International Journal of Security and Its Applications
Vol. 9, No. 4 (2015), pp. 25-32
http://dx.doi.org/10.14257/ijsia.2015.9.4.04

Perceived K-value Location Privacy Protection Method Based on LBS in Augmented Reality

Yang Yang

Department of Information Technology, Nanjing Radio and TV University, Nanjing City Vocational College, Nanjing, Jiangsu 210002, China
Email:nj.yangyang@163.com

Abstract

In Augmented Reality (AR), users' main concern includes privacy and safety of data. Since location based services(LBS) are one of the major applications of the AR, it is important to have a privacy-aware management of location information, providing location privacy for clients against vulnerabilities or abuse. Here we analyzed the merit and demerit of exiting location privacy protection method. Then a perceived K-value location privacy protection method was raised. Hereafter the protocol of this algorithm was described and simulated in detail. The results demonstrated this method can effectively realize the location privacy protection.

Keywords*: Location Based Services(LBS); location privacy; k-anonymity method; pseudonym method*

1. Introduction

The term AR was coined in 1990 by Thomas Caudell, an employee of Boeing [1]. The technology which allows adding images and information generated by a computer to the normally perceived reality is called the Augmented Reality (AR) [1].

AR has evolved through different stages from many years and now it is becoming one of the commonly used technologies. One of the commonly accepted definitions of AR today is given by Ronald Azuma [2]. Azuma's definition says that Augmented Reality:

combines real and virtual
is interactive in real time
is registered in 3D

With the development of sensors and wireless devices, it is possible to access to personal accurate position in anytime and anywhere, so Location Based Services (LBS) is a new class of applications. Location based services are essentially the service which is related the location of the user making the request [3]. Location based services are one of the common services provided by AR. LBS normally consists of mobile devices, location system, network and service provider (LBS server). User sends queries to LBS server through mobile device, such as mobile phone. Then the location system, GPS, acquires the location of queries. Hereafter, LBS server returns the feedback to user through network, such as 3G net.

Location Determination Technology (LDT), such as Cell-ID, A-GPS, EOTD, etc., [4] gives the location information which consists of the X-Y co-ordinates. There are many categories of services LBS can provide. They are Emergency and Safety, Communities and Entertainment, Information and Navigation, Tracking and Monitoring, and M-Commerce etc. In 2003, CSTB (Computer Science and Telecommunications Board) in the "IT Roadmap to a Geospatial Future" pointed that LBS would be a very important part of future computing environment and infiltrated into all aspects of the future life. Market research firm ABI Research forecasts, the global number of people to enjoy location-based services from 1.2 million in 2006 increases to 31.5 million in 2011.

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2015 SERSC

A technology boom is happening in the case of AR and LBS are one of the most widely used services of AR. But it presents users widely known serious privacy threats. These important threats are the leak of service content and position privacy. Service content threat is the potential exposure of service uses. Just like regular Internet access, a user may not want to be identified as the subscriber of some LBS, especially when the service is sensitive. The leak of location privacy is user's location disclosed in her service request. It may reveal sensitive private information such as health conditions, lifestyles and so on. Leak of location privacy restricts the use of LBS, which has also become the bottleneck of the development of LBS and AR technology.

2. Way of Location Privacy Leak

Location privacy threaten refers to, under unauthorized circumstance, attacker tracks the original position information through location device and technology, infers the privacy information related to user location through reasoning. There are three ways for location privacy leak.

If they know that a particular user 'U' is living in a particular place P and if they observe that all the requests coming from P have the same user id, then they can guess that the user requesting the service is 'U'. So from these they can track the user by simple Connect the dots approach [5]. This type of attack is called Restricted Space Identification [6]. For example, if user sent a message in some room of some hotel, the exact location coordinate information (x, y) in this message and related exterior knowledge can be used to trace the user in this room. Then attacker can infer what other service request has been sent by this user.

The second attack is one which reveals the user's identity using location-identity received with a service request message. If an LBS provider gets a report that a user 'U' is going to visit a place during a period of time and if it observes that all the request coming from that place during this period of time are sent by a single user. Then they can infer that the user requesting for the service is 'U'. This kind of attack is called Observation Identification [6].For example, if user leaked out its location information and identification in the previous message and still sent messages in same position, attacker can infer and identify the source of subsequent message through the location information in previous message, whether these latter messages are anonymous or not.

If the attacker can define the property value of some individual in quasi-identifier through known data set (published data and data obtained from other way), the sensitive property value of this individual and its location can be deduced, which induces the location information leakage. This situation is named as linking attack [7,8]. For example, property set (birth date, sex, residential address and zip code) can make up a quasi-identifier. It has been demonstrated that about 87% U.S. inhabitant can be uniquely identified through this quasi-identifier [8].

3. Related Works

In order to solve the problem of location privacy leakage, privacy protection is also required. Many researchers try to find the balance point between the service quality and privacy protection, which means the best service with least location privacy exposure.

Now we have already made a number of privacy protection methods. Location privacy protection is the method that sends the false location information or anonymous identity and location information to the server in the location service. These methods can be divided into two categories: one is to protect the user's ID information (conceal anonymity or pseudonym), making the server service does not know the requestor true ID; the other is to protect the location information of the user by submitting a region instead of true location of the user.

 Copyright ⓒ 2015 SERSC

Existing methods, such as pseudo-location method, pseudonym method, k-anonymity method and other methods based on it, such as personalized k-anonymity, have some defects which will reveal the location privacy [9-15].

Perceived K-value location privacy protection method in this paper makes improvement as compared with the methods mentioned above. It combines the advantage of pseudonym method and k-anonymity method and suggests a location privacy protection method based on perceived K-value to realize the protection.

4. Comparison of the Existing Location Privacy Protection Method

There are many location privacy protection methods based on the location service at present. Here their merit and demerit are analyzed.

4.1 Pseudo-location Method

Pseudo-location method [9] can realize the confusion effect. There are two situations for pseudo-location method to realize the location privacy protection [16,17]. The first one is that user forms some pseudo-location by himself and sends it with his real location to the LBS provider when user put forward the service request. So the attacker can not discriminate the pseudo and real location, which protects the user's location privacy. The other situation is that user only sends one specified pseudo-location when putting forward the service request. Then the server increases the resent adjacent inquiry according to this pseudo-location and sends the results to the client. So user can retrieve the requisite answer according to the results. Because attacker doesn't acquire the real location of user, the location privacy of user can still be protected. But the defect of this method is obvious. In this method, it is hypothesized that user only act in some restricted space. And the level of privacy protection in this method is not fixed, which is proportional to the distance between the pseudo and real location.

4.2 Pseudonym Method

Pseudonym method [10] changes the real ID to a pseudo-ID and then sends the service request to the anonymous server. Every user can realize the concealment of the real ID through the pseudo-ID. Even attacker obtain the accuracy position information from the server, the exact interconnection between user's position information and real ID information still can't be established, which realizes the location privacy protection. But the shortage of this method still exists. All information of user's request and corresponding IP address will be stored in the server, which will lead to the location privacy leak.

4.3 k-anonymity Method

K-anonymity method [18,19,20] was firstly proposed by Gruteser and Grunwald. Before sending to the LBS provider, user deletes the personal information and publishes hypo-accurate data, which induces that every record has identical quasi-identifier value with other k-1 record in the data list to realize the location privacy protection. But the restriction of this method is that there is no protection mechanism for leak of sensitive attribute data, and there is no any constraint for sensitive attribute data in this method. It is easy for attacker to infer the individual corresponding sensitive attribute data and identify the relationship between data and individual through the background information, which leads to the location privacy leak.

4.4 Other Methods based on the k-anonymity Method

Other methods have been proposed according to the defect of k-anonymity method. L-diversity model was proposed by A.Machanavajjhala [11]. But this model is only

Copyright ⓒ 2015 SERSC

suitable for handling classification sensitive attribute data instead of numerical sensitive attribute data. P-sensitive k-anonymity model may lost a lot of information usability in some data set and can't resist the skewed attack and similarity attack to the sensitive attribute data [12]. (α,k)- anonymous model[13] still can't avoid the skewed attack and similarity attack with the significant loss of data during the anonymous process. (k, e)-anonymous model[14] has similar defect. T-closeness frame can fix the skewed attack and similarity attack to the sensitive attribute data. But it reduces the usability of published data.

4.5 Personalized k-anonymity Method

Personalized k-anonymity method was proposed by Gedik and Liu [15]. In this method, every user can define the desired anonymous level and adjust the least anonymous level and maximum tolerable time, spatial resolution. This method can provide different level of privacy protection to sensitive attribute data, which will decrease the data lost from the unified anonymous. But the defect of this method is undefined information and the proportion of anonymous information will decrease when the K value increase.

5. Perceived K-value Location Privacy Protection Method

There are three main models used for achieving the privacy in LBS. The first one is non-cooperative model. The second one is a peer to peer cooperative model. The last model is a centralized trust third party (TTP) model. Perceived K-value location privacy protection method is based on the centralized trusted third party model. User location anonymous, service request anonymous and feedback to the user will all be realizes by the third party, who brings a communication bridge to the user and LBS provider.

5.1 The Analysis of Location Privacy Protection Level

There are two kinds of approaches for attacker to acquire location when communication goes between user terminal and LBS. The first one is directly achieving query information from user terminal. As the user have control power on location information of himself, attacker can't directly communicate with the user and achieve his location information in un-cooperated model. The second one is achieving query information of user from LBS. On this occasion attacker can speculate user's location. With the hypothesis of p for real position of terminal, p' for location of query spot and q_i for the i^{th} query result acquired from terminal, the information received by attacker include query spot p' and orderly result set $\{q_1, q_2, q_3, ...q_m\}$ centered on the p'. Also the hypothesis is set that the known user employ incremental close neighbours query and the attacker take the q_j as expected query results of user. According incremental query ending condition, the supposed user location p may meet the equation as follows:

$$dis(p,p') + \min_{1\le m\le n-1}^{j} dis(p,q_m) > dis(p',q_{n-1}) \quad ①$$

$$dis(p,p') + \min_{1\le m\le n}^{j} dis(p,q_m) \le dis(p',q_n) \quad ②$$

In the inequation①②, $dis(.,.)$ represents the distance between query spot of user and supposed user location of attacker. The solution of equation above represents the possible user location area speculated by attacker. But attacker can not achieve the real user query results saved in terminal. As there were many different solutions representing different possible user location for the equation above, the attacker still can not make sure

 Copyright ⓒ 2015 SERSC

with the specific location of user.

5.2 Algorithms and Procedure

Algorithms:

Set the minimum value of K is $k_{\min}$, set the maximum value of K is $k_{\max}$

$k_{\min}=2$, $k_{\max}=6$

1. The user sends the service request
2. the trusted third party receives the service request
3. if K $\in (k_{\min,} k_{\max})$
6. the trusted third party process the privacy protection with k-anonymity method and pseudonym method.
7. else
8. if K> $k_{\max}$
9. the trusted third party process the privacy protection with pseudonym method
10. else
11. if K< $k_{\min}$
12. the trusted third party process the privacy protection with k-anonymity method
13. end if
14. end if
15.end if

Procedure:

When K value is located in the set range, the trusted third party will anonymize the user's location information with k-anonymity and pseudonym methods and sent service request to the LBS provider, who will answer this request and return the results to the mobile terminal user. When the K value is higher than $k_{\max}$, the trusted third party will anonymize user's location with pseudonym method. Here the real id will be replaced by pseudo-id which will be saved in the trusted third party list with the real id and other detailed information of the user. When the trusted third party sends the result from the LBS provider to the mobile terminal, pseudo-id is checked with corresponding real id of user in the list and then all primal data will be feedback to the mobile terminal user. When the K value is lower than $k_{\min}$, the trusted third party will anonymize user's location with k-anonymity method and transmit the result to the LBS provider, who will send the feedback to the mobile terminal user.

5.3 Experiment Simulation and Analysis of Algorithm Efficiency

Moving object generator is used to simulate the automobile along the road. The service request is sent according to the location information of moving object generator. The map used here is national mapping map provided by U.S. Geological Survey [21], which utilizes the spatial data transmission standards [22]. OPEN GL is used to simulate this map.

Experiment circumstance is Inter(R) Core(TM) i3 2.26 GHz for CPU, 2GB for memory in Windows XP. Programming circumstance is MyEclipse+Hibernate+SQL Server 2005. In this experiment, 300 moving object generators were used to simulate the automobile along the road and 370 service request information were received. K value was set as 2,3,5,6.

Copyright ⓒ 2015 SERSC

5.3.1. Anonymized Success Rate: Different K values are input so as to check the working of the algorithm in different contexts. Success rate is an important measure of performance evaluation. Success rate is the ratio of the number of request anonymized by the TTP to the total number of request send to the TTP [5].

According to the simulate experiment, it is discovered that most information is anonymized with k-anonymity method when k value is less. If the k value is set as 2, 292 information is anonymized with k-anonymity method while only 78 information by pseudonym method. But more and more information will be anonymized by pseudonym method with the enlargement of K value. When K value is set as 6, only 181 information is anonymized with k-anonymity method while 189 information by pseudonym method (Fig.1). That is, when the k value is less, the k-anonymity method will be used more and as the k value increases the pseudonym method usage will get increased.

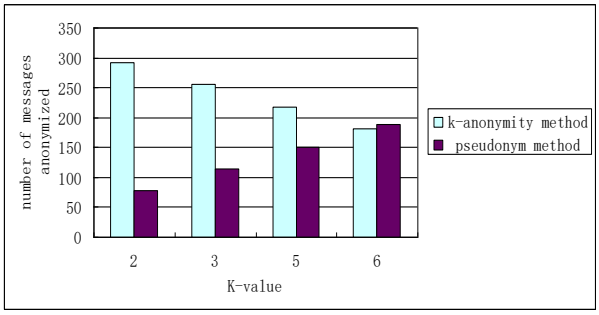


Figure 1. Number of Information Anonymized by k-anonymity Method and Pseudonym Method

5.3.2.Execution Time: Execution time is the time of anonymous process for all inquiry requests from a certain scale of mobile users, which reflects the efficiency of anonymous algorithm. The execution time is shorter; the anonymous algorithm is more efficient.

When comparing the execution time of perceived K-value location privacy protection method and personal k-anonymity method, we realize that the execution time of latter is significantly longer, which is owing to its more deeper refinement to the data and bigger searching space. After every refinement, personal k-anonymity method will calculate the restraint of every new anonymous group and undertake the sensitive attribute generalization, which induce longer execution time(Fig.2)

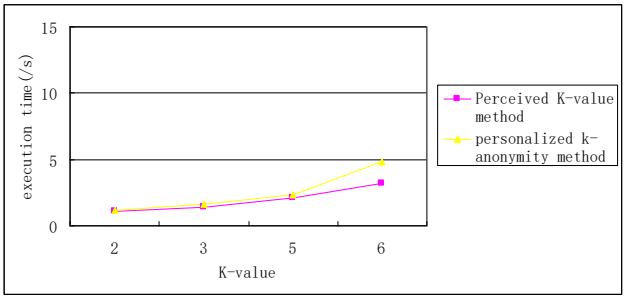


Figure 2. Comparison of execution time

6. Conclusion

In this paper, the merit and demerit of existing location privacy protection is analyzed. Then an effective perceived K-value location privacy protection method is raised and its efficiency is validated through simulation. This method can effectively anonymize all service requests with shorter execution time, which will realize the position privacy protection more efficiently.

 Copyright ⓒ 2015 SERSC

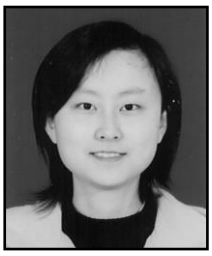
Acknowledgments

Foundation item: This paper is sponsored by Qing Lan Project.

References

[1] T. H. Hollerer and S. K. Feiner, "Mobile Augmented reality", Taylor and Francis Books Ltd, **(2004)**.
[2] Wikipedia, Augmented reality, [Online], Available: http://en.wikipedia.org/wiki/Augmented reality.
[3] M. F. Mokbel, "Privacy in location-based services:start-of-the-art and research directions", Proceeding of 8th International Conference on Mobile Data Management (MDM), **(2007)**; Mannheim, Germary.
[4] Northstream, Location based services: considerations and challenges, [Online], Available: http://www.palowireless.com/lbs/docs/LocationBasedServices.pdf, **(2001)**.
[5] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms", IEEE Trans. Mobile Computing, vol. 9, no. 1, **(2008)**, pp. 1–17
[6] M. Gruteser and D. Grunwald, "Anonymous usage of location based services through spatial and temporal cloaking", Proc. ACM Int'l Conf. Mobile Systems, **(2003)**.
[7] P. Samarati, "Protecting respondents' identities in microdata release", IEEE Trans. on Knowledge and Data Engineering, vol. 13, no. 6, **(2001)**, pp. 1010−1027.
[8] L. Sweeney, "k-anonymity: A model for protecting privacy", Int'l Journal on Uncertainty, Fuzziness and Knowledge-based Systems, vol. 10, no. 5, **(2002)**, pp. 557−570.
[9] H. Kido, Y. Yanagisawa and T. Satoh, "Protection of location privacy using dummies for location-based services", Proc. the 25th International Conference on Distributed Computing Systems (ICPS), **(2005)**.
[10] P. Xiao, X. Zhen, M. X. Feng, "Survey of location privacy-preserving", Journal of Computer Science and Frontiers, vol. 1, no. 3, **(2007)**, pp. 268-281
[11] K. H. Sang, S. H. Woo and M. H. Jeong, "Improved-quality Real-time Stereo Vision Processor", Proc. of the 22nd International Conference on VLSI Design, [S. l.]: IEEE Press, **(2009)**.
[12] T. M. Truta and B. Vinay, "Privacy protection: p-sensitive k-anonymity property", Proceedings of the 22nd International Conference on Data Engineering Workshops (ICDEW), IEEE Computer Society, **(2006)**; Washington, DC, USA.
[13] C. R. Wong, J. Li and A. Fu, "(α, k)-anonymity: an enhanced k-anonymity model for privacy preserving data publishing", Proceedings of the 12th ACM SIGKDD Conference, , PA: ACM Press, **(2006)** ; Philadelphia.
[14] N. Koudas, D. Srivastava and T. Yu, "Aggregate query answering on anonymized tables", Proc of the23th International Conference on Data Engineering, IEEE, **(2007)**; Pisctaway, NJ.
[15] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms", IEEE Trans. Mobile Computing, vol. 9, no. 1, **(2008)**, pp. 1–17
[16] H. Kido, Y. Yanagisawa and T. Satoh, "An anonymous communication technique using dummies for location-based services", Proceedings of the IEEE International Conference on Pervasive services, **(2005)**; Santorini, Greece.
[17] M. Yiu, C. Jensen, X. Huang and H. Lu, "Spacetwist: managing the trade-offs among location privacy, query performance, and query accuracy in mobile services", Proceedings of the 24th International Conference on Data Engineering, **(2008)**; Cancun, Mexico.
[18] P. Samarati and L. Sweeney, "Generalizing data to provide anonymity when disclosing information (Abstract)", Proc. of the Seventeenth ACM Sigact-Sigmod-SigartSymposium on Principles of Database Systems, **(1998)**; New York ACM Press.
[19] L. Sweeney, "k-anonymity: a model for protecting privacy", International Journal of Uncertainty, Fuzziness and Knowledge-based Systems, vol. 10, no. 5, **(2002)**, pp. 557-570
[20] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression", International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, vol. 10, no. 5, **(2002)**,pp. 571-588
[21] U. D. of the Interior, Us geological survey web page, [Online].Available: http://www.usgs.gov/, **(2003)**.
[22] M. C. M. Center, Spatial data transfer format.[Online].Available:http://mcmcweb.er.usgs.gov/sdts/, **(2003)**.

Authors



Yang Yang was born in Nanjing, The People's Republic of China, on Nov.23, 1980. She has joined Nanjing Radio and TV University, Nanjing City Vocational College as a teacher since 2002. Now, she is associate professor. Her research direction include network, grid computing and augmented reality.

Copyright ⓒ 2015 SERSC

 Copyright ⓒ 2015 SERSC