Acceptable Margin of Error: Quantifying Location Privacy in BLE Localization

Viktoriia Shubina*†, Aleksandr Ometov*, Dragos Niculescu†, and Elena Simona Lohan*
* Tampere University, Finland, emails: firstname.lastname@tuni.fi
† University "Politehnica" of Bucharest, Romania, email: firstname.lastname@cs.pub.ro

***Abstract*—Location privacy poses a critical challenge as the use of mobile devices and location-based services becomes more and more widespread. Proximity-detection data can reveal sensitive information about individuals, making it essential to preserve their location data. One way to achieve privacy protection is by adding noise to ground-truth data, which can introduce uncertainty while still allowing moderate utility for proximity-detection services and Received Signal Strength (RSS)-based localization. However, it is important to carefully adjust the amount of noise added in order to balance the privacy and accuracy concerns. This paper expands our previous work on evaluating location privacy bounds based on measurement error and intentionally added noise. Our model builds upon existing work in differential privacy and introduces other techniques to estimate privacy bounds specific to proximity data. By using real-world measurement data, we measure the privacy-accuracy trade-off and suggest cases where additional noise could be added. Our framework can be utilized to inform privacy-preserving location-based applications and guide the selection of appropriate noise levels in order to achieve the desired privacy-accuracy balance.**

***Index Terms*—Location privacy, RSS, BLE, localization, proximity detection.**

I. Introduction

With the advent of Location-Based Services (LBSs) and the widespread adoption of localization through wireless signals, users are becoming more willing to share their location with friends and family on their social networks and via various applications. These situations might not raise ethical concerns instantaneously, but privacy becomes a problem only when it is breached [1]. This argument is supported by the survey on Location Privacy-Preserving Mechanisms (LPPMs) in [2], where the authors explicitly highlighted the differences between different database types. Furthermore, the LBS having to estimate the distances among given devices poses a privacy risk when the database is not stored securely or a third party gains access to the information.

Since widespread services allow accurate location estimation, the need to quantify privacy is a significant concern to the research community working on indoor localization. The reader is advised to read further about the subject in [3]. While many studies have focused on improving the accuracy and efficiency of Bluetooth Low Energy (BLE) indoor positioning systems, there needs to be more literature regarding the optimal privacy values for these systems. BLE indoor positioning systems typically use the Medium Access Control (MAC) address of the BLE devices to locate them, and this can be easily tracked and identified by malicious actors. In addition, the use of proximity-based authentication can also leak sensitive information about the users' locations and movements. Some studies have addressed the privacy concerns of BLE indoor positioning systems by proposing different obfuscation techniques or modifying the BLE protocol to enhance privacy [4], [5]. However, there is still a need for more research in this area, especially considering the increasing adoption of BLE indoor positioning systems in various domains, for instance, healthcare, retail, and smart buildings.

BLE enables many opportunities for proximity detection, supports mesh network operations that open ways for data exchange among the devices, and thus can be used for estimating the distances between devices. Nowadays, proximity detection is covered mainly by BLE, as the widespread adoption of the technology conditions it. However, many other technologies can implement the proximity-detection scenario: UWB, light, and acoustic sensors, among many others. In proximity detection services, the device needs to find only the range towards another smartphone, item, or Access Points (APs), e.g.,in [6], the average accuracy range for the distance estimates was within 0.79 and 2.28 m.

Moreover, with the increasing availability of BLE chipsets in mobile phones and wearable devices providing various services for users, including proximity detection, the problem of quantifying and preserving privacy appears more relevant in all layers within the OSI model. The authors in [7] performed an independent evaluation of privacy of the proximity-detection setting on the Physical Layer (PHY) for various devices: from mobile phones to wearables. The researchers in [7], demonstrated that a fingerprinting attack is feasible since the devices regularly send beacons, making their presence in the room relatively simple to detect.

Privacy-preserving methods, such as obfuscation, are implemented in the OSI model at higher (above PHY) levels. Thus, the study in [8] described developing a privacy-preserving RSS-based indoor positioning system. By adopting homomorphic encryption, the system protects location privacy for the users and the server while reaching a moderate degree of location accuracy.

The study in [9] provided a strong privacy guarantee by letting individuals alter their data locally on the edge device before transmitting the location information to a third party. In contrast, our paper refers to the noise added on the server side. The processing location — on the user's device or server

— significantly distinguishes these two methods. Local noise addition is more effective than service-based computations and uses fewer resources because it does not tax the server capacity. However, it might not offer as strong a guarantee of privacy as the server-side insertion of noise.

For years, challenges in BLE RSS positioning have been a subject of interest, and several research groups have made open-access data from controlled experiments available. Currently, many RSS BLE datasets are in open access, published by the researchers [10]–[12]. As a result of its relevance and future use in obtaining the statistics for further theoretical investigation of privacy levels for BLE proximity-detection scenarios, the data gathered and published in [13] was selected for our study.

The list of the present paper's contributions is as follows:

- As a continuation of our last contributions [4], this paper aims to study the degrees of privacy in BLE localization while also adding value by implementing privacy metrics.
- We derived the channel path-loss models from the BLE measurement data from one of our previous studies [13] and quantified the margin of error from those measurements at observed distances of 1, 2, and 3 meters.
- Then, we combined the theoretical research findings and experimentation with actual RSS data and analyzed the implementation of the differential privacy (DP) algorithm.
- For the analyzed measurement and simulated data, we compared the privacy budget, characterized by ϵ parameter (lower ϵ, higher privacy) to analyze the privacy-accuracy trade-off for the considered BLE localization and proximity-detection scenarios.

II. BLE RSS PARAMETERS

BLE is implemented with prevalence as a System-on-a-Chip (SoC) or as a separate ready-made BLE module. The technology operates at 2.4 GHz radio frequencies on 40 channels, 3 of which are used for advertising, namely 37, 38, and 39. The distance computation is also affected by the adopted BLE advertising channel and whether the channel is known on the RX side. Based on the results from [14], the distortion caused by the frequency-dependent gains [15], together with the frequency-dependent free-space signal propagation, may all be compensated. Primarily in controlled experiments using RPIs, where the channel on which a packet was received is known, the issue of multi-path propagation, typical for indoor scenarios, can also be minimized.

The one-slope path-loss model is often favored by researchers over the Free-Space Path Loss (FSPL) when it comes to RSS modeling [10]:

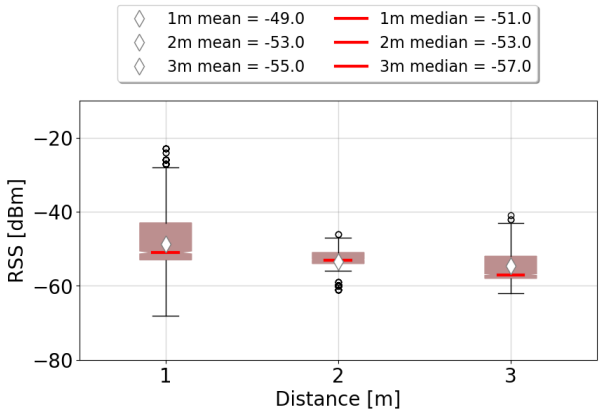
$$P_R = P_{T_a} - 10nlog_{10}d + \eta, \tag{1}$$

where the apparent transmit power P_{T_a} (typically computed as transmit power at 1m away from the transmitter), n is the path-loss coefficient or factor, d is the TX–RX distance in m, and η is a noise factor.

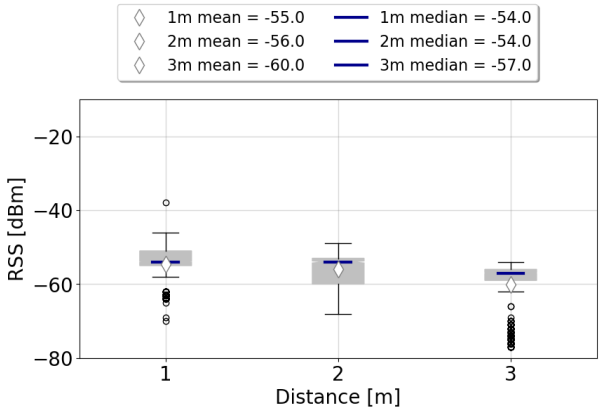
The path loss factor n can also indicate the level of interference in the environment; it is related to the power decay rate of the signal with distance. For example, a high value of n may indicate a highly obstructed environment with many reflections, diffraction, and scattering. In contrast, a low value of n may indicate a relatively open environment with few obstacles and minimal interference. When n is smaller, the RSS curve (P_R) is flatter as a distance function, making it more difficult to discern between close distances (for example, between 1 m and 2 m or between 2 m and 3 m).

The shadowing variance $\hat{\sigma}_\eta^2$ could be defined as the error between N_{meas} measurements of the received signal strength $P_{R_i}, i = 1, \ldots, N_{meas}$ at various distances d and the reconstructed data, namely:

$$\hat{\sigma}_\eta^2 = \frac{1}{N_{meas}} \sum_{i=1}^{N_{meas}} \left(P_{R_i} - P_{T_a} - 10nlog_{10}(d) \right)^2. \tag{2}$$



(a) LOS: UPB premises



(b) LOS: TAU premises

Fig. 1. RSS distributions against actual distances of 1, 2, and 3 m respectively at two different locations at UPB and TAU deploying identical hardware.

Different variables, including human body absorbance, signal multipath and ambient influences, antenna gains and device orientation, and hardware features, contribute to the instability of RSS recordings. Based on the data acquired via RPIs used as TX and RX from [13], we plotted the following distributions, corresponding to distances of 1, 2, and 3 m respectively, a total number of 5 recordings per fixed distance was used, 320 measurements per recording at each

site were used to produce the graphs. Fig. 1 shows the results acquired with the same devices, and both Figs. 1b and 1a convey the message that means and medians (expressed in dBm) are inversely proportional to the TX–RX increasing distances. In the case of UPB, more outliers are present for the measurements of 1 m. However, we observe more outliers for TAU in the case of the 1 and 3 m distance. With aggregated data from two different locations (UPB and TAU), Table I depicts path-loss parameters for line-of-sight (LOS) and non-line-of-sight (NLOS) settings using three different BLE advertising channels.

In this case, the calculated value of σ_n derived from the eq. 2 and values of n from Table I are used to derive distance errors for multiple channels and environments. These values of σ_m are subsequently used as a source of privacy, which we refer as the measurement error. The columns of Table I specify the location (TAU or UPB), conditions that included LOS and NLOS, advertising channel indices, number of samples varying per scenario in the shared dataset (referred to as recording number), derived mean, median and n values in each of the considered scenarios.

III. Privacy Metrics

Even in cases where the data collected by an indoor positioning system is anonymized, there is still a risk that individuals could be re-identified by an attacker, which could potentially use additional data sources to link the anonymized data to specific individuals. This facilitates the motivation to quantify and preserve privacy in the considered scenario.

The scheme presented in Fig. 2 shows the privacy-preserving proximity-detection scheme. Assume we have two users, Alice and Bob, who want to know whether they are near one other yet unwilling to share their actual positions (obtained via other phone sensors using trilateration). Thus, in order to avoid disclosing the true position, the server (which owns the dataset with all distances) has two alternatives for preserving the location: a measurement error or an intentional error — the DP algorithm. The measurement error σ_m becomes apparent once the RSSI data have been converted to distances. Then, the trusted observer is shown as an example in the scheme, and at this point, the additional error is introduced per the DP mechanism. Hence, it becomes unfeasible for a malicious entity to subsequently compromise one's privacy, even if it has access to the LBS's database of proximity information (distances) between the devices.

We analyze the data from the side server perspective (as a trustworthy entity), independently of the user equipment (UE), and infer the data from the received RSS values. By possessing extensive information with RSS values and timestamps, we might receive the information raw from the software, split the results into the ones including the measurement error, and then add the noise and evaluate how much privacy a user could gain in case an LPPM was applied.

Therefore, to ensure that indoor positioning systems protect the privacy of individuals, it is important to use privacy-preserving techniques, such as DP, that limit the amount of sensitive information that can be extracted from the data. The following equation gives the formal definition of DP:

$$Pr(D) = exp(\epsilon)Pr(D'), \tag{3}$$

where $Pr(D)$ is the probability distribution of the algorithm's output on the original dataset D, $Pr(D')$ is the probability distribution of the output on a neighboring dataset D', and ϵ is a non-negative privacy parameter that controls the amount of noise added to the algorithm's output to achieve privacy known as the privacy budget. The larger the value of ϵ, the more privacy is sacrificed for greater accuracy/utility. Conversely, the smaller the value of ϵ, the greater the privacy protection at the expense of accuracy/utility.

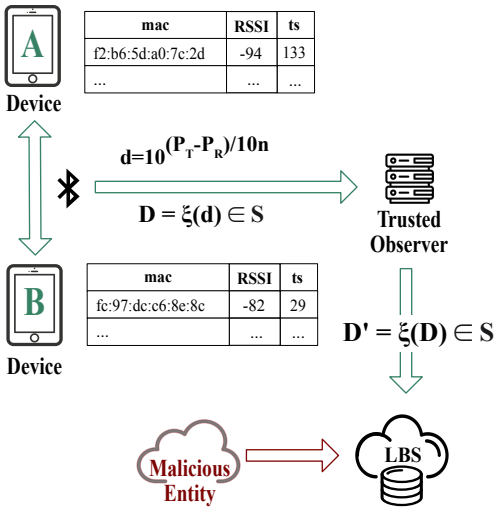


Fig. 2. The figure depicts the proximity detection scheme, in which devices of Alice and Bob exchange beacons and then the data is transferred further with some measurement error and in case of smaller σ_n values, additional noise could be added.

DP is a technique used to protect the privacy of individuals when releasing data or performing analyses on sensitive datasets. For example, laplacian noise is often used in differential privacy because it allows adding random noise to a dataset, making it more difficult for an attacker to infer sensitive information about individuals from the released data [16].

The Laplace distribution is a continuous probability distribution with a high probability of generating values near zero and a gradually decreasing probability of generating larger values. This property makes it well-suited for adding noise to sensitive datasets, as it ensures that the added noise is more likely to be small while still allowing for the possibility of larger noise values.

The Laplacian noise with μ=0 with a scale factor of $1/\epsilon$, as shown in eq. (4), is modelled as:

$$f_{Laplace}(\epsilon) = \frac{1}{2b} e^{(-\frac{|x-\mu|}{b})}, \tag{4}$$

where $b > 0$. In case of location additional error, and in the context of DP, Laplacian distribution is the most commonly used [17].

TABLE I
STATISTICS DERIVED FROM THE MEASUREMENT DATA BETWEEN TWO RPIS USED AS TX AND RX AT d=2 m APART.

Location	LOS/NLOS	Channel index	Rec. number	Samples	Mean [dB]	Std. [dB]	n [-]
TAU	LOS	37	7	320	-50.48	7.58	0.81
TAU	LOS	38	1	3215	-46.02	5.61	3.24
TAU	LOS	39	1	2607	-54.18	1.71	1.37
TAU	LOS	all (37, 38, 39)	5	736	-45.58	7.13	0.98
UPB	LOS	37	7	326	-50.43	5.23	1.56
UPB	LOS	38	1	3215	-51.64	3.29	3.41
UPB	LOS	39	1	2607	-52.27	4.80	2.75
UPB	LOS	all (37, 38, 39)	5	736	-51.36	7.43	2.19
TAU	NLOS (wall)	all (37, 38, 39)	1	1824	-58.15	2.92	2.51
UPB	NLOS (wall)	37	3	1726	-55.37	5.96	2.20
UPB	NLOS (human)	all (37, 38, 39)	1	495	-60.03	4.34	1.76
UPB	NLOS (door)	all (37, 38, 39)	1	1808	-48.65	3.27	2.03

The amount of noise added to a dataset depends on the sensitivity of the data and the desired level of privacy protection. Adding Laplacian noise to the data protects individuals' privacy, as it becomes much more difficult for an attacker to determine the values of individual data points from the released dataset.

Another sort of random noise that is often used in a variety of applications, such as signal processing, data analysis, and privacy protection, is referred to as Gaussian noise. Regarding the added noise factor ϵ in eq. 3, two noise distributions are considered for the purpose. These are a Gaussian distribution with a standard deviation equal to $1/\epsilon$, as shown in eq. (5). Accordingly, $f_{Gauss}(\epsilon)$ is modeled as

$$f_{Gauss}(\epsilon) = \frac{1}{\sigma_m\sqrt{2\pi}} e^{-\frac{(\epsilon-\mu_m)^2}{2\sigma_m^2}}, \tag{5}$$

where μ_m is the mean error and σ_m is the standard deviation (SD) of the distance error. The reference to measurement error is highlighted by the subscript m. Since ϵ stands for a distance error, only the positive component of $f_{Gauss}(\epsilon)$ properly describes the distance error, namely, $f_{Gauss}(\epsilon)S(\epsilon)$, in which $S(\epsilon)$ is a step function ($S(\epsilon) = 1$ if $\epsilon \geq 0$ and $S(\epsilon) = 0$ if $\epsilon < 0$).

When it comes to DP, Laplacian noise is often preferred over Gaussian noise for several reasons. One of the main reasons for using Laplacian noise in differential privacy is that it provides stronger privacy guarantees than Gaussian noise for the same amount of added noise. This is because the tails of the Laplace distribution decay more slowly than the tails of the Gaussian distribution, which means that Laplacian noise can add more robust privacy protection, especially for outlier data points.

Another reason for using Laplacian noise is that it is computationally efficient to generate and add to data. The Laplace distribution has a simple mathematical form and can be easily sampled using standard software libraries, making it a practical choice for large-scale data analysis.

In contrast, Gaussian noise can be more challenging to work with in the context of differential privacy because it can result in a high risk of outliers. This means that even with small amounts of added Gaussian noise, it is possible for an attacker to reconstruct the original data with high accuracy, potentially compromising privacy protection. In summary, Laplacian noise is often used in differential privacy because it provides a way to add random noise to a dataset that protects the privacy of individuals while still allowing useful information to be extracted from the data.

To summarize, while Gaussian noise can be useful in some contexts, Laplacian noise is often preferred in differential privacy because it provides stronger privacy guarantees and is computationally efficient to generate and implement [18].

DP is a guarantee that the privacy of individuals is not placed at risk when sending queries to datasets that contains sensitive data. One application of differential privacy is in location data where there is a trade-off between protecting sensitive information about users and mining useful information from datasets. For example, in order to determine moving patterns and other trends. Differential privacy makes inference and tracking attacks less likely. The metrics are further explained in [19].

Sensitivity (δ) refers to how much the output of a function differs when a single individual's data point in the input dataset is updated or deleted in the context of differential privacy. Technically, the sensitivity of a function f is defined as the maximum amount by which f can vary when the data sample in the input dataset is changed:

$$f_{Sensitivity} = max_{D,D'}||f(D) - f(D')||_1, \tag{6}$$

where D and D' are two databases that differ by at most one individual's data point, $||.||_1$ denotes the L1 norm (or some norm, usually the L1-norm or the L2-norm that determines how the distance between the two function outputs is measured), which is the sum of the absolute values of the differences between corresponding elements of $f(D)$ and $f(D')$. Sensitivity is a key parameter in the design of differentially private algorithms, as it determines the amount of noise that needs to be added to the function output to achieve a desired level of privacy protection. The larger the sensitivity, the more noise needs to be added to the function output to ensure that individual data points cannot be inferred from the output with high probability. Higher sensitivity could result

in greater noise being added, which could reduce accuracy, while lower sensitivity could lead to less noise being added but could also result in reduced privacy protection.

As introduced in [20], another utility metric is the Mean Absolute Error (MAE), expressed by the following:

$$MAE = \frac{1}{N} \sum_{n \in N} |d_n^{true} - d_n^{observed}|, \tag{7}$$

where d_{true} stands for the actual location, $d_{observed}$ stands for the one with the measurement noise and N denotes the number of observations.

Whereas, Normalized Cell Error (NCE) refers to computing the differences as follows:

$$NCE = \frac{1}{|S|} \sum_{n \in N} d_n^{true} - d_n^{synth}|, \tag{8}$$

where d_{synth} is the location with the added noise and S denotes the set of d_{synth} locations, and $|S|$ is the cardinality of S.

In this part, we primarily focused on outlining the scenario we took into account and detailing the metrics we utilized to weigh the privacy against utility trade-off.

Privacy metrics, such as ϵ provides a quantifiable measure of the privacy guarantees of the algorithm, which can be used to assess the level of privacy protection provided by different noise levels.

On the other hand, utility metrics measure the accuracy and usefulness of any application. By using utility metrics, such as MAE and NCE we can assess the LBS performance quality and ensure that the data processing provides meaningful and useful results.

IV. Results And Discussion

In this section, we present a DP implementation for BLE RSS localization that enables the collection and analysis of location data while protecting the privacy of the individuals involved.

The following procedure was used in our study:

- In 2D space, define a grid of cells, with a grid step of 1 m. Each cell has a fixed size and occupies a tiny portion of the available space.
- Count the number of users whose locations fall inside each cell to get the actual number of users in each cell.
- For every cell, compute the differentially private distances using a differentially private mechanism with the Laplace or Gaussian noise.
- At the next step, compute NCE, which is calculated as the greatest absolute difference between noisy and true distances divided by the total of true distances.
- The second utility metric, MAE is calculated as the absolute difference between each values obtained and the corresponding real value, adds them together, and then computes the average by dividing the total by the number of observations.

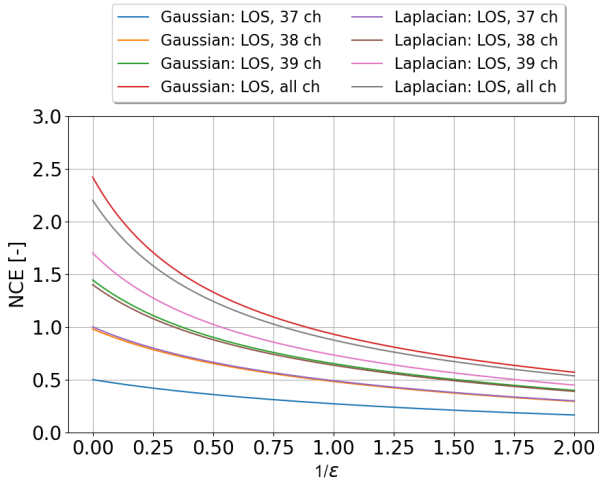


Fig. 3. The plot illustrates the privacy-utility trade-off for LOS scenarios. Due to an increase in the total quantity of noise that is introduced, Accuracy and NCE (which is reversely related to the Utility) both deteriorate when ϵ is increased.

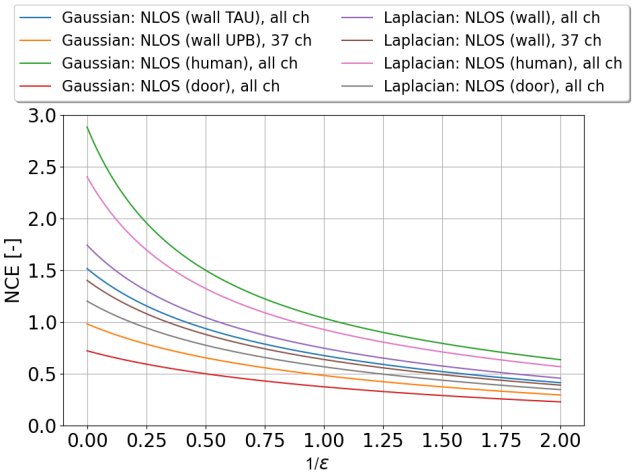


Fig. 4. The figure shows the privacy-utility trade-off for NLOS scenarios. Here, a gain in ϵ leads to a decrease in privacy, along with NCE, which indicates an increase in utility.

Respectively, Fig. 3 and Fig. 4 provide an evaluation of the trade-off from the perspective of NCE, comparing the results to the privacy budget ϵ. We used the LOS data collected on different BLE channels for the plot in Fig. 3. There is no drastically leading type of noise, evidently, σ_m has a more significant impact on the discrepancy between Laplacian or Gaussian distributions.

Looking at the plots for varying parameters of Gaussian and Laplacian distributions, we can see that as ϵ decreases (i.e., stronger privacy protection), the NCE values increase (i.e., accuracy decreases). This is expected, as stronger privacy protection generally requires more noise to be added to the data, which can result in reduced accuracy.

However, there is a trade-off between privacy and accuracy, and we can see that there is a region where the NCE

values are relatively low while still providing reasonable privacy protection. This region corresponds to a moderate ϵ value, where the added noise is not too high to impact accuracy severely. Of course, the optimal value of the privacy budget ϵ will depend on the specific application and privacy requirements.

Another approach to evaluate the same trade-off is to plot MAE against the privacy budget ϵ, as shown in Fig. 5 and Fig. 6 measuring the average magnitude of errors in a set of data. It indicates how far the observed values are from the actual ones. A lower MAE demonstrates that the model is more accurate, while a higher MAE means that the model is less accurate (has lower utility for a proximity-based detection application such as finding the nearest shop, etc.).

While it is difficult to pinpoint which distribution behaves better from Fig. 3 where different proximity-detection distances are considered, Fig. 4 states it clearly that Gaussian distribution shows a slightly better performance for the same values of δ.

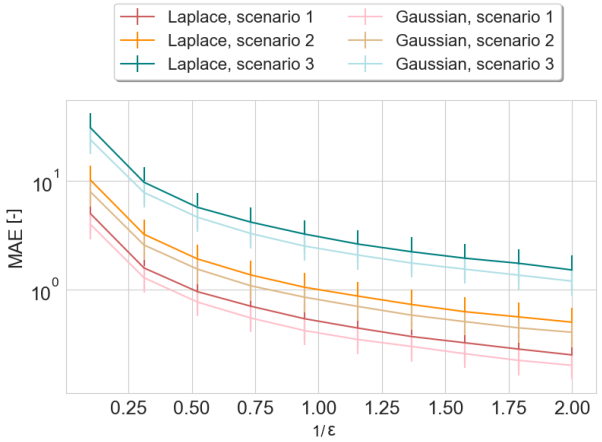


Fig. 5. This figure shows MAE vs ϵ for each scenario utilizing the Laplace mechanism and Gaussian mechanism for various proximity-detection situations with additional noise, when Sensitivity (δ) = 1. The three scenarios assigned with digits from 1 to 3 refer to the different distances between the target users of 2, 5 and 10 m respectively.

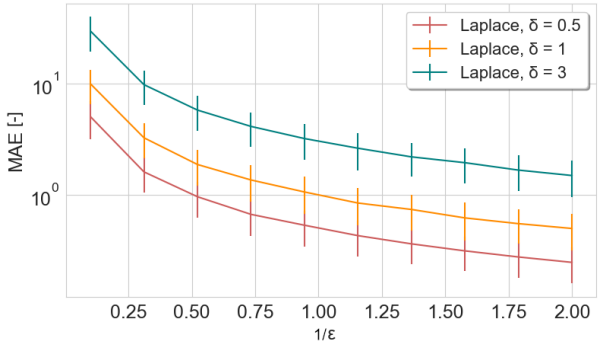


Fig. 6. The MAE versus ϵ relation is depicted herein using the Laplace mechanism for a number of different proximity-detection scenarios that involve extra noise and varied Sensitivity values (δ).

Following the Elbow rule described in [21], we arrive at the conclusion that for the majority of proximity-detection services deployed in smart buildings, a value of ϵ between 0.31 and 0.75 would be optimal, based on the situations and factors we considered. This proposal, however, is of a general nature and cannot be applied to every possible DP implementation.

V. Conclusions and Future Work

To determine the optimal point, one should consider the specific requirements and constraints of the application. For example, on one hand, if the application is a medical study, a higher level of privacy may be required to protect sensitive information, even if this results in a slightly higher normalized cell error. On the other hand, if the application is a marketing study, a slightly lower level of privacy may be acceptable in order to achieve a more accurate analysis.

Therefore, the optimal point will vary depending on the specific use case, and should be determined by considering the trade-off between privacy and accuracy in the context of the application. Generally, the optimal point is where the NCE is reasonably low while maintaining a high level of privacy.

Future research will focus on implementing more privacy-preserving techniques that can provide accurate indoor positioning while maintaining user privacy. Moreover, developing privacy-aware design guidelines and best practices for BLE indoor positioning systems can help ensure that these systems are privacy-preserving by default.

Acknowledgments

The authors gratefully acknowledge funding from European Union's Horizon 2020 Research and Innovation programme under the Marie Skłodowska Curie grant agreement No. 813278 (A-WEAR: A network for dynamic wearable applications with privacy constraints, http://www.a-wear.eu/).

References

[1] S. Bennati and A. Kovacevic, "Modelling imperfect knowledge via location semantics for realistic privacy risks estimation in trajectory data," *Scientific reports*, vol. 12, no. 1, p. 246, 2022.

[2] J. W. Kim, K. Edemacu, and B. Jang, "Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey," *Journal of Network and Computer Applications*, p. 103315, 2022.

[3] M. Cäsar, T. Pawelke, J. Steffan, and G. Terhorst, "A survey on bluetooth low energy security and privacy," *Computer Networks*, vol. 205, p. 108712, 2022.

[4] V. Shubina, A. Ometov, S. Andreev, D. Niculescu, and E. S. Lohan, "Privacy versus Location Accuracy in Opportunistic Wearable Networks," in *Proc. of International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2020, pp. 1–6.

[5] Z. Zong, M. Yang, J. Ley, C. T. Butts, and A. Markopoulou, "Privacy by projection: Federated population density estimation by projecting on random features," *Proceedings on Privacy Enhancing Technologies*, vol. 1, pp. 309–324, 2023.

[6] M. Fachri and A. Khumaidi, "Positioning Accuracy of Commercial Bluetooth Low Energy Beacon," in *Proc. of IOP Conference Series: Materials Science and Engineering*, vol. 662, no. 5. IOP Publishing, 2019, p. 052018.

[7] H. Givehchian, N. Bhaskar, E. R. Herrera, H. R. L. Soto, C. Dameff, D. Bharadia, and A. Schulman, "Evaluating physical-layer ble location tracking attacks on mobile devices," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 1690–1704.

[8] Z. Hu, Y. Li, G. Jiang, R. Zhang, and M. Xie, "Prihorus: Privacy-preserving rss-based indoor positioning," in *ICC 2022-IEEE International Conference on Communications*. IEEE, 2022, pp. 5627–5632.

[9] H. Navidan, V. Moghtadaiee, N. Nazaran, and M. Alishahi, "Hide me behind the noise: Local differential privacy for indoor location privacy," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2022, pp. 514–523.

[10] E. S. Lohan, J. Talvitie, P. F. e Silva, H. Nurminen, S. Ali-Löytty, and R. Piché, "Received Signal Strength Models for WLAN and BLE-based Indoor Positioning in Multi-Floor Buildings," in *Proc. of International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2015, pp. 1–6.

[11] L. Clark, A. Papalia, J. T. Carvalho, L. Mastrostefano, and B. Krishnamachari, "Inter-Mobile-Device Distance Estimation Using Network Localization Algorithms for Digital Contact Logging Applications," *Smart Health*, vol. 19, p. 100168, 2021.

[12] P. Pascacio, J. Torres-Sospedra, A. R. Jiménez, and S. Casteleyn, "Mobile Device-based Bluetooth Low Energy Database for Range Estimation in Indoor Environments," *Scientific Data*, vol. 9, no. 1, p. 281, 2022.

[13] L. Flueratoru, V. Shubina, D. Niculescu, and E. S. Lohan, "On the High Fluctuations of Received Signal Strength Measurements with BLE Signals for Contact Tracing and Proximity Detection," *IEEE Sensors Journal*, vol. 22, no. 6, pp. 5086–5100, 2021.

[14] C. Gentner, D. Günther, and P. H. Kindt, "Identifying the BLE advertising channel for reliable distance estimation on smartphones," *IEEE Access*, vol. 10, pp. 9563–9575, 2022.

[15] E. Song, S. Kim, J. Han, and K. Kwon, "A 2.4-ghz quadrature local oscillator buffer insensitive to frequency-dependent loads for bluetooth low energy applications," *IEEE Microwave and Wireless Components Letters*, vol. 30, no. 10, pp. 961–964, 2020.

[16] J. Zhang, Q. Huang, Y. Huang, Q. Ding, and P.-W. Tsai, "Dp-trajgan: A privacy-aware trajectory generation model with differential privacy," *Future Generation Computer Systems*, vol. 142, pp. 25–40, 2023.

[17] P. Zhao, H. Jiang, J. C. Lui, C. Wang, F. Zeng, F. Xiao, and Z. Li, "P 3-loc: A privacy-preserving paradigm-driven framework for indoor localization," *IEEE/ACM Transactions on Networking*, vol. 26, no. 6, pp. 2856–2869, 2018.

[18] Q. Geng and P. Viswanath, "The optimal noise-adding mechanism in differential privacy," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 925–951, 2015.

[19] C. Meehan and K. Chaudhuri, "Location Trace Privacy Under Conditional Priors," in *Proc. of International Conference on Artificial Intelligence and Statistics*. PMLR, 2021, pp. 2881–2889.

[20] T. Cunningham, G. Cormode, and H. Ferhatosmanoglu, "Privacy-Preserving Synthetic Location Data in the Real World," in *Proc. of 17th International Symposium on Spatial and Temporal Databases*, 2021, pp. 23–33.

[21] Y. Ṣenbabaoğlu, G. Michailidis, and J. Z. Li, "Critical limitations of consensus clustering in class discovery," *Scientific reports*, vol. 4, no. 1, p. 6207, 2014.