Karlsruher Institut für Technologie

Institute of Information Security and Dependability (KASTEL)
IT Security
Prof. Dr. Thorsten Strufe

The filtering attack against trajectory anonymization

Project Group "Praxis der Forschung"
Summer Term 2022

1 Project

GPS tracks every user's movement, creating thus an unlimited input of trajectories. Since the GPS tracking systems are often slightly imprecise, filters exist which try to correct these imprecisions to reconstruct the real trajectories. On the other hand, users' trajectories contain highly sensitive information which must be anonymized, and one common type of anonymization technique is based on random noise addition. As one could think, if filters can be used to correct GPS impressions, they can potentially be used to undo an anonymization step based on random noise addition, reverting therefore any privacy guarantees.

2 Goal

The goal of this project is to analyze the possibility and potential of this attack against such anonymization techniques. We are interested in understanding how the filters and noise addition techniques work, how they are used to eliminate GPS location imprecisions and how effectively they do so, and, more importantly, we are looking to provide an experimental evaluation or formal proof showing if filters are capable of eliminating noise added by any anonymization mechanism, or a subset of them. On the other hand, we will be also interested in studying if we can find (or create) a noise-based mechanism with strong privacy guarantees (such as differential privacy) that is secure against filtering attacks.

3 Starting References

[1] motivates and overviews the project's setting. Chapter 1 in [2] provides includes a list of different filters present in the state of the art for spatial trajectories. The Laplacian mechanism of differential privacy is a known example of an anonymization technique based on noise addition; they are defined in [3]. [4] provides a syntactic privacy notion and mechanism based on spatial translation and very briefly talks about GPS imprecisions.

4 Contact

Alex Miranda Pascual <alex.pascual@kit.edu>

References

[1] Hao Wang, Zhengquan Xu, Shan Jia, Ying Xia, and Xu Zhang. "Why current differential privacy schemes are inapplicable for correlated data publishing?" In: *World Wide Web* 24.1 (2021), pp. 1–23. DOI: 10.1007/s11280-020-00825-8.

[2] Chris Brunsdon. “Computing with spatial trajectories, edited by Yu ZhengXiaofang Zhou, Berlin, Springer, 2011, 1st ed., £84.99 (hardcover), 308 pp. ISBN-10: 1461416280; ISBN-13: 978-1461416289”. In: *Int. J. Geogr. Inf. Sci.* 27.1 (2013), pp. 208–209. DOI: 10.1080/13658816.2012.741688.

[3] Cynthia Dwork and Aaron Roth. “The Algorithmic Foundations of Differential Privacy”. In: *Found. Trends Theor. Comput. Sci.* 9.3-4 (2014), pp. 211–407. DOI: 10.1561/0400000042.

[4] Osman Abul, Francesco Bonchi, and Mirco Nanni. “Never Walk Alone: Uncertainty for Anonymity in Moving Objects Databases”. In: *Proceedings of the 24th International Conference on Data Engineering, ICDE 2008, April 7-12, 2008, Cancún, Mexico*. Ed. by Gustavo Alonso, José A. Blakeley, and Arbee L. P. Chen. IEEE Computer Society, 2008, pp. 376–385. DOI: 10.1109/ICDE.2008.4497446.