International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Achieving Location Privacy through the Impact of Changing Pseudonyms

S. Sharath Chandra[1], Dasu Vaman Ravi Prasad[2]

[1]M.Tech Student, Dept of CSE, Anurag Group of Institutions (Formerly CVSR College of Engineering), Hyderabad, T.S, India
[2]Associate Professor, Dept of CSE, Anurag Group of Institutions, (Formerly CVSR College of Engineering), Hyderabad, T.S, India

Abstract: ***In mobile networks, authentication is a required primitive for most security protocols. Unfortunately, a competitor can monitor pseudonyms used for authentication to track the location of mobile nodes. A regularly proposed solution to protect location privacy suggests that mobile nodes collectively change their pseudonyms in regions called mix zones. This approach is very expensive. Self-interested mobile nodes might thus decide not to cooperate and jeopardize the achievable location privacy. In this paper, we examine non-cooperative behaviour of mobile nodes, where each node aims at increasing its location privacy at a least cost. As in practice mobile nodes do not know their rivals' payoffs, we then consider static incomplete information. By means of numerical outcomes, we then predict the behaviour of selfish mobile nodes.***

Keywords: Security and privacy protection, pseudonym, mobile computing, network protocols, mix zones.

1. Introduction

The growing popularity of Bluetooth and WiFi in ad hoc mode [3], and other similar techniques is likely to fuel the adoption of peer-to-peer wireless communications. Corporations are developing wireless peer-to-peer technologies such as Nokia Instant Community [4] and Qualcomm FlashLinQ [8]. In addition to classic infrastructure based communications, mobile devices communicate directly with each other in an ad hoc wireless fashion. Such communications dramat1ically increase mobile devices' awareness of their environment, enabling a new breed of context-aware applications. The integration of peer-to-peer wireless communications into mobile devices brings new security challenges, due to their mobile and ad hoc nature. Wireless communications are inherently dependent on geographic proximity: mobile devices detect each other's presence by periodically broadcasting beacon messages. These messages include pseudonyms such as public keys in order to identify communicating parties, route communications and secure communications. Much to the detriment of privacy, outer parties can monitor pseudonyms in broadcasted messages in order to track the locations of mobile devices.

A change of pseudonym by an isolated device in a wireless network can be trivially identified by an external party noticing transmitted messages. Hence, a change of pseudonym should be spatially coordinated among mobile devices, i.e., a collective effort. One solution consists in changing pseudonyms periodically, at a predetermined frequency. This works if at least two mobile nodes change their pseudonyms in proximity, a rarely met condition. Base stations can be used as coordinators to synchronize pseudonym changes, but this solution needs help from the infrastructure. This approach enables mobile nodes to change their pseudonyms at specific time instances. However, this solution achieves location privacy only with respect to the infrastructure. Another approach [1] coordinates pseudonym changes by forcing mobile nodes to change their pseudonyms within predetermined regions called mix zones. This approach lacks flexibility and is liable to attacks because a central authority fixes mix zone locations and must share them with mobile nodes.

2. Preliminaries

System Model

A network where mobile nodes are autonomous entities equipped with Wi-Fi or Bluetooth enabled devices that communicate with each other upon coming in radio range. In other words, consider a mobile wireless system such as a vehicular network [10] or a network of directly communicating hand-held devices. Without loss of generality, assume that each user in the system has a single mobile device and thus corresponds to a single node in the network.

Now assume that mobile nodes automatically exchange information (unbeknownst to their users) as soon as they are in communication range of each other. Note that the evaluation is independent of the communication protocol. Without loss of generality, assume that mobile nodes advertise their presence by periodically broadcasting proximity beacons containing the node's identifying/ authenticating information (i.e., the sender attaches its pseudonym to its messages). Due to the broadcast nature of wireless communications, beacons enable mobile nodes to discover their neighbors. For example, when a node s receives an authenticated beacon, it controls the permissibility of the sender by checking the certificate of the public key of the sender. After that, s verifies the signature of the beacon message.

Threat Model

An adversary À aims at tracking the location of some mobile nodes. In practice, the rivals can be a rogue individual, a set of malicious mobile nodes even deploy its own infrastructure (e.g., by placing eavesdropping devices in the considered area). Let's consider that the adversary is passive and simply eavesdrops on communications. In the worst case, À obtains complete coverage and tracks mobile nodes throughout the entire area. And characterize the latter type of adversary as global.

À collects identifying information (e.g., the MAC address or the public keys used to sign messages) from the entire network and obtains location traces that allow him to track the location of mobile nodes. Hence, the problem occurred here consists in protecting the location privacy of mobile nodes, that is, to prevent other parties from learning a node's past and current location. It must be noted that, at the physical layer, the wireless transceiver contains a wireless fingerprint that the adversary could use to identify it. However, this requires a costly installation for the adversary and stringent conditions on the wireless medium, it remains unsure how much identifying information can be extracted in practice from the physical layer and do not consider this threat.

Mix Zone Model

This mix zone model assumes the existence of a trusted middleware system, positioned between the underlying location system(s) and un-trusted third party applications. Applications register interest in a geographic space with the middleware, Assume this space as an application zone. Example spaces include hospital grounds, university buildings or a super-market complex. Users register interest in a particular set of location-aware applications and the middleware limits the location information received by applications to location sightings of registered users located inside the application zone.

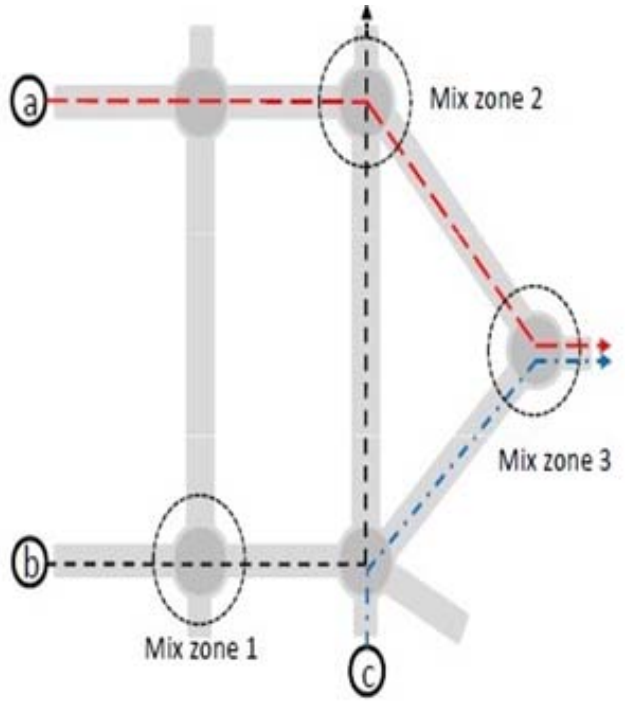

Figure 1: Example of System Mode. Nodes move on plane (x, y) according to trajectories defined by flows a, b and c. To achieve privacy, nodes change pseudonyms in mix zones.

Each user has one or more unregistered geographical regions where no application can trace user movements, these areas are called as mix zones, because once a user enters such a zone, user identity is mixed with all other users in the mix zone, as will become clearer shortly. The pseudonym allows communication between user and application such communication must pass through a trusted intermediary to prevent trivial linking of a pseudonym with an underlying user identity. The pseudonym of any user changes whenever the user enters a mix zone. The aim of the mix zone model [2] is to prevent tracking of long-term user movements, but still permit the operation of many short-term location aware applications.

Consider the example in Fig. 1: Mix zone 3 has three entry/exit points that are all traversed by flows. Based on the flows traversing a mix zone, it is possible to evaluate the different trajectories of mobile nodes in each mix zone.

User-Centric Location Privacy

We access the location privacy provided by multiple pseudonyms and propose a user centric model of location privacy to capture achievable, potential location privacy over time.

Location Privacy

There are several techniques to diminish the tracking of mobile nodes. We consider the advantage of multiple pseudonyms over time, the mobile nodes change the pseudonym to sign messages, to reduce their long term link ability. To avoid spatial interrelationship of their location, mobile nodes in proximity correlate pseudonym changes in regions known as mix zones. We assume that as soon as a node changes the pseudonym, the old pseudonym expires and is detached from the node's memory. In other words, two nodes cannot share the same pseudonyms over the same time.

Mix zones can also hide the trajectory of mobile nodes to protect against the spatial interrelation of location traces, e.g., by using (i) silent/encrypted mix zones (ii) regions where the adversary has no coverage. Without loss of generality, we consider silent mix zones: mobile nodes turn off their transceivers and stop sending messages for a limited period of time. If at least couple of nodes changes their pseudonyms in a silent mix zone, a mixing of their absolute position occurs and the mix zone becomes a confusion point for the adversary.

User Centric Model

This entropy measures the location privacy achieved in certain mix zones at some point in time. However, location privacy requires to individuals vary depending on time and location. It is thus required to protect location privacy in a user centric manner, so that each user can decide when and where to protect its location privacy. We consider a user centric model of the location privacy, where each mobile node monitors its location privacy over time locally [5], [7], [9]. A network-wide metric could access the network but might ignore that some nodes have a low location privacy level and are traceable for long distances.

As a user centric approach captures the evolution of location privacy of users over time, then the mobile nodes can evaluate the distance over which they are potentially tracked by an adversary and can act upon it by deciding whether and when to change its pseudonym. By a user-centric model, mobile nodes can request a pseudonym change from other nodes in proximity if their local location privacy level is lower than a desired level.

3. Conclusion

We have considered the problem of sensibility in location privacy schemes based on pseudonym changes. We introduced a user-centric model of location privacy to estimate the evolution of location privacy over time an evaluated the strategic behavior of mobile nodes with a game pseudonym change model. We analyzed the scenario with complete and incomplete information and derived the equilibrium strategies for each node for both static and dynamic pseudonyms. The obtained equilibria allow us to predict the strategy of mobile nodes seeking to achieve location privacy in a non-cooperative environment. This analysis results in the design of pseudonym changes that coordinate to protecting location privacy.

In future work, game theoretical models may be considered to include other strategic aspects, such as the evolution of user strategies across various games. It would also be interesting to consider how obtaining the distribution in a distributed and noisy fashion may affect results.

References

[1] J. Freudiger, R. Shokri, and J.-P. Hubaux, "On the Optimal Placement of Mix Zones," Proc. Ninth Int'l Symp. Privacy Enhancing Technologies (PETS), 2009.
[2] "TIGER Maps," http://www.census.gov/geo/www/tiger, 2012.
[3] "WiFi Alliance,"Wi-Fi CERTIFIED Wi-Fi Direct: Personal, Portable Wi-Fi that Goes with You Anywhere, Any Time, http://www.wi-fi.org/Wi-Fi_Direct.php, 2010.
[4] Official Nokia Blog, "Nokia Instant Community Gets You Social," http://conversations.nokia.com/2010/05/25/nokia-instantcommunity-gets-you-social, 2010.
[5] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.-C. Herrera, A.M. Bayen, M. Annavaram, and Q. Jacobson, "Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring," Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), pp. 15-28, 2008.
[6] L. Buttyan, T. Holczer, and I. Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs," Proc. Fourth European Conf. Security and Privacy in Ad-Hoc and Sensor Networks (ESAS), 2007.
[7] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Preserving Privacy in GPS Traces via Path Cloaking," Proc. 14th ACM Conf. Computer and Comm. Security (CCS), 2007.
[8] X. Wu, S. Tavildar, S. Shakkottai, T. Richardson, J. Li, R. Laroia, and A. Jovicic, "FlashLinQ: A Synchronous Distributed Scheduler for Peer-to-Peer Ad Hoc Networks," Proc. 48th Ann. Allerton Conf. Comm., Control, and Computing, pp. 514-521, 2010.
[9] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy," Proc. Fifth ACM Workshop Privacy in Electronic Soc. (WPES), 2006.
[10] H. Hartenstein and K. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc Networks," IEEE Comm. Magazine, vol. 46, no. 6, pp. 164-171, June 2008.

Author Profile

Sammeta Sharath Chandra received the B.Tech degree in Information Technology from JNTU Hyderabad in 2011 and pursuing M.Tech degree in Computer science and Engineering from JNTU Hyderabad.

Dasu Vaman Ravi Prasad working as associate professor in Computer Science Engineering from CVSR College of Engineering from Anurag Group of Institutions Venkatapur (V), Ghatkesar (M), Ranga Reddy District, Hyderabad-500088, Telangana State.