QUANTIFYING THE EFFECT OF CO-LOCATION INFORMATION ON LOCATION PRIVACY

MANCHALA MALAKONDRAYUDU Student (MCA), NRI INSTITUTE OF TECHNOLOGY, A.P., India.
R.SEETHARAM Assistant Professor, Dept. of MCA, NRI INSTITUTE OF TECHNOLOGY, A.P., India.

Abstract —This paper, is to report co-locations with other users on social networks, e.g., by tagging friends on pictures they upload or in the messages they post. Practical opportunities such as urban planning and location recommendation are created by being able to quantify location sociality. The users' IP addresses also constitute a source of co-location information. Combined with (possibly obfuscated) location information, such co-locations can be used to improve the inference of the users' locations, thus further threatening their location privacy: As co-location information is taken into account, not only a user's reported locations and mobility patterns can be used to localize her, but also those of her friends (and the friends of their friends and so on). In this paper, we study this problem by quantifying the effect of co-location information on location privacy, considering an adversary such as a social network operator that has access to such information.

INTRODUCTION

Quantifying Interdependent Privacy Risks with Location Data Nowadays, sharing their geographical locations, i.e. check-ins, is quite common for OSN users. In addition, location-based social networks (LBSNs) are created as a special type of OSNs dedicated to location sharing. Two representative companies are Foursquare and Yelp. A large quantity of human mobility data becomes available with the emergence of LBSNs. in particular location-based social networks, have become immensely popular. 1 For instance, our preliminary survey involving 132 Foursquare users, recruited through Amazon Mechanical Turk, reveals that 55:3% of the participants report collocations in their check-ins and that for the users who do so, on average, 2.84%_0.06 of their check-ins contain collocation information. In fact, co-location information can be obtained in many different ways, such as automatic face recognition on pictures (which contains the time and location at which the picture was taken in their EXIF data, e.g., Facebook's Photo Magic [2]), Bluetooth-enabled devicesniffing and reporting neighboring devices. Similarly, users who connect from the same IP address are likely to be attached to the same Internet access point, thus providing evidence of their co-location. Such data falls into the category of multiple-subjects personal data [3].

Attacks exploiting both location and co-location information (as mentioned in [4]) can be quite powerful, as we show in this paper. Figure 1 depicts and describes two instances in which co-location can improve the performance of a localization attack, thus degrading the location privacy of the users involved. It is clear that the proper exploitation of such information by an attacker can be complex because he has to consider jointly the (co-)location information collected about a potentially large number of users. This is due to the fact that, in the presence of co-location information, a user's location is correlated with that of her friends, which is in turn correlated to that of their own friends and so on.

LITERATURE SURVEY

AUTHORS: K. Chatzikokolakis, C. Palamidessi, and M. Stronati,

This paper presents the capabilities of modern devices, coupled with the almost ubiquitous vailability of Internet connectivity, have resulted in photos being shared online at an unprecedented scale. This is further amplified by the popularity of social networks and the immediacy they offer in content sharing. Existing access control mechanisms are too coarse-grained to handle cases of conflicting interests between the users associated with a photo.

AUTHORS: Y. De Mulder, G. Danezis, L. Batina, and B. Preneel,

 DOI : 10.36893.DRSR.2021.V08I14.118-121

As devices move within a cellular network, they register their new location with cell base stations to allow for the correct forwarding of data. We show it is possible to identify a mobile user from these records and a pre-existing location profile, based on previous movement. Two different identification processes are studied, and their performances are evaluated on real cell location traces. The best of those allows for the identification of around 80% of users.

AUTHORS: R. I. M. Dunbar

Two general kinds of theory (one ecological and one social) have been advanced to explain the fact that primates have larger brains and greater congnitive abilities than other animals. Data on neocortex volume, group size and a number of behavioural ecology variables are used to test between the various theories. Group size is found to be a function of relative neocortical volume, but the ecological variables are not. This is interpreted as evidence in favour of the social intellect theory and against the ecological theories.

PROPOSED SYSTEM

A GENERAL FRAMEWORK FOR CONSTRUCTING AND USING PROBABILISTIC MODELS OF COMPLEX SYSTEMS THAT WOULD ENABLE A COMPUTER TO USE AVAILABLE INFORMATION FOR MAKING DECISIONS. MOSTTASKS REQUIRE A PERSON OR AN AUTOMATED SYSTEM TO REASON--TO REACH CONCLUSIONS BASED ON AVAILABLE INFORMATION. THE FRAMEWORK OF PROBABILISTIC GRAPHICAL MODELS, PRESENTED IN THIS BOOK, PROVIDES A GENERAL APPROACH FOR THIS TASK.

- Attacks exploiting both location and co-location information can be quite powerful.
- projects on Quantifying Interdependent Privacy Co-location can improve the performance of a localization attack, thus degrading the location privacy of the users involved.

In the proposed system, the system has implemented the effect on users' location privacy when co-location information is available, in addition to individual (obfuscated) location information. To the best of our knowledge, this is the first paper to quantify the effects of co-location information that stems from social relationships between users on location privacy; as such it constitutes a first step towards bridging the gap between studies on location privacy and social networks. Indeed, most studies on geo-location and social networks look at how social ties can be inferred from co-locations between individuals and how social ties can be used to de-anonymize mobility traces. The system has shown that, by considering the users' locations jointly, an adversary can exploit co-location information to better localize users, hence decreasing their individual privacy. Although the optimal joint localization attack has a prohibitively high computational complexity, the polynomial-time approximate inference algorithms that we propose provide good localization performance. An important observation from our work is that a user's location privacy is no longer entirely in her control, as the co locations and the individual location information disclosed by other users significantly affect her own location privacy.

Advantages

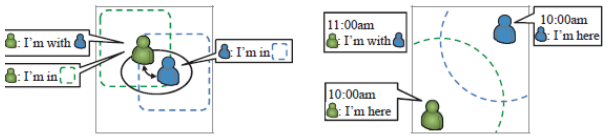
- Location-Privacy Protection Mechanisms on Location data
  - Many techniques are involved in the implementation of Data Protection on Locations
  - Even in the case where a user does not disclose any location information, her privacy can decrease by up to 21% due to the information reported by other users.

RELATED WORK

This family of attacks and their complexity is precisely the focus of this paper. More specifically, we make the following four contributions: (1) We identify and formalize the localization problem with co-location information, we propose an optimal inference algorithm and analyze its complexity. We show that, in practice, the optimal inference algorithm is intractable due to the explosion of the state space size. (2) We describe how an attacker can drastically reduce the computational complexity of the attack by means of well-chosen approximations. We present a polynomialtime heuristic based on a limited set of considered users (i.e., optimal inference with the data of only two or three users) and

 DOI : 10.36893.DRSR.2021.V08I14.118-121

an approximation based on the belief propagation (BP) algorithm executed on a general Bayesian network model of the problem (approximate inference with the data of all the



(a) (b)

Fig. 1. Examples showing how co-location information can be detrimental to privacy. (a) A user reports being in a given area, and a second user reports being in another (overlapping) area and that she is collocated with the first user. By combining these pieces of information, an adversary can deduce that both users are located in the intersection of the two areas, thus narrowing down the set of possible locations for both of them. (b) Two users (initially apart from each other, at 10am) declare their exact individual location. Later (at 11am), they meet and report their co-location without mentioning where they are. By combining these pieces of information, the adversary can infer that they are at a place that is reachable from both of the initially reported locations in the amount of time elapsed between the two reports. users). (3) Using a mobility dataset, we evaluate and compare the performance of the different solutions in different scenarios, with different settings. The belief propagation based solution, which does not appear in the first version of this work [1], gives significantly better results (in terms of the performance of the inference) than the heuristic. (4) We propose and evaluate some countermeasures (i.e., socialaware location-privacy protection mechanisms) including fake co-locations reporting and coordinated location disclosure. This last contribution also constitutes new content with respect to the first version of this work [1]. In this revised and extended version, we also update the formalism and the evaluation to take into account the fact that users can report being co-located when, in fact, they are not. Our experimental results show that, even in the case where the adversary considers co-locations with only a single friend of the targeted user, the median location privacy of the user is decreased by up to 62% in a typical setting. Even in the case where a user does not disclose any location information, her privacy can decrease by up to 21% due to the information reported by other users. A paramount finding of our work is that users partially lose control over their location privacy as co-locations and individual location information disclosed by other users substantially affect their own location privacy. Our experimental results also show that a simple countermeasure (i.e., coordinated location disclosure) can reduce the privacy loss by up to 50%. To the best of our knowledge, this is the first attempt to quantify the effects of co-location information that stems from social relationships, on location privacy; thus making a connection between OSNs and location privacy.

CONCLUSION

In this paper , Quantifying Interdependent Privacy have proposed a new notion in this paper, namely location sociality, to describe whether a location is suitable for conducting social activities. Experimental results of millions of Instagram check-in data validate location sociality with some in-depth discoveries. Two case studies, including friendship prediction and location recommendation, show the usefulness of our quantification.

REFERENCES

[1] A.-M. Olteanu, K. Huguenin, R. Shokri, and J.-P. Hubaux, "Quantifying the Effect of Co-locations on Location Privacy," in PETS, 2014, pp. 184–203.
[2] "Facebook Messenger adds fast photo sharing using face recognition," The Verge, http://www.theverge.com/2015/11/ 9/9696760/facebook-messenger-photo-sharing-face-recognition, nov 2015, last visited: Nov. 2015.
[3] S. Gnesi, I. Matteucci, C. Moiso, P. Mori, M. Petrocchi, and M. Vescovi, "My Data, Your Data, Our Data: Managing Privacy Preferences in Multiple Subjects Personal Data," in Annual Privacy Forum, 2014, pp. 154–171.

 DOI : 10.36893.DRSR.2021.V08I14.118-121

[4] C. Vicente, D. Freni, C. Bettini, and C. S. Jensen, "Location-related privacy in geo-social networks," IEEE Internet Computing, vol. 15, no. 3, pp. 20–27, 2011.
[5] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in S&P, 2011, pp. 247–262.
[6] L. E. Baum and T. Petrie, "Statistical inference for probabilistic functions of finite state markov chains," The Annals of Mathematical Statistics, vol. 37, no. 6, pp. 1554–1563, 1966.
[7] A. Narayanan and V. Shmatikov, "De-anonymizing social networks," in S&P'09: Proc. of the 30th IEEE Symp. on Security and Privacy, 2009, pp. 173–187.
[8] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in SIGMOD, 2008, pp. 121–132.
[9] R. L. Stratonovich, "Conditional Markov Processes," Theory of Probability & its Applications, vol. 5, no. 2, pp. 156–178, 1960.
[10] D. Koller and N. Friedman, Probabilistic graphical models: principles and techniques. MIT press, 2009.
[11] J. Pearl, Probabilistic reasoning in intelligent systems: networks of plausible inference. Morgan Kaufmann, 2014.
[12] K. P. Murphy, Y. Weiss, and M. I. Jordan, "Loopy belief propagation for approximate inference: An empirical study," in UAI. Morgan Kaufmann Publishers Inc., 1999, pp. 467–475.

 DOI : 10.36893.DRSR.2021.V08I14.118-121