Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1002 – 1006

RESEARCH ARTICLE

AN APPROACH TO SECURE LOCATION OF USER IN PERVASIVE COMPUTING ENVIRONMENT

SUDHEER KUMAR SINGH, SHANSHANK SINGH, NITIN GOEL, RAHUL RANJAN

sudheer@iul.ac.in, shashank@iul.ac.in, ngoel@iul.ac.in, rahul@iul.ac.in

Assistant Professor, Department of Computer Science and Engineering, Integral University, Lucknow

Abstract- Location privacy is a particular type of information privacy that can be defined as the ability to prevent others from learning one's current or past location. In general security in every area counted so security issues related to location based services are mandatory without it our application devices are not perfectly reliable . We are proposing a new technique that uses user anonymity and dummy locations for location privacy while using location aware application server. User communicates with the server through a trusted proxy server. It sends dummy locations to the application server with its original position. The user uses temporary pseudonyms that are changed frequently according to some algorithm. Whenever pseudonyms are changed by a user, dummy locations are chosen in a tricky fashion. By the mathematical formula of path and number of dummies that makes the task of tracing the user very difficult. Security of user location will be hence increased.

Keywords- Location privacy, pseudonym, de-anonymize, dummy-Locations, location anonymity, trusted proxy

I. INTRODUCTION

The Indian Constitution of 1950 does not expressly recognize the right to privacy. However, the Supreme Court first recognized it in 1964 that there is a right of privacy implicit in the Constitution under Article 21 of the Constitution, which states, "No person shall be deprived of his life or personal liberty except according to procedure established by law." The 1948 Universal Declaration of Human Rights [1] declares that everyone has a right to privacy at home, with family, and in

correspondence. The field of anonymous communication originated with Chaums mix networks [2] and the dining cryptographer algorithm [3]. In [2], he proposed an untraceable communication system called the mix that used a mail system, digital signatures. In [3], he also proposed intractability between sender and recipient and the origin of Anonymity Set. A prominent work on location privacy is Mix Zones [1], which is similar to mix networks. In Mix Zones, infrastructure provides an anonymous service using pseudonyms that collects and reorders messages from users within a mix zone to confuse observers. There must be enough users in the mix zone for effective location privacy. Gruteser and Grunwald proposed another mechanism called spatial and temporal cloaking [4] that conceals a user within a group of k people, called k-anonymous, which originated from k-anonymity [5]. To achieve k-anonymous, spatial or temporal accuracy of location information is reduced. But when there are few people in a small area, the accuracy of location information is too low to use for location based services.

This paper concentrates on location privacy. Location privacy is a type of information privacy that can be defined as the ability to prevent others from learning one's current or past locations [1]. Location privacy is more important in pervasive computing environment. That implicitly implies that the communication device is mobile and wireless. User might not care if someone finds out where she was yesterday at 10:30 a.m., but if this someone could inspect the history of all her movements, recorded every second with great accuracy, might prove dangerous.

There are two main difficulties .First, the state for a given user (common to all that user's pseudonyms) must be stored elsewhere and then supplied to the application in a random fashion .Second, the application must not be able to determine that two sets of preferences map to the same user, so this approach might have to add small, random variations. However, insignificant variations might be recognizable to a aggressive observer, whereas significant ones could negatively affect semantics and therefore functionality. There are many different approaches for achieving location privacy in a location-based application system. First one is to remove the need for authentication. Second approach is to develop some mechanism for anonymity. Users can achieve Location privacy using pseudonyms and a trusted proxy. Location privacy becomes more robust using temporary pseudonyms and a trusted proxy. We can improve over that by using location anonymity. In this method there is a scope of direct communication with the application without revealing our actual location. This new technique that uses user anonymity and dummy locations for location privacy while using location aware application server, User communicates with the server through a trusted proxy server. It sends dummy locations to the application server with its original position. The user uses temporary pseudonyms that are changed frequently according to dummy generation algorithm, whenever pseudonyms are changed by a trusted proxy, which makes the task of tracing the user very difficult.

II. LOCATION DEPENDENT (AWARE) APPLICATIONS

To protect the privacy of our location information while taking advantage of location-aware services, we wish to hide our true identity from the applications receiving our location; at a very high level, this can be taken as a statement of our security policy. Now we try to develop a more sophisticated system for location-based service (Fig1) [1]. Here the user accesses the application server through a trusted proxy server. The user is authorized to use the service by this trusted proxy. The proxy and the user decide a pseudonym for the user. User sends the location and the requested service to proxy. The trusted proxy sends location and the request to the application server with user's pseudonym. Response from the application server reaches the user through proxy. There are many users requesting the service through proxy. Proxy has to maintain a table for the user ID and the

corresponding pseudonym redirect the response from the application to appropriate user. Here the application is aware of the location and the request from the user but doesn't know her identity. Pseudonyms are changed frequently. So indirectly location privacy is gained.

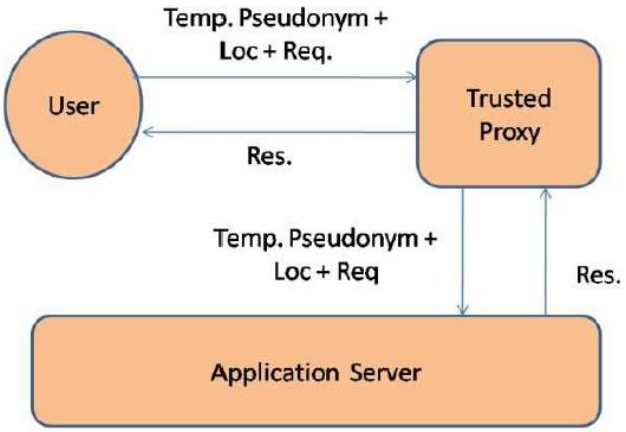

Fig1. Location privacy using Temporary pseudonyms and a trusted proxy.

III. AN IMPROVEMENT USING DUMMYLOCATIONS (DL)

Problem with previously discussed solution is that, if the system's spatial and temporal resolutions were sufficiently high, could easily link the old and new pseudonyms, defeating the purpose of the change.

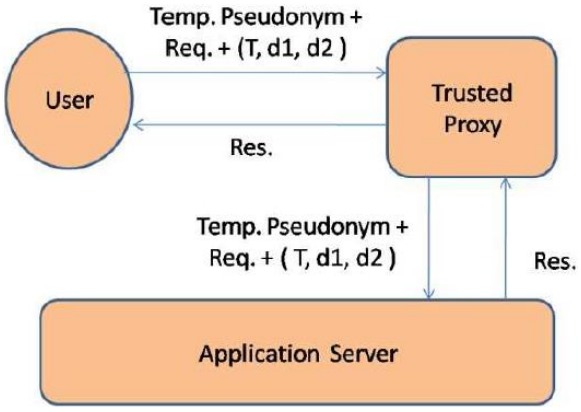

Fig2. An improvement over location privacy using pseudonyms, a trusted proxy and Dummy-Locations

In a new approach we can develop a system for location-based service that uses pseudonyms (Fig2). Here too the user accesses the application server through a trusted proxy server. The proxy provides a pseudonym to the user after authenticating it. The user gets the ID from the proxy server administrator on request. User communicates with the application through the proxy server (Fig2). The users change pseudonyms frequently, even while they are being tracked: users adopt a series of new, unused pseudonyms for each application with which they interact [1]. Proxy has to maintain a table for the pseudonym and the

corresponding user ID so that it can redirect the response from the application to appropriate user. Here too the application is aware of the location and the request from the user but doesn't know her identity.

Now one more factor is added to make the system more secure. This can be called location anonymity approach (Fig2) [6]. Here the user sends a few dummy locations with its actual location to the application and requests some service. The application server responds with solutions (services) for all locations. The user probability of loss of privacy will decrease chooses the solution for actual location. Hence, Fig6 shows how dummy locations are chosen for multiple locations requests (queries). AL is the actual location. L1 and L2 are chosen to make the application wonder that which one is the correct location of the user. There can be different ways of choosing the dummy locations (DL).

Form the above discussion it is clear that If there are K dummies and K users change their pseudonym concurrently using this trick to initialize dummies, the probability becomes 1/K. If in time T, users change their pseudonyms N times then there are K^N different paths possible for every user in time T. For time 2T, possible paths are K^{2N}. Now even if one has additional information, Adversary is not able to break into the privacy of user. Value of K can be chosen taking in account the present computational speeds of machines (the attacker, the proxy server and the application server) for obvious reasons.

A new improved model proposed for location-based services to protect location privacy using dummies. The client creates dummy position data that is sent to the application server with its original position. There is a proxy server in between that anonymizes, the user by providing it a pseudonym for communication with the application server. Pseudonyms are changed frequently. If there are K dummies and K users change their pseudonym concurrently and in time T, users change their pseudonyms N times then there are K^N different paths possible for every user. This makes this method a good contender for being used in pervasive computing environment.

As discussed and implement our proposed technique this is clear in Figure 5.1 which show that when the number of dummies increases, location anonymity also increases. We set the number of dummies between 0 and 11, and a unit of F was the percentage of the entire area whose scale is about 15 x 15 Km and the number of regions was 8x8, 10x10, 12x12 or 15x15.

Figure 5.1 shows that for location anonymity, a setting in which one dummy is generated in 8x8 regions is higher than another setting in which a dummy is not generated in 12x I2 regions. Moreover, as expected, the more dummies, the larger the value of F.As shown in Figure 5.1, if a user achieves 65% of F, we conclude that the user needs three dummies in 12x12 regions.

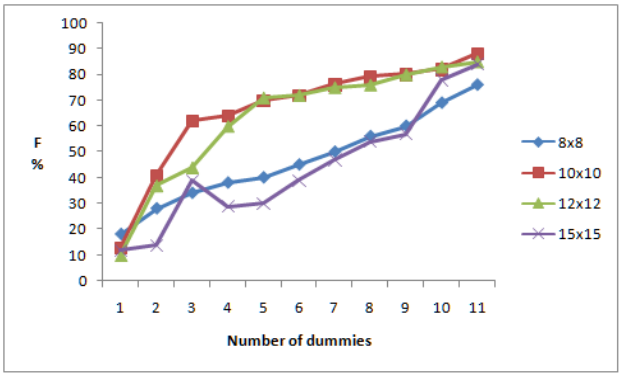

Figure 5.1 comparisons between number of dummies and ubiquity F.

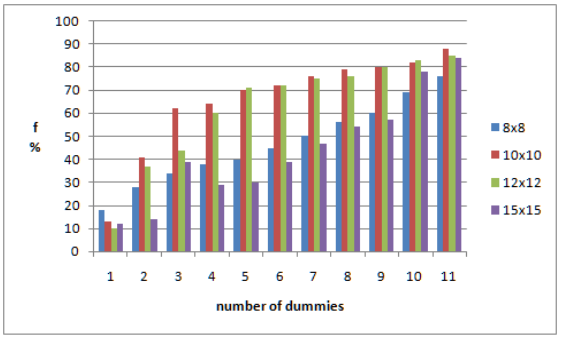

Figure 5.2 comparisons between number of dummies and ubiquity F.

IV. CONCLUSION

In this paper, we proposed a new technique for location-based services to protect location privacy using dummies. The client creates dummy position data that is sent to the application server with its original position. There is a proxy server in between that anonymizes the user by providing it a pseudonym for communication with the application server. Pseudonyms are changed frequently. If there are K dummies and K users change their pseudonym concurrently and in time T, users change their pseudonyms N times then there are K^N different paths possible for every user. This makes this method a good contender for being used in pervasive computing environment.

In future we will try to find out its actual effectiveness by simulating it in real-like scenario. Also we need to find out how should the dummies move (what imaginary path should dummies take) so they can't be distinguished from real users.

REFERENCES

[1] Alastair R. Beresford and Frank Stajano, "Location Privacy in Pervasive Computing", IEEE Pervasive computing, January–March 2003, pp. 46-55.
[2] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications ofrhe ACM, 4(2), February 1981.
[3] D. Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability, Journal of Cryproiagy, 1:65-75, 1988.
[4] M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In Proceedings of the First Inremafional Conference on Mobile Systems, Applications, and Services, pages 3 1-42, 2003.
[5] P. Samarati and L. Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical report, 1998.
[6] Tun-Hao You, Wen-Chih Peng, Wang-Chien Lee, "Protecting Moving Trajectories with Dummies", 2007 www.cs.nctu.edu.tw.

