Security and Privacy Issues in Location Dependent Services for Mobile Communication: A Synergistic Review

Chitrangada Chaubey¹, Swapnil Raj² ans Suresh Kaswan³
¹,²,³ School of Engineering and Information Technology, Sanskriti University, Mathura, India. *chitrangada111@gmail.com

Abstract. With a growing rate of mobile usage in the current networking era, mobile devices have been adopted widely. With mobile proliferation, location awareness is gaining huge insights in mobile and communication technologies for which, information subsystem has to be maintained on geo-located systems. Location Dependent Services (LDS) fetch relevant information from the geo-located information subsystems and deliver it to the user based on their location preferences and choices. Despite having the desirable features and services, LDS does not provide satisfactory protection to the user’s geographic location. Preservation of location has become one of the utmost concerns in mobile network communication. In this paper, we will go through the security & privacy challenges for LDS in mobile networks. Precisely, this paper covers the cryptographic approaches and technologies to enhance privacy to promote location privacy in mobile network communication. The different approaches covered in the review are first compared and then the further research areas have been identified as well as concluded.

1. Introduction
With the increasing usage rate of wireless appliances and the headway in sensing technology, it has become very easy to locate or spot any individual’s precise location anytime and anywhere. Hence, as a result, a new service of application—LDS is being coined [1-4]. Precisely, location-dependent service is a mobile computing application that is associated with the user’s location: this location is shared through requesting location access [5,6]. It felicitates the users to make use of the device’s geographical position for different services LDS allows the users to access the latest location information about their nearby entities and also permits the businesses to share the recent updates against client’s query [7-9].

The location information of the user consists of X-Y-Z coordinates which are generated by either of Location Determination Technology (LDT), like EOTD, GPS, Cell-ID, etc [10-12]. Location-based information is the basic section of the smartphone experience that promotes the mobile computing applications which are being used for Geographic location-based social networking, route navigation while traveling, land searches in real estate, retail and digital marketing, advertisements and product promotions, finding friends, restaurants, gym, petrol pump, medical shop, etc within the range [13,14]. With the proliferation of location-dependent services, LDS users are facing some crucial issues of their detailed and sensitive data getting accessed by someone [15]. As our location redirects our personality more than what we have mentioned in our resume and portfolio, so this problem of getting location accessed is becoming a serious privacy threat in our lives. By accessing a user’s location anyone can misuse it in many ways so this should be considered and resolved by discovering privacy measures [16]. If the user wants to access this service along with confidence, that their private data is completely protected[17,18]. Considering security & privacy threats, because of the location data exchange, some privacy & security threats to clients exist too [19]. This paper has considered and extracted the location-dependent services, their components, and different privacy and security issues involved with them. Also, a detailed case study has been done and the findings have been listed. Figure 1 represents the various application areas of Location Dependent Services [17-19].
1.1 Components of LDS

Figure 2 shows the typical architecture of LDS[20-22] which requires four basic components as:

- **Mobile Device and User:** A device through which the user submits the service information. This requested service can be interpreted by either graphs, pictures, text, speech, and so on. These devices(gadgets) include Laptops, Mobile Phones, and PDAs [23].
- **Positioning:** GPS falls under the most popular positioning system, which tracks the client’s location and conveys the same as asked by the user [24,25].
- **Communication:** It works as a channel for network units. It is used to exchange the data & resource request of a client from a mobile terminal to the LDS provider and afterward the information services from the service contributor to the user or client [26,27].
- **Server:** It acts as a content Provider to hold and convey geographic data of the client.

Figure 3 represents the basic areas of research for the Location Dependent Services [28].
2. Security & Privacy Requirements in Location Dependent Services

Considering Location Dependent Services, most of the security & privacy intimidations related to LDS have still not been appropriately addressed. Internet of Things and cryptography (apart from being an emerging concept) is being expected that various usage areas like transportation, healthcare, and manufacturing, will get benefit from these two [29-31]. The following are some properties with definitions necessary for privacy & security in mobile communication networks.

2.1 Security Concerns

1. **Authentication**: Only authenticated users are supposed to grant permission when they request for joining the LDS i.e. when the Service Provider (SP) is requested for location information by the user through a connecting station [32,33].

2. **Traceability**: Any user who mishandles the network is supposed to get traceable and reported by an authority. This helps in reducing the impact of the misbehaving user all across the network [34,35].

3. **Confidentiality**: It assures that the message delivery is done to authorized parties only. It can be achieved through a secure key management system’s encryption techniques [36].

4. **Efficiency**: A lightweight management scheme should be used to ensure effective operation.

2.2 Privacy Concerns

1. **Anonymity**: The ability of a user to access something without disclosing the identity to the third-parties [37].

2. **Short-term linkability**: A receiving vehicle (VANET) must be capable of verifying that the multiple messages it is receiving within a small-time frame [38].

3. **Pseudonymity**: It gives assurance of resource access by a user without sharing its identity, but can still be answerable for that use [39].

4. **Location Privacy**: The location of the user must be shielded from unapproved access [40].

3. Literature Survey

Below are some issues related to location preservation and security in Mobile Networks, that have been reviewed in the current paper.
Table 1. Location privacy addressed by various Privacy Enhancement schemes in mobile networks.

| Category   | References | Privacy Metric | Location Privacy attack Reported | Issues Reported                                                                 |
|------------|------------|----------------|----------------------------------|--------------------------------------------------------------------------------|
| Mix        | [32]       | Anonymity lot  | Correlation                      | Makes it hard to track the users along with their Orientation.                  |
| Mix        | [29]       | Tracking of Location | Tracing success                  | Used an optimized algorithm for deployment of mix-zone strategy to improve user’s location privacy. |
| Mix        | [40]       | Size of anonymity lot & Entropy | Timing & Transition              & Used a variety of placement algorithms for mix-zone and Constructions to improve user’s privacy. |
| Obfuscation | [35]       | Obfuscation lot size | Easy Tracking                    | Provides an overview of obfuscated LDS to Intuitively raise privacy preferences. |
| Obfuscation | [36]       | Imprecise range of LDS query | Inference                       | A random query was used to hide the user’s identity in the query with cloaked enabled information evaluation. |
| Cloaking   | [22]       | Size of Anonymity lot | tracking of Location             | The intention of the LDS data is altered to reach enumerated anonymity limitations in the region. |
| Cloaking   | [39]       | Anonymity lot size | N/A                             | A set of peers is formed by the mobile node before requesting for LDS using either multi-hop or single routing. |
| Cloaking   | [1]        | Anonymity lot size | N/A                             | TTP application, Casper which enables the users to register a particular privacy profile, through which the user’s exact location is blurred by anonymizer into a cloaked area. |
| Cloaking   | [30]       | Entropy         | Trail analysis                   | Used an optimal technique of mobility-aware cloaking to restrict the tracing.    |
| Cloaking   | [3]        | Periodic Queries & cloaked spatial region | Query sampling and tracking     | Used a spatial information-based cloaking technique to differentiate between the boundary of location access and query privacy. |
| Cloaking   | [2]        | Anonymity lot size | Inference                        | A decentralized system, Prive (for query depersonalization), which assures it under any of the user spread. |
| Cloaking   | [13]       | Anonymity lot size | Correlation                      | Users’ privacy profiles are defined by cluster isolated algorithms.            |
| Cloaking   | [11]       | Anonymity lot size | Inference                        | A prohibition-based linear computation is used for spatial query processing.     |

Table 2. Location privacy addressed by various cryptographic schemes in mobile networks.

| Category | Strategy                  | Privacy Metric                      | Location Privacy attack Reported | Issues Reported                                                                 |
|----------|---------------------------|-------------------------------------|----------------------------------|--------------------------------------------------------------------------------|
| PIR      | Nearest neighbor [20]     | K-degree of anonymity               | Correlation                      | Approximation of Nearest neighbor using Hilbert ordering                        |
| PIR      | Nearest neighbor [31]     | Communication cost & overhead       | Disclosure of User’s identity    | User and database both are protected by location generalization into coarse-grained regions. |
| PIR      | Oblivious transfer & PIR [32], [33] | Performance-based On communication efficiency | Disclosure of User’s identity | Privacy is preserved using oblivious transfer for location data queries.        |
| PIR      | $k$ nearest neighbors [40] | Computation complexity & overhead  | Data & Location privacy          | LBS grant to retrieve location as per user’s request.                          |
| PIR      | $k$ nearest neighbors [14] | Communication overhead & complexity | Location privacy and Query processing | As per the user-cantered request, Location information is retrieved.            |
4. Conclusion

This paper has presented a broad review of location privacy in LDS. Security and privacy in mobile networks have been discussed along with the shortcomings and technologies used in previous work and methodologies. A codification has been introduced for recent publication’s comparison along with the privacy metrics concerns and adversary models. This paper has subdivided the current research work into two categories that are cryptographic approaches and privacy enhancement for location privacy in mobile networks. Also, various categories of location privacy issues and challenges have been identified and discussed along with enhancement suggestions.

References

[1] Zongda Wu1, Guiling Li, Shigen Shen1, Xinze Lian, Enhong Chen, Guandong Xu, 2020 ‘Constructing dummy query sequences to protect location privacy and query privacy in location-based services’, Springer Science+Business Media, LLC.

[2] Fabian Burmeister, Paul Drews, Ingrid Sachirmer, 2021 ‘Modeling the C(0)urse of Privacy-critical Location-based Services – Exposing Dark Side Archetypes of Location Tracking’, Proceedings of the 54th Hawaii International Conference on System Sciences.

[3] Abdur R. Shahid, Niki Pissinou, S.S. Iyengar, Kia Makki, 2020 ‘Delay-aware privacy-preserving location-based services under spatiotemporal constraints’, Int J Commun Syst.

[4] Y. Cao, S. Yang, G. Min, X. Zhang, H. Song, O. Kaiwartya, and N. Aslam, 2017 ‘A cost-efficient communication framework for battery-switch-based electric vehicle charging’, IEEE Communications Magazine, 55, pp. 162–169.

[5] E. C. Eze, S. Zhang, and E. Liu, 2014 ‘Vehicular ad hoc networks (vanets): Current state, challenges, potentials and way forward’, 20th International Conference on Automation and Computing, pp. 176–181.

[6] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, 2014 ‘An overview of internet of vehicles’, China Communications, 11, pp.1–15.

[7] J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu, and W. Zhao, 2017 ‘A real-time end-route route guidance decision scheme for transportation-based cyberphysical systems’, IEEE Transactions on Vehicular Technology, 66, pp.2551–2566.
[8] Y. Cao, Y. Miao, G. Min, T. Wang, Z. Zhao, and H. Song, 2016 ‘Vehicular-publish/subscribe (v-p/s) communication enabled on-the- move ev-charging management’, *IEEE Communications Magazine*, 54, pp.84–92.

[9] J.-H. Song, V. W. Wong, and V. C. Leung, 2008 ‘Secure Location Verification for Vehicular Ad-hoc Networks’, *IEEE Global Telecommunications Conference*, pp.1–5.

[10] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. T. Lin, and X. Liu, 2016 ‘Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects’, *IEEE Access*, 4, pp. 5356–5373.

[11] S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, and A. Lei, 2017 ‘A lightweight authentication and privacy-preserving scheme for vanets using tesla and bloom filters’, *ICTExpress*.

[12] Y. Leng and L. Zhao, 2011 ‘Novel design of intelligent internet-of-vehicles management system based on cloud-computing and internet-of-things’, *Proceedings of 2011 International Conference on Electronic Mechanical Engineering and Information Technology*, 6, pp. 3190–3193.

[13] J. Lim, H. Yu, K. Kim, M. Kim, and S. B. Lee, 2017 ‘Preserving location privacy of connected vehicles with highly accurate location updates’, *IEEE Communications Letters*, 21, pp. 540–543.

[14] A. Wasef, R. Lu, X. Lin, and X. Shen, 2010 ‘Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]’, *IEEE Wireless Communications*, 17, pp. 22–28.

[15] M. Srivatsa, A. Iyengar, J. Yin, and L. Liu, 2009 ‘Scalable key management algorithms for location-based services’, *IEEE/ACM Transactions on Networking*, 17, pp. 1399–1412.

[16] K. Rabieh, M. M. E. A. Mahmoud, and M. Younis, 2017 ‘Privacy-preserving route reporting schemes for traffic management systems’, *IEEE Transactions on Vehicular Technology*, 66, pp. 2703–2713.

[17] A. Wasef and X. Shen, 2013 ‘Emap: Expedite message authentication protocol for vehicular ad hoc networks’, *IEEE Transactions on Mobile Computing*, 12, pp. 78–89.

[18] X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, 2014 ‘Practical k nearest neighbour queries with location privacy’, *IEEE 30th International Conference on Data Engineering*, pp. 640–651.

[19] X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, 2016 ‘Practical approximate k nearest neighbour queries with location and query privacy’, *IEEE Transactions on Knowledge and Data Engineering*, 28, pp. 1546–1559.

[20] H. Hu and J. Xu, 2009 ‘Non-exposure location anonymity’, *IEEE 25th International Conference on Data Engineering*, pp. 1120–1131.

[21] T. Xu and Y. Cai, 2007 ‘Location anonymity in continuous location-based services’, *Proceedings of the 15th Annual ACM International Symposium on Advances in Geographic Information Systems*, 39:1–39:8.

[22] W. Luo and U. Hengartner, 2010 ‘Veriplace: A privacy-aware location proof architecture’, *Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pp. 23–32.

[23] T. Peng, Q. Liu, and G. Wang, 2017 ‘Enhanced location privacy preserving scheme in location-based services’, *IEEE Systems Journal*, 11, pp. 219–230.

[24] T. H. You, W. C. Peng, and W. C. Lee, 2007 ‘Protecting moving trajectories with dummies’, *International Conference on Mobile Data Management*, pp. 278–282.
[25] X. Lin, X. Sun, P. H. Ho, and X. Shen, 2007 ‘Gsis: A secure and privacy preserving protocol for vehicular communications’, IEEE Transactions on Vehicular Technology, 56, pp. 3442–3456.

[26] L. Buttyán, T. Holczer, and I. Vajda, 2007 ‘On the effectiveness of changing pseudonyms to provide location privacy in vanets’, Proceedings of the 4th European Conference on Security and Privacy in Ad-hoc and Sensor Networks, pp. 129–141, Springer-Verlag.

[27] J. Freudiger, M. Raya, M. F. P. Papadimitratos, and J.-P. Hubaux, 2007 ‘Mixzones for location privacy in vehicular networks’, WiN-ITS Vancouver, British Columbia, Canada.

[28] C. Zhang, R. Lu, P. H. Ho, and A. Chen, 2008 ‘A location privacy preserving authentication scheme in vehicular networks’, IEEE Wireless Communications and Networking Conference, pp. 2543–2548.

[29] S. Guo, D. Zeng, and Y. Xiang, 2014 ‘Chameleon hashing for secure and privacy-preserving vehicular communications’, IEEE Transactions on Parallel and Distributed Systems, 25, pp. 2794–2803.

[30] C. Bettini, S. Mascetti, X. S. Wang, and S. Jajodia, 2007 ‘Anonymity in location-based services: Towards a general framework’, International Conference on Mobile Data Management, pp. 69–76.

[31] R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux, 2009 ‘A distortion-based metric for location privacy’, Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society, WPES ’09, (New York, NY, USA), pp. 21–30.

[32] J. Krumm, 2007 ‘Inference attacks on location tracks’, Proceedings of the 5th International Conference on Pervasive Computing, PERVASIVE’07, pp. 127–143, Springer-Verlag.

[33] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, 2007 ‘Efficient and robust pseudonymous authentication in vanet’, Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks, VANET ’07, (New York, NY, USA), pp. 19–28.

[34] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, 2008 ‘Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications’, IEEE INFOCOM 2008 - The 27th Conference on Computer Communications.

[35] X. Lin, R. Lu, X. Liang, and X. Shen, 2011 ‘Stap: A social-tier assisted packet forwarding protocol for achieving receiver-location privacy preservation in vanets’, Proceedings IEEE INFOCOM, pp. 2147–2155.

[36] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, 2011 ‘Anonymity analysis on social spot-based pseudonym changing for location privacy in vanets’, IEEE International Conference on Communications (ICC), pp. 1–5.

[37] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, 2012 ‘Pseudonym changing at social spots: An effective strategy for location privacy in vanets’, IEEE Transactions on Vehicular Technology, 61, pp. 86–96.

[38] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, 2016 ‘Mixgroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks’, IEEE Transactions on Dependable and Secure Computing, 13, pp. 93–105.

[39] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, 2007 ‘Amoeba: Robust location privacy scheme for vanet’, IEEE Journal on Selected Areas in Communications, 25, pp. 1569–1589.

[40] S. Eichler, 2007 ‘Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility’, IEEE Intelligent Vehicles Symposium, pp. 541–546.