International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 04|July-2015 www.irjet.net p-ISSN: 2395-0072

Preserving Trajectory Privacy using Personal Data Vault

T. Manasa[1], Dr.S.Vasundra[2]

[1] Student, Department of CSE, JNTU Anantapur, Andhra Pradesh, India
[2] Professor, Department of CSE, JNTU Anantapur, Andhra Pradesh, India

---

Abstract - ***The Location Based Services (LBS) are becoming more popular in modern days. The actual work of the LBS is to access the user location information and return search results to the users based on that location .LBSs provide location aware services to users based on their location obtained from their smart phones. Along with the fast development of mWSNs (mobile Wireless Sensor Networks), the Trajectory Privacy Protection (TPP) solutions are in urgent need. However, only a few studies have been done to address this issue. Many existing studies focus on privacy preservation in WSNs with the premise that all the network components are static. In other words, nodes lack mobility to be deployed in mWSNs. Studies in Location Based Services (LBS) indicate that they have much lower computational and communication capabilities. This paper proposes a novel time obfuscated algorithm for protecting the trajectory privacy. The system utilizes the concept of personal data vaults in order to store and forward the location details. The location details are encrypted using the AES (Advanced Encryption Standard) and stored in the personal vault and then forwarded to the central server. The entire system is deployed under peer architecture.***

Key Words: *Location based services, Trajectory Privacy Protection, Personal Data Vault, location privacy*

1. INTRODUCTION

In recent years, the field of location-aware sensing devices has been rapidly expanding. The age of combining sensing environments, processing data and communication in one device, is expected to bring an enormous increase of location-aware applications. Along with the novel applications, a new class of sensor networks, mobile Wireless Sensor Networks (mWSNs), is emerging. While on the move, sensors continuously transmit data streams of sensed values and spatiotemporal information, known as "trajectory information". However, the mobile sensors, which compose such networks, are susceptible to trajectory privacy and security attacks by an adversary tracking the devices over time and space.

The convergence among mobile services and positioning technologies paves the way for a range of new, innovative services, which are commonly referred to as LBSs. Emergence of LBSs creates a demand for novel data management technologies to efficiently support new data types, operations, and workloads. A single anonymity server for employing TPP techniques has been proposed [1] that could not provide complete privacy protection.

Context awareness, as one of the most important features of LBSs, is integrated in mobile devices so that these devices have information about the circumstances under which they operate and can react accordingly. To support context awareness in LBSs, real location data of mobile users has to be collected so that spatio temporal patterns can be extracted by data mining methods. This brings a new conflict of interest: the data mining methods want precise location data, while the mobile users want to protect their privacy by not disclosing their exact movements.

The following example describes the problem scenario. Movements of mobile users are often modeled as trajectories in 2D space. Data mining on the trajectory data has many applications, not only in LBSs, but also in telematics and Intelligent Transportation System (ITS). Methods have been proposed to extract patterns, such as dense regions [2, 3] and frequent routes [4] from the trajectory data. An existing solution for protecting the location and trajectory data in LBSs is to anonymize the users' location data by decreasing the spatio temporal resolution of the locations. After this "anonymization" step, the exact location data becomes a set of spatio temporal rectangles. Although such ambiguity protects the mobile users' privacy, it also reduces the accuracy of the data mining results.

Motivated by these observations, this paper defines new privacy requirements for location/trajectory data and presents a system for collecting users' trajectory

data in a privacy preserving manner. Compared to existing solutions, the proposed system does not require trusted components, yet it protects the privacy of users and preserves the accuracy of privacy protection by keeping the location data intact.

2. EXISTING TPP TECHNIQUES

2.1 Trajectory Privacy Protection (TPP) in sWSNs

Privacy preservation has so far been studied in stationary WSNs (sWSNs) in the existing literature under the assumption that both the sensor nodes and the sink/base station are static. According to the taxonomy of privacy preservation techniques for WSNs in [5], there are two main types of privacy concerns, data-oriented and context-oriented concerns. Context-oriented privacy, named as trajectory privacy in this article, concerns the spatiotemporal information of an event. Particularly, TPP aims to protect the location and time of an event monitored by static nodes, or the location of the sink in sWSNs. In this article, the trajectory privacy of source nodes is of interest. Source node represents the node that generates the message once it observes active events in the network.

2.2 Location Privacy of the Source Node

The location of a source node is crucial in the case that attackers may catch or follow the moving object that is monitored by the sWSNs, such as protected animals, soldiers, etc. The existing techniques fall into two categories: routing path randomization, and cryptographic technique. We review these techniques as follows.

2.2.1 Routing Path Randomization:

This main idea of this technique is to prevent attackers from tracking back the message source location by adding random routing hops en route to the sink. Researchers described the Panda-Hunter Game to study location privacy of the data source node [6]. In order to hide the location of the Panda from adversaries who try to capture the panda by back-tracing the routing path of the event message, Phantom random walk routing is proposed. This routing protocol works in the way that when the source sends an event message, the message is firstly uni-casted randomly or in a directed random fashion for certain hops before it is flooded or routed to the sink. To improve the randomness of the routing paths, Greedy Random Walk (GROW) is proposed. GROW requires the sensor node to randomly route the message to one of its neighbors, which has not participated in the previous random walk [7].

Li et al. studied a dynamic routing protocol which explicates the restricted random selection of intermediate nodes for message forwarding [8]. The authors suggest that in small scale WSNs, routing through single-intermediate nodes is efficient. Such intermediate nodes are randomly selected by the source and need to be away from the source with a minimum distance restriction. However, this method is not suitable for large-scale networks since attackers may deduce that the source is located within a circle region. The excessive long random routing paths cost unnecessary network resources as well. Therefore, the authors suggest angle-based and quadrant-based multi-intermediate nodes selection, where multiple intermediate nodes are selected based on their relative angle and distance to the source according to the sink. This method performs better in terms of message delivery ratio and privacy preservation. However, since the source node needs to predetermine the selected intermediate nodes and the quadrant reference frame, the computation could become a high cost for the source.

2.2.2 Cryptographic Techniques:

A straightforward technique is to use cryptographic techniques to encrypt users' identities and data. Although symmetric and Public Key Cryptography (PKC) have already been applied in resource-constrained environments, there are still concerns in the implementations. For example, symmetric cryptography requires complex protocols that suffer from other constraints. "Software realizations of PKC lead to relatively long duty cycles (operating intervals) which in turn require a significant amount of energy. Computation is negligible if the PKC is performed by power efficient hardware accelerators. In such cases, the corresponding transmission power becomes much more significant and dedicated hardware is required" [9].

Furthermore, only relying on cryptographic methods cannot resolve trajectory privacy issues in an effective and efficient way. Although the adversary does not have the knowledge of encrypted sensor data, data packets headers are usually left unencrypted for routing purposes where the source identity is revealed. In the case when data packet headers are also encrypted, the adversary still can obtain some public information of users, such as working and home addresses. Researchers have already shown how the adversary can crack users' encrypted/anonymized identities [10] with adequate background knowledge. An effective cryptographic method to prevent such encryption cracking to some extent is to encrypt or change the header or node identities every hop en route of message transmissions [11].

However, such technique faces the issue of synchronizing the encryption between nodes and the LBS in implementations. Trajectory privacy protection methods in LBS inherently consider users' mobility in that

they are implemented on smart mobile devices. In some of these methods, k-anonymity is applied, that is, a predetermined value of k is set, such that when a user submits a query, either the query is aggregated with queries from k−1 users or the query includes k Point Of Interests (POIs). For example, in reference [12], researchers proposed a framework that requires a trusted third party or extra unit, known as an anonymizer/cloaking agent. Upon receiving the query from a mobile user, the anonymizer produces an "imprecise" service request and forwards it to the server. The imprecise result is produced by removing the user's ID and aggregating the query with k − 1 queries from other users in a certain cloaking region. After the server responds to the queries, the anonymizer translates/filters the response and sends the "precise" results back to the user. Building on this framework, the following methods were implemented: In reference [13], researchers employed a grid-based complete pyramid data structure that hierarchically decomposes the space into H levels to create cloaking regions. In reference [14], researchers generated cloaking regions by implementing a Hilbert space filling curve.

In reference [15], researchers generated cloaking regions by computing the exact k Nearest Neighbors (kNN) in an incremental fashion. In reference [16], researchers proposed a personalized k-anonymity model that allows each mobile user to define and modify the anonymity level in both temporal and spatial dimensions.

2.3 Trajectory Obfuscation:

The TPP issue in GeoSNs is more complex compared with in other LBS applications. There are only a few works that have been proposed to address this issue. One of the major approaches is to apply the trajectory obfuscation technique, such as spatiotemporal cloaking and space transformation. Cuellar et al. first formally defined a number of notions for evaluating a location obfuscation function. The authors formalize the concept of indistinguishability of obfuscation functions, which requires that the user's actual location should be indistinguishable from a set a possible positions, e.g. an obfuscation region which includes the real location and noise. Indistinguishability needs to be satisfied under different scenarios:

1) when the attacker queries a user's position at regular intervals, the attacker should not be able to increase the precision of his knowledge on the real location up to the predefined threshold chosen by the user;
2) an adversary should not be able to determine the destination from the user's original position and location updates in route;
3) An adversary cannot deduce that the user revisits a certain location. Additionally, with such indistinguishable properties, the obfuscation region needs to be constant for all points contained within it.

For better trajectory privacy protection, the obfuscation function needs to prevent attackers from determining users' current and past routes as well. Although this work defined an explicit concept of indistinguishability, it did not consider the impact of social relationships and interactions among users on the privacy leakage, which is highly possible to be utilized by the adversary to infer users' locations.

3. PROPOSED TPP

This paper proposes a novel trajectory privacy protection using the personal data vault.

- The key idea behind the technique is to store the location details in the personal data vaults rather than directly sending them to the LBS server. By doing this the location information will not be disclosed to the server directly.
- The next enhancement is the encryption. The location information is stored after encrypting it and then forwarded to the LBS server after verification.
- The LBS server then forwards the data to the desired peer.
- The decryption details are shared directly through the peer to peer via mail client. The receiver peer then uses those decryption details to visualize the current location of the sender peer.

The steps of the proposed system include the following:

- Peer registration.
- Getting Location Information.
- Sharing Location Information.
- Sharing Secret key Details via mail client.
- Decryption and plotting the location details.

Peer registration process is done for both the sender and the receiver using the same process. Once the registration is completed the peers are provided with two functionalities which are:

- Sharing Current Location &
- Sharing Requested Location

The current location is shared by the sender peer and the requested location is shared by the receiver peer. The

entire process of the proposed technique is depicted in figure 1.

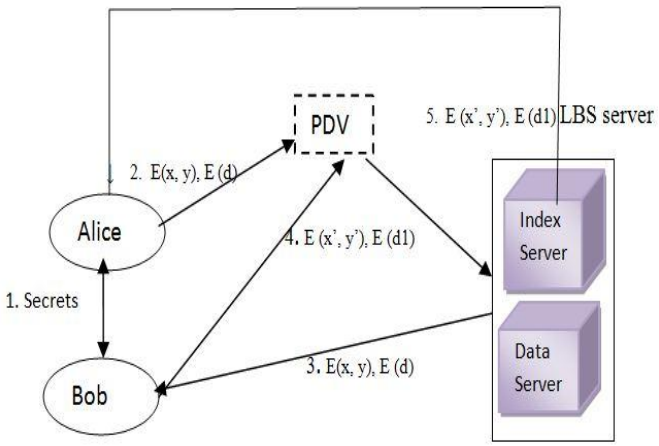

Fig-1: Flow of the Proposed TPP.

The figure clearly depicts that

1. The secret information is directly sent to the peer via a mail client.
2. In the second step, the sender peer shares the current location information (Longitudes and Latitudes) along with message (E (x, y), E (d)).That location information is encrypted using the AES algorithm and then stores the location information along with the secret message.
3. Then the location data can be verified by the peer user by logging into his/her data vault and check whether the data is secured or not. If the data is secured then the sender can forward the data to the LBS server. The encrypted location details can be seen in figure 2.

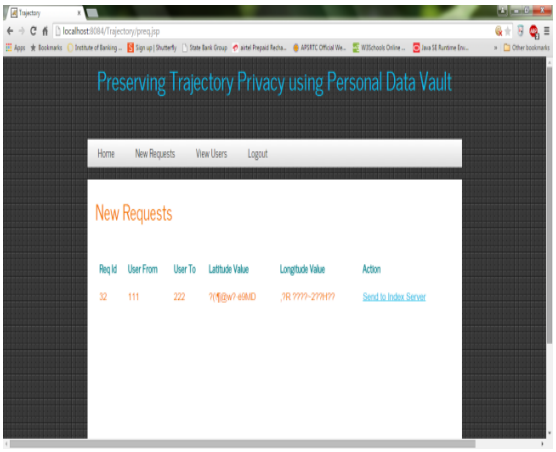

Fig-2: Encrypted Location Details in Data Vault

4. Then the LBS server forwards the location data along with the secret message to the receiver Peer (Bob). Note that the LBS server cannot get the location details as they are encrypted and the encrypted details are not even stored in the server. The location and message details are in the encrypted format which is depicted in figure 3.

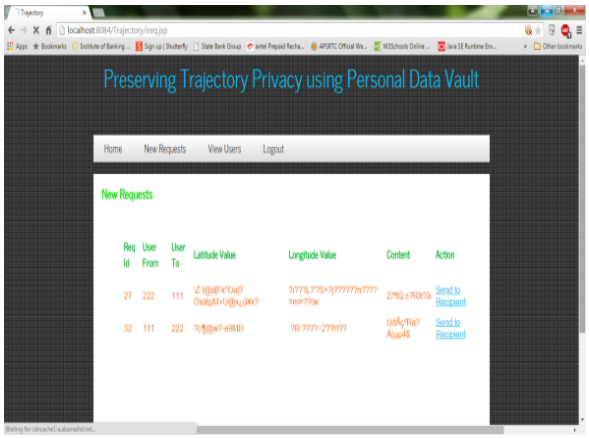

Fig- 3: Encrypted Details in Data Server

5. Then the receiver gets the decryption details via mail and can get the secret message along with the sender current location. Then the receiver will share the requested location and then stores that location in the Data Vault.

Then the process from step 1 to step 4 will be repeated. Finally the sender will get the requested location securely using the mail client.

4. SYSTEM ANALYSIS

As the proposed system shares the secret keys and information via a live mail client, the time taken to share the secret keys and the time taken to forward the location details from peer to server must be calculated. This analysis section considers the time factor as the major metric to test the performance of the proposed system and the results are compared with the existing system.

4.1 Performance Analysis:

The measurement is the encryption time. The time varies with the size of the message. As the secret message size goes on increasing then the encryption time also increases. The results are shown in figure 4.

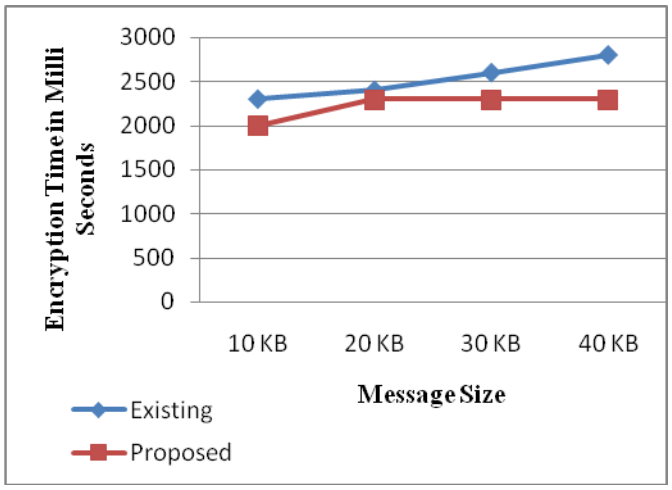

Chart-1: Encryption Time Comparison

The next aspect is to measure the query processing time. The query processing time is the time taken to complete the entire process and to get back the shared location details. This can also be referred to as the complete execution time. The query execution time is calculated at each step. Hence the time taken to execute each step is measured. The results are plotted in the figure 5.

The figure 5 clearly depicts the time at each step. For the proposed system, from 1500ms it has taken different time for different steps from that of existing system.

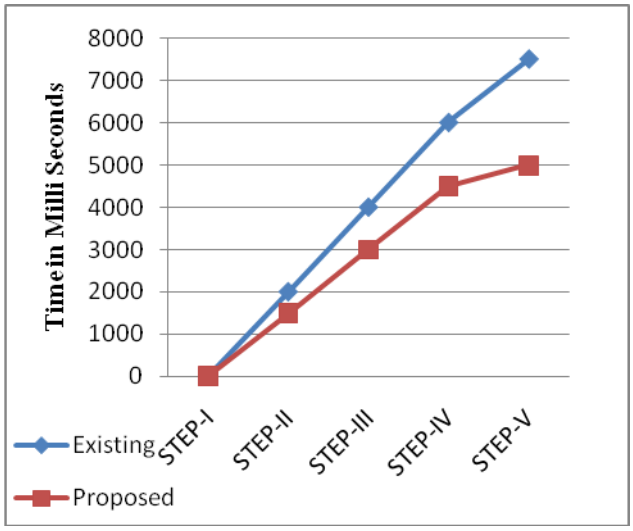

Chart-2: Query Execution Time

4.2. Privacy Analysis:

The next and foremost aspect is to verify the security issues and how well the proposed system is resilient to those attacks.

4.2.1 Protecting against an attacker with right to use the data on the servers:

The data stored on two servers will not reveal any information about their locations to the attacker. The location details on the index server contain transformed coordinates and the data on the LBS server will also be encrypted. By this, an attacker who has permission to access the data on the servers cannot de-anonymize the location data associated with the peer users.

4.2.2 Location privacy for the duration of server access:

Even the intruder with permission to track both the data and LBS servers will not be able to link accesses to the data server and Data Vault for the reason that the indices stored on the index server are encrypted. Only the peer users know the decryption keys to the encrypted indices. Without the decryption keys, the intruder will not be able to link these records to figure out even the transformed location of the users accessing the requested location.

5. CONCLUSIONS

The vast applications of location-aware mobile sensing devices will accomplish severe missions in human-unattainable environments, as well as bring significant convenience to our daily lives. However, these applications will remain elusive unless the trajectory privacy of mobile nodes is properly protected from unauthorized entities. This paper proposed a TPP technique where the use of Personal Data Vaults increases the security of the trajectory privacy. Further, the system is tested for various parameters and the results clearly depicts that the proposed model outperformed the existing model. The use of mail client increases the authenticity level of the location sharing and takes minimum time period to complete a query provided by the peer and the peer architecture improves the performance of the system with high level of data abstraction where location information and the secret messages are encrypted properly.

REFERENCES

[1] Ren-Hung Hwang, Yu-Ling Hsueh, and Hao-Wei Chung, “A Novel Time-Obfuscated Algorithm for Trajectory Privacy Protection”, IEEE Transactions On Services Computing, Vol. 7, No. 2, April-June 2014, pp.126-139.

[2] M. Hadjieleftheriou, G. Kollios, D. Gunopulos, and V. J. Tsotras,”On–Line Discovery of Dense Areas in Spatio–Temporal Databases”, In *Proc. of the 8th International Symposium on Spatial and Temporal Databases, SSTD*, volume 2750 of Lecture Notes in Computer Science, pp. 306–324, Springer, 2003.

[3] C. S. Jensen, D. Lin, B. C. Ooi, and R. Zhang,"Effective Density Queries on Continuously Moving Objects", In *Proc. of the 22nd International Conference on Data Engineering, ICDE*, pp. 71–81, IEEE Computer Society, 2006.

[4] G. Gid´ofalvi and T. B. Pedersen, "Mining Long, Sharable Patterns in Trajectories of Moving Objects", In *Proc. of the 3rd Workshop on Spatio– Temporal Database Management, STDBM*, volume 174 of Online Proceedings of CEUR–WS, pp. 49–58, CEUR–WS, 2006.

[5] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham. Privacy preservation in wireless sensor networks: A state-of-the-art survey. Ad Hoc Netw., 7(8):1501–1514, November 2009.

[6] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk. Enhancing source-location privacy in sensor network routing. In Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on, pages 599 –608, june 2005.

[7] Y. Xi, L. Schwiebert and W. Shi.," Preserving source location privacy in monitoring-based wireless sensor networks", In Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International, page 8 pp., april 2006.

[8] Y. Li and J. Ren,"Source-location privacy through dynamic routing in wireless sensor networks", In INFOCOM, 2010 Proceedings IEEE, pages 1 –9, march 2010.

[9] S. Peter, P. Langend¨orfer, and K. Piotrowski,"Public key cryptography empowered smart dust is affordable", International Journal of Sensor Networks, 4:130–143, 2008.

[10] Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam,"L-diversity: privacy beyond k-anonymity", In Data Engineering, 2006. ICDE '06. Proceedings of the 22nd International Conference on, page 24, april 2006.

[11] K. Pongaliur and X. Li. Maintaining source privacy under eavesdropping and node compromise attacks. In INFOCOM, 2011 Proceedings IEEE, pages 1656 –1664, april 2011.

[12] L. Sweeney. K-anonymity," a model for protecting privacy", International Journal of Uncertainty, Fuzziness and Knowledge-based Systems, 2002.

[13] M. F.Mokbel, C. Chow, and G. Aref,"The new casper: Query processing for location services without compromising privacy", In In VLDB, pages 763–774, 2006.

[14] G. Ghinita, P. Kalnis, and S. Skiadopoulos. Mobihide: a mobile a peer-to-peer system for anonymous location-based queries. In Proceedings of the 10th international conference on Advances in spatial and temporal databases, SSTD'07, pages 221–238, Berlin, Heidelberg, 2007. Springer-Verlag.

[15] M. Yiu, C.S. Jensen, X. Huang, and H. Lu. Space twist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services. In Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on, pages 366 –375, april 2008.

[16] Gedik and L. Liu,"Protecting location privacy with personalized k-anonymity: Architecture and algorithms", Mobile Computing, IEEE Transactions on, 7(1):1 –18, jan. 2008.

BIOGRAPHIES

T.Manasa currently pursuing M.Tech in Software Engineering at JNTUA College of Engineering and Technology Anantapur, Andhra Pradesh. Her area of interest is Computer Networks.

Dr.S.Vasundra is a professor and Head of the department of Computer Science and Engineering at JNTUA College of Engineering and Technology Anantapur, Andhra Pradesh. Her areas of interest includes MANET'S, Computer Networks, Design Patterns, Algorithms, Data Communication systems etc.

