ISSN (Online) : 2319 - 8753
ISSN (Print)   : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st&22ndMarch Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

TRPF: A Trajectory Private- Preserving Frame Work for Participatory Sensing

Mejil Lieoncy.S[1], Muthusankar.B[2],Anitha.A[3]

Department of Computer & Communication Engineering, M.A.M College of Engineering, Tamilnadu, India.[1]

Department of Computer & Communication Engineering, M.A.M College of Engineering, Tamilnadu, India.[2]

Department of Information &Technology, M.A.M College of Engineering, Tamilnadu, India.[3]

Abstract- The ubiquity of the various cheap embedded sensors on mobile devices, for example cameras, microphones, accelerometers, and so on, is enabling the emergence of participatory sensing applications. While participatory sensing can benefit the individuals and communities greatly, the collection and analysis of the participators' location and trajectory data may jeopardize their privacy. Existing proposals mostly focus on participators' location privacy, and few are done on participators' trajectory privacy. The effective analysis on trajectories that contain spatial-temporal history information will reveal participators' and the relevant personal privacy. To propose a trajectory privacy-preserving framework, named TrPF, for participatory sensing. Based on the framework, improve the theoretical mix-zones model with considering the time factor from the perspective of graph theory. It analyze the threat models with different background knowledge and evaluate the effectiveness of proposal on the basis of information entropy, and then compare the performance of proposal with previous trajectory privacy protections. Finally, the results prove that the proposal can protect participators' trajectories privacy effectively with lower information loss and costs than what is afforded by the other proposals.

Keywords*–Trajectory, jeopardize, mix-zones, spatial-temporal information*

I. INTRODUCTION

With the development of wireless communication technologies such as WLAN, 3G/LTE, WiMax, Bluetooth, Zigbee and so on. Mobile apparatus are equipped with kind of embedded sensors surveyed in [1] as well as powerful feeling, storage and processing capabilities. Participatorysensing [2] whichprocess that endows individuals to assemble isinvestigated and share localized knowledge with their own wireless devices, emerges as required under these well conditions.

Compared with WSNs, participatory feeling boasts a number of benefits on deployment charges, accessibility, spatial-temporal treatment, power consumption and so forward. It has captivated numerous investigators in different localities such as smart Transportation System, healthcare and so on. There is lots of existing prototype systems and so on.

Nowadays, participatory feeling submissions mainly depend on the assemblage of datas over wide geographic localities. The sensor data uploaded by participators are invariably tagged with the spatial-temporal information when the readings were noted. According to the investigation in [3], the likely risks to a participator's privacy data that encompass supervising data assemblage positions, finding his/her trajectory, taking photographs of personal scenes and recording the intimate chat logs.

Once participators recognize the grave consequences with the disclosure of their perceptive data, they are reluctant to participate in the campaign and use the services. Since the success of participatory sensing crusade strongly counts on the altruistic method of data collection, if the participators are reluctant to assist their assembled data, it would dwindle the popularity and influence of this campaigns established at large scale while furthermore reducing the benefits to the users. Thus, the privacy difficulties are the significant barriers to data assemblage and distributing. How to double-check the participators' privacy is the most urgent task.

In usual participatory sensing applications, the uploaded data reports may reveal participators' spatial-temporal information. Analysts could get some valuable outcomes from the published trajectories for conclusion making, for demonstration, merchants may decide where to build a supermarket that can produce maximum profit by investigating trajectories of customers in a certain locality and the Department of Transportation can make an optimized vehicle arranging scheme by supervising trajectories of vehicles.

It may introduce serious threats to participators' privacy. Adversary may probably investigate the trajectories which comprise wealthy spatial-temporal annals data to connection multiple reports from the identical participators and work out certain private information such as the places where the data reports are collected. Therefore, it is essential to unlink the participators' identities from sensitive data collection locations. To best of our knowledge, living work on privacy in participatory feeling mostly focus on data assistance and describing process. If an adversary has a priori knowledge of a participator's trajectory, it is effortless to de-anonyms' his/her reports.

In TrPFtrajectory privacy-preserving framework usedfor participatory feeling. To observe that the positions on or nearby participators' trajectories may not all be sensitive, and with this thought, a proposal only agreements with the sensitive trajectory segments that will be discussed in the following. Moreover, mix-zones are regions [4], [5] where no applications can track participators' movements. Some works [6], [7] concentrated on road network mix-zones, which are not applicable in participatory feeling. For one thing, they all construct mix-zones at street intersection, which may constraint the random data assemblage time and the number of ingress/egress locations; for another thing, the trajectory segments at the road intersection may not be sensitive, while the others would be.

Thus, to improve the theoretical mix-zones form [4], [5]to construct trajectory mix-zones form for protecting sensitive trajectory segments from the viewpoint of graph theory. Compared with living trajectory privacy-preserving suggestions, my suggestion has benefits of lower charges and data decrease while the privacy level would not decline.

In TrPF, the major assistance of a work is summarized as pursues:

- To suggest a structure TrPF of participatory sensing for trajectory privacy protection;
- To improve the theoretical mix-zones form with considering time factor from the perspective of graph idea to construct trajectory mix-zones model for protecting participators' perceptive trajectory segments;
- To formalize privacy level metric, privacy loss metric and information loss metric, and then analyze the attack models with distinct backdrop knowledge;
- Compared with previous trajectory privacy protections, run a set of replication trials to assess the effectiveness of our suggestions and then make an evaluation of the presentation.

II. RELATED WORKS

In this part, the present state of the art of privacy-preserving methods is prescribed in participatory feeling. The first implementation of a privacy aware architecture, entitled AnonySense, for the anonymous task allocation and data describing is projected. From the perspective of cryptography, investigated the very sensible architectural assumptions and privacy obligations, and then supplied an instantiation that achieved privacy protection in participatory feeling with provable security.

Christian *et al.*[9] surveyed the privacy and security significances in three types of application scenarios. They investigated the privacy trials in participatory feeling applications in detail and surveyed the privacy protection in terms of data privacy protection, position privacy protection and trajectory privacy protection in position-based services. Liu [10] reviewed the definitions, the models and the appropriate position privacy protection techniques from the perspective of mobile data administration.

A. LOCATION PRIVACY PROTECTION

There are several works that survey the location privacy-preserving schemes. They classify them into the following aspects.

1)Dummy Locations: Mechanismplanned in [11], [12] mostly employ the idea of dummy positions to protect auser's location privacy. In preceding work [13] concentrated on the tradeoff between location and trajectory privacy protection and QoS founded on the dummy events.

2) Location k-Anonymity: Much of the work regarding position privacy protection derive from k-anonymity form which is first suggested by Sweeney in database [14]. For demonstration, spatial and temporal cloaking on the cornerstone of this form to defend position privacy was first suggested by Gruteser and Gruwald [15].Take the persons' obligations on location privacy into concern, suggested a scalable architecture for position privacy protection. It anticipated a prescribed structure to defend a user's anonymity when demanding location-based services. They supplied the safeguards that were specific for distinct types of information accessible to attacker.

3) Obfuscation: To defend a user's position privacy by deliberately degrading the correctness of his/her spatial-temporal information. Obfuscation is a class of the significant approaches in position privacy. Much of the work that belongs to it can be forced through perturbation or generalization [16].

4) Mix-Zones: Pseudonym is utilized to break the linkage between a user's identity and his/her events. The process of its change is generally performed in some pre-determined localities called mix-zones [4], [5] and the concept of construction mix-zones at street intersections has been suggested in [6], [7]. The troubles of optimal placement of mix-zones are investigated in, where rectangular or circular formed zones that routinely utilized by these mix-zones techniques.

To best of my information [6], [7] only take into account the effect of timing strike in the building process. In TrPF, take the time interval into consideration and improve the theoretical mix-zones form from the perspective of graph idea to defend the data collectors' trajectories privacy in participatory feeling

B. TRAJECTORY PRIVACY PROTECTION

To realize that one time a user's trajectory is identified, the user's positions are revealed. Some works [17], [18] have summarized the trajectory privacy protection methods, where the most direct and simple ways are dummy trajectories and suppression technique. To be specific, the former developed a dummy trajectory randomly from the starting point towards the place visited and the subsequent did it by rotating the user's trajectory. The trajectory similarity may affect the anonymity value.

Thus, how to develop dummy trajectories that look like a normal user's trajectory is one of the main challenges of this kind of work. To prevent adversary from inferring a user's unknown positions by utilizing his/her partial trajectory knowledge, it suggested a location suppression method to alter a database of trajectories, which can prevent the disclosure of the user's whole trajectory with high likelihood. Although, those trajectory segments that are stifled would origin the assembled data lost.

Trajectory k-anonymity that expands from position k-anonymity is broadly utilized in trajectory privacy protection. For convenience, only address some typical and recent studies. To assembly the trajectories founded on log cost metric and then enforce k-anonymity on each experiment position. Eventually, a random reconstruction procedure was offered to enhance anonymized trajectory privacy further. Inspired by the inherent uncertainty of localization, the concept of anonymity for wireless object databases, where comprised the possible location imprecision. Then, they suggested Never Walk solely (NWA) to achieve k-anonymity through clustering and space transformation. Specifically, when it had degenerated into the traditional micro-aggregation that restored trajectories by the trajectories clustering center over the identical time interval.

To anonymize wireless things with dynamic perceptive attributes, to accomplish the new notion of anonymity they suggested for wireless things through extreme amalgamation and symmetric anonymization.It exploited chronicled positions to construct trajectory k-anonymity and then offered algorithms for spatial cloaking.Huo [18], enquired the selection of trajectory anonymity sets based on graph partition. In the follow-up work, they suggested a procedure called You Can stroll Alone (YCWA) to advance NWA by anonymizing the stay points that were extracted efficiently on people's trajectories. They generated k-anonymity zone founded on two algorithms called grid-based approach and clustering-based approach.

As mentioned above, that dummy trajectories and almost all the trajectory anonymity techniques deal with the whole trajectory, which result in the increase of costs such as computation, storage and query with a certain privacy level. Sensitive location suppression technique may reduce the overhead costs with a same privacy level. If the sensitive locations on trajectories are suppressed too much, it might cause lots of information loss. Observe that not all the locations on the trajectory are sensitive. There have been some works to analyze the sensitive locations on or nearby the published trajectory. It projected a method to find interesting locations and frequent travel sequences in a given geographic region.

A method of clustering-based stops [19] and moves of trajectories to compute important places based on the change of the speed of the trajectory.In this works privacy is rarely considered. It distinguished the semantics of the visited place between sensitive and quasi-identifier places and proposed an algorithm for generalizing the visited place based on taxonomy. Near overcome the defects above, to propose a preferable trajectory privacy protection method to reduce the costs and information loss; meanwhile the privacy level will not decrease.

III. OVERVIEW OF TRPFSYSTEM

In this part, first depict the trajectory privacy preserving framework TrPF for participatory feeling and then focus the privacy problem with the revelation of users' trajectories. Eventually to define some basic notions.

A. THE ARCHITECTURE OF TrPF FOR PARTICIPATORY SENSING

Mix Network purposes as an anonym zing intermediary between Mobile Nodes and the Report Server that is widely utilized [8], [9]. Take [20] for example, it paths accounts by multi-hop transmission, adding hold ups and blending with the data from other causes to other destinations. Such process makes adversary can neither connection a wireless node's accounts together either identify which wireless node dispatched the report, or learn when and where the reports were described.

Based on [20], suggest a trajectory privacy-preserving framework TrPFfor participatory sensing scheme depicted as Fig.1. Contrasted with the preceding architecture, consider the component of participators' privacy and substitute the mix network with a Trusted Third Party Server constituent. Due to the exclusion of mix network, it will optimize the data accounts transmission. The addition of Trusted Third Party Server can function as a privacy-preserving agency, which can trade off the efficiency of data transmission and privacy protection. It can decrease the mesh jumps of data accounts transmission path by wireless mesh. According to the different functions of function characteristics, the main constituents of TrPF are made up of the following entities.

1) Data Collectors: Wireless Nodes are apparatus with the capabilities of feeling, computation, memory and wireless connection, which act as data collectors in participatory feeling scheme. They can be utilized for context-aware data arrest and conveyed along with each participator. The engagement of data collectors in this feeling crusade is voluntary. Any participator who likes to provide submission server with shared data desires to get a certificate from Trusted Third Party Server.

To prevent adversary from disguising as a legitimate participator to upload malicious datas, only the one who has been validated can access the participatory feeling scheme and upload his/her collected data reports. And formalize the data reports assembled by participator as, where comprises the identity of, position and Time is the spatial-temporal information tagged with the assembled datas that compose trajectories of data collectors.

2) Trusted Third Party Server (TTPs): In the direction of double-check scheme security and participators' privacy, TTPs shops participators' applicable information such as certificates and pseudonyms information. Certificates are utilized for verifying participators' validity so as to exclude malicious attacker. The revelation of the spatial-temporal information may also intimidate the participators' privacy. To eliminate the linkage between the participators' spatial-temporal data and their identities based on pseudonym technique.

*3) Report Server:*Report Server is to blame for dealing with two facets: (a) Interact with TTPs to verify the validity of the participators' identityby the certificates contained in the data reports; (b) Simplify the uploaded data reports such as data aggregation, and then drive the data reports to submission Server.

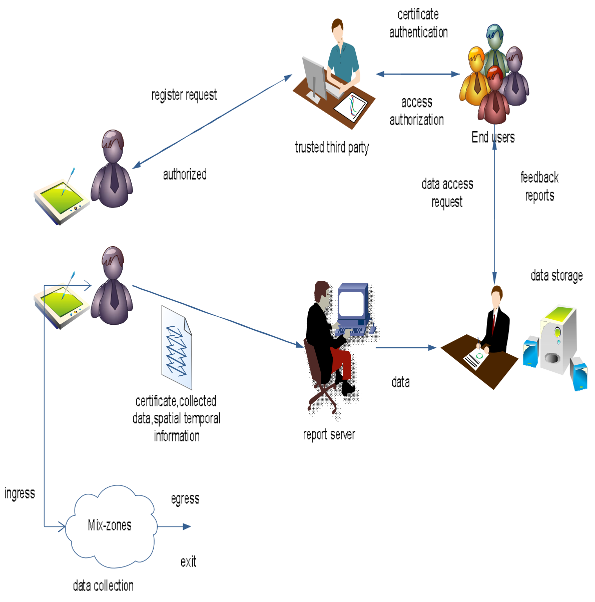

Fig.1. Architecture of TrPF for participatory sensing.

4) Application Server: Application Server actions as a data center. It can supply kinds of data services for end users and play the following functions: (a) *Data Storage:* store the processed data accounts received from data report server; (b) *Data distributing*: any legitimate end client can access the accessible data services; (c) *Data Publish:* release the data accounts for the end users to query.

In systemarchitecture, Application Server may be untrustworthy. It may leak participators' perceptive data to adversary. For demonstration, the revelation of participators' trajectories may show where the data reports are collected. Maybe some of the positions such as home address are sensitive. Adversary can use the published trajectories to connection participators' data reports with sensitive positions. As an outcome, the participators are cognizant that their privacy might be invaded seriously so that they may not desire to share their assembled data reports with end users.

*5) Queriers:*Queriers are end users that request sensor accounts in a granted participatory sensing submission, which can be individual users or community users. They access and consult the data accumulated by the data collectors according to their requirements. The queriers include, for example, data collectors are proposing to confer their own assembled data, medical practitioners ascertaining their patients' records, environmentalists querying the climate data of a certain locality or the general public for other purposes.

Note that only the registered end users can get access to the distributed data accounts. End users drive certificate authentication demands to TTPs. Any person who has listed before can get the access authorization and only and figures accounts that are supplied by data collectors.

B. PROBLEM STATEMENT

In participatory sensing system, data reports collected by participators are tagged with spatial-temporal information. Since thelocation information thatattached to the collected data reports are commonly shared, a prominent attack is thus the Trajectory Inference. For example, suppose an adversary learns through background knowledge that a data collector P_i has visited a specific location at a certain time t_i, while the location happens to be the only sample on P_i's trajectory at time t_i in the data reports. The adversary would synthesize this information to infer the whole trajectory of P_i, which may relate to a certain sensitive attribute.

Additionally, the analysis of trajectories over several data reports may help adversary to exploit the frequently visited locations and reveal participators' identities, e.g., a data collector usually spends the same time on arriving at a specific location from a fixed location every day in the morning. Adversary can use the frequent information to deduce the starting location in the morning may be his/her home and the location reached after the time may be the work place. Consequently, the participators' privacy would suffer a huge threat with the disclosure of sensitive locations.

On the way to prevent from linking participators' identities with their uploaded data reports, to propose a method to protect participators' identities and trajectories privacy from the perspective of graph theory based on mix-zones model and pseudonym technique. In fact, only parts of the locations on or nearby their trajectories are sensitive. Only need to protect the sensitive parts of participators' trajectories in their collected data reports.

IV.TRAJECTORY MIX-ZONES GRAPH MODEL

In trajectory mix-zones graph model, to suggest ananonymize sensitive trajectory segment from the perspective of graph idea. Toward decrease information decrease and charges at a certain privacy-preserving grade, split up the whole locality into several parts. According to the perceptive positions on or close by the trajectories, to split up the whole trajectories into perceptive trajectory segments and non-sensitive trajectory segments. Only defend sensitive trajectory segments based on mix-zones model and pseudonym technique.

Any Data Collector who goes into the Sensitive locality should choose a pseudonym provided by TTPs to anonymize thelinkability between his identity and his assembled data accounts. Meantime, they record their ingress and egress time. A participator's information recount as a tuple:

Ii = (IDp,R_i, S_i,$t_{ingress}$, Δt_{egress}), where IDp comprises the participator 's pseudonym supplied by TTPs, $R_i$is the mapping from participator's identity to his pseudonym, $S_i$is the sensitive locality the participator passes by,$t_{ingress}$ presents the set of participators' enter time and Δt_{egress} is the participator's egress time gap.

A. TRAJECTORY GRAPH CONSTRUCTION

To suggest the Trajectory Mix-zones as Directed Weighted Graph(DWG), which is formalized as G = {V,E}.V is the set of vertexes which are assembled by the pseudonyms supplied by TTPs. A participator goes into the sensitive locality with a pseudonym and leaves it with another pseudonym. It can be depicted as V = {(v_{11},v_{12},….v_{1n}),(v_{21},v_{22},….v_{2n})}.E is the set of perimeters that comprise the participators' trajectory mapping from the ingress to the egress in the sensitive area.As a result of pseudonym method, there may be some difficulties for adversary to connection the ingress and egress participator with the same identical.

In detail, DWG is an entire bipartite graph with distinct weights on each brim. The time of participators resides in mix-zones can either be unchanging or alter. Palanisamy*et al.* [7] analyzed the two distinct situations in street mesh. They sharp out that if the residence time was unchanging, it would meet First In First out (FIFO) strike. That is to state, the first exit participator corresponds to the first one that goes into the mix-zones and the pseudonym method takes no effect.

In TrPF, assume that the appearances of participators at the trajectory mix-zones follow a Poisson process. Given a time gap T,k participators go in the trajectory mix-zones with mean appearance rate λ to accomplish k-anonymity. Note that the time gap and the appearance rate decide the number of participators that goes into the trajectory mix-zones. Additionally, the participators' appearance time should not differ by a large worth, or adversary could infer the first go out might correspond to the first go in. The time of data collectors that spend in mix-zones is random.

B.WEIGHT CONSTRUCTION ALGORITHM

A participator v_i goes into the mix-zones at time $t_{ingress}$(vi) and exits the mix-zones in a time interval from t_j to t_{j+1}. Let P(v_i,t) present the likelihood of participator exits the mix-zones in above-mentioned time gap [t_j,t_{j+1}] .P(v_i,t) numerically identical with to the likelihood that participator v_i takes data collection time in mix-zones from $t_j - t_{ingress}$(vi) to $t_{j+1} - t_{ingress}$(vi) . The data assemblage time in mix-zones Δ'(t) pursues normal distributions Δ'(t)~ N(μ,σ).

Similarly, the other participators go out in the time gap [t_j,t_{j+1}] can be computedas overhead. Thus, the likelihood of all participators exit in the gap time can be computed by

$$P(v', t) = \sum_{i=1}^{k} \mathrm{P}(V_i\,, \mathrm{t}) \qquad (1)$$

However, only one of them is the genuine participator. Therefore, the probability that participator v_i exits in [t_j, t_{j+1}] is v_i , denoted as P (v_i[t_j, t_{j+1}]) is granted by the following conditional probability

$$\mathrm{P}\big(V_i\,[\mathrm{t}_j\,,\mathrm{t}_{j+1}\,\big) = \frac{\mathrm{P}(V_i\,,\mathrm{t})}{P(v',t)} \quad , \quad i = 1{,}2, \ldots..k \qquad (2)$$

Each participator enters with one of the pseudonyms and exits the sensitive area with a different one after he/she finishes thedatacollection.

V.METRIC

A.PRIVACY LEVEL METRIC

Privacy level metric can achieve based on Information Entropy. The concept of information entropy defined by Shannon [21] is a quantitative measure of information content and uncertainty over a probability distribution. In this paper, the probability distribution represents the chance that adversary can identify each participator. The more uniform the probability distribution is, the higher the information entropy is and the more difficult the real participator can be identified. Otherwise, if there is a significant difference in the probability distribution, it will be easy to confirm the real participator for the low information entropy. Thus, it is feasible to measure the trajectory privacy level can achieve using information entropy.

B.PRIVACY LOSS METRIC

Privacy loss is defined as the probability that an adversary will be able to gain sensitive trajectory segment about a participator. It could be calculated by combining the identity leakage and the pseudonym mapping index

C.INFORMATION LOSS METRIC

Information loss is defined as the reduction in the probability with which people can accurately determine the position of an object. The sum of area size of anonymity regions are used to measure the information loss. It can be computed by (3).

$$IL = \sum_{i=1}^{k} \sum_{j=1}^{n} \mathrm{Area}\{\ \mathrm{S}\big(o_i, t_j\big)\,\} \qquad (3)$$

Where IL represents the information loss with different number of trajectories, Area{S(o_i,t_j)} represents the area size of the generalized regions of o_i at time t_j, k is the number of trajectories and n is the number of timestamps in anonymity regions.

VI. PERFORMANCE EVALUATION

TABLE 1:Two Groups of Statistical Parameters

Ingress time Interval(T)	Arrival rate (λ)	Time interval Parameter(μ,σ)	The number of participators(k)
0.5	5	(2.5,0.5)	5
1	10	(3,1)	20

Two groups of experiments with different statistical parameters are shown in Table I. As a result of participators' different arrival rates λ = λ (5, 10) depict, the number of participators that enters the mix-zones is different. Specifically, to ensure k-anonymity, consider the number of participators with [2λT] , which is showed in Table I during ingress time interval T=T(0.5,1). The arrival time should not differ at a large value so as to prevent from time attack. The probability density function of time interval in mix-zones with (μ, σ) = {(2.5, 0.5) (3.1)}. The weight of edge is each probability mapping from the ingress pseudonym to the egress pseudonym.

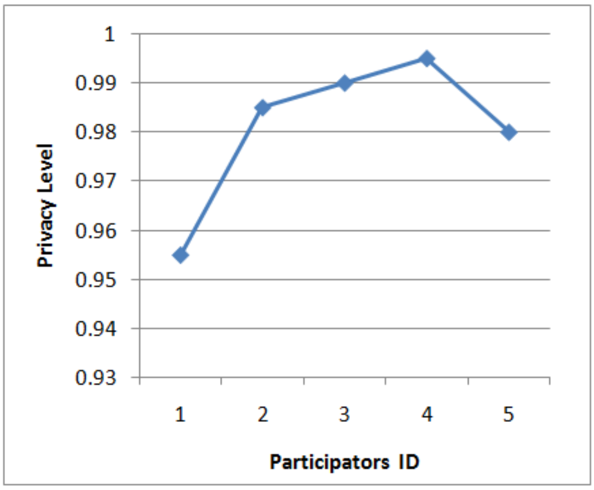

Fig.2 Privacy Level

As mentioned, the uncertainty of mapping among pseudonyms can be evaluated. According to the discussion, the maximum entropy achieves if and only if the mapping probabilities are equal. In this paper, to improve the theoretical mix-zones model with considering the time factor. The maximum entropy and actual entropy can be computed according to the probability distributions depict correspondingly. The probability distributions represent the probabilities of k participators that exit trajectory mix-zones at each egress time interval. More uniform of the mapping probability distributions are, the higher the actual entropy is. When the mapping probabilities are equal, the maximum entropy achieves.

Privacy level can be calculated depicted by Fig.2.It evaluates the privacy-preserving level. The higher privacy level is, the stronger the trajectory privacy-preserving scheme. Consequently, the privacy leak is lower. Moreover, once define the privacy level, it is important to measure the privacy loss. Considering a given participator such as P_{11}, demonstrate the privacy loss of a model compared with the theoretical mix- zones model according to the computational model proposedin Section V-B. As illustrated by the results, in the theoretical mix-zones, the mapping probabilities of P_{11} from the ingress pseudonym v_{11} to the egress pseudonym v_{2i}, i=1,2,...k are the same.

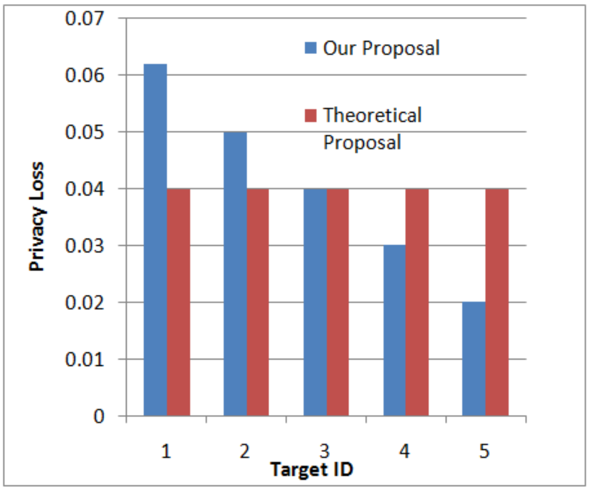

Fig.3 Privacy Loss

Thus, the privacy loss is the same whatever the target pseudonym the ingress pseudonym is mapping near. However, when taking the other factors such as time interval in the mix-zones into consideration, the privacy loss is different for the different probabilities of mapping index. Additionally, Fig.3 the privacy loss decreases with the number of participators in the mix-zones increases.Furthermore, discussion based on the number of participators that enters the mix-zones k will changes with the arrival rate λ and ingress time interval T changing. Clearly, the number of participators increases along with the increase of arrival rate and time interval.

Evaluate the average entropy with various values of arrival rate λ and ingress time interval T under the same experimental setting in Table I. The average entropy of the mix-zones increases with the increasing of the number of participators. That is because a large number of participators raise the uncertainty of the mix-zones. Consider the maximum mapping probability as the adversary success probability. As for a certain data collector such as P_{11}, presents the success probability of an adversary in guessing and tracking P_{11} under the two groups of parameters.

Obviously, the first group makes easier for the adversary to guess and track than the second one based on their time intervals. That is because there are less data collectors for lower entropy of the first group than that of the second one in the same time interval. Additionally, we analyze the effects of arrival rate λ to adversary success probability under the same collection time. Since a larger arrival rate may increase the number of data collectors in the mix zones, the adversary success probability in guessing and tracking P_{11} decreases.

ACKNOWLEDGMENT

I would like to express my special thanks of gratitude to Mr.A.Shenbagarajan as well as our guide Ms.A.Anitha who helped me in completing my work. Secondly I would like to thank my parents, my friends and well wishers who were a constant source of Inspiration.

VII. CONCLUSION

Disclosure of personal data privacy collection trends of major risks country. Countries can help provide the data. In this paper, a system of protection of privacy TRPF propose a trend in the sense of participation. Then, from the point of view of trends protect countries idea map suggests a tendency to form mixed zones map. Into account the model time factor is to improve mixing zones. It may be more realistic in practice.

Third, lack of privacy and individual definition quality measurement metrics privacy in terms of lack of information, knowledge of the background of the distinct forms of risk analysis. Finally, group of single parameters uses the metric to assess the efficiency and effectiveness of our business model diagram of mixing zones. Go to map the effects of mixing zones in the form of replication effectively trends Country protect the privacy and other programs that can be verified by comparing the data loss and reduce costs.

REFERENCES

[1] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. campbell, "*A survey of mobile phone sensing*," IEEE Commun.Mag., vol. 48, no. 9, pp. 140–150, Sep. 2010.

[2] J. A. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava, "*Participatory sensing*," in Proc. Work- shop on World-Sensor-Web (WSW'06): Mobile Device Centric Sensor Networks and Applications, 2006, pp. 117–134, ACM.

[3] D. Christin, A. Reinhardt, S. Kanhere, and M. Hollick, "*A survey on privacy in mobile participatory sensing applications*," J. Syst. Softw., vol. 84, no. 11, pp. 1928–1946, 2011.

[4] A.R. Beresford and F. Stajano, "*Location privacy in pervasive computing*," IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, 2003.

[5] R. Beresford and F. Stajano, "*Mix zones: User privacy in location-aware services*," in Proc. 2nd IEEE Ann. Conf. Pervasive Computing and Communications Workshops, 2004, pp. 127–131, IEEE.

[6] J. Freudiger, M. Raya, M. Flegyhzi, P. Papadimitratos, and J. P. Hubaux, "*Mix-zones for location privacy in vehicular networks*," in Proc. 1st Int. Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS 07), Vancouver, BC, Canada, 2007.

[7] B. Palanisamy and L. Liu, "*Mobimix: Protecting location privacy with mix-zones over road networks*," in Proc. IEEE 27th Int. Conf. Data Engineering (ICDE), 2011, pp. 494–505.

[8] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "*Anonysense: Opportunistic and privacy-preserving context collection*," Pervasive Comput., vol. 5013, pp. 280–297, 2008.

[9] D. Christin, M. Hollick, and M. Manulis, "*Security and privacy objectives for sensing applications in wireless community networks*," in Proc. IEEE 19th Int. Conf. Computer Communications and Networks (ICCCN), 2010, pp. 1–6.

[10] L. Liu, "*From data privacy to location privacy: Models and algorithms*," in Proc. 33rd Int. Conf. Very Large Data Bases (VLDB2007), 2007, pp. 1429–1430, VLDB Endowment.

[11] H. Kido, Y. Yanagisawa, and T. Satoh, "*An anonymous communication technique using dummies for location-based services*," in Proc. Int. Conf. Pervasive Services, 2005, pp. 88–97.

[12] H.Lu, C.S.Jensen, and M.L.Yiu,"*Pad:Privacy-area aware, dummy-based location privacy in mobile services*,"in Proc.7th ACM Int.Workshop on Data Engineering for Wireless and Mobile Access, 2008, pp. 16–23, ACM.

[13] S. Gao, J. Ma, W. Shi, and G. Zhan, "*Towards location and trajectory privacy protection in participatory sensing*,"inProc.Mobile Computing, Applications and Services, Los Angles, CA, USA, 2011, pp. 381–386.

[14] L.Sweeney, "*k-anonymity: A model for protecting privacy*, "Int.J.Un-certainty Fuzziness and Know.Based Syst., vol.10,no.5,pp.557–570, 2002.

[15] M. Gruteser and D. Grunwald, "*Anonymous usage of location-based services through spatial and temporal cloaking*," in Proc. ACM 1st Int. Conf. Mobile Systems, Applications and Services, 2003, pp. 31–42.

[16] Ardagna, M. Cremonini, E. Damiani, S. De Capitani Di Vimercati, and P. Samarati, "*Location privacy protection through obfuscation- based techniques*," Data and Applications Security XXI, pp. 47–60, 2007.

[17] Y. Chow and M. F. Mokbel, "*Trajectory privacy in location-based services and data publication*,"ACMSIGKDD Explorations Newsletter, vol. 13, no. 1, pp. 19–29, 2011.

[18] Z. Huo, Y. Huang, and X. Meng, "*History trajectory privacy-preserving through graph partition*," in Proc. ACM 1st Int. Workshop on Mobile Location-Based Service, 2011, pp. 71–78.

[19] A.T. Palma, V. Bogorny, B. Kuijpers, and L. O. Alvares, "*A clustering-based approach for discovering interesting places in trajectories*," in Proc. 2008 ACM Symp. Applied Computing, 2008, pp. 863–868, ACM.

[20] A.Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "*Anonysense: Privacy-aware people-centric sensing*," in Proc. ACM 6th Int. Conf. Mobile Systems, Applications, and Services, 2008, pp. 211–224.

[21] C.E.Shannon, "*A mathematical theory of communication* ,"ACMSIG-MOBILE Mobile Comput. Commun. Rev., vol l.5, no.1,pp.3–55,2001.