Future Challenging Issues in Location based Services

Amit Kumar Tyagi
Research Scholar
Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry-605014, India.

N.Sreenath, Ph.D
Professor
Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry-605014, India.

ABSTRACT
The fast advances of mobile devices and positioning technologies has led to the flourish of Location-Based Services (LBS), in that people want to enjoy wireless services everywhere like in hotels, colleges, etc. LBS, the branch of computer program level services used in various fields and support, the application are broadly classified as Maps and Navigation, Information service, Tracking service, Social networking, Games, Vehicular navigation and Advertising etc. Now a days, LBSs attract millions of mobile users for example include POI finders such as Qype, which help the users to find the next POI such as bars or cinemas, and enrich the provided information. But during this communication, Security and Privacy of personal location information (of LBSs users) is becoming an increasingly important issue for future. So concerning it (privacy) as an important issue, discusses several privacy preserving location issues for vehicular (mobile) users (since knowledge of a vehicle's location can result in leakage of sensitive information). Location privacy for mobile users is mainly determined into two levels such as internally by a device or externally by systems and kind of networks with which the device interrelates. Users wish to maintain the vehicle's information is known only to those legally authorized to have access to them and remain unknown to anybody unauthorized. Hence the purpose and contribution of this paper is to discussed about various privacy and challenges issues in LBSs increasing in future that have not been published in the any research journal so far.

General Terms
Location Privacy, Location Based Services (LBSs), Security.

1. INTRODUCTION
Technological advancements in mobile computing have spawned a growth in location based services. Such services use the location information of the subscriber to provide better functionalities. Improper usage of location information may compromise the security and privacy of an individual. Providing a single definition of privacy is difficult. But as for Definitions of privacy, (a) Personally Identifiable Information (PII) - "PII" is information that we can use to identify you as an individual. PII includes your name, address, telephone number and any other information that is connected with you personally. (b) "Site(s)" means the website for which the e-Trust is endorsing the privacy policy. *As other definition, Beresford and F. Stajano defined location privacy as "the ability to prevent other parties from learning one's current or past location" [11]*. Here privacy means "for all application" even not limited for human being only i.e. privacy means "hide yourself from others" i.e. hiding your personal information from unknown/unauthorized activities. Moreover this, Privacy can be distinguished as *hard privacy* and *soft privacy*, as proposed by Danez is [15]. The data protection goal of hard privacy refers to *data minimization*, based on the assumption that personal data is not divulged to third parties.

Soft privacy, on the contrary, is based on the assumption that data subject lost control of personal data and has to trust the honesty and competence of data controllers. The data protection goal of soft privacy is to provide data security and process data with specific purpose and consent, by means of policies, access, control, and audit. .Security is too often viewed as a purely technical issue [15, 20]. Most of the people think security and privacy are same thing. Actually both terms have different meaning but they are inextricably related. Security is a process, privacy is a consequence. Security is action, privacy is a result of successful action [20]. Security is a condition, privacy is the prognosis. Security is the strategy, privacy is the outcome. Privacy is a state of existence, security is the constitution supporting the existence [20]. Security is a tactical strategy, privacy is a contextual strategic objective. Security is the sealed envelope, privacy is the successful delivery of the message inside the envelope. Security and privacy are two integrated issues in the deployment of vehicular networks. Privacy-preserving authentication /techniques are key techniques to addressing these issues for example mix-zone, k-anonymity [3, 11, 19] etc.

The essential aim of this paper is to discussed about only privacy's issues challenges etc. LBS provides services to VANETs users about any location whatever they need for example coffee shop, etc. VANET is developed to support Car-to-Car (C2C) and Car-to-Infra (C2I) communication. For many years, global researchers and projects have been investigating VANETs research issues: *routing, security, address allocation etc. [1, 5]*. Because vehicle is an extremely personal device and so its communication data should be secured and driver's privacy should be unrevealed from malicious users [13].

Generally an extensive survey of personal privacy [4, 7] was first carried out by Privacy International as part of the Global Internet Liberty Campaign. The original 1998 report is now revised and extended on a yearly basis by both Privacy International and the Electronic Privacy Information Center (for the 2003 report [21]). It identifies four broad personal privacy categories which are as [22]:

- **Information privacy:** it contains protection of data containing personally-identifiable information; for example: personal data include medical records, bank statements and governmental data.
- **Bodily privacy:** in this, protection of people from physical invasion; for example: bodily invasion include drug tests, cavity searches and genetic testing.
- **Privacy of communications:** in this, protection of all forms of communication from interception; for example: interception include monitoring telephone, email and written correspondence.
- **Territorial privacy:** in this, protection of domestic, work and public space from intrusion; for example:

intrusion include search warrants, video surveillance and identity checks.

Based on privacy's definition, three elements directly related to the property of location privacy, which are:

- Adversary
- Individual
- Location information

Now here we categorize inference-prevention techniques in the following classes:

- *Identity privacy* techniques attempt to forestall the re-identification of users (deprived of their real identity) in LBSs providing anonymous services
- *Location privacy* techniques apply to forestall the transmission of *exact* users' positions to the LBS provider. Knowing precisely the positions in which individuals are located (or not located) jeopardizes their privacy and physical safety.
- *Semantic location* privacy techniques aim at preventing the disclosure of the places in which users stay because those locations can reveal sensitive data and behavioral information.

Hence to provide a secure communication and higher desired level of location privacy to LBSs user is the main issue of this paper.

Location-based services (LBSs): With the rapid development of wireless and positioning technologies has led to the flourish of Location-Based Services (LBS), in that people want to enjoy wireless services everywhere like in hotels, colleges, etc. Other example are friend finder services such as Loopt [2], which determine all friends in the vicinity of a user, or geo-social networks such as Facebook Places [3] or Foursquare [4], where users "check-in" to bars, restaurants, etc. to share their current position with friends. Besides check-ins at individual locations, more and more users also share their complete movement trajectory, for instance, showing their last hiking trail or jogging path. Although these services are very popular, their usage can also raise severe privacy concerns as shown in [18] for example revealing precise user positions may allow an adversary to infer sensitive information if a user visits, for instance, a hospital or a night club. For that, *First* we need to know, which information the user actually wants to protect, i.e., his privacy goal. *Second*, we need to know what kind of information is available to an attacker and "how an attacker could use this information to infer private user information w.r.t. the defined protection goal". Perfect privacy is clearly impossible as long as communication takes place. But moreover this, most location service providers probably have good intentions with their services. Hence Location privacy is an important issue in vehicular networks since knowledge of a vehicle's location can result in leakage of sensitive information [7].

Hence as Contribution of this paper, it is twofold: (a). we explain privacy requirement arise in LBS for vehicle users. We consider in some detail, Location privacy is becoming increasingly pervasive issue. Moreover, this paper can represent various factors of privacy-aware. This first contribution provides the background knowledge and the motivation of the work. (b). we outline the privacy issues and challenges to a secure framework providing the higher privacy service i.e. unrevealing of information by malicious users in nil. We define the key points of location privacy issues and for each of them we describe research challenges also, the current state of- the-art, and propose directions of research. And this paper organized as; section 2 discusses about general privacy requirements in LBS. In Sections 3, we discusses privacy issues that particularly aims to protect privacy of the participants. Section 4 and section 5 discussed about privacy challenges, future and future research problems**.** Finally sections 6 conclude this paper in brief.

This paper interchangeably use 'mobile users', 'VANET users' vehicle users, and vehicle

2. GENERAL PRIVACY POLICY REQUIREMENTS

Too often privacy is considered a purely legal issue, the responsibility for which is often handed to organizational legal counsel. Privacy, Trust and Security all are related terms in each and every one i.e. Security is a process, privacy is a consequence. Security is action, and privacy is a result of successful action [20]. And trust include privacy with a) Application-level confidentiality and integrity aspects, example, for content that is owned by the relying party or third parties. b) Protection against attacks on components that are not related to identity management [25].

The fast advances of mobile devices and positioning technologies has led to the flourish of Location-Based Services (LBS). Location base services, the ability to determine geographical position, is an emerging technology with both significant benefits and important privacy implications for vehicle users. LBS, the branch of computer program level services used in various fields and support, the application are broadly classified as Maps and Navigation, Information service, Tracking service, Social networking, Games, Vehicular navigation and Advertising etc. [7] i.e. now days LBSs are becoming an important source of revenue for operators of mobile networks. Improper usage of location information may compromise the security and privacy of an individual. So we should protect vehicle user information /identity from unwanted /malicious entities. To provide desired level of privacy to LBS users, it must consist:

a) Treat all Personally Identified Information (PII) [30] gathered on the site in accordance with the privacy policy. During this, a user of the site must be given the option of not giving their PII if the information collected is not related to the primary purpose for which the information was collected or the PII was disclosed to third parties [32]. And user's choice about PII should be disclosed to third parties must be honoured. The user must also have the means to change their choice.

b) Can use third party PII to send a one-time email message to the person to whom the information concerns to solicit their consent to using their PII.

c) All newsletters and promotional email messages that are sent to users, apart from the messages the user has agreed to receive as a condition of using your service, must include an unsubscribe link [31].

d) If the user has stated that he/she is under 13 years of age you should not collect any PII on your site without the knowledge and permission of their parent or guardian [31]. If there are certain web pages within your Site that require users to be at least 13 years of

age, anyone under the age of 13 should be restricted from participating in such web page activities.

e) Take reasonable steps when collecting, creating, maintaining, using and disclosing PII, to assure that the data are accurate, complete and timely for the purposes for which they are to be used [29]; and you also implement reasonable security procedures, such as encryption, to protect personally identifiable information.

f) Provide a link to the Privacy Policy from the home page or any page collecting PII.

As discussed above, Perfect privacy is clearly impossible as long as communication takes place between vehicle users in LBSs, but to achieve high privacy protection, various privacy policy requirements are discussed as [29]:

a) It is possible to use pseudonyms as identifiers instead of real-world identities and possible to change these pseudonyms. Generally the number of pseudonym changes depends on the application and its privacy threat model [28]. Pseudonyms used during communication can be mapped to real-world identities in special situations.

b) A set of properties and/or privileges can be cryptographically bound to one or more pseudonyms.

c) Full description of how users of the site can contact to the licensee and e-Trust regarding licensee's privacy policy or for token generation.

d) Inform the users about any third parties, either on your behalf or for themselves that are collecting PII through the site. In some cases, depending on the nature of information, these third parties will also need to have an e-Trust privacy certification [28, 30]. And also inform the users "how the Personally Identified Information (PII) collected through the site is used" and "how to access and change the PII provided by them to you" [29].

e) What tracking technology, if any, (example cookies) is used on the site. And get information about how PII collected by the site.

f) Inform the users that all PII gathered can be disclosed to judicial or other government agencies subject to warrants, subpoenas or other governmental orders [29]. And also inform users that PII posted by them in online bulletin boards, chat rooms, and news groups or other public forums may be displayed publicly.

g) Inform users of the notification procedures w.r.t any changes in privacy policy and use of the user's PII. Also, the means by which the users can take appropriate action concerning this change.

h) If any PII is disclosed to third parties to facilitate the primary purpose it should be declared in the privacy policy [2].

i) If payment information is collected by the site the details of this, and how it is secured should be stated. If no payment information is collected best practice is to state this [29].

j) Detail the ownership transfer or data destruction that will occur in the event of a merger, likewise in the event that the business declares bankruptcy or ceases trading.

This section dealt with requirements required to measure /provide higher location privacy to LBSs users. Now next section 3 contains information regarding to privacy issues arising in location based services.

3. PRIVACY ISSUES

With the growth of wireless and mobile technologies i.e. an increase in location-based services (LBSs). Although LBSs provides enhanced functionalities, they open up new vulnerabilities that can be exploited to cause security and privacy breaches. As definition of location privacy, privacy is "the ability to prevent other parties from learning one's current or past location" [11]. Among all LBS categories, Location privacy becomes extremely critical when the user's location information reveals his personal attributes, example, special diseases, hobby, or home address etc. Hence this section discusses about various privacy issues existed in location based services as [27]:

a) Should users of location-enabled devices be informed when location tracking is in use? Should they be permitted to turn it off? Should an opt-in or opt-out approach be used? What factors will determine these answers?

b) Should users of location-aware devices be permitted to control the storage of location information?

c) Should location information as stored be personally identifiable [27], or should the user have options to preserve degrees of anonymity?

d) What legal protection should a person's historical location information have against unreasonable search and seizure?

e) Should there be other controls governing aspects of stored location information, such as verifying accuracy, specifying retention periods, requiring particular levels of security, etc.?

f) Does the use of location information by a second party such as a communications carrier, [27] even if not disclosed to third parties, create the potential for unfair advantage for those carriers or abusive use of the information by those carriers?

g) To what extent should users of location enabled services be allowed to choose their own level of identifiability /anonymity?

h) What level of disclosure control should be dictated by government regulation? By the affected individual customers, users, etc.? By other parties?

i) What governmental legislation and regulation is appropriate to assure citizens' rights of privacy in an era of location-aware mobile devices?

j) Will non-governmental, voluntary standards be sufficiently strong and sufficiently accepted by industry and consumers to be effective?

k) Will industry/trade group standards [12, 14] be sufficiently strong and sufficiently accepted by industry and consumers to be effective?

l) Will advocacy/public interest groups be capable of sufficiently monitoring the burgeoning location-aware industries [27], and sufficiently effective in protecting the public's interests?

m) Will consumers demand, and will suppliers provide, privacy-related capabilities, features, and policies with their products and services that are sufficiently strong and accepted to be effective?

This section dealt with the main contribution points of this paper i.e. privacy issues in detail. Now next section discusses privacy challenges issues arising in LBSs for vehicle users.

4. PRIVACY CHALLENGES

Most of the people think security and privacy are same thing. Actually both terms have different meaning but they are inextricably related like security is a process, privacy is a consequence. Security is action, privacy is a result of successful action [20]. Now this paper have sketched vision for an information processing world where individuals can retain control over their information. As challenging, the first challenge in location privacy research is the increasing need for understanding various location privacy vulnerabilities through the development of privacy threat models and the corresponding defense methods. Location privacy research is still in fundamental level. The second challenge is to develop a unifying framework for supporting privacy in all types of LBSs in order to enable wide deployment of location privacy protection solutions and techniques. Of course, the challenges to achieve this vision are huge, and in closing mention some as:

4.1 Interfaces for Entities, Agents and Humans

Adequate programmatic interfaces need to be defined for entities, agents, agencies, predicate evaluators and notaries. Agent interfaces for dealing with information types will have generic and application dependent parts [26] for example an agent may be asked to create a service handle that is limited for one day (a generic restriction) or a handle that only allows charges of up to 100 dollars (application specific for money-related handles). Traceable copies of data may require embedding of application-dependent fingerprints [26]. It will be important to explore application specific controls and services that would be useful. Human interfaces must be invented that enable people to describe their privacy goals and select appropriate policies for their agents. The interface must also educate people about risks of their options. The recent work on privacy interfaces for ubiquitous computing will be useful here. Research there has highlighted that individuals tend to release information subjectively while weighing in factors like information function, information sensitivity, and trust in recipient [26] which mirror our owner type level of control dimensions.

There has recently been an interest in exploring the nature of privacy as a value determined by market forces [26]. Instead of a declarative policy, individuals in this model may be willing to relax their level of control in return for a fair compensation. How can such schemes be incorporated in the interface, and indeed, the framework?

4.2 Reasoning about Information Privacy

While we have presented a few useful points in the *ownership - type - level of control* spectrum, it is important to specify information work flows for a variety of interactions and formally reason about privacy guarantees as an aggregate of an entity's interactions.

In main design, we postulated that each entity will log *all* interactions it has participated in with other entities. The agent will use an entity's log to pre-process (or even abort) current interactions to prevent violation of the entity's privacy policies. An entity can query its logs to deduce the personal information that has been released to a particular entity. However, such logs will quickly grow to be quite large. Efficient log management, analysis and summarizing algorithms will need to be invented to allow online entity interactions to be fast. Can we design interactions with properties (for example, TRIM) that reduce the size of logs? Analysis of logs and auditing of P4P queries will require extending statistical databases techniques for audit of aggregate queries in new directions. Furthermore, how would such an audit scheme work against an open-world adversary with its knowledge of auxiliary datasets that may not be currently known to the individual's agent?

4.3 Architecture of a Privacy Agent/Agency

We touched upon various privacy policy requirements in designing privacy preserving protocols in Section 2. Perhaps the recent advances [26] in designing efficient group signatures [4, 7] for anonymous authentication can be used to devise a Notary Protocol? A group signature scheme allows a member M of a group G to sign messages on behalf of G such that the resulting signature does not reveal M's identity. Some schemes should allow the individual to increase the level of anonymity of interactional data by using various information hiding schemes (example, k-anonymity [4, 9], perturbation [7]). The infrastructure should, however, provides statistics to indicate the level of anonymity achieved. How can such statistics be maintained?

4.4 Trust Management

It will be important to understand the interactions between the P3P privacy policies and our privacy control mechanisms. The P3P framework still plays an important role in describing how trusted organizations will manage data they own or have a copy of. Perhaps the agency can play a role in managing trust for the entities it represents [26]. For example, the agency can track privacy breaches (for example, misuse of limited-use emails or pseudonyms) by organizations and assign them "trust ratings". Such trust ratings can be used by individuals to determine policies for their interactions with an organization.

4.5 Secure Society

Individual privacy and societal security are sometimes at logger heads with each other. For example, the "no integration" level of control precludes, among other things, the construction of credit reports and profiling of criminals. Such integration of information without the individual's intervention is essential for a smooth functioning of society [26]. The moral dilemma here is akin to the one faced by designers of mechanisms to ensure communication privacy: the technology is of as much use to drug traffickers, terrorists and subversive elements as to law abiding citizens. Can the P4P framework be designed with sufficient "hooks" to allow law-enforcement agencies to monitor interactions that hamper societal security?

4.6 Others

The offering of LBSs requires an in depth knowledge of the subscribers' whereabouts. Thus, with untrustworthy service providers the deployment of LBSs may breach the privacy of the mobile users for example, a service request originating

from the house of a user. The request contains sufficient information to identify the requester, even if it lacks of any other identification data for example, the user ID, the user name, etc. [16]. This is true since the mapping of the exact coordinates that are part of the user request to a publicly available data source of geocoding information can reveal that the request originated from a house and thus increase the confidence of the service provider that the requester is a member of the household. Moreover, if a series of requests for LBSs are matched to the same individual then it is possible for the service provider to identify places that this user frequently visits, reveal his/her personal habits, political/ religious affiliations or alternative lifestyles, as well as build a complete profile of the user based on the history of his/her movement in the system [6, 16]. Consequently, without the existence of strict safeguards, the deployment of LBSs and the sharing of location information may easily lead the way to an abuse scenario, similar to Orwell's Big Brother society. To avoid this situation and adequately protect the privacy of the users when requesting LBSs, sophisticated algorithms have to be devised [16].

Hence this section dealt with privacy challenges arises in LBSs (in future) in detail. Now next section dealt with future research work to be done as for further research.

5. FUTURE RESEARCH VIEWS

Location privacy is defined as the ability to prevent other unauthorized/malicious parties from learning one's current or past location. Improper usage of location information may compromise the security and privacy of an individual. Location privacy research is still in fundamental level. Although many research efforts have been focused on privacy-preserving LBS, there still exist many open research issues and challenges in this area that including: (1) unlink ability problem; (2) wireless link breakage problem (3) Collusion of malicious users trouble; (4) broad cast storm problem (5) Operation in multiple responder; (6) Identity privacy (7) safety problem (8) LBS server difficulty; and (9) Middleware network issue 9) Jointly consider both traffic characteristic and different levels of protection demands for potential mix zone locations. (10) Design secure and efficient communication and coordination protocols to achieve distributed establishment of mix zones.(Since various model relies on a trusted central authority, it may not be suitable for some distributed communication scenario, where mobile devices communicate in ad-hoc fashion and central authorities are not available) (11) Strategically insert dummy users in the system as well as maintain traffic and protection level requirements to handle the situation that there are few users in the system. (12) Provide any guidelines to the mobile users for specifying their privacy preferences.

Although many research efforts have been focused on privacy-preserving LBS. But still there too many open research issues existed in this area that can be discussed as:

A. From User's prospective: Existing privacy-preserving LBS frameworks are designed from the technology's prospective. There is still need to study the location privacy issue from the user's prospective for example, how can a casual user define privacy requirements? Is it possible to define privacy levels as low, medium, and strict, and then users would choose among them? How can a user achieve a trade-off between the privacy requirements and the quality of services? How can the user evaluate the privacy risk she has from using a certain LBS [17].

B. Privacy-aware location-based query types: Existing privacy-preserving LBS frameworks support only private range and nearest-neighbour queries over public or private data [17]. One of the future directions is to extend existing frameworks to support other kinds of location-based queries, for example: reverse nearest-neighbour queries [17] and aggregate nearest-neighbour queries where the query processor does not know the actual location information about the query and/or data.

C. Privacy scores: there is no standard procedure to measure privacy score, means how much privacy need to a user in term of scores.

D. Road networks environments: Existing location privacy techniques mainly consider the Euclidean space where users can move freely. In reality, most of the object movement is constrained by the underlying road network. Applying existing location privacy techniques directly to the road network environment is not practical as adversaries would have more information about the possible user locations, derived from the knowledge of the underlying road network [17]. Thus, it is important to design new specialized location anonymization and privacy-preserving query processing techniques for road network environments.

E. Privacy measures and adversary attacks: There is a need to define a formal privacy measure and adversary attacks of anonymized location information in different environment settings, [24] for example: the Euclidean space, road network, and wireless sensor networks, and for different privacy-aware query types, example, static and continuous queries. Such measures and attacks can be used to evaluate the degree of privacy protection of existing and forthcoming location anonymization echniques in terms of the trade-off between privacy and system performance.

F. Algorithmic support for generating indirect surveys: this paper focused on t privacy issues and problems. For other privacy problems, is there a principled way to go from the problem to a set of associated attributes (like importance and sharing in the case of content privacy)? [24].

G. What are the requirements for various location-based applications? How does their variety affect the design of the privacy protection system?

Hence this section dealt with future research work to be done for further research in location based services to protect privacy of vehicle user's. Finally section 6 conclude this work in brief.

6. CONCLUSION

Location based services provides services to vehicular users about any location whatever they need during their way example for coffee shop, hotel, petrol pump etc. Although LBSs provides enhanced functionalities, they open up new vulnerabilities that can be exploited to cause security and privacy breaches**.** Now days, vehicle is an extremely personal device, its communication data should be secured and the driver's privacy should be unrevealed. Moreover this, various approaches focused on the user's location privacy and trouble-free frame works for interconnecting the mobile network and privacy model server [12]. For instance k-anonymity [16, 19]; cloaking algorithm; TTP; mix-zones [3], mobi-crowd addressed in various literatures but still no one is an efficient tool to handle the location privacy threats. Even (*Note that*- Approaches mentioned above are all focused on the geographic based algorithm instead of geometry based algorithm). Even though various models for example mix

zones, mobi-crowd etc. also have been proposed to resolve the privacy problem in LBS but they were unsuccessful to provide 100% privacy protection to users. Perfect privacy is clearly impossible as long as communication takes place, but we can achieved a higher level of privacy protection for LBSs users after considering all issues in our model/framework. So this paper focused (in detail) on privacy requirements; location privacy issues and challenges arises in the Location Based Service (LBS). So everybody is warmly invited to participate in this intrepid journey to explore these future views/issues i.e. to provide maximum privacy protection to vehicle users.

7. REFERENCES

[1] M.E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security Issues in a Future Vehicular Network," Proc. EuropeanWireless Conf. '02, Feb. 2002.

[2] Yasser Toor and Paul Mühlethaler, Inria, "Vehicle Ad Hoc Networks: Applications and Related Technical Issues", IEEE Communications Survey, 3rd Quarter 2008, Volume 10, No. 3 www.comsoc.org/pubs/surveys

[3] J. Freudiger, M. Raya, M. Feleghhazi,P. Papadimitratos and J. P.Hubaux., "Mix zones for location privacy in vehicular networks," in Proc. International Workshop on Wireless Networking for Intelligent Transportation Systems, Vancouver, British Columbia, Aug., 2007.

[4] David Antolino Rivas, Jose M. Barcelo Ordinas, Manel Guerrero Zapata, Julian D.Morillo Pozo, "Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation", Journal of Network and Computer Applications 34 (2011) 1942–1955.

[5] Ahren Studer, Elaine Shi, Fan Bai, & Adrian Perrig, "TACKing- Together Efficient Authentication, Revocation, and Privacy in VANETs", CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the Army Research Office.

[6] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. Fourth Workshop Hot Topics in Networks (HotNets IV), Nov. 2005.

[7] Marius Wernke, Pavel Skvortsov et al., Kurt Rothermel, "A Classification of Location Privacy Attacks and Approaches", Sprinzer 2013.

[8] S. Biswas and J. Misic, "Location-based Anonymous Authentication for Vehicular Communications", in Proceedings of the 22nd IEEE Symposium on Personal, Indoor, Mobile and Radio Communications (PIMRC 2011).

[9] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications", IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[10] Machanavajjhala, A., Kifer, D., Gehrke, J., Venkitasubramaniam," L-diversity: Privacy beyond k-anonymity," ACM Transactions on Knowledge Discovery from Data 1(1) (2007) 3.

[11] Beresford, A.R., Stajano, F." Location Privacy in Pervasive Computing", IEEE Pervasive Computing 2, 46–55 (2005).

[12] Fuentes, J.M., González Tablas, A.I., Ribagorda, A." Overview of Security Issues in Vehicular Ad-Hoc Networks", 2010.

[13] A.I. González-Tablas, A. Alcaide, J.M. de Fuentes, J. Montero, "Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations", Elsevier, 2013.

[14] Dr. Robert P. Minch, "Privacy Issues in Location-Aware Mobile Devices", Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.

[15] Mina Deng, KimWuyts, Riccardo Scandariato et al. "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements", Springer, 2010.

[16] Aris Gkoulalas–Divanis et al. "Providing K–Anonymity in Location Based Services", SIGKDD Explorations, Volume 12, Issue 1, 2010.

[17] Chi-Yin Chow et al. "Privacy in Location-based Services: A System", Architecture Perspective, ACM, 2009

[18] B. Palanisamy and L. Liu," MobiMix: Protecting Location Privacy with Mix-zones over Road Networks" In Proc. of ICDE'11, pages 494–505, 2011.

[19] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," Int. J. Uncertain. Fuzziness Knowl.-Based Syst., vol. 10, no. 5, pp. 571–588, 2002.

[20] http://www.privacyguidance.com/downloads/privacyandsecurity.pdf

[21] http://www.ics.uci.edu/~ics215/papers/UCAM-CL-TR-612.pdf

[22] AR Beresford "Privacy issues in geographical information technologies", 2006.

[23] Abul, O., Bonchi, F., Nanni, M., "Never walk alone: Uncertainty for anonymity in moving objects databases," In: IEEE 24th International Conference on Data Engineering (ICDE 2008), April 2008, 376–385.

[24] Laura granka et al. "Indirect Content Privacy Surveys: Measuring Privacy without Asking about It, "Symposium on Usable Privacy and Security (SOUPS), 2011.

[25] Rainer Hörbe, "A Model for Privacy enhanced Federated Identity Management, "Identinetics GmbH, 19 January 2014.

[26] Agarwal, Gag et al. Bawa, M, "Vision Paper: Enabling Privacy for the Paranoids," VLDB conference, 2004.

[27] Dr. Robert P. Minch, "Privacy Issues in Location-Aware Mobile Devices", Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.

[28] http://mediatum.ub.tum.de/doc/627707/file.pdf

[29] http://www.privacytrust.org/about/privacy.html

[30] http://www.velocityworldmedia.com/Privacy-Policy

[31] http://mirskylegal.com/wpcontent/uploads/2012/07/Handout-Privacy-for-Business-032712.pdf

[32] http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/qa-privacy