Location Tracking Using Smartphone Accelerometer and Magnetometer Traces

Khuong An Nguyen
Department of Computer Science,
Royal Holloway, University of London
Egham, United Kingdom
Khuong.Nguyen@rhul.ac.uk

Raja Naeem Akram,
Konstantinos Markantonakis
ISG-SCC, Royal Holloway, University of London
Egham, United Kingdom
r.n.akram,k.markantonakis@rhul.ac.uk

Zhiyuan Luo, Chris Watkins
Department of Computer Science,
Royal Holloway, University of London
Egham, United Kingdom
Zhiyuan.Luo,C.J.Watkins@rhul.ac.uk

ABSTRACT

We demonstrate a breach in smartphone location privacy through the accelerometer and magnetometer's footprints. The merits or otherwise of explicitly permissioned location sensors are not the point of this paper. Instead, our proposition is that other non-location-sensitive sensors can track users accurately when the users are in motion, as in travelling on public transport, such as trains, buses, and taxis. Through field trials, we provide evidence that high accuracy location tracking can be achieved even via non-location-sensitive sensors for which no access authorisation is required from users on a smartphone.

KEYWORDS

Smartphone, Location Tracking, Privacy, Zero-Permission Apps.

ACM Reference Format:
Khuong An Nguyen, Raja Naeem Akram, Konstantinos Markantonakis, and Zhiyuan Luo, Chris Watkins. 2019. Location Tracking Using Smartphone Accelerometer and Magnetometer Traces. In *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019) (ARES '19), August 26–29, 2019, Canterbury, United Kingdom.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3339252.3340518

1 INTRODUCTION

With the growing use of smartphones[1] and smartphone Apps, people are no longer just defined by who they are but also by where they are (location) and what activity they are taking part in (social networking/games). Many of the services provided by feature-rich smartphone Apps require access to your location – to serve your needs better. For example, Strava, a fitness App, revealed the location and staffing of military bases and spy outposts around the world. Strava collects the GPS information about their users' activities (walking, running and cycling) and charts them over a map - which was made public.

A study published by AT&T [5] in 2010 showed that 19 out of 20 mobile online social networks shared location information with third parties in a way that enabled easy identification of individual users.

Another revelatory example of the current situation on location privacy is the "PleaseRobMe[2]" that aggregated information from Foursquare[3] and other location services to identify homes that were empty – due to "oversharing" [7] of location information, homeowners have revealed that no one is at home. Such an emergent privacy threat is referred to as "Cybercasing" [3, 10].

Two of the major smartphone platforms (Apple iOS and Google Android) have deployed the user's explicit opt-in scheme for mobile sensors. In this scheme, a user is asked whether (s)he would permit an application to use a particular sensor. For this scheme, the sensors present in smartphones are categorised into sensors that require permission and sensors that do not. An application that uses sensors from the latter category (that does not require permission) is referred to as permission-less mobile App in this paper.

In some prior work (discussed succinctly in Section 2.2), it has been shown that some of the sensors that do not require permissions can be used to inference the location of a user. However, in this paper, we explore the possibility of tracking a users journey over public transport using a permission-less mobile App. The case scenario we consider relates to users being commuting either via a train, bus and/or taxi and based on non-location-sensitive sensors.

1.1 Paper's Contributions

The prime proposition of the paper is that non-location sensitive sensors used by a permission-less mobile App can accurately (to a high degree of confidence) location track users over public transport. In this respect, this paper contributes:

(1) A novel scenario where an adversary may mimic the sensor trace of a victim on a bus, by tailing him in a car behind in busy traffic. Additionally, we examine the data collection for four different sets of scenarios related to public transport, in which both the adversary and the victim are travelling on: a) a train, b) a taxi, c) a bus.

[1] A handset that can host and run applications, with additional features than just basic text and voice call.

[2] A website that states on their website "Our intention is not, and never has been, to have people burgled". Website: http://pleaserobme.com

[3] A mobile App that provides local search and discovery features about local attractions, best eateries and other facilities - based on user feedback. Since this revelation, they have changed their privacy policies.

ARES '19, August 26–29, 2019, Canterbury, United Kingdom

ACM ISBN 978-1-4503-7164-3/19/08…$15.00
https://doi.org/10.1145/3339252.3340518

(2) A permission-less mobile App that efficiently (with low computation and battery-consumption footprint) collects the non-location sensitive sensor data.
(3) Analysis technique and results to show successful location-tracking and location-proximity/co-location (two or more users being in proximity to each other at a particular point in time) using the non-privacy sensitive sensors.

In this paper, we will refer to location-tracking, location proximity and co-location frequently. Therefore, the definition of these terms in the context of this paper are:

- Location-Tracking: This relates to either collection location information directly from sensors like GPS, or inferring a user's location indirectly like WiFi networks and non-privacy sensitive sensors like accelerometer and magnetometer - as discussed in this paper.
- Location Proximity / Co-Location: Proximity or co-location detection relates to identifying two or more users being in the vicinity to each other – either through direct or indirect location tracking.

One point to note is that co-location without location tracking is just an assessment whether two (or more) devices are near each other without any GPS point of reference.

2 MOBILE SENSORS AND LOCATION PRIVACY

In this section, we briefly discuss off-the-shelve sensors, location privacy and prior work.

2.1 Mobile Sensor Access Privilege

Modern mobile phones (aka smartphones) are equipped with sensors, which are a silicon-based design that measures physical or environmental features. Table 1 lists the sensors available on an Android smartphone.

Table 1: Sensor Availability on Android Platform

Sensors	Privilege Access	Location Sensitivity
Accelerometer	No	Yes+
Bluetooth	Yes	Yes*
Geomagnetic Rotation Vector	No	No
GPS	Yes	Yes
Gyroscope	No	No
Magnetometer	No	Yes+
Network Location	Yes	Yes
Pressure	No	No
Sound	Yes	Yes*
WiFi	Yes	Yes
Light	No	No
Proximity	No	No
Relative Humidity	No	No
Ambient Temperature	No	Yes*

These sensors are categorised as privileged and un-privileged sensors. The privileged sensors are the one for whom you require explicit permission from the user (before using them), for un-privileged sensors no user permission is required. In Table 1, privileged sensors are represented as 'Yes' in the privilege access column. Furthermore, in the location sensitive column, we identify potential sensors that have location privacy implications. Some of these sensors, like ambient temperature do not have a direct inference of locations, but it can be used to build proximity inference of multiple devices to be at the same location (discussed in Section 2.2.2) - and if one of them is sharing GPS data, location of all other devices is easy to infer. For example, a crowd at a concert, where an application only needs one user to permit it for using GPS. All other devices can deny this permission, but their location can still be inferred. The representation 'Yes' in location sensitivity column means direct inference of location, 'Yes*' indicated indirect inference and 'Yes+' indicates that you can build location profiles of an environment (e.g., train or bus route) that later can be used for direct inference.

2.2 Prior Work in Location Tracking and Proximity Detection

There is a number of ways in which the location of a user can be tracked via smartphone and associated infrastructure. The two related methods for location tracking related to this paper are discussed as below:

2.2.1 Permission-less Mobile Applications. A mobile App collects non-location sensitive sensors, and from this data, users location is calculated.

Nawaz et al. [11] proposed the use of gyroscope and accelerometer to profile users travel patterns and based on these travel patterns notify the user about potential traffic alerts to enhance their travel experience.

Following the above-discussed work, Narain et al. [9] highlighted the privacy issues related to calculating a user location and his/her travel patterns using the side-channels (i.e. non-location sensitive sensors). They utilised gyroscope, accelerometer and magnetometer to construct the sensors data from both real routes and simulated ones (mimicking the real routes data). From this data, they constructed the graph of routes in a city and an efficient search mechanism to identify what profile of the three sensors matches with the which segment of the route (in a given city). They showed with high accuracy that they were able to identify the user routes based on the three sensors. For this analysis, they have collected data from an extensive simulation, where in our case we show that this extensive profiling can be replaced by proximity (similarity) between journeys collected from the users.

Here we would like to identify that both Nawaz et al. [11] and Narain et al. [9] were primarily focused on the user travelling in a car in optimal conditions (e.g., not taking into account the traffic congestion, driving behaviour and vehicle/road conditions etc.). These conditions in many cases influence the sensor readings and can give false results (false positive, false negative). Furthermore, they were looking into the gyroscope and accelerometer together to track users. In the case of Narain et al. [9], he also utilised magnetometer in their papers. Our experiments, detailed in this paper are different because:

- We collected data from taxies (car), buses and trains that include the environmental conditions (congestion, behaviour and vehicle/road condition).

- For location identification, we utilised the notion of proximity with a higher degree of GPS correlation rather than route profiling.
- We use the accelerometer for taxi and bus, where for trains we include the magnetometer. For taxi and bus, the magnetometer was not an effective data source in our trials.
- We also ran a bus and a car shadowing the bus, to explore the potential of tracking users across vehicles with high accuracy travelling on the same route at the same time.

2.2.2 Proximity Detection based on Sensors. Halevi et al. [4] demonstrated the suitability of using ambient sound and light for proximity detection. Here, the authors analysed the sensor measurements collected for 2 and 30 seconds duration for light and audio respectively – using a range of similarity comparison algorithms. Extensive experiments were performed in different physical locations, with a high success rate in detecting co-located devices.

Truong et al. [13] evaluated four different sensors. Similarly to previous studies, their sample collection was from 10-120 seconds. Shrestha et al. [12] used specialised hardware known as Sensordrone, with many ambient sensors, but did not evaluate the commodity ambient-sensors available on commercial handsets, did not provide the sample collection duration, and only mentioned that data from each sensor was collected for a few seconds.

3 EXPERIMENTAL TESTBED DEVELOPMENT

This section describes our testbeds including the test devices, test environments, and the data processing platform.

3.1 Test devices

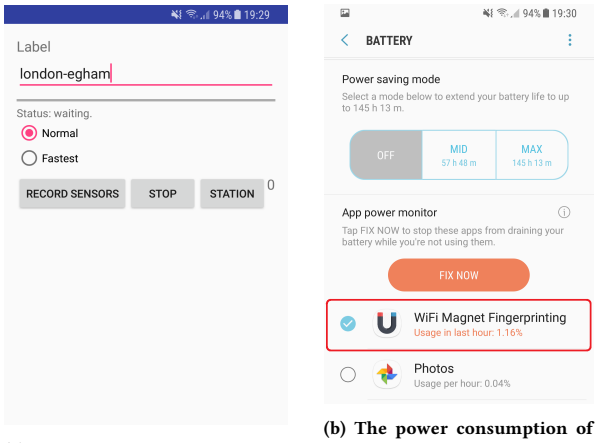
Six Android devices (five phones and one tablet) were used in this research, namely the Galaxy Nexus, LG Nexus 5, Samsung S4, Samsung S8, Lenovo Phab Pro 2, and Nexus 9, covering a variety of Android OS and sensor manufacturers. Their sensors' specifications are detailed in Table 2. Measurement-wise, all sensors on our test devices achieve a fine-grained sampling rate at a minimum of 49.65 Hz (about 50 samples per second) for the magnetometer and 99.5 Hz for the accelerometer, with the latest model capable of doubling these numbers. In all experiments, our devices were held naturally in the hands, left in the pocket or in the bag of their respective owners. Their local clocks were synchronised before each experiment by setting to the same time zone, then connecting to the Google server to get the current time.

Table 2: The sensors specifications of our test devices.

	G. Nexus	Nexus 5	S. S4	S. S8	Lenovo 2	Nexus 9
Magnetometer sampling rate	100 Hz	50 Hz	100 Hz	100 Hz	50 Hz	100 Hz
Accelerometer sampling rate	100 Hz	200 Hz	100 Hz	500 Hz	200 Hz	100 Hz
Release date	2011	2013	2013	2017	2016	2014
Android OS	4.3	5.0.1	5.0.1	7.0	6.0.1	6.0.1

3.2 Test environments

We set out to examine the sensor traces on all types of public transport in London (i.e. taxi, bus, and train), using our test devices described above. The test routes were chosen to cover a vast amount of areas in London (see Table 3 and Figure 2).



(a) The user interface of data collection app.

(b) The power consumption of our app was estimated at just over 1% in one hour.

Figure 1: The Android app we developed for this work.

Table 3: The details of the test routes.

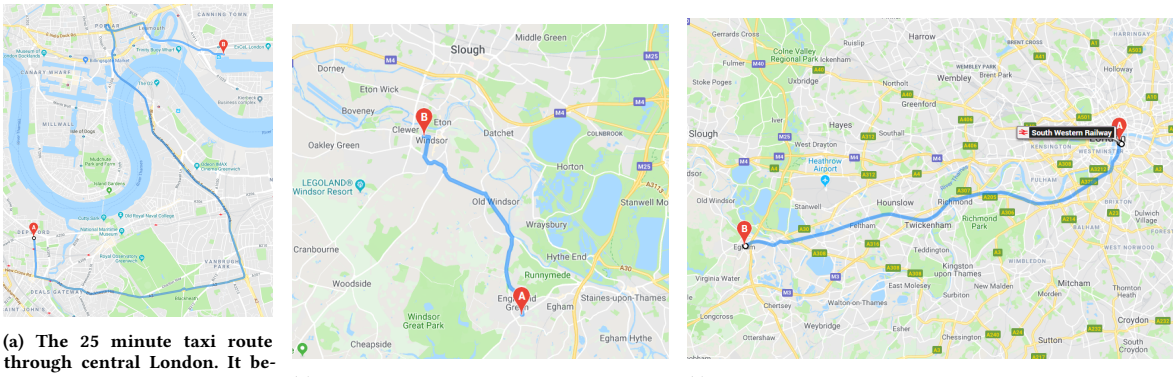
	Taxi	Bus	Train
Distance travelled	11.6 km	10 km	34 km
Duration	25 minutes	25 minutes	40 minutes
Number of stops	3	19	6

3.3 Sensor Data Collection

We developed an Android app that runs passively in the phone's background to record the sensors' readings into a text file stored locally on each device (see Figure 1a)[4]. The app's interface was intended to be minimalistic, which only requires the user attention to specify the file name and how frequently the app should log the sensors. The 'Station' button allows the users to specify if she has arrived at a station to aid the data analysis. At the end of the trial, the data file will be transferred to a PC for further analysis. The format of the file is as follows. Each line describes a snapshot of all sensors' measure, accompanied by a time stamp. For this paper, we will examine just the accelerometer and magnetometer. Both of these sensors report three measures per inquiry, corresponding to the strength along the (x, y, z)-axis.

Battery consumption wise, one hour of continuous inquiry and writing the data to a file on one of our test models consumed as little as 1% of battery, according to the inbuilt Android power measure as shown in Fig1. It is worth noting that our current procedure is grossly unoptimised. The majority of the workload is originated from the I/O operation of flushing all sensors data into the phone's memory 100 times per second on 'normal' mode. In reality, the sampling rate could be reduced, and not all sensors need to be recorded. Additionally, we may compress the data before logging

[4]Our app can be downloaded free of charge on the Google App store, by searching for "Fingerprinting WiFi Magnet".



(a) The 25 minute taxi route through central London. It began in Deptford, and ended near the ExCeL exhibition centre.

(b) The 25 minute bus route. It began in Egham town, and ended near Windsor town.

(c) The 40 minute train route. It began at Waterloo station, and ended at Egham station.

Figure 2: The test routes visualised on Google Maps, using GPS data.

them into the memory, or reduce consecutive data with similar readings. Hence, there is room for further improvement.

3.4 Data Processing Platform

To analyse the sensors data and plot the results, we used Matlab (version R2017b) with the Signal Processing Toolbox, running locally on an Intel Core i7-4770k 3.50 GHz Desktop CPU with 16 GB of RAM.

Since the sensor of each phone has different sensitivities and sampling rates, we employed Dynamic Time Warping (DTW) to align the sensor traces [8]. DTW is a proven method with well-known applications in speech recognition research. In short, it stretches the shorter trace to match the longer one by finding the optimal warping path between them, using the following recursive steps.

(1) Given two time series vector $t = (t_1, \ldots, t_m)$ and $r = (r_1, \ldots, r_n)$, DTW finds the optimal warped path of length $k : (p_1, q_1), \ldots, (p_k, q_k)$ that minimises $\sum_{i=1}^{k} |t(p_i) - r(q_i)|$

(2) We define $D(i, j)$ as the DTW distance between t and r. $D(1, 1)$ is initialised as $|t(1) - r(1)|$.

(3) We recursively calculate

$$D(i,j) = |t(i) - r(j)| + min\left\{ \begin{array}{l} \text{D(i-1, j)} \\ \text{D(i-1, j-1)} \\ \text{D(i, j-1)} \end{array} \right\}$$

with $i = 1 : m$ and $j = 1 : n$.

To quantify the difference between each data sample, we used two metrics, namely the Euclidean distance and the Kullback-Leibler metric. Since the sensor trace may have different lengths, the DTW score is calculated as the sum of the difference between all aligned samples on the two traces, normalised by the length of the optimal warped path.

To assess the uniqueness of each sensor trace (i.e. what is the chance of two different routes having a similar sensor trace?), we will apply the 'Fourier transform' on each trace [14]. In short, it measures every possible cycle to identify if there are repeated patterns within the time series.

4 RESEARCH QUESTIONS

Having understood the theories and the objectives of permissionless Apps for co-location tracking, we are now in a good position to set out the following research questions to be examined later on.

(1) How similar are the accelerometer and magnetometer traces of passengers on the same public transport (i.e. taxi, bus, and train)?

(2) Is it possible for an adversary driving on a car to mimic the sensor trace of a victim riding on a bus on the same road? If so, how similar the traces will be?

5 EMPIRICAL EXPERIMENTS

This section conducts the experiments on the taxi, bus, and train to assess the research questions set out in Section 4.

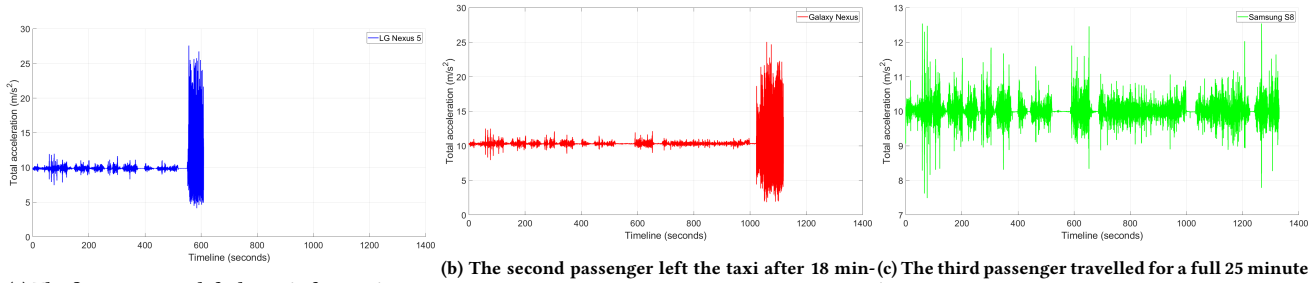
5.1 Experiment with the sensors trace in the taxi

To verify the similarity of the accelerometer and magnetometer's readings in the same car, three passengers shared one taxi for a 25-minute journey through central London (see Figure 2a). The first passenger left the taxi after 9 minutes, and the second one followed up after 18 minutes. Both of them continued walking for a few minutes after leaving the vehicle.

Figure 3 demonstrates that the accelerometer is capable of picking up the slightest changes in movements, not just when the car accelerates or decelerates, but also as it goes through speed bumps. The high measures from the accelerometer happened when the first and second passengers walked.

If we consider the portion of the traces, when all three passengers were together in the taxi, the overlapped sequence's shape was remarkably similar (see Figure 4a). To quantify this similarity, we compared the DTW scores of different portions of the traces including those that are not overlapped (see Table 4). The co-located traces scored consistently lower than non-co-located ones.

However, the magnetometer's traces of the passengers were relatively flat, with little spatial variation throughout the 9-minute drive (see Figure 4b). In addition, the spectrogram indicated that there were repeated patterns, due to the magnetic field's low spatial

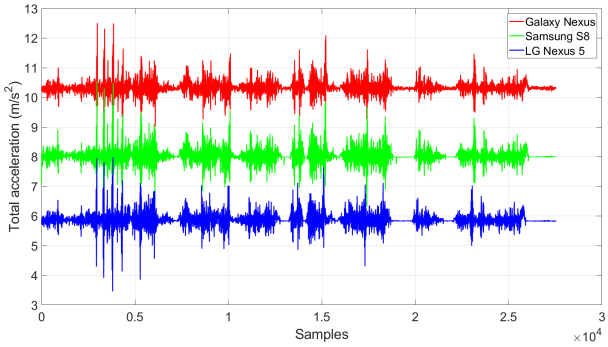


(a) The first passenger left the taxi after 9 minutes.

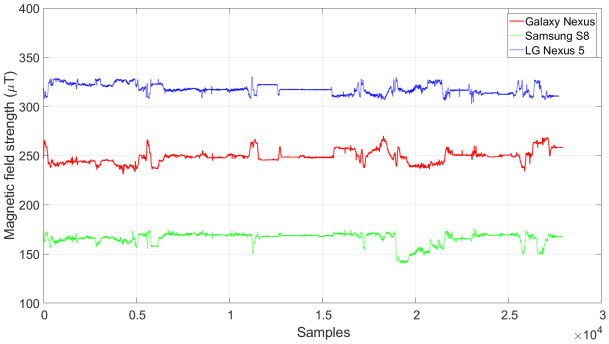
(b) The second passenger left the taxi after 18 minutes.

(c) The third passenger travelled for a full 25 minute journey.

Figure 3: The full accelerometer traces of three passengers in the same taxi. Note the high measures when the passengers travel on foot after leaving the taxi.



(a) The accelerometer traces in the taxi. The Samsung S8 and Nexus 5's traces were shifted 2 and 4 units vertically with respect to the Galaxy Nexus' trace for comparison purpose.



(b) The magnetometer measures in the taxi have very low spatial variation.

Figure 4: The overlapped sensor traces of three passengers travelling together in the same taxi for 9 minutes.

variation (see Figure 5). Since taxis are running on petrol, they do not alter the onboard magnetic field. The roads and pavements are a mixture of cement and sand which have no impact on magnetism. These conditions made it impractical for location tracking with the magnetometer traces.

Table 4: The DTW scores between different accelerometer traces on taxi and on foot (lower number means more similar). The co-located traces scored consistently lower than non-colocated ones.

	Euclidean	Kullback-Leibler
Co-located Galaxy Nexus & Nexus 5 on taxi	0.0776	0.0012
Co-located Galaxy Nexus & Samsung S8 on taxi	0.0991	0.0021
Co-located Nexus 5 & Samsung S8 on taxi	0.0525	0.00057
Nexus 5 on foot, Samsung S8 on taxi	1.8472	0.66055
Galaxy Nexus on foot, Samsung S8 on taxi	2.3226	1.1896

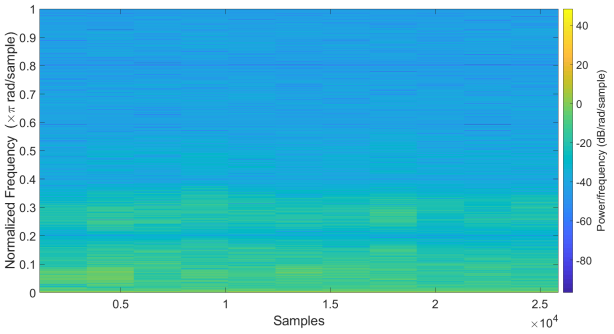
5.2 Experiment with the sensors trace on the bus

To verify the similarity of the sensor readings on the bus, four surveyors rode the same bus for 25 minutes (see Figure 2b). They sat in different places on the bus with their phones held naturally in their hands or left in pockets. Compared to the previous taxi experiment, the bus environment possesses similar features (i.e. both are petrol-based vehicles, running on the same road-material surface). Hence, its accelerometer and magnetometer traces are similar to the taxi's.

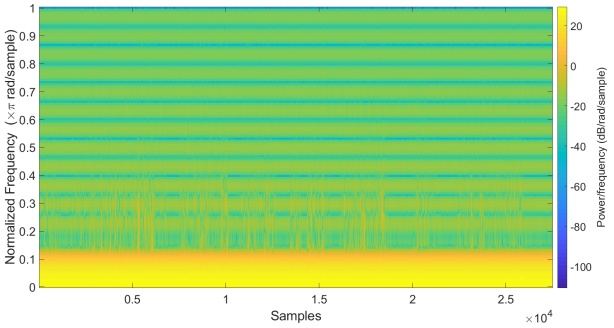
We applied the same methods to visually and computationally compare the sensor traces, as in the last experiment. A visual presentation of the four accelerometer traces revealed a similar shape (see Figure 6a), which was re-affirmed by their DTW scores (see Table 5). The magnetometer measure had low spatial variation, as expected, and would not be recommended to be used for sensor matching (see Figure 6b). Similarly, the spectrogram of the magnetometer trace indicated that there were repeated patterns, due to its low spatial variation, whereas the spectrogram of the accelerometer trace had no such indication (see Figure 7).

Table 5: The DTW scores between four accelerometer traces on the bus (lower number means more similar).

	Euclidean	Kullback-Leibler
Co-located Galaxy Nexus & Samsung S8 on bus	0.10141	0.0030335
Co-located Galaxy Nexus & Lenovo 2 on bus	0.085535	0.001989
Co-located Galaxy Nexus & Nexus 5 on bus	0.084074	0.001923



(a) The accelerometer's spectrogram indicates there is no clear repeated patterns.



(b) The magnetometer's spectrogram indicates there are repeated patterns, visualised by the horizontal lines.

Figure 5: The spectrogram of the accelerometer and magnetometer traces in the taxi to investigate the repeated patterns.

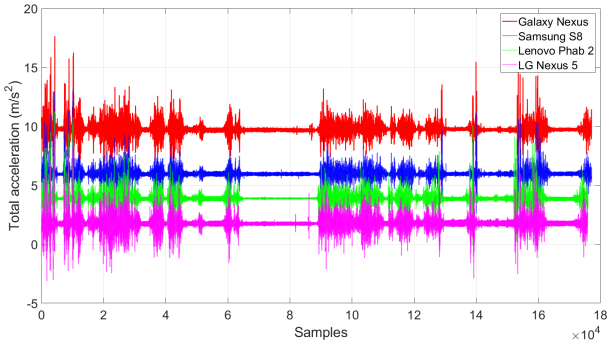
5.3 Experiment with the sensors trace on a car tailing a bus

Another potential scenario is matching the sensor measurements of two different users on a dissimilar mode of transport (a bus and a car in this instance). For this experiment, one rode the bus, while the other two tailing the bus in a car for a 20-minute journey.

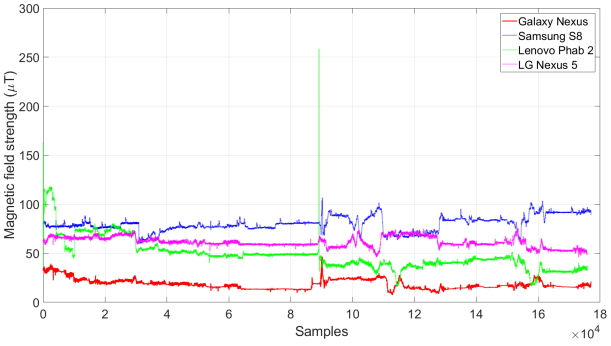
Figure 8 revealed a highly similar shape of the bus accelerometer trace, backed up by their DTW scores (see Table 6). Since the car followed behind the bus in the traffic, we considered the trace lag to be minimal (i.e. the impact of a speed bump on the bus was just about 1 second ahead).

Table 6: The DTW scores between one accelerometer trace on the bus and one in the car (lower number means more similar).

	Euclidean	Kullback-Leibler
Samsung S4 & Nexus 9 in car	0.11469	0.0030534
Samsung S4 in car & Samsung S8 on bus	0.12066	0.004992
Nexus 9 in car & Samsung S8 on bus	0.09675	0.0033772



(a) The accelerometer traces on the bus. The Samsung S8, Lenovo 2 and Nexus 5's traces were shifted 2, 4 and 6 units vertically with respect to the Galaxy Nexus' trace for comparison purpose.



(b) The magnetometer traces on the bus have very low spatial variation. Note the unusual spike of one device was caused by the electric noise.

Figure 6: The sensor traces of four passengers riding on the same bus for 25 minutes.

5.4 Experiment with the sensors trace on the train

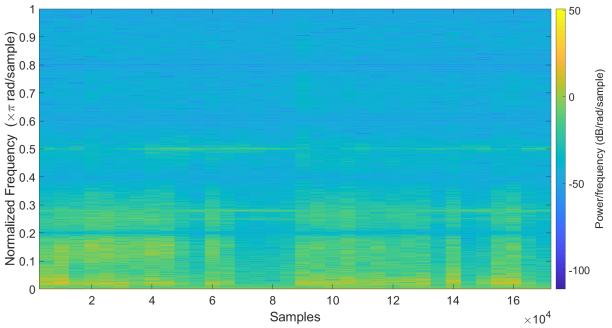
Compared to the last three experiments on the taxi and bus, trains are operated by electricity, which has a major impact on the onboard magnetic field.

For this experiment, four surveyors sat in different places throughout the train for a 40-minute journey (see Figure 2c). A visual presentation of the four accelerometer and magnetometer traces revealed a similar shape (see Figure 9a), backed up by their DTW scores (see Tables 7 and 8).

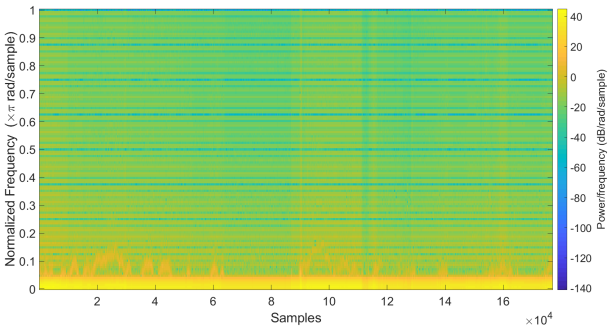
Table 7: The DTW scores between four accelerometer traces on the train (lower number means more similar).

	Euclidean	Kullback-Leibler
Co-located Galaxy Nexus & Samsung S8 on train	0.0757	0.0011091
Co-located Galaxy Nexus & Lenovo 2 on train	0.03	0.00019595
Co-located Galaxy Nexus & Nexus 5 on train	0.0870	0.0014

However, the spectrogram of the accelerometer traces indicated that there might be some repeated patterns, whereas the spectrogram of the magnetometer had no such indication (see Figure 10).



(a) The accelerometer's spectrogram indicates there is no clear repeated patterns.



(b) The magnetometer's spectrogram indicates there are repeated patterns, visualised by the horizontal lines.

Figure 7: The spectrogram of the accelerometer and magnetometer traces on the bus to investigate the repeated patterns.

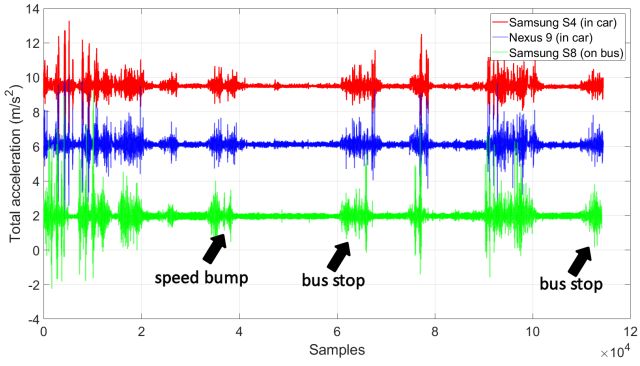
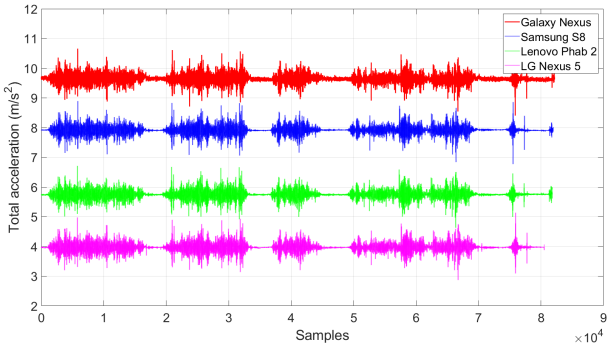
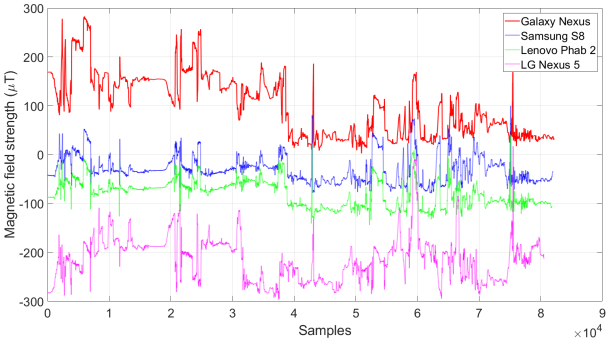


Figure 8: The accelerometer traces of two phones in car tailing another phone on a bus. The Nexus 9 and Samsung S8's traces were shifted 4 and 8 units vertically for the Samsung S4's trace for comparison purpose. The overall shape of the whole journey is similar.

The reason was that trains often run at a constant speed in long trips, and only accelerated at the beginning, and decelerated by the end of the next stop.



(a) The accelerometer traces on the train. The Samsung S8, Lenovo 2 and Nexus 5's traces were shifted 2, 4 and 6 units vertically with respect to the Galaxy Nexus' trace for comparison purpose.



(b) The magnetometer traces on the train. The Samsung S8, Lenovo 2 and Nexus 5's traces were shifted 100, 200 and 300 units vertically with respect to the Galaxy Nexus' trace for comparison purpose.

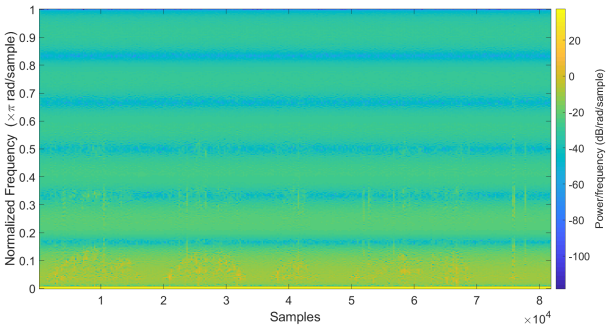
Figure 9: The sensor traces of four passengers travelling on the same train for 40 minutes.

Table 8: The DTW scores between four magnetometer traces on the train (lower number means more similar). Note that the magnetometer measures are on a different scale unit than the accelerometer ones.

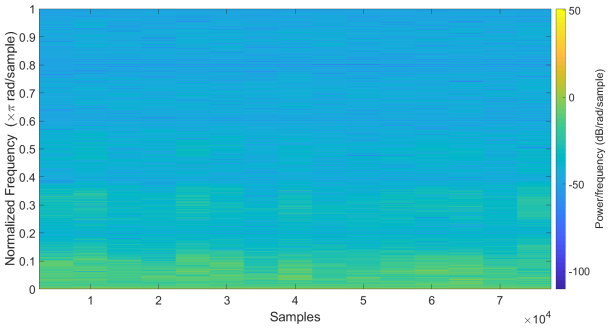
	Euclidean	Kullback-Leibler
Co-located Galaxy Nexus & Samsung S8 on train	31.0739	14.7643
Co-located Galaxy Nexus & Lenovo 2 on train	7.7437	1.7670
Co-located Galaxy Nexus & Nexus 5 on train	14.4307	10.2470

5.5 Summary of the experimental results

In this part, we briefly summarise the results obtained in previous sections, addressing the research questions outlined in Section 4. Firstly, the accelerometer traces of the passengers in the same vehicle demonstrated promising similarity, through-out the experiments on a taxi, bus, and train. Secondly, the accelerometer measures showed a high spatial variation on taxis and buses, thanks to the frequent accelerations, decelerations, and the uneven surface of the roads (e.g. speed bumps). The accelerometer's measures may be applied to match passengers' traces. However, since trains tend to run at a constant speed during long journeys, the traces are not



(a) The accelerometer's spectrogram indicates there may be some repeated patterns, visualised by the horizontal lines, although they are not perfectly clear.



(b) The magnetometer's spectrogram indicates there is no repeated patterns.

Figure 10: The spectrogram of the accelerometer and magnetometer traces on the train to investigate the repeated patterns.

as distinctive as those on taxi and bus. Thirdly, the magnetometer measures were distinctive on the trains, but not on the taxis and buses. The reasons were that the trains in London are powered by electricity, and the rail-lines are made of metal composite materials, which alter on the onboard magnetic field. In contrast, London taxis and buses are petrol-based vehicles. The roads are also a mixture of sand and cement which have no impact on the magnetic field. Fourthly, we demonstrated the possibility of mimicking the accelerometer trace on a bus, by tailing it in a car on the same road in busy traffic. Finally, a summary of the sensors' potential usage for location tracking, drawn from the above experiments, is outlined in Table 9.

Table 9: A summary of the potential usage of mobile sensors for location tracking.

	Difference in magnetometer traces	Difference in accelerometer traces
For Taxi	Low	High
For Bus	Low	High
For Train	High	Average

6 PRIVACY IMPLICATIONS AND POTENTIAL WAY FORWARD

This section briefly discusses the implication of this work and potential defence mechanism with their pros and cons.

6.1 Location Privacy and Mobile Sensors

In this paper, we have shown with field trials that non-location sensitive mobile sensors can be used to track users over public transport. Our results show that the existing techniques that limit the sensor permission to perceived location sensitive sensors are not effective. The results of this paper, along with the prior research discussed in Section 2.2.1 provides clear evidence that sensors that are perceived to have no privacy consequences like magnetometer can, in fact, enable location tracking.

Location data is privacy-sensitive, and there is a number of regulations that enshrine user's rights about location privacy. For example, the US Congress Location Privacy Protection Act 2014. Furthermore, with evolving regulation around the world like the introduction of General Data Protection Regulation (GDPR) [2] will require the management of data collected via sensors that are not deemed privacy sensitive to be carefully considered. If an application developer uses these sensors for legit reasons, they still have to treat them as privacy sensitive information and under GDPR they might be liable for hefty fines if they do not adequately protect this information.

6.2 Potential Way Forward

One of the main position privacy campaigners have taken is the concept of "choice and informed consent" about data collection from individual users. This concept does not take into account:

- User awareness of technology, including the unintended consequence of it.
- Complexity of length terms and conditions that normal users will not read and issues with such a position.
- Lack of transparency about and control on privacy data - after it is being collected.

For the unintended sensor access problem highlighted in this paper, a potential countermeasure proposed based on choice and informed consent include "Sensor Guardian" [1], which extends the application permissions to traditionally considered non-privacy sensitive sensors.

Normal users want flexibility, convenience and least among of hassle to perform their tasks, asking for additional permission at regular intervals has the potential of desensitising them [6]. A potential solution can be towards behaviour analysis of the applications that are accessing sensor data. If an application is accessing data often and for longer periods of time, the application may be tracking the user.

7 CONCLUSION

This paper put forward a proposition that users can be location tracked over public transport using non-location sensitive sensors to high accuracy. To empirically support this statement, we developed a low footprint mobile application for data collection and an efficient analysis framework. We collected sensor data for

accelerometer and magnetometer over four different settings - ranging on different public transport mechanisms including taxi, bus, and train. The results of our experiments showed that a user could be accurately tracked over the public transport network. Furthermore, we stipulated that the standard option of choice and informed consent might not be a preferable solution. To conclude as future research, we will investigate the behaviour based sensor privacy guard that can prevent sensor data access if an application is behaving as such that it is tracking a user via non-location sensors.

REFERENCES

[1] Xiaolong Bai, Jie Yin, and Yu-Ping Wang. 2017. Sensor Guardian: prevent privacy inference on Android sensors. *EURASIP Journal on Information Security* 2017, 1 (08 Jun 2017), 10. https://doi.org/10.1186/s13635-017-0061-8

[2] 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* L119 (4 May 2016), 1–88.

[3] Gerald Friedland and Robin Sommer. 2010. Cybercasing the Joint: On the Privacy Implications of Geo-tagging. In *Proceedings of the 5th USENIX Conference on Hot Topics in Security (HotSec'10)*. 1–8.

[4] Tzipora Halevi, Di Ma, Nitesh Saxena, and Tuo Xiang. 2012. Secure Proximity Detection for NFC Devices Based on Ambient Sensor Data. In *Computer Security – ESORICS 2012*, Sara Foresti, Moti Yung, and Fabio Martinelli (Eds.). 379–396. https://doi.org/10.1007/978-3-642-33167-1_22

[5] Balachander Krishnamurthy and Craig E. Wills. 2010. Privacy Leakage in Mobile Online Social Networks. In *Proceedings of the 3rd Wonference on Online Social Networks (WOSN'10)*. 4–4.

[6] Kat Krol, Matthew Moroz, and M Angela Sasse. 2012. Don't work. Can't work? Why it's time to rethink security warnings. In *risk and security of internet and systems (CRiSIS), 2012 7th International conference on*. 1–8.

[7] Hai Liang, Fei Shen, and King-wa Fu. 2017. Privacy protection and self-disclosure across societies: A study of global Twitter users. *new media & society* 19, 9 (2017), 1476–1497.

[8] Meinard Müller. 2007. Dynamic time warping. *Information retrieval for music and motion* (2007), 69–84.

[9] Sashank Narain, Triet D. Vo-Huu, Kenneth Block, and Guevara Noubir. 2016. Inferring User Routes and Locations Using Zero-Permission Mobile Sensors.. In *IEEE Symposium on Security and Privacy*. 397–413.

[10] Arvind Narayanan, Narendran Thiagarajan, Mugdha Lakhani, Michael Hamburg, Dan Boneh, et al. 2011. Location Privacy via Private Proximity Testing.. In *NDSS*.

[11] Sarfraz Nawaz and Cecilia Mascolo. 2014. Mining users' significant driving routes with low-power sensors. In *Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems*. 236–250.

[12] Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, and N Asokan. 2014. Drone to the rescue: Relay-resilient authentication using ambient multi-sensing. In *International Conference on Financial Cryptography and Data Security*. Springer, 349–364.

[13] Hien Thi Thu Truong, Xiang Gao, Biva Shrestha, Navrati Saxena, N Asokan, and Petteri Nurmi. 2014. Comparing and Fusing Different Sensor Modalities for Relay Attack Resistance in Zero-Interaction Authentication. In *Pervasive Computing and Communications (PerCom), 2014 IEEE International Conference on*. IEEE, 163–171.

[14] William WS Wei. 2006. Time series analysis. In *The Oxford Handbook of Quantitative Methods in Psychology: Vol. 2*.