ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Location Among User Queries for Privacy through Collaboration

B.Ravindra Naik
M.Tech Student,
Department of CSE,
Sree Rama institute of Technology and Science,
Kuppenakuntla, Penuballi, Khammam,TS India.

N.Naveen
Assistant Professor,
Department of CSE,
Sree Rama institute of Technology and Science,
Kuppenakuntla, Penuballi, Khammam,TS India.

ABSTRACT:

Location-aware smart phones support various location-based services (LBSs): users query the LBS server and learn on the fly about their surroundings. However, such queries give away private information, enabling the LBS to track users. We address this problem by proposing a user-collaborative privacy-preserving approach for LBSs. Our solution does not require changing the LBSserver architecture and does not assume third party servers; yet, it significantly improves users' location privacy. The gain stems from the collaboration of mobile devices: they keep their context information in a buffer and pass it to others seeking such information.

Thus, a user remains hidden from the server, unless all the collaborative peers in the vicinity lack the sought information. We evaluate our scheme against the Bayesian localization attacks that allow for strong adversaries who can incorporate prior knowledge in their attacks. We develop a novel epidemic model to capture the, possibly time-dependent, dynamics of information propagation among users. Usedin the Bayesian inference framework, this model helps analyze the effects of various parameters, such as users' querying rates and the lifetime of context information, on users' location privacy.

The results show that our scheme hides a high fraction of location-based queries, thus significantly enhancing users' location privacy. Our simulations with real mobility traces corroborate our model-based findings. Finally, our implementation on mobile platforms indicates that it is lightweight and the cost of collaboration is negligible.

Index Terms:

Mobile networks, location-based services, location privacy, Bayesian inference attacks, epidemic models

INTRODUCTION:

SMARTPHONES, among other increasingly powerful mobile computing devices, offer various methods of localization. Integrated GPS receivers, or positioning servicesbased on nearby communication infrastructure (Wi-Fi access points or base stations of cellular networks), enable users to position themselves fairly accurately, which has led to a wide offering of Location-based Services (LBSs). Such services can be queried by users to provide real-time information related to the current position and surroundings of the device, e.g., contextual data about points of interest such as petrol stations, or more dynamic information such as traffic conditions. The value of LBSs is in their ability to obtain on the fly up-to-date information. Although LBSs are convenient, disclosing location information can be dangerous. Each time an LBS query is submitted, private information is revealed. Users can be linked to their locations, and multiple pieces of such information can be linked together. They can then be profiled, which leads to unsolicited targeted advertisements or price discrimination.Even worse, the habits, personal and private preferences, religious beliefs, and political affiliations, for example,can be inferred from a user's whereabouts. This could make her the target of blackmail or harassment. Finally, real-time location disclosure leaves a person vulnerable to absence disclosure attacks: learning that someone is away from home could enable someone to break into her house or blackmail her . An stalker can also exploit the location information.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Existing System:

There are many collaborative schemes for mobile networks. Mobile users, for example, can collectively build a map of an area . Collaboration is also needed when sharing content or resources (e.g., Internet access) with other mobile nodes . Various threats associated with sharing location information have been identified in the literature. For example, users can be identified even if they share their location sporadically. Knowing the social relations between users can help an adversary to better de-anonymize their location traces . Finally, location sharing of a user not only diminishesher own privacy, but also the privacy of others . Techniques proposed to protect location privacy in LBSs can be classified based on how they distort the users' queries before the queries reach the LBS server. The queries can be anonymized (by removing users' identities), pseudonymized (by replacing users' real names with temporal identifierscalled pseudonyms), or obfuscated (by generalizing or perturbing the spatiotemporal information associated to the queries). Queries can also be camouflaged by adding some dummy queries, or be completely eliminated and hidden from the LBS . Combinations of these methods have been employed in the existing (centralized or distributed) mechanisms.We now discuss these approaches in more detail.

Proposed System:

We consider N users who move in an area split into M discrete regions/locations. The mobility of each user u is a discrete-time Markov chain on the set of regions: The probability that user u, currently in region ri, will next visit region rj is denoted by puðrjjriÞ. Let puðriÞ be the probability that user u is in region ri. Each user possesses a location-aware wireless device, capable of ad hoc device-to-device communication and of connecting to the wireless infrastructure (e.g., cellular and Wi-Fi networks).As users move between regions, they leverage the infrastructure to submit local-search queries to an LBS, at some frequency that we term LBS access frequency. The frequency at which users query the LBS varies depending on the type of requested information, on the dynamics of information update in the LBS database, or on the geographical region in the sense that it is no longer valid. Note that information expiration is not equivalent to the user accessing the LBS: A user accesses the LBS when her information has expired and she wishes to receive the most up-to-date version of it.

In addition, the information the LBS provides is self verifiable,i.e., users can verify the integrity and authenticity of the server responses. This can be done in different ways; in our system, the user device verifies a digital signature of the LBS on each reply by using the LBS provider's public key. As a result, a compromised access point or mobile device cannot degrade the experience of users by altering replies or disseminating expired information.

EPIDEMIC MODEL FOR THE DYNAMICS OF MOBICROWD:

The performance of our system depends on various parameters, such as the rate of contacts and the level of collaboration between users, the rate of LBS query generation, etc. We now describe a model for MobiCrowd, with the help of which we can directly evaluate the effect of various parameters on users' location privacy. Observing the effect of the parameters also helps when designing a system and testing "what-if" scenarios.

For example, we can immediately see the level of collaboration required to achieve a desired privacy level or how the privacy level will change if the usersmake queries more frequently or less frequently. We draw an analogy between our system and epidemic phenomena: location-context information spreads like an infection from one user to another, depending on the user state (seeking information, having valid information, etc.). For example, a seeker becomes "infected" when meeting an "infected" user, that is, a user with valid information..

Model States and System of ODEs:

As mentioned earlier, users move in an area partitioned into multiple regions. The state of context knowledge within a region intuitively corresponds to the disease status in an epidemic. In general, a user's knowledge state would be multi-dimensional, because a different piece of information is relevant for each region. Thus, for each region we would have an associated epidemic model, with the same structure but different parameters. However, the state of knowledge about a region is unrelated to the knowledge about other regions, so different regions can be analyzed separately. We present our model for a single region, with users entering and exiting it; and we describe the states and the dynamics of our epidemic model for that single region.

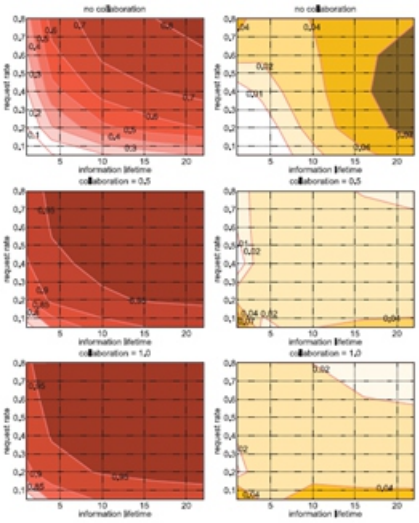
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

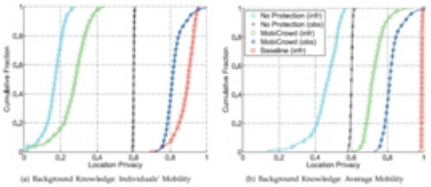
QUANTITATIVE ANALYSIS:

The direct objective of Mobi Crowd is to hide user queries from the server. We quantify this objective, as our first evaluation metric, through the hiding probability: the probability that a user's query becomes hidden from the server due to Mobi Crowd protocol. Under various user mobility and information spreading dynamics, we compute this metric using the results of the time-dependent epidemic model,and we compare to the results of simulations on a data setof real mobility traces. In Section 7, we show that the simulation results corroborate our model-based findings about the hiding probability.

EVALUATION:

The location traces that we use belong to 509 randomly chosen mobile users (vehicles) from the epfl/mobility data set at CRAWDAD [39]. We set the time unit of the simulation to 5 minutes and we consider the users' locations at integer multiples of the time unit, thus synchronizing all the traces. We group time units into three equal-size time periods: morning, afternoon, evening. We divide the Bay Area into 10 _ 25 equal-size regions. Two users in a region are considered to be neighbors of each other if they are within 100 m of each other (using Wi-Fi). We run our simulation for 100 times on the traces and compute the average of the results. From the location traces, we construct the timedependent mobility model of each individual user, in the format of transition probability matrices (one matrix per time period). We also compute the average mobility model, which reflects how the whole crowd moves. For each region and time period we compute the mobility parameters _, m, and b separately .





CONCLUSION:

We have proposed a novel approach to enhance the privacy of LBS users, to be used against service providers who could extract information from their LBS queries and misuse it. We have developed and evaluated MobiCrowd, a scheme that enables LBS users to hide in the crowd and to reduce their exposure while they continue to receive the location context information they need. MobiCrowd achieves this by relying on the collaboration between users, who have the incentive and the capability to safeguard their privacy. We have proposed a novel analytical framework to quantify location privacy of our distributed protocol. Our epidemic model captures the hiding probability for user locations, i.e., the fraction of times when, due to MobiCrowd, the adversary does not observe user queries. By relying on this model, our Bayesian inference attack estimates the location of users when they hide. Our extensive joint epidemic/ Bayesian analysis shows a significant improvement thanks to MobiCrowd, across both the individual and the average mobility prior knowledge scenarios for the adversary. We have demonstrated the resource efficiency of MobiCrowd by implementing it in portable devices.

Securely determining own location:

[1] "Pleaserobme," http://www.pleaserobme.com, 2014.

[2] J. Meyerowitz and R.R. Choudhury, "Hiding Stars With Fireworks:Location Privacy through Camouflage," Proc. MobiCom'09, 2009.

[3] F. Olumofin, P.K. Tysowski, I. Goldberg, and U. Hengartner,"Achieving Efficient Query Privacy for Location Based Services,"Proc. 10th Int'l Conf. Privacy Enhancing Technologies, 2010.

[4] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan,"Private Queries in Location Based Services: Anonymizers areNot Necessary," Proc. ACM SIGMOD Int'l Conf. Management ofData, 2008.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[5] R. Anderson and T. Moore, "Information Security Economics—and Beyond," Proc. 27th Ann. Int'l Cryptology Conf. Advances inCryptology, 2007.

[6] R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux, "A Distortion-Based Metric for Location Privacy," Proc. Eighth ACM Workshopon Privacy in the Electronic Society (WPES '09), pp. 21-30, 2009.

[7] M. Piorkowski, N. Sarafijanovic-Djukic, and M. Grossglauser, "AParsimonious Model of Mobile Partitioned Networks withClustering," Proc. First Int'l Conf. Comm. Systems and Networks,2009.

[8] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P.Hubaux, "Quantifying Location Privacy," Proc. IEEE Symp. Securityand Privacy, 2011.

[9] J. Krumm, "A Survey of Computational Location Privacy," PersonalUbiquitous Computing, vol. 13, no. 6, pp. 391-399, 2009.

[10] R. Shokri, J. Freudiger, and J.-P. Hubaux, "A Unified Frameworkfor Location Privacy," Proc. Ninth Int'l Symp. Privacy EnhancingTechnologies (HotPETs), 2010.

[11] R. Shokri, P. Papadimitratos, G. Theodorakopoulos, and J.-P.Hubaux, "Collaborative Location Privacy," Proc. IEEE Eighth Int'lConf. Mobile Ad-Hoc and Sensor Systems, Oct. 2011.

[12] R. Shokri, P. Papadimitratos, and J.-P. Hubaux, "Mobicrowd: ACollaborative Location Privacy Preserving LBS Mobile Proxy(Demonstration)," Proc. Eighth ACM Int'l Conf. Mobile Systems,Applications, and Services (MobiSys), 2010.

[13] "NIC": Nokia Instant Community," http://conversations.nokia.com/2010/05/25/nokia-instant-community-gets-you-social/.

[14] "Wi-Fi Direct," http://www.wi-fi.org/wi-fi_direct.php, 2013.

[15] R.K. Ganti, N. Pham, H. Ahmadi, S. Nangia, and T.F. Abdelzaher,"GreenGPS: A Participatory Sensing Fuel-Efficient MapsApplication," Proc. ACM Eighth Int'l Conf. Mobile Systems, Applications,and Services (MobiSys '10), 2010.

[16] Y. Liu, A. Rahmati, Y. Huang, H. Jang, L. Zhong, Y. Zhang, and S.Zhang, "xShare: Supporting Impromptu Sharing of MobilePhones," Proc. Seventh Int'l Conf. Mobile Systems, Applications, andServices, 2009.

[17] J. Freudiger, R. Shokri, and J.-P. Hubaux, "Evaluating the PrivacyRisk of Location-Based Services," Proc. Fifth Int'l Conf. FinancialCryptography and Data Security (FC '11), pp. 31-46, 2012.

[18] M. Srivatsa and M. Hicks, "Deanonymizing Mobility Traces:Using Social Network as a Side-Channel," Proc. ACM Conf. Computerand Comm. Security, pp. 628-637, 2012.

[19] N. Vratonjic, K. Huguenin, V. Bindschaedler, and J.-P. Hubaux,"How Others Compromise Your Location Privacy: The Case ofShared Public IPs at Hotspots," Proc. 13th Privacy Enhancing TechnologiesSymp. (PETS), 2013.

[20] B. Hoh and M. Gruteser, "Protecting Location Privacy throughPath Confusion," Proc. First Int'l Conf. Security and Privacy for

Author's:

B.Ravindra Naik is a student of Sree Rama Institute of Technology & Science, Kuppenakuntla,Penuballi, Khammam, TS,India.Presently he is Pursuing his M.Tech (CSE) from this collegeHis area of interests includes Information Security, Cloud Computing, Data Communication & Networks.

Mr. N.Naveen is an efficient teacher, received M.Tech from JNTU Hyderabad is working as an Assistant Professor in Department of C.S.E, Sree Rama Institute of Technology & Science, Kuppenakuntla, Penuballi, Khammam, AP,India. He has published many papers in both National & International Journals. His area of Interest includes Data Communications & Networks, Database Management Systems, Computer Organization, C Programming and other advances in Computer Applications.