International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Secured Location-Based Rewarding System by using the user Digital Signature (SLBRDS)

Rubina Ashfaque Shah[1], Dr. Rahat Khan[2]

[1]Department of Computer Science and Engineering Marthawada Shikshan Prasark Mandal's Deogiri Institute of Engineering & Management Studies, Aurangabad Maharashtra state, India 2015-16

[2]Associate Professor Department of Computer Science and Engineering Marthawada Shikshan Prasark Mandal's Deogiri Institute of Engineering & Management Studies, Aurangabad Maharashtra state, India 2015-16

Abstract: ***In the past few years the explosion of mobile devices has motivated the mobile marketing to surge. In recent few years the new type of mobile marketing term as mobile location based services has attracted strong attention. Regrettably, current MLB techniques have a lot of limitations and raise many concerns, especially about the security and privacy of the system. Here we proposed a novel location based rewarding system which termed as SLBRDS. In this system mobile user can gather area base tokens from the token wholesalers, and then exchange their collected tokens at token collectors for beneficial rewards. Here, develop a security and privacy aware location based rewarding protocol for the SLBRDS system, and proves the completeness and soundness of the protocol. Furthermore, we also shows that the proposed system is capable to flexible different assaults and versatile client security can be well protected. Also for the security purpose in our framework the trusted third party who at first authenticate or registered the mobile users trace the digital signature of the mobile user. When the mobile user request for the token to the token distributors, token distributor checks the digital signature of the mobile user, token collector also checks the digital signature of the mobile user when versatile client demand for token to the token gatherer. In the proposed system we detect an attack by tracing the IP address of the attacker.***

Keywords: Mobile location-based services, security, privacy, digital signature.

1. Introduction

In recent few years the new type of mobile marketing term as mobile location based services has attracted strong attention. Regrettably, current MLB techniques have a lot of limitations and raise many concerns, especially about the security and privacy of the system. Here propose a novel location based rewarding system which termed as SLBRDS. In this system mobile client can gather location base tokens from the token distributors, and then exchange their collected tokens at token collectors for beneficial rewards. We develop a security and privacy aware location based rewarding protocol for the SLBRDS structure, and demonstrate the result and soundness of the protocol. Moreover, we likewise demonstrates that the propose framework is capable to resilient various attacks and mobile user privacy can be well protected. Also for the security reason in our framework the trusted third party who initially authenticate or registered the mobile users trace the digital signature of the mobile user. When the mobile user request for the token to the token distributors, token distributor checks the digital signature of the mobile user, token collector also checks the digital signature of the mobile client when mobile client demand for token to the token collector. In the proposed system we detect an attack by tracing the IP address of the attacker.

All the more as of late, another sort of MLBSs called location base registration amusement, which is produced in light of area based person to person communication lets clients procure gainful prizes on the off chance that they visit certain spots. Specifically, a few applications, including Foursquare and Loopt Star let clients check in diverse areas (e.g., coffeehouses, eateries, shopping centres) to contend with companions in recreations, as well as acquire remunerates, focuses, or rebates from retailers and associations. The prizes and remunerate sums can be distinctive relying upon time of day, how habitually the individual has checked it previously, etc. On the other hand, these area based registration frameworks are restricted in a few perspectives. First of all, customers can just get and reclaim rewards at the same brand stores or even the same store just. For example, if a client visits a Gap store twice, he/she can get a markdown on the buys at Gap stores (or the same Gap store) just, not at some other spots like Starbucks. This significantly debilitates the clients' inspirations for going to the regions. Second, from an administration supplier's point of view, security is not ensured in the current frameworks. Since clients can get advantages for going by a few spots, They have motivations to assert that they are at sure areas despite the fact that they are most certainly not. The greater part of those area based registration applications (e.g., Foursquare) utilize the GPS on a client's cell phone to check the area guaranteed by the client. In any case, clients may undermine their areas by, for instance, jail breaking their cell phones. This issue is truth be told extremely basic in many MLBSs and have not been attractively tackled by existing works. Third, from clients' point of view, clients' protection including character security and area security has been to a great extent overlooked in the present registration frameworks. Specifically, since the present frameworks use focal servers to store every one of clients' records, they can without much of a stretch know which clients have ever been to which puts at what times for what purposes.

In this paper, it protected, a privacy-saving, and realistic mobile location-based rewarding framework, called Secured Location-Based Rewarding System by using the users digital signature which endeavors to address the above concerns.

The proposed framework comprises of a trusted third party (TTP), mobile users (MUs), token distributors (TDs), token collectors (TCs), and a central controller (CC). The TTP issue every MU with a actual personality and a relating certificate. A legal MU has the capacity obtain a location-based token when it visits a commercial element that participates in the framework, i.e., a TD. The issue tokens at a choice of TDs have the similar set-up yet perhaps diverse indicated values. With all the gathered tokens, a MU can reclaim them for beneficial rewards not just at the same store or brand stores, additionally at any different retailers or commercial elements, i.e., TCs, that have joined the framework. The amount of got rewards relies upon the value spoke by the customer collected tokens. Moreover, the CC stores token audition information sent by TDs and gives it to TCs when required.

At that point, a security and privacy aware location based rewarding convention for the proposed SLBRDS framework. We assume that TDs, TCs, and the CC work in the semi honest mode, i.e., they faithfully and effectively execute the framework convention however are interested about MUs' privacy, including their personal information like real characters, token information, and location histories. Specifically, the convention is made out of three parts: personality initiation, token dissemination, and token recovery. In personality initiation, the TTP issues each MU with a character and a relating certificate. The certificate is utilized for a client's character authentication without revealing its real personality. In token conveyance, a TD needs to confirm if a MU asking for a token is a legal client in the framework without knowing its real ID. After that, the TD issues the MU with an anonymous token which can be recovered at any TC for rewards. Since the token contains a portion of the MU's private information, it is just kept by the MU however not any other system elements, including TCs and the CC. The TD then generates relating trial information for the token and send it in its place of the token itself to the CC for future token verification. In token reclamation, a TC first checks whether the present MU attempting to reclaim a token is a legal framework client, without knowing its real ID. At that point, the TC verifies whether the token to be reclaimed is intact and has not been tampered since it was generated with the assistance of the CC, without knowing the substance of the token. After that, the TC checks if the token belongs to the MU. In the event that the MU passes all these verification phases, the TC checks whether the value of the token claimed by the MU is genuine, and assuming this is the case, appropriates the relating rewards to him/her. In this way, in our proposed framework, nobody else other than the TTP can know a MU's real character. As the CC and TCs just have the learning of token audition information, they don't have the foggiest idea about the substance of any token. Since a TD/TC is just aware of the location of the tokens it issued/accepted and there is no essential server to store all the chronological location information, no element could make sense of any particular MU's location history.
Plus, We analyze the security and privacy of the Secured Location-Based Rewarding System by using the user's digital signature (SLBRDS) framework. We come to that the framework is adaptable to various attacks, for example, multi-token solicitation attack, duplicate token recuperation attack, impersonation attack, token tampering attack, and charming attack. We also demonstrate that the MUs' privacy can be all around secured. In addition, We manufacture a tested involving an Android Smartphone and a laptop to execute our proposed framework. We validate the viability of Secured Location-Based Rewarding System by using the users digital signature (SLBRDS) as far as computation, communication, vitality utilization, and storage costs through broad tests.

2. Literature Survey

The fast developments of mobile gadgets, mobile location based service have occurred as a new kind of mobile promotion According to a 2010 reported by Pew Research Centers, on some specified day, 1 percent of online Americans used MLBSs [1]. Juniper examine expect that the proceed from mobile location based service will flow to more than $12.7 billion by 2014 [2]. Presently, there are few type of mobile location based service. One of these location based social networking, is Facebook Places [3]. Additional kind of mobile location based service call for the users to deliver present or historical location resistant to reach some resolution [4], [5], [6]. Mobile business is alternative division of MLBSs, for example, forward advertisement to clients when they are near a business advertisement [7]. These mobile location based administration don't think remunerating administrations.

Further in recent times, a new form of mobile location based administration named location based check in diversion, which is built up based on location based social networking, lets users get worthwhile prizes in the event that they visit certain spots. In particular, certain applications, together with Foursquare [8], and Loopt Star [9], let clients designed in various locations to not only participate with friends in games, but also get rewards, or rebates from venders and organizations. on time of day, how over and again the individual has checked it. The rewards and reward expanses can be diverse depending on time of day, how repeatedly the individual has checked it in the past, et cetera. Be that as it may, these location based check in frameworks are deficient in a few angles. Major customers can only collect and trade in rewards at the same assortment stores or even the same store just. For instance, if customer appointments a Gap store twice, he/she can become a rebate on the buys at Gap stores just, not at any other places like Starbucks. This importantly deteriorates the clients' inspirations for going to the regions. Another, from an administration supplier's standpoint, security is not guaranteed in the present frameworks. Since clients can be given benefits for going to a few locations, they have supportive gestures to benefit that they are at sure locations even all the same they are most certainly not. The majority of those location based check in applications utilize the GPS on a client's mobile gadget to confirm the location guaranteed by the client. This issue is truth be told extremely basic in many MLBSs and have not been sensibly determined by a la mode works [5],[6], [11], [12], [13]. Another, from Mobile clients' perspective, Mobile clients' protection with personality security and location protection has been for the most part overlooked in the present frameworks. In

particular, since the present frameworks use focal servers to store every single mobile client's records, they can absolutely perceive which mobile clients have dependably been to which places at what period for what purpose. Past instruments on client singularity protection in remote networks are not proper to, mobile location based administration situations [14], [15]. While there has been a few examination on location protection concerning general location based administrations, for example, k-anonymity cloaking [16], [17], [18], [19], location disarray [20], [21], [22], [23], [24], imaginary name trades in blend areas [25], [26], [27], [28], they completely have their limits. Note that this procedure does not include any dependable server for producing/Storage location proof like in [3], [5], [8], [13], or for cautious client location protection like in [16], [17], [19] [25] [27]. Moreover, We have demonstrated both the totality and the reliability of the convention, while prior frameworks just concentrate on their fulfilment.

Regardless of the way that range based applications have existed for very much a drawn-out period of time, checking the exactness of a customer's stated region is a test that has pretty much starting late got thought in the examination bunch. Existing architectures for the period and check of such territory confirmations have obliged flexibility. For example, they don't support the proactive social event of territory affirmations, where, at the season of securing a zone check, a customer does not yet know for which application or organization she will use this proof. Supporting proactive region checks is trying in light of the fact that these proofs may engage affirmation benefactors to track a customer or they may manhandle a customer's territory insurance by revealing more information around a customer's zone than totally essential to an application. We present six key framework targets that a versatile region confirmation building configuration should meet. In addition, we show a territory check development displaying that comprehends our design targets and that joins customer indefinite quality and range assurance as key diagram parts, rather than past proposals.

Area evidence is an electronic type of report that ensures somebody's vicinity at a sure area sooner or later in time. An area verification structural planning is a component with which portable clients can get area proofs from evidence backers and with which applications can check the legitimacy of these confirmations. So as to be really valuable, an area verification structural planning must be adaptable. For instance, in some application situations, for example, the protection or police situations said above, clients won't not know while being at a specific area that they will require a proof for having been at this area later on. In this way, it must be workable for clients to assemble area proofs proactively. Be that as it may, the proactive social event of area evidences must be done deliberately, generally confirmation guarantors can track clients and individuals' security will be in peril. In addition, distinctive applications have diverse necessities for the substance of area evidence, for example, the granularity of the ensured area. For instance, an insurance agency might need to know just that a customer drives around chiefly in steady Waterloo (instead of occupied Toronto), yet not where precisely in Waterloo. When a client does not think about the application that area verification will be utilized for, she likewise does not think about the area granularity that will be required by the application. Counting fine-grained area data in any area evidence would tackle this issue. On the other hand, showing such a proof to an application may uncover more data than should be expected about the client, and her security would get abused.

Location proofs – a basic primitive that permits mobile devices to demonstrate their location to mobile applications furthermore, benefits. At an abnormal state, an location confirmation is a little piece of meta-information issued by a part of the remote framework (e.g., a Wi-Fi access point or a cell tower) as a team with a mobile gadget. Any gadget can ask for location evidence from the base when it is inside of correspondence range; the beneficiary gadget can then transmit the confirmation got from the framework to any application that wishes to check the gadget's location. Location proofs are likewise time stamped permitting the beneficiary gadget to store them and use them later for the situation when an application needs to confirm a gadget's location eventually before. At long last, location proofs are marked by the foundation. To make utilization of location verification, an application must trust the base all together to confirm the location confirmation's signature.

Location proofs use public keys to speak to the characters of mobile devices and the framework segments. This permits applications to utilize a personality arrangement of their decision the length of there is a system to delineate personalities to the related public keys. Based on this, location proofs have a few appealing security properties – they are not forgeable and they are not transferable from one gadget to another. What's more, location proofs have an extra security property clients can choose when to demand them and whether to present them to applications and administrations. The base does not have to oversee or screen any of these mobile devices, accordingly definitely diminishing administration expenses and security concerns. A substitute strategy for executing location confirmations is a "noteworthy kin" arrangement in which the framework continually screens the territories of mobile customer location evidences are incrementally deployable – any cell tower on the other hand Wi-Fi access point can start to support them with outstandingly confined coordination with various parts of the base. This coordination is obliged to the affirmation verifier requiring a trust association with the affirmation supplier (i.e., the general population key.

Numerous applications just require a little scale organization of base prepared to do passing out locations proofs. For instance, an espresso store can begin running an advancement promising a free toast any clients that gone by their store every day in the earlier week. A Wi-Fi access point that issue location proofs is a basic and shoddy method for executing such advancement. Essentially, an instructor can offer prizes to those understudies who never miss a class amid the semester. With location proofs, understudies can gather them and submit them toward the end of the semester to get their prize. location2 will exhibit a few such uses of location proofs and develop their usage. Any remote framework part can convey location proofs to close-by cell phones. To

perform this, the framework segment must execute a straightforward two-way convention that issues location proofs. When issued to a gadget, an location confirmation exhibits that the gadget was inside of radio scope of the base. These extents contrast contingent upon the sort of the framework, from a couple of hundred meters for Wi-Fi to a couple of kilometres for cell towers. This paper exhibits an outline of location proofs just for Wi-Fi. we picked Wi-Fi on the grounds that the standard is transparent, making it simple for anybody to actualize our outline and use it in their portable application.

Preventing location based identity deduction of clients who issue spatial inquiries to Location Based Services. we propose changes in view of the entrenched K-anonymity idea to process definite responses for reach and closest neighbour seek, without uncovering the question source. Our routines improve the whole procedure of anonymizing the solicitations and handling the changed spatial questions. Broad exploratory studies recommend that the propose systems are material.

All things considered, the question itself inadvertently uncovers touchy data. In our illustration, the LBS require the directions of the client keeping in mind the end goal to prepare the closest neighbour (NN) query. Since the LBS is not trusted, Alice can team up with the LBS and get the area of Bob and his question result (i.e., wagering office). The following step is to relate the directions to a particular client. Alice may browse an assortment of methods, for example, physical perception of Bob, triangulating his cell telephone's signal1, or counselling openly accessible databases. On the off chance that, for occurrence, Bob utilizes his telephone inside of his living arrangement, Alice can without much of a stretch change over the directions to a road address (most on-line maps give this administration) and relate the location to Bob by getting to an online white pages administration.

For an expansive discourse on the dangers of uncovering delicate data in area based administrations. Practically speaking, clients would be hesitant to get to an administration that may reveal their political/religious affiliations or option ways of life. Besides, given that the LBS is not trusted, clients may be reluctant to ask harmless inquiries, for example, "find out the nearby place store" or "which are the eateries in my area" since, once their uniqueness is uncovered, they may confront spontaneous ads, e-coupons, and so forth. Propelled by this, we create systems to ensure the protection of clients issuing spatial inquiries against area based assaults. In particular, we keep an aggressor from adapting so as to deduce the identity of the question source the settled K anonymity strategy to the spatial area.

A Privacy-Preserving Location verification Updating System (APPLAUS), which does not rely on upon the wide sending of framework establishment or the excessive trusted handling module. In APPLAUS, Bluetooth enabled PDAs in degree regularly make location proofs, which are exchanged to an un-trusted location evidence server that can affirm the trust level of each location confirmation. An affirmed verifier can address and recuperate location proofs from the server. What's more, our location evidence framework guarantees customer location security from every social event. More especially, we use quantifiably updated pseudonyms each wireless to shield location security from each other, and from the un-trusted location verification server. we develop a customer driven location security model in which particular customers survey their location assurance levels continuously and pick whether and when to acknowledge a location evidence sales.

To protect against contriving strikes, we also present between's situating based and association gathering based systems for special case distinguishing proof. Wide exploratory and re-sanctioning results in light of various data sets exhibit that APPLAUS can reasonably give location proofs, basically spare the source location insurance, and enough recognize intriguing attacks.

On singleton survey (SR) spam attack identification, and "spammer" suggests "SR spammer" if not for the most part demonstrated. As demonstrated by the above observations, a novel approach that maps the SR spam recognition issue to an unusually joined common sample discovery issue. The count relies on upon multi-scale multidimensional time game plan eccentricity location. In particular, it fabricates bits of knowledge whose joint peculiarity could be an in number marker of SR spam attacks. The perceived estimation fuses the typical rating, the total number of audits, and the extent of singleton surveys among all audits. It accumulate these estimations from examinations and surveys for each store to fabricate the multidimensional time course of action, base on which it develop a SR spam discovery model. It merges transient curve fitting and LCS (Longest Common Sub-gathering) estimations to make sense of sporadic territories in each estimation of the time course of action. It then devises a situating based computation to cement the qualities in all estimations to make feeling of momentarily related peculiar zones. Additionally, since momentary instabilities are fundamental in the assembled time game plan, it start with a greater time window (e.g. 2 months) to smooth out such boisterous changes of the time course of action, so that any basic strange sample can be perceived generously, thus diminishing false positive rate. After any singleton survey attack is recognized, it downsizes the window size, so that the precise odd centers end up being all the more clear and one can quickly locate the suspicious audits.

Besides, examine the security and protection of the SLBRDS framework. We find that the framework is hearty to various attacks, for example, multi token solicitation attack, copy token rebuilding attack, takeoff attack, token modifying attack, and plotting attack. Also demonstrate that the mobile client security can be very much ensured. In aggregation, we frame a perceived containing of an Android Smartphone and a tablet to apparatus our future framework. Which validate the adequacy of SLBRDS seeing someone of calculation, correspondence, vitality utilization, and capacity costs finished up wide research.

3. Existing System

In Exiting system location-delicate administration depends on client's cell phone to decide its location and send the location to the application. Existing system permits individual to cheat by transmitting his fake location through his gadget, which will empower unapproved individual to get to a confined asset mistakenly or give counterfeit explanations. To address this issue, Existing system framework propose A Privacy-Preserving Location evidence Updating System (APPLAUS) in which co-found Bluetooth empowered cell phones commonly produce location proofs and redesign to a location confirmation server. APPLAUS which does not depend on the wide sending of system framework or the costly trusted figuring module is proposed. Location-delicate applications oblige clients to demonstrate that they truly are (or were) at the guaranteed locations. Much of the time most portable clients have advanced cell gadgets which are fit for finding their locations; a percentage of the LBS utilizing clients can undermine their real locations and which brings about absence of secure component to give their present or past locations to applications and administrations.

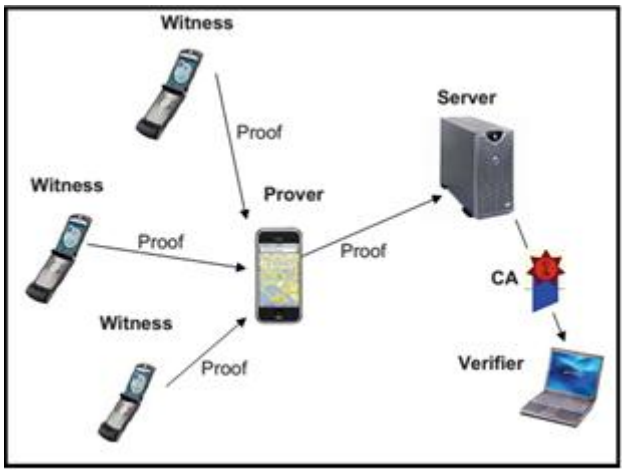

Figure 1: Existing System architecture

Occasionally changed aliases utilized by the cell phones to secure source location protection fake individuals, and from the location verification server which can't be trusted. This framework even created client driven location protection model in which singular clients assess their location security levels progressively and choose whether and when to acknowledge a location evidence trade demand taking into account their location security levels. It utilized factually changed aliases every gadget to ensure source location security. For additional learning, this is the first work to address the joint issue of location confirmation and location protection. Trial yields and reenactment execution results have demonstrated that plan can give location proofs viably while protecting the source location security in the meantime.

4. Conclusion

In this paper we have talked about around a secure, privacy conserving, and realistic location-based rewarding framework. We have planned a security and privacy aware convention for the framework and perceived its culmination and soundness. We find that the framework is impervious to numerous sorts of assaults and portable clients' privacy can be very much ensured. we have additionally evaluated the framework viability by general genuine experiment with and demonstrate that the framework working out correspondence, vitality, and capacity expenses are low. Moreover, while the longed for security and privacy aware location-based rewarding convention is for our framework, the techniques in this can be summed up to address security and privacy issues in general location based administrations and different ranges.

References

[1] Pew Research Center: Internet, Science & Technology [Online].Available: http://pewinternet.org/~/media/Files/Reports/2010/PIP-Location%20based%20services.pdf, 2010. [Accessed 3 November 2015].
[2] Juniper Research, Mobile Location Based Services Applications, Forecasts and Opportunities 2010-2014, [Online]. Available: https://www.juniperre search.com/reports/mobile location_based_services, 2010. [Accessed 5 November 2015].
[3] Facebook - Log In or Sign Up [Online]. Available: http://www.facebook.com/about/location. [Accessed 5 November 2015].
[4] W. Luo and U. Hengartner, *"Proving Your Location without Giving up Your Privacy,"* Proc. 11th Workshop Mobile Computing Systems Applications, Feb. 2010.
[5] S. Saroiu and A. Wolman, *"Enabling New Mobile Applications with Location Proofs,"* Proc. 10th Workshop Mobile Computing Systems Applications, Feb. 2009.
[6] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, *"Location-Based Trust for Mobile User-Generated Content: Applications, Challenges and Implementations,"* Proc. Ninth Workshop Mobile Computing Systems Applications (HotMobile '08), Feb. 2008.
[7] S. Loreto, T. Mecklin, M. Opsenica, and H.- M. Rissanen, *"Service Broker Architecture: Location Business Case and Mashups,"* IEEEComm. Magazine, vol. 47, no. 4, pp. 97-103, Apr. 2009.
[8] Foursquare Labs, Inc. [US]. [Online]. Available: https://foursquare.com/. [Accessed 5 November 2015].
[9] Loopts Labs, [Online]. Available:http://www.loopt.com/about/tag/loopt-star/. [Accessed 5 November 2015].
[10] Z. Zhu and G. Cao, *"Towards Privacy Preserving and Collusion Resistance in Location Proof Updating System,"* IEEE Trans. Mobile Computing, vol. 12, no. 1, pp. 51-64, Nov. 2011.
[11] B. Waters and E. Felton, *"Secure, Private Proofs of Location, "*Technical Report TR-667-03, Dept. of Computer Science, Princeton Univ., Jan. 2003.
[12] N. Sastry, U. Shankar, and D. Wagner, "*Secure Verification of Location Claims,"* Proc. Second ACM Workshop Wireless Security(WiSe '03), Sept. 2003.
[13] W. Luo and U. Hengartner, *"Veriplace: A Privacy-Aware Location Proof Architecture,"* Proc. 18th SIGSPATIAL Int'l Conf. Advances Geographic Information Systems (GIS '10), Nov. 2010.

[14] K. Ren and W. Lou, *"A Sophisticated Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks,"* Proc. 28th Int'l Conf. Distributed Computing Systems(ICDCS '08), June 2008.
[15] C. Ardagna, S. Jajodia, P. Samarati, and A. Stavrou, *"Providing Mobile Users' Anonymity in Hybrid Networks,"* Proc. 15thEuropean Symp. Research Computer (ESORICS), Sept. 2010.
[16] M. Gruteser and D. Grunwald, *"Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking,"* Proc. First Int'l Conf. Mobile Systems, Applications Services (Mobisys '03),May 2003.
[17] B. Gedik and L. Liu, *"Protecting Location Privacy with Personalize dK-Anonymity: Architecture and Algorithms,"* IEEE Trans. Mobile Computing, vol. 7, no. 1, pp. 1-18, Jan. 2008.
[18] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, *"Preventing Location-Based Identity Inference in Anonymous Spatial Queries,"* IEEE Trans. Knowledge Data Eng., vol. 19, no. 12,pp. 1719-1733, Dec. 2007.
[19] B. Gedik and L. Liu, *"Location Privacy in Mobile Systems: A Personalized Anonymization Model,"* Proc. IEEE 25th Int'l Conf. Distributed Computing Systems (ICDCS), June 2005.
[20] H. Kido, Y. Yanagisawa, and T. Satoh, *"An Anonymous Communication Technique Using Dummies for Location-Based Services,"* Proc. IEEE 25th Int'l Conf. Distributed Computing Systems(ICDCS), July 2006.
[21] H. Lu, C.S. Jensen, and M.L. Yiu, *"Pad: Privacy-Area Aware, Dummy-Based Location Privacy in Mobile Services,"* Proc. ACM Seventh ACM Int'l Workshop Data Eng. Wireless Mobile Access(MobiDE), June 2008.
[22] M. Duckham and L. Kulik, *"A Formal Model of Obfuscation and Negotiation for Location Privacy,"* Proc. Int'l Conf. Pervasive Computing, May 2005.
[23] C.A. Ardagna, M. Cremonini, S.D.C. di Vimercati, and P. Samarati,*"An Obfuscation-Based Approach for Protecting Location Privacy,"* IEEE Trans. Dependable Secure Computing, vol. 8, no. 1, pp. 13-27, Jan. 2011.
[24] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, *"Cap: A Context-Aware Privacy Protection System for Location-Based Services,"* Proc. IEEE 29th Int'l Conf. Distributed Computing Systems(ICDCS '09), June 2009.
[25] A. Beresford and F. Stajano, "*Location Privacy in Pervasive Computing,"* IEEE Pervasive Computing, vol. 2, no. 1, pp. 46-55,Jan.-Mar. 2003.
[26] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, *"Preserving Privacy in Gps Traces via Uncertainty-Aware Path Cloaking, "*Proc. 14th ACM Conf. Computer Comm. Security (CCS '07), Jan. 2007.
[27] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, *"Traffic-Aware Multiple Mix Zone Placement for Protecting Location Privacy,"* Proc. IEEE INFOCOM, Mar. 2012.
[28] J. Meyerowitz and R.R. Choudhury, *"Hiding Stars with Fireworks: Location Privacy through Camouflage,"* Proc. ACM MobiCom, Sept. 2009.
[29] www.yelp.com - Google Search. [Online]. Available: http://www.yelp.com/, 2012. [Accessed 5 November 2015].