International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 6659-6674

http://www.ripublication.com

A Novel Method to Preserve Privacy: Two- Tiered Privacy Preservation

B.A.Sabarish[1], Divya.C[2], Harini Shankar[3]and Pradisa.S[4]

Amrita School of Engineering,
Department of Computer Science and Engineering, Coimbatore, India
sabarishpm@gmail.com
dividivya.cd@gmail.com
harini2905@gmail.com
pradisa.s@gmail.com

Abstract

Advances in hardware technology like mobile phones, GPS enabled devices etc., have increased the capability to locate and store the spatio-temporal data of moving objects and thereby obtain information about individuals and their behavior. Data leakage from such Location Based Services (LBS) is increasing with the exponential growth of technology, resulting in an innate risk of privacy threats. Data, thus obtained, may be used for a variety of intrusive and malicious purposes and privacy attacks, such as user identification attack, sensitive location tracking attack, sequential tracking attack, etc. A framework is essential to the preserve location privacy of moving objects. In this paper, a two-tier security framework is proposed. In the first tier, algorithms SSET and SIMET are implemented to provide efficient means to encrypt the SIM and IMEI numbers respectively, thus protecting user identity. In the second-tier, Enhanced Privacy Framework (EPF) is used which is a combination of HERMES framework and Statistical framework that protects users against the major attacks on location privacy. Combining these two approaches, a new method named TTPP (Two Tiered Privacy Preservation) is proposed.

Index Terms—moving object database, privacy, anonymity.

I. INTRODUCTION

1.1 LBS

With the increasing need for location specific services such as traffic management and store locator services, the prevalence of Location Based services (LBS) has been established. A location-based service (LBS) is a software application for an IP-

capable mobile device that requires knowledge about where the mobile device is located. [1] LBS typically provide information or entertainment. They have two major actions, obtaining the location of user and utilizing this information to provide a service.

LBS services can be used in a variety of contexts, such as health, work, personal life, etc. Examples of such services include position-enabled tourist services, traffic coordination services and management, rescue operations, safety and security services, targeted advertising etc. LBS deal with large amount of user-movements related spatio-temporal data [2]. Thus, Moving objects databases (MOD) [3] are employed.

MODs are used to store and represent different kinds of moving objects such as moving point, line, or region. Data analysis and data mining is performed on the moving objects to obtain meaningful patterns. A diverse and huge volume of individual location records has to be collected for such data analysis. In this scenario, an individual's participation in a moving objects statistical database substantially increases risk to his privacy.[4]

A user's location can also be acquired from his/her mobile phone and used to facilitate privacy related attacks. With the developments in the field of wireless communications and with the vast availability of RFID chips, a digital trace is mostly left whenever there is a user or object movement thereby resulting in a digitized environment. The knowledge induced from this data through intelligent analysis could reveal sensitive patterns and therefore simple de-identification of the data is not sufficient. [5]

1.2 Classification

LBS systems can be broadly divided into four categories, based on how the location of a user is identified.[6]

- **Network Based Techniques**

They make use of the service provider's network infrastructure to determine the location. They can be implemented non-intrusively, without affecting the handsets.

- **Handset-based technology**

Client software must be installed on the handset to determine its location by cell identification, and signal strengths of the home and neighboring cells, which is continuously sent to the carrier. Accuracy is improved if the handset is also equipped with GPS.

- **Using SIM**

In GSM and UMTS handsets, information such as serving Cell ID, round trip time and signal strength can be acquired. The type of information obtained using the SIM can differ from what is available from the handset. For example, it may not be possible to obtain any raw measurements from the handset directly, yet still obtain measurements using the SIM.

- **Hybrid positioning systems**

A combination of network-based and handset-based technologies is used for location determination. For example, Assisted GPS (A- GPS) uses both GPS and network information to compute the location more precisely.

II. LITERATURE SURVEY

2.1 Disclosure

Disclosure relates to improper attribution of information to a respondent, i.e., an individual or an organization. There are three types of information disclosure. [7]

- **Identity Disclosure**

It occurs when a respondent is identified with the help of released data. Revealing that an individual is a subject of a particular data collection may violate confidentiality requirements.

- **Attribute Disclosure**

It occurs when sensitive information about a respondent is revealed through released data. Confidential information is either directly revealed or can be closely estimated. It comprises identification of the respondent.

- **Inferential Disclosure**

The released data makes it possible for the attacker to determine the value of some attribute of the respondent with more accuracy than otherwise would have been possible. It is difficult to consider inferential disclosure because if disclosure is equivalent to inference, then no data could be released. Also, inferences are used to predict aggregate behavior and not individual attributes. Hence, it is a poor predictor of individual data values.

2.1 Framework Analysis

The following are some of the common attacks as per framework analysis.

TABLE I. ANALYSIS OF FRAMEWORKS

Models	**Attacks**
Statistical framework	Traffic Analysis attacks.
Privacy Aware Monitoring framework (PAM)	Spatio temporal correlation inference attacks.
Hermes framework	User identification attack, Sequential tracking attack & Sensitive location attack

Traffic analysis is a special type of inference attack technique that looks at communication patterns between entities in a system. It is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic.

But here, traffic analysis attacks is emphasized in the context of location based data where patterns could be generated from one's movement in a given region in a given time.

Spatio Temporal Correlation Inference attacks where spatiotemporal event correlation approach to capture the abnormal patterns of a wide class of attacks, whose activities, when observed individually, may not seem suspicious or distinguishable from normal activity changes. This approach correlates events across both space and time, identifying aggregated abnormal event patterns to the host state updates. By exploring both the temporal and spatial locality of host state changes, our approach identifies malicious events that are hard to detect in isolation, without foreknowledge of normal changes or system-specific knowledge.

User identification, Sequential tracking & Sensitive location attacks with their names itself it is clear as to what actually mean. Basically these are related to authentication. By such means, the attacker could generate patterns like frequent visits, timings, etc. of a particular user.

III. TTPP IMPLEMENTATION

3.1 Tier One

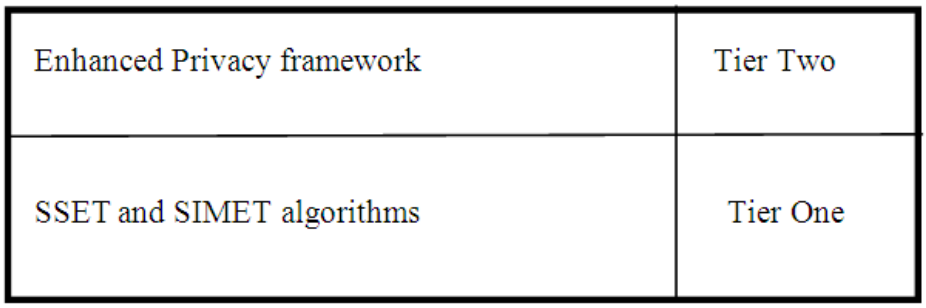


Figure 1.Architectural Diagram

The architecture and depiction of the two tiers is represented diagrammatically in the above figure. In the first tier, identity disclosure is dealt with. By encrypting the SIM and IMEI numbers using the algorithms SSET and SIMET [8] respectively, the probability of identifying the individual is reduced. In the second tier, EPF framework is implemented which prevents attribute disclosure because the probability of identifying the location and other sensitive attributes of the individual is minimal.

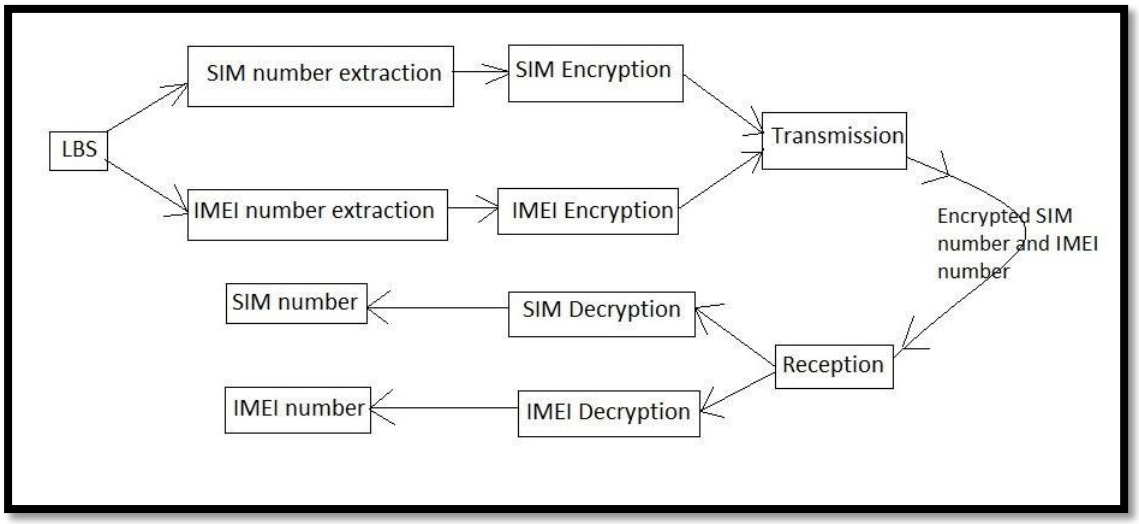


Figure 2.Architectural Diagram

The mechanism for implementation of Tier One is depicted in Figure 2.

3.2 Tier Two

Enhanced Privacy Framework is implemented as an android application**.** The framework is an integration of two other frameworks namely Statistical framework and HERMES framework. The top tier is the Statistical framework and the output from the Statistical framework is fed as input to the HERMES framework which is the second tier of the Enhanced Privacy Framework. The input is the Latitude and Longitude coordinates which is collected by tracking persons using an application named WAYGPS TRACKER. This input is used by the Statistical framework. Once this framework is implemented, a level of privacy is achieved. To obtain an increased level of privacy the output coordinates from the Statistical framework is given as input to the HERMES framework.

Statistical Framework

For any analysis, it is mandatory to begin with statistics. Statistics is the study of the collection, organization, analysis, interpretation and presentation of data. It could either be descriptive or inferential. Descriptive is the one which involves methods of organizing, picturing and summarizing information from data while Inferential involves methods of using information from a sample to draw conclusions about the population. Statistics basically gives a rough idea on how to proceed with the required implementation. It acts as a prototype. To begin with, statistical framework is implemented first, after which the anonymization part is applied so as to provide security from traffic analysis attacks. This implementation is a step by step process for providing maximum security to moving objects such as mobile, tablets, etc. which are generally GPS enabled.

Application Of Statistical Framework

For applying statistical framework, k-means algorithm is chosen. **K-means** clustering is a method of vector quantization, originally from signal processing, that is popular for cluster analysis in data mining. K-means clustering aims to partition **n** observations into **k** clusters in which each observation belongs to the cluster with the nearest mean, serving as a prototype of the cluster. Here, observations will correspond to location based datasets i.e. latitude and longitude. K-means clustering would involve the following steps in order.

- Collection of datasets
- Determination of Seed points
- Computation of Euclidean distances
- Clustering of datasets
- Prediction Analysis

i. Collection of datasets

In this module location based datasets are tracked and collected with the help of an android app named Latitude Longitude. Seven coordinates have been considered starting from source to destination respectively for trial purpose.

ii. Determination of Seed points

Three seed points have been chosen. Choice of seed points is based on the number of clusters to be obtained as number of seed points chosen is equal to number of clusters obtained. Here, two of the three seed points are source location point and destination location coordinate point respectively. The last seed point would be the critical point where probability of changing standard route is maximum.

iii. Computation of Euclidean distances

After determining the seed points, Euclidean Distance is computed among the all seven coordinates with that of seed points. Euclidean distance is calculated using the following formula,

$$d\,(a,b)\;=\;\sqrt{(x_b-x_a)^2+(y_b-y_a)^2}$$

wherex_b&$x_a$correspond to latitude while y_b&y_a correspond to longitude.

After computing the respective distances, the results are tabulated in a predefined format. The format for tabulation of results is given in Table II.

TABLE II.FORMAT FOR CLUSTER TABULATION

Seed Points → Coordinates ↓	Seed PointA1 (source)	Seed Point A4 (critical point)	Seed point A7 (destination)
A1			
A2			
A3			
A4			
A5			
A6			
A7			

iv. Clustering of datasets

After computation of Euclidean distances, we group all the seven coordinates in their respective clusters.

Say,

d (A1, seed1) = x

d (A1, seed2) = y

d (A1, seed3) = z

If x is smallest among all the other three values, then:

A1 ∈ cluster1

If y is smallest among all the other three values, then:

A1 ∈ cluster2

If z is smallest among all the other three values, then:

A1 ∈ cluster3

Likewise, the same computation is carried out until all the coordinates have been grouped into various clusters.

v. Prediction Analysis

Prediction analysis has been done using Rapid Miner tool which is a part of Data mining Toolkit of the output phase. Predictive Analytics encompasses a variety of statistical techniques from modelling, machine learning, and data mining that analyses current and historical facts to make predictions about future, or otherwise unknown, events.

With the generation of the three clusters, traffic can be very well predicted on that respective location at a given time. Frequently visited places can also be well analyzed.

In rapid miner, there are various parameters which performs various functions. In the Figure 2 given below, parameters are **Read Excel, Generate Attributes & Select Attributes**.

The parameter Read Excel reads the log file which contains location based datasets. Log file must be in excel format. To perform this function, path can be set with help of Import configuration Wizard which would import the required log file. In the log file, attributes such as location name, latitude, longitude and time are stored. With the help of Generate Attributes parameter, Euclidean distances, Smallest and Clusters (to

which it belongs to) are computed. Generate Attributes accepts user defined functions. After running the program the output obtained is shown in Figure3.
For better understanding, plot view can also be generated, as shown in Figure 4. Since here, four seed points have been considered, hence four clusters are generated. With this view, frequently visited located location of a particular user are tracked.
This analysis will act as an input for next framework which is the Hermes Framework.

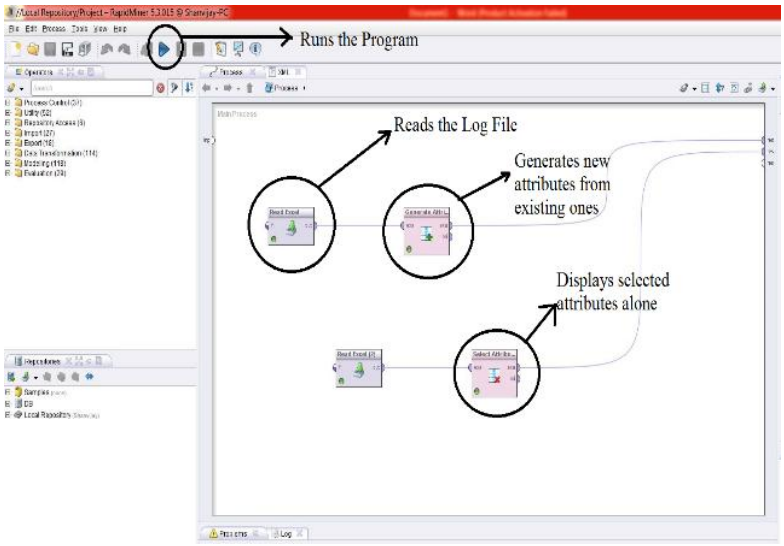
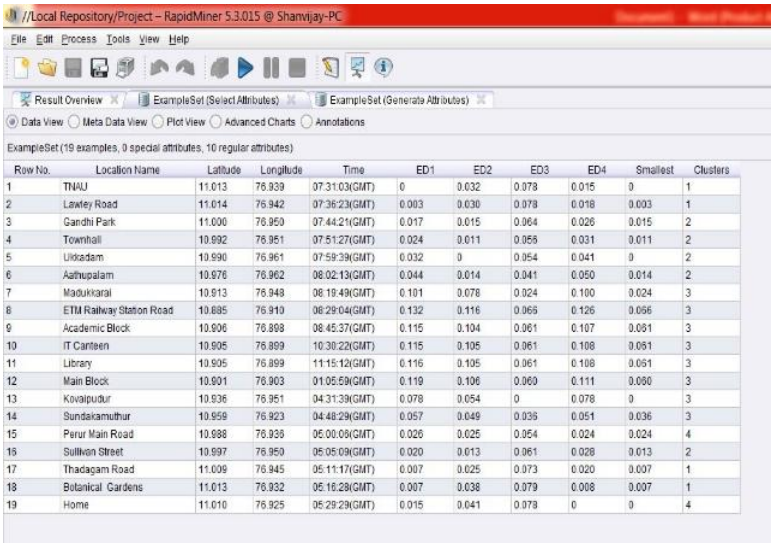


Figure 2.Rapid Miner Input Screen



Row No.	Location Name	Latitude	Longitude	Time	ED1	ED2	ED3	ED4	Smallest	Clusters
1	TNAU	11.013	76.939	07:31:03(GMT)	0	0.032	0.078	0.015	0	1
2	Lawley Road	11.014	76.942	07:36:23(GMT)	0.003	0.030	0.078	0.018	0.003	1
3	Gandhi Park	11.000	76.950	07:44:21(GMT)	0.017	0.015	0.064	0.026	0.015	2
4	Townhall	10.992	76.951	07:51:27(GMT)	0.024	0.011	0.056	0.031	0.011	2
5	Ukkadam	10.990	76.961	07:59:39(GMT)	0.032	0	0.054	0.041	0	2
6	Aathupalam	10.976	76.962	08:02:13(GMT)	0.044	0.014	0.041	0.050	0.014	2
7	Madukkarai	10.913	76.948	08:19:49(GMT)	0.101	0.078	0.024	0.100	0.024	3
8	ETM Railway Station Road	10.885	76.910	08:29:04(GMT)	0.132	0.116	0.066	0.126	0.066	3
9	Academic Block	10.906	76.898	08:45:37(GMT)	0.115	0.104	0.061	0.107	0.061	3
10	IT Canteen	10.905	76.899	10:30:22(GMT)	0.115	0.105	0.061	0.108	0.061	3
11	Library	10.905	76.899	11:15:12(GMT)	0.116	0.105	0.061	0.108	0.061	3
12	Main Block	10.901	76.903	01:05:59(GMT)	0.119	0.106	0.060	0.111	0.060	3
13	Kovaipudur	10.936	76.951	04:31:39(GMT)	0.078	0.054	0	0.078	0	3
14	Sundakamuthur	10.959	76.923	04:48:29(GMT)	0.057	0.049	0.036	0.051	0.036	3
15	Perur Main Road	10.988	76.936	05:00:06(GMT)	0.026	0.025	0.054	0.024	0.024	4
16	Sullivan Street	10.997	76.950	05:05:09(GMT)	0.020	0.013	0.061	0.028	0.013	2
17	Thadagam Road	11.009	76.945	05:11:17(GMT)	0.007	0.025	0.073	0.020	0.007	1
18	Botanical Gardens	11.013	76.932	05:16:28(GMT)	0.007	0.038	0.079	0.008	0.007	1
19	Home	11.010	76.925	05:29:29(GMT)	0.015	0.041	0.078	0	0	4

Figure 3. Output Screen

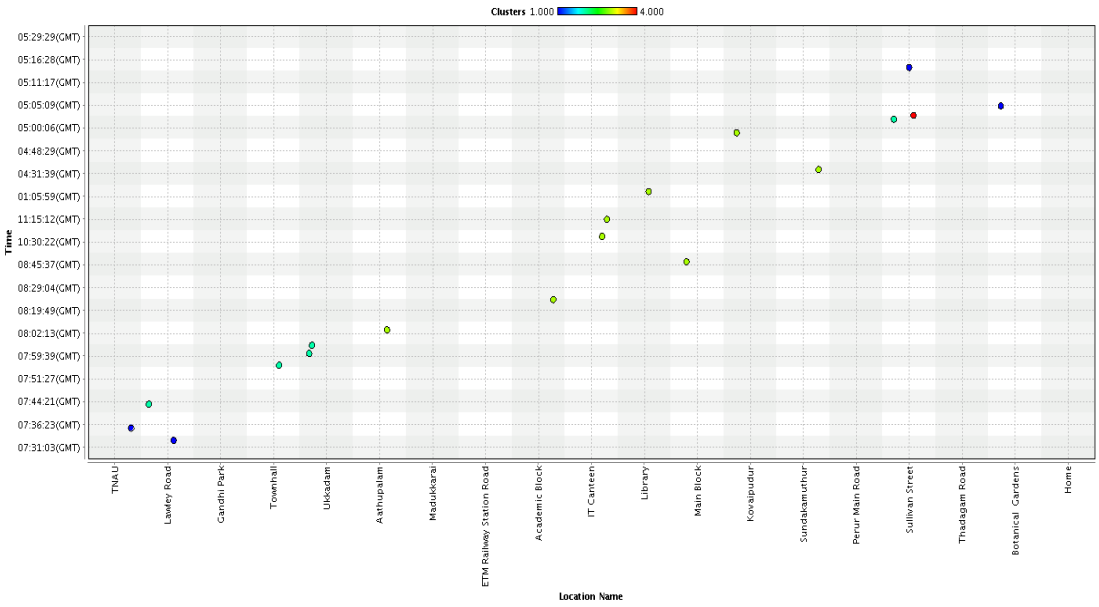


Figure 4. Plot View

HERMES Framework:

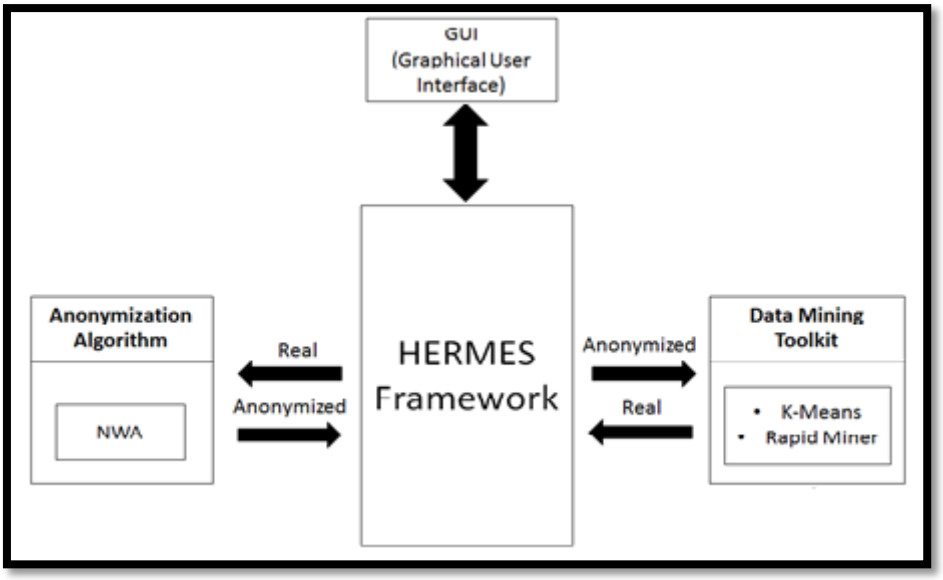


Figure 5. Implementation of HERMES Framework

HERMES framework comprises of anonymization and data mining approach.The implementation of it is shown in Figure 5. Anonymization involves generation of fake trajectories for the original trajectory and data mining used in generation of clusters hence aiding in comparison and evaluation. HERMES [9] framework which is

implemented as an android application is integrated with the Google Map to display the path of the tracked person from source to the destination. Integration with the Google Map involves the following steps:

- Create a new android application (Compile with Google API).
- Import the Google Play Services Lib.
- Obtain the application's SHA1 fingerprint**.**
- Extract the map key by using the obtained SHA1 key.
- Create the AndroidManifest.xml.
- Once the new application is created, the Google Play Services Lib has to be imported and the procedure is,
- Google Play Services Lib is found under the path:
- "....\android-sdk\adt-bundle-windows-x86_64-20130522\adt-bundle-windows-x86_64-20130522\sdk\extras\google". It is moved to the workspace.
- Import Google Play Services library into Eclipse: "File\Import\Existing Android Code into Workspace"
- Add Google Play Services to the application by choosing the library from the properties option.
- Obtain the API key.

Now, NWA [9] algorithm is applied which results in the generation of fake trajectories, corresponding to the original trajectory. The fake coordinates are random coordinates with the source and destination restricted to a particular range with respect to the original trajectory, say 1000 meters. Now the fake coordinates are plotted as fake trajectories in the map thereby unable to distinguish between the original and fake trajectory ensuring an increased level of privacy.

Clusters are already generated for the original coordinates using the Statistical framework. Further clusters are generated for fake coordinates using the K-means algorithm by using the Euclidean distance. Steps involved in K-means algorithm in HERMES framework are:

- The algorithm proceeds by collecting the real-time data sets and using it as fake coordinates for the coordinates resulting from the Statistical framework.
- Three fake seed points are chosen. The first and the last seed points are the original source coordinate and destination coordinate respectively. The last seed point is chosen as a random coordinate that deviates much from the original coordinates.
- Five fake trajectories are generated by collecting the coordinates of five persons.
- Now, Euclidean Distance is computed for each of the fake trajectories. Euclidean distance is calculated using the following formula,

$$d\ (a, b) = \sqrt{(x_b - x_a)^2 + (y_b - y_a)^2}$$

- Once the Euclidean Distance is calculated clusters are generated.

The final output screen with the HERMES and Statistical framework integrated is shown in Figure 6.
The clusters for both the original and fake coordinates are plotted in the Google Map using markers in green and red colour respectively using the "Marker Options". The trajectory and cluster generation is shown in Figure 6.
In Figure 6, only the green trajectory is the original trajectory and the blue, red and pink are fake trajectories.

Figure 6.Output Screen of Enhanced Privacy Framework.

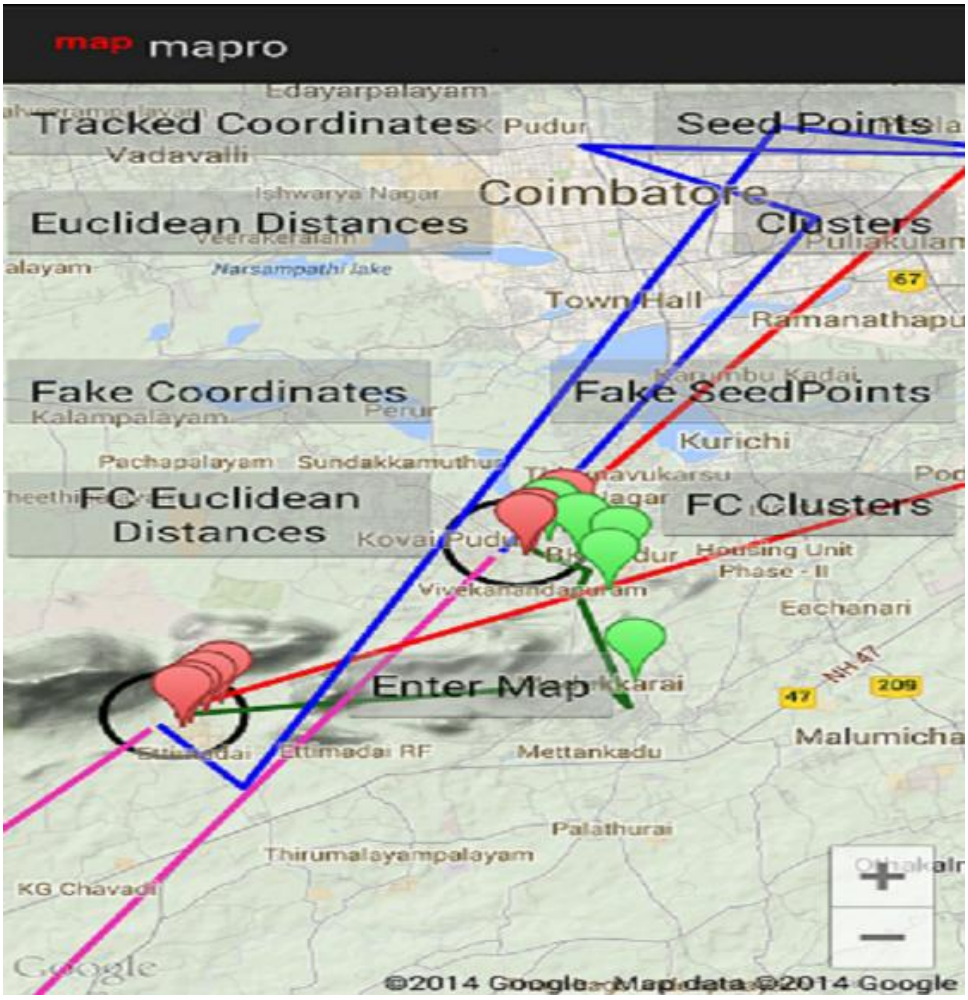


Figure 7.Generated Real and Fake trajectories and clusters.

III. CONCLUSIONS

Though the growth in mobile devices provide numerous benefits, it has brought privacy threats. By implementing TTPP, it is possible to prevent the attacks from malicious users and improve security of moving objects. SIMET and SSET algorithms protect the privacy of the user at the basic level. Enhanced Privacy Framework is thereby implemented with the integration of HERMES framework, Statistical framework and PAM framework. This framework resolves almost all the common attacks on moving objects. By combining the above two, an increased level of privacy is ensured.

Future work concentrates on extending this application as a query based engine to respond to the location based queries of the users.

ACKNOWLEDGMENT

This acknowledgement is intended to be a thanks giving measure to all those involved directly or indirectly with this research. This work was supported by Mr.B.A.Sabarish by providing necessary information and data regarding the research. The authors extend their sincere thanks to their family and friends for helping and motivating during the course of the project.

REFERENCES

[2] Sheng Gao, Jianfeng Ma, Weisong Shi, Guoxing Zhan and Cong Sun. TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing. *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, 2013.

[3] Xinyi Huang, Yang Xiang, Ashley Chonka, Jianying Zhou and Robert H. Deng. A Generic Framework for ThreeFactor Authentication: Preserving Security and Privacy in Distributed Systems. *IEEE Transactions on Parallel and Distributed Systems,* vol. 22, no. 8, 2011.

[4] Basel Alomair, Andrew Clark, Jorge Cuellar and RadhaPoovendran. Towards a Statistical Framework for Source Anonymity in Sensor Network.*IEEE Transactions on Mobile Computing*, vol.12, no.2, 2013.

[5] Nikos Pelekis, AnargyrosPlemenos, ArisGkoulalas-Divanis, DespinaKopanaki, MariosVodas and Yannis Theodoridis. A Benchmark Framework for Privacy Preserving Mobility Data Querying and Mining Methods. Extending Database Technology, 2012.

[6] M. Shao, Y. Yang, S. Zhu and G. Cao.Towards Statistically Strong Source Anonymity for Sensor Networks.In *Proceedings of the 27th Conference on Computer Communications–INFOCOM'08. IEEE Communications Society*, 2008, pp. 466–474.

[7] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar and G. Cao.Towards event source unobservability with minimum network traffic in sensor networks. In *Proceedings of the first ACM conference on Wireless network security–WiSec'08. ACM*, 2008, pp. 77–88.

[8] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie. Random-walk based approach to detect clone attacks in wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 677–691, 2010.

[9] N. Li, N. Zhang, S. Das and B. Thuraisingham. Privacy preservation in wireless sensor networks: A state-of-theart survey. Elsevier Journal on Ad Hoc Networks, vol. 7, no. 8, pp. 1501 –1514, 2009.

[10] H. Wang, B. Sheng, and Q. Li. Privacy-aware routing in sensor networks. *Elsevier Journal on Computer Networks*, vol. 53, no. 9, pp.1512–1529, 2009.

[11] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy and T. La Porta.Cross-layer Enhanced Source Location Privacy in Sensor Networks.*In Proceedings of the 6th Annual IEEE communications society conference on Sensor, Mesh and Ad Hoc Communications and Networks–SECON'09. IEEE Communications Society*, 2009, pp. 324–332.

[12] B. Carbunar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan. Query privacy in wireless sensor networks. *ACM Transactions on Sensor Networks*, vol. 6, no. 2, pp. 1 –34, 2010.

[13] N. Pelekis, E. Frentzos, N. Giatrakos, and Y.Theodoridis. HERMES: Aggregative LBS via a trajectory DBengine. *In Proceedings of SIGMOD.*

[14] N. Pelekis, A. DivanisGkoulalas, M.Vodas, D.Kopanaki and Y.Theodoridis.Privacy-Aware Querying over Sensitive Trajectory Data.*In Proceedings of CIKM*.

[15] Oracle, the Swing Tutorial. URL: http: //download.oracle.com/javase/tutorial/uiswing.(Accessed 19 Jan.2012).

[16] NASA, World Wind Java SDK. URL:http://worldwind.arc.nasa.gov/java. (Accessed: 19 Jan. 2012).

[17] O. Abul, F. Bonchi and M. Nanni. Anonymization of moving objects databases by clustering and perturbation. Information Systems, 35(8):884-910.

[18] O. Abul, F.Bonchi and M.Nanni. Never walk alone: Uncertainty for anonymity in moving objects databases. In *Proceedings of ICDE*.

[19] J.G. Lee, J.Han and K.Y. Whang. Trajectory clustering: a partition-and-group framework. *In Proceedings of SIGMOD.*

[20] M. Nanni and D.Pedreschi.Time-focused clustering of trajectories of moving objects.*Journal of Intelligent Information Systems*, 27(3):267-289.

[21] N. Pelekis, I. Kopanakis, E. Kotsifakos, E. Frentzos and Y. Theodoridis.Clustering uncertain trajectories. Knowledge and Information Systems, 28(1):117-147.

[22] L. Kaufman, P.J. Rousseeuw. Finding Groups in Data: An Introduction to Cluster Analysis.Wiley, NY.

[23] M. Steinbach, G. Karypis, V. Kumar. A comparison of document clustering techniques.*In Proceedings of KDD Workshop on Text Mining.*

[24] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 1981.

[25] M. Reed, P. Syverson, and D. Goldschlag.Anonymous connections and onion routing.*IEEE Journal on Selected Areas in Communications*, 1998.

[26] M. Gruteser and D. Grunwald.Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking.*In Proceedings of the 1st international conference on Mobile systems, applications and services*, 2003.

[27] Y. Xi, L. Schwiebert and W. Shi.Preserving source location privacy in monitoring-based wireless sensor networks. In IPDPS 2006.*The 20th International Parallel and Distributed Processing Symposium*, 2006.

[28] B. Hoh and M. Gruteser.Protecting Location Privacy through Path Confusion. In Secure Comm 2005. *First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, 2005.

[29] M. Shao, Y. Yang, S. Zhu, and G. Cao.Towards Statistically Strong Source Anonymity for Sensor Networks. INFOCOM 2008.*The 27th IEEE Conference on Computer Communications*, 2008.

[30] S. Saltenis, C.S. Jensen, S.T. Leutenegger and M.A. Lopez.Indexing the Positions of Continuously Moving Objects. *Proc.ACM SIGMOD*, 2000.

[31] R. Benetis, C.S. Jensen, G. Karciauskas and S. Saltenis. Nearest Neighbor and Reverse nearest Neighbor Queries for Moving Objects. *Proc. Int'l Database Eng. and Applications Symp.(IDEAS),* 2002.

[32] Y. Tao, D. Papadias and J. Sun. The TPR*-Tree: An Optimized Spatio-Temporal Access Method for Predictive Queries. *Proc. Int'l Conf. Very Large Data Bases (VLDB),* 2003.

[33] Y. Tao, D. Papadias and Q. Shen.Continuous Nearest Neighbor Search. *Proc. Int'l Conf. Very Large Data Bases (VLDB),* 2002.

[34] G. Iwerks, H. Samet and K. Smith.Continuous k-Nearest Neighbor Queries for Continuously Moving Points with Updates. *Proc. Int'l Conf. Very Large Data Bases (VLDB),* 2003.

[35] K. Raptopoulou, A. Papadopoulos and Y. Manolopoulos. Fast Nearest-Neighbor Query Processing in Moving Object Databases. GeoInfomatica, vol. 7, no. 2, pp. 113-137, 2003.

[36] G.S. Iwerks, H. Samet and K. Smith. Maintenance of Spatial Semi join Queries on Moving Points. *Proc. Int'l Conf. Very Large Data Bases (VLDB),* 2004.

[37] Y. Tao, C. Faloutsos, D. Papadias and B. Liu.Prediction and Indexing of Moving Objects with Unknown Motion Patterns. *Proc. ACM SIGMOD*, 2004.

[38] J. Xu, X. Tang and D.L. Lee.Performance Analysis of Location Dependent Cache Invalidation Schemes forMobile Environments. *IEEE Trans. Knowledge and Data Eng*., vol. 15, no. 2, pp. 474-488, Mar./Apr. 2003.

[39] J. Zhang, M. Zhu, D. Papadias, Y. Tao and D.L. Lee. Location Based Spatial Queries. *Proc. ACM SIGMOD*, 2003

[40] http://searchnetworking.techtarget.com/definition/location-based-service-LBS

[41] Christian S.Jensen, Anders Friis-Christensen et al. 'Location-Based Services—A Database Perspective'.http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.78.459&rep=rep1&type=pdf

[42] R. G¨uting and M. Schneider, *Moving Objects Databases. Morgan Kaufmann Publications*, 2005.

[43] Shen-ShyangHo .*'Preserving Privacy for Moving Objects Data Mining'*.

[44] ArisGkoulalas-Divanis and Vassilios S. Veryki.'*Exact Knowledge Hiding through Database Extension' .IEEE Transactions on Knowledge and Data Engineering*, VOL. 21, NO. 5, MAY 2009

[45] 'Location-based service (LBS): Categories of Methods, Techniques and Technologies', March 2012.http://www.mediabuzz.com.sg/archives/2012/march/1529-location-based-service-lbs-categories-of-methods-techniques-and-technologies

[46] Samarati, Pierangela. '*k-anonymity', Foundations of Security Analysis and Design (FOSAD)*', 2008.

[47] Sabarish B A, Pradisa S, Nithyasri J. '*Privacy Preservation of Mobile Data using Matrix Transformation'. International Journal of Computer Applications*, Volume 87 - Number 14, 2014.

[48] Sabarish B A,Divya.C,HariniShankar '*Enhanced Privacy Framework for Privacy in Moving Objects'*, 2014. *International Conference on Computer Science and Engineering (ICCSE 2014), IPCSIT vol. 1 (2014) © (2014) IACSIT Press, Singapore.*

[49] Nikos Pelekis, AnargyrosPlemenos, ArisGkoulalasDivanis, DespinaKopanaki, MariosVodas, and YannisTheodoridis, '*A Benchmark Framework for Privacy Preserving Mobility Data Querying and Mining Methods', Extending Database Technology'*, 2012.

[50] O. Abul, F. Bonchi, and M. Nanni, '*Never walk alone: Uncertainty for anonymity in moving objects databases', Proceedings of ICDE*', 2008.