ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

MAINTAINING SECURITY ON MULTI-DIMENSIONAL AREA IN CONTEXT-AWARE MOBILE NETWORKS

*Riji.J **RamMohan.NR
Sun College of Engineering &Technology,Erachakulam jrijicse78@gmail.com,
nrrammohan@yahoo.co.in

ABSTRACT-In recent years, in generally guided opportunity of modern mobile devices with cheap integrated position sensors, location based services(LBS)have become more and more popular. Important examples are nearest friends finding in mobile common networks and the points of interest finders such as the nearest gas stations, hospitals, or places of interests etc. However, the users' privacy information such as location is threatened, when users enjoy the convenience and effectiveness provided by such location services. Therefore, how to secure users' privacy information must be taken into consideration. Many different approaches have been proposed to protect users' identity, location and so on. This paper reviews and analyzes existing privacy protection research works from an integrated perspective, gives the LBS category from two views, and discusses the challenges of securing privacy information. Lastly, our suggestions for future research works are presented.

Keywords:sensors, location based services, networks, privacy information, location services, security.

1.INTRODUCTION

The convergence of technologies such as Geographic Information System(GIS),networks and mobile devices give birth to location based services(LBS), In these services, requests which contain users' locations are sent to Third Service Provider(TSP)[9],and TSP then responds with a few required information for the users. Common examples are finding the nearest Places of Interests(POI) such as gas stations, hospitals, etc. In this process, users' privacy like locations is open and threatened.[10]Privacy is generally the information that you don't want others toknow.

In fact, users' privacy information has suit a service commodity: users provide their location information in replace for free modified services[9][10]. Profits gained by such information reversely guarantee the operation of such services. Therefore, from this perspective, it seems that there is no need to put much intervention on users' location information[10], because both users and service providers seem to have no willingness to protect privacy. But in reality, most users don't understand this process. By this mean, it's necessary to make stronger users' awareness of privacy data run from the position of security, thus equality can be ensured. [1]There have been various delegate works regarding protecting users' privacy so far, such as these mentioned. But one problem is that they only considered just one aspect. For example, just discussed privacy security techniques, [11]but disused related rule and law issues, and they all implicit TSP is the potential risk entity. In fact, in LBS, users must first get their own locations which are provided by Location Provider(LP).If LPs are not trusted, all security methods will not work correctly.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

2. ARCHITECTURE,OBJECTS AND CATEGORY OF LBS

The application architecture is showed in Figure 1.In this model, we assume LPis trusted. Users first request their locations from LP. [8]When done, service request together with their locations will be sent to the LBS provider[8][9]. Then the LBS providers will response with some kind of service after receiving these requests. In this process, we can they say that see the data flow of user's location, which is LP[9], user, LBS provider and user. Actually, the data flow of user's information is much more complicated in practice. For example, the LBS providers may sell users' information to other individuals or organizations for their profits. But, users' privacy security largely depends on the LBS providers[11], especially different kinds of LBS providers are rife in recent years; this is also the reason why most research works on privacy protection in LBS focused on the LBS providers.

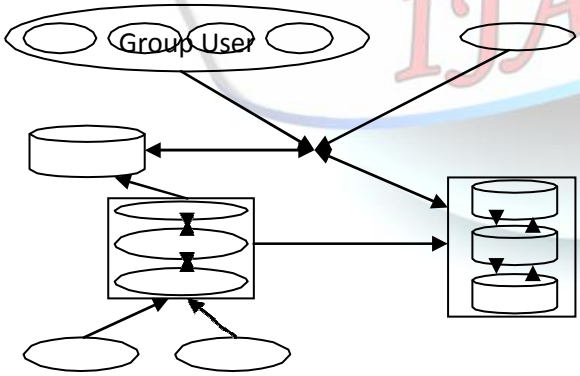

Fig A.1 Architecture ofConventional LBS Application Model

The defensive goals in LBS include three parts: user's identity(ID), spatial information and time-related information[5]. Imagine that you are using an attracting navigation system which is based on your own locations; if you don't want the system know your name, you may choose to be anonymous. But as described the user ID can still be leaked out if his/her locations are revealed. [7]An attacker can gather that some two places are home and work place if somebody visits these two places repeatedly every day

3.FROM THE VIEW OF POLICY AND LAW

A privacy policy specifies the privacy practices of an organization, mainly what kind of personal information is collected, for what purpose, and how theinformation will be used. Policy-based technology reliesmainly on standard protocolswhich are made by third standard associations such as IETF Geopriv, and these protocol must comply with some law such as European standard and must be enforced to protect users' privacy. [10][15]The simplest protocol is described by natural language and enforced manually. Apparently, this way is too costly and is easily neglected by users. The early research on standard protocol such as the famous P3P focused on the compulsory automation.P3P allows websites to release their own standards by XML files. Although P3P is supported by most main browsers, it's not used very often because of its bad usability.

From the viewpoint of law, privacy protection standards state that users' privacy information can only be used under some conditions. In summary, there are three aspects: transparency, legitimate purpose and proportionality. Transparency means users have the right to be informed and access all related data when their privacy data is being dealt with. Legitimate means users' [10]privacy data can only be used for lawful purposes which are clearly declared. Proportionality means that only those data

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

which are needed to complete a user's request can be dealt, and not more than what is needed.

FROM THE VIEW OF TECHNIQUES

Privacy protection techniques use some algorithms to deal with users' privacy raw data and communicate with TSP using processed data. This is the most studied field in LBS at present, and lots of progresses have been made. But all these techniques are designed just for particular scenario and conditions, and their classification criteria are different. Proposed three protection architectures, which are used as classification criterion; Three aspects: identity, location and language are described. In this paper, we summarize existing research achievements in principle and discuss from three aspects: fake data method, k-anonymity[14], obfuscating method. They have some intersections, for example,[14] k-anonymity contains both fake data and obfuscating ideology.

FAKE DATA METHODS

Fake data methods protect users' [5]privacy by sending fake data instead of real data to service providers, such as using pseudonym to protect the user's ID. By sending false locations which are called dummies, users' real location can be protected[9]. This method can be easily implemented, because users themselves can make dummies.[10]The degree of privacy protection depends on the distance between false and real locations

4.EXPERIMENTAL ANALYSIS

Fig A.2 Meeting Location Data privacy And Message privacy

Fig A.3 Group user- login Creation

5. CONCLUSION

With the development of powerful smart phones, LBS will become more and more popular. When enjoying these convenient services, users need to provide their privacy information such as location which is likely abused.[2] Many kinds of existing privacy preserving technologies are reviewed in this paper. [8]We first introduced two classes of LBS: satellite-based LBS and web-based LBS which is rife now a days, and pointed out the privacy threats that users encounter and possible solutions. Then, [11]we continued to discuss security mechanisms from two aspects: [9]policy-based and computational-based techniques. Policy-based mechanism can support more flexible protection, but the precondition is that LP is trusted. Otherwise, [13]it will not work correctly. By this mean, computational-based technology is essential[9], which can guarantee the validity of privacy protection.

Privacy protection is an important research challenge. Although progresses have been made in recent years, lots of problems are still unresolved and more solutions are needed to put forward. Following are some possible research challenges that we can foresee in near future.

1. Evaluation criteria about privacy protection

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

Progresses of technology in any fields largely rely on the advance of evaluation criteria in that field, so as to privacy protection in LBS, [8]that is, how to evaluate the user privacy and quality of service. As for some specific techniques, how to quantify properly is of much importance. For example, since spatial obfuscation mentioned above uses an area to replace users'[19] location, it's obvious that bigger obfuscation area means higher degree protection but lower QoS.

2. New universal framework of privacy protection

Internet is global, so that users' data is most likely to flow to different regions or countries,[11] but exiting security framework such as European standard can work only in limited regions. Therefore, a new universal framework must be proposed by some international organization, [2]or at least let users have the right to choose when meeting with several different frameworks.

3. New attack model in context-aware condition

Most recent privacy protection techniques are designed just for specific context[5][10], but when attackers gained new knowledge of users, lots of new problems will appear. How to find new attack model and propose corresponding solutions is also a research challenge in the future.

REFERENCES

1.A. Loukas, D. Damopoulos, S. A. Menesidou, M. E. Skarkala, G. Kambourakis, and S. Gritzalis, "MILC: A secure and privacypreserving mobile instant locator with chatting," Inf. Syst. Frontiers, vol. 14, no. 3, pp. 481–497, 2012.

2.C.-H. O. Chen et al., "GAnGS: Gather, authenticate 'n group securely," in Proc. 14th ACM Int. Conf. Mobile Computing Networking, 2008, pp. 92–103.

3.D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in Proc. TCC, 2005, pp. 325–341.

4.E. Valavanis, C. Ververidis, M. Vazirgianis, G. C. Polyzos, and K. Norvag, "MobiShare: Sharing context-dependent data & services from mobile sources," in Proc. IEEE/WIC Int. Conf. WI, Oct. 2003, pp. 263–270.

5.G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K. Tan, "Private queries in location based services: Anonymizers are not necessary," in Proc. ACM SIGMOD, 2008, pp. 121–132.

Bilogrevic, M. Jadliwala, K. Kalkan, J. Hubaux, and I. Aad, "Privacy in mobile computing for location-sharing-based services," in Proc. 11th Int. Conf. PETS, 2011, pp. 77–96.

Freudiger, M. Jadliwala, J.-P. Hubaux, V. Niemi, P. Ginzboorg, and I. Aad, "Privacy of community pseudonyms in wireless peer-to-peer networks," Mobile Netw.Appl., vol. 18, no. 3, pp. 413–428, 2012.

8.J. Freudiger, R. Shokri, and J.-P. Hubaux, "Evaluating the privacy risk of location-based services," in Proc. 15th Int. Conf. Financial, 2011, pp. 31–46

9.J. Krumm, "A survey of computational location privacy," Personal Ubiquitous Comput., vol. 13, no. 6, pp. 391–399, 2009.

10.M. Chignell, A. Quan-Haase, and J. Gwizdka, "The privacy attitudes questionnaire (PAQ): Initial development and validation," in Proc. Human Factors and Ergonomics SocietyAnnu. Meeting, 2003.

11.M. Jadliwala, S. Zhong, S. J. Upadhyaya, C. Qiao, and J.-P. Hubaux, "Secure distance-based localization in the presence of cheating beacon nodes," IEEE Trans. Mobile Comput., vol. 9, no. 6, pp. 810–823, Jun. 2010.

12.M. Robshaw and Y. Yin, "Elliptic curve cryptosystems," RSA Lab., Bedford, MA, USA, Tech. Rep., 1997.

13.O. Goldreich, Foundations of Cryptography: Basic Applications. Cambridge, U.K.: Cambridge Univ. Press, 2004.

14.P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in Proc. 7th Int. Conf. Pervasive Computing, 2009, pp. 390–397.

15.P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. 17th Int. Conf. Theory Application Cryptographic Techniques, 1999, pp. 223–238.

16.R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.

17.T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, vol. 31, no. 4, pp. 473–481, Jul. 1985.

18.V. Vazirani, Approximation Algorithms. New York, NY, USA: Springer-Verlag, 2001.

19.Y. Kaneda, T. Okuhira, T. Ishihara, K. Hisazumi, T. Kamiyama, and M. Katagiri, "A run-time power analysis method using OS-observable parameters for mobile terminals," in Proc. ICESIT, 2010, pp. 1–6.

20.Y.-H. Lin et al., "SPATE: Small-group PKI-less authenticated trust establishment," in Proc. 7th Int. Conf. MobiSys, 2009, pp. 1–14.