Quality Estimation for Zone–based LBS under Realistic Positioning Systems

Philipp Marcus
Ludwig–Maximilians–Universität München
Oettingenstr. 67
80538 Munich, Germany
philipp.marcus@ifi.lmu.de

Claudia Linnhoff–Popien
Ludwig–Maximilians–Universität München
Oettingenstr. 67
80538 Munich, Germany
linnhoff@ifi.lmu.de

ABSTRACT

Location–based Services (LBS) are typically provided to users depending on their geographic location. Zone–based LBS form a subclass, that restricts the service provisioning to users within a predefined authorized zone. However, when deployed with real positioning systems, such LBS are exposed to position measurements with probably large errors compared to the size of the LBS's authorized zone. This may cause wrong authorization decisions and severe service malfunctions. Hence, a methodology to choose and rate an appropriate positioning system for such LBS in the forefront of their deployment is urgently needed. In order to solve this problem, this paper first presents three geospatial Quality of Service (QoS) metrics for LBS. A methodology to compute the expected QoS values for LBS when operated with a given positioning system is presented. This approach finally allows to determine if a given positioning system yields sufficiently high QoS values for the underlying LBS. Consequently, an appropriate positioning system can be identified and rated. Finally, the effectiveness of the approach is illustrated in a case study comprising two indoor LBS in a typical office environment.

Categories and Subject Descriptors

D.2.8 [**Software Engineering**]: Metrics; D.4.6 [**Operating Systems**]: Security and Protection—*Access controls*

General Terms

MEASUREMENT,SECURITY

Keywords

Location–based Service, Positioning, Quality of Service

1. INTRODUCTION

With the emergence of smartphones with embedded sensors, the user's context can easily be measured and used for adaptive mobile applications and context–aware services. Such context can be the user's location, current activity and many more. A context–aware service allows for providing information, data and arbitrary services to users depending on the user's current context. A popular subset of context–aware services are location–based services (LBS), which adhere the user's current location [6]. In this paper, zone–based LBS are defined to restrict the mobile access to users within an authorized zone that is predefined by the developer. For example, assume a museum, that provides visitors a mobile application with an integrated audio guide. The museum has special exhibition rooms with an extra fee. For such rooms, the audio guide's explanations must only be accessible to users that payed up and are within such rooms. In order to decide about such zone–based authorizations, the user's current position is estimated by a positioning system, for example Wi–Fi fingerprinting or GPS [9, 12]. Unfortunately, such systems are inherently subject to environmental and physical perturbations, which lead to errors in the derived position estimate. Hence, a definitive proposition if the user really resides within the authorized zone cannot be made. If the observed errors of the used positioning system are very large compared to the authorized zone, anomalies when operating the LBS arise. For example, users within the authorized zone are estimated to be outside and thus refused to use the LBS. Even the opposite is possible, whereby users outside the authorized zone are erroneously allowed to use the LBS. When applied to the museum example, users may skip the extra fee and listen from outside. Consequently, the museum has to bear the costs of lower earnings. On the other hand, legal users within the special room need support by an employee to manually activate the audio guide if the position estimate indicates that the user is outside. Again, costs for the museum arise. In order to reduce the running cost of zone–based LBS, this paper addresses the important problem to choose an underlying positioning system and rate its suitability.

Therefore, this paper first proposes a methodology to compute authorization models for LBS and a given positioning system. Authorization models describe for each spatial point the probability of getting position estimates that authorize for using the LBS. In the next step, the derived authorization model is used to assess the quality of the LBS when operated with the positioning system. Three quality of service (QoS) metrics are derived for zone–based LBS. One metric assesses the availability within the authorized zone. The next measures the vulnerability, i.e., the chance to get an authorization from outside in order to misuse the LBS. Finally, a metric for the LBS's importunity perceived by passersby

ICCASA 2014, October 15-16, Dubai, United Arab Emirates

DOI 10.4108/icst.iccasa.2014.257183

is presented that assesses effects of unwanted proactive and pushed provisioning. Consequently, a sufficient positioning system can be identified and rated instead of running into unexpected malfunctions when deploying the LBS.

The rest of the paper is structured as follows: First, Section 2 discusses related work. In Section 3, the concept of authorization models and QoS metrics for LBS are presented. Based on these results, Section 4 presents a case study for an indoor LBS in an office environment. Finally, Section 5 concludes the paper.

2. RELATED WORK

Several approaches for QoS metrics, selection of a positioning system, and zone–based authorization have been proposed in related work.

Martin-Escalona et al. propose MILCO, a middleware for selecting the cheapest acceptable positioning method for given LBS and constraints [10]. Here, the user specifies for each LBS the maximum allowed positioning error and delay. The proposed middleware then iteratively checks the available positioning methods until the cheapest sufficing one is found. However, these two quality parameters do not express the resulting quality of the LBS but only of the underlying positioning system. Filjar et al. adhere the horizontal and vertical accuracy of the positioning system as well as its response time as QoS requirements of LBS [4]. Again, for each LBS, minimum required QoS levels are defined. A suitable positioning system is iteratively found by comparing its specification with the limitations obliged by the user, e.g., maximum cost or power consumption. Similar to Martin-Escalona et al., only the requirements on the positioning system are investigated instead of investigating the LBS's behavior when operated with the chosen positioning system. Machaj et al. describe the availability, horizontal and vertical accuracy, time of response and position report frequency as criterion for the quality of LBS [8]. The proposed approach requires an expert to derive a weight factor for each of these QoS parameters as well as a maximum allowed upper bound. The resulting score of a positioning system for the underlying LBS finally computes as the weighted sum of the positioning system's deviations from the LBS's upper bounds. Unfortunately, this approach does not describe, which weights and upper bounds lead to a proper behavior of the LBS. Dhar et al. define locational accuracy, response time and reliability of operation as the QoS parameters of LBS [3]. The requirements on each parameter are described textually for each LBS. These parameters shall support the design and operation of the positioning infrastructure. However, no means for rating how well a given LBS works under a specific positioning system are provided. Ardagna et al. propose an approach for location–based authorization, which also comprises zone–based authorization [2]. Here, the positioning system is chosen based on its confidence and timeout according to predefined service level agreements (SLA). However, the impact of too low SLA levels on the authorization is neither analyzed nor described, leaving the choice of a suitable positioning system open. Shin et al. present a similar approach for zone–based authorization [11]. A uniform probability density function (pdf) is used to describe user locations and the probability of being within the zone. The authorization is granted if this probability exceeds a predefined threshold. High thresholds are required for security–sensitive zones compared to less sensitive ones. However, the quality of the zone–based authorization is not assessed, e.g., to what degree critical access from outside is possible or if a strict threshold impairs the availability.

3. METHODOLOGY

Due to imperfect accuracy and precision of positioning systems, users from outside the authorized zone may erroneously obtain a position estimate indicating a position within. In case this position estimate satisfies the conditions of the LBS, the user is granted a false positive authorization. Similarly, a false negative authorization occurs if a user inside the authorized zone is refused to use the LBS. In this section, first formal prerequisites for modeling positioning systems and zone–based LBS are given. Next, the derivation of a probability distribution for a LBS with an assigned positioning system is defined. This distribution assigns each geographical point X the probability to get a positive authorization $Auth$. This distribution is denoted as $\mathbf{P}(Auth|X)$ and called the authorization model for the rest of this paper. Finally, the quality of the LBS is rated based on three metrics extracted from the derived authorization model.

3.1 A Probabilistic Model for Positioning Systems

Zone–based LBS depend on the user's current location, which is determined by positioning systems. For outdoor LBS, GNSS based positioning systems like GPS have become very popular. However, indoor LBS are often based on other techniques like, e.g., Wi–Fi Fingerprinting. All approaches have in common, that a position estimate μ of the user's current coordinate is reported. Unfortunately, the process of position determination is affected by physical and environmental influences, which impair the systems accuracy and precision [6, 12]. For example, the root mean square of GPS's errors typically ranges from $9-11$ m while the errors of Wi–Fi fingerprinting show a mean of $1-2$ m [12, 9]. The resulting uncertainty about the user's ground truth position can be quantified by means of error estimation [7]. Here, one approach is to describe the user's ground truth position via a pdf derived from characteristics of the conducted position measurement [9]. Such pdf finally help to determine the probability that a user resides within a given zone [11]. For the rest of this paper, such pdf are denoted as $f_{(\mu,\Sigma)}$ and assumed to be defined using the position estimate μ and a scale parameter Σ derived by an error estimator. Thus, a position fix consists of a tuple (μ, Σ). Examples for such pdf $f_{(\mu,\Sigma)}$ in the literature are e.g., Gaussians represented by a mean μ and a covariance matrix Σ or uniform distributions represented by a median μ and a radius Σ [9]. Assuming a perfect error estimator, the distribution $\mathbf{P}_{error}(\Sigma)$ of scale parameters Σ characterizes the underlying positioning system. This distribution is employed in the next section to rate a positioning system's fitness for operation with a given LBS.

3.2 Theoretical Model for Location–based Services

In this paper, a zone–based location–based service LBS_i is restricted to users within an assigned authorized zone $\mathcal{Z}_i$, for example an office or exhibition room. However, as seen in

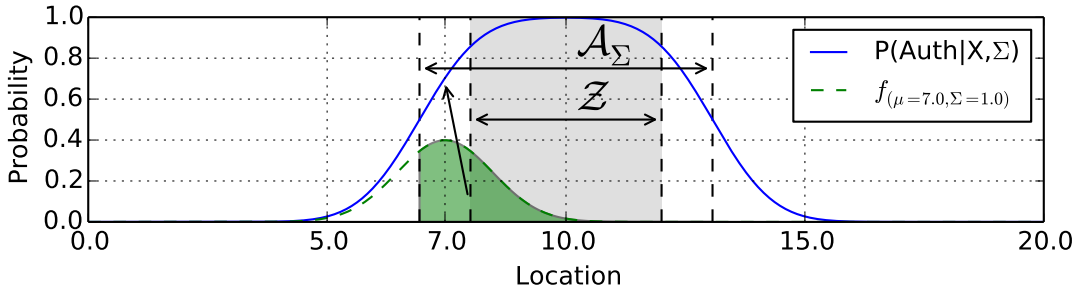

Figure 1: 1-D example with authorized zone $\mathcal{Z}$ (gray), effective authorized zone $\mathcal{A}_\Sigma$ for a fixed Σ and the according distribution $\mathbf{P}(Auth|X,\Sigma)$. The green area under the exemplary Gaussian $f_{\mu=7,\Sigma=1}$ is its integral over $\mathcal{A}_\Sigma$ and corresponds to $\mathrm{P}(auth|7,1)$.

Section 3.1, position estimates are subject to errors, which complicate the enforcement of this restriction. If LBS_i is proactive, passersby outside of $\mathcal{Z}_i$ should not be importuned by a pushed provisioning (pushed false positive authorization). Furthermore, the chance of malicious users to consciously misuse LBS_i outside of $\mathcal{Z}_i$ should be minimal (pulled false positive authorization). If users within $\mathcal{Z}_i$ are not able to use LBS_i either proactive or reactive, a false negative authorization happened.

The user's position estimate (μ, Σ) is adhered to decide about the provisioning of LBS_i. Basically, false positives and false negatives have to be prevented, as their incidence causes LBS–specific costs. Cost from possible misuse caused by malicious users outside of $\mathcal{Z}_i$ via pulled false positive authorizations is denoted as c_{fp_mis}. Cost from importuning passersby with pushed false positive authorizations is denoted c_{fp_imp}. Similarly, cost from either pushed or pulled false negative authorizations of users within $\mathcal{Z}_i$ are denoted as c_{fn}. Note, the specific costs strongly depend on the characteristics of LBS_i and need to be derived by experts in general. When deciding about authorizations, the most basic approach is to ignore possible errors and costs by simply checking if $\mu \in \mathcal{Z}_i$ [1]. However, risk–based authorization on uncertain attributes, e.g., the user's location, has been shown to be theoretically optimal [5]. In the following, the risk–based approach is adopted for LBS. In detail, the expected cost of a false positive and false negative authorization are compared. That decision with the least risk, i.e., expected cost, is chosen. This requires both the definition of possible cost and the probability of their occurrence.

The probability of a false negative stems from the uncertainty of the position estimate and corresponds to the probability $p_{\mathcal{Z}_i}$ that the user is inside of $\mathcal{Z}_i$. The opposite holds for false positives, where $(1 - p_{\mathcal{Z}_i})$ is used. Note, the probability $p_{\mathcal{Z}_i}$ is computed for a position estimate (μ, Σ) by integrating the pdf $f_{\mu,\Sigma}$ over $\mathcal{Z}_i$. The provisioning of LBS_i is finally decided using the described risk–based authorization by the predicate `is_authorized` with $C_{fp} = \{c_{fp\_mis}, c_{fp\_imp}\}$:

$$\texttt{is\_authorized}(\mu, \Sigma) = \bigwedge_{c_{fp} \in C_{fp}} (1 - p_{\mathcal{Z}_i}) \cdot c_{fp} \quad \leq \quad p_{\mathcal{Z}_i} \cdot c_{fn} \tag{1}$$

According to Equation 1, a LBS_i is only provided if the risk of a false positive undershoots the risk of a false negative.

3.3 The Quality of Zone–based LBS

Based on the given definitions, this section first defines authorization models for zone–based LBS and derives corresponding QoS metrics from these models.

3.3.1 Authorization Models for LBS

Authorization models are highly specific to the underlying LBS i and positioning system j and need to be separately computed for each combination (i, j) of interest. In order to compute the authorization model, beneath the specification of LBS i, also the error distribution $\mathbf{P}_{error}(\Sigma)$ of the positioning system j needs to be given according to Section 3.1.

The final formula is derived bottom–up. First, the *effective authorized zone* $\mathcal{A}_\Sigma$ is derived for position estimates with an error estimate of size Σ. This area comprises all possible position estimates μ, which will be authorized for the LBS when reported with an error estimate of Σ. Formally, $\mathcal{A}_\Sigma$ is defined as:

$$\mathcal{A}_\Sigma = \left\{\mu \in \mathbb{R}^2 \,|\, \texttt{is\_authorized}(\mu, \Sigma)\right\} \tag{2}$$

Example 3.1. A one–dimensional example is given in Figure 1. Let $c_{fp\_mis} = c_{fp\_imp} = 1$ and $c_{fn} = 6$. Assume the error estimates are Gaussians with a std. deviation of Σ and a mean of μ. The effective authorized zone for $\Sigma = 1$ overlaps $\mathcal{Z}_i$. This results from Equation 1, as only such (μ, Σ) with $p_{\mathcal{Z}_i} > 14.2\%$ are authorized. Points μ sufficing this requirement are also found outside of $\mathcal{Z}_i$.

Next, assume the size Σ of the error estimate is given and fixed. For any possible ground truth location x, the chance to obtain the position estimate (μ, Σ) with fixed μ and Σ corresponds to the value of $f_{(x,\Sigma)}(\mu)$.

As seen in Equation 2, those position estimates (μ, Σ) are authorized, which satisfy $\mu \in \mathcal{A}_\Sigma$. Consequently, the chance to obtain a position estimate with $\mu \in \mathcal{A}_\Sigma$ for any point x corresponds to the probability of authorization given Σ:

$$\mathrm{P}(Auth = \texttt{true}|X = x, \Sigma) = \int_{\mathcal{A}_\Sigma} f_{(x,\Sigma)}(\mu)\, \mathrm{d}\mu \tag{3}$$

As outlined in Section 3.1, the values of Σ returned by error estimators of real positioning systems are not fixed to static values. The occurring values of Σ rather follow a distribution $\mathbf{P}_{error}(\Sigma)$. In order to respect this fact and to obtain a

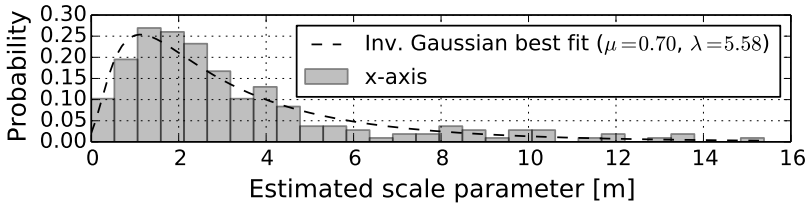

Figure 2: Observed error estimation variances for the SMARTPOS positioning system [9].

distribution $\mathbf{P}(Auth|X)$ independent of a fixed Σ, the final authorization model is obtained by marginalizing over the distribution of $\mathbf{P}_{error}(\Sigma)$:

$$\mathrm{P}(Auth = \texttt{true}|X = x) = \int_0^\infty P(Auth = \texttt{true}|X = x, \Sigma)\ \mathrm{P}_{error}(\Sigma)\ \mathrm{d}\ \Sigma \quad (4)$$

This distribution $\mathbf{P}(Auth|X)$ represents the derived authorization model for the underlying LBS i and positioning system j.

3.3.2 Definition of QoS Parameters

In order to determine the quality of a LBS i when operated with a given positioning system j, first, the real authorization model $\mathbf{P}(Auth|X)$ for this combination (i, j) needs to be derived based on the previous section. In the next step, this model is employed to derive the quality parameters of the LBS. However, in the theoretical case of an optimal error–free positioning system *opt*, the *optimal authorization model* is obtained:

$$\mathbf{P}(Auth = \texttt{true}|X = x) = \begin{cases} 1, & \text{iff } x \in \mathcal{Z} \\ 0, & \text{otherwise} \end{cases} \quad (5)$$

The deviation of the real from the optimal authorization model is used as the foundation for deriving quality ratings of a LBS i with its assigned positioning system j. As mentioned in Section 3.2, the quality of LBS i perceived by benevolent users within $\mathcal{Z}_i$ as well as passersby and malicious users (attackers) outside of $\mathcal{Z}_i$ is affected by this deviation. In practice, a LBS i with its assigned positioning system j has to be able to properly process requests of all three groups of users. Consequently, the quality parameters of availability, vulnerability and importunity are defined based on the real authorization model in the next step.

Benevolent users try to legally use the LBS i from within $\mathcal{Z}_i$. The chance to get the necessary authorizations is described as the LBS's availability.

Definition 3.1 (Availability)**.** The $availability_{i,j}$ of a LBS i operated with a positioning system j is defined on the real authorization model $\mathbf{P}(Auth|X)$ for this combination (i, j). Its value computes as the expected probability of being authorized for users located in the authorized zone $\mathcal{Z}_i$ with area $|\mathcal{Z}_i|$:

$$availability_{i,j} = \frac{1}{|\mathcal{Z}_i|} \int_{\mathcal{Z}_i} \mathbf{P}(Auth = \texttt{true} \mid X = x)\ \mathrm{d}x \quad (6)$$

High values of $availability_{i,j}$ are necessary to reliably provide LBS i. However, in case of the optimal authorization model, the value of $availability_{i,opt}$ would be 1 and all justified requests are authorized. Consequently, any real positioning system j yields ratings with $0 \leq availability_{i,j} \leq 1$.

Contrary to benevolent users, malicious users (attackers) try to maximize their chance of being authorized while standing outside of $\mathcal{Z}_i$ in order to misuse the LBS i and cause monetary cost. Hence, the worst–case needs to be assumed.

Definition 3.2 (Vulnerability)**.** The $vulnerability_{i,j}$ of a LBS i operated with a positioning system j is defined on the real authorization model $\mathbf{P}(Auth|X)$ for this combination (i, j). Its value computes as the maximum probability of authorization for any point x outside of the authorized zone:

$$vulnerability_{i,j} = \max(\{\mathbf{P}(Auth = \texttt{true} \mid X = x)\,|x \notin \mathcal{Z}_i\}) \quad (7)$$

Clearly, the vulnerability of any combination (i, j) needs to be low in order to hold off attackers. For indoor LBS, Equation 7 can be refined to only respect such $x \notin \mathcal{Z}_i$ not located on walls of the building. Note, according to Equation 5, the optimal authorization model always yields $vulnerability_{i,opt} = 0$, indicating that no malicious user may ever gain access to LBS i from outside of $\mathcal{Z}_i$. However, for real positioning systems, it holds that $0 \leq vulnerability_{i,j} \leq 1$.

Passersby outside of the authorized zone $\mathcal{Z}_i$ don't want to be importuned by proactive and pushed provisioning of any LBS i. The size of the region around $\mathcal{Z}_i$ where this happens more likely than α characterizes this property.

Definition 3.3 (α–Importunity)**.** The α–$importunity_{i,j}$ of a LBS i operated with a positioning system j is expressed as the largest distance from $\mathcal{Z}_i$ where still an authorization is granted with a probability greater equal α:

$$importunity_{i,j} = \max(\{d(\mathcal{Z}_i, x)\,|x \notin \mathcal{Z}_i \wedge \mathbf{P}(Auth = \texttt{true} \mid X = x) \geq \alpha\} \cup \{0\}) \quad (8)$$

Here, $d(\mathcal{Z}_i, x)$ denotes the distance of any point x from the authorized zone $\mathcal{Z}_i$. If no point x suffices the required property, 0 is returned. Again, for indoor LBS, Equation 8 can be refined to also exclude points x located on walls of the building. Clearly, the optimal authorization model yields $importunity_{i,opt} = 0$ for any value of α. Thus, the lower the obtained importunity, the better the perceived quality of LBS i when operated with positioning system j.

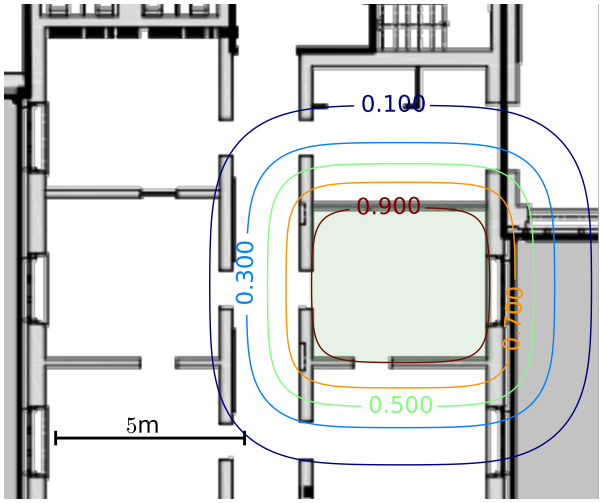

Figure 3: Authorization model for LBS_1.

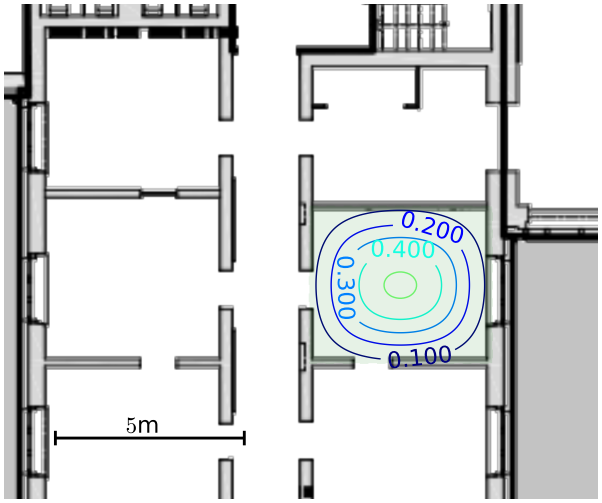

Figure 4: Authorization model for LBS_2.

To conclude, these QoS values assess for each of the three identified user groups the impact of any deviation from the optimal authorization model. Consequently, these QoS values suffice to rate if a given positioning system fulfills the requirements. This is illustrated in the next section by a case study.

4. CASE STUDY: DEPLOYING AN INDOOR LBS

This section illustrates the practical application of the described methodology in a case study. The underlying scenario is a typical office environment, where a single office of 16.2 m^2 is used as authorized zone $\mathcal{Z}$ for the underlying LBS. This site is depicted in both Figure 3 and Figure 4 with the authorized zone office filled green. As positioning system, the previously developed SMARTPOS approach was applied [9]. SMARTPOS is based on Wi–Fi fingerprinting and uses a weighted kNN algorithm to derive position estimates. Its error estimator yields Gaussians with a covariance of 0 and a variance derived from the kNN's distance to the position estimate. SMARTPOS' pdf $\mathbf{P}_{error}(\Sigma)$ of observed error estimation variances Σ was derived from a large set of test data and is depicted in Figure 2. An inverse Gaussian distribution can be fitted well to the observed error estimates and is thus used to model $\mathbf{P}_{error}(\Sigma)$ in the following.

In the next step, two LBS, LBS_1 and LBS_2, with different cost functions were defined for the authorized zone office. The assigned cost functions are defined in Table 1. For LBS_1, false positive authorization decisions are rather cheap compared to false negatives. Contrary, LBS_2 shows much higher costs for false positives compared the costs of false negatives. Intuitively, this causes highly different authorization characteristics and diverse quality parameters for both LBS. Here, both real authorization model were numerically approximated.

The derived models are illustrated in form of contour lines in Figures 3 and 4. Clearly, a strong deviation from the optimal authorization model is visible. LBS_1 shows a probability of authorization larger 0 in a notable area around $\mathcal{Z}$. Contrary, for LBS_2 this value is significantly below 1 in most points within $\mathcal{Z}$.

Next, for both LBS, the availability, vulnerability and 0.05–importunity was computed. The level $\alpha = 0.05$ is chosen here to obtain the surrounding where passersby are importuned by the LBS more likely than 5%. The results are shown in Table 1. The resulting values strongly correlate with the models depicted in Figures 3 and 4. LBS_1 shows larger values for all three quality parameters. Except for the availability, this can be considered as a drawback compared to the behavior of LBS_2 as the vulnerability and importunity is much higher. However, as LBS_1's cost functions c_{fp_mis} and c_{fp_imp} are low compared to the cost of c_{fn}, the requirements on the vulnerability and importunity are not high. Contrary, LBS_2 shows a very low availability, which indicates that the LBS is poorly available. However, the vulnerability is very low and the probability that passersby are importuned by LBS_2 is lower than 5% at any point outside of $\mathcal{Z}$. To conclude, the derived values help to decide if a deployment of each LBS using SMARTPOS is reasonable. In case of LBS_1, where false negatives are much more expensive than false positives, SMARTPOS's precision suffices. However, LBS_2 highly suffers from the size of occurring positioning errors and according error estimates. This finally makes LBS_2 hardly usable in the described scenario. Consequently, the conducted analysis shall be iteratively repeated with a more precise positioning system for LBS_2 in order to finally obtain sufficient quality parameters. This finally also allows to deploy LBS_2 with sufficiently high quality parameters.

5. CONCLUSION

Zone–based LBS are services only provided to users within an authorized geographical zone. Such LBS are impaired by errors of the underlying positioning system. This paper presented an approach to assess the quality of service (QoS) of zone–based LBS when positioning errors occur. This allows to finally choose a sufficient positioning system. In order to assess the quality, authorization models were presented. These models describe for each geographical point the prob-

LBS	c_{fp_mis}	c_{fp_imp}	c_{fn}	Availability	Vulnerability	0.05–Importunity
LBS_1	1	1	6	0.92	0.75	2.89 m
LBS_2	6	6	1	0.28	0.03	0

Table 1: Cost functions and derived QoS values for LBS_1 and LBS_2.

ability to obtain such position estimates that lead to an authorization to use the LBS. Three QoS metrics were defined based on the shape of authorization models. The availability is rated based on the expectation to be authorized when standing within the zone. The LBS's vulnerability is defined as the maximum chance to be authorized outside the zone. The importunity measures the distance to the zone where an uninvolved passerby may still be importuned by a pushed provisioning of the LBS. A case study with two indoor LBS showed the effectiveness of the presented approach to decide about the suitability of an underlying positioning system.

The presented approach allows to rate the impact of an positioning system's errors on three distinct aspects of a LBS. However, existing approaches choose positioning systems based on their specification without investigating the impact on the LBS's authorization behavior.

In detail, the QoS metrics give a detailed insight how well the LBS will work for benevolent users, attackers and passersby. Thus, the presented approach allows for a sophisticated choice of a positioning system in the forefront of a LBS's deployment. This finally leads to lower costs of operating LBS and a better acceptance.

However, the derived QoS metrics are only approximations of the real behavior. Future work is seen in extending the approach to trajectories and continuous authorization.

6. REFERENCES

[1] R. Abdunabi, W. Sun, and I. Ray. Enforcing spatio-temporal access control in mobile applications. *Computing*, 96(4):313–353, 2014.

[2] C. Ardagna, M. Cremonini, S. Capitani di Vimercati, and P. Samarati. Access control in location-based services. In *Privacy in Location-Based Applications*, volume 5599 of *LNCS*, pages 106–126. Springer, 2009.

[3] S. Dhar and U. Varshney. Challenges and business models for mobile location-based services and advertising. *Commun. ACM*, 54(5):121–128, May 2011.

[4] R. Filjar, L. Bušić, S. Dešić, and D. Huljenić. Lbs position estimation by adaptive selection of positioning sensors based on requested qos. In *Next Generation Teletraffic and Wired/Wireless Advanced Networking*, pages 101–109. Springer, 2008.

[5] L. Krautsevich, A. Lazouski, F. Martinelli, and A. Yautsiukhin. Cost-effective enforcement of access and usage control policies under uncertainties. *Systems Journal, IEEE*, 7(2):223–235, June 2013.

[6] A. Küpper. *Location-based Services: Fundamentals and Operation*. John Wiley & Sons, 2005.

[7] H. Lemelson, M. B. Kjærgaard, R. Hansen, and T. King. Error estimation for indoor 802.11 location fingerprinting. In *Location and Context Awareness*, pages 138–155. Springer, 2009.

[8] J. Machaj, P. Brida, and N. Majer. Novel criterion to evaluate qos of localization based services. In *Intelligent Information and Database Systems*, pages 381–390. Springer, 2012.

[9] P. Marcus, M. Kessel, and M. Werner. Dynamic nearest neighbors and online error estimation for smartpos. *Int'l Journal On Advances in Internet Technology*, 6(1 and 2):1–11, 2013.

[10] I. Martin-Escalona and F. Barcelo-Arroyo. Qos-driven middleware for optimum provisioning of location based services. In *Communication Systems Software and Middleware, 2nd Int'l Conference on*, pages 1–6. IEEE, 2007.

[11] H. Shin and V. Atluri. Spatiotemporal access control enforcement under uncertain location estimates. In *Data and Applications Security XXIII*, pages 159–174. Springer, 2009.

[12] P. A. Zandbergen. Positional accuracy of spatial data: Non-normal distributions and a critique of the national standard for spatial data accuracy. *Transactions in GIS*, 12(1):103–130, 2008.