International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-3 Issue-5 September-2012

Location Privacy Using User Anonymity and Dummy Locations

Prince Kumar Sahu[1], Saroj Kumar Chandra[2]
Department of Computer Science & Engineering, Chouksey Engineering College, Bilaspur

Abstract

This paper concentrates on location privacy, a particular type of information privacy that can be defined as the ability to prevent others from learning one's current or past location. Here 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. That makes the task of tracing the user very difficult.

Keywords

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

1. 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.

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.

2. 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.

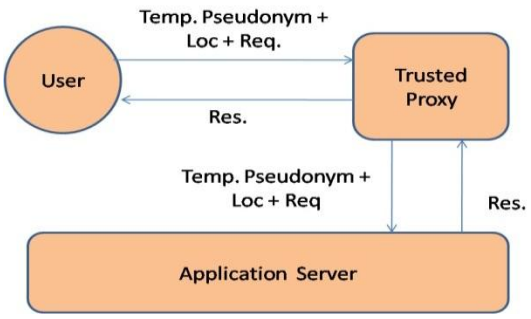

Fig1. Location privacy using Temporary pseudonyms and a trusted proxy.

3. An Improvement using Dummy-Locations

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

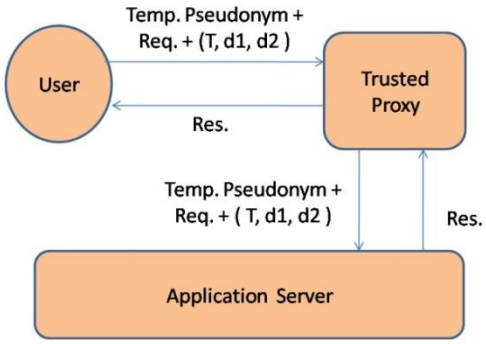

Fig2. An improvement over location privacy using pseudonyms, a trusted proxy and Dummy-Locations

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).

Now we will discuss the proposed method in detail. For illustration we take 5X8 grid area.

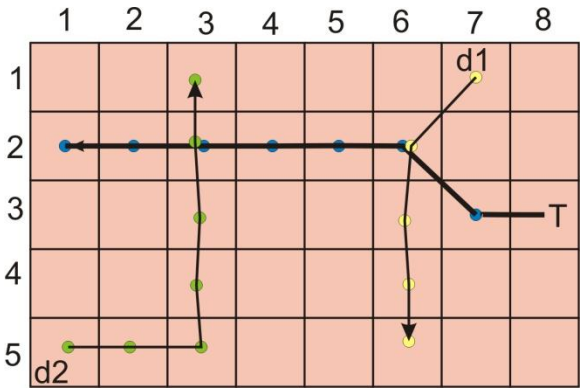

Fig3. Path followed by a user and its dummies.

Fig3 shows the user T and its dummies i.e. d1, d2. T starts from (3, 8) goes to (2, 1). Dummy d1 starts at (1, 7) and reaches (5, 6). Dummy d2 starts at (5, 1) and its destination in (1, 3). The user and dummies are guided by application server. When original user moves one block the dummy also moves one block. They continuously send their location to the server through trusted proxy. Users have temporary pseudonyms. They change their pseudonyms according to some algorithm while moving. The application server is in no position to identify them. But it is easy to identify relationship between temp pseudonyms of same user. So complete path followed by a user can be found. Any additional information from some other source can be used to identify the actual user. If user identity is found location privacy is lost. So we have to devise some other method for maintaining location privacy of the user.

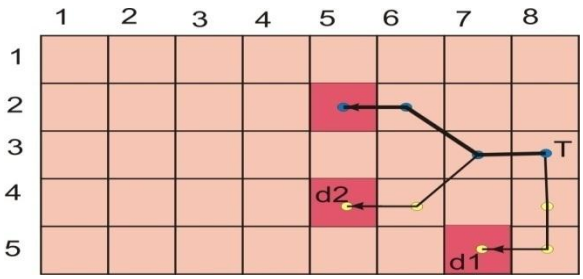

Fig4. Path followed by T and its dummies till the change of pseudonym.

Now, suppose T, T_x, T_y are three users accessing application server through trusted proxy.

Fig4 shows a user T. The bold line shows the original path followed by the user. Dummies d1 and d2 follow path shown by thin lines. The red squares show the positions when the user changes pseudonym.

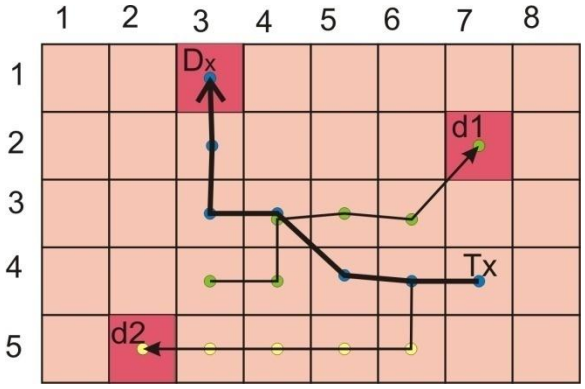

Fig5. Path followed by T_x and its dummies till the change of pseudonym.

Fig5 shows a user T_x. The bold line shows the original path followed by the user. Dummies d1 and d2 follow path shown by thin lines. The red squares show the positions when the user changes pseudonym.

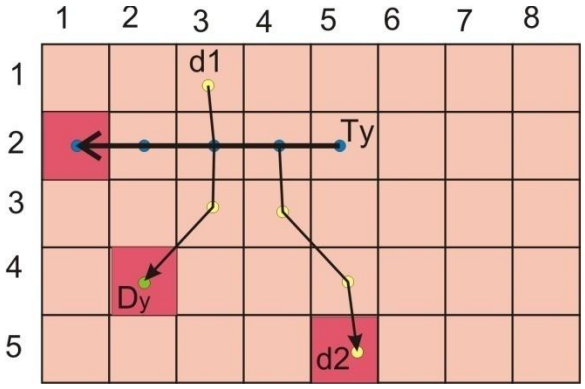

Fig6. Path followed by T_y and its dummies till the change of pseudonym.

Fig6 shows a user T_y. The bold line shows the original path followed by the user. Dummies d1 and d2 follow path shown by thin lines. The red squares show the positions when the user changes pseudonym. Important: T, T_x, T_y change their pseudonyms at the same time.

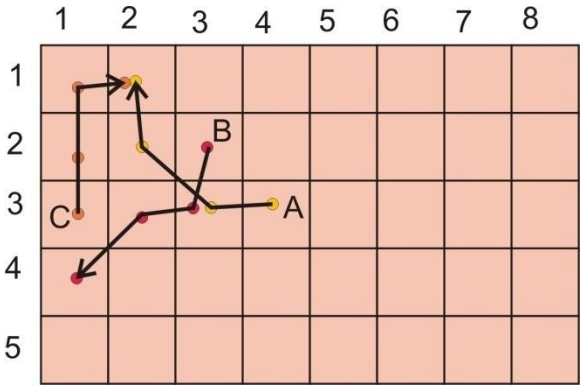

Fig7. Path followed by some user and its dummies after change of pseudonym.

Fig7 shows the path followed by some user (T or T_x or T_y) and its two dummies. It is very difficult to guess who among the three this user is. Why? It will become clear after seeing next fig6.

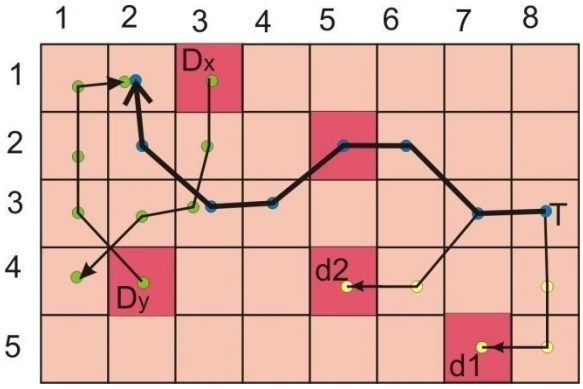

Fig8. Complete path followed by T and its dummies before and after change of pseudonym.

Fig8 completes fig5. A in fig5 is same user that is T. B and C are dummies. In fig2 we can see that T changes pseudonym when it leaves block (2, 5) and moves to (3, 4). In fig3 we can see that T_x changes pseudonym when it leaves block (1, 3). In fig2 we can see that T_y's dummy changes pseudonym when it leaves block (4, 2). Now when T appears with new pseudonym the proxy server initializes its dummies i.e. D_x (or B), D_y (or C) in a tricky fashion. D_x is chosen one move away from block (1, 3) where T_x changes pseudonym. D_y is chosen one move away from block (4, 1) where d1 (one of the dummy) of T changes pseudonym. So T appears as A with dummies B, C. What happens next is shown by fig5. So, we can relate it to all three users i.e. T, T_x, T_y. Probability of finding that A is T equals to 1/3. 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, she 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.

4. Related Work

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.

5. 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.

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: Uncondi- tional 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 cloak- ing. In Proceedings of the First International 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.

Prince Kumar Sahu,Received his B.E.(I.T.) Degree from Guru Ghasidas University Bilaspur(C.G),India,in 2006, and M.Tech(C.S.E) Degree from Punjab Engineering College in 2009.Currently working as Assistant professor in Chouksey Engineering College Bilaspur (C.G.) in the Department of Computer Science & Engineering.

Saroj Kumar Chandra ,Received his B.E.(I.T.) Degree from Guru Ghasidas University Bilaspur(C.G),India,in 2007, and M.Tech(C.S.E) Degree from National Institute Of technology Durgapur(W.B),India in 2010. Currently working as Assistant professor in Chouksey Engineering College Bilaspur (C.G.) in the Department of Computer Science & Engineering.