# A Privacy Preserving Mobile Crowdsensing Architecture for a Smart Farming Application

Lars Huning, Jan Bauer, and Nils Aschenbruck
University of Osnabrück - Institute of Computer Science
Osnabrück, Germany
{lhuning,bauer,aschenbruck}@uos.de

## ABSTRACT

Smart Farming refers to the act of utilizing modern information and sensor technology in conventional industrial farming. An important plant parameter that can be estimated by sensor technology in the context of Smart Farming is the leaf area index (LAI) which is a key variable used to model processes such as photosynthesis and evapotranspiration. Nowadays, leveraging the enhanced sensor peripherals of current devices and their computing capabilities, smartphone applications present a fast and economical alternative to estimate the LAI compared to traditional methods. This paper exemplarily extends such an application, namely Smart fLAIr, with features of Mobile Crowdsensing (MCS) in order to create a system for a crowd-sensed LAI enabling an increased spatio-temporal resolution of LAI estimations. Besides the system design, this paper conducts a threat analysis for user privacy in the application-specific scenario which can be transferred to general Smart Farming scenarios. As a consequence, a perturbation based privacy mechanism is developed and applied in conjunction with a Trusted Third Party (TTP) architecture to ensure user privacy. Subsequently, its impact is demonstrated. Moreover, the energy consumption of the extended Smart fLAIr application is evaluated showing negligible additional costs of the proposed MCS extension.

## CCS CONCEPTS

• **Networks** → **Network privacy and anonymity**; • **Applied computing** → *Environmental sciences*; • **Computer systems organization** → *Embedded and cyber-physical systems*;

## KEYWORDS

Mobile Crowdsensing, Privacy, Smart Faming, Leaf Area Index

**ACM Reference format:**
Lars Huning, Jan Bauer, and Nils Aschenbruck. 2017. A Privacy Preserving Mobile Crowdsensing Architecture for a Smart Farming Application. In *Proceedings of First ACM Workshop on Mobile Crowdsensing Systems and Applications, Delft, Netherlands, November 6–8, 2017 (CrowdSenSys),* 7 pages.
https://doi.org/10.1145/3139243.3139250


*CrowdSenSys, November 6–8, 2017, Delft, Netherlands*

ACM ISBN 978-1-4503-5555-1/17/11…$15.00
https://doi.org/10.1145/3139243.3139250

## 1 INTRODUCTION

Using modern information, communication, and sensor technology to improve the efficiency of agriculture is called *Smart Farming*. Information gained by this approach can be leveraged as decision support for various agricultural processes and allow for a sustainable and site-specific management of agricultural fields. An important plant parameter that can be estimated by modern sensor technology is the *leaf area index (LAI)*. The LAI is defined as the one-sided leaf area per unit horizontal ground surface area. It is the main variable of many models used to describe vegetative processes such as photosynthesis and evapotranspiration [21] and can also greatly support agricultural decisions and yield predictions. The LAI is usually estimated indirectly, i.e. it is derived by the measurement of a related quantity such as solar radiation. Available devices range from commercial hand-held instruments to in-situ Wireless Sensor Networks (WSNs) and Remote Sensing [18]. Recently, due to the technological progress in the smartphone evolution, a few indirect LAI approaches for smartphones were proposed. Implemented as a smartphone application (app) that can be installed on common devices, these approaches greatly reduce the hardware costs required by traditional approaches. They are promising to significantly increase in-situ LAI information and, thus, providing ground truth for validating Remote Sensing approaches.

Mobile Crowdsensing (MCS) is an emerging sensing paradigm that employs smartphone owners jointly measuring data via inbuilt smartphone sensors or additional sensor equipment to share these data or to provide them to a certain processing entity. This idea is very promising for being integrated into Smart Farming, particularly for in-situ assessments of plant parameters, and is sometimes referred to as *farmsourcing* [16]. LAI estimates, for instance, could be collectively gathered with a relatively high spatio-temporal resolution. These estimates could then be forwarded to another entity, e.g., commercial farm management information systems (FMISs) or related software platforms for agricultural services, analyzing and processing these data. This integration would have a significant added value for farming activities.

Besides an appropriate communication architecture, minimized energy consumption, and mechanisms for data quality and incentives, a core challenge in MCS systems is *privacy*. In order to properly analyze the data submitted by the users, it is necessary that the data are tagged with spatio-temporal information. However, without adequate privacy measures, many users might be unwilling to share this private information publicly or even with a tasking entity.

This paper proposes a privacy preserving MCS architecture for LAI apps. The architecture addresses two application-specific challenges: (1) the demand for a high spatial precision, since it is

important to reliably determine the location and the crop type for which a sample was measured, and (2) the typically sparse population in the vicinity of farming fields, which results in a comparably small number of participants, thus, impedes user privacy. The core contributions of this paper are: (1) a threat analysis for MCS systems in a smart farming context, (2) a privacy preserving MCS architecture for scenarios that require high spatial precision, based on a Trusted Third Party (TTP) and data perturbation, and finally (3) a prototypical MCS extension of *Smart fLAIr*[1], based on a widely used IoT messaging protocol, including a backend server and a prototype client.

The remainder of the paper is organized as follows: Section 2 presents related work in privacy preserving MCS architectures as well as specific privacy mechanisms for protecting spatio-temporal information. The basis for the MCS LAI app, Smart fLAIr, is briefly described in Section 3. Section 4 conducts a threat analysis in the application-specific scenario. Then, in Section 5, the developed privacy mechanisms as well as the designed architecture are described. The privacy mechanisms are evaluated and experiments regarding the energy consumption of the extended Smart fLAIr app are performed in Section 6. Finally, Section 7 concludes the paper.

## 2 RELATED WORK

One of the most common privacy models is *k-anonymity*, which has been introduced in the context of Location Based Services (LBS) in [8, 9]. Here, k-anonymity means that a user's spatio-temporal information is indistinguishable from at least $k-1$ other users. Spatio-temporal information is defined as a tuple containing three intervals $([x_1, x_2], [y_1, y_2], [t_1, t_2])$, where the $[x_1, x_2]$ and $[y_1, y_2]$ intervals describe the spatial coordinates of a user and the interval $[t_1, t_2]$ describes the time range in which the user was present at this location area [9]. A user's spatio-temporal tuple is then k-anonymous, if it overlaps the corresponding tuples of at least $k-1$ other users. The process of changing a precise value of data, i.e., a tuple of spatio-temporal information, to a more uncertain interval, is called *obfuscation* and is the most common method to achieve k-anonymity [8]. Approaches such as *l-diversity* [15] and *t-closeness* [14] extend the concept of k-anonymity and achieve an even stronger degree of privacy. Another complementary privacy method is data *perturbation* [5]. While obfuscation approaches anonymize data by creating an interval, perturbation approaches anonymize data by adding some form of noise to the sample. Another common privacy method in the literature is the use of a TTP. A TTP is an entity that the users trust with their original, precise spatio-temporal information. Its role is to anonymize the data of the users and distribute these anonymized data to LBS providers.

There are several privacy-aware participatory MCS architectures proposed in the literature. One privacy-aware participatory MCS architecture is called *PEPSI* [4]. It employs identity-based encryption in order to prevent unauthorized access by clients to a user's samples. While PEPSI prevents unauthorized clients from accessing user samples, authorized clients gain access to the raw, unanonymized data submitted by the users. In [23], a privacy-aware architecture for periodic data collection is proposed. It operates under the assumption that user privacy is ensured when neither a global eavesdropper nor the reporting service can link submitted reports to users. For that purpose, [23] employs a two-phase peer-to-peer scheme that utilizes public key encryption. In [5], a mathematical model of data perturbation and reconstruction techniques is developed for participatory MCS systems. It takes into account, that simply adding random noise to the data does not always ensure user privacy [11] and consequently develops a mechanism for users to perturb their data using a phenomenon-specific noise model. SSPEAR [7] tries to provide a comprehensive privacy architecture, where users can still be held accountable for their actions. The general idea is that users are uniquely identified via a device ID, whereas they submit samples using frequently changing pseudonyms.

While above privacy approaches are designed to protect users' spatio-temporal information, they are only partially suited for a Smart Farming scenario, as they take neither the high need for spatial precision nor the sparse population near farming fields into account. The system designed in this paper is a participatory MCS system. Hence, only privacy-aware participatory MCS systems from the literature are mentioned here, as opportunistic MCS systems face slightly different challenges regarding user privacy.

## 3 SMARTPHONE-BASED LAI ESTIMATION

The direct (i.e. mainly destructive) LAI measurement is infeasible in practice. For that reason, this important quantity is usually estimated by indirect approaches that basically measure the interaction of solar radiation with green vegetation by using photosynthetically active radiation sensors or digital hemispherical photography. Complementary to commercial hand-held instruments or novel agricultural WSNs, due to the technological evolution and proliferation of smartphones, a few indirect LAI apps were recently introduced such as *PocketLAI* [3] and *Smart fLAIr* [1]. These apps differ in their methodology and were evaluated in different type of crops. While currently mostly being used for scientific and farm consulting purposes [16], they were shown to achieve sufficient accuracy. However, none of the existing LAI apps feature MCS support yet. Therefore, we exemplarily developed an MCS extension for *Smart fLAIr* with a special focus on privacy and energy-efficiency, since both factors strongly affect user acceptance. However, our extension is generic and not limited to this specific smartphone app.

Smart fLAIr is an economical alternative for LAI estimation and implemented in Android. It takes advantage of the inbuilt ambient light sensor (ALS) to successively measure the luminance above and below the canopy. Using these measurements the LAI is subsequently derived. To mitigate the effects of small-scale environmental noise, several luminance readings are performed and averaged for each particular LAI estimation and located using the GPS sensor. For additional details of Smart fLAIr, please refer to [1].

## 4 THREAT MODEL AND PRIVACY GOALS

### 4.1 Privacy Attacks

To the best of our knowledge, there exist no dedicated surveys of possible privacy attacks against MCS systems. For this reason, this section will cover privacy attacks in general LBSs. A survey on such attacks is presented in [22]. In the first category, the attacker

[1] Smart fLAIr Android APK available at https://sys.cs.uos.de/smartflair/index.shtml

only has a single *snapshot* of spatio-temporal information. In the second and third category, the attacker is in possession of several snapshots. A priori, these snapshots are not linked in the second category, i.e., it is unknown which user submitted which sample. In the third category, such links are known a priori, e.g., via user pseudonyms that are part of the submitted samples.

*4.1.1 Single snapshot of spatio-temporal information.* Sometimes the size of obfuscation intervals for k-anonymity may be very limited. *Homogeneity attacks* [15] use this circumstance to breach user privacy in such cases. In case a spatial or temporal k-anonymity obfuscation interval stretches from an area with few users to an area with many users, a *distribution attack* [17] may conclude that the subject is in the area with few users. A *personal context linking attack* [9] uses personal information about the subject, e.g., about his hobbies or habits, in order to breach his privacy. In an *observation attack* [9], the attacker physically observes the subject to gather more context knowledge, i.e., in order to link a pseudonym with a real world identity. The *map matching attack* [13] can reduce obfuscation intervals, in case such intervals encompass physical areas which are (almost) inaccessible. In a *probability distribution attack* [19], the attacker uses probability distributions, e.g., about user mobility, in order to shrink the size of an obfuscation interval.

*4.1.2 Multiple unlinked snapshots of spatio-temporal information.* The main purpose of attacks in this category is the linking of several snapshots, which are available to the attacker, to specific users. A common approach to achieve this linking is the *location tracking attack* [9]. If a user's location is updated frequently, an attacker may link subsequent location updates to the same user. A more general form of a tracking attack is the *identity matching attack* [2]. It utilizes other, mostly user-specific, attributes that users provide to the LBS in order to link snapshots together.

*4.1.3 Multiple linked snapshots of spatio-temporal information.* In a *shrink region attack* [20] the attacker monitors changes in the k-anonymity set during consecutive messages. If the attacker is able to correlate consecutive messages being made by the same subject, changes in the k-anonymity set can be utilized to identify the user. A *region intersection attack* [20] can be used against simple obfuscation approaches. It calculates the intersections of subsequent location updates, which can be used to narrow down the subject's location. Using estimations of the subject's movement speed, the *maximum movement boundary attack* [6] calculates the maximum distance the subject could have moved between two subsequent location updates. Alternatively, the minimum duration needed to reach the locations of the updates is calculated. If the obfuscation interval is beyond this limit, it can be significantly reduced.

## 4.2 Threat Analysis

In the MCS extension of Smart fLAIr, users submit a variety of privacy sensitive information with each sample. These include the spatio-temporal information of the sample and, for future data quality and incentive extensions, a user pseudonym. Additionally, users may optionally provide the name of the crop whose LAI was measured. This name can be selected from an exhaustive list of crop names provided by the application. In some cases this crop name

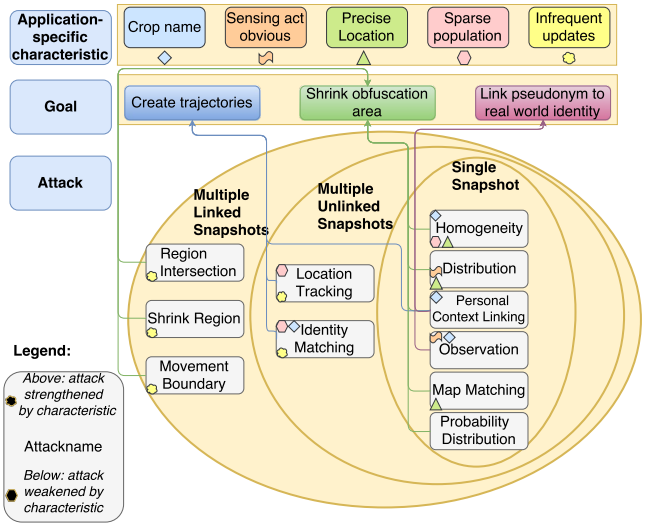


**Figure 1: Privacy attacks, their goals, and how they are influenced by application-specific characteristics.**

can serve as a quasi identifier, e.g., because a single user always provides the wrong crop name. The LAI value itself contains no personal information. However, the LAI, as estimated by Smart fLAIr, exhibits significant fluctuations throughout the day, depending on changes in environmental conditions such as the zenith angle of the sun or the cloud coverage. Due to the dependence on the zenith angle of the sun, the fluctuations in a single day are bigger than the fluctuations between two days when they are measured at the same time of day.

Figure 1 shows how the privacy attacks described in Section 4.1 are influenced by several scenario-specific characteristics. In order to properly analyze the gathered data, it is important that the spatial information of each sample is as precise as possible. It is common that different crops are located in neighboring farming fields, and imprecise spatial information could lead to ambiguity for which kind of crop the sample was measured. This characteristic prevents the use of many common privacy mechanisms that coarsen spatial information. The population near farming fields usually tends to be sparse. This makes user privacy more difficult, as users need to be anonymized in a small group of other users in their vicinity. Furthermore, it is easier for an attacker to link multiple samples to a specific user, if the overall number of users in the targeted area is small (location tracking and identity matching attack). Moreover, the physical act of measuring the LAI using a smartphone is clearly visible. Thus, no privacy measure can ensure user privacy, if the attacker can observe a user during a measurement (observation attack). As farming fields tend to cover a large area and there may be an arbitrary distance between two farming fields, users will only submit samples relatively infrequently. This weakens all attacks that depend on multiple snapshots of spatio-temporal information. The crop name which users may optionally provide has detrimental effects for user privacy, e.g., because it may serve as a quasi identifier in an identity matching attack or personal context linking attack.

### 4.3 Privacy Goals

According to [22], there are three kind of privacy goals in LBSs: the identity of a user, his spatial information, and his temporal information. Solely protecting user's identity is often not enough, because the user's identity can be inferred by coupling the spatio-temporal information of samples with additional context knowledge [22]. Thus, while the user identity should be protected, it is also necessary to protect either the subject's spatial or temporal information. The LAI is only measured in the vicinity of farming fields, which generally have no relationship with specific users (except perhaps living somewhere in the vicinity). Thus, location information holds only very limited value for attackers. As precise spatial information is an important requirement for the analysis of the gathered samples, we assume that users are willing to provide the exact location of their samples, if the other two privacy goals are met.

## 5 SYSTEM DESIGN AND IMPLEMENTATION

### 5.1 Privacy Measures

One privacy measure which is widely used in the literature and adopted by the system is the use of a TTP. This allows users to send additional, privacy sensitive data to the server, which are retained when clients query the backend server for samples. By doing so, the additional data are available only at the backend server for further computation, while not compromising user privacy, because the TTP is assumed to be a trusted entity. Thus, methods that result in the highest data quality, while still preserving user privacy, can be chosen. While the use of pseudonyms is detrimental to user privacy, it also offers many advantages, e.g., for data quality or incentive purposes. For example, malicious users can be banned only if these users can be identified (via a specific pseudonym). Additionally, many incentive mechanisms require users pseudonyms [12]. For this reason, users are required to submit samples with a pseudonym. However, this pseudonym is only visible to the TTP, i.e., the admin user and the backend server. Clients can only retrieve samples without their respective pseudonyms. While preventing client access to user pseudonyms strengthens user privacy, it is not sufficient. For example, if a user is the only one who submits samples in a certain area, this user can be linked to all samples within this area. As the population near farming fields tends to be sparse, this likelihood is not negligible in a Smart Farming scenario. This means that user privacy needs to be increased by coarsening either the spatial or temporal dimension of the samples. As high location precision is necessary for proper analysis of the LAI, the coarsening will be applied to the temporal dimension.

Common k-anonymity approaches face the challenge, that measurements by multiple users may be spread far apart in the temporal dimension in our scenario, because of the sparse population. This may result in a large distortion of the temporal information of the sample. Obfuscation approaches that do not use k-anonymity approaches, i.e., have arbitrary interval sizes, face the challenge that no other user may have submitted samples in this time range, thus, reducing the intended privacy gain. For this reason, perturbation approaches will be used to coarsen the time domain in farming applications.

Due to the fluctuations of the estimated LAI depending on the time of day, the day component of the samples is perturbed along with the minute component. The perturbation will be applied at two entities: once at the backend server and once at the Smart fLAIr application. The backend server can use additional information, e.g., knowledge of other samples, to perform a more intelligent perturbation than Smart fLAIr. The range of perturbation applied at the backend server is uniform random noise from the intervals $t_d^b = [-2, 2]$ days and $t_m^b = [-60, 60]$ minutes. Since the temporal behavior of the LAI regarding environmental factors is plant-specific and as, to the best of the our knowledge, there exist no adequate models that describe this behavior, adjusting the LAI value to the perturbed time is left for future work. As the perturbed time may lie in the future, the backend server ensures that samples are only returned to clients' requests in case the perturbed time has already passed. Furthermore, the samples which are accessible to clients will only be updated once a day. The perturbation of Smart fLAIr serves as a privacy mechanism for users that distrust the TTP, e.g., because they fear that it will be compromised. Users will be able to select two distinct perturbation values, the number of days and the number of minutes. However, to provide a certain data accuracy, users can only perturb their sample in the time intervals $t_d^s = [-1, 1]$ days and $t_m^s = [-60, 60]$ minutes.

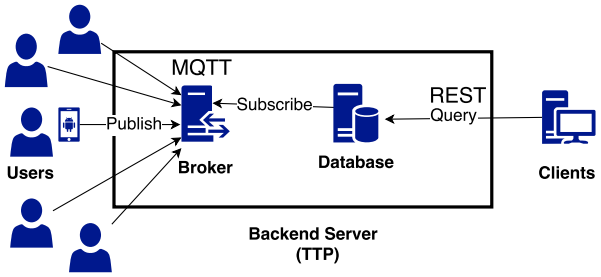


**Figure 2: Communication architecture overview. MCS participants publish and share samples on the broker, to which the database server is the only subscriber. Clients can query the database for anonymized samples.**

### 5.2 Communication Architecture

For the communication between the users' smartphones and the backend server, a widely used IoT messaging protocol, Message Queue Telemetry Transport (MQTT)[2], is employed. Its advantages are the small communication overhead as well as its publish-subscribe principle, which is well suited for MCS applications. Users measure data with the help of the extended Smart fLAIr app and publish these data via MQTT on a predefined topic on a broker running on the backend server. An additional application on the backend server is subscribed to this topic and is responsible for anonymizing those data and storing them into a database. In order to ensure the reliable delivery of each sample, we use Quality of Service (QoS) level 1 of MQTT. For the representation of LAI samples, we use a message format based on Protocol Buffers (protobuf)[3] that offers an efficient and platform-neutral binary serialization of structured data decreasing the communication overhead. Clients

[2] http://mqtt.org
[3] https://developers.google.com/protocol-buffers/

such as FMISs can get an anonymized version of these data by querying the backend server via a REST service, as it is a standard method of requesting data in the Internet. Figure 2 shows an overview of the communication architecture.

With regard to future incentive and data quality mechanisms, e.g., against malicious users, users have to register with the backend server before they can submit samples. This process is done automatically upon the first execution of the app. An *universally unique identifier (UUID)* is created and serves as the username, while a random integer from the interval $[0, 2^{130} - 1]$ is used as a password in its base-32 encoded form. All communication between the users' smartphones and the backend server is protected by Transport Layer Security (TLS), which provides encryption and integrity for the communication. Appropriate access control mechanisms at the broker ensure that only the backend server can subscribe to the topics for registration and sample submission. A prototype client that can query the backend server for new samples was realized as a web interface.

As WiFi access in rural areas in the vicinity of farming fields is likely to be very rare and to preserve the data volume of mobile communication, users have the option to postpone the delivery of samples. Instead of immediately transmitting samples via mobile infrastructure after recording, these samples are locally buffered until a dedicated button is pressed. Furthermore, the MQTT connection is kept alive for a user-chosen period (default: 15 min) after a sample has been published in order to prevent unnecessary connection initiations when a user submits several samples subsequently in a short time period and, thus, reduce the communication overhead.

# 6 SYSTEM EVALUATION

## 6.1 Impact of Privacy Measures

The privacy measures used in our system prevent the attacks described in Section 4.1. Figure 3 shows which attack is prevented by which privacy measure. Some of the attacks mentioned are not applicable, because they are designed against privacy measures that were not chosen for this system, e.g., k-anonymity. These include the homogeneity, the distribution, and the map matching attack as well as the shrink region and the region intersection attack. Other attacks are made more difficult by the employed privacy measures. The use of a TTP, which prevents access to the users' pseudonyms, weakens all attacks that link samples together as they contain no a priori identifier (location tracking and identity matching attack). This kind of attack is further mitigated due to the infrequent samples in the daily server updates, which will in most cases prevent linking of samples based on the spatio-temporal information. Only in some very specific circumstances, e.g., a person being the only user in a certain area, linking attacks can still be successful. Even in case such attacks are successful, the perturbation mechanisms ensure user privacy, as the attacker can no longer determine when the subject measured the sample exactly. This protects against probability distribution, location tracking, identity matching, and movement boundary attacks. It also weakens personal context linking and observation attacks. An attacker would gain only little personal information about the user in relation to the amount of context knowledge that is necessary to conduct a successful attack. Despite the large privacy gain by the perturbation of the samples with the

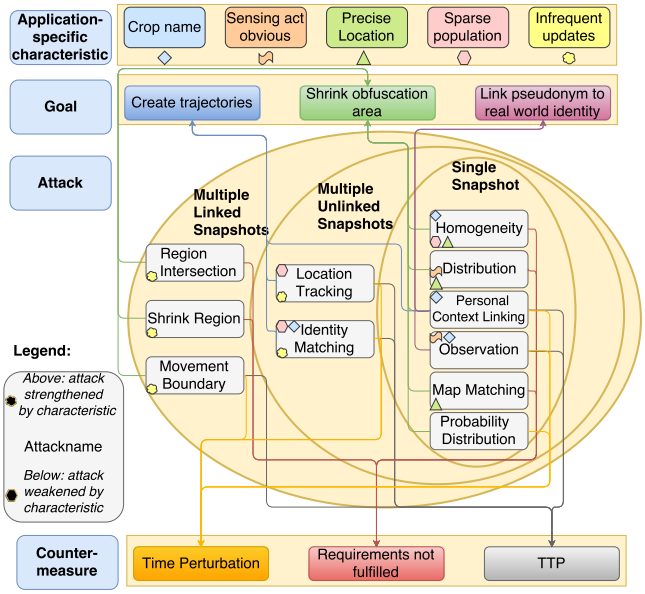


**Figure 3: Privacy attacks and how they are prevented by the privacy measures (assuming an uncompromised TTP).**

day component, the relatively slow growth of crops results in only marginally less data quality.

## 6.2 Energy Considerations

As field trials with the original Smart fLAIr revealed a high energy consumption, the energy consumption during the LAI estimation process is examined in this section, as well as the additional energy consumption by the integrated MCS features, i.e. essentially the communication to the backend server. For the evaluation of the energy consumption of Smart fLAIr, the *Trepn*[4] power profiler is used. According to [10], Trepn achieves the highest accuracy for energy consumption estimation among current energy profilers for smartphones. All measurements are conducted on a Sony Xperia Z1 smartphone (Android 5.1.1, Qualcomm Snapdragon 800 MSM8974 SoC, Kernel 3.4.0, Build 14.6.A.1.236).

First of all, the influence of various components during the LAI estimation process on the energy consumption is evaluated. These components are the GPS functionality, the ALS, and a live graph that displays the currently sensed luminosity for usability purposes. Afterwards, the additional energy consumption of the communication mechanism is measured, once with and once without TLS usage. During the communication experiments, a new sample is automatically created every second and sent to the backend server. All experiments are conducted over a period of 30 minutes. As the raw power oscillates with high frequency, a median filter over the range of one second is applied.

The results of the experiments are visualized in Figure 4. As expected, the active GPS sensor significantly increases the energy consumption (cf. (a) and (b)) The same observation can be made for the internal ALS (cf. (d) and (e)). While these components increase the energy consumption, they are mandatory system components.

[4]https://developer.qualcomm.com/software/trepn-power-profiler

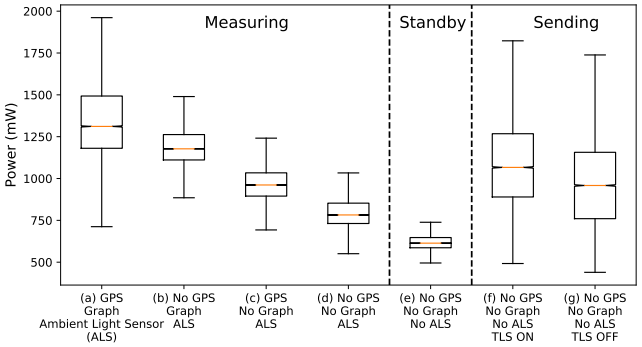


**Figure 4: Energy consumption of relevant Smart fLAIr components during the LAI measurement process and MCS communication in comparison with the standby consumption.**

However, the live graph, which displays the currently sensed luminosity, is merely a utility tool to aid the user while taking a measurement. Despite this, it consumes more energy than GPS sensor or the ALS (cf. (a) and (c)). This raises the general question of how important visual aids during the measurement process are in relation to the increased energy consumption in MCS systems. Hence, we decided to make the live graph an optional feature of Smart fLAIr that can be en- or disabled by the user.

As expected, the boxplots (f) and (g) reveal the higher energy overhead of TLS. Thus, privacy mechanisms that provide user privacy without using TLS may decrease the energy consumption of the MCS system. However, the absolute energy consumption during the sending process is smaller than the energy consumption during the measurement process. As the sending process only takes a fraction of the time the measurement process consumes (roughly 1:10), the negative impact of TLS on the total energy consumption is reduced. Thus, we strongly recommend TLS from security prospective. Overall, concerning the energy demand of the prototype app, we believe that neither Smart fLAIr nor the additional MCS extension will have an impeding impact on the user acceptance.

## 7 CONCLUSION AND FUTURE WORK

This paper presented a privacy preserving participatory Mobile Crowdsensing architecture for LAI smartphone applications. Based on a TTP and an application-tailored perturbation mechanisms, users can publish samples via MQTT to a backend server, while protecting their privacy. Furthermore, the energy consumption of the developed application was studied, revealing a trade-off between user aiding visualization and energy consumption. The concepts presented can be transferred to other crowdsensing applications with similar properties, e.g., wildlife monitoring. Future work could adjust the LAI value to the perturbed timestamps based on yet to be developed LAI models that also include other environmental conditions. Furthermore, other crowdsensing features, like data quality and incentive mechanisms could be integrated into our architecture.

## ACKNOWLEDGMENTS

This work was partially funded by the German Federal Ministry of Education and Research (BMBF) within the Program "Innovations for Tomorrow's Production, Services, and Work" (02K14A19K) and managed by the Project Management Agency Karlsruhe (PTKA). The authors are responsible for the contents of this publication.

## REFERENCES

[1] J. Bauer, B. Siegmann, T. Jarmer, and N. Aschenbruck. 2016. Smart fLAIr: a Smartphone Application for Fast LAI Retrieval using Ambient Light Sensors. In *Proc. of the 11th IEEE Sensors Applications Symposium (SAS)*. Catania, Italy.

[2] A. R. Beresford and F.Stajano. 2004. Mix Zones: User Privacy in Location-Aware Services. In *Proc. of the 2nd IEEE Annual Conf. on Pervasive Computing and Communications Workshop (PERCOMW)*. Orlando, Florida, USA, 127–131.

[3] R. Confalonieri, C. Francone, and M. Foi. 2014. The PocketLAI Smartphone App: an Alternative Method for Leaf Area Index Estimation. In *Proc. of the 7th Int. Congress on Environmental Modelling and Software (iEMSs)*. San Diego, California, USA, 288–293.

[4] E. De Cristofaro and C. Soriente. 2013. Extended Capabilites for a Privacy-Enhanced Participatory Sensing Infrastructure (PEPSI). *IEEE Transactions on Information Forensics and Security* 8, 12 (October 2013), 2021–2033.

[5] R. K. Ganti, Y. Tsai N. Pham, and T. F. Abdelzaher. 2008. PoolView: Stream Privacy for Grassroots Participatory Sensing. In *Proc. of the 6th ACM Conf. on Embedded Network Sensor Systems (SenSys)*. Raleigh, North Carolina, USA, 281–294.

[6] G. Ghinita, M. L. Damiani, C. Silvestri, and E. Bertino. 2009. Preventing Velocity-Based Linkage Attacks in Location-Aware Applications. In *Proc. of the 17th ACM SIGSPATIAL Int. Conf. on Advances in Geographic Information Systems*. Seattle, Washington, USA, 246–255.

[7] Stylianos Gisdakis, Thanassis Giannetsos, and Panos Papadimaitratos. 2014. SPPEAR: Security & Privacy-Preservering Architecture for Mobile Crowd-Sensing Applications. In *Proc. of the 2014 ACM Conf. on Security and Privacy in Wireless and & Mobile Networks (WiSec)*. Oxford, United Kingdom, 39–50.

[8] A. Gkoulalas-Divanis, P. Kalnis, and V. S. Verykios. 2010. Providing K-Anonymity in Location Based Services. *ACM SIGKDD Explorations Newsletter* 12, 1 (June 2010).

[9] M. Gruteser and D. Grunwald. 2003. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *Proc. of the 1st Int. Conf. on Mobile systems, Applications and Services (MobiSys)*. San Francisco, USA, 31–42.

[10] M. A. Hoque, M. Siekkinen, K. N. Khan, Y. Xiao, and S. Tarkoma. 2016. Modeling, Profiling, and Debugging the Energy Consumption of Mobile Devices. *Comput. Surveys* 48, 3 (February 2016).

[11] Z. Huang, W. Du, and B. Chen. 2005. Deriving Private Information from Randomized Data. In *Proc. of ACM Conf. on Management of data (SIGMOD)*. Baltimore, Maryland, USA, 37–48.

[12] L.G. Jaimes, I.J. Vergara-Laurens, and A. Raij. 2015. A Survey of Incentive Techniques for Mobile Crowd Sensing. *IEEE Internet of Things Journal* 2, 5 (October 2015), 370–380.

[13] J. Krumm. 2007. Inference Attacks on Location Tracks. In *Proc. of the 5th Int. Conf. on Pervasive Computing (PERVASIVE)*. Toronto, Canada, 127–143.

[14] N. Li, T. Li, and S. Venkatasubramanian. 2007. T-Closeness: Privacy Beyond K-Anonymity and L-Diversity. In *Proc. of the 23rd IEEE Int. Conf. on Data Engineering (ICDE)*. Istanbul, Turkey, 106–115.

[15] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam. 2007. L-diversity: Privacy Beyond K-Anonymity. *ACM Transactions on Knowledge Discovery from Data* 1, 1 (March 2007).

[16] J. Minet, Y. Curnel, A. Gobin, J.-P. Goffart, F. Mélard, B. Tychon, J. Wellens, and P. Defourny. 2017. Crowdsourcing for agricultural applications: A review of uses and opportunities for a farmsourcing approach. *Computers and Electronics in Agriculture* 142 (2017), 126–138.

[17] M. F. Mokbel. 2007. Privacy in Location-Based Services: State-Of-The-Art and Research Directions. In *Proc. of the 8th Int. Conf. on Mobile Data Management (MDM)*. Mannheim, Germany, 228.

[18] Y. Qu, Y. Zhu, W. Han, J. Wang, and M. Ma. 2014. Crop Leaf Area Index Observations With a Wireless Sensor Network and its Potential for Validating Remote Sensing Products. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing* 7, 2 (February 2014), 431–444.

[19] R. Shokri, G. Theodorakopoulos, J. Le Boudec, and J. Hubaux. 2011. Quantifying Location Privacy. In *Proc. of the 31st IEEE Symposium on Security and Privacy*. Oakland, California, USA, 247–262.

[20] N. Talukder and S. I. Ahamed. 2010. Preventing Multi-Query Attack in Location-Based Services. In *Proc. of the 3rd ACM Conf. on Wireless Network Security (WiSec)*. Hoboken, New Jersey, USA, 25–36.

[21] M. Weiss, F. Baret, G.J. Smith, I. Jonckheere, and P. Coppin. 2004. Review of Methods for In Situ Leaf Area Index (LAI) Determination: Part II. Estimation of LAI, Errors and Sampling. *Agricultural and Forest Meteorology* 121, 1-2 (January 2004), 37–53.

[22] M. Wernke, P. Skvrotsov, F. Duerr, and K. Rothermel. 2014. A Classification of Location Privacy Attackes and Approaches. *Personal and Ubiquitous Computing* 18, 1 (January 2014), 163–175.

[23] Y. Yao, L. T. Yang, and N. N. Xiong. 2015. Anonymity-Based Privacy-Preserving Data Reporting for Participatory Sensing. *IEEE Internet of Things Journal* 2, 5 (October 2015), 381–390.