Privacy versus Location Accuracy in Opportunistic Wearable Networks

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

***Abstract*—Future wearable devices are expected to increasingly exchange their positioning information with various Location-Based Services (LBSs). Wearable applications can include activity-based health and fitness recommendations, location-based social networking, location-based gamification, among many others. With the growing opportunities for LBSs, it is expected that location privacy concerns will also increase significantly. Particularly, in opportunistic wireless networks based on device-to-device (D2D) connectivity, a user can request a higher level of control over own location privacy, which may result in more flexible permissions granted to wearable devices. This translates into the ability to perform location obfuscation to the desired degree when interacting with other wearables or service providers across the network. In this paper, we argue that specific errors in the disclosed location information feature two components: a measurement error inherent to the localization algorithm used by a wearable device and an intentional (or obfuscation) error that may be based on a trade-off between a particular LBS and a desired location privacy level. This work aims to study the trade-off between positioning accuracy and location information privacy in densely crowded scenarios by introducing two privacy-centric metrics.**

***Index Terms*—Location privacy, location accuracy, wearable, opportunistic networks, measurement errors, intentional errors, obfuscation**

I. Introduction and Problem Statement

Opportunistic ad-hoc networks are known to provide seamless and robust wireless connectivity in the scenarios where the traditional infrastructure mode is not continuously available. As an evolution of mobile wireless ad-hoc networks, opportunistic communication can route the data dynamically without collecting the complete information about the network topology [1]. A potential niche for applying such networks can reside in the field of wearable devices. The notion of wearables stands for connected devices carried by users that sense and collect data, track physical activity, and improve user experience across different application domains that altogether form the Internet of Wearable Things (IoWT) [2].

In the case of wearables, opportunistic wireless solutions may offer more benefits to users compared to standalone wearable technologies. For example, no infrastructure is needed to perform the desired functions, due to the properties of devices being interconnected opportunistically to exchange information in a faster, more convenient, and less energy-consuming way than in an infrastructure mode. Such opportunistic networks can improve communications, positioning, and sensing capabilities of one's wearables even in the situations facing a limited power consumption of resource-constrained wearable ecosystems. One of the underlying reasons for such energy reduction is the possibility of computation offloading and distributed processing [3], e.g., by shifting the more demanding tasks to edge devices with higher computing power than one's wearables.

Since progress in wearable device development is driven by miniaturization and reduced energy consumption, products may not be equipped with conventional Global Navigation Satellite System (GNSS) support. One of the opportunistic ways to introduce a GNSS-based positioning is to utilize more advanced devices with known locations, which we call Anchor Nodes (ANs), to provide information to neighbors. ANs can be fixed or mobile. Hence, lower-cost wearables can perform self-positioning even in the absence of advanced signal processing capabilities or cutting-edge positioning chipsets. The downside of such opportunistic communication and positioning in a wearable scenario is a potential degradation in the privacy levels, especially when the exchange of data pertains to the location information of one's wearables. For example, wearable devices equipped with GNSS modules or more advanced Inertial Measurement Units (IMUs) acting as ANs for their proximate wearables with lower computational resources will have to disclose their locations to nearby nodes. This approach helps the nodes in the ANs' vicinity to self-locate. The process can also run in a cooperative manner, where each node takes turns to act as AN for other nodes in its vicinity, based on its previously computed position. Localization can be performed by relying on distance measurements to the neighboring ANs transmitting their estimated location to the devices within range [4]. Such distance measurements, in their turn, can be obtained from time, angle, or power measurements.

Our proposed system modeling for this opportunistic scenario starts with the assumption that neighboring wearable nodes are, to some extent, trusted and transmit their estimated location without an additional (e.g., intentional) error over proximity-based Device-to-Device (D2D) links [5]. A neigbouring wearable is defined as a gadget within the transmission range of the target device. The user location privacy depends on three main factors: i) how accurately such a location is estimated based on prior knowledge and/or information collected from the nearby nodes, ii) how accurately wearables disclose their estimated location in a futuristic scenario where users have full control of how and at which level of accuracy they can share own location information with other nodes, and iii) how many users with similar locations are there in the

978-1-7281-6455-7/20/$31.00 ©2020 IEEE

area. A relevant parameter to be able to quantify the location privacy in such situations can be the likelihood of mistaking a target user as being in the position of another user inside a specified geographical area, e.g., in a shopping mall, an office building, a transport hub. Clearly, such location privacy metric will depend both on the user density and their distribution in a certain area, as well as on the location estimation errors.

Multiple works focus on diverse aspects of location data privacy. For example, the study in [6] concentrates on developing a Privacy-Preserving Indoor Localization (PPIL) protocol for Received Signal Strength (RSS)-based indoor localization by encrypting the RSS values. In the subject work, the authors do not specify a Key Performance Indicator (KPI) for location privacy, and the paper primarily studies the deterioration of positioning accuracy as a consequence of applying PPIL. It also addresses the complexity of such an approach, which proves to be excessive. Concerning opportunistic wearable networks, a study in [7] considers a scenario where a user is opportunistically targeted and tracked via a dynamic cluster of sensor nodes. The respective algorithm is tested in two situations i) high-node density areas, where the solution proves to enhance the energy efficiency; ii) low-node density areas, where it displays robust performance despite coverage gaps. Another study on location privacy in [8] introduces a unified framework for the concept of privacy-preserving systems. The authors claim that users may adjust the degree of disclosable location information by deliberately misleading or accidentally providing erroneous data, while obfuscation is proposed as a privacy-enhancing solution. Generally, this method assumes intentional degrading of the information quality and thereby results in inaccuracy or imprecision [9].

Based on the reviewed literature, studies with a focus on location obfuscation and privacy-preserving algorithms do not propose location accuracy models. Therefore, the goal of this paper is to investigate the trade-offs between location data privacy and location accuracy in opportunistic wearable networks by evaluating the main factors affecting the levels of user privacy. Our methodology is to model the metrics relevant for location accuracy and location privacy via a Monte-Carlo statistical analysis in various multi-floor indoor scenarios. In particular, we target physical layer data processing and do not focus on the domain of higher-layer privacy protocols, in contrast with past works [4], [6], [10], which emphasize location privacy from another perspective. We also derive numerical results on the accuracy–privacy trade-off in localization under various user distributions inside a building, for different positioning technologies, and mindful of positioning measurements and intentional error models.

II. Selected Location-Specific Metrics

A. Location accuracy metrics

In the field of positioning, location accuracy is the primary KPI, which is introduced either as the probability distribution function (PDF) of the error, or, more commonly, as the error mean and is connected with the error variance that characterizes precision. One of the central challenges in the field is to achieve seamless localization with a decrease in the positioning error. The corresponding positioning errors occur due to the positioning algorithm properties as well as due to the environment properties (e.g., indoor versus outdoor, number of multipath components). Hereinafter, we refer to such positioning errors stemming from positioning technique as ‘measurement errors’, and their mean and variance are denoted in what follows by μ_m and σ_m^2, respectively. As a suitable example, the state-of-the-art Ultra-Wideband (UWB)-based positioning solutions provide sub-meter accuracy while performing localization indoors [11], [12]. Moreover, different evaluations studied the impact of the wearable placement on the localization accuracy [13]. Therefore, in our scenario, we assume multiple positions of wearable devices on a human body to assess potential positioning errors for specific body alignments in different situations.

Due to the body shadowing effects, the PDF of the positioning or ranging error varies for different on-body placements of wearable devices. Three primary locations for wearable sensors are considered under various conditions: the head or forehead position, the upper-body position, i.e., the chest and hand position and the limbs, i.e., the wrist, arm, ankle, and thigh.

According to [13], for scenarios where wearable sensors are head-mounted, the likelihood of line-of-sight (LOS) situations between the ANs and a wearable is high, and therefore the Gaussian PDF $f_{Gauss}(\epsilon)$ in (1) offers suitable modeling for the 3D range errors ϵ, i.e., ϵ is the Euclidian distance between the estimated position and the true position. According to the literature [14], Gaussian range-error modeling is valid not only for UWB Time-of-Flight (TOF) but also for positioning via Time of Arrival (TOA), Angle of Arrival (AOA), and RSS measurements for other systems, such as WiFi, Bluetooth Low Energy (BLE), Radio Frequency Identification (RFID), and others. Gaussian PDF $f_{Gauss}(\epsilon)$ is modeled as

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

where μ_m is the mean error and σ_m is the standard deviation (SD) of the positioning error. The subscript m stands for measurement. As ϵ is a distance error, thus always positive, only the positive part of $f_{Gauss}(\epsilon)$ actually characterizes the distance error, namely, $f_{Gauss}(\epsilon)S(\epsilon)$, where $S(\epsilon)$ is a step function ($S(\epsilon) = 1$ if $\epsilon \geq 0$ and $S(\epsilon) = 0$ if $\epsilon < 0$).

According to [12], in the situations where wearables are located in the upper-body area, the PDF $f_{GG}(\epsilon)$ of the positioning error can be modeled by a sum of Gaussian and Gamma distributions as

$$\begin{aligned} f_{GG}(\epsilon) &= \delta(RHA)\left(\frac{1}{\sigma_1\sqrt{2\pi}} e^{-\frac{(\epsilon-\mu_1)^2}{2\sigma_1^2}}\right) \\ &\quad + (1-\delta(RHA))\left(\lambda e^{-\lambda\epsilon}\frac{(\lambda\epsilon)^{k-1}}{\Gamma(k)} + c\right), \end{aligned} \tag{2}$$

where the ranging errors depend on the relative heading angle (RHA) between the user, wearable sensor, and ANs as well as on the body placement. Therefore, the term $\delta(RHA)$ in (2) is a unit Dirac impulse function equal to 0 for $RHA \in$ [0°, 112.5°) ∪ (247.5°, 360°]; and equal to 1 in case $RHA \in$ [112.5°, 247.5°]. The above σ_1 and μ_1 are the SD and the mean of the Gaussian-distributed part of the overall PDF, while λ and k are the parameters of the Gamma-distributed part of the overall PDF. Examples of σ_1, μ_1, λ, and k values are provided in [12], based on experimental work with UWB measurements.

In the case of $f_{GG}(\cdot)$, it is more likely that both LOS and non-line-of-sight (NLOS) situations between the ANs and the target wearable are present, as compared to the classic LOS case characterized by $f_{Gauss}(\epsilon)$.

The overall measurement errors in terms of mean μ_m and SD σ_m can then be computed as

$$\mu_m = \int_0^\infty \epsilon f_{GG}(\epsilon) d\epsilon, \tag{3}$$

$$\sigma_m^2 = \int_0^\infty (\epsilon - \mu_m)^2 f_{GG}(\epsilon) d\epsilon, \tag{4}$$

where ϵ and $f_{GG}(\cdot)$ are defined above, see (2).

According to [13], when the wearable sensors are located on limbs, and NLOS situations occur with high probability, the Gamma distribution in (5) models the positioning error ϵ

$$f_{Gamma}(\epsilon) = \delta(RHA)\left(be^{-b\epsilon}\frac{(b\epsilon)^{a-1}}{\Gamma(a)}\right) + (1-\delta(RHA))\left(\lambda e^{-\lambda\epsilon}\frac{(\lambda\epsilon)^{k-1}}{\Gamma(k)}\right) + c, \tag{5}$$

where b, a, λ, k, and c are the model parameters established experimentally in [13]. The measurement-based mean μ_m and SD σ_m follow a relationship similar to that in (3), where $f_{GG}(\cdot)$ is replaced by $f_{Gamma}(\cdot)$.

Additionally, as reported in [11], we consider the log-normal distribution $f_{Log-norm}(\epsilon)$ as a possible PDF for modeling the positioning error ϵ,

$$f_{Log-norm}(\epsilon) = \frac{1}{\sigma_m\sqrt{2\pi}} e^{-\frac{(ln(\epsilon)-\mu_m)^2}{2\sigma_m^2}}. \tag{6}$$

The aforementioned PDFs, namely, (1), (2), (5), and (6) are analyzed in the considered scenarios.

B. Location privacy metrics

Privacy is a fundamental right to be preserved, especially in the context of location. As reported in [10], *location privacy* is a unique type of information privacy which relates to the user decision on how, when, and to which extent one will disclose own location data to others. Therefore, the ability to be in charge of positioning information is crucial in the context of location privacy, and it is one of the main premises of our work to be investigated. As future smart wearables may allow higher user control of the location accuracy, more robust location-obfuscation methods should be implemented to perform privacy-preserving positioning.

In our study, we rely on the systematic survey provided in [15] with a taxonomy for key privacy metrics designed for diverse use cases. As it is known, entropy measures the uncertainty related to predicting the value of a random variable and is considered as a privacy-related metric to express the probability of incorrect user identification. Consequently, we examine two approaches for entropy measurements: Shannon and asymmetric entropy. Shannon entropy as an indicator of uncertainty is mentioned, for example, in [16]. One of our adopted privacy metrics is thus Shannon entropy, which is defined globally over all wearables in the system, as

$$H = -\sum_{i=1}^{N_w}\sum_{j=1}^{N_w}\int_\epsilon p_{ij}(\epsilon) log_2 p_{ij}(\epsilon) d\epsilon, \tag{7}$$

where H stands for what we call further ‘Shannon entropy’, p_{ij} is the probability of user i to be mistaken for another user j, and N_w is the number of wearables in the considered space. Various ϵ stand for all potential positions of wearables.

H essentially determines how likely it is that a wearable device disclosing its position with (intentional or unintentional) errors can be mistaken for another wearable in the crowd. In our simulations, we approximate the integral via sums by splitting the entire continuous space into smaller cells of $0.5m \times 0.5m$.

Additionally, we define the second privacy metric called asymmetric entropy by following the work in [15]

$$H_a = \sum_{i=1}^{N_w}\sum_{j=1}^{N_w}\int_\epsilon \frac{p_{ij}(\epsilon)(1-p_{ij}(\epsilon))}{(-2\alpha+1)p_{ij}(\epsilon)+\alpha^2} d\epsilon. \tag{8}$$

H_a reflects a situation where a third party has access to the distribution of user locations with the highest uncertainty at the point α. In our simulations, we set $\alpha = 0.5$ by following the approach of [17]. In our system model, we use the sum of asymmetric entropy, which is also known as cumulative asymmetric entropy. In the context of location, this metric uses p_{ij} and identifies the attacker's chances to mistake one user for another.

We argue that the probability p_{ij} to mistake a wearable i for another wearable j can be further calculated as

$$p_{ij}(\epsilon) = f_{distrib}(\epsilon)\Pi_{ij}, \tag{9}$$

where $f_{distrib}(\cdot)$ is the positioning-error PDF, namely, one of the distributions given in the previous section, and Π_{ij} is the probability of a cell being at ϵ distance away from user i to be occupied by user j. For example, the uniform distribution of users can be represented as

$$\Pi_{ij} = N_w/N_c, \tag{10}$$

where N_w is the observed number of wearable devices and N_c is the number of cells in the considered space. Similarly, the probability of a cell to be occupied for hotspot distributions, where the number of wearables is more likely to be higher in the vicinity of another wearable than farther away from it, can be modeled with an exponentially decreasing factor

$$\Pi_{ij} = exp(-\xi d_{ij}), \tag{11}$$

where ξ is a constant parameter (e.g, equals 1) and d_{ij} is the distance between wearable i and wearable j.

In the following sections, the metrics introduced above are used for investigating the trade-off between the privacy level and the location accuracy in the considered scenarios.

III. Definition of Scenarios

To illustrate the considered environment, we provide a graphical example of a potential indoor scenario for the opportunistic exchange of positioning information in Fig. 1, and we explain the modeling parameters used in the simulations.

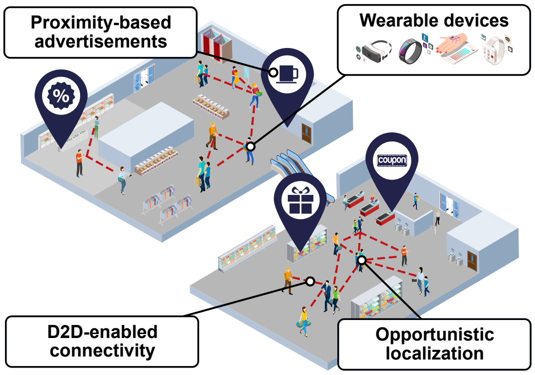

Fig. 1. Illustration of an indoor multi-floor scenario where wearables can disclose their location with the desired degree of obfuscation.

We refer to the multi-floor indoor scenario, which introduces a situation where each user has one wearable device with an opportunity to be in charge of own location information, i.e., being able to disclose it at the desired granularity and with the preferred intentional error. Each wearable can thus have particular preferences to which extent to disclose its position to other wearables or access nodes within a specified range. In such a way, the overall location error has a measurement error part (coming from the inherent uncertainty of knowing one's location, e.g., due to the positioning estimation algorithm, such as RSS, TOA, or AOA) and an intentional error part, which is user-defined.

The overall location error's SD is considered to be a sum of the measurement error and the intentional error. The intentional uncertainty is added on top of the measurement uncertainty, which is created by the location estimation algorithm. Further, each wearable can compute its position opportunistically owing to other wearable devices in proximity, which transmit their location information with some uncertainty and based, for instance, on distance measurements. Additionally, wearable location information can be acquired via power, time, or angle measurements using trilateration or triangulation procedures. As an example, the RSS measurements to nearby wearables may be converted into distance measurements subject to suitable path loss models. Another technique takes into account round-trip time measurements, which can be converted into distance measurements by multiplying the results of computations with half of the speed of light.

In our system model, we consider a two-floor densely crowded building (e.g., a shopping mall) with the square size of $150m \times 150m$. Therein, wearable devices are deployed according to various distributions:

- Uniform – wearables are assumed to be uniformly distributed inside the two-floor building.
- Queue – the scenario, where we consider that people with wearables stand in a line inside the building.
- Hotspot – the allocation with users, who gather within 'hotspots' modeled here as circles with certain radii, as illustrated in Fig. 2.

The entire building is divided into smaller rectangular areas called cells for modeling tractability, as shown with the empty gray circles in Fig. 2.

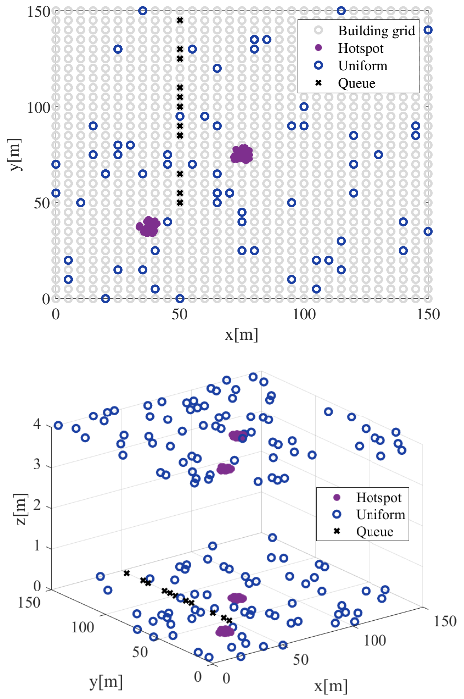

Fig. 2. Examples of three user distributions inside a building. Upper plot: floor-wise view with hotspots of 5 m raduis. Lower plot: 3D view with hotspots of 10 m radius.

A user can either be present or missing in a specific cell, and the respective flag will define the distribution of wearables inside the building. For clarity, Fig. 2 demonstrates $5m \times 5m$ cell size, but in our simulations, we utilized $0.5m \times 0.5m$ cell size to reduce the possibility that two users are placed precisely in the same cell (i.e., 0.5 m was considered here as the minimum comfort distance between two users in a public space). In our model, we refer to the the World Geodetic System (WGS84) as a reference coordinate system. In terms of the number of wearable devices, we followed the guide in 'Fire and Rescue Service' [18] and estimated the expected number of wearable devices per a shop sales area, i.e., for the spaces where persons reside (corridors, service rooms, and stairways are assumed as unusable space).

IV. Performance Analysis

In this section, we assess the main factors affecting the levels of user privacy in the considered scenario with respect to the chosen privacy metrics. In our study, we consider and evaluate two use cases, namely:

- The first use case provides an assessment of privacy metrics solely according to measurement errors (i.e., only the errors in disclosing one's location are triggered by specifications of the employed positioning algorithm). The fixed μ_m and σ_m measurement errors are adopted from the literature for three types of positioning methods: RSS-based positioning, TOA-based positioning, and AOA-based positioning. The examples are offered in Table I.

TABLE I
Estimation parameters.

Technique	μ_m	σ_m	References
RSS	1-5m	1-3m	[19], [20]
TOA	1m	1m	[21]
AOA	0m	1-2m	[22]

- Another use case considers a situation where users deliberately transmit their location with an intentional error. Therefore, we evaluate the performance under an assumption of an obfuscated location in our simulations with cumulative values of μ and σ.

Overall, as visible in Figs. 3-6, a higher number of users with wearable devices located inside the building provides better entropy results in comparison with a lower number of users. Moreover, scenarios, where hotspot distributions are assumed, offer better privacy protection than the use cases with uniformly distributed wearable devices inside the building. Additionally, the results shown in Fig. 3 follow the same trend, whereas Fig. 4 displays an increase in the privacy levels for all deployment types due to the value of the parameter α in (8), which equals 0.1 in this case. Therefore, it can be clearly observed that an increase of the uncertainty parameter α up to 0.5 causes a significant improvement in the privacy levels, particularly for the scenario where users are uniformly distributed inside the building.

Furthermore, obfuscating the positions via Gaussian noise proves to be better than obfuscating them via Gamma/Gaussian distributions due to the initial properties. The conventional Gamma distribution was not included for comparison in Fig. 6 as it relies on several parameters that are not directly mapped onto the SD of the positioning error; thus, the comparison would be unfair.

Based on the results in Fig. 6, we achieve around a two-fold increase in the Shannon entropy results for both Gaussian and Gaussian/Gamma distributions of errors and for both uniform and hotspot distributions of wearables inside the building by intentionally doubling the positioning error. The privacy gain with accumulating the positioning error is higher for smaller positioning errors, and it converges to a $1:1$ gain when the positioning error increases. As it can be learned from the obtained simulation results, the optimal strategy for users with accurate location estimates for enhancing the levels of privacy in the location domain is to obfuscate deliberately their precise coordinates.

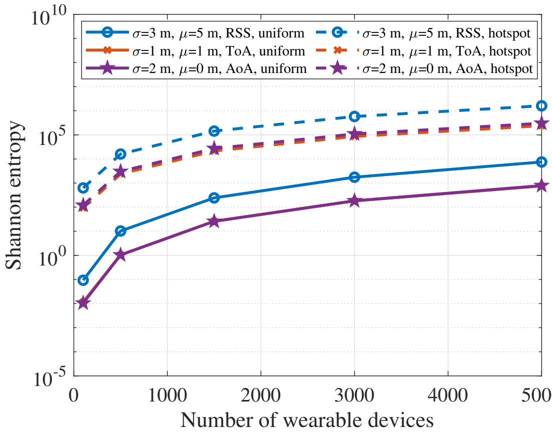

Fig. 3. Shannon entropy results for various Gaussian distributions versus the number of wearable devices inside the building.

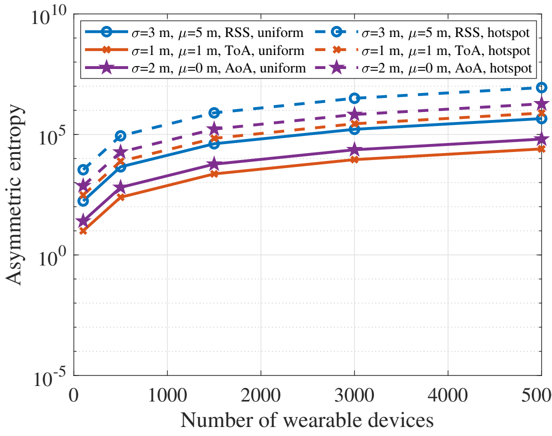

Fig. 4. Asymmetric entropy results for various Gaussian distributions versus the number of wearable devices inside the building, with the lowest $\alpha = 0.1$.

V. Discussion and Future Work

In this study, we characterized two metrics for location accuracy and location privacy, as well as described and assessed the levels of entropy in opportunistic wearable networks. The considered concept of transmitting the obfuscated location by adding random noise to the ground-truth coordinates was targeted under the assumption that not all LBSs out of those operating in public spaces require an accurate and precise location information. It may be of particular interest for wearable devices to mitigate the battery drain instead of utilizing sophisticated algorithms to achieve higher privacy.

As an example, there are certain location-based applications, where the granularity level of location accuracy can be ad-

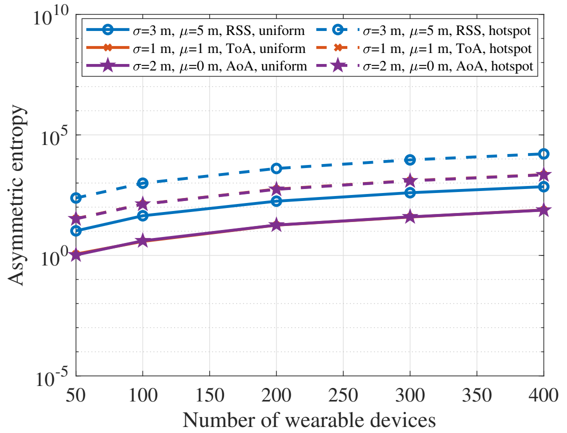

Fig. 5. Asymmetric entropy results for various Gaussian distributions versus the number of wearable devices inside the building, with the highest $\alpha = 0.5$.

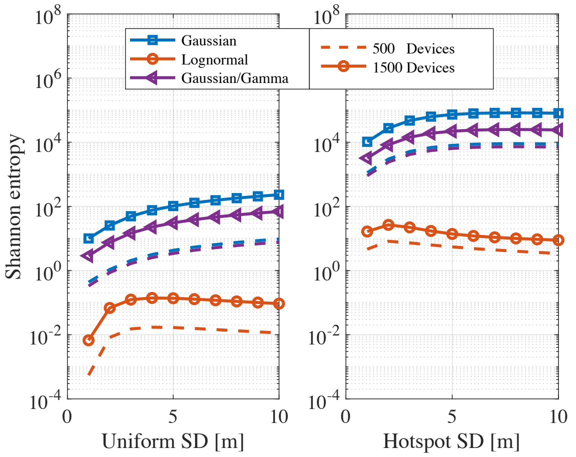

Fig. 6. Shannon entropy versus the SD of the positioning error.

justed to offer the actual service to the users without much degradation, e.g., information services, social networks.

To understand the simulation results for an opportunistic wearable scenario, we introduced three possible use cases based on various distributions of people inside a building: uniform, hotspot, and queue. As the queue concept shows limited scalability, the aspect is left for assessment and evaluation in the future together with the investigation of significant differences between Shannon entropy and asymmetric entropy results in the second use case.

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/). Also, the authors thank Roman Kovalchukov and Aleksei Ponomarenko-Timofeev for their valuable support with the software.

References

[1] C. B. Avoussoukpo, C. Xu, and M. Tchenagnon, "Ensuring Users Privacy and Mutual Authentication in Opportunistic Networks: A Survey," *International Journal of Network Security*, vol. 22, no. 1, pp. 118–125, 2020.

[2] A. Ometov, S. V. Bezzateev, J. Kannisto, J. Harju, S. Andreev, and Y. Koucheryavy, "Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 843–854, 2016.

[3] M. C. Silva, V. J. Amorim, S. P. Ribeiro, and R. A. Oliveira, "Field Research Cooperative Wearable Systems: Challenges in Requirements, Design and Validation," *Sensors*, vol. 19, no. 20.

[4] N. Baroutis and M. Younis, *Location Privacy in Wireless Sensor Networks*. Springer International Publishing, 2019, pp. 669–714. [Online]. Available: https://doi.org/10.1007/978-3-319-91146-5_18

[5] A. Ometov, E. Olshannikova, P. Masek, T. Olsson, J. Hosek, S. Andreev, and Y. Koucheryavy, "Dynamic Trust Associations over Socially-Aware D2D Technology: a Practical Implementation Perspective," *IEEE Access*, vol. 4, pp. 7692–7702, 2016.

[6] K. Järvinen, H. Leppäkoski, E.-S. Lohan, P. Richter, T. Schneider, O. Tkachenko, and Z. Yang, "PILOT: Practical Privacy-Preserving Indoor Localization Using Outsourcing," in *Proc. of IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2019, pp. 448–463.

[7] J. Z. Hare, J. Song, S. Gupta, and T. A. Wettergren, "POSE. R: Prediction-based Opportunistic Sensing for Resilient and Efficient Sensor Networks," *arXiv preprint arXiv:1910.10795*, 2019.

[8] R. Shokri, J. Freudiger, and J.-P. Hubaux, "A unified framework for location privacy," LCA, EPFL, Switzerland, Tech. Rep., 2010. [Online]. Available: http://infoscience.epfl.ch/record/148708

[9] M. Duckham and L. Kulik, "A Formal Model of Obfuscation and Negotiation for Location Privacy," in *Proc. of International Conference on Pervasive Computing*. Springer, 2005, pp. 152–170.

[10] M. Duckham and L. Kulik, "Location Privacy and Location-Aware Computing," pp. 63–80, 2006.

[11] N. Alsindi, B. Alavi, and K. Pahlavan, "Spatial characteristics of UWB TOA-based ranging in indoor multipath environments," in *Proc. of 18th International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE, 2007, pp. 1–6.

[12] T. Otim, A. Bahillo, L. E. Díez, P. Lopez-Iturri, and F. Falcone, "FDTD and Empirical Exploration of Human Body and UWB Radiation Interaction on TOF Ranging," *IEEE Antennas and Wireless Propagation Letters*, vol. 18, no. 6, pp. 1119–1123, 2019.

[13] T. Otim, A. Bahillo, L. E. Díez, P. Lopez-Iturri, Peio and F. Falcone, "Impact of Body Wearable Sensor Positions on UWB Ranging," *IEEE Sensors Journal*, vol. 19, no. 23, pp. 11 449–11 457, 2019.

[14] R. Zekavat and R. M. Buehrer, *Handbook of position location: Theory, practice and advances*. John Wiley & Sons, 2011, vol. 27.

[15] I. Wagner and D. Eckhoff, "Technical Privacy Metrics: A Systematic Survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 3, p. 57, 2018.

[16] A. Serjantov and G. Danezis, "Towards an Information Theoretic Metric for Anonymity," in *Proc. of International Workshop on Privacy Enhancing Technologies*. Springer, 2002, pp. 41–53.

[17] E. Ayday, J. L. Raisaro, J.-P. Hubaux, and J. Rougemont, "Protecting and Evaluating Genomic Privacy in Medical Tests and Personalized Medicine," in *Proc. of 12th ACM Workshop on privacy in the electronic society*, 2013, pp. 95–106.

[18] "Calculating Occupancy in Places of Assembly," Merseyside Fire & Rescue Service [Online] https://www.merseyfire.gov.uk/aspx/pages/protection/pdf/Calculating_Occupancy_assembly_buildings_GT.pdf, 2020.

[19] E. Lohan, J. Torres-Sospedra, H. Leppäkoski, P. Richter, Z. Peng, and J. Huerta, "Wi-Fi Crowdsourced Fingerprinting Dataset for Indoor Positioning," *Data*, vol. 2, no. 4.

[20] Y. Lu, P. Richter, and E. S. Lohan, "Opportunities and Challenges in the Industrial Internet of Things based on 5G Positioning," in *Proc. of 8th International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2018, pp. 1–6.

[21] B. Alavi and K. Pahlavan, "Modeling of the TOA-based Distance Measurement Error Using UWB Indoor Radio Measurements," *IEEE Communications Letters*, vol. 10, no. 4, pp. 275–277, 2006.

[22] S. Wielandt, J.-P. Goemaere, and L. De Strycker, "Multipath-Assisted Angle of Arrival Indoor Positioning System in the 2.4 GHz and 5 GHz band," in *Proc. of International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. IEEE, 2016, pp. 1–6.