., Iftode, L.: Roadspeak: enabling voice chat on roadways using vehicular social networks. In: Proceedings of the 1st Workshop on Social Network Systems, Glasgow, Scotland, pp. 43–48. ACM (2008)
99. von Arb, M., Bader, M., Kuhn, M., Wattenhofer, R.: Veneta: Serverless friend-of-friend detection in mobile social networking. In: 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Avignon, France, pp. 184–189. IEEE (2008)
100. Clements, M., Serdyukov, P., De Vries, A.P., Reinders, M.J.: Using flickr geotags to predict user travel behaviour. In: Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval, Geneva, Switzerland, pp. 851–852. ACM (2010)
101. Lane, N.D., Miluzzo, E., Lu, H., Peebles, D., Choudhury, T., Campbell, A.T.: A survey of mobile phone sensing. IEEE Commun. Mag. **48**(9), 140–150 (2010)
102. Li, J., Zhang, Z., Zhang, W.: Mobitrust: trust management system in mobile social computing. In: 10th IEEE International Conference on Computer and Information Technology, Bradford, UK, pp. 954–959. IEEE (2010)
103. Ellis, K., Godbole, S., Marshall, S., Lanckriet, G., Staudenmayer, J., Kerr, J.: Identifying active travel behaviors in challenging environments using GPS, accelerometers, and machine learning algorithms. Front. Public Health. **2**, 36 (2014)
104. Erra, U., Capece, N.: Engineering an advanced geo-location augmented reality framework for smart mobile devices. J. Ambient. Intell. Humaniz. Comput. **10**(1), 255–265 (2019)
105. Mohan, P., Padmanabhan, V., Ramjee, R.: Nericell: rich monitoring of road and traffic conditions using mobile smartphones. In: Proceedings of ACM Sen Sys, Raleigh, NC (2008)
106. Alvear, O., Zamora, W., Calafate, C.T., Cano, J.C. and Manzoni, P.: EcoSensor: monitoring environmental pollution using mobile sensors. In: 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1–6. IEEE (2016)
107. Rahimi, R., Hassan, A., Tekin, O.: Augmented reality apps for tourism destination promotion. In: Destination Management and Marketing: Breakthroughs in Research and Practice, pp. 1066–1077. IGI Global (2020)
108. Falk, J.H., Ballantyne, R., Packer, J., Benckendorff, P.: Travel and learning: a neglected tourism research area. Ann. Tour. Res. **39**(2), 908–927 (2012). https://doi.org/10.1016/j.annals.2011.11.016
109. Pica, A., Reynard, E., Grangier, L., et al.: GeoGuides, urban geotourism offer powered by mobile application technology. Geoheritage. **10**, 311–326 (2018)
110. Kötteritzsch, A., Weyers, B.: Assistive technologies for older adults in urban areas: a literature review. Cogn. Comput. **8**(2), 299–317 (2016)
111. Bhargava, B., Angin, P., Duan, L.: A mobile-cloud pedestrian crossing guide for the blind. In: International Conference on Advances in Computing & Communication (2011)
112. Cai, J.L.Z., Yan, M., Li, Y.: Using crowdsourced data in location-based social networks to explore influence maximization. In: IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications, pp. 1–9. IEEE (2016)

113. Satyanarayanan, M.: Mobile computing: the next decade. In: Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond, pp. 1–6 (2010)
114. Chang, W., Wu, J., Tan, C.C.: Friendship–based location privacy in mobile social networks. Int. J. Secur. Networks. **6**(4), 226–236 (2011)
115. Krishnamurthy, B., Wills, C.E.: On the leakage of personally identifiable information via online social networks. In: Proceedings of the 2nd ACM Workshop on Online Social Networks. Barcelona, Spain, pp. 7–12. ACM (2009)
116. Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.G., Cox, L.P., Jung, J., McDaniel, P., Sheth, A.N.: TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In: Proceedings of the 9th USENIX conference on Operating systems design and implementation, Vancouver, BC, Canada, pp. 393–407. ACM, (2014)
117. Liang, X., Li, X., Zhang, K., Lu, R., Lin, X., Shen, X.S.: Fully anonymous profile matching in mobile social networks. IEEE J. Sel. Areas Commun. **31**(9), 641–655 (2013)
118. Cho, E., Myers, S.A., Leskovec, J.: Friendship and mobility: user movement in location-based social networks. In: Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, San Diego, CA, pp. 1082–1090. ACM (2011)
119. KitLocate. http://www.kitlocate.com/ (2019). Accessed 12 Dec 2019
120. Liben-Nowell, D., Kleinberg, J.: The link-prediction problem for social networks. J. Am. Soc. Inf. Sci. Technol. **58**(7), 1019–1031 (2007)
121. Scellato, S., Noulas, A., Mascolo, C.: Exploiting place features in link prediction on location-based social networks. In: Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Diego, CA, pp. 1046–1054. ACM (2011)
122. Bliss, C.A., Frank, M.R., Danforth, C.M., Dodds, P.S.: An evolutionary algorithm approach to link prediction in dynamic social networks. J. Comput. Sci. **5**(5), 750–764 (2014)
123. Li, Q., Li, H., Russell, P., Chen, Z., Wang, C.: CA-P2P: context-aware proximity-based peer-to-peer wireless communications. IEEE Commun. Mag. **52**(6), 32–41 (2014b)
124. da Rocha, R.C.A.: Middleware for Location-based Services. Laboratory for Advanced Collaboration, Pontificia Universidade Catolica do Rio de Janeiro, pp. 1443-1454 (2004)
125. Kinsner, W.: Challenges in the design of adaptive, intelligent and cognitive systems. In: 6th IEEE International Conference on Cognitive Informatics, Lake Tahoo, CA, pp. 13–25. IEEE, (2007)

Satellite Navigation

Girija Narasimhan

1 Introduction

The moon and earth are natural satellites. Man-made satellites are mechanical devices. Therefore, they termed as artificial satellites. That will orbit the earth, the moon, black holes, and other solar system planets like Mars. Most of the satellite orbits earth for facilitating humane society such as forecast the climate, telecommunication purpose, navigating transportation like ships and aircraft and military security purposes. Satellite design classified based on the scope of the satellite. The spy satellites for the military. The earth remote sensing satellites for forecasting the weather. The communications satellites providing various services like broadcasting, data communication, and telecommunication services.

Any moving object position, speed, and direction controlled by navigation technology [1]. Electricity consumption used to power an electronic navigation system. The electronic navigation method includes various navigation systems like the radar navigation system, radio navigation system, and satellite navigation system [2]. The navigation systems classified based on either object position inland or space. As shown in Fig. 1, namely, they are terrestrial systems and space-based systems [3]. Depending on the sector the terrestrial systems classified as land navigation, for example Advanced Land Navigation System (ALNS) and marine navigation as Ship's Inertial Navigation System (SINS). The space-based systems further subclassified into aeronautic navigation i.e., Tactical Air Navigation (TACAN) and satellite navigation system or satnav system well known Global Navigation Satellite System (GNSS).

G. Narasimhan (✉)
Department at the Higher College of Technology (HCT), University of Technology and Applied Science, Muscat, Sultanate of Oman

S. Paiva (ed.), *Precision Positioning with Commercial Smartphones in Urban Environments*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-71288-4_5

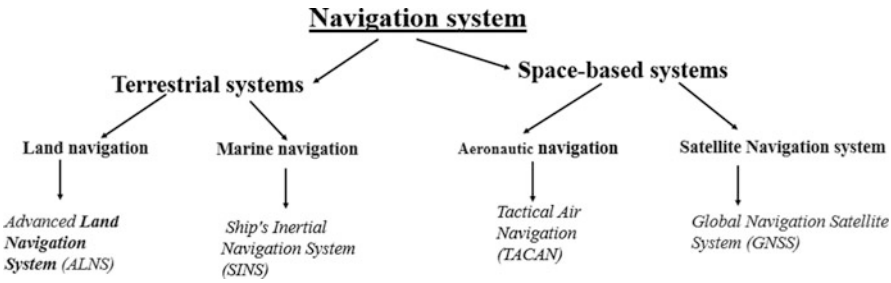


Fig. 1 Classification of navigation system

Table 1 List of navigation satellite system

Global Navigation Satellite Systems (GNSS)	USA—Global Positioning System (GPS)
	Russia—GLObal Navigation Satellite System (GLONASS)
	China—BeiDou Navigation Satellite System (BDS)
	European Union—Galileo
Regional Navigation Satellite System (RNSS)	Japan—Quasi-Zenith Satellite System (QZSS)
	India—Indian Regional Navigation Satellite System (IRNSS)/Navigation with Indian Constellation (NAVIC)

This chapter classified into following sections like the GNSS system, GNSS architecture, regional navigation satellite system and satellite signals, satellite technology, and satellite application and conclusion.

The navigation satellite system classified into global and regional. The global navigation satellite systems are GPS, GLONASS, Galileo, and BeiDou. The regional navigation satellite systems are QZSS and IRNSS/NavIC.

The navigation system classified based on their operation namely the Global Navigation Satellite System (GNSS) and Regional Navigation Satellite System (RNSS). Table 1 gives the name of the country that launched the navigation system and the name of the navigation system. In this introductory section describes GPS, GLONASS, BDS, and Galileo satellite information. This section describes the beginning stage, design scope, and operational details of each global navigation system. As per Table 1 information, the third section explains the regional navigation satellite systems complete operational details.

The second section describes the GNSS architecture. This portion elaborates on the signal service based on the factor Position, Navigation, and Timing (PNT). GNSS architecture consists of three substantial segments. The first segment is the space segment, the task of the space segment, and the orbit plane details discussed. The second segment is the control segment. It gives details about the Master Control Station (MCS) and Backup Master Control Station (BMCS) and Monitor Stations (MS). The third segment is the user segment in the GNSS architecture. It represents

a receiver device portion. This specific section adequately explains each process of satellite signals and at the end usage of signals in the GNSS application.

GNSS was composed of a combination of abundant technologies. Especially the augmentation technology using for finding out accurate signal errors. Testing and assessment technology are useful for assessing receiver quality. Fusion technology is inside the interior part of the satellite engine. Jumping and spoofing technology supports signal calculation and receiver-based aspects. Atomic clock was most crucial to discriminate against the local time of each country around the globe. Most of the countries don't have their GNSS, but they are leading in GNSS based research technologies like a chip-scale atomic clock and hydrogen maser clock. Whenever laymen society gradually starts using any application in their routine life, then that application using technology becomes inevitable.

Explicitly humans need nature predicting tools like satellite imagery and satellite mapping technology. Simultaneously, conventional business, agriculture, and ocean technology and defense also need satellite applications. In the conclusion part, updating satellite technology policy between countries discussed. An orbit stands a general area of all the countries. Each country establishes agencies for tracking communication between them and finding the latest updates in satellite policies. In this growing field, participants of research publications via conferences and research journals are noteworthy. At the same time, artificial intelligence (AI) involved in all navigation research challenges. Because of AI involvement, the navigation system achieves a fantastic precise prediction methodology.

2 Global Navigation Satellite system (GNSS)

This section explains all the currently available GNSS and its country vision. It also explains every development phase of each navigation system and its country target mission.

2.1 Global Position System (GPS)

In 1978 the GPS satellite launched. GPS developed for the United States government military services. Radio signals are used in GPS satellites to determine the time and position of the globe. During 1994, the GPS holding 24 satellites in the satellite constellation. GPS satellites divided into six different types, namely, BLOCK I, BLOCK II/IIA, BLOCK IIR, BLOCK IIR-M, BLOCK IIF, and GPS III satellites [4]. In March 1990, the enhanced model of GPS called the Differential Global Positioning System (DGPS). DGPS provides much accuracy of position data than GPS. GPS accuracy is about 10 m but DGPS accuracy is around 1 m to 10 cm. That is a reason, DGPS eliminates the pseudorange errors better than GPS. Especially

the U.S. coast guard benefited from the DGPS system. Using DGP receiver the longwave frequency signals are broadcast on the longwave marine. DGPS is one of the elements of all the commercial GPS operation units.

2.2 Global Navigation Satellite System (GLONASS)

Around 1976, the USSR (United of Soviet Socialist Republic) started developing the GLONASS system. Currently, Russia is operating this system. In October 1982, the first satellite of Russia GLONASS launched. Close to a similar time, the USA developed GPS. Therefore, GPS launched in 1978, which seems to be a reason GPS achieves the first GNSS system. In 1991 year-end, many economic and political disarray collapse in USSR. Even though the beginning of 1996, Russia's global navigation satellite system constellation completed and fully operational [5]. Based on space segment moderation, the GLONASS satellite namely second generation of satellites GLONASS-M launched. The third generation GLONASS-K1 and GLONASS-K2, GLONASS-KM until GLONASS-V all are under planning and development process up to 2030.

2.3 BeiDou Navigation Satellite System (BDS)

The chines BeiDou navigation satellite system (BDS) implemented in the stage-by-stage process, namely BDS-1, BDS-2, and BDS-3. It is a regional navigational satellite system. Each stage of BDS provides unique services. The BDS-1 project developed for providing Radio Determination Satellite Service (RDSS). The BDS-1 project started in 1994 and the procedure completed in 2000. The second project BDS-2 started in 2004 and completed by 2012. Next, BDS-2 furnished with Radio Navigation Satellite Services (RNSS) and Satellite-Based Augmentation Services (SBAS) [6]. The entire Asia-Pacific region this project provides positioning, velocity measurement, short messaging facility, and timing services [7]. BDS-3 project under process, it started in 2009 may expect to complete 2020. BDS global network provides global positioning, global user short message, international search, and rescue service.

2.4 Galileo

In 1999, the European Space Agency (ESA) represented a group of three countries. Namely, Italy, Germany, and France initiated the Galileo program. In 2003, the European Union (EU) and ESA agreed to develop the Galileo. The Galileo is the first GNSS designed for civilian access. It typically allows all civilians. Other GNSS

systems like GPS, GLONASS, and BDS launched for armed services [8]. In 2005, the first experimental satellite GIOVE-A (Galileo In-Orbit Validation Element) launched. In 2007, In-Orbit Validation (IOV) phase completed successfully and the remaining satellites launched. In 2008, the second testing satellite GIOVE-B launched. From 2011 onwards, Galileo takeoffs it's a successful operation. From the period 2011 to 2014, there are four Galileo-IOV satellites launched. From 2015 onward Galileo-FOC types of satellites are in the operational stage. Until now, some satellites are in a testing phase.

3 Global Navigation Satellite System (GNSS) Architecture

In GNSS, the evergreen key factor as a signal. The performance of GNSS services estimated by signal quality. GNSS signal services estimated by three components like Position, Navigation, and Time referred to as short term PNT [9]. The performance of GNSS calculated based on the time length of signal travel from the satellite to the receiver and multiplied by the speed of light. This performance calculation factor used for quantifying the length between the signal transmitting and receiving position i.e., the distance between satellites and receiver. The name of this measurement as pseudorange measurements. It means pseudorange = time difference speed of light. The GNSS receivers get the primary device for satellite positioning. The operation of the GNSS receiver is to convert the accepted signals (i.e. electromagnetic waves or radio signals) from satellite and transfer to earth control segment monitoring position. The GNSS is a general term, based on the country product as given Table 1 the various receiver devices used in GPS, BDS, Galileo, and Glonass [10]. GNSS architecture includes a combination of three segments. Those are the space segment, the control segment, or the ground segment and user segment [11].

3.1 Space Segment

The core task of the space segment is to generate and transmit the signals to the control segment (shown in Fig. 2). It also stores broadcasted navigation messages which were uploaded by the control segment.

The space segments designed by a collection of satellites. This collection of satellites called satellite constellation. The highly constant atomic clock in the satellite controls every space segment transfer. Each satellite in satellite constellation placed in equally spaced orbital planes surrounding the earth. This path called an orbit path (shown in Fig. 4). All orbit paths, not a perfectly round path, it may be cyclical or ellipse or parabola or hyperbola. Every satellite orbits the earth. But it doesn't stay at a similar distance from earth. Therefore, the distance from the earth changes depending on where the satellite orbit. The orbit eccentricity represents a method

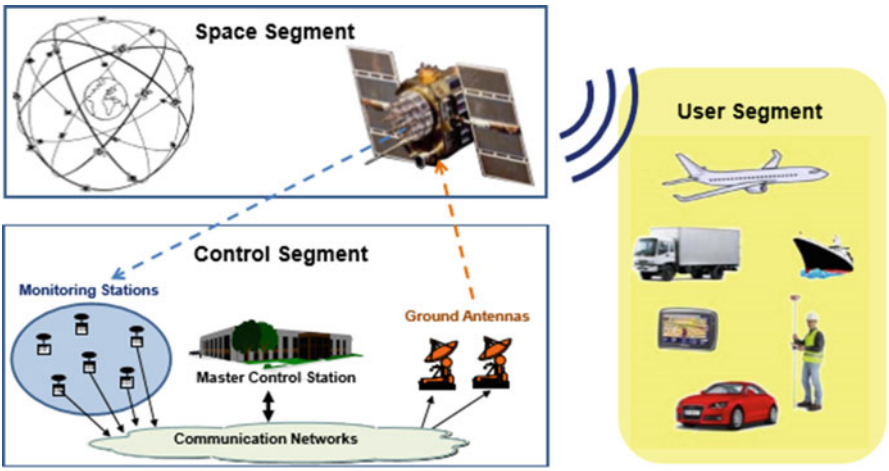


Fig. 2 GNSS segment [9]

of measuring orbit path movement. The eccentricity measure distance value of the orbit path moves away from the perfect circle. The orbit types classified into open or close depends on the on-orbit eccentricity measurement value. Open orbit type also called an escape orbit. In open orbit type, the eccentricity value is equal to one then termed as parabolic orbit. Otherwise, if the value of eccentricity value is greater than one then it is referred to as hyperbolic orbit. Closed orbit type also mentions as periodic orbit. In the closed orbit type, if the eccentricity value is equal to zero then it is circular orbit. Otherwise, if eccentricity value is greater than zero and less than one, then it is mention as elliptical orbit. If orbit type either open or close, then radial orbit. In the radial orbit type, the orbit zero angular momentum with zero eccentricity value (shown in Fig. 3). Various dimension names indicated to the satellite orbit distance. The adjacent distance from the earth indicated as perigee. Remote distance from the earth refers to the apogee. And then its inclination represents the angle, the orbit makes with the earth equator [12].

The classifying aspect of the orbit path is orbital altitude and orbital period. A polar orbit is an inclination of 90° to earth's equator. This polar orbit operated for observing earth movement from one point to another particularly weather and telecommunication satellites. The Low Earth Orbit (LEO) consists of 160–2000 km orbital altitude, and the orbital period is 87–127 min, for example, international space stations. Satellites in this orbit distance from the apogee and perigee are each only about 483 km. The Medium Earth Orbit (MEO) includes 2000–35,786 km orbital altitude and the orbital period takes place 127 min to 24 h, for example, GPS and GLONASS. The Geostationary Earth Orbit (GEO) consists of 35,786 km orbital altitude and the orbital period remains 23 h 56 min 4.1 s, for example, IRNSS satellites. Orbits represent a nearly elliptical path, and the GEO is an ellipse path. This GEO orbit the satellite speed synchronized with the earth's rotation therefore the satellite launched in this orbit halt in the equivalent relative position [12, 13].

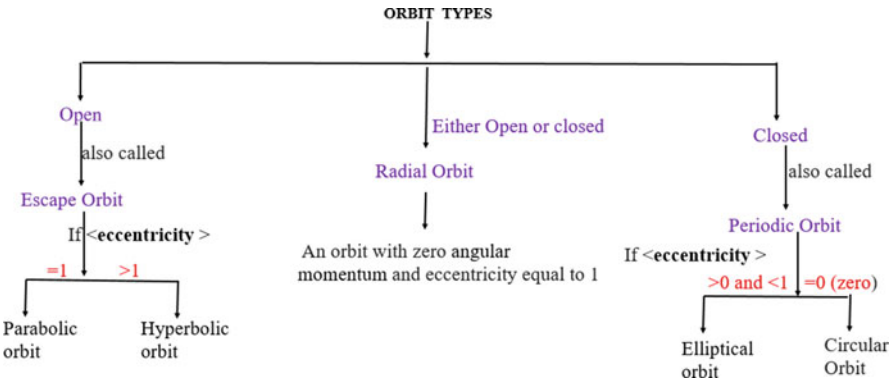


Fig. 3 Orbit types

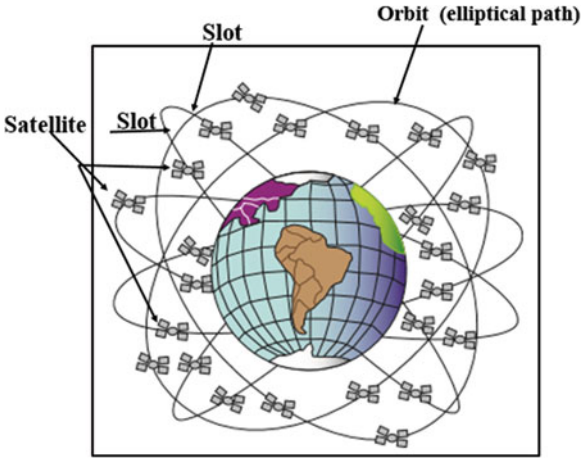


Fig. 4 GNSS satellite orbit [11]

For example, GPS satellites are occupying six orbital planes and each orbital plane has four slots. Therefore, each slot is restraining the satellites. So, six orbital planes multiply by four slots i.e., a total of 24 satellites located as shown in Fig. 4. This significant idea of 24 satellite arrangements is to confirm at least four satellites in view from virtually any point on the planet. There is a spare satellite slot in each orbital plane, that slot is occupied by the standby or backup satellite. High Elliptical Orbit (HEO) satellites provide coverage from one location for long periods, for example, each QZSS satellite covers 8 h above Japan.

Table 2 describes the details about currently available GNSS and its number of stateliest of each navigation system status. Every navigation system, some satellites are active or in operation and some satellites are testing purpose and inactive satellite i.e., retired and stand by like backup satellite. For example, only 27 satellites are active, and the remaining four satellites are backup. Orbit plane where exactly each navigation system satellites are located information available in Table 2 [11, 12].

Table 2 GNSS orbit details

Navigation system	Number of satellites	Orbital plane details
GLONASS	24 satellites	Three orbital planes, with eight satellites per plane
Galileo	30 satellites.(22 usable, 2 testing only, 2 unavailable, and 2 retired (2/2020))	Ten satellites will occupy each of three orbital planes inclined at an angle of 56° with respect to the equator
BeiDou Navigation Satellite System (BDS)	35 satellites	Which include 5 geostationary orbit satellites for backward compatibility with BeiDou-1, and 30 non-geostationary satellites (27 in medium Earth orbit and 3 in inclined geosynchronous orbit), that will offer complete coverage of the globe
GPS	31 (27 are in use and remaining are standbys)	Six earth-centered orbital planes with four operation satellites

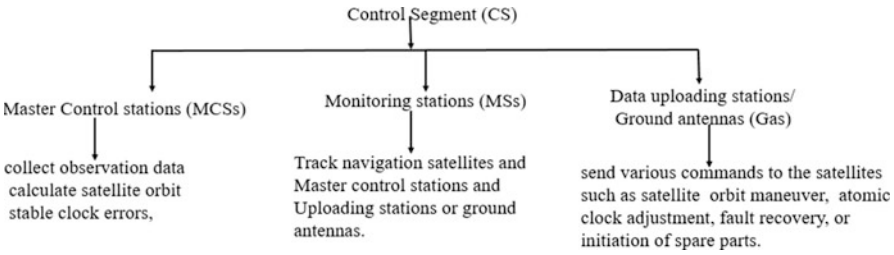


Fig. 5 Control segment task

3.2 Control Segment

The control segment comprises the following segment of GNSS architecture. As shown in Fig. 5, this segment consists of the Master Control Station (MCS), Backup Master Control Station (BMCS), Monitor Stations (MSs), and data uploading station or Ground Antennas (GAs). Master control stations (MCS) collect data with atomic clock errors. Monitoring stations monitors all the control segment such as master control stations and uploading stations including space segment satellites also. The prime task of control segments to track the satellite monitor transmissions. Data uploading stations responsible for sending various signal transmission commands such as atomic clock adjustment and recovering error in a stable clock. And then perform analyses based on received transmission signals. Based on the analyses report send navigation messages like commands and data to the satellite constellation [14].

As per the 2017, May month report [14], the GPS control segment is managing six air force monitor stations, four ground antenna and one master control station, one alternate master control station, seven AFSCN remote tracking stations, and ten NGA monitor system.

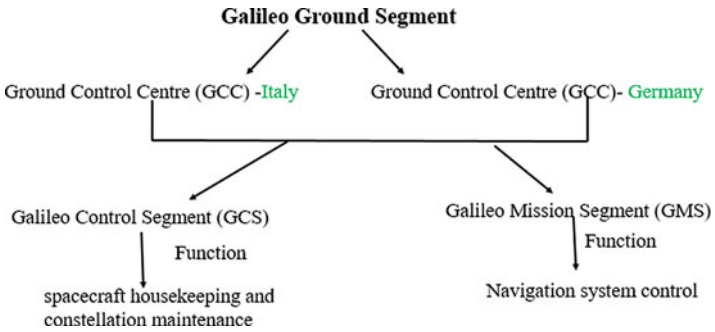


Fig. 6 Galileo ground segment

The china satellite navigation office released a report in December 2019 [7] as the development of the BeiDou navigation satellite system (Version 4.0). This navigation system developed by the China Academy of Space Technology (CAST) and the Chinese Academy of Sciences (CAS) [6]. As per a report, the control segment is operating various ground stations. Which includes master control stations, time synchronization/uplink stations, and monitoring stations. As per the report of 2018, it has one master control station, 10 upload stations, and 30 monitor stations.

The Galileo ground segment has two control centers [15] has shown in Fig. 6. Each control centers are managing control function like housekeeping and maintenance of constellation by Ground Control Centre (GCC). And also managing mission functions like navigation system control by Galileo Mission Segment (GMS). The GCC and GMS interfaced with worldwide ground stations like six Telemetry, Tracking & Control stations (TT&C), and ten Galileo Uplink Stations (ULS) and Galileo Sensor Stations (GSS) and one service center.

Figure 7 shows the complete ground segment architecture of the Galileo navigation system located in various countries. Ground mission segment in Italy and ground control segment in Germany. Tracking and telecommand stations are in Sweden and French [8]. The GLONASS ground control complex (as of 24 November 2016) consist of merely two system control centers, nine reference stations, six uplink stations, and laser ranging stations [5].

3.3 User Segment

The user segment element is the receiver device which will find the user position, velocity, and precise time (PVT) by processing the signal broadcasted by satellites. The receiver device consists of an antenna with a preamplifier, radiofrequency section, microprocessor, intermediate precision oscillator, and data storage memory devices and an interface with a user. In the given below Fig. 8, the user segment each

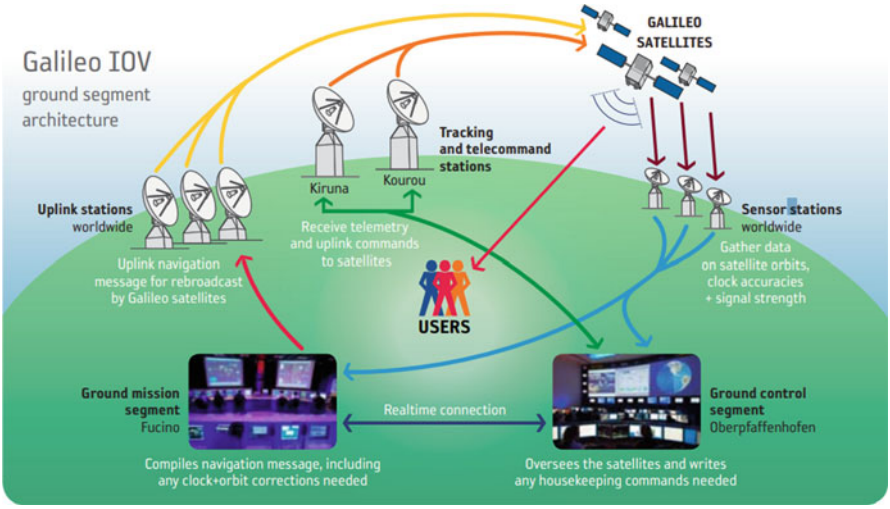


Fig. 7 Galileo ground segment architecture [8]

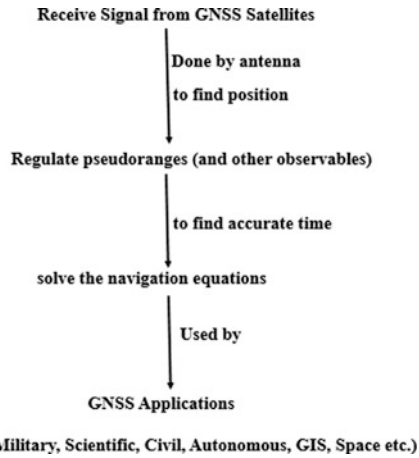


Fig. 8 User segment functions

function explained adequately. Whatever signal received from GNSS satellites with the aid of the antenna it merely finds the position using pseudorange measurement. This pseudorange measurement function phase called the antenna phase (refer to Sect. 2.2). After that, it will solve the navigation equation for finding time accuracy and then it transmitted successfully to various sectors of the GNSS applications. The GNSS applications used in sectors like civil application, modern agriculture, road navigation, a military application like Joint Direct Attack Munition (JDAM) target attack, autonomous autopilot applications.

4 Regional Navigation Satellite System

There is three regional navigation satellite system (RNSS) are available namely BDS-1 conform china already discussed in Sect. 2.1. Next, NAVigation with Indian Constellation (NAVIC) from India and Quasi-Zenith Satellite System (QZSS) from Japan. The following section discusses the NAVIC and QZSS project development, orbit plan, and its operations.

4.1 NAVigation with Indian Constellation (NAVIC)

In 2006, the Indian Regional Navigation Satellite System (IRNSS) approved the project developed by the Indian Space Research Organisation (ISRO) under the control of the Indian government. The operational name of IRNSS is NAVIC. The NAVIC complete details are explained in Fig. 9, like coverage mainly for Indian border territories and orbit as GSO circular path and services. NAVIC has two types of services restricted services for defense and standard position service for civilians. This constellation includes eight independent India self-made satellites namely IRNSS-1A, IRNSS-1B, IRNSS-1C, IRNSS-1D, IRNSS-1E, IRNSS-1F, and IRNSS-1G and IRNSS-11 in that first four satellites are in GSO orbit [16]. The next batch spacecraft are IRNSS-1J, IRNSS-1K, IRNSS-1L, IRNSS-1M, and IRNSS-1N are under the planning process. India also plans to develop a global navigation satellite system. The project name is Global Indian Navigational System (GINS) which has a constellation of 24 satellites and a position 24,000 km above the earth.

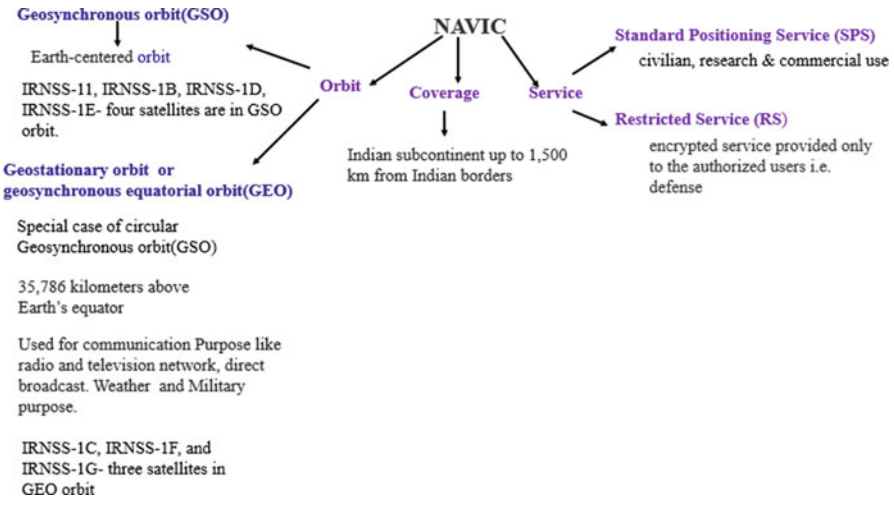


Fig. 9 NAVIC details

4.2 Quasi-Zenith Satellite System (QZSS)

In 2002, under the space development program, the Japanese government authorized a regional navigation satellite system as the Quasi-Zenith Satellite System (QZSS) [17]. QZSS satellites orbited in two orbits namely Highly Elliptical geosynchronous Orbit (HEO) and Geo-stationary Orbit (GSO). Three satellites placed in periodic HEO also called Quasi-Zenith Orbits (QZO) and four satellites in a GSO. These satellites cover the quasi-zenith region which includes East Asia and Oceania, and Japan region. The satellite orbited in HEO orbits are stable and every 8 h (3 satellite $\times$ 8 h $=$ 24 h) at least one satellite will go on over Japan. QZSS plans and development consist merely of three phases. In the first phase, quasi-zenith satellite QZS-1 which picks up a derisive nickname as Michibiki launched in 2010, by the Japan Aerospace Exploration Agency (JAXA) [18]. It orbited nearly 32,000–40,000 km altitudes. In the second phase, QZS-2 and QZS-3 also orbited in the corresponding orbit of QZS-1 [19]. There is two authorized body governing the QZSS operation. The commercial operation supported by Quasi-Zenith Satellite System Services Inc. (QSS). The research and development operations supported by JAXA.

QZSS architecture consists of two elements, namely space segment and ground segment. Currently, the space segment consists of four satellites. The ground segment includes two Master Control Station (MCS) located in Hitachi-Ota and Kobe. Approximately, 30 Monitoring Station (MS) and seven Tracking and Controlling Stations (TCS) and other country research institutes are also part of the ground segment.

5 Signals

Each Satellite constantly emits the microwave radio signals towards the earth. These satellites are also called space vehicles. The satellite signals transmitted into a limited boundary area called the footprint as shown in Fig. 10. The ground stations those within boundary area it means within the footprint area only receive the satellite signals. The direct communication between satellite and earth signal links called uplink frequency and downlink frequency [20].

Through signal, the communications exchanged between a ground station in the earth and the satellite. This transmitting signal name is uplink frequency. The ground station signal received by satellite antenna. The signal from the satellite to the ground station termed downlink frequency. As explained in Fig. 11, both satellite and ground stations equipped with more components involved in generating, receiving, and transmitting signal processes [20]. Each signal includes three components carrier signals, ranging code, and navigation data. The carrier signal is an electromagnetic pulse or wave. Each satellite transmits two sinusoidal carrier signals in the waveform, like Long-band (L-band) namely L1 and L2. The

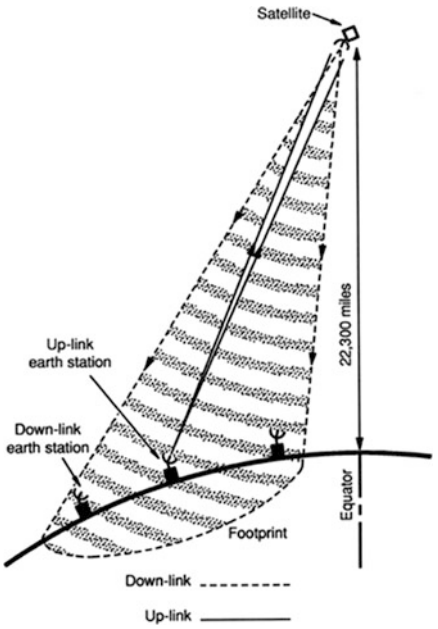


Fig. 10 Uplink and downlink direction [20]

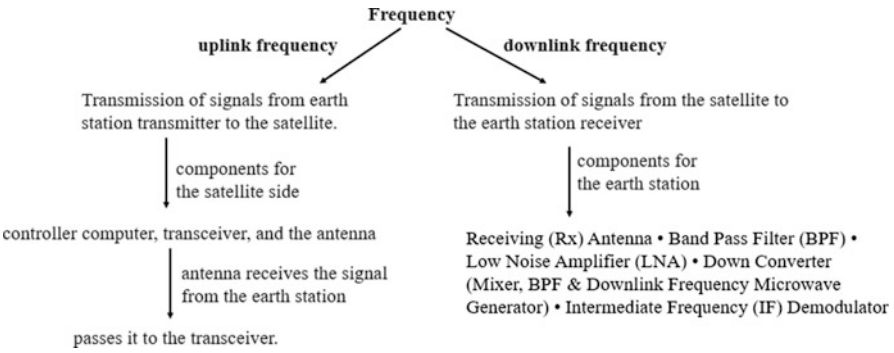


Fig. 11 Uplink and downlink frequency components

frequency of L1 is 1575.42 MHz and L2 1227.60 MHz [21]. The number of waves passing in a specified interval called frequency. The frequency measurement by hertz abbreviated as Hz. One hertz measured by the number of times sound wave repeats every second or one cycle per second. One thousand hertz as kHz and one million hertz as MHz, in Fig. 12 various frequency measurement information, are available. These carrier signals used for radio communication.

Band names differentiated by frequency range. For Example, L Band (long wavelength) frequency range is 1.2–1.8 GHz. And Ku-band exploits approximately 12–18 GHz. The Ka-band services are 26.5–40 GHz in the electromagnetic spectrum. Many radio frequency ranges like C, X, Ku, Ka, and even EHG

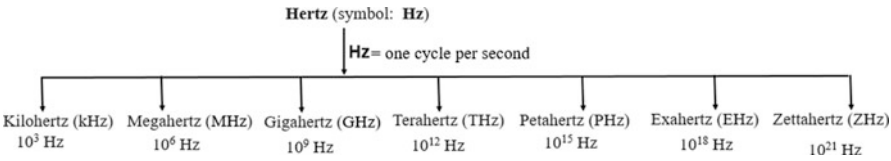


Fig. 12 Frequency measurement

and V-band used in satellite communication. These waves categorized into radio waves, microwaves, infrared, visible light, ultraviolet, X-rays, and gamma rays. The Frequency and wavelength are inversely proportionate. Whenever frequency increases then wavelength decreases. If the wavelength is high than the receiving satellite antenna size should be large [21].

The radio wave consists of time and position. Time indicates when the continuous signal transmitted based on the atomic on-board clock. This process called a ranging code. These ranging codes consist of sequences of zero and one. Each sequence number called Pseudorandom Noise (PRN) sequences or PRN codes. The two schemes of PRN, Coarse/Acquisition (C/A) code, and restricted Precision (P) code. C/A code is a free scheme and used for the civilian. P-code is typically reserved for defense applications. The P(Y) code is an encrypted format of restricted precision (P) code. Each satellite in the constellation has a unique space vehicle number. PRN codes used for identifying each satellite signal in the constellation. And every operating space vehicle has a space vehicle identifier [22].

The orbit position of the satellite considered position. Satellite signal travels at the speed of light called velocity. This information called navigation data. The overall process called Navigation Signal Generation Unit (NSGU). The analog signals are from NSGU and then passing through the L-band converter and power amplifier. The microprocessor control modules and Navigation Signal Generation (NSG) modules are two modules in NSGU. The microprocessor control module used for a power converter. The high-speed navigation signals generated by the NSG modules.

6 Satellite Technology

Launching expenses depend upon their satellite heaviness and size. Therefore, the satellite should be light weighted and small. At the same time, reliable technology and durable material need for designing such types of satellites. The entire lifespan the satellite function in orbit is nonstop. For nonstop functioning, it generates power using solar panels. The batteries are recharged by solar panels whenever sunlight is available in the orbit. For tedious work, the satellite needs high-end technology.

6.1 Satellite Navigation Augmentation Technology

In general terms, the augmentation increases the process of quality and values by resolving errors. In GNSS augmentation technology is a method in geosynchronous satellite systems which will detect the satellite signal errors. Simultaneously, it will do transfer correction and then uplinked to the Satellite Based Augmentation Systems (SBAS) satellite [23]. Corrections are aware to calculate ionospheric delay, satellite timing, and satellite orbits. On that occasion, it will broadcast to GNSS receivers for corrections. Next, it will apply throughout the SBAS coverage area for improving the navigation system's accuracy, reliability, and availability in user application. In Fig. 13, the classification of augmentation technology details available. All three system SBAS, GBAS, and ABAS base functionality detecting and rectifying signal errors. Because GBAS doing integrates monitoring using control system previously explained in Fig. 5. As explained in Fig. 13, these systems mostly used by airport applications [24].

SBAS is a well-known augmentation system in the satellite navigation system. The SBAS segment functions flow shown in Fig. 14. Two key stations are monitor stations and master stations in the SBAS segment. Monitor station receiving the signal from GNSS satellites. After collecting the signal frequency code and the pseudorange, it will observe and repair the errors in the dual-frequency carrier. After the resultant navigation message synchronized pseudorange code forwarded to the master station. The master station key task to include various correction processes like long-term correction, fast correction, and ionospheric correction. The purpose of these many corrections to improve GNSS accuracy of position. After completing the correction process, the SBAS augmentation message passes to the earth station. Through earth station, this message uploaded to satellite and then as download link

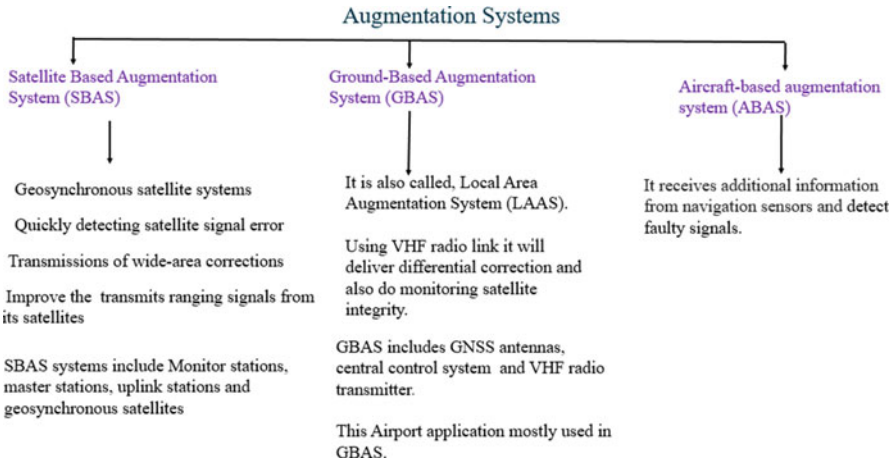


Fig. 13 Classification of augmentation system

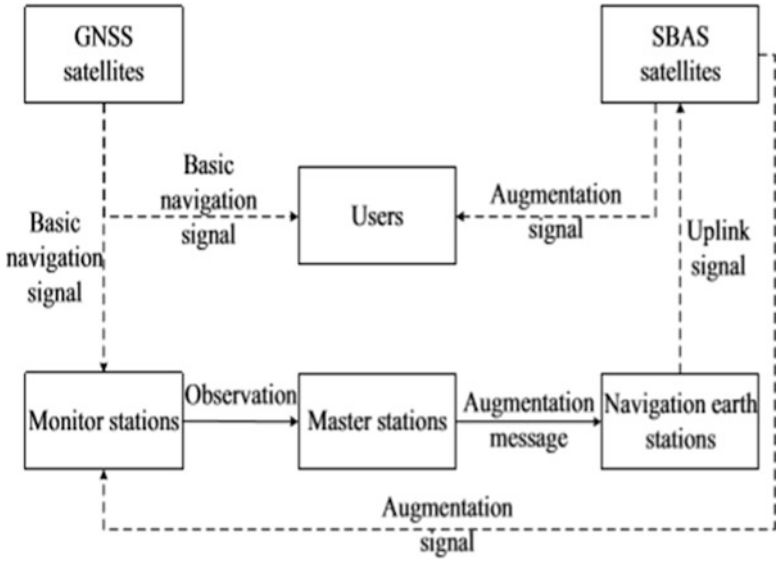


Fig. 14 SBAS function [21]

Table 3 SBAD services and countries

SBAS services	Country
Wide area augmentation system (WAAS)	US Federal Aviation Administration (FAA)
European geostationary navigation overlay system (EGNOS)	European Commission (EC) and EUROCONTROL (European Organization for the Safety of Air Navigation)
Multifunctional satellite augmentation system (MSAS)	Japan
GPS-aided GEO augmented navigation (GAGAN) only payload is operational from 2015	Airports Authority of India (AAI) and Indian Space Research Organization (ISRO).
SNAS (Satellite Navigation Augmentation System)	Republic of China
System for Differential Corrections and Monitoring (SDCM)	Russian Federation

frequency signal it broadcast to end-user [21]. The SBAS services WAAS, EGNOS, and MSAS already in operation. GAGAN and SNAS and SDCM under planning construction. Each country SBAS service name and its country details are given in Table 3.

6.2 Test and Assessment Technology

In the GNSS, the key aspect is positioning performance and the receiver interprets. Testing and assessment procedure needed for improving explicit accuracy and quality. The list of GNSS testing's is:

- The receiver under test (RUT) checks the position performance of satellite navigation. This RUT combined with radiofrequency front-end system and local oscillator quality [25].
- NMEA 0183 standard verified for testing and evaluating GNSS receivers [26].
- To maintain extremely reliable signal communication and good quality links, the ground stations are performing unmanned aerial vehicle (UAV) technology (commonly known as drone technology) and VSTA antenna testing technology [27].

6.3 Fusion Technology

Direct Fusion Drive (DFD) engine was invented in early 2000 at Princeton Plasma Physics Laboratory (PPPL) by Samuel Cohen. The concept of DFD is to design low radioactivity and nuclear fusion rocket engines, especially for robotic spacecraft. The purpose of this technology to generate electricity with less radiation. DFD engine type is the most suitable plasma propulsion engine for long-distance spacecraft travel [28]. The interior of the plasma propulsion engine contains a combination of hot plasma of helium and deuterium and a special heavy hydrogen nucleus produces one neutron. These elements will fuse the plasma and generate massive energy is called aneutronic fusion. This engine expected to be operational in 2028.

6.4 Anti-interference Technology

Intentionally satellite signals disturbed are termed as jamming and spoofing. In Fig. 15, explained jamming and spoofing represent two types of satellite signal interference. Spoofing means, it transmits a fake signal from the ground station to the satellite. The impact of a fake signal, satellite receiver calculate the incorrect position and mislead the navigator. Next jamming, include more noise in the satellite signal. Due to overpowering the signal, it means a week signal doesn't allow the receiver to track the GNSS signal. As a result, it never allows the receiver to operate automatically receiver becomes inactive [29]. To control signal disturbances, the concerned researchers proposing anti-jamming and anti-spoofing algorithms such as antenna array power inversion algorithms [30]. This type of algorithm improves the

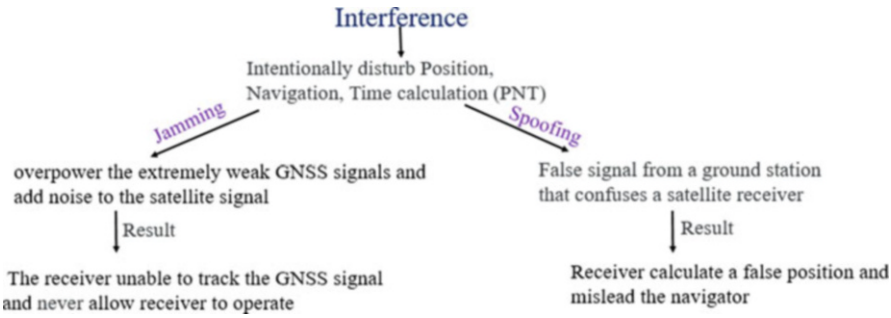


Fig. 15 Interference technology [29]

output signal-to-noise ratio (SNR). Another technology using metallic concentric rings techniques to compress the jammer electromagnetic wave signal.

6.5 High Precision Clock Technology

The Coordinated Universal Time (UTC) is normally using standard time by the entire world. UTC is a combination of International Atomic Time (TAI) and Universal Time (UT). The international atomic time utilized for exposing local time around the globe using an atomic clock. Universal time (UT) based on the average speed of earth rotation. For GNSS, the accurate and stable precision atomic clock as critical equipment for providing Space-Time Reference (STR). Each satellite in the constellation contains multiple atomic clocks. For example, each GPS satellite includes four atomic clocks. Each atomic clock generates accurate precise time data to the satellite signals. The satellite receiver decrypts these signals effectively and synchronizing each receiver to the atomic clocks. This synchronization is helpful for worldwide trade. Especially to decide the financial market transaction timestamp, power grid, and communication system [31].

In the atomic clock, the commonly used basic atom components are pendulum and cesium. Cesium atomic clock accuracy defined as a possible error of 1 s every one-hundred million years or so. The various distinct precision clock types are cesium atomic clock, hydrogen maser clock, and rubidium atomic clock. The maser device which stimulates the radiation emission. The maser device generates coherent monochromatic electromagnetic radiation in the microwave range. The hydrogen maser device is a primary atomic master clock. It performs a function as the stable frequency source using an atomic frequency standard and additionally serves as a backup frequency source. The first Passive Hydrogen Maser (PHM) is the master clock used in orbit with GIOVE-B (Galileo satellite's payload) [32].

The rubidium atomic clock (Rb) using rubidium atoms. It controls output frequency standard namely Rubidium Atomic Frequency Standard (RAFS). The

RAFS standard is to specify the hyperfine transition of electrons in rubidium-87 atoms using optical pumping technique to measure the atomic transition frequency. GPS and Glonass are utilizing this type of clock [33].

In 2011 Symmetricom Inc. introduced the first commercially cesium Chip scale atomic clocks (CSAC) with model number SA.45 in the market [34]. This project development started in 2004 by the Defense Advanced Research Projects Agency (DARPA) and the National Institute of Standards and Technology (NIST). This is the first generation chip-scale has admittedly limited performance. NIST and Honeywell's extensive research, progress on the Atomic Clock with Enhanced Stability (ACES) program is next-generation assembling atomic clock technologies at the wafer scale. Which is most cost-effective, at the same time its battery-power CSACs with 1000× improvement in key performance restrictions than the exiting chip atomic clock.

In 1949 the first atomic clocks developed by the U.S. National Institute of Standards and Technology (NIST). It absorbs ammonia, it is not that much accurate than currently using a cesium standard atomic clock. In 1955, the National Physical Laboratory (UK) developed the currently using accurate cesium standard atomic clock. Various countries like Singapore, Hong Kong, Poland, and Japan started the manufacturing of the cesium atomic clock. Hydrogen maser is manufacture by Indonesia, Japan, and Colorado. It is under process in India, the Space Application Centre (SAC) is developing an atomic clock.

7 Satellite Applications

Predominantly satellite applications used to determine an earth location for communication. The international telephony most established technology of satellite communication application. Telephone technology transmitting an electrical signal for interactive audio and video communication between distinct destinations. Especially this technology primarily adopted in ships and airplanes for the connection of uplink signals of the satellite. Approximately, more than 2000 communications satellites are in earth orbit. The radio and television broadcasting using the Direct Broadcast Satellite (DBS) and fixed service satellite (FSS) application. FSS operates more limited bandwidth than DBS [35]. Amateur radio satellite is an artificial satellite used by free of charges for licensed radio operators for voice FM and SSB. These satellites transmitting signals using amateur radio frequency between Orbiting Satellite Carrying Amateur Radio (OSCAR) and amateur radio station.

Agriculture and Farming are not only creating a natural environment, but it is also a source for everyone living on the earth. Earth observation satellite (EOS) used in the agriculture sector in farming management called precision agriculture (PA) or satellite farming [36]. This application is session decision support for farmers to identify the water resources and manage agriculture precisely by the weather forecast and soil information, yield estimation and educating knowledge in pest incidence frequency, etc., Normalized difference vegetation index (NDVI) is

a graphical indicator used for analyzing remote sensing standardized measurement of the crop [37, 56] . This method practiced in remote agriculture farms to detect an unhealthy plant and healthy plant stamina. For calculating the density of green in Farm the NDVI exploited various near-infrared sunlight reflected by the plants.

The satellite imagery is a collection of earth planet images. Some of the satellites like MODIS, Sentinel, Aster, GeoEye, and DigitalGlobe have taken high-resolution satellite imagery. For forecasting the atmosphere, the meteorology department using satellite images. Some popular satellite imagery tools are USGS earth explorer, land viewer, Copernicus open access hub, and sentinel hub.

Landsat8 is an earth observing satellite type. It orbited in circular sun-synchronous polar orbit. It launched in 2013, specifically for monitoring current water resources using the Thermal Infrared Sensor (TIRS) and Operational Land Imager (OLI) sensor. This sensor used for estimating mineral exploration, and soil moistures [38, 57]. Cartography satellite mapping comprises a core component of modern satellite mapping technology. For easy online accessing the mapping applications such as google earth and Bing maps are using satellite data [39]. Space-based laser constellations comprise combinations of SBL satellites. This satellite used in the field of satellite imagery processing. Automatic image registration (AIR) has been an extensive study in the fields of medical imaging, computer vision, and remote sensing using satellite images. The image registration (IR) process, which will determine the spatial transformation that maps the points in the sensed image to the points in the reference image [40, 58].

The underwater depth of ocean study is considered Bathymetry. In the ocean or marine navigation geostationary operational environmental satellite-16 (GOES-16) are the first U.S. National Oceanic and Atmospheric Administration (NOAA) next-generation geostationary weather satellites [41]. This type of satellite collecting information about the ocean and aiding the field of ocean bathymetry. This field of study includes sea surface temperature, ocean color, coral reefs, and migration of whales. It is not only hospitable in sea living and also for humane society for emergency beacons which assists the fisherman in a boat, airplanes in the remote area.

Predominantly, most of the innovative technology used by defense purposes. Then gradually, the common public is allowed to use technology. For example, the internet and computer technology primarily used by the defense. In the same manner, the early stages satellite technology used for defense mission especially for the war on terror. The U.S. regularly launching missiles for defense tracking satellites. Boeing X-37 is a reusable robotic spacecraft that can return to earth from orbit. The next-generation satellite technology X-37B speed above the earth 28,040 km/h. It also knows as the Orbital Test Vehicle (OTV) [42]. Already OTV1, OTV2 up to OTV5 mission is successfully landed. The United States and Russia and China these countries are substantially having spy satellites. The U.S. defense additionally using Ultra High-Frequency Follow-On system (UFO) satellite communication for Navy based ground voice and data communication across the continent for war operations [43, 59].

8 Conclusion

The countries those who launched and active the GNSS system constantly updating the technology. Based on technology policy updating also an essential part of GNSS. European Space Agency (ESA) and NASA Interagency, Tracking, Communications, and Operations Panel (ITCOP) decided to form a multi-agency forum in the meeting called Inter-Operability Plenary (IOP). In 1999, the first IOP (IOP-1) meeting established the Operations Advisory Group (IOAG) forum. In the IOAG forum, the multi-space agencies discuss the space communications policy, high-level procedures, and technical interfaces. The goal of the IOP meeting to accomplish the multi-agency agreement to share or joint space communication and navigation. Agency members should support and share navigation resources and deep space missions [44, 60].

In 2005, the United Nations (U.N.) established the International Committee on Global navigation satellite systems (ICG). ICG recommendations encourage the providers, agencies, and research organizations to publish details of GNSS. The GNSS space users to contribute services related to civil satellite-based positioning, navigation, timing, and value-added services to the IOAG database. IOAG license agencies or ICG Working Groups (WG) encourages the IOAG database to be up-to-date. Two types of membership in the IOAG forum, full and observer members. The full member can claim voting rights. But observer members don't possess voting rights. The full member agencies list as given at the end, the number of member of each agency details are available in Fig. 16. The Fig. 16 also gives details about number of times each agency updated the IOAG database in the year 2018 and 2019 [44, 45, 60]:

- Agenzia Spaziale Italiana (ASI)
- Canadian Space Agency (CSA)
- Centre National d'Etudes Spatiales (CNES)
- Deutsches Zentrum für Luft- und Raumfahrt (DLR)
- European Space Agency (ESA)
- Japan Aerospace Exploration Agency (JAXA)
- National Aeronautics and Space Administration (NASA)
- Korea Aerospace Research Institute (KARI)

The observer's members are:

- China National Space Administration (CNSA)
- Indian Space Research Organisation (ISRO)
- Russian Federal Space Agency (RFSA)

There is no doubt; navigation technology is the looming next-generation technology. Conspicuously, more research journals are available in this field to reform researcher knowledge. Some of the established journals noticed at the end in the navigation field are:

Fig. 16 IOAG agency country details [44]

IOAG Missions & Programs Relying on GNSS

Agency	Country	2018	2019
ASI	Italy	4	4
CNES	France	10	10
CSA	Canada	5	5
DLR	Germany	11	7
ESA	Europe	17	18
JAXA	Japan	12	12
KARI	Republic of Korea	-	8
NASA	USA	43	44

- NAVIGATION: Journal of the Institute of Navigation
- Advances in Space Research: Elsevier
- Journal of Space Exploration: Trade Science Inc.

At the same time, for pioneering knowledge to attend technical meet and conferences, and panel discussion and showcases about products and services will give more gain under one roof. In this field, more events and conferences conducted almost every month worldwide. Some of the events are Multi-GNSS Asia (MGA) conferences in Asia Oceania region, International conference on GIS and remote sensing, the institute of navigation (ION) arranges huge international GNSS related product showcases, and innovative research in technical meetings.

Concluding this chapter is difficult. Since this field is completely dominating and also widespread technology for every object present on the earth. For modern life, technology domination consecutive ever-ending process. Naturally, the human mentality to detect the secrecy of space. As well as to find, unknown findings from the known planet. The sky represents a maximum height for any achievement. In the field of navigation, technology is apart from sky height and boundlessly mounting.

References

1. Lee, J.: Introduction to navigation systems. In: Rustamov, B.R. (ed.) Multi-purposeful Application of Geospatial Data. Intechopen, London (2018)
2. Electronics Technician-Volume 05—Navigation Systems: US Navy Training Course.http://electronicstechnician.tpub.com/14090/css/Electronic-Navigation-12.htm (2014). Accessed 23 Mar 2020
3. Navigation Systems and Equipment. Surface Officer Warfare School Documents. https://fas.org/man/dod-101/navy/docs/swos/e1/MOD4LES4.html. Accessed 20 Mar 2020
4. Shi, C., Wei, N.: Satellite navigation for digital earth. In: Guo, H., Goodchild, M., Annoni, A. (eds.) Manual of Digital Earth. Springer, Singapore (2020)

5. Mirgorodskaya, T.: Global Navigation Satellite System (GLONASS): status and development. Paper Presented at the UN-Nepal Workshop on the Applications of Global Navigation Satellite Systems, Kathmandu, Nepal (2016)
6. Liu, L., Zhang, T.: Improved design of operational system in BDS-3. Navigation. **66**(1), 37–47 (2019). https://doi.org/10.1002/navi.297
7. China Satellite Navigation Office: Development of the BeiDou Navigation Satellite System (Version 4.0). http://m.beidou.gov.cn/xt/gfxz/201912/P020191227430565455478.pdf (2019). Accessed 4 Jan 2020
8. Blair, S., EJR-Quartz: Birth of the European Satellite Navigation constellation. Galileo in-orbit. An ESA communications Production. Noordwijk, Netherlands (2011)
9. He, C., Lu, X., Guo, J., et al.: Initial analysis for characterizing and mitigating the pseudorange biases of BeiDou navigation satellite system. Satell. Navig. **1**, 3 (2020). https://doi.org/10.1186/s43020-019-0003-3
10. Alhmiedat, T.A., Abutaleb, A., Gassan Samara, G.: A prototype navigation system for guiding blind people indoors using NXT Mindstorms. Int. J. Online Eng. **9**(5), 52–58 (2013)
11. Jeffrey, C.: An Introduction to GNSS: GPS, GLONASS, Galileo and Other Global Navigation Satellite Systems, 1st edn. Novatel Inc., Canada (2010)
12. Regan, R.D.: Satellite technology. https://www.encyclopedia.com/computing/news-wires-white-papers-and-books/satellite-technology (2020). Accessed 22 Mar 2020
13. Subirana, S.J., Zornoza, J.M.J., Pajares, M.H.: GNSS Data Processing, Volume I: Fundamentals and Algorithms. ESA Communications, Netherlands (2013)
14. GPS Control Segment Map: Vandenberg AFB, California. https://www.gps.gov/multimedia/images/GPS-control-segment-map.pdf (2017). Accessed 23 Mar 2020
15. European Global Navigation Satellite Systems Agency: European GNSS Service Centre, Czech Republic. https://www.gsc-europa.eu/galileo/system (2020). Accessed 2 Feb 2020
16. Department of Space, Indian Space Research Organisation: Indian Regional Navigation Satellite System (IRNSS): NavIC Tender for NacIC Receiver Module Development. https://www.isro.gov.in/irnss-programme (2019). Accessed 20 Mar 2020
17. GPS Ground Segment: Navipedia: The GNSS Wiki. https://gssc.esa.int/navipedia (2011). Accessed 4 Jan 2020
18. Cabinet Office, National Space Policy Secretariat: What is the Quasi–Zenith Satellite System (QZSS)? https://qzss.go.jp/en/overview/services/sv02_why.html (2020). Accessed 18 Mar 2020
19. Harima, K., Choy, S., Kakimoto, H., Kogure, S., Collier, P.: Utilisation of the Japanese Quasi-Zenith Satellite System (QZSS) Augmentation System for Precision Farming in Australia. In: International Global Navigation Satellite Systems Society IGNSS Symposium 2015, Outrigger Gold Coast, QLD, Australia (2015)
20. Chick, W. Boyle, A., Halfman, M., Poynton, M.: How Satellite Work. http://www.physics.udel.edu/~watson/scen103/projects/99s/satellites/howtheywork.html (1999). Accessed 19 Mar 2020
21. Li, R., Zheng, S., Wang, E., et al.: Advances in BeiDou navigation satellite system (BDS) and satellite navigation augmentation technologies. Satell. Navig. **1**, 12 (2020). https://doi.org/10.1186/s43020-020-00010-2
22. Dardari, D., Falletti, E., Luise, M.: Satellite and Terrestrial Radio Positioning Techniques: A Signal Processing Perspective. Elsevier (2011). https://doi.org/10.1016/C2009-0-61856-0.
23. United space in Europe: Augmented satnav teams work together for safer flying. https://www.esa.int/Applications/Nvigation/Augmented_satnav_teams_work_together_for_safer_flying (2020). Accessed 20 Mar 2020
24. IIT Bombay Student Satellite Project. https://www.aero.iitb.ac.in/satelliteWiki/index.php/Downlink (2018). Accessed 15 Mar 2020
25. Vinande, E.T., Weinstein, B., Chu, T., Akos, D.: GNSS receiver evaluation record. GPS World. **21**(1), 28–34 (2010)

26. Han, O.W., Subari, M.D.: GNSS Receiver's Testing: Study of GPS Test Software. Available via Geospatial World. https://www.geospatialworld.net/article/gnss-receivers-testing-study-of-gps-test-software/ (2009). Accessed 18 Mar 2020
27. Lim, C., Yoon, H., Cho, A., Yoo, C.-S., Park, B.: Dynamic performance evaluation of various GNSS receivers and positioning modes with only one flight test. Electronics. **8**, 1518 (2019). https://doi.org/10.3390/electronics8121518
28. Wall, M.: Fusion-powered spacecraft could be just a decade away. https://www.space.com/fusion-powered-spacecraft-could-launch-2028.html (2019). Accessed 12 Feb 2020
29. Dobryakoval, L., Lemieszewski, L., Ochin, E.F.: Method, algorithm and implementation of vehicles GNSS information protection with help of anti-jamming and anti-spoofing. Paper Presented at the Proceedings of the 2nd International Workshop on Radio Electronics & Information Technologies, Yekaterinburg, Russia (2017)
30. Yang, Q., Yi, Z., Tang, C., Lian, J.: A combined antijamming and antispoofing algorithm for GPS arrays. Hindawi Int. J. Antennas Propagat. (2019). https://doi.org/10.1155/2019/8012569
31. Official U.S. Government Information about the Global Positioning System (GPS) and Related Topics: Application: timing. https://www.gps.gov/applications/timing/ (2019). Accessed 17 Mar 2020
32. Hugentobler, U., Plattner, M., Heinze, M., Klein, V., Voithenleitner, D.: Optical clocks in future global navigation satellites. EFTF, Paper Presented at the 24th European Frequency and Time Forum (2009)
33. Rochat, P., Droz, F., Wang, Q., Froidevaux, S.: Atomic clocks and timing systems in global navigation satellite systems. Paper Presented at the European Navigation Conference, Gdansk, Poland (2012)
34. Smithsonian: Commercial Chip Scale Atomic Clock (CSAC). https://timeandnavigation.si.edu/multimedia-asset/commercial-chip-scale-atomic-clock-csac (2012). Accessed 18 Mar 2020
35. Pakistan Space & Upper Atmosphere Research Commission: Application of satellites. http://www.suparco.gov.pk/pages/applications-satellite.asp (2020). Accessed 23 Mar 2020
36. Agriculture and Horticulture Development Board: Satellites for agriculture. https://ahdb.org.uk/knowledge-library/satellites-for-agriculture (2018). Accessed 18 Mar 2020
37. Igor, I.: How satellites are making agriculture more efficient. https://medium.com/remote-sensing-in-agriculture/how-satellites-are-making-agriculture-more-efficient-4b8dc6d443bf (2017). Accessed 8 Mar 2020
38. Micromine Intuitive Mining Solutions: Satellite imagery in mineral exploration: Part I. https://www.micromine.com/satellite-imagery-in-mineral-exploration-part-1/ (2015). Accessed 2 Mar 2020
39. Pillai, N.A.: Five applications of satellite data. https://www.gislounge.com/five-applications-of-satellite-data/ (2015). Accessed 2 Mar 2020
40. Chen, Q., Wang, S., Wang, B., Sun, M.: Automatic registration method for fusion of ZY-1-02C satellite images. Remote Sens. **6**(1) (2013). https://doi.org/10.3390/rs6010157
41. NOAA: How are satellites used to observe the ocean? https://oceanservice.noaa.gov/facts/satellites-ocean.html (2017). Accessed 2 Mar 2020
42. Lee, R.J., et al.: Military use of satellite communications, remote sensing, and global positioning systems in the war on terror. J. Air L. Com. **79**(1) (2014). https://scholar.smu.edu/jalc/vol79/iss1/2
43. Malik, T.: Space.com. https://www.space.com/topics/military-space (2018). Accessed 2 Mar 2020
44. Parker, J., Miller, J.J.: NASA GNSS Space User Update. Paper Presented at the ICG-14 Working Group B, National Aeronautics and Space Administration (2019)
45. IOAG PROCEDURES MANUAL: Procedures Manual for the Interagency Operations Advisory Group (IOAG). https://www.ioag.org/Public%20Documents/IOAG%20Procedures%20Manual.pdf (2013). Accessed 20 Mar 2020
46. Munawer, H.A.: Satellite communications tutorials. http://www.just.edu.jo/~hazem-ot/Session%206_%20Space%20segment.pdf (2016). Accessed 23 Mar 2020

47. Moore, T.: GNSS Modernisation and future developments. In: Geospatial Research and Applications Centre of Excellence (GRACE). The University of Nottingham. Accessed 26 March 2020 (2001)
48. International Civil Aviation Organization: Global Navigation Satellite System (GNSS) Manual, 1st edn, Canada (2005)
49. Barwacz, A.: Augmented satnav meeting focuses on future development. Available via GPS GNSS position Navigation Timing World. https://www.gpsworld.com/augmented-satnav-meeting-focuses-on-future-development/ (2020). Accessed 23 Mar 2020
50. Boulton, P., Borsato, R., Butler, B., Judge, K.: GPS interference testing: lab, live, and lightsquared, Inside GNSS. https://insidegnss.com/gps-interference-testing/ (2011). Accessed 10 Mar 2020
51. Salim, A., Tripathi, S., Tiwari, R.K.: Applying geo-encryption and attribute based encryption to implement secure access control in the cloud. Int. J. Comput. Networks Commun. **11**(4) (2019). https://doi.org/10.5121/ijcnc.2019.11407
52. Berceau, P., Taylor, M., Kahn, J., Hollberg, L.: Space-time reference with an optical link. IOP Class. Quantum Gravity. **3**(13) (2016). https://doi.org/10.1088/0264-9381/33/13/135007.
53. Xie, W., Huang, G., et al.: Characteristics and performance evaluation of QZSS onboard satellite clocks. Sensors. **19**(23), 5147 (2019). https://doi.org/10.3390/s19235147
54. Rajiv: What are satellite navigation systems and applications. https://www.rfpage.com/what-are-satellite-navigation-systems-and-applications/ (2018). Accessed 8 Mar 2020
55. By Inside GNSS: GNSS and Inertial Manufacturers Team for Rapid, High-Volume Supply.https://insidegnss.com/gnss-and-inertial-manufacturers-team-for-rapid-high-volume-supply/ (2019). Accessed 1 Mar 2020
56. Igor I (2017) How Satellites Are Making Agriculture More Efficient. https://medium.com/remote-sensing-in-agriculture/how-satellites-are - making-agriculture-more-efficient-4b8dc6d443bf. Accessed 8 Mar 2020
57. Micromine Intuitive Mining Solutions (2015). Satellite imagery in mineral exploration: Part I. https://www.micromine.com/satellite-imagery-in-mineral-exploration-part-1/. Accessed 02 Mar 2020.
58. Chen, Q., Wang, B., Sun, M.: Automatic Registration Method for Fusion of ZY-1-02C Satellite Images. Remote Sensing. Special Issue Satellite Mapping Technology and Application. **6**(1) (2013). https://doi.org/10.3390/rs6010157
59. Malik T (2018) Space.com https://www.space.com/topics/military-space. Accessed 2 Mar 2020
60. Parker J, Miller JJ (2019). NASA GNSS Space User Update. Paper presented at the ICG-14 Working Group B, National Aeronautics and Space Administration , 10 Dec 2019.

Bluetooth Low Energy (BLE) Beacon-Based Micro-Positioning for Pedestrians Using Smartphones in Urban Environments

Raiful Hasan and Ragib Hasan

1 Introduction

Smart devices and digital technologies have changed our day to day lives. The multi-functional devices are increasing the computation power and the ability to do the task than ever before, for example, the smartphone, smartwatch, etc. The smartphone has revolutionized the communication way and changed the concept of personal computers [1]. In modern life, people use smartphones for various purposes besides talking and texting, including entertainment, navigation, safety systems, as a monitoring device, etc. Statistics show more than three billion people currently use the smartphone in the world [2]. The smartphone is the booming industry, and in the future, this device will be attached to our daily lives permanently. Moreover, smart cities are providing more services that are accessible to the smartphone. The manufacturers are adding smart technologies and functions to the phone to make compatible with those services. For example, the city provides the condition of the roads to residents beforehand to avoid traffic congesting and increase mobility, the weather condition, block by block air quality, amenities finding, and so on [3–6]. In addition, various researchers are discovering new ways to help peoples with disabilities, especially those who have a visual impairment [7]. However, location accessibility and the internet is required for most of these services. The Global Positioning System (GPS) is a widely used technology for navigation, localization, tourism, and engineering. The accuracy of GPS depends on a strong signal between the user and the navigational satellite. The lack of GPS signals in the indoor environment and the horizontal error of accuracy in outdoor often limit its uses.

R. Hasan (✉) · R. Hasan
Department of Computer Science, University of Alabama at Birmingham, Birmingham, AL, USA
e-mail: raiful@uab.edu; ragib@uab.edu

S. Paiva (ed.), *Precision Positioning with Commercial Smartphones in Urban Environments*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-71288-4_6

For that, the quality of GPS data collected using smartphones is not comparable with the dedicated GPS receiver. There is a trade-off between accuracy and battery consumption of smartphones for positioning.

Beacon technology with other IoT is integral now in smart cities to accomplish sustainability and accessibility. Both the industrial and public sectors are adopting this technology to easing civic life. For example, the City of Columbus, Georgia, USA, established a network containing more than 1000 beacons at the Chattahoochee Riverwalk. The city police will be notified of the location by this network if there is any suspicious activity occurred [8]. According to a report from ABI Research (a US technology market intelligence company), more than 500 million beacons will have been shipped by 2021 [9]. In 2013, Apple first popularised these geo-location transmitters; it is designed to interact with Bluetooth enabled devices, such as smartphones, tablets, cars, etc. There are already over 8.2 billion Bluetooth-equipped devices globally, and that number does not include just tablets and smartphones. Over 90% of vehicles released in 2016 were expected to have the technology [10]. Cities are using beacon technology to solve one of the most visible consequences of urban population growth; transportation, and traffic congestion. Different bodies of the city embedding these devices independently. For example, the emergency management department, traffic management, police, waste management, etc. In addition, private companies, such as Walmart, Macy's, Apple inc, etc., installing beacons at their stores for better customer engagement, navigation, advertising purpose. The debate between BLE, WiFi, and GPS in terms of accuracy, energy, and accessibility is not new. But in urban life, when the users need to handle the micro-location proximity-based activities, the BLE beacons give better accuracy in those activities. In addition, though smartphones are invaluable in daily life nowadays. Their battery consumption limits their usefulness, which provokes frequent charging. The companies are struggling with power consumption in GPS technology. Many mobile devices use Bluetooth Low Energy (BLE) technology to realize wireless communication connections to address this problem.

Contributions The contributions of this paper are as follows:

1. We proposed a generic architecture in an urban environment using beacons and smartphones for micro-positioning.
2. We provided an access-control based mechanism which allows implementing and operating such a system by protecting user privacy.
3. We set up a testbed in urban areas using BLE beacons and smartphones. The results show it improves the horizontal error by 10–40%.

Organization The rest of this chapter is organized as follows:

- Section 2—Background of GPS and Bluetooth based positioning.
- Section 3—System requirements and architecture.
- Section 4—Test deployment.
- Section 5—Findings from the experiments.
- Section 6—Concluding remarks.

2 Background

Modern smartphones have the functionality for both Global Positioning System (GPS) and Assisted GPS (A-GPS). The GPS draws its information from the satellites orbiting the Earth. AGPS draws its information from local cell towers and enhances the performance of standard GPS on mobile devices connected to a cellular network [11]. However, GPS and A-GPS's position accuracy at the mobile is not accurate where GPS signals are weak or unavailable, especially in the urban areas [12]. Early study found the average location accuracy of GPS enabled devices (i.e., iPhone, iPod, iPad, etc.) between 108 and 655 m [13]. Mok et al. [14] found the accuracy is around 20 m in one study using GPS enabled devices. More recently, a study found that the smartphone's GPS accuracy is between 6–13 m [15]. However, this level of accuracy is often influenced by the characteristics of the landscape of the city. In addition, this accuracy can be achieved in the outdoor environment; usually, the GPS signal is not accessible in the indoor or a building.

BLE beacons have been using for tracking and positioning the people and assets for several years in the indoor. For example, Apple Inc. installed beacons in the 254 Apple Store in the United States to better customer experience. Using these beacons, they give the products, deals, and notifications to the customer. The department store chain Macy's installed over 4000 beacons in their stores in 2014 for the same reason as Apple Inc. To help the visually impaired people at London's Underground network, the Royal London Society for Blind People (RLSB's) developed an app called "Wayfindr" [16]. The application receives the signal from pre-installed beacons at the subway and provides the turn by turn audio navigation to the users. It also provides the obstacles information within the route to the user to avoid the collision. Multiple research has been conducted to get the proper indoor location using beacons [17–19]. Cheraghi et al. [20] designed a Bluetooth beacon-based navigation system for vision-impaired individuals, allowing them to use a Bluetooth enabled cell phone to describe topology and offering real-time notifications about large indoor spaces. Beak et al. developed an underground navigation system using Bluetooth beacon to facilitate mining operations [21]. Jung et al. [22] used the Bluetooth beacon to measure the transport time of mining equipment in underground mines.

2.1 Bluetooth Beacons

Bluetooth Low Energy (BLE) beacons or BLE beacons are small devices that broadcast wireless signals in a specific range to other electronic devices [23]. BLE beacon is a one-way communicator and cannot broadcast a large amount of data. It is part of Bluetooth 4.0 [24] and currently supports most of the Bluetooth enabled smartphones. The power consumption in BLE beacons technology is relatively low as it broadcast only a small size of data with the identifying information. These hardware devices are used in scenarios where energy consumption is more important

Fig. 1 Most of the modern smart devices now support the BLE beacons. The device receives the signal and take subsequent action accordingly

than data transfer speed. It does not know how many beacons or receiving devices are in the area, and it does not connect with them. An example of a high-level beacon operation is shown in Fig. 1.

A beacon broadcasts a signal to all nearby devices that can receive the Bluetooth signal, i.e., the devices with a Bluetooth receiver and the receiver is on. The receiver can catch signals from the devices and identify the distance from where the signal has come from. All modern smartphone supports BLE technology. For example, the Android phone newer than Jelly Bean (Android version 4.3) or iPhone newer than version 4 supports the BLE technology. Several BLE beacon manufacturer companies compete in the market, including Estimote[1], RadBeacon[2], BlueCats[3], Kontakt[4], Gimbal[5].

2.2 *BLE Beacons Protocols*

The standards of communication and message format are beacon protocols. There are different type of beacon protocols exists. iBeacon and Eddystone are the most popular. Both protocols have some specific terminology and standards.

[1] https://estimote.com.
[2] https://store.radiusnetworks.com.
[3] https://www.bluecats.com.
[4] https://kontakt.io.
[5] https://gimbal.com.

iBeacon: iBeacon introduced by Apple, was the first BLE beacon technology [25]. iBeacon broadcast four types of information:

1. **UUID:** Universally Unique Identifier, this is a 16-byte string used to differentiate a large group of related beacons.
2. **Major:** A 2-byte string, identifying a subset of beacons within a large group.
3. **Minor:** A 2-byte string, identifying a specific beacon within the subset.
4. **Tx Power:** Transmission Power is used to determine proximity (distance) from the beacon. TX power is defined as the strength of the signal exactly 1 m from the device.

Eddystone: Announced by Google, is another protocol that defines a BLE message format for proximity beacon messages [26]. The Eddystone protocol transmits these different frames-types:

1. **Eddystone-UID:** A 10-byte Namespace component and a 6-byte Instance component, which is used to identify the individual beacon.
2. **Eddystone-EID:** similar to UID, but "encrypted". Only authorized apps and services can make use of it.
3. **Eddystone-URL:** A short URL encoded directly into the packet.
4. **Eddystone-TLM:** telemetry data such as battery voltage, uptime, etc.

3 System Design

3.1 System Requirements

Our high-level goal in this research is to design a framework to determine position using a smartphone. The desired properties of our system include:

1. The system should work without any other communication medium in basic mode. On top of that, it can provide additional functionality with the help of other beacons and Internet.
2. The system should be portable. It would be deployed with minimal human cost and accessible to everyone.
3. The available beacons in a specific region should work combinedly where possible to get better accuracy.

3.2 System Components

There are three components of our proposed systems:

1. Bluetooth Low Energy Beacons.
2. A Mobile Application for the Users
3. A Backend Server.

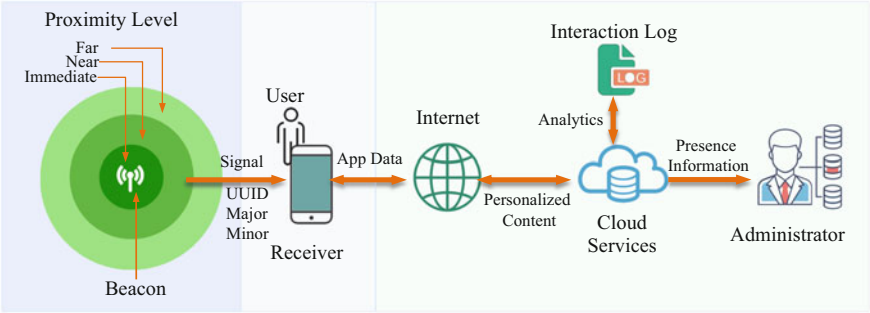


Fig. 2 A high-level architecture of the proposed system

There are two modes in the mobile application; the basic mode can work without communicating with the server; no other service (i.e., the Internet) is required for positioning. The advance mode sends data to the server and receives the data (i.e., ID, Type, etc.) for the beacons. In addition, we can remotely monitor the beacons by sending data to the server. Figure 2 shows the architecture of the system.

3.3 Mobile Application

The Bluetooth enabled devices can receive the beacon signal. For that, we have developed a mobile application to capture the signal and determine the position. We developed the application for both Android and iOS platforms. The android application supports Android 6.0 (Marshmallow) or the newer version, where the iOS supports the iOS version 12.1 or newer. In both versions, Bluetooth service permission is required. There are some benefits in the iOS versions; the OS handles the allocation (enables/disable) of required services. So it manages all the services in an efficient way. In contrast, in the Android application, the app requests the service, and OS gives permission to use it. So the application needs to handle it carefully. After calculates the nearest beacon from the multiple signals, the application shows the distance to the user. Figure 3 shows the mobile application for Android and iPhone.

3.4 Distance Calculation

BLE beacons offer excellent potential to calculate the distance. The Received Signal Strength Indicator (RSSI) represents the relationship between transmission and received power [27]. The signal strength depends on distance and Broadcasting Power value. The distance calculated in this project by the following formula:

Fig. 3 Mobile application interface, (**a**) Android Phone: shows the nearest beacon distance in a specific zone. (**b**) iPhone: shows the nearest Restroom

$$RSSI = -(10 \times n) log_{10}(d) + A$$

where, d = distance; A = txPower; and n = signal propagation constant. In this formula, RSSI is the radio signal strength indicator in dBm. In free space $n = 2$, but it will vary based on local geometry, for example, in urban areas, a wall will reduce *RSSI* by approximately 3dBm and will affect n accordingly. Upon receiving the signal, the smartphone application determines the approximate distance from the beacon with relative accuracy using the signal strength. The application must identify unique information about the beacons. Although, the distance calculations are performed in real-time, it takes some time (not more than 2 s) to receive the signal. The user can get an RSSI signal from the multiple beacons at the same time. However, it is crucial to determine the difference between multiple signals. In addition, the triangulation of multiple signals is also necessary to accurately detect a user's position and direction. For that, we need to calculate the ordering of the nearest distances. Algorithm 1 shows the procedure to find the nearest beacons.

Algorithm 1 Nearest Beacons

Input: Beacon Information
/*name, color, uuid, major, minor*/
Output: Nearest distances

```
Beacon beaconsOfInterest = filter(allBeacons, beaconIDs)
var filteredBeacons = NULL
for T in allBeacons do
    BeaconID = BeaconID.fromBeacon(T)
    if (beaconIDs in beaconID) then
        filteredBeacons.add(T)
    end if
end for
var nearBeacons = NULL
if (User in range of beaconsOfInterest) then
    for K in filteredBeacons do
        var distance = computeAccuracy(k);
        if distance > -1 and distance < CurrentNearest then
            nearBeacons.add(distance)
        end if
    end for
end if
return nearBeacons
```

3.5 User Direction Using Beacon-Signal and Time

We have calculated the direction of the user using the beacon signal and time. If the distance decreases with respect to the time, then the user is going toward the beacons. The direction will be opposite if the distance is increasing. We divide the beacon signals into three portions; immediate, near, and, far; where the most intense signal means immediate and far means the low signal.

3.6 Message Format and Server Communication

BLE beacon application communicate to the server through Application Programming Interface (API). As several beacons protocol is available, the server keeps identifiable pieces of information and signal data along with receiver sensor data. The application has to send the basic beacon data, such as UUID/EUID, Group information, distance, etc. Table 1 shows the required parameter to send data from the receiver application to the server:

Table 1 Message format for send data from the receiver to the server

ID → [APPLICATIONID]
PROTOCOL → [IBEACON, EDDYSTONE]
RECEIVER → [PHONE, CAR, WATCH, ...]
ACTION → [GET, POST]
FRAMEHEADER → [EVENTTYPE, SENDER, TIMESTAMP, PAYLOADSIZE]
EVENTTYPE → [EVENTTYPEDETAILS]
SENDER → [USERID, STATUS]
TIMESTAMP → [TIMESTAMP]
PAYLOADSIZE → [PAYLOADDATASIZE]
BEACONDATA → [BEACONGROUP, SUBSET, SPECBEACON, DISTANCES]
BEACONGROUP → [UUID, UID]
SUBSET → [MAJOR, EID]
SPECBEACON → [MINOR, URL, TLM]
DISTANCES → [DISTANCE 1, DISTANCE 2, ...]
DEVICEINFO → [SOURCE, DEVICESPEC, STATUS]
SOURCE → [ANDROID, IOS, WINDOWS, ...]
DEVICESPEC → [IMEI, MODEL, , HARDWARESPEC, ...]
STATUS → [ORIENTATION, IN USE, APPLICATIONS]
SENSORDATA → [MOTION, REGULAR]
REGULAR → [LIGHT, SOUND, ...]
MOTION → [ACCELEROMETE, GYROSCOPE, MAGNETOMETE, ...]

4 Test Deployment

To test the feasibility of the system, we have set up a testbed. The testbed contains multiple regions on an urban university campus, including traffic intersection localization, amenities positioning in the metropolitan area, detour alert, etc. The Bluetooth enabled devices captured these signals and detected the user positions. We used Bluetooth beacons developed by Estimote.[6]Broadcasting power for all of the beacons are set at +4 dBm, a power that is effectively expected to transmit signals at a distance of up to 100 m. This distance is sufficient for our setup. We have set the advertising interval to 100 ms because we need the most stable signal possible. Figure 4 shows installed beacons at the experimental site.

We continuously monitor battery life remotely using the Estimote cloud console and replace beacon batteries if needed. We used Amazon Web Services (AWS)[7] to store the data collected from users. We created an AWS Elastic Computer Cloud (EC2) virtual machine instance and implemented all the necessary API for

[6]https://estimote.com.

[7]http://aws.amazon.com.

Fig. 4 Some installed beacons at the testing sites

communication between the smartphone and server. For storing data, we used the AWS Relational Database Service (RDS). The mobile application does not collect any data or perform any calculation outside of the target location used in the study.

4.1 Practical Challenges and Mitigation Strategies

The Bluetooth beacons transmit radio signals around every direction in a spherical way. To get the accurate signal, we need to set up the beacons in a proper and optimal way. During the study, we have faced several challenges while establishing the experiment. There are several issues that affect the distance calculation that ultimately makes the triangulation process more challenging. Here, we discuss the challenges we faced during deployment and how we resolved them.

4.1.1 Beacon Placement and Orientation

The beacons transmit the signals spherically at the environment. However, the facing is important during the placement; the signal strength of beacons on the front side (i.e., the side that faces the user) was adequate to meet our requirements. It is much weaker than expected on the rear side of the posts. Through trial and error, we determined the optimal placement and orientation of each beacon in order to determine the location of users accurately.

4.1.2 Weatherproofing

We should need to take action for beacon waterproofing if it has to install for a long long period of time. Moreover, we had to address environmental challenges like heat, cold, rain, wind, and so on. We should install the beacons in such a way so that no rainwater could enter the plastic bag and interfere with the efficiency and signal strength of the beacons. We selected a thin plastic bag because we found thicker ones weakened the signal. We used transparent plastic bags and duct tape to install the beacons on the posts and stakes.

4.1.3 Vertical Position

The placement height from the ground and the distance between each beacon are additional factors we considered to obtain the most accurate results possible and to provide alerts to users at precisely the best time. To consider the optimal height to place beacons, we considered the height at which user might carry their smartphones and installed the beacons on the lampposts at 2–3 m high and beacons on the stakes at 1–1.5 m high.

4.1.4 Fluctuation of RSSI

RSSI is the strength of beacon's signal that is received by the enabled device (in our case, a smartphone). Usually, the value of RSSI depends on distance or measured power. However, the value also may fluctuate due to absorption, interference, or diffraction. This fluctuation makes the distance calculation result error-prone because the measured distance varies with the fluctuation of RSSI. We divided the distance radius into three zones. The first 20 m radius is the *Immediate Zone*, the next 40 m is the *Near Zone* and the remaining radius signal is the *Far Zone*. We divided the distance radius into three zones. In the normal condition, the *Immediate Zone* signal works perfectly. However, the *Near Zone* and *Far Zone* signal can be distracted by the crowd and excessive obstacles. We conducted our experiment in the normal condition; usual traffic on the street and crowd on the pavement.

4.1.5 Battery Drainage of the Smartphone

Android-based smartphones presented us with battery drainage issues. For the iOS version, usage of hardware such as Bluetooth and GPS are maintained by the operating system itself, so battery usage was not affected. On Androids, however, our application uses GPS, Bluetooth, internet connectivity, and sensors to perform its operations. Many of these features are used by the app for data collection from the users. We coped with battery drainage issues on Android by minimizing the usage

of these features. Specifically, the activates start sensors and enable the location service only when the user needs to start the service. When users leave the zone, the application disables all types of sensor and location services to stop battery draining.

5 Findings

In the study, we use iPhone 8 plus, iPhone XR for the iOS application and moto g7, Google Pixel 4 for the android application. First, we collected the GPS position from three locations at the urban university campus called P1, P2, P3. P1 is situated between the two-building; one is eight storied, another is 12 storied. P2 is a traffic intersection, in which three sides have three buildings less than five-storied, and another side is a park. P3 is near a roadside; in which one side is empty (trees and open space), the opposite side (another side of the road) is a four-storied building (Fig. 5).

After manually collects the GPS position couple of times at different times and days without WiFi, we installed the beacons in the same location. Again we collected the position and distance with mobile applications. Then we manually measured the length with a distance measuring tape. We got the estimated error after

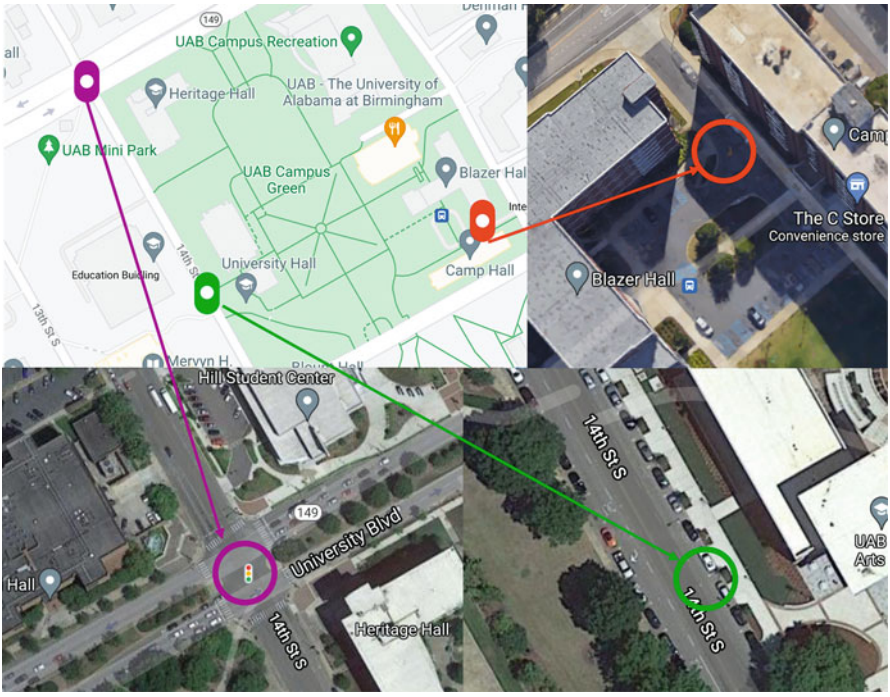


Fig. 5 Testing site location and three locations (P1, P2, P3) at the testbed

Table 2 Errors between GPS and BLE beacons

Technology	Environment	Error (m)
GPS	P1	6–10
	P2	6–9
	P3	3–8
BLE Beacons	P1	1–8
	P2	2–7
	P3	3–4

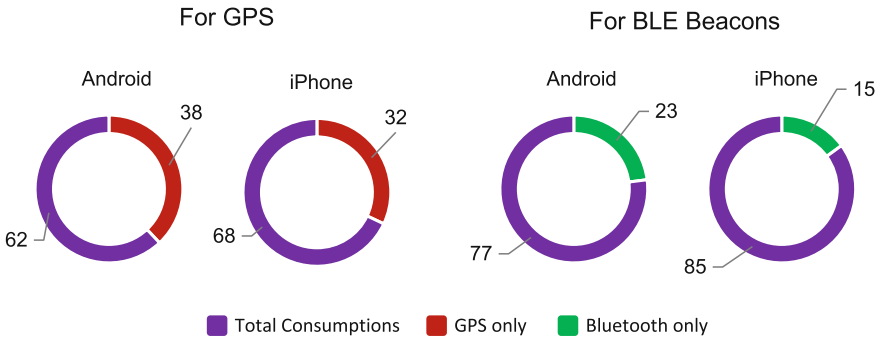


Fig. 6 Data points that need to handle in every hour in the testing sites

subtracting these lengths with the mean values of GPS value and beacons value. Though the error is not the same among the locations (P1, P2, P3), the difference is very negligible (less than 1 m) for both GPS and BLE. Table 2 shows the average errors between GPS and BLE beacon at our testing sites. The results show the BLE beacon system provides less error than GPS in micro-positioning in the urban environment. In the P1 location, the GPS accuracy gave 6–10 m errors; in contrast, the beacons error within 1–8 m.

To use the GPS and beacon positioning, the user has to use the receiver device (i.e., smartphone, smartwatch, etc.). The user has to enable the location service or Bluetooth service in their receiver device to get data for GPS and beacons, respectively. However, power consumption is a major issue when smart devices use these services. We measured the power consumption in the smartphone for both services. We actively use these services in the testing sites for 45 min–2 h a couple of times. During that time, the user device gets data from the beacons and GPS position data. The time is measured individually, and we calculate the average values at the end of the study. During the experiment, all phones are in standard settings. Figure 6 shows the detailed results of battery consumption. The result shows the location service consumes more than 32% battery. In contrast, the Bluetooth service consumes the highest 23% battery during that time. Besides, android operated phone consumes more battery than the iPhone. For example, during the location service, the iPhone consumes on average 32% battery where android phones are responsible for on average 38% battery.

6 Conclusion

This paper reports the design, implementation, and evaluation of the Bluetooth beacon-based positioning in the urban context. The proposed system provides the micro-location where the traditional location service is unavailable or has limited access. The proposed model presents a novel architecture for Beacon-as-a-Service for the outdoor environment in the city. We have conducted experiments on an urban university campus. The site consists of three locations surrounded by different combinations of obstacles and open space. The empirical testing demonstrates that it allows for 10–40% less accuracy error than GPS positioning at the testing sites. On the other hand, Bluetooth service consumes less battery of smartphones than the location service.

Acknowledgment This research was supported by the National Science Foundation through awards DGE-1723768, ACI-1642078, CNS-1351038, and ECCS-1952090 and by the National Institutes of Health grant 1R21HD095270-01.

References

1. Sarwar, M., Soomro, T.R.: Impact of smartphone's on society. Eur. J. Sci. Res. **98**(2), 216–226 (2013)
2. Holst, A.: Smartphone users worldwide 2016–2021 (2019). https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ [Online; accessed 10 October 2020]
3. Delmastro, F., Arnaboldi, V., Conti, M.: People-centric computing and communications in smart cities. IEEE Commun. Mag. **54**(7), 122–128 (2016)
4. Krieg, J.-G., Jakllari, G., Toma, H., Beylot, A.-L.: Unlocking the smartphone's sensors for smart city parking. Pervas. Mobile Comput. **43**, 78–95 (2018)
5. Habibzadeh, H., Qin, Z., Soyata, T., Kantarci, B.: Large-scale distributed dedicated- and non-dedicated smart city sensing systems. IEEE Sens. J. **17**(23), 7649–7658 (2017)
6. Hasan, R., Hasan, R.: Towards designing a sustainable green smart city using bluetooth beacons. In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), pp. 1–6. IEEE, New York (2020)
7. Borozdukhin, A., Dolinina, O., Pechenkin, V.: Approach to the garbage collection in the "Smart Clean City" project. In 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), pp. 918–922. IEEE, New York (2016)
8. Owen, M.: Piper app, network of beacons make Columbus the first 'Safe City' (2015). https://www.ledger-enquirer.com/news/article48009000.html [Online; accessed 13 October 2020]
9. Bay, O.: ABI research finds the future of BLE beacon shipments is not in retail. https://www.abiresearch.com/press/abi-research-finds-future-ble-beacon-shipments-not/, August 2016. [Online; accessed 12 October 2020]
10. Hollander, D.: The state of bluetooth in 2018 and beyond. https://www.bluetooth.com/blog/the-state-of-bluetooth-in-2018-and-beyond/. April 2018. [Online; accessed 14 October 2020]
11. Vallina-Rodriguez, N., Crowcroft, J., Finamore, A., Grunenberger, Y., Papagiannaki, K. (2013). When assistance becomes dependence: Characterizing the costs and inefficiencies of A-GPS. ACM SIGMOBILE Mobile Comput. Commun. Rev. **17**(4), 3–14 (2013)
12. Massad, I., Dalyot, S.: Towards the crowdsourcing of massive smartphone Assisted-GPS sensor ground observations for the production of digital terrain models. Sensors **18**(3), 898 (2018)

13. Von Watzdorf, S., Michahelles, F.: Accuracy of positioning data on smartphones. In Proceedings of the 3rd International Workshop on Location and the Web, pp. 1–4 (2010)
14. Mok, E., Retscher, G., Wen, C.: Initial test on the use of GPS and sensor data of modern smartphones for vehicle tracking in dense high rise environments. In 2012 Ubiquitous Positioning, Indoor Navigation, and Location Based Service (UPINLBS), pp. 1–7. IEEE, New York (2012)
15. Merry, K., Bettinger, P.: Smartphone gps accuracy study in an urban environment. PloS One **14**(7), e0219890 (2019)
16. Giannoumis, G.A., Ferati, M., Pandya, U., Krivonos, D., Pey, T.: Usability of indoor network navigation solutions for persons with visual impairments. In Cambridge Workshop on Universal Access and Assistive Technology, pp. 135–145. Springer, New York (2018)
17. Rida, M.E., Liu, F., Jadi, Y., Algawhari, A.A.A., Askourih, A.: Indoor location position based on bluetooth signal strength. In 2015 2nd International Conference on Information Science and Control Engineering, pp. 769–773. IEEE, New York (2015)
18. Zhou, C., Yuan, J., Liu, H., Qiu, J.: Bluetooth indoor positioning based on RSSI and Kalman filter. Wirel. Pers. Commun. **96**(3), 4115–4130 (2017)
19. Chen, H., Cha, S.H., Kim, T.W.: A framework for group activity detection and recognition using smartphone sensors and beacons. Build. Env. **158**, 205–216 (2019)
20. Cheraghi, S.A., Namboodiri, V., Walker, L.: GuideBeacon: beacon-based indoor wayfinding for the blind, visually impaired, and disoriented. In 2017 IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 121–130. IEEE, New York (2017)
21. Baek, J., Choi, Y., Lee, C., Suh, J., Lee, S.: BBUNS: Bluetooth Beacon-based Underground Navigation System to support mine Haulage operations. Minerals **7**(11), 228 (2017)
22. Jung, J., Choi, Y.: Measuring transport time of mine equipment in an underground mine using a bluetooth beacon system. Minerals **7**(1), 1 (2017)
23. Lindh, J.: Bluetooth low energy beacons. Texas Instr., 2. January 2015
24. Bluetooth Special Interest Group. Bluetooth 4.0 core specification. https://www.bluetooth.com/specifications/bluetooth-core-specification. [Online; accessed 14 October 2020]
25. Apple. Getting started with iBeacon. https://developer.apple.com/ibeacon/. [Online; accessed 15 October 2020]
26. Google Beacon Platform, Eddystone. https://developers.google.com/beacons/eddystone. [Online; accessed 15 October 2020]
27. Elnahrawy, E., Li, X., Martin, R.P.: The limits of localization using signal strength: a comparative study. In 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004, pp. 406–414. IEEE, New York (2004)

Legal Issues and the Need to Engineer Positioning Systems for Protection of Privacy and Personal Security

Michael Martin Losavio

1 Introduction

The engineering of systems occurs within the global social domain of rights, obligations, laws, regulations and people affected by those systems. Security and privacy are two domains that may be impacted by information systems and how that information is used. Regulation of positioning systems, and liability for injuries from them, may develop through a balancing of the benefits and risks of those systems as they are used in the world. Re-engineering may be necessary for regulatory compliance and reduction and avoidance of injury to others. Where risks outweigh benefits, positional systems may even be removed from operation until that imbalance can be remedied and the protection of security and privacy assured. Where those risks manifest as injuries to others, the developers and operators of those systems may face financial or criminal liability.

Precise positioning systems improve the efficiency of personal and commercial activities in many domains, from transportation to access to services, using wireless network access points, satellite signals and cellular tower triangulation [1]. Transportation systems have helped assure that drivers don't get lost in most urban environments, and that farmers can plant their fields with greater efficiency [2]. The cellular smartphone with enabled positioning services can provide these and directions for access to a myriad of social, commercial and personal services.

Location and positioning are the heart of many of the functions of the Smart City, which seeks to optimize services to citizens. That optimization includes transportation services for automobiles and public transport, public services such as utilities and waste management. Integrated with the Internet of Things in the

M. M. Losavio (✉)
Department of Criminal Justice, University of Louisville, Louisville, KY, USA
e-mail: michael.losavio@louisville.edu

S. Paiva (ed.), *Precision Positioning with Commercial Smartphones in Urban Environments*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-71288-4_7

positional data generated by devices within that paradigm, smart appliances, energy sensors, security sensors and activity sensors can all both optimize their operations and those of other parts of the overall ecosystem for the Smart City and the Internet of Things. With these enhanced public functions come new challenges to the privacy and security of the citizens, with the data open to compromise of both [3].

Positional systems, integrated with systems for commercial products and services, can speed access in multiple domains for people needing them. Incorporating these systems into residential buildings can promote the well-being and safety of the residents [4]. Within industrial environments, augmented reality positioning systems have been proposed for close-in industrial operations to enhance occupational safety for dangerous marine operations [5].

One partial taxonomy of positional system uses includes the management and tracking of people, the management and tracking of assets, healthcare and mobile monitoring of patients, security services, emergency services, gameplay, commerce, advertising, marketing, entertainment, tourism and the post-provision analysis for all of these services [6]. As the United States Supreme Court noted in *United States v. Carpenter,* its first case to address privacy issues with cellular telephone locational data via Cell Site Location Information (CSLI), a phone's user is rarely more than two meters from that phone during the day. This makes it functionally a potential tracking device that may invoke the privacy protections fundamental to laws of many nations, including, as discussed below, American law.

This listing of uses demonstrates a spectrum of sensitivity of information that could impact how positioning data creating a privacy violation could injure others. Issues of the privacy in computational information and location are concerns for pervasive computing, context-aware computing and generally with all location-based applications [7–9]. The enhanced power, low-cost and pervasiveness of positioning systems, especially smartphones, mandates developer and engineering attention to the legal, social and ethical challenges that their use and compromise may present.

Straightforward examples of the power, benefit and risks relating to positioning systems, especially smartphones, can be found as answers to these three simple questions:

"Where have you been?"
"Where were you last night?"
"Where were you on July 4, 2027 at 7:48 PM?"

These are the kinds of questions asked by a parent, spouse or police interrogator, leading to a variety of possible outcomes for the person being questioned as to their time and location delimited activities. They are inquiries into a subject's particular location at a particular time, which may correlate to other information regarding other activities at that particular time and place. These are questions that systems of precise positioning might or might not answer with greater reliability than that of human memory. The outcomes of those answers may be for good, or ill.

"Where have you been?" has been asked by every parent of every child coming home late. It may lead to a simple admonition to just be careful or to call, or it may

lead to the revocation of juvenile privileges for the next 2 weeks. Parental systems for the ultimate location tracking device, a teenager's cell phone, are deployed to give real-time tracking of the child's location [10].

"Where were you last night?" Perhaps this is a question of simple spousal curiosity, or more complex spousal suspicion. The grounds for that question, and the answer to it, it may lead to family discord or worse. Location-based services have become new tools of abuse in relationships, provided by the ease of constant monitoring, and constant stalking, of victims [11, 12]. They may enable a heightened level of surveillance and stalking, with potentially terrible, mortal consequences where the stalker may assault or murder the victim [13]. But to this risk positional systems may offer benefits. GPS positional tracking of domestic violence offenders may reduce recidivism, reoffending and danger to the targeted victim [14].

It is never good to be asked "Where were you on July 4, 2027 at 7:48 PM?" The need for timestamped geospatial information may come from an officer of the state, and it may be essential in a criminal investigation to know who was at or near the scene of a crime at the time of the crime. CSLI has been used to solve crimes where there were no leads or other evidence of possible offenders upon whom an investigation should focus. Location and positioning systems used in criminal justice and law enforcement highlight the challenge of balancing the benefits and risks the technology presents.

But anything you say can and will be used against you, especially where your memory is faulty. Location-based positioning data can supplement a faulty memory, but it may also risk the creation of false inferences of relationships from coincidental or partial positional data.

In these and other scenarios, precise positioning, historical and real-time, of people, transportation and systems creates a foundation for efficient and safe urban environments, especially for Smart Cities. It can optimize the movement of people and the delivery of services, including public safety. For a child coming home or husband out last Tuesday night, it can affirm virtuous behavior. They may also reveal fewer savory activities that may have unfortunate consequences for all those involved. They may lead to inferences which may or may not be correct, but which may lead to unintended and possibly unjust outcomes. The collection, storage and analysis of this positioning data may create challenges to privacy, personal autonomy and the security of the people.

As these technologies themselves must exist within a framework of laws and policies for democratic societies, it is essential their engineering anticipate broadly the outcomes from implementation, conform those outcomes to the law and be flexible enough that they may be modified to accommodate future changes in law and policy.

Legal discussions and regulations for positioning systems offer guidance and extrapolate to issues that must be considered for the future of the systems. Failure to incorporate flexible engineering to address legal and policy mandates will lead to issues and problems with regulation, and justice, for positioning technologies and their use.

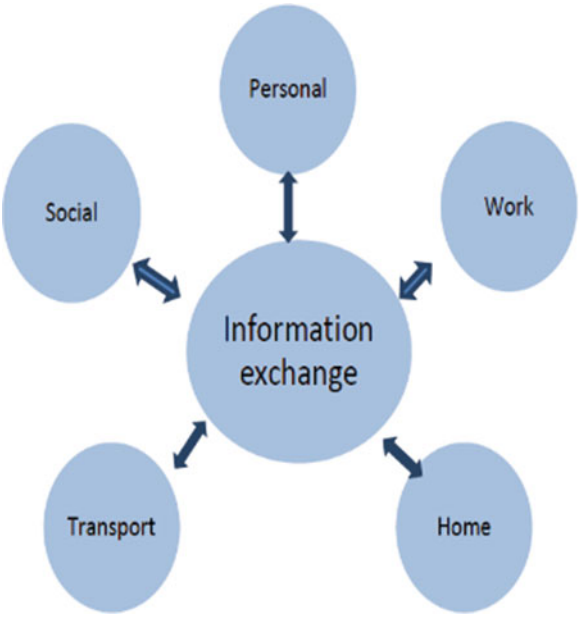


Fig. 1 Nodes for information generation, exchange and collection [15]

But legal development may lag behind the speed of technological innovation. This is especially true when we look at rapid innovations regarding the Smart City for government services and the Internet of Things for an even larger deployment of sensing devices. And the phenomenal growth of smartphone use throughout the world has, in effect, deployed a vast personal positional sensor system everywhere for nearly everyone, regardless of wealth, position or social status. This growth in sensing systems, often incorporating positioning technology, creates a vast data profile on each and every individual. This is seen in Fig. 1, which details the different domains from which information regarding the lives of others may be generated, exchanged and collected for analysis:

Each of these domains may generate information as to where and when a person has been over a considerable period of time. This information profile may be matched with those of others and data collections of a broad array of information as to create both direct and inferential "facts" about a person. It becomes an electronic dossier that would be the envy of any state intelligence agency. System engineering must consider the legal, social and ethical impact of these systems.

This chapter analyzes legal case studies that offer guidance for the present and future regulation of positioning systems, their engineering and the people whose lives they change. This examination looks at

1. the possible impact of positional systems and location data on peoples' lives,
2. foundations of Law for privacy, technology and positional data, seen in case studies wrestling with the balance between positional data and personal rights, particularly privacy, and

3. other issues of present and future responsibility and possibilities for regulation of positional systems that may require sufficiently flexible engineering to adapt to that regulation.

This examination can guide the effective, reliable and just use of positional systems as engineering can anticipate and remediate risks from them. This supports designing flexibility for modification as needed in compliance with changing regulation.

The rest of the paper is structured as follows. In Sect. 2 we discuss the possible impact on privacy and security of positioning systems. In Sect. 3 we examine the emergence of positioning systems as issues in litigation, the rule of law and the administration of justice. Section 4 discusses a case-based analysis of major legal issues with privacy, security and positional data systems in relations to fundamental rights. Section 5 sets out other possible issues relating to accountability and responsibility in positional systems under U.S. and European Union regulations and potential methods to remediate risks of injury to other. We conclude that issues of liability and responsibility for these systems will grow with their ubiquity, and that their engineering must both minimize injury to others and be flexible as to accommodate future changes in their regulation.

2 Positioning Systems and Possible Impact on the Privacy and Security of Others

Privacy and security are personal rights, to varying degrees, of people in nearly all nations. Statutes and legislation, and common law rights and privileges, detail some areas within which a person's privacy and security are protected. The general framework for this under the laws of the United States, despite its lack of a comprehensive privacy regime and data regulation framework, can give a sense of how this is structured into general categories that are mirrored in other nations' laws. The partial list of privacy violations includes:

1. intrusion into personal affairs and protected space (the home),
2. revelation and publicity of personal affairs not of public interest,
3. revelation and publicity of personal affairs portrayed in a false light [16].

Privacy considered as a right to a certain level of personal autonomy is a key value and legal right around the world. Security is an interrelated value for both the protection of the individual and their personal autonomy and that of their adjunct spaces, domains and relations. While rights to privacy and security may vary from one legal jurisdiction and nation to another, they are of general import for most nations of the world.

Positional data may play a key role in both privacy and security. One stark example of this relates to positional/locational data of parties in domestic violence disputes. The United States, despite its general lack of a statutory regime of privacy,

has enacted statutes prohibiting the distribution by its several states of drivers' license location information after several abusers used that information to locate, stalk and murder their former partners who had sought to escape them [17, 18]. This highlights the security and privacy value of where a person is and how revelation of positional information can lead to terrible outcomes.

Kolodziej and Hjelm detail privacy concerns with locational systems as being at the connection-level, the service-level and the application-level [19]. Connection-level privacy concerns invoke the relationship between locational data and identifiers relating to the connecting device/individual. Allocation of IP addresses between static and dynamic assignment may impact that relationship.

For service-level privacy the identifiers may serve as a foundation for a privacy violation. Evidencing the importance of these issues and in response to the growth in the use of locational information across multiple domains, the Internet Engineering Task Force (IETF) working group on Geographic Location/Privacy was founded [20]. It examines issues relating to location within Internet protocols and focus on the fundamental security concerns presented by them: authorization, integrity and privacy. The GeoPriv working group is directed towards harmonized standards to ensure privacy and security in location-aware systems in its charter:

> *The working group will work with other IETF working groups and other standards development organizations that are building applications that use location information to ensure that the requirements are well understood and met, and that no additional security or privacy issues related to location her left unaddressed as these location information is incorporated into other protocols.*
>
> *It remains a goal of the GOP working group to deliver specifications of broad applicability that will become mandatory to implement for IETF protocols that are location aware* [20].

This, in turn, leads to issues of application-level locational privacy protection in location-based services (LBS) [21]. Users, once aware of the implications of location data generation and their applications, might wish to implement privacy protections. Position awareness, sporadic queries and location tracking are three aspects of location-based services that may involve the user, a positioning-service provider and a general service provider. These situations, relationships and potential for misuse may present issues relating to the need for privacy protection and the balancing of security against degradation of location services. Gruteser and Liu suggest that this balancing has to consider the nature, importance and sensitivity of the locational data against its impact on the accuracy of the location-based services [21]. Table 1 shows positional data in applications and related possible invasions and violations of personal privacy and security:

Positional and location-based systems carry the potential of significant injury to persons and their reputations, even as their developers are primarily focused on the benefits of such systems. Good intentions are not enough; developers must consider the possible negative impacts of these systems and remediate them. For example, police system developer Axon, concerned about issues with the use of AI-enabled facial recognition systems for law enforcement, convened an ethics panel to study these issues; the panel concluded such AI-enabled systems for mobile body-cameras

Table 1 Positional data and injury to privacy and security

Data point	Application	Privacy	Security
Time and place of individual	Personal tracking	Revelation of personal activities, from within the home to out in the world	Location for direct attack or attack in absence against a protected space, e.g., home, office
Time and place of multiple individuals	Proximity matching	Revelation of personal associations otherwise private, mis-inference of associations	Mis-inference leading to conduct and sanctions by private and public actors
Time and place of multiple individuals mapped against other data sources	Analytics against multiple data sources	Revelation of direct and inferential private facts, mis-inference as to private and public facts	Mis-inference of private and public facts, including false negatives and false positives regarding conduct involving inferred conduct and sanctions by private and public actors

were not ready for deployment, due to both system performance issues and the risk of misuse by some agencies [22]. Although this level of review may be difficult for some smaller system developers, it offers a template for review that every developer should follow to try and minimize unintended injury from systems.

3 The Emergence of Positioning Systems as Issues for the Rule of Law and the Administration of Justice

Its novelty and power have led to a number of intellectual property cases challenging rights to positioning system implementations [23]. Beyond that, given its power positioning data has served a key role in litigation with its ability to show time and place. As such, it is been both supported and attacked as to reliability based on the implications from that data as to civil and criminal liability. Failure to properly plot and use positioning data with due care may lead to liability where there is a duty to do so. One example was where the United States Coast Guard was found negligent and at fault for mispositioning warning Buoy No. 4 such that a marine vessel grounded on a reef [24]. The extent of evidentiary use, and the potential for liability where systems fail or are inaccurate, is growing and becoming a more frequent issue in litigation.

Discussion of positional and location-based data systems has gradually become a legal-practice issue. Examination of US case law databases show that prior to 2005 positional data was discussed infrequently in US cases, with data indicating single

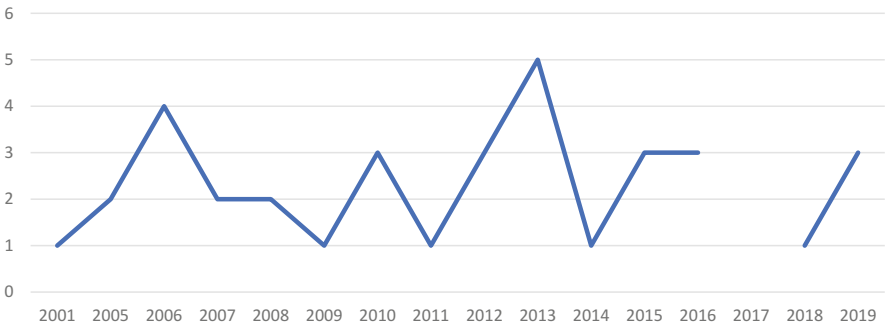


Chart 1 Case Frequency of Positioning Discussion US Law (Source: Nexis Uni Academic Database, Lexis Nexis Corp. published, accessed 20 October 2020)

discussions in 1977, 1982, 1987 and 2001-only for such mentions in 25 years- and none in the other intervening years. This indicates the *facts* of positioning systems and data were not often relevant to legal issues in litigation during this time.

Beginning in 2005 fact issues relating to positioning data became constant in US litigation. This does indicate an increased prominence of positioning data as with evidence in various types of legal disputes. It also indicates possible liability for the effectiveness and reliability of positioning information for various purposes, from transport to surveillance.

The variety of disputes where positional and location-based data played a role has grown in both civil and criminal litigation. These range from the identification of alleged wrongdoers in civil private personal injury cases to crimes as serious as murder. Examples of the use of positioning data as evidence are discussed below; Chart 1 shows this frequency distribution of discussions of positioning information in US case law over the past several decades and the increased discussion of since 2005:

In civil litigation between private parties, the case of *Morgan v. U.S. Xpress, Inc* (2006) involved a collision between Morgan's semi-truck and another semi-truck that was initially unidentified [25]. Morgan sought positioning data from the Defendant, over the defendant's objection in order to identify the truck he alleged caused the accident. The court summarizes the foundation for expert and lay testimony regarding the operations of positioning systems and the data storage of the information generated. In *Tokio Marine & Fire Ins. Co v. Flora MV*, (2001) expert attacks on the accuracy of geographic positioning system data were rejected in holding a marine bulk carrier libel for a collision of two vessels at sea [26]. In *Kane County v. United States* positioning data was used to define boundaries for property rights of way across land owned by the United States [27].

Criminal investigations and prosecutions by the state of its citizens benefit from positioning data. As in *Morgan*, in *Brown v. State of Texas* geographic positioning data from an interstate truck service was used to co-locate the defendant, this time in association with the murder of a young woman from New Jersey whose body

was recovered in Texas [28]. In the state criminal prosecution of *State v. Trott* (2016) the positioning data generated by a stolen iPhone led police to the culprit [29]. Geographic positioning data from a cellular telephone was used to locate a defendant at the scene of a violent carjacking and prove guilt in *United States v. Jackson* (2019) [30]. Similarly, in *United States v. Bailey* (2016) positioning data from the defendant's cellular telephone was used to prove involvement in narcotics trafficking [31].

The state case of *Commonwealth v. Davis* (2020) was an evidentiary challenge to the use of positioning data in a criminal prosecution under the reliability standards of U.S. federal and Massachusetts state law [32–34]. In particular, under Massachusetts law GPS evidence must be qualified for reliability because "at its core, is scientific evidence, [its] reliability ... had to be established before ... it could be admitted" [35].

At issue in *Commonwealth v. Davis* was the GPS positioning data from an ET1 monitoring device worn by Davis; this data, as interpreted by an expert would show Davis's location and rate of travel. The trial judge examined that expert regarding the data reliability in urban/dense urban settings, and speed determinations via the ET1 system; the expert noted the monitor's operations and that the positional accuracy of the ET1 monitor have been tested to an accuracy rate of 98% within 16 ft/5 m and 50% within 3 ft/1 m. The appeal review court noted that "GPS technology ... is widely used and acknowledged as a reliable relator of time and location data," and thus it was properly used for that purpose [36]. The evidence of the rate of travel did not sufficiently establish its reliability, but the key issue was where the defendant was at the time of the shooting, not how quickly he got there.

The growth in the use of positional and location-based data for the resolution of the most serious disputes shows the importance of their reliability. It presages the foundational challenges they may present to the rule of law, unintended injuries and the potential liability of developers and users of those systems.

4 Case-Based Analysis on the Legal Issues for Privacy, Security and Positional Data Systems

4.1 The US Supreme Court cases of United States v. Katz and United States v. Kyllo and the Impact of New Technologies on Traditional Rights Under the Law [37, 38]

Position and location information have historically had limited protections under United States law, both under its Constitution and statutory law. The original and primary focus for privacy protection was the home, with extensions to nearby structures and commercial locations. The invasion of privacy was envisioned as a physical one, a trespass to the premises. Historically there was no reasonable expectation of privacy in one's activities out in public or in information or data

held by third parties absent a special privacy right. The US Supreme Court, in the landmark ruling in *United States vs Katz*, moved away from the historical physical trespass doctrine to one that protected the privacy of people, not places, even in the face of technological innovation of telecommunications [37]. In ruling that telephone communications could not be intercepted without a court order by law enforcement, even via access to telephone lines owned and operated by third parties, the Supreme Court overruled an opinion from 40 years earlier that found no right of privacy as there was no physical trespass. This established a radically different foundation protect the rights of individuals where they had "a reasonable expectation of privacy" that a society and the law would respect.

The ruling and the law established in *Katz* was applied in one of the first technological challenges to privacy and location addressed by the US Supreme Court in the case of *United States v. Kyllo* [38]. In *Kyllo* the issue was whether or not the use of infrared surveillance technology to observe activity within a home, a non-physical trespass, was legal. Was the technology an illegal invasion of privacy absent a judicial order that there was probable cause of criminal activity as to justify the surveillance? The Supreme Court held that it was an illegal invasion of privacy absent a judicial order issued upon a finding that it was more likely than not that evidence of criminal activity would be found in that location. The intrusiveness of the invasion of privacy was extended because it allowed full surveillance of all the activities of the people in the home, wherever they went in regardless of which room they visited, with no notice that they were being watched. As the people in the home clearly had a reasonable expectation of privacy in their activities within that home, the use of technical means to see through the walls, even with no physical trespass, was an unreasonable and illegal search.

4.2 The US Supreme Court Case of United States v. Jones and GPS Tracking [39]

A direct challenge to positional information in real time was presented to the US Supreme Court in *United States v. Jones* [39]. In that case the government had attached a Global Positioning System (GPS) tracking device to Jones's car, which would then transmit in real time locational data to a storage system which could in turn be used to generate tracking maps of Jones's travels as to location and time. It directly presented the impact on data privacy and security from novel means of positional data collection, analysis and use. In *Jones* the Supreme Court chose to avoid the issue and held that the act of attaching the GPS tracking device was a physical trespass and thus, without a judicial order, was illegal. But several of the judges wrote concurring opinions that focused and expanded on the core issues of positional data privacy presented by the case.

Justice Sonya Sotomayor, considered a liberal jurist, wrote that the technologies of inexpensive GPS positional data generation, transmission and collection had the

potential for massive disruption of how people viewed the privacy of their affairs, even in public. Such systems provide the grist for Geographic Information Systems (GIS) that it become key to intelligence-based policing. She suggested that because of their low cost, ease of operation and massive data collection, such systems could "alter the relationship between citizen and government in a way that is inimical to democratic society."

Justice Samuel Alito, considered a conservative jurist, noted that the space for positional data is being constantly expanded through a myriad of devices deployed more and more throughout society: Closed Circuit Television, tolling systems, automobile automatic notifications systems, cellular telephones and other wireless devices. Such historical positional profiling over the long-term would clearly constitute a violation of a citizen's reasonable expectation of privacy in their life activities.

4.3 The US Supreme Court Case of Carpenter v. United States and Cell Site Locational Information [40]

The jurisprudential recognition of the novel impact on personal privacy of electronic data in the new world of Information and Communications Technologies (ICT) continued in the case of *Riley v. California* [41]. The Supreme Court in *Riley v. California* was again presented with the question of privacy interests in a personal cell phone taken from a person incident to the arrest of that person; traditional doctrine provided that a person could be searched upon arrest any items found on them seized and examined in order to assure officer safety and preserve evidence from destruction [42–44]. Under this traditional doctrine a cell phone and its contents taken from a person under arrest could then be examined by the police without any further judicial oversight or permission. The Supreme Court, acknowledging the changed circumstances presented by new data technologies, ruled to expand privacy protections for mobile data devices due to their unprecedented ability to store information. The Court noted that new data devices permitted huge portions of the intimate aspects of a person's life to be collected and stored, from text messages to pictures to contact lists to audio files to videos.

The analysis applied in *Riley* is instructive. The Supreme Court said that it would decide whether or not to exempt a given type of search from the court-ordered warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.", citing an earlier Supreme Court case, *Wyoming v. Houghton* (1999) (US) as well as the balancing in *United States v. Robinson* (1973) (US) of a search to promote officer safety and evidence preservation noted in *Chimel v. California* (1969) (US) [45].

These court rulings impact the evolution of law in lower courts, where most litigation and case law develop. Even in failing to prevail in a final ruling, the

opinions of judges who "dissent" from the majority ruling in a multi-judge case may still have persuasive impact on other courts, including the Supreme Court. In one dissent from a 2016 ruling upholding technical invasions of privacy, a judge predicted further invasions as technical deployment of Internet of Things devices kept growing [46]. That dissent provided a detailed analysis of the threat from positional data:

> *The majority does not take seriously this idea—that information might be automatically generated without user involvement. See ante, at 16 ("[T]here can be little question that cell phone users 'convey' CSLI to their service providers. After all, if they do not, then who does?"); id. ("Perhaps Defendants believe that . . . the [service] provider just conveys CSLI to itself."). But even in the era of Miller and Smith, human beings were not the only entities capable of collecting and conveying information. That is also surely the case now, and will only become increasingly relevant going forward. See, e.g., Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934, 1940 (2013) [47] ("The incentives for the collection and distribution of private data are on the rise. The past fifteen years have seen the rise of an Internet in which personal computers and smartphones have been the dominant personal technologies. But the next fifteen will likely herald the "Internet of Things", in which networked controls, sensors, and data collectors will be increasingly built into our appliances, cars, electric power grid, and homes, enabling new conveniences but subjecting more and more previously unobservable activity to electronic measurement, observation, and control."); . . .*
>
> *. . . Today, the majority saddles us with a rule that does not distinguish between information an individual himself conveys and information that computerized devices automatically record, generate, and transmit. In other words, the majority's expansive interpretation of Miller and Smith will, with time, gather momentum—with effects increasingly destructive of privacy. (emphasis added)* [48]

Yet this analysis on the power and danger of positional data ultimately prevailed in a different case 2 years later. Positional data became the heart of privacy litigation in the 2018 case of *United States v. Carpenter* [40]. The Supreme Court detailed therein the fundamental dangers to privacy in this growing information sphere as related to cell site location information. It noted that with most people always within 2 m of their cell phones, those devices become the penultimate personal positional tracker.

The Supreme Court in *Carpenter* acknowledged the inherent privacy dangers and found that a person held a privacy interest in their cell phone locational data. This applied even though transmitted to and held by a third-party provider, a practice that traditionally ended any reasonable expectation of privacy due to a third party's knowledge. This protection in law as to law enforcement access engaged both the security of an individual from privacy as well as the liability for the breach of that privacy, both direct and for collateral consequences that they flow from that breach.

The Supreme Court, per Chief Justice Roberts, said:

> As Justice Brandeis explained in his famous dissent, the Court is obligated—as "[s]ubtler and more far-reaching means of invading privacy have become available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections. *Olmstead* v. *United States*, 277 U. S. 438, 473–474 (1928). Here the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort

> the Framers, "after consulting the lessons of history," drafted the Fourth Amendment to prevent. *Di Re*, 332 U. S., at 595 [49–52].
>
> We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.

Key issues to this opinion related to the intimacy of the data collection sensors-the cell phone-and its near constant physical association with their owners, the constancy of the 24/7 generation of locational data and the extended duration of the data collection. All of these factors, whether or not a particular cell phone was being used, argued in support of the need to protect personal privacy in such historical CSLI. Law enforcement will be forced to adjust to it [53].

This recognition of the modern challenge of computational positional analysis sets the floor for regulation of access and use of positional data. Systems for generating positional data must be able to accommodate that regulatory structure and adapt to changes in regulation. Those systems must also be able to secure the information generated as to protect the subjects of that data from its misuse.

This case was heralded as one that may potentially set new legal precedents regarding privacy rights of individuals in their digital information even where held by third parties [54]. In turn, this decision was expected to affect many different businesses given the growth in the generation and use of location and positional services by a variety of businesses and organizations [55].

The significance of *Carpenter* lies, in part, in the Supreme Court's willingness to look at the concept of privacy in the context of new and potentially invasive technologies. This is particularly significant regarding new information technologies that collect and store massive amounts of data on people's lives, and then provided as grist for analytical engines generating inferences about all aspects of human behavior and activity.

But the Court in *Carpenter* was careful to limit the impact of their ruling and the potential to extrapolated it to other location-based data resources, creating some concerns that it may have created a whole new domain of issues regarding what positional data is protected and what is not [56]. Other types of data not expressly covered by *Carpenter* were found not to be protected by each reasoning, such as telephone call dialing records metadata regulated under the Stored Communications Act (US) [57, 58]. Bitcoin records have been analogized to bank records and denied privacy protection under the third-party doctrine that there is no expectation of privacy in records held by others, a doctrine the Supreme Court held did not apply to historical CSLI in *Carpenter* [59].

Yet the impact of *Carpenter* and issues relating to privacy and rights in positional data continue to evolve [60]. De Zayas suggests *Carpenter* will be extended to browsing activity [61]. Kassotis extends *Carpenter's* data protection reasoning to analysis of hash-value matching for surveillance of a person's online activity [62]. This extension may occur despite the lack of comprehensive US law on mass data collection beyond collection via unfair or deceptive practices [63]. Holland

proposes a new framework regarding protections for all digital metadata and that the jurisprudence of *United States v. Jones*, *Riley v. California* and *Carpenter v. United States* extends new protections in personal data.

5 Other Concerns for Present and Future Accountability for Positional Data Systems

The invasion of rights and injuries to persons is a primary concern in designing systems so as not to hurt others. But there is the ancillary issue of who is responsible and liable for damages when those injuries occur. The limitation on liability provided for in contracts and contract law, particularly that related to service level agreements and end user license agreements, will not necessarily protect a system user/operator, vendor or designer who system leads to injury to others due to problems with the design or use. Depending on the particular nation and jurisdiction, there may be a variety of statutory liability provisions regarding the operations and injuries that result from the. Various nations have developed legal regimes of products liability for injuries caused by a particular system or device. Under that legal regime a product that is deemed to have inherent defects as to lead to third-party injuries will create damages liability for the developer and seller of that product; contractual efforts to create a liability shield fail as to those third parties who have been injured. Nations may by law negate any efforts to avoid liability for injuries from errors in or misuse of positional data.

Criticality of function plays a role here [64]. If there is a particular mission-critical system that relies on positional data and location-awareness, the developer must assure that the system will perform at key moments. Problems of high latency in system operation and difficulty supporting mobile systems in a timely manner may cause a system to fail to timely perform when needed.

Statutory legal regimes regulating information systems, including those generating positioning data, may categorize the activities involving data and regulate one or all of those categories. Generally, those regimes look at

1. data collection,
2. data storage,
3. data transmission,
4. data analysis, and
5. data use.

Regulation may occur at any of these categories such that violation may lead to financial or liberty punishments. The regulations may prohibit action involving positioning data or mandate practices relating to it, or both. Prohibitions on data collection may completely forego data-related activities, at least as to the law-abiding. Transmission and storage controls may limit by whom the data may be used and the circumstances by which it may be secured from malicious attacks.

Analysis and use controls constrain application of the data findings and inferences as to limit possible privacy violations and security compromises. The Stored Electronic Communications Act (US), for example, allows the voluntary disclosure of electronic data as needed for system operations but states "a provider of remote computing service or electronic communication service to the public *shall not knowingly divulge a record or other information* pertaining to a subscriber to or customer of such service *to any governmental entity."* (emphasis added) absent a court order, subject to exceptions including "an emergency involving danger of death or serious physical injury" [65].

In *United States v. Carpenter* (2019), above, access to CSLI data could be collected, stored, transmitted, analyzed and used by third parties for the efficient operations of commercial cellular telephone services. But that CSLI data could not be accessed, analyzed and used by US federal, state or local law enforcement agents without a court order based upon a judicial finding there was probable cause to believe this data was evidence of criminal activity.

This framework is incorporated within and expanded by the European Union's General Data Protection Regulation (EU) (GDPR) [66]. The GDPR requires broader and more specific obligations for collection and storage of data, access to and processing of personal data and the rights of data subjects. The rights of data subjects include rights to be informed of the nature of the data collection and any analytical decisions based on that data, to permit collection, opt out of collection, review their data and require its correction and erasure, and the protection of the data from disclosure.

The GDPR applies where positional and locational data may have some connection to the European Union; the provision for compliance with the General Data Protection Regulation is essential. To assist with compliance, inventories of requisite elements can aid in the analysis of compliance and privacy issues, such as De and Le Metayer's Privacy Risk Analysis Methodology (PRIAM) [67]. Article 35 requires the data holder do analyses of the risks a data system may pose to the data subject (Data Protection Impact Assessment) and then mitigate the risks of injury presented [68].

Compliance with privacy protections and the GDPR may look to other privacy-preserving methodologies, such as encrypting or pseudonymizing data that may be integrated into systems or be accessible to users. These may offer automatic or opt-in/opt-out privacy protections to users and data subjects. Hasanzadeh, et al. suggest a context sensitive anonymization of data in relation to the use of Public Participation Geographic Information System (PPGIS) data [69]. They evaluate privacy concerns in positional data under the GDPR.

This has implications beyond protection from state actions; it goes directly to matters of personal security. Extrapolating from the reasoning of Justices Sotomayor and Alito in the *Jones* case, both Opportunity Theory and Routine Activity Theory from criminology posit significant personal danger to the security of people beyond that of state actors [70]. As with legislation limiting access to driver' s license databases to protect people's locational information, a motivated offender would be able to use this positional data to victimize a vulnerable target. Guardian protections

could be avoided through similar use of positional data. The sexual exploitation of children via online means could become an even greater risk through the use of unmediated positional data.

Lastly, the impact of powerful analytics against large bodies of positional data on large populations is only now being explored. Early adoption of systems for government operation, even against limited and stylized data, has led to concerns of effectiveness, as the least, and financial and personal injury, at worst. Government systems for the computational administration of unemployment compensation have been found to generate false positives as to insurance fraud [71]. These computational errors, in turn, led to extensive financial injury and penalties beyond the denial of benefits, further leading to bankruptcy and residential eviction.

6 Conclusion

Positional data has been a part of establishing legal liability, civil and criminal, from the earliest days of human society. It can now be used in historical and real-time analysis for consumer-level, person-level decisions, good and bad. The unprecedented explosion and the amount and availability of positional data creates challenges for accountability for the use of that information. The ways in which we address those challenges will determine for what and how we will be held accountable. We can expect a similar growth in potential liability for the use of positional data to broadly create injuries and risk of injuries to others. That, in turn, should lead to growth in the regulation on the collection, storage and analysis of positional data because of the risks now associated with it through the threat of misconduct, including invasion of privacy and the personal autonomy of individuals, their families and communities. A great boon to police investigations may become the destruction of an innocent person's reputation and life.

Because positional and locational information is so intimately associated with people and their activities, the injuries from the systems can extend well beyond mere inconvenience. The compromise of privacy, corrupted positional data and misinference from otherwise correct data can lead to humiliation, reputational damage, erroneous prosecution, and physical injury. The people behind the engineering of systems for positional and locational data generation, collection and analysis are responsible for all of the outcomes from the use of those systems.

As such, there will be increasing efforts through both courts and legislatures to define the proper balance between the rights and liberties of citizens and the benefits entailed by positional data. The challenges will be even greater for democratic societies seeking to address growing online and ideological threats while preserving the rights of their citizens, all while using the great benefits positional technology offers. The engineering of positional systems must anticipate and minimize any risks to others from their use. Further, that engineering must be flexible enough to allow

for modification as new risks develop and new regulations are implemented. We as scientists, engineers and policymakers must work to address those challenges before people are injured, as if these are the early days of a better world.

References

1. Skyhook Wireless, Inc. v. Google, Inc., 28 Mass. L. Rep. 625, 2010 Mass. Super. LEXIS 362, 2010 WL 5348732 (Superior Court of Massachusetts, At Suffolk December 6, 2010, Filed)
2. Trimble Navigation, LTD v. RHS, Inc., 2007 U.S. Dist. LEXIS 41267 (United States District Court for the Northern District of California May 29, 2007)
3. Kasar, S., Kshirsagar, M.: Open challenges in smart cities: privacy and security. In: Tamane, S.C., Dey, N., Hassanien, A.E. (eds.) Security and Privacy Applications for Smart City Development. Studies in Systems, Decision and Control, vol. 308. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-53149-2_2
4. Pešić, S., Radovanović, M., Ivanović, M., Tošić, M., Iković, O., Bošković, D.: Graph-Based Metadata Modeling in Indoor Positioning Systems, Simulation Modelling Practice and Theory, vol. 105 (2020)
5. Dominguez Ollero, R.: Benefits and implications of augmented reality positioning systems for offshore topside installations. Thesis, Delft University of Technology (2017)
6. Krzysztof, W., Kolodziej, J.H.: Local Position Systems: LBS Applications and Services, CRC Press (2017)
7. Beresford, A., Stajano, F.: Location privacy in pervasive computing. IEEE Pervasive Comput. **2**(1), 46–55 (2003)
8. Smailagic, A., Kogan, D.: Location sensing and privacy in a context aware computing environment. IEEE Wireless Comm. **9**, 10–17 (2002)
9. Myles, G., Friday, A., Davies, N.: Preserving privacy in environments with location-based applications. IEEE Pervasive Comput. **2**(1), 56–64 (2003)
10. BestParentalControlApps.Com: Digital kids: how to track a cell phone location without them knowing. https://bestparentalcontrolapps.com/track-a-cell-phone-location-without-them-knowing/. Accessed 16 Oct 2020
11. Southworth, C., Dawson, S., Fraser, C., Tucker, S.: A high-tech twist on abuse: technology, intimate partner stalking, and advocacy 2 (2005)
12. Baddam, B.: Technology and its danger to domestic violence victims: how did he find me? Albany Law J. Sci. Technol. **1**, 73–93 (2017)
13. McFarlane, J.M., et al.: Stalking and Intimate Partner Femicide. Homicide Stud. **300**, 310 (1999)
14. Raddi, G.: How GPS Tracking Technology Can Curb Domestic Violence, WIRED Magazine, 15 Jan 2019
15. Losavio, M., Elmaghraby, A., Losavio, A.: Ubiquitous Networks, Ubiquitous Sensors: Issues of Security, Reliability and Privacy in the Internet of Things, Ubiquitous Networking, Lecture Notes in Computer Science, Springer Nature Switzerland AG (2018)
16. The American Law Institute, Restatement of the Law, Second, Torts, § 652 (1977) (US)
17. Driver's Privacy Protection Act, 18 USC 2721, Prohibition on release and use of certain personal information from State motor vehicle records (2000) (US)
18. Electronic Privacy Information Center: The Drivers Privacy Protection Act and the Privacy of Your State Motor Vehicle Record. https://epic.org/privacy/drivers/. Accessed 26 Oct 2020
19. Kolodziej, K.W., Hjelm, J.: Local Position Systems: LBS Applications and Services. CRC Press (2017)
20. Charter, Geographic Location/Privacy Working Group, Internet Engineering Task Force, 2001-06-14. https://datatracker.ietf.org/doc/charter-ietf-geopriv/. Accessed 16 Oct 2020

21. Gruteser, M., Liu, X.: Protecting privacy in continuous location-tracking applications. IEEE Security and Privacy Magazine (2004)
22. First Report of the Axon Artificial Intelligence and Policing Technology Ethics Board, June 2019
23. Nokia Corp. v. Apple Inc., 2011 U.S. Dist. LEXIS 158540 (United States District Court for the Western District of Wisconsin January 5, 2011, Filed)
24. Olympia Sauna Compania Naviera, S.A. v. United States, 670 F. Supp. 1498, 1987 U.S. Dist. LEXIS 13934, 1987 AMC 1530 (United States District Court for the District of Oregon April 14, 1987, Filed)
25. Morgan v. U.S. Xpress, Inc., 2006 U.S. Dist. LEXIS 7225 (United States District Court for the Middle District of Georgia, Columbus Division February 3, 2006, Filed)
26. Tokio Marine & Fire Ins. Co. v. Flora MV, 235 F.3d 963, 2001 U.S. App. LEXIS 22, 2001 AMC 1697 (5th Cir. 2001) (US)
27. Kane County v. United States, 2013 U.S. Dist. LEXIS 40118 (United States District Court for the District of Utah, Central Division March 20, 2013, Filed),
28. Brown v. State, 163 S.W.3d 818, 2005 Tex. App. LEXIS 3949 (Court of Appeals of Texas, Fifth District, 2005)
29. State v. Trott, 2016 N.J. Super. Unpub. LEXIS 651 (Superior Court of New Jersey, Appellate Division March 24, 2016, Decided)
30. United States v. Jackson, 918 F.3d 467, 2019 U.S. App. LEXIS 7201, 2019 FED App. 0041P (6th Cir. 2019)
31. United States v. Bailey, 2016 U.S. Dist. LEXIS 165162, 2016 WL 6995067 (United States District Court for the Western District of New York November 29, 2016, Filed)
32. Commonwealth v. Davis, 97 Mass. App. Ct. 633, 150 N.E.3d 770, 2020 Mass. App. LEXIS 72 (Appeals Court of Massachusetts June 11, 2020, Decided)
33. Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 113 S. Ct. 2786, 125 L. Ed. 2d 469 (1993)
34. Commonwealth v. Lanigan, 419 Mass. 15, 641 N.E.2d 1342 (1994)
35. Commonwealth v. Camblin, 471 Mass. 639, 640, 31 N.E.3d 1102 (2015) (Camblin I), S.C., Camblin II, 478 Mass. 469
36. Commonwealth v. Thissell, 457 Mass. 191, 198, 928 N.E.2d 932 (2010)
37. United States vs Katz, 389 U.S. 347 (1967)
38. United States v. Kyllo, 533 U.S. 27 (2001)
39. United States v. Jones, 565 U.S. 400 (2012)
40. United States v. Carpenter, 585 U.S. 2206 (2018) (US)
41. Riley v. California, 134 S.Ct. 2473 (2014) (US)
42. Chimel v. California, 395 U. S. 752 (1969) (US)
43. United States v. Robinson**,** 414 U. S. 218 (1973) (US)
44. Arizona v. Gant, 556 U. S. 332 (2009 (US)
45. Wyoming v. Houghton, 526 U.S. 295, 300 (1999) (US)
46. United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc) (US)
47. Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934, 1940 (2013)
48. United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc) (US), dissenting opinion of Judge Wynn
49. United States v. Carpenter, 585 U.S. 2206 (2018) (US), majority opinion by Roberts, Chief Justice
50. Olmstead v. United States, 277 U. S. 438, 473–474 (1928)
51. U.S. Constitution Amendment IV (1791)
52. United States v. Di Re, 332 U.S. 581 (1948)
53. Technology After Carpenter. Officer.com, September 1, 2018
54. Daniel Golightly. (June 21, 2018 Thursday). Carpenter v. United States May Set Digital Privacy Standard. Android Headlines
55. Cooley LLP. (June 29, 2018 Friday). Alert: Carpenter v. United States: What It Means for Companies that Collect Location Data. JD Supra

56. INSIGHT: Cracking Open a Can of Worms: Why Carpenter v. United States May Not Be the Privacy Decision That Was Needed or Wanted. PracticeView Database. (July 11, 2018 Wednesday)
57. 18 United States Code section 2703 (US)
58. Tim Cushing. (July 11, 2018 Wednesday). Post-Carpenter Ruling Says Call Records Aren't Content Or Cell Site Location Info; Thus, No 4th Amendment Protection. Techdirt
59. Polsinelli PC. (July 14, 2020 Tuesday). United States v. Gratkowski Beware of Inanimate Objects That Violate Your Privacy. Newstex Blogs National Law Review
60. James, D., LaVerne, D., Martinez, M., Schoeman, P.H., Ettari, S.V., Katz, A.W., Cohen, M.A., Shepson, S.B.: United States: U.S. Supreme Court Upholds Criminal Defendant's Fourth Amendment Interest in Cell Site Data Held by Third Party. Mondaq Business Briefing (2018)
61. De Zayas, D.: Comment: Carpenter V. United States And The Emerging Expectation Of Privacy In Data Comprehensiveness Applied To Browsing History. American University Law Review, 68, 2209 (August, 2019)
62. Kassotis, D.: NOTE: The Fourth Amendment and Technological Exceptionalism After Carpenter: A Case Study on Hash-Value Matching. Fordham Intellectual Property, Media & Entertainment Law Journal, 29, 1243 (Summer, 2019)
63. Wang, C.: Information Privacy And Data Security Laws: An Ineffective Regulatory Framework, Colum. Undergraduate L. Rev. (Oct. 31, 2017)
64. Lorenz, T., Schiering, I.: Privacy in location-based services and their criticality based on usage context. In: Friedewald, M., Önen, M., Lievens, E., Krenn, S., Fricker, S. (eds.) Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity 2019. IFIP Advances in Information and Communication Technology, vol. 576. Springer, Cham (2020)
65. Stored Electronic Communications Act, 18 USC § 2702 (US)
66. Directive 95/46/EC of the European Parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)
67. De, S.J., Le Métayer, D.: PRIAM: a privacy risk analysis methodology. In: Livraga, G., Torra, V., Aldini, A., Martinelli, F., Suri, N. (eds.) Data Privacy Management and Security Assurance. DPM 2016, QASA 2016. Lecture Notes in Computer Science, vol. 9963. Springer, Cham (2016)
68. Article 35, Directive 95/46/EC of the European Parliament and of the council of 24 October 1995
69. Hasanzadeh, K., Kajosaari, A., Häggman, D., Kyttä, M.: A context sensitive approach to anonymizing public participation GIS data: From development to the assessment of anonymization effects on data quality. Comput. Env. Urban Syst. **83** (2020)
70. Felson, M., Clarke, R.: Opportunity Makes the Thief: Practical theory for crime prevention, Police Research Series, Paper 98, Barry Webb, Ed., Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, Home Office, UK
71. Cahoo v. SAS Analytics, Inc, 912 F.3d 887 (6th Cir. 2019) (US)

Index

S. Paiva (ed.), *Precision Positioning with Commercial Smartphones in Urban Environments*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-71288-4