IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 22-25
www.iosrjournals.org

Improve Dummy-Based User Location Anonymization under Real-World Constraints

M.K.Patil[1], M.N.Sonawane[2] and R.A.Mandlik[3]
[1, 2, 3] *(Department of computer engineering, LoGMIEER, Nashik, India)*

Abstract: *In this paper we have discussed numerous of papers which are based on mobile computing we also have done comparative analysis of those paper with different parameter which include domain application Since system user never transmit actual location information, Location of Mobile device does not consider this issue .The message processing time may become a critical issue and Privacy is a big issue .Previous studies proposed methods to preserve a user's privacy Successfully system user transmit actual location information. We have solved user privacy problem .In this paper, we focus on considers traceability of the user's locations to quickly recover from an roller reveal of the* user's *location..To observe movements of a user and dummies and try to find the real user.*

Keywords: *Privacy, Location-Based-Service, User, Dummy user*

I. Introduction

In this paper, we constantly focus on such constraints and purpose of a location privacy preservation method which can be applicable to a real environment. In particular, our method anonymizes the user's location which generates dummies which we simulate to behave like an real human. The model also considers traceability of the user's locations which can quickly recover from an accidental reveal of user's location. As per the growth of mobile devices related with a GPS receiver, a large number of location based services (LBSs) have been launche.The First requirement is important to have the entire ecosystem beneficial, otherwise, no users and LBSs would use the privacy preservation system. In results show that the we proposed method can ensure that the user's location can be anonymous within the range of a required area size .It Also show that the proposed method avoids fixing connected positions of the user and dummies, which decreases a possibility to be inferred which location is the users.

We need to take into consideration such road information to make our method more robust in a real environment .In this method we need to pool users location and thus assign a trusted third-party server to mediate interaction between the user and the LSB server or uses peer-to-peer collaboration among mobile users. However, it is practically difficulty to deploy a completely safe third-party server in addition mobile peer-to-peer relationship is suffered by the same location privacy problem since users have to share their location information.

II. Literature Survey

In [1] occurred issue is corollary history attack solved by novel suite of algorithm. In [2] Privacy issue are occurred it solved by geographical queries.[3] In that system a user never transmit actual location information. Solved by User-Defined Privacy Grid System called dynamic grid system.[4] This issue are Non trivial issue because of the complexity of the radio propogation it solved by Nonparametric statistically procedure for diagnosis' of the finger print model.[5] LBS issue related to query privacy. solved by the a dummy query generation scheme which takes into account the user motion.[6] To generate context dependent fake information that resembles genuine user solved by geographic and semantic featured of real location trace.[7] In processing nearest neighbor queries solved by defend against colluding.[8] Location of Mobile device does not consider this issue solved by Users using RF signals and neural network can offer solution.[9]The message processing time may become a critical issue it solved we experimentally study the behaviour of our clique clock algorithm.[10]Privacy issued solved by there are active RFID tag.

III. Architecture

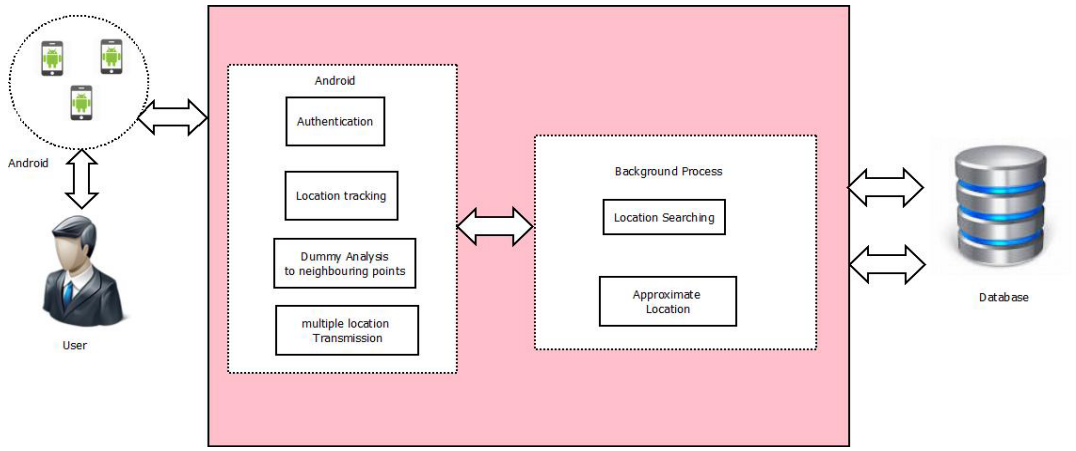


Fig. 1: System Architecture

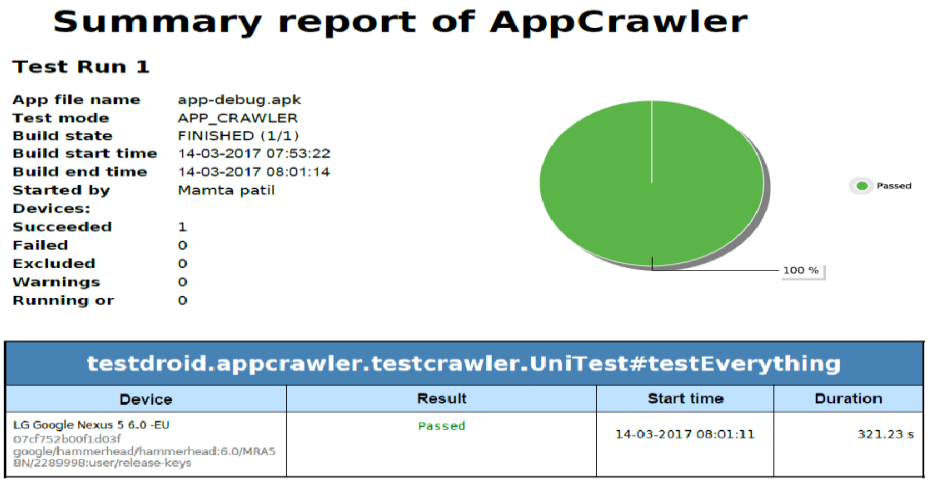
In this system, we qualitatively evaluate the method to see whether humans can distinguish a real user and dummies by observing their location histories. This experiment is more challenging for our method since humans can have much better sense to detect unnatural movement of dummies. The proposed method generates and arrays dummies around the user in a grid formation considering geographical constraints. It simulates dummies' movement to be natural so that an LBS provider cannot distinguish the user from dummies. In addition our method lets dummies to cross with the user to reduce the traceability of the user's location.

User can handle android devices in this devices many facilities can be provided by android devices. Using that devices user can handled location of real user and dummies. Dummies analyzed neighbor location which is moved real user. In system architecture background process done searching location and show the dummies approximate location around the real user.

IV. Algorithm

1. Identify current location of android device.
2. Add current location to tlocation set.
3. Identify nearby locations.
4. Initialize random variable R1 from 1 to size of nearby locations set.
5. Add location at index R1 from nearby locations set to tlocation set.
6. Initialize random variable R2 from 1 to size of nearby locations set.
7. Add location at index R2 from nearby locations set to tlocation set.
8. Transmit tlocation (trace location) set for processing.
9. Identify the list of locations coordinates received from android
10. Initialize tlatitude =0
11. Initialize count =0.
12. for location[i] in locations.
13. Add latitude of location[i] to tlatitude.
14. Increment Count
15. End for
16. Calculate aggregate latitude =tlatitude/count
17. Initialize tlongitude =0.
18. Initialize Count =0.
19. for location[i] in locations.
20. Add longitude of location[i] to tlongitude.
21. Increment count
22. End for
23. Calculate aggregate longitude=tlongitude/count.
24. Store location (aggregate latitude aggregate longitude) and for further processing.

V. Result Analysis



Summary report of AppCrawler

Test Run 1

App file name	app-debug.apk
Test mode	APP_CRAWLER
Build state	FINISHED (1/1)
Build start time	14-03-2017 07:53:22
Build end time	14-03-2017 08:01:14
Started by	Mamta patil
Devices:	
Succeeded	1
Failed	0
Excluded	0
Warnings	0
Running or	0

testdroid.appcrawler.testcrawler.UniTest#testEverything			
Device	**Result**	**Start time**	**Duration**
LG Google Nexus 5 6.0 -EU 07cf752b00f1d03f google/hammerhead/hammerhead:6.0/MRA58N/2289998:user/release-keys	Passed	14-03-2017 08:01:11	321.23 s

Fig 2: Testing Report Generation

Our paper was developed and we have conducted On Line Testing on that .Dashboard show the test success summary or overall success result. In our paper done the integration testing black box testing white box testing, unit testing. Each an every module test separately we have covered the all module to test online.

Screen Short for App

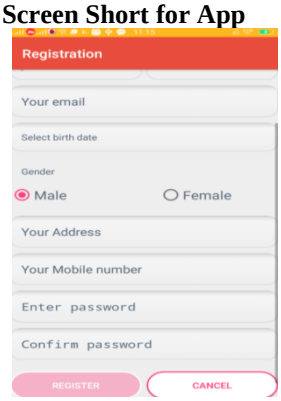


Fig.3 (a): Registration

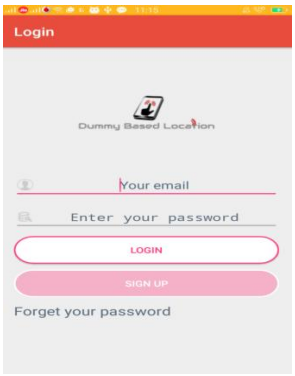


Fig.3 (b) :Login

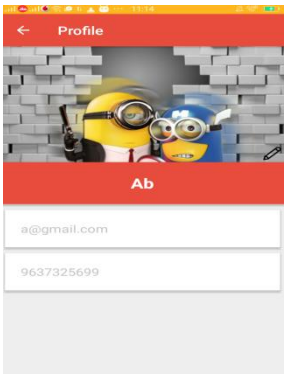


Fig.3(c) : Profile

Fig.3 (d): Map Module

VI. Conclusion

Grid formation we have change the position of grid then change all dummies position in particular position. We consider the reliability of locations on a road network in successive queries and also related positions of a user in a grid formation. Therefore we apply dummy based method is robust. Our method lets dummies to cross with the user to reduce the traceability of the user's locations. Using Searching type of location using predefined entities nearby (eg. Restaurant, malls, ATM) as generate using Aggregate function to approximate location. In this paper expected to run on client-side .For example smart phone application on the top of LSB operation, user can their requirements on the anonymize area and the number of dummies assume that it is more desirable that the system.

Therefore, we suggest dummy based method is robust against assumption attacks based on geographical constraints, i.e. an attacker cannot distinguish a user from dummies using the geographical constraints take location acceptable into user account. Deep learning is a new part of machine learning research. In this paper, our method lets dummies to cross with the user to reduce the traceability of the user's locations.

REFERENCE

[1] G. Acs, C. Castelluccia, and R. Chen, "Differentially private histogram publishing through lossy compression," in Data Mining (ICDM), 2012 IEEE 12th International Conference on. IEEE, 2012.

[2] A Perez, M. Labrador and P. Wightman, Location-Based Information Systems. USA. CRC Computer and Information Science Series. CRC Press, 2011.

[3] F . Liu, K. Hua, Y. Cai. Query I-Diveristy in LocationBased Services.International Conference On Mobile Data Management,2009.

[4] B Gedik and L. Liu, "Protecting location privacy with personalized k anonymity: Architecture and algorithms," IEEE TMC, 2008.

[5] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, Tan, and KianLee. Private queries in location based services: Anonymizers are not necessary. In SIGMOD, 2008.

[6] M. Hendrickson, "The state of location-based social networking," 2008.

[7] A Kushki and A. V. K.N. Plataniotis, "Kernel-based positioning in wireless local area networks," IEEE Trans. on Mobile Computing, June 2007.

[8] E. B. Moran, M. Tentori, V. M. Gonzalez, J. Favela, and A. I. MartinezGarcia, "Mobility in hospital work: Towards a pervasive computing hospital environment," 72–89, 2006.

[9] Computer Science and Telecommunications Board. IT Roadmap to a Geospatial Future. The National Academics Press, November 2003.

[10] M. Muñoz, M. Rodriguez, J. Favela, V. M. Gonzalez, and A. I. Martinez-Garcia, "Context-aware mobile communication in hospitals," IEEE Computer. , Sept. 2003.