Privacy Preserving Location-Based Services Through K-Anonymized Vehicular Social Network

Ubaidullah Rajput^{1,*}, Ahsan Ansari², Sammer Zai², Aakash Narwani³

¹Department of Computer Systems Engineering, QUEST, Nawabshah, Pakistan

²Department of Computer Systems Engineering, MUET, Jamshoro, Pakistan

³Department of Information Technology, QUEST, Nawabshah, Pakistan

*Corresponding author: ubaidullah@quest.edu.pk

Abstract

In order to use location-based services (LBS), a user needs to provide his/her location coordinates (geo-coordinates) to the LBS server. The revelation of a user's location/identity may seriously jeopardize his/her privacy. A common solution to this problem is the use of an intermediate anonymizer that obfuscates the real location of a user among K other users. However, in this scenario, the anonymizer must be a trusted entity and therefore, inherits the trust related issues. Not only this, but it may also become a single point of failure. Moreover, if anonymizer is compromised, then the privacy of all the users is compromised. A Vehicular Social Network (VSN) is formed by drivers/passengers who share common interests or location. Similar to mobile nodes, the vehicles also utilize LBS services. However, an anonymizer cannot be used in this scenario because it needs to be updated with current locations of vehicles and therefore, may jeopardize the privacy of vehicles. A VSN can provide significantly help in this scenario. This research proposes a distributed K-anonymity based scheme that considers the social ties between the users of VSN and enables vehicles to use LBS in a privacy preserving manner. The proposed scheme uses a semi-trusted authority (TA) such as a government law enforcement agency that registers vehicles. However, the TA is a semi-trusted entity and does not know what services are requested by a vehicle. On the other hand, the LBS server does not know which vehicle is requesting the service. The computational overhead of the scheme is also presented along with security and privacy analysis. The low computational overhead of TA, LBS server and vehicles shows that the scheme is computationally feasible. The security and privacy analysis shows that a user remains anonymous to the LBS as well as keeps a TA from learning which service was requested by the user.

Keywords—Location based services, Privacy, Trusted Authority, Vehicular Social Network

1 Introduction

THE Location-Based Services (LBS) are used through users' mobile devices and provide them with the information regarding nearby restaurants, hospitals, gas stations, shopping malls, cinema (to name a few) [1]. Another application of LBS is social networking. People find their friends with the applications such as Google Buzz [2]. Many of the LBS services are now mobile-based and enable a user to send his/her real time location. This paves the way for an exciting new way of using mobile phones. With all these benefits of location-based services, we have the threat of compromising a user's privacy. To provide

services, an LBS server would require user's location, and therefore, increases the threat of violating user's location privacy. When a user uses location-based services and send query to LBS provider, he/she sends his/her current location as well. A malicious attacker or eavesdropper can trace user's activities from location information and can harass him/her or perform any kind of malicious activity with this information. Another privacy threat is the fact that LBS provider itself can track user's history, such as various locations visited by the user in the past and therefore, can deduce extract information such as home or office address. Protecting user's privacy and application secrecy from adversaries is of paramount importance to establish and maintain consumers' trust in the mobile platform, especially in social network, mobile social network, and vehicular social network (VSN).

ISSN: 2523-0379 (Online), ISSN: 1605-8607 (Print)

DOI: 10.52584/QRJ.1802.24

This is an open access article published by Quaid-e-Awam University of Engineering Science & Technology, Nawabshah, Pakistan under CC BY 4.0 International License.

K-anonymity is a technique that hides a user among its $K-1$ neighbors. This solution has been widely practiced, but has two major issues: first, the anonymizer needs to be a trusted entity and second, it may become a single point of failure. A vehicular adhoc network (VANET) is a subset of a mobile adhoc network (MANET) with some unique characteristics such as rapid speed of nodes (vehicles) that causes vehicles to quickly change their typologies. A vehicular social network is a combination of VANET and online social network. The characteristics used to form a VSN include common hobbies, same route and current location. A VSN enables connected vehicles to share information on regular basis [12], therefore, vehicles in VSN frequently exchange messages.

In this paper, we provide a scheme to preserve location privacy of users in VSN during acquiring services from an LBS. The main contribution of our scheme is twofold. Firstly, our scheme proposes to use an already established VSN to act as an anonymizer. This greatly saves the overload of establishing an anonymizer. Secondly, with the already distributed nature of VSN, we prevent our VSN based anonymizer to become a single point of failure.

The remaining paper is organized as follows. Section 2 highlights the related work and their limitations. Section 3 provides proposed scheme. Section 4 provides results and discussion, and Section 5 concludes the paper along with the future work.

2 Related Work

The literature survey discusses many approaches that have been put forward for location-based services, but each have their benefits and limitations. These schemes utilize various techniques such as cloaking or K-anonymity, private information retrieval (PIR), generation of dummies and homomorphic encryption-based techniques. Many of these approaches have certain disadvantages such as computational infeasibility and lack of privacy.

Spatial cloaking or K-anonymity [3][4] is a technique that works by hiding a user's location among few of his/her neighbors. These locations are then sent to a trusted third party (TTP) called the anonymizer which hides user's position among other users and sends service query for all of them to LBS provider. Because the anonymizer acts as a trusted third party, it knows the identities of K users. Cloaking or k-anonymity is efficient in terms of processing time because all computation is done on TTP; albeit, it has a high probability of identifying user's location. Generation of dummies [5] is a technique that hides

a user's location and trajectory by sending several queries instead of only one. The drawback is the slow response, DoS attack and studies show that user's true information is easily revealed.

Other widely used techniques are based on the cryptographic approach [6] that guarantees strong privacy at the cost of higher computational complexity. Therefore, the high computational and communication complexity make these approaches almost impractical. One of such approaches is private information retrieval (PIR) [7] where a user requests queries in encrypted form and therefore, the server cannot learn the request. However, PIR incurs significant computational overhead. Another issue is the assumptions that are needed to be made regarding a server's computational abilities. Due to the higher computational requirements, the server should have sufficient computational resources.

The work of Rakesh et. al. [8] proposes two example situations for timely distribution of safety messages in a VANET based on fog and a mixture of fog and Software-Define Network (SDN). The approach by Femi et. al. [9] suggests that when a user gets the service, he does not know that his private information is leaked and therefore, they propose that a scheme that ensures that a user's personal information is not stolen during the information retrieval from a database server. Fan et. al. [10] suggest a technique that temporarily reduces the cost of privacy protection by using a two-tier diagram that is based on K-Anonymity principle. Concretely, to maximize the privacy, level one proxy is selected to generate mock locations and share the returned results from LBS provider.

Hong et. al. [11] use a K-Anonymity based mechanism to query privacy in LBS and study a new proposed algorithm DLS. The algorithm presents a circle segment to provide privacy of real query. They propose two algorithms which are MEE and MER to gain effective query privacy in general cases. Yin et. al. [12] propose a new method which they name as Protecting Location Privacy with Clustering Anonymization (PLPCA). It is used for location-based services in vehicular networks. Sun et. al. [13] attempt to protect the location privacy by proposing a scheme that uses a dummy location-based algorithm to solve a users' privacy problem. During a service request, the users generate dummy locations to send dummy users instead of actual users. However, dummy selection by a naïve user may expose actual location of a user.

Hong et. al. [14] use a social network to share trustworthy information in a vehicular network. They noted that in measuring of direct trust and modeling indirect trust in online social networks, there is strong

correlation between trust and users' interests. Their observations are based on the data that is taken from real online communities. In each dataset, a user's interest profile is constructed from the ratings.

Zhang et. al. [15] propose multi-level caching and spatial K-anonymity based scheme to send user location to LBS privately. The scheme utilizes the markov model. It predicts the next query by forming a spatial K-anonymity, location related to the user's mobility and then selects K cells based on the predicted location, cell's cache contribution rate, and data freshness to improve cache hit rate between users and LSP to reduce the interaction and improves user privacy. Ruchika et. al. [16] propose a P2P communication model which is called CAST. This scheme establishes trust of employees to use their cached mobile data to collaborate with each other. Results are provided locally with low latency rate. The proposed algorithm preserves a user's privacy and performs effectively under pull-based sporadic query scenario. Recently, Jiang et. al. [17] highlight the location privacy mechanism in LBS and also mention the limitations of the current approaches.

By looking at various issues in the above-mentioned approaches, we conclude that a robust, yet simple approach is needed, which requires moderate computational resources, secure communication between client and the server, and avoids a fully trusted third party. Keeping in view all these aspects, we propose a secure and privacy preserving scheme that enable users of LBS to use the services anonymously.

3 The proposed Scheme

The proposed scheme is based on the use of K-Anonymity inherently exists in a VSN. We assume the existence of an already established VSN. This scheme uses three phases. During the initial setup, a user vehicle is registered and acquire tokens from a semi-trusted authority (TA) using cryptographic primitives. In next phase, a vehicle in a VSN sends an encrypted request containing service and an anonymous token to the LBS server and the server responds to the request. In the third phase, the LBS provides the token to TA that charges the vehicle for the service.

3.1 System Model

Figure 1 shows the system model that consists of vehicles, RSUs, LBS and TA. RSUs are an integral part of VANET and VSN and their most basic purpose it to enhance the transmission range of vehicles. They are also used to send information to the vehicles from traffic authorities as well as other system entities.

Fig. 1: The proposed system model

Notation	Explanation
V_i	Initiator Vehicle
TA	Semi-trusted Authority
PKLBS	LBS Public Key
SKTA	TA Private Key/ TA signature
TEXP	Expiry time of Token
n	10 bytes random number

TABLE 1: Notations

In our system model, vehicles can transmit messages to nearby RSU and other neighboring vehicles that forward this to LBS. The semi-trusted authority (TA) and LBS are the application server which receive requests from vehicles through V2V and V2I communication standards.

3.2 Notations

Table 1 shows the notations used in the proposed scheme.

3.3 Working of the Proposed Systems

The proposed scheme has following steps.

3.4 Step 1: Initialization

- Token: $(n||Texp)SK_{TA}$, where n is a 10 bytes integer that serves as the unique identifier of the token. $Texp$ is the expiration time of the token. A vehicle is assigned a number of tokens on a request.
- $TA \rightarrow V_i$ Tokens
- TA keeps a database to maintain the correspondence between a user vehicle and tokens that are assigned to that user vehicle.

3.5 Step 2: Service Request

- $V_i \rightarrow VSN \text{ users} \rightarrow LBS : (Service||Token||VSN \text{ Id})PK_{LBS}$

- VSN Id is an increment counter. It changes after a short time period. Every vehicle keeps track of it. The VSN Id serves as an identifier for the particular VSN from where the service request has been originated. The request encrypted in LBS's public key ensures that no vehicle learns the requested service. Therefore, the vehicles or the RSUs only forward this message without knowing the contents. In this way, that VSN becomes an anonymizer.

3.6 LBS Provides Services to the Users

- After receiving the encrypted message, LBS decrypts it and finds the service and the token. Because of the anonymous token, the LBS cannot learn which vehicle has sent this request.
- *LBS → VSN: Service Response* VSN Id LBS processes the required service and sends back the response. This response contains VSN Id along with the service.

3.7 Step 4: Service Received

V_i gets the service (identifiable to V_i via VSN Id).

3.8 Billing Process

LBS provides token to TA so that the TA could use it for future billing purposes.

4 Results & Discussion

The performance of our scheme is based on two factors. One is the computational cost that consists of measuring the encryption and decryption time of service requests, as well as signing and verification times of tokens. The other aspect is the security and privacy analysis. For the computational cost, the proposed scheme is implemented using JAVA on Eclipse IDE with JDK 7. The test bench is comprised of an i7 processor-based machine with 16 GB RAM. The implementation computes the computational cost of up to 500 services and 500 tokens. Computational cost is calculated by computing the RSA encryption, decryption, signature creation and verification.

4.1 Encryption Time for Services

During implementation, the total number of services is 500 and the time is calculated in seconds. Figure 2 shows the encryption of requesting services by a vehicle. The proposed scheme takes around 8.8ms for a single service and around 0.23 seconds for 50 services. In reality, a vehicle may not send such a higher number of requests simultaneously.

Fig. 2: Encryption time for services

Fig. 3: Decryption time for services

4.2 Decryption Time for Services

The LBS server receives the encrypted requests and therefore, it is important to find the time for decryption for incoming encrypted requests. The decryption time for service is also calculated during the experiment. It is noted that the decryption takes more time than that of encryption. The results are shown in Figure 3. In case the LBS receives 50 encrypted requests, it decrypts them in just 0.83 seconds, and 500 requests in around 9.9 seconds. The result in Figure 3 shows that a single machine is sufficient to entertain about 200 to 250 requests, however, a server needs to be comprised of more than one machines to decrypt increasing number of incoming requests.

4.3 Signing Time for Tokens

The TA issues a number of tokens to a user. One token is needed to receive a single service. Each token contains TA's signature. Figure 4 shows the time to sign tokens that is around 0.136 seconds for 50 tokens, and around 1.26 seconds for 500 tokens. Importantly, these tokens are not required in real time and can be downloaded in off time such as at night. Therefore,

Fig. 4: Signing time for tokens

Fig. 5: Verification time for tokens

this does not create any delay on vehicles getting the service as well as on TA.

4.4 Verification Time for Tokens

Once a request is received, the LBS needs to verify the signature on the token. Figure 5 shows the time taken by an LBS machine for signature verification. The total time taken is 0.22 seconds for 50 tokens, and 2.35 seconds for 500 tokens. The result in Figure 5 shows that the LBS can verify a number of signatures in a very short time period.

4.5 Privacy & Security Analysis

Another important aspect of this work is the privacy and security analysis. When a user sends a service request to LBS, then the contents of the request are encrypted in LBS public key. This prevents the members of the VSN as well as an adversary learning what service is being requested. Similarly, when LBS receives the requests and decrypts it, it only finds a token associated with the service request and therefore, cannot learn which user has requested the service. The responsibility of TA is to issue and receive the token from the LBS that has been utilized for the service

request. Therefore, the TA cannot learn what service has been requested by the user. Using a VSN with its K-1 neighbours prevents the LBS learning the exact location and identity of the user. Another important advantage is that a VSN is distributed and therefore, cannot become a single point of failure, which is a disadvantage with most of the K-anonymizers.

5 Conclusion & Future Work

This research proposed a scheme that enables VSN users to use LBS services without revealing their location or identity. The proposed scheme takes benefit of the existing social ties between the users of VSN where vehicles cooperate with each other. The proposed scheme uses TA to register vehicles and provides a pseudo identity in the form of an anonymous token. The LBS server is unable to know which user vehicle is requesting the service. The VSN members do not know the service or identity of the vehicle which is requesting the service. Finally, the TA does not know anything about the requested service. The results show the low computational overhead of the scheme on TA, LBS and users. The privacy and security analysis show that a user's privacy and the request confidentiality remains intact.

In future, we aim to provide the network analysis of the scheme for communication feasibility as well as aim to evaluate it for various network-based attacks.

References

- [1] H. T. Dinh, C. Lee, D. Niyato and P. Wang, "A survey of mobile cloud computing: Architecture, application and Approaches," *Wireless communication mobile computing-wiley*, vol. 13, issue 18, pp. 1587-1611, 2013.
- [2] A. Nasir Khan, M. L. Mat Kiah, S. U. Khan, "Towards Secure Mobile Cloud Computing: A survey," *Future Generation of Computer system*, ELSEVIER, vol. 29, issue 5, pp. 1278 - 1299, 2012.
- [3] S. Wang and X. S. Wang, "In device spatial cloaking for mobile user privacy assisted by the cloud", 11th IEEE International Conference on Mobile Data Management, pp. 381-386, 2012.
- [4] M. Gruteser, and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," *ACM 1st international conference on Mobile systems, applications and services*, pp. 31-42, 2003.
- [5] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," *IEEE International Conference on Pervasive Services*, pp. 88-97, 2005.
- [6] Y. Gahi, M. Guennoun, Z. Guennoun, and K. El-Khatib, "Privacy preserving scheme for location-based services," *Journal of Information Security*, pp. 105-112, 2012.
- [7] A. Khoshgozaran, C. Shahabi, "Private information retrieval techniques for enabling location privacy in location-based services," *Privacy in Location-Based Applications*, *Lecture Notes in Computer Science*, vol. 5599, pp. 59-83, 2009.

- [8] S. Rakesh, R. Bajracharya, and S. Y. Nam, “Challenges of Future VANET and Cloud-Based Approaches”, *Wireless Communications and Mobile Computing*, 2018.
- [9] F. Olumofin, P. K. Tysowski, I. Goldberg, and U. Hengartner, “Achieving Efficient Query Privacy for Location Based Services” *International Symposium on Privacy Enhancing Technologies Symposium*, pp. 93-110. Springer, Berlin, Heidelberg, 2010.
- [10] F. Fan., S. Li, H. Dai, C. Hu, W. Dou, and Q. Ni, “A K-Anonymity Based Schema for Location Privacy Preservation”, *IEEE Transactions on Sustainable Computing* ol. 4, pp. 156-167, 2017.
- [11] J. Wang, Z. Cai, C. Ai, D. Yang, H. Gao H, and X. Cheng, “Differentially Private K-Anonymity: Achieving Query Privacy in Location-Based Ser-vices”, *International Conference on Identification, Information and Knowledge in the Internet of Things*, 2016.
- [12] B. Ying, and A. Nayak, “Social location privacy protection method in vehicular social networks”, *IEEE International Conference on Communications Workshops (ICC Workshops)*, vol. 84, issue 481, pp. 616-634, 2017.
- [13] S. Zhang, X. Li, Z. Tan, T. Peng, and G. Wang, “A caching and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services”, *Future Generation Computer Systems*, vol. 94, issue 2, pp. 40-50, 2019.
- [14] R. Gupta, and U. R. Pratap, “Achieving location privacy through CAST in location based services”, *Journal of Communications and Networks*, vol. 19, issue 3, pp. 239-249, 2017.
- [15] C. Caballero-Gil, J. Molina-Gil, J. Hernández-Serrano, O. León, and M. Soriano-Ibañez, “Providing k-anonymity and revocation in ubiquitous VANETs”, *ELSEVIER Ad Hoc Networks*, vol. 36, issue 2, pp. 482-494, 2016.
- [16] S. Zhang, G. Wang, and M. Alam Bhuiyan, “Achieving Effective k Ano-nymity for Query Privacy in Location-Based Services”, *IEEE Access*, vol. 5, pp. 24580-24592, 2017.
- [17] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, “Location Privacy-preserving Mechanisms in Location-based Services: A Comprehensive Survey,”*ACM Computing Surveys (CSUR)*, vol. 54, issue 1, 1-36, 2021.