Managing Privacy in LBAC Systems

Claudio Agostino Ardagna Marco Cremonini Ernesto Damiani
Sabrina De Capitani di Vimercati Pierangela Samarati
Dipartimento di Tecnologie dell'Informazione - Università degli Studi di Milano, Italy
{ardagna,cremonini,damiani,decapita,samarati}@dti.unimi.it

Abstract

One of the main challenges for privacy-aware location-based systems is to strike a balance between privacy preferences set by users and location accuracy needed by Location-Based Services (LBSs). To this end, two key requirements must be satisfied: the availability of techniques providing for different degrees of user location privacy and the possibility of quantifying such privacy degrees. To address the first requirement, we describe two obfuscation techniques. For the second requirement, we introduce the notion of relevance as the estimator for the degree of location obfuscation. This way, location obfuscation can be adjusted to comply with both user preferences and LBS accuracy requirements.

1. Introduction

Preserving user data privacy is one of the hottest topics in computer security. Security incidents, faulty data management practices and unauthorized trading of users personal information have often been reported in recent years, exposing victims to ID theft and unauthorized profiling [8]. These issues are raising the bar of privacy standards, fostered innovative research, and driven new legislations. Many approaches aimed at privacy protection focus on preventing leakage of personal information while in transit or once it has been released to an authorized party, for example, by delayed enactment of privacy preferences [10]. Others deal with minimizing unnecessary release of personal information. Our work addresses the latter concern in the framework of location-based services. Specifically, we consider privacy requirements for Location-Based Access Control (LBAC) systems, which are systems that require, for the provision of an online service, to evaluate conditions expressed with location-based predicates depending on the physical locations of users [1]. In the LBAC area, privacy has been mostly addressed by developing models and techniques that let users access anonymously to online services [2, 3, 6]. Solutions providing different degrees of privacy according to user preferences or business needs are instead less explored. For instance, obfuscation techniques applied to user locations are well-suited to degrade the location accuracy for privacy reasons. In this context, however, only solutions based on increasing the granularity of a location measurement have been investigated and implemented in practice [6, 7]. Moreover, the importance of striking a balance between obfuscating locations for privacy reasons and preserving an acceptable accuracy for LBAC policies evaluation is often mentioned but not yet fully supported. In particular, key for managing such contrasting requirements is the availability of an estimator (*relevance*, in our work) measuring, at the same time, the achieved privacy level and the required accuracy. This estimator should be independent from technological details of location measurements and from LBAC systems peculiarities. This way privacy and accuracy requirements can be evaluated, negotiated, compared, and integrated in a coherent framework.

2 Related work

Although privacy issues related to location technologies have gained great relevance only in recent years, several solutions already exist that can be partitioned in two classes: *anonymity-based* and *obfuscation-based.*

Anonymity-based solutions rely on the notion of *anonymity* [2, 3, 6]. Beresford and Stajano [2] present *mix zones* a method developed to enhance privacy in location-based services managed by a trusted middleware. The infrastructure provides an anonymity service by making unlinkable the users entering the *mix zones*, where all users are indiscernible from the one on the other, from the users leaving it. Bettini et. al. [3] propose a framework in charge of evaluating the risk of sensitive location-based information dissemination, and a technique aimed at supporting k-anonymity [9]. Gruteser and Grunwald [6] define k-anonymity in the context of location obfuscation, providing a middleware architecture and adaptive algorithms to adjust location information resolution, in spatial or temporal

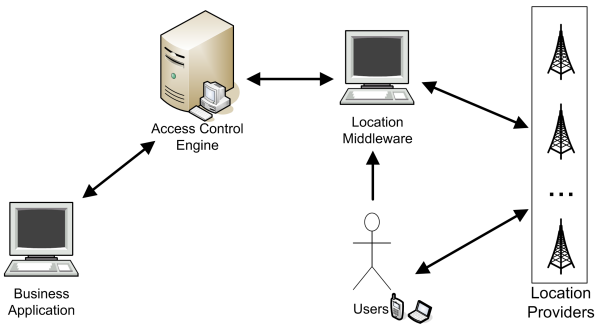

Figure 1. LBAC Architecture

dimensions, to comply with specified anonymity requirements. Our approach is complementary, rather than alternative, to these anonymity-based solutions because it is focused on situation where user identification is required and locations cannot be anonymized.

Obfuscation-based solutions adopt an approach similar to ours by developing different types of obfuscation techniques aimed at location privacy protection. Duckham and Kulik [5] set out a formal framework that provides a mechanism for balancing individuals needs for high-quality information services and location privacy. In the commercial arena some products provide obfuscation services based on location gateways [7]. Most products, such as Openwave, assume that users specify their privacy preferences in terms of a *minimum distance*. In general, these solutions share some limitations that our proposal aims to improve. First, they do not provide a quantitative estimation of the actual privacy level, making them highly dependent on the application contexts, and difficult to integrate into a full fledged location-based application scenario [1]. Second, all the implemented solutions support only a single type of obfuscation based on increasing the granularity of a location measurement. Our proposal includes instead different obfuscation solutions.

3 Reference Scenario

Our reference LBAC architecture (see Fig. 1) includes the *users*, whose location is captured through their mobile devices, and four components.

Business applications are generic customer-oriented applications whose resource accesses are ruled by LBAC policies. *Access control engine (ACE)* is the component for the enforcement of LBAC policies. *Location providers (LPs)* are companies providing user location measurements through sensing technologies (e.g., mobile phone companies). *Location middleware (LM)* is the core component of our architecture. It receives requests for location-based services from the ACE, which must be evaluated by collecting location measurements from a LP and by respecting the privacy preferences set by users.

In particular, the ACE requires to the LM a service that takes the form of a LBAC predicate evaluation whose value depends on location measurements. For instance, the LBAC predicate `inarea`(*user_term*, *area_term*) takes a *user_term* as first argument and an *area_term* as second argument, which denote a user identifier and a map region, respectively, and evaluates whether a user is located within a specific area (e.g., a city, a building) [1]. The ACE then receives from the LM a boolean response and an estimate of the *relevance* of that answer. The relevance is an estimator of the accuracy of the predicate evaluation and it is needed by the very nature of location-based information, which is radically different from other context-related knowledge inasmuch it is both approximate (all location systems have a margin of error) and time-variant (location is subject to fast changes, especially when the user is in motion). In addition, the LM has to satisfy privacy preferences set by users, whose effect in this paper is to further degrade location accuracy. Finally, given this intrinsic inaccuracy of LBAC predicate evaluation, the ACE is likely to set a threshold value for the evaluation accuracy. For values below such a threshold, the ACE may consider the evaluation not relevant to enforce LBAC policies.

Our work relies on two working assumptions: *i)* the area returned by a location measurement is circular, which is the actual shape resulting from many location technologies [4]; *ii)* the distribution of measurement errors within a returned area is uniform. For each user *u*, her location $Area(r, x_c, y_c)$, returned by a LP, is a *circular area* of radius *r*, centered in (x_c,y_c) that certainly contains the real user position (x_u,y_u).

Formally, if $f_r(x, y)$ is the probability density function (pdf) and the user location is $Area(r, x_c, y_c)$, the joint probability *P* is:

$$P((x_u, y_u) \in Area(r, x_c, y_c)) = \oint_{Area(r,x_c,y_c)} f_r(x, y)dxdy = 1$$

Since we assume that the probability distribution within an area is a *continuous uniform* distribution, the pdf is:

$$f_r(x, y) = \begin{cases} \frac{1}{\pi r^2} & \text{if } x, y \in Area(r, x_c, y_c) \\ 0 & \text{otherwise.} \end{cases}$$

The two assumptions, circular area and uniform distribution, simplify the analysis proposed in this paper without loss of generality.

4 User Preferences and Location Relevance

Several proposals in the location privacy field assume that users specify their privacy preferences in terms of a *minimum distance* [5, 7], since it is simple to understand

and implement. For instance, a user can require 100m as the minimum location accuracy, which, in this work, corresponds to an area of radius 100m. Obfuscation is then achieved by increasing the granularity of the measurement. The definition of a minimum distance, however, has two drawbacks: it is only meaningful when related to a specific application context, and it applies to just one specific obfuscation technique (i.e., increasing measurement's granularity).

A different way for users to specify privacy requirements consists in defining a *relative* degradation of the location accuracy, which is modeled through index $\lambda \in [0, \infty)$, where $\lambda = 0$ corresponds to no degradation, $\lambda \to \infty$ to full degradation, and intermediate values correspond to different degrees of degradation (e.g., $\lambda = 1$ corresponds to 100% of degradation). Although both minimum distance d and index λ are easy to specify for users, λ is a more general solution because independent from a specific location measurement and obfuscation technique.

To accommodate the peculiar characteristics of privacy-aware LBAC services, we introduce the notion of *relevance* as the estimator of the accuracy of all location-based measurements and evaluations. A relevance is a number $\mathcal{R} \in [0, 1]$, where value 0 means that the location information is completely inaccurate; value 1 means that the location information is completely accurate; and values in (0,1) means that accuracy is uncertain. The relevance estimator is associated with all location measurements managed by a LBS. The relevance depends on: *i)* the intrinsic measurement error of sensing technologies, and *ii)* the privacy preferences expressed by the users. According to our approach, the LM has to manage different relevance values that we now present.

LBAC relevance ($\mathcal{R}_{LBAC}$) is defined by the ACE and represents the minimum accuracy required by the ACE for a location measurement or for a location-based predicate evaluation. *Technological relevance* ($\mathcal{R}_{Tech}$) represents the accuracy of the location measurement provided by a LP given a mobile technology and its technical quality. *Privacy relevance* ($\mathcal{R}_{Priv}$) represents the accuracy of an obfuscated location and therefore the level of privacy. *Evaluation relevance* ($\mathcal{R}_{Eval}$) represents the accuracy of a LBAC predicate evaluation. Among these relevances, $\mathcal{R}_{LBAC}$ and $\mathcal{R}_{Tech}$ are assumed to be known, $\mathcal{R}_{Priv}$ derives from the privacy preferences expressed by users, and $\mathcal{R}_{Eval}$ is calculated by the system (see Section 6). In particular, $\mathcal{R}_{Priv}$ is defined as:

$$\mathcal{R}_{Priv} = (\lambda + 1)^{-1} \mathcal{R}_{Tech} \tag{1}$$

If privacy preference is expressed through a minimum distance r, it is straightforward to derive λ from r. The obfuscated area is then calculated by applying an obfuscation technique over the location measurement and by satisfying the user required uncertainty (i.e., $\mathcal{R}_{Priv}$).

Example 4.1 *Suppose that the ACE requires the LM to evaluate the* `inarea`(John, Milan) *predicate. The LM's goal is:* i) *to compute $\mathcal{R}_{Priv}$ according to formula (1);* ii) *to obfuscate the location returned by LP by reducing the location measurement relevance from $\mathcal{R}_{Tech}$ to $\mathcal{R}_{Priv}$;* iii) *to evaluate predicate* `inarea` *matching the geographical position of* Milan *with the obfuscated location of* John. *A boolean value is then returned by the LM together with an estimate of the relevance of the statement, i.e., $\mathcal{R}_{Eval}$. $\mathcal{R}_{Eval}$ is then compared with $\mathcal{R}_{LBAC}$ to check whether the privacy-aware location service is able to satisfy the requirement sets by the ACE.*

5 Obfuscation techniques for user-privacy

We now introduce two obfuscation techniques. In both cases, the idea is to modify the user location to reduce the accuracy until the privacy preference is matched. Users' preferences, as said, are expressed with index λ, which permits to calculate relevance $\mathcal{R}_{Priv}$ associated with the obfuscated location. The shape and position of the obfuscated area are then calculated.

5.1 Scaling the radius

By scaling the radius of the circular area $Area(r, x_c, y_c)$ from radius *r* to r_u (see Fig. 2(a)), the associated pdf decreases, that is, $\forall r, r_u : r < r_u \Rightarrow f_r(x, y) > f_{r_u}(x, y)$. The relevance $\mathcal{R}_{Priv}$ of the location information after spatial obfuscation can be derived from $\mathcal{R}_{Tech}$ by considering the ratio of the two pdf as the scalar factor:

$$\mathcal{R}_{Priv} = \frac{r^2}{r_u^2} \cdot \mathcal{R}_{Tech}, \quad with\, r < r_u \tag{2}$$

Given the privacy preference $\lambda \geq 0$, the radius of the obfuscated area r_u is calculated from (1) and (2) as follows:

$$r_u = r\sqrt{\lambda + 1}$$

In this case, for evaluating the LBAC predicate, LM uses the obfuscated area having same center of the area measured by LP and radius r_u.

5.2 Shifting the center

Shifting the center of the area returned by the LP is another way of obfuscating a user's location measurement. The obfuscated area is derived from the original area by calculating the distance d between the two centers. Let $Area(r, x_c + \Delta x, y_c + \Delta y)$ be the obfuscated

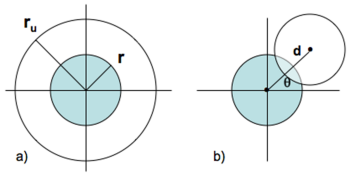

Figure 2. Scaling (a) and shifting (b)

area. If the distance d is equal to $2r$, then $P((x_u, y_u) \in Area(r, x_c + \Delta x, y_c + \Delta y)) = 0$; otherwise (i.e., $0 < d < 2r$), $0 < P((x_u, y_u) \in Area(r, x_c + \Delta x, y_c + \Delta y)) < 1$.

The privacy gain, in this case, can be measured by considering the intersection of the original and obfuscated areas, denoted $Area_{Tech \cap Priv}$. Intuitively, the degree of privacy is inversely proportional to the intersection of the two areas and therefore it is directly proportional to the distance d between the two centers. In particular, if $d = 0$, there is no privacy gain; if $d = 2r$, there is maximum privacy; and if $0 < d < 2r$, there is an increment of privacy. We stress the fact that we do not consider acceptable to produce obfuscated areas disjoint to the original location area. The reason is that, having all of them probability equals to zero of including the real user location, they are indiscernible for our relevance estimator and must be considered as false location information. LBS and related applications cannot, in general, deal with false information to provide a service.

With regard to angle θ (see Fig. 2(b)), there is no meaning for a user to specify it, so it must be defined by LM. Angle θ can be randomly chosen, since all values of θ are equivalent with respect to the privacy preferences of users. However, in the next section, we will discuss how LM can make a reasonable choice of this parameter to maximize the relevance $\mathcal{R}_{Eval}$. $\mathcal{R}_{Priv}$ is derived, starting from (1), as a composite probability.

$$\mathcal{R}_{Priv} = \frac{Area_{Tech \cap Priv} \cdot Area_{Tech \cap Priv}}{Area(r, x_c, y_c) \cdot Area(r, x_c + \Delta x, y_c + \Delta y)} \cdot \mathcal{R}_{Tech} \quad (3)$$

Given the privacy preference expressed by $\lambda \geq 0$, the distance d between the centers of the original and obfuscated area is calculated from (1) and (3) as follows:

$$(\lambda + 1)^{-1} = \frac{Area_{Tech \cap Priv} \cdot Area_{Tech \cap Priv}}{Area(r, x_c, y_c) \cdot Area(r, x_c + \Delta x, y_c + \Delta y)}$$

Expanding the term $Area_{Tech \cap Priv}$ as a function of distance d between the centers, we can calculate numerically distance d, and hence the obfuscated area.

6 LBAC predicate evaluation

The final task of the LM, once the obfuscated area has been produced, is to evaluate the LBAC predicate sent by the ACE and to calculate $\mathcal{R}_{Eval}$. The procedure for computing $\mathcal{R}_{Eval}$ is similar to the one adopted for computing $\mathcal{R}_{Priv}$ when the original area is obfuscated. During the obfuscation process, we have derived $\mathcal{R}_{Priv}$ starting from $\mathcal{R}_{Tech}$ (accordingly, we calculated the obfuscated area from the original measure). In this case, we must derive $\mathcal{R}_{Eval}$ from $\mathcal{R}_{Priv}$ and make use of the obfuscated area and the area specified by the LBAC parameter to calculate the scalar factor between the two relevances. Similarly to the obfuscation case, the relevance of the LBAC predicate evaluation depends on the degree of overlapping between the obfuscated area and the area identified by the LBAC parameter. We denote the obfuscated area simply as $Area_{Priv}$, the area defined by LBAC predicate as $Area_{LBAC}$,[1] and the intersection between the two areas as $Area_{Priv \cap LBAC}$. $\mathcal{R}_{Eval}$ can then be calculated as follows.

$$\mathcal{R}_{Eval} = \frac{Area_{Priv \cap LBAC}}{Area_{Priv}} \cdot \mathcal{R}_{Priv} \quad (4)$$

In the following, we provide two examples of LBAC predicates evaluation based on two location predicates: `inarea` and `distance` [1]. Specifically, `inarea(`*user_term*,*area_term*`)` evaluates whether *user_term* is located within *area_term*, and `distance(`*user*,*entity*,d_{min},d_{max}`)` evaluates whether the distance between *user* and *entity* is within the interval [d_{min},d_{max}].

Example 6.1 *Suppose that ACE requires user* John *to be located in* Milan *with a given relevance $\mathcal{R}_{LBAC}$ to access a service. Also, suppose* John*'s privacy preference requires that the actual accuracy of his location should be degraded of λ=0.25. To enforce John's access request, the ACE asks the LM to evaluate the predicate* `inarea(`John, Milan`)`, *where* John *represents the located user. Let the location measurement of* John *be $Area_{Tech}$ with $\mathcal{R}_{Tech}$=1 and from (1) let the relevance $\mathcal{R}_{Priv}$ be equal to 0.8. Fig. 3 shows graphically an example of $\mathcal{R}_{Eval}$ computation when the obfuscation by scaling the radius is applied. Since the intersection between the obfuscated area $Area_{Priv}$ and Milan is equal to two third of $Area_{Priv}$, the scalar factor $\frac{Area_{Priv \cap LBAC}}{Area_{Priv}}$ is equal to 0.75. From (4), we can produce the final relevance $\mathcal{R}_{Eval}$ associated with the predicate evaluation: $\mathcal{R}_{Eval}$=0.75 · $\mathcal{R}_{Priv}$=0.6. The predicate evaluation process is concluded and the result $(True, 0.6)$ is returned to the ACE. Finally, the ACE compares $\mathcal{R}_{Eval}$ with $\mathcal{R}_{LBAC}$, and if the quality of the evaluation satisfies the LBAC requirements,* John *gains the access.*

Example 6.2 *Suppose that the ACE requires* John *to stay at least 1000m away from a restricted area (i.e.,* Danger-

[1] Note that $Area_{LBAC}$ can assume different shapes depending on the predicate.

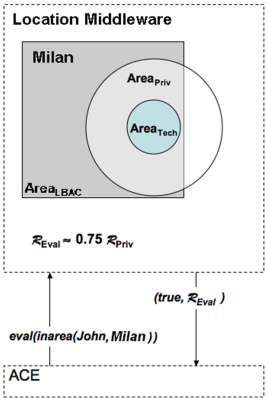

Figure 3. LM `inarea` predicate evaluation

ous *in Fig. 4) used for stocking dangerous material to access a given service. Again, John's privacy preference requires that the actual accuracy of his location should be degraded of* λ*=0.25. Whenever* John *submits an access request, the ACE asks the LM to evaluate the predicate* `distance`(John,Dangerous,d_{min},d_{max}) *, where* John *represents the located user,* d_{min}*=1000m, and* $d_{max} = +\infty$*. The predicate distance identifies an area* $Area_{LBAC}$ *(see grey area in Fig. 4), around the* Dangerous *area, which contains all the points outside the* Dangerous *area that have a distance between* d_{min} *and* d_{max}*. Let the location measurement of John be* $Area_{Tech}$ *with* $\mathcal{R}_{Tech}$*=1 and let the relevance* $\mathcal{R}_{Priv}$ *be equal to 0.2. Fig. 4 shows graphically an example of* $\mathcal{R}_{Eval}$ *computation when the obfuscation by shifting the center is applied. Since the intersection between the obfuscated area* $Area_{Priv}$ *and* $Area_{LBAC}$ *is equal to half of the* $Area_{Priv}$*, the scalar factor* $\frac{Area_{Priv \cap LBAC}}{Area_{Priv}}$ *is equal to 0.5. From (4), we calculate the final relevance* $\mathcal{R}_{Eval}$ *associated with the predicate evaluation:* $\mathcal{R}_{Eval}$=$\frac{Area_{Priv \cap LBAC}}{Area_{Priv}} \cdot \mathcal{R}_{Priv}$*=0.1. The predicate evaluation process is concluded and the result* $(True, 0.1)$ *is returned to the ACE meaning that* John *is far from the* Dangerous *area of at least* d_{min} *with a relevance of 0.1. Finally, the ACE, if possible, enforces* John*'s request.*

7 Maximization of $\mathcal{R}_{Eval}$

There is a subtlety to consider when obfuscation by shifting the center is applied. As already noted, there are infinite values of angle θ that could be chosen, all equivalent with respect to the $\mathcal{R}_{Priv}$ value. When the LBAC predicate is evaluated, however, the choice of θ is relevant, because according to the position of the obfuscated area, the value of $\mathcal{R}_{Eval}$ may change. The goal of LM is to maximize $\mathcal{R}_{Eval}$, because ACE compares it with the lower

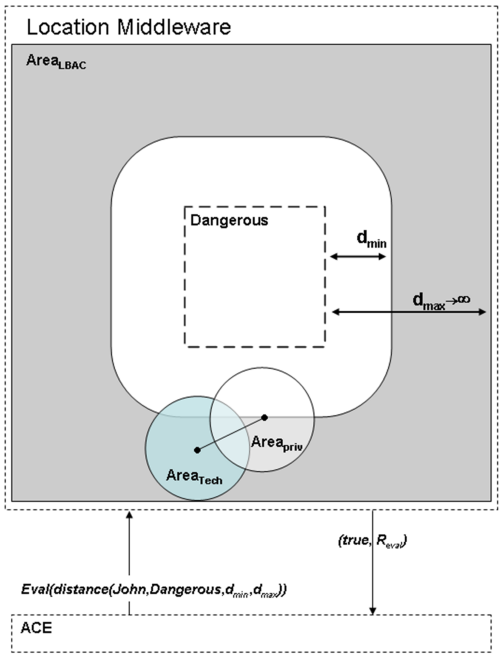

Figure 4. LM `distance` predicate evaluation

bound $\mathcal{R}_{LBAC}$ and the evaluation is considered valid only if $\mathcal{R}_{Eval}$ is greater than or equal to $\mathcal{R}_{LBAC}$. Fig. 5 shows an example with three obfuscated areas, namely *Area1*, *Area2*, and *Area3*, that provide the same $\mathcal{R}_{Priv}$ value and different $\mathcal{R}_{Eval}$ values, denoted $\mathcal{R}_{Eval}$(*Area1*), $\mathcal{R}_{Eval}$(*Area2*), and $\mathcal{R}_{Eval}$(*Area3*), respectively. It is easy to see that $\mathcal{R}_{Eval}$(*Area1*) is greater than $\mathcal{R}_{Eval}$(*Area2*) (i.e., the overlap between *Area1* and *Milan* is larger than the overlap between *Area2* and *Milan*) and, correspondingly, the value of angle θ that LM should take into consideration is the one that produces *Area1*.

A problem could arises with *Area3*, which has clearly the greatest overlap with *Milan*. *Area3* could provide a $\mathcal{R}_{Eval}$ greater than the one that would have provided the original area. This would lead to an inconsistent LBAC predicate evaluation. The reason is that LM would have an incentive to configure the obfuscation as a way to artificially increase the odds of satisfying the $\mathcal{R}_{LBAC}$ threshold. To avoid such a side effect, we introduce an additional constraint. Let $Area_{Tech \cap LBAC}$ be the intersection between $Area_{Tech}$ and the predicate's area term. $\mathcal{R}_{Eval}$ must satisfy the following constraint.

$$\mathcal{R}_{Eval} \leq \frac{Area_{Tech \cap LBAC}}{Area_{Tech}} \cdot \mathcal{R}_{Tech} \quad (5)$$

In the example showed in Fig. 5, if we consider *Area3*, then $\frac{Area_{Priv \cap LBAC}}{Area_{Priv}}$=1. By considering equations from (1)

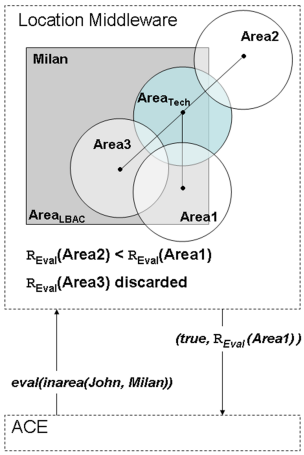

Figure 5. Area selection

and (4), the constraint expressed by (5) could be simplified as: $(\lambda + 1)^{-1} \leq \frac{Area_{Tech \cap LBAC}}{Area_{Tech}}$. *Area3* does not satisfy this constraint and it is discarded in favour of *Area1*.

However, there is a secondary effect selecting angle θ as the one that gives the best available $\mathcal{R}_{Eval}$: the user location privacy can decrease. The reason is that the obfuscation effect can be reduced by trying to reverse engineer the obfuscation and maximization procedures. An adversary knows that if the shift operation has been applied (however, the choice of the technique is not released), the center of the original area is at most at a distance of $2r$. This is the standard obfuscation effect of the center-shifting. However, if the LBAC predicate is known, the reference area $Area_{LBAC}$ (e.g., Milan) is known too. This additional information, together with the constraint (5) and the maximization procedure may allow restricting the possible location of the center of the original area to few zones only. This effect, which varies according to specific instances, is equivalent to a privacy reduction which is unaccounted in $\mathcal{R}_{Priv}$ and $\mathcal{R}_{Eval}$.

This example is relevant to highlight the subtleties of balancing the privacy preferences of users and location accuracy. The design of privacy-oriented solutions must consider similar side effects that, if not addressed, could strongly degrade privacy protection. In our case, two general solutions are possible: a technical solution and a negotiated solution. From the technical point of view, we can keep constraint (5) and avoid maximizing $\mathcal{R}_{Eval}$ by selecting angle θ randomly. Otherwise, for each specific situation, such a degradation of the actual privacy level can be quantified and the solution negotiated between the LBAC and the user. For instance, according to the specific context and the nature of the LBAC service, a user could decide to relax her privacy preference (for that specific case only) allowing the LBAC to manage a better location accuracy.

8 Conclusions

We presented a solution for enforcing the privacy preference of users that is compatible with the needs of accuracy required by LBAC systems. We analyzed two obfuscation techniques and introduced a general estimator, called relevance, that can be used for both measuring the degree of location privacy and the degree of accuracy required. Issues still to be investigated include the analysis of secondary effects of LBAC predicate evaluation, de-obfuscation techniques, and negotiation strategies.

Acknowledgments

This work was partially supported by the European Union within the PRIME Project in the FP6/IST Programme under contract IST-2002-507591, by the Italian Ministry of Research Fund for Basic Research (FIRB) under project RBNE05FKZ2 and by the Italian MIUR under project MAPS.

References

[1] C. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati. Supporting location-based conditions in access control policies. In *Proc. of the ACM Symposium on Information, Computer and Communications Security*, Taipei, Taiwan, March 2006.

[2] A. R. Beresford and F. Stajano. Mix zones: User privacy in location-aware services. In *Proc. of the 2nd IEEE PERCOMW'04*, 2004.

[3] C. Bettini, X. Wang, and S. Jajodia. Protecting privacy against location-based personal identification. In *Proc. of the 2nd SDM*, Trondheim, Norwey, September 2005.

[4] E. Damiani, M. Anisetti, and V. Bellandi. Toward exploiting location-based and video information in negotiated access control policies. In *Proc. of the ICISS 2005*, India, 2005.

[5] M. Duckham and L. Kulik. A formal model of obfuscation and negotiation for location privacy. In *Proc. of the 3rd International Conference on Pervasive Computing*, Munich, Germany, May 2005.

[6] M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proc. of the 1st International Conference on Mobile Systems, Applications, and Services*, 2003.

[7] Openwave. *Openwave Location Manager*, 2006. http://www.openwave.com/.

[8] Privacy Rights Clearinghouse/UCAN. *A Chronology of Data Breaches*, 2006.

[9] P. Samarati. Protecting respondents' identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering*, 13(6):1010–1027, 2001.

[10] K. Seamons, M. Winslett, T. Yu, L. Yu, and R. Jarvis. Protecting privacy during on-line trust negotiation. In *Proc. of the 2nd Workshop on Privacy Enhancing Technologies*, San Francisco, CA, April 2002.