Challenges of Privacy-aware Localization on Wearable Devices

Viktoriia Shubina[(1)], Aleksandr Ometov[(1)], Dragos Niculescu[(2)], Elena Simona Lohan[(1)]

[(1)] Tampere University, name.surname@tuni.fi

[(2)] University "Politehnica" of Bucharest, dragos.niculescu@cs.pub.ro

Abstract

In this paper, we give a brief survey of the main research results in the area of wearable localization solutions, with a particular focus on the privacy constraints in the localization on wearable devices. We identify several open research challenges and define open questions for further research directions. It is shown that finding adequate methods to protect the user location privacy on wearables is becoming increasingly important with the advent of new Location-Based Services relying on wearable devices.

1 State-of-the-art and motivation

The gradual increase[1] of IoT connected devices in recent years has been caused by the evolution of wireless technology and advanced discoveries in this field. The expansion in the number of wireless devices in use, and, in particular, in wearable devices, is inextricably intertwined with privacy concerns. Despite their typically small sizes, wearable devices are created to sense, collect, and store the data to assist in various application areas, such as healthcare [1], education [2], or industrial manufacturing [3].

Users already spend quite a lot of time with their smartphones in the pockets or close to their bodies, and such smart devices are continuously recording data about their owners. Wearables are also becoming more powerful and smarter in terms of being able to collect more and more user-related sensitive data, such as biometric parameters, e.g., heart rate, breath rate, sleep patterns, blood pressure, or activity-related parameters, e.g., number of steps, location [4]. Data sensitivity is defined in the EU GDPR[2].

There are several significant differences between a smartphone and a wearable device: (i) the smartphone typically serve as a gateway for the wearable, (ii) the location accuracy is still worse on a low-cost wearable device than on a smartphone equipped with a GPS receiver, (iii) accuracy requirements may be different for different applications, (iv) certain technologies may not be miniaturized enough for wearables, e.g., angle measurements require large antenna arrays of the order of $\lambda/2$ (with λ being the signal wavelength), and they also exhibit coupling problems. However, wearables of the future have the potential of a much higher user tracking ability, as they might continuously be in use (day and night), and mounted on the body unlike most of the smartphones.

Some relevant studies [5, 6] have demonstrated that most of the modern wearable devices include built-in sensors, which provide accurate location data, information about physical activity level, and possibly about the user mental health. The study [5] also shows that wearable data are typically easily accessible even without user awareness. There is no unique solution to cover all possible threats appearing in the use of wearable technology. Thus, further research and development are required. Our paper gives an overview of open challenges related to wearable-based localization and it is structured as follows. Section 2 describes the main localization technologies applicable to wearables, Section 3 summarizes the challenges and open questions in preserving the location privacy on wearables, while Section 4 concludes the paper.

[1] See "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)" by Statista, 2019: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[2] See "What personal data is considered sensitive?" by European Commission, 2019: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/.

2 Localization aspects of wearable technology

Wearable devices can be classified in function of their type, their purpose of use, proximity to human body [7], etc. If the wearables are endowed with various wireless sensors and own computationally intensive functions, such as localization features, researchers often call such devices "smart" in order to highlight the difference with other categories of machines without their own computationally intensive features. Three main categories of wearable devices were mentioned in [8] as (i) *accessories*, such as wrist wearables, head-mounted gadgets, and other smart jewelry; (ii) *e-Textiles*, meant to be worn as part of clothes; (iii) *e-Patches*, needed to be tattooed on human body; and we include (iv) *smart implants*, i.e., sensor implants in human body, typically of nano sizes.

Wearables and their in-built sensors are a crucial part of wireless data exchange processes. They can support diverse wireless connectivity ranges, from ultra-short and short to long ranges (the latter being less common than the former). After collecting data, wearables typically send it to a nearby smartphone or straight to the cloud database for further use.

Whereas GPS/GNSS technology can provide an excellent accuracy outdoors, indoor systems require to be equipped with non-GNSS sensors, such as accelerometers, gyroscopes, Bluetooth Low Energy (BLE) or WiFi chipsets, for improving range and accuracy of localization. A comparison of main localization techniques that may be utilized of wearables is illustrated in Table 1. The comparison is given in terms of achievable accuracy and privacy levels according to the Authors' evaluation: '++' stands for a good level, '+' stands for a moderate level, '-' stands for a low level. There is clear evidence that usually higher accuracy is achievable in trade-off to lower privacy and vice-versa.

Table 1: Comparison of Main Localization Techniques for Wearables.

Title	**Accuracy**	**Privacy**
Received Signal Strength (RSS) / Fingerprinting (FP)	-	++
Time of Arrival (TOA) / Time Difference of Arrival (TDOA)	++	-
Angle of Arrival (AOA)	++	-
Proximity	-	+
Inertial	+	+
Infrastructure-less (e.g., sounds, lights, odor)	-	++

One of the goals in future location-enabled wearables is to achieve a better user privacy level. For example, the term "location information" raises a number of concerns regarding ethics, such as possible unauthorized access, utilization, disclosure, alteration, and other types of fraud interaction with location sharing [9]. The security issue is also related to privacy in the context of a spatio-temporal location's integrity. In case such integrity is compromised, attackers can possibly exploit the user location data.

Another aspect related to wearable-based localization is the cooperative localization involving proximity-based device-to-device communications (D2D). Indeed, D2D architectures are increasingly penetrating many use cases, in particular, due to the rising trend of the 5G networks [10, 11]. One of the main advantages of D2D mode is the ability to share the information without intermediaries, such as access nodes (ANs), which reduces the amount of possible data leaks and decreases the latency by sharing the information directly within the network. Besides, D2D architectures can avoid physical-, protocol-, and other level privacy attacks [11] to maintain the integrity of the whole system.

Yet a diverse aspect related to wearable-based localization is the novel concept of delegation of use [12] referring to pools of (wearable) devices being shared by a pool of different users, i.e., a similar concept with shared bikes in smart cities.

All these various aspects of wearable-based localization are illustrated in a futuristic vision of a wearable-supporting network architecture in Fig. 1. The pool of wearable devices, i.e. the wearable cloud, can be shared, can belong to a static or moving person, and can act as standalone devices connected directly to a service provider or as terminals requiring a gateway (e.g., mobile device) to the network. The service provider related to location is the Location Solution Provider (LSP), namely the provider of the actual location technology (e.g., Google, HERE technologies) and the Location-Based Service Provider, namely the provider of a wearable service (e.g., Fitbit, Bittium) [13, 14].

Both D2D and AN-enabled modes are envisioned in our architecture, with examples of ANs given in Fig. 1 based on cellular, WiFi, or BLE networks (with the note that many other wireless supporting technologies can also fit in here). The numbered places (1 to 5) represent possible weak points of user privacy chain in a wearable architecture, from the cloud servers (numbered with 1) which might be insecure, to the *LBSP* and *LSP* providers, which may be offered by the same entity or by different entities, and to D2D or to the device-to-infrastructure (D2I) wireless links and third parties involved in the Location-Based Service (LBS) provisioning.

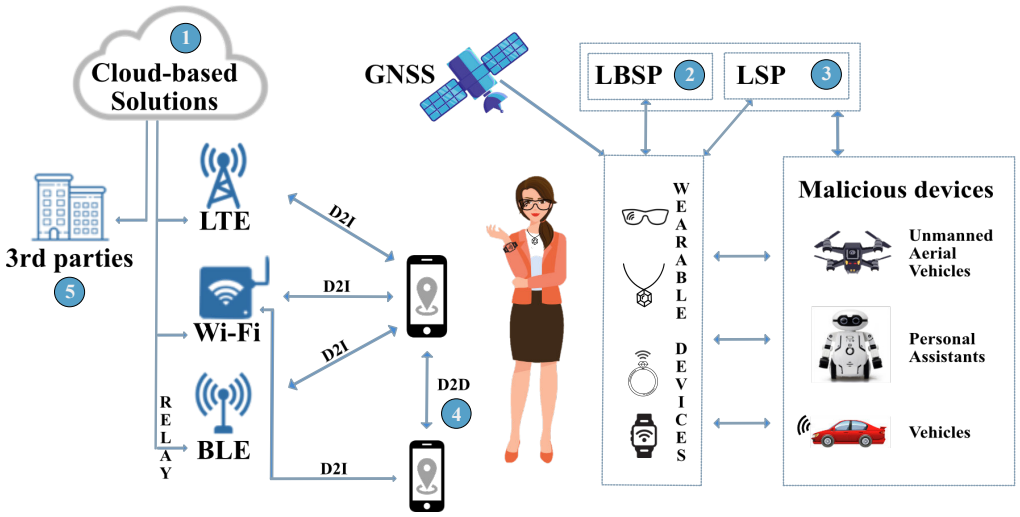

Fig. 1: Localization strategies for wearable scenario.

3 Location privacy challenges and open questions for future research

Mills et al. [6] claim that wireless wearable technology is one of the wireless technological solutions most exposed to privacy threats, due to their proximity to the human body. Privacy threats can manifest not only as of the harm for the data integrity but could also adversely affect the owner physically. Location privacy is a particular case of the privacy on wearable devices and it is analyzed in Table 2 from two different aspects: technical and ethical. We identify eight main research challenges related to location privacy on wearables. We refer to different existing solutions of these research problems, and also emphasize the open challenges.

Table 2: Privacy-aware challenges of localization and current solutions.

Research problem	**Possible solutions**	**Open challenges**
Low complexity for privacy preserving device-centric location solutions	Data encryption and compression [15]	To find a trade-off between processing delays vs compression/encryption efficiency
Privacy protection in network-centric localization solutions	Application of Hilbert transformation to mimic the real location in addition to anonymization [16]	To set the metrics to measure the trustability of LSP and LBSP
Cooperative localization solutions in D2D architectures	Advanced anonymization and indistinguishability methods implementation [11]	To prevent location data leakage to untrusted D2D nodes
Location and user data privacy protection when delegation-of-use concept is employed	Utilization of advanced encryption mechanisms along with secure storage [12]	To achieve high level of data security during the delegation of use to untrusted user
Dealing with long delays if encryption mechanisms are used to protect location data [17]	Storage of partially encrypted location data	To ensure high protection / high security in real time
Efficient data compression solutions for FP-based solutions with wireless transfer of FP databases	Estimating the actual location using Machine Learning algorithms [18]	To develop efficient lossless compression techniques
Computational complexity vs Battery trade-off	Online and offline location privacy protection mechanisms for configuration optimal parameters according to main user's objectives [19]	To reduce privacy leaks at the cost of highly complex hardware and software
Privacy vs Accuracy trade-off	k-anonymity, l-diversity and successors [20]	To balance efficiently accuracy and anonymity

4 Conclusions

In this summary, we have observed the main localization techniques, listed main privacy challenges, and analyzed the potential solutions. We conclude that there are several concerns related to location privacy on wearables, which need to be carefully addressed and solved in privacy-aware localization strategies for wearable technology.

Acknowledgements

The authors gratefully acknowledge funding from European Union's Horizon 2020 Research and Innovation programme under the Marie Sklodowska Curie grant agreement No. 813278 (A-WEAR, `http://www.a-wear.eu/`).

References

[1] J. Li et al. Health monitoring through wearable technologies for older adults: Smart wearables acceptance model. *Applied ergonomics*, 75:162–169, 2019.

[2] J.M. Liang et al. Smart Interactive Education System Based on Wearable Devices. *Sensors*, 19(15):3260, 2019.

[3] J. Barat and P.R. da Cunha. Safety Is the New Black: The Increasing Role of Wearables in Occupational Health and Safety in Construction. In *Int. Conf. on Business Inf. Syst.*, pages 526–537. Springer, 2019.

[4] Ometov et al. Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications. *IEEE Network*, 33(2):82–88, 2019.

[5] P. Datta et al. A Survey of Privacy Concerns in Wearable Devices. In *Proc. of IEEE International Conference on Big Data (Big Data)*, pages 4549–4553. IEEE, 2018.

[6] A. J. Mills et al. Wearing safe: Physical and informational security in the age of the wearable device. *Business Horizons*, 59(6):615–622, 2016.

[7] M. Mardonova and Y. Choi. Review of wearable device technology and its applications to the mining industry. *Energies*, 11(3):547, 2018.

[8] S. Seneviratne et al. A survey of wearable devices and challenges. *IEEE Communications Surveys & Tutorials*, 19(4):2573–2620, 2017.

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

[10] P. Gandotra et al. A survey on device-to-device (D2D) communication: Architecture and security issues. *Journal of Network and Computer Applications*, 78:9–29, 2017.

[11] M. Haus et al. Security and privacy in device-to-device (D2D) communication: A review. *IEEE Communications Surveys & Tutorials*, 19(2):1054–1079, 2017.

[12] A. Ometov et al. Facilitating the delegation of use for private devices in the era of the Internet of Wearable Things. *IEEE Internet of Things Journal*, 4(4):843–854, 2016.

[13] E.S. Lohan et al. 5G Positioning: Security and Privacy Aspects. *A Comprehensive Guide to 5G Security; John Wiley & Sons Ltd.: Hoboken, NJ, USA*, page 281, 2018.

[14] L. Chen et al. Robustness, security and privacy in location-based services for future IoT: A survey. *IEEE Access*, 5:8956–8977, 2017.

[15] K. Jarvinen et al. PILOT: practical privacy-preserving indoor localization using outsourcing. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 448–463. IEEE, 2019.

[16] N. Alikhani et al. A Privacy Preserving Method for Crowdsourcing in Indoor Fingerprinting Localization. In *Proc. of 8th International Conference on Computer and Knowledge Engineering*, pages 58–62. IEEE, 2018.

[17] J. Wei. How Wearables Intersect with the Cloud and the Internet of Things: Considerations for the developers of wearables. *IEEE Consumer Electronics Magazine*, 3(3):53–56, 2014.

[18] E. Toch et al. Analyzing large-scale human mobility data: a survey of machine learning methods and applications. *Knowledge and Information Systems*, 58(3):501–523, 2019.

[19] V. Primault et al. The long road to computational location privacy: A survey. *IEEE Communications Surveys & Tutorials*, 2018.

[20] I. Wagner and D. Eckhoff. Technical privacy metrics: a systematic survey. *ACM Computing Surveys (CSUR)*, 51(3):57, 2018.