International Journal of Hybrid Information Technology
Vol.9, No.3 (2016), pp. 221-240
http://dx.doi.org/10.14257/ijhit.2016.9.3.21

Providing Together Security, Location Privacy and Trust for Moving Objects

Amit Kumar Tyagi[1] and Dr. N. Sreenath[2]

Research Scholar[1], Professor[2]
Department of Computer Science and Engineering
Pondicherry Engineering College, Puducherry-605014, India
amitkrtyagi025@gmail.com, nsreenath@pec.edu

Abstract

In last few years, vehicular networks (or moving objects) are gaining more and more attraction from the researchers and the automobile industries. In that, Location-Based Services (LBSs) become more feature-rich and versatile due to the explosion of mobile devices and the advances of positioning technologies. Trust and Privacy are the two key parts of security and it is undoubtedly a necessity to develop (or maintain) trust for moving objects (or vehicular users). The main aim of this paper is to propose a trust model for vehicular environment with desired level of privacy protection. The proposed model contains two different modules. First, this paper analyzed the merit and demerit of exiting location privacy protection method.Then a perceived k-value location privacy protection algorithmdiscussed to provide desired level of privacy protection. Hereafter the protocol (or procedure) of this algorithm; simulation result are discussed in detail.Second,it provides a model to maintain trust for vehicle Ad-hoc Network (VANET) users in LBSs. The results show that proposed method outperforms the existing privacy preservation method by effectively enhances privacy and trust against various adversaries. Hence,the purpose of this work is to maintain trust and certain level of privacy among vehicular users without revealing her identity in LBSs.

Keywords: *Location Based Services, Privacy Protection, Trust Level, k-anonymity, Vehicle Ad-Hoc Network, Location Privacy*

1. Introduction

Nowadays safety of human lives is the major concern, because every year thousands of peoples died in road accidents over the globe.Moving objects define here like a vehicle (or a mobile) user who can access services providedby Location-Based Services (LBSs) or to provide communication to neighbor vehicle users.VANET is special kind of network that aims to reduce death rate and improves traffic safety system. In VANET, vehicles can send and receive safety messages to each other on the road to ensure safety of human life.In Augmented Reality (AR) [17], user's main concern includes safety and privacy of data. Since location based services (LBS) are one of the major applications of the AR, it is important to have a privacy-aware management of location information, providing location privacy for clients against vulnerabilities or abuse. Actually, the term AR was coined in 1990 by Thomas Caudell, an employee of Boeing. The technology which allows adding images and information generated by a computer to the normally perceived reality is called the Augmented Reality (AR). Azuma's definition says that Augmented Reality:

- combines real and virtual
- is interactive in real time
- is registered in 3D

ISSN: 1738-9968 IJHIT

With the development of sensors and wireless devices, it is possible to access to personal accurate position or any other relevant information anytime and anywhere with the help of Location Based Services (LBS). Location based services are essentially the services which are related to the location of a user making the request [7]. Location based services are one of the common services provided by AR. LBS normally consists of mobile devices, location system, network and service provider (i.e. LBS server). Mobile user (or vehicle user) sends queries to LBS server through mobile device, such as mobile phone etc. Then the location system, GPS, acquires the location of queries. Hereafter, LBS server returns the feedback to vehicle user through network, such as 3G net, 4G network *etc*.

Location Determination Technology (LDT), such as Cell-ID, RFID, A-GPS, EOTD, Bluetooth etc., [5] gives the location information which consists of the X-Y co-ordinates. There are many categories of services that LBS can provide for e.g. Emergency and Safety, Communities and Entertainment, Information and Navigation, Tracking and Monitoring, and M-Commerce etc. In 2003, Computer Science and Telecommunications Board (CSTB) in the “IT Roadmap to a Geospatial Future” pointed that LBS would be a very important part of future computing environment and infiltrated into all aspects of the future life. However, Location-Based Services (LBSs) can classify in: Positionaware and Location-Tracking Applications, Reactive and Proactive LBSs, Location-of-target and Target-at-location LBSs, Sporadic Queries, Self and Cross Referencing LBSs, Single and Multi-target, Content and Application-orientation, Outdoor and Indoor services [5]. Market research firm ABI Research forecasts[16], the global number of people to enjoy location-based services from 1.2 million in 2006 increases to 31.5 million in 2011 andwill cross one billion mark till 2020.

As discussed, technology boom is happening in the case of Augmented Reality (AR).Location based services(LBS) are one of the most widely used services of AR. But it presents users widely known serious privacy threats. These important threats are the leak of service content and position privacy. Service content threat is the potential exposure of service uses. Just like regular Internet access, a user may not want to be identified as the subscriber of some LBS, especially when the service is sensitive or confidential. Actually information can be in different forms like simple, important, sensitive and highly confidential etc., for example; for a vehicle user, one day tracing movement does not matter, but it matter when it is being continuously (let more than five days) by some unidentified people. Same the information of a user from a hospital about her diseases can breaches her privacy and trust between hospital’s staffs. The leak of location privacy is user’s location disclosed in her service request. It may reveal sensitive private information such as health conditions, lifestyles, habits and so on. Leaking of location privacy restricts the use of LBS, which has also become the bottleneck of the development of LBS and AR technology. Ultimately, privacy is about feeling, and it is awkward for one to scale her feeling using a number. For example, why woulda user feel that her privacy is well-protected if$K$ = 20, but not if K = 19?,i.e. it is hard to tell the difference between the two K values in terms of privacy feeling. A user can always choose a large K to ensure a sufficient privacy protection, but this will result in unnecessary reduction of location resolution. A very coarse location will make it difficult to provide meaningful LBS.There are three important metrics for measuring the level of location privacy guarantee one could provide: (i) location k-anonymity, (ii) location l-diversity, and (iii) road segment s-diversity. Each and every term can explain as:

- k-anonymityis one among of them[1, 2, 4]. The concept of k-anonymity for location privacy was introduced by Gruteser and Grunwald [6]. Anonymity can be seen as “a state of being not identifiable within a set of subjects, the anonymity set”. The idea of their approach is that a user reports an obfuscation area to a client containing his position and the positions of $k – 1$ other users instead of his precise position that is protected by a pseudonym. Moreover this, the basic concept of *k*-anonymity has been extended by various approaches to increase privacy protection.

- l-diversity [1, 3] is a form of group based anonymization that is used to preserve privacy in data sets by reducing the granularity of a data representation. A location is called *l*-diversified if there are at least *l* (> 1) differentgeographical/postal addresses associated to this location. A location area that satisfies location *k*-anonymity but fails to observe location *l*-diversity may be in danger of the location privacy of a mobile, because all *k* users are associated to only one geographical address (such as a AIDs treatment center or a church), thus an adversary can infer with the certainty that all *k* users are linked to that address [27].
- However, road segment s-diversity:It consists definition similar to l-diversity, i.e.a location is *s*-diversified if there are at least *s* (>1) different road segments associated to this location. Mobile users typically travel on road networks or walk paths. Thus, the location privacy of a mobile user also depends on road segment *s*-diversity. This is because a location area that satisfies location *k*-anonymity but fails to observe road segment *s*-diversity may jeopardize the location privacy of a mobile [1, 27]. Hence as discussed, further most prominent extensions of k-anonymity are *strong k-anonymity, l-diversity, t-closeness,p-sensitivity [1], and historical-k-anonymity [1, 4] etc.* The idea is that before publishing, the trajectories of at least k users are co-located within a "space tunnel" of radius *δ/*2 that defines an uncertainty level. The enhancement of *k*-anonymity can provide guarantee location privacy, but if it is improved by taking into account the temporal and spatial component of the user's location information. Due to unable to count spatial and temporal information of VANETs users, it does not provide desired level of privacy protection.

1.1 Privacy and Trust Challenges in LBSs

Privacy is generally the information that you don't want others to know.SimilarlyLocation privacy is defined as the ability to prevent other unauthorized (or malicious) parties from learning one's current or past location [1, 3-5]. Further, Trust can be described as the expectation and belief aboutfuture behavior, based on experiences and evidences collectedin the past, either direct or indirect [21]. Trust is a vitally important part of human being. It develops as early as the first year of life and continues to shape our interactions with others until the day we die.

As discussed, Location Privacy and Trust has been a serious concern for mobile users who used location-based services to acquire geographical location. 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 (*e.g.*, the user ID, the user name, *etc.*). 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 [4]. 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 [4]. 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.Finallyhere two questions arises;first “How to protect user’s privacy against compromised LBS providers and attackers are of vital to exiting systems”? Andsecond “Who is trusted client and How to find it”?Moreover this, a centralized model for providing certain level of privacy for LBSs is discussed in Figure 1.

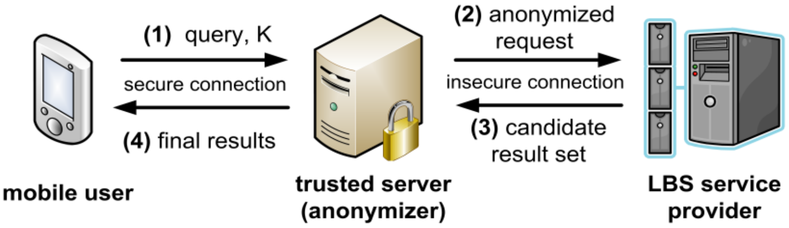

Figure 1. The Centralized Model for Privacy in LBSs

In Figure 1, a mobileuser is user (or moving object) who wants to access services in an area/zone provided by LBSs. Trusted server perform as a middle entity between two partiesi.e.client and receiver, to exchange secured communication. While LBSs service provider are on road providers who provides services to moving objects like information about nearest hotels, petrol pumps *etc*., moreover this, levels of trust can be in form of zero, weak and strong one (refer Table 1, appendix-A). For instance, Strong trust; in this every entity in a network performs his/her/its duties correctly and is therefore trusted, it is known as strong trust. This is a perfect situation as no attackers are present in the network and each entity carries out his duties correctly. While in case of weak trust, only some entities are bothered by the attacks; some of the entities of the network are unaffected by the attacks and can continue to serve the users of the network and perform their duties correctly. And in last zero trust means when there is no communications in network, which means that the trust value for sending and receiving is zero due to specific attacks.

Finally the organization of the rest of the paper is followed as: Section 2 presents the ways of location privacy and trust leakage. Section 3 discusses about related works to this paper.Existed privacy preserving approaches in LBSs with comparison are discusses in Section 4. Following that, in Section 5, presents a K-valuemethod/algorithm for the offering of privacy in LBSs. Then Section 6, presents a novel idea for the offering of trust in LBSs to moving objects. Section 7 discusses about future work. Finally, Section 8 concludes this work in brief.This paper interchangeably uses ‘mobile users’, ‘VANET users’ or vehicle users’ words with respect of moving objects.

2. How Location Privacy and Trust Leaked?

The advances in wireless communication and mobile positioning technologies have resulted in increasingly popularity of location-based services (LBS) in recent years, which also bring a considerable attention in privacy protection. In this paper, Location privacy threaten refers to, under unauthorized circumstance, attacker tracks the original position information through location device and technology, infers the privacy information related to user location through reasoning. Moreover this, Security is an important issue especially in this kind of network where one altered message can creates problem for the users in many ways. Users can take benefit of these applications if we can secure the communication between all entities (components) of the network.Hencethere will be no chances for any attackers to create trouble for vehicle users in the requiring network. But attackers create problem directly and indirectly by launching different kind of attacks.*There are three ways for location privacy leak and two types of possible attack on k-anonymity.*

If attacker know that a particular user ’A’ is living in a particular area/place P and if attacker observe that all the requests coming from area P have the same user id, then an attacker can easily guess that the user requesting the service is ’A’. So from these guessing,attackercan easily track the user by simple connect the dots approach [8]. This type of attack is called Restricted Space Identification (RSI) for example; if user sent a message in some room of some hotel, the exact location coordinate information (x, y) in this message and related exterior knowledge can be used to trace the user in this room. Then attacker can infer what other service request has been sent by this user.

Further for second attack, in which reveals the user’s identity using location-identity received with a service request message. If an LBS (*i.e.*, on road service) provider gets a report that a user ’A’ is going to visit a place during a particular period of time and if it observes that all the request coming from that place during this period of time are sent by a single user. Then similarly as RSI attack, here also attacker can infer that the user requesting for the service is ’A’. This kind of attack is called Observation Identification (OI) attack for example; if user leaked out its location information and identification in the previous message and still sent messages in same position, attacker can infer and identify the source of subsequent message through the location information in previous message, whether these latter messages are anonymous or not.

Finally for third attack,if the attacker can define the property value of some individual in quasi-identifier through known data set (published data and data obtained from other way), the sensitive property value of this individual and its location can be deduced, which induces the location information leakage. This situation is named as linking attack,for example; property set (birth date, sex, residential address, blood group, and zip code) can make up a quasi-identifier. It has been demonstrated that about 87% U.S. inhabitant can be uniquely identified through this quasi-identifier [28]. Moreover this, two attacks are possible on k-anonymity, which can be discussed as:

- **Homogeneity Attack**: This attack leverages the case where all the values for a sensitive value within a set of *k* records are identical. In such cases, even though the data has been *k*-anonymized, the sensitive value for the set of *k* records may be exactly predicted.
- **Background Knowledge Attack**: This attack leverages an association between one or more quasi-identifier attributes with the sensitive attribute to reduce the set of possible values for the sensitive attribute. This attack use some features of linking attack.

Now talking about trust, Trust is a vitally important part of human existence. The issue of trust in the use of LBS recalls Perolle’s notion of surveillance being practiced in low-trust situations, and the idea that the very act of monitoring destroys trust [29]. Again, this is a situation where a woman monitors her ailing spouse. She does not trust her husband more enough *i.e.*, does not allow to let him make his own decisions. He probably resents her 24*7 intrusion into his daily activities, but tolerates it out of love and because he does not wish to upset his wife. Their relationship could be expected to become increasingly dysfunctional, if there is a breakdown of trust. As an another example, if vehicle user are using services offered by LBS over road network then these services required some basic information of users like name, vehicle id or habits etc. So LBS should not be revealing this information (*i.e.*, a vehicle identity) to another vehicle. If it shares any information of a user with other vehicle user, then trust is not more existed here between third party and vehicles users. It is near impossible to predict the complex effects of LBS when used to track humans in this way, especially as each person has a different background, culture and upbringing. Freedom and trust go hand-in-hand. These are celebrated concepts which have been universally connected to civil liberties by most political societies.

Hence this section dealt with leakage of privacy and trust in different scenarios with different attacks on privacy and k-anonymity. Now next section discusses about related work about this research.

3. Related Works

Location-based services (LBS) become more feature-rich and versatile due to the explosion of mobile devices and the advances of positioning technologieswhich also bring a considerable attention in privacy protection.As discussed in [1, 4], to provide privacy, security is must but this is not true inversely.While security is a condition, a strategy, constitution supporting the existence for human being. In response of this, privacy is the prognosis, outcome, and a state of existence. 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 [1, 4]. Security involves a combination of hardware and software. For VANET, there are many types of embedded hardware module used in vehicle, none of which is specifically meant for trust. Privacy andsecurity are two important issues in deployment of location based services with inversely propositional to each other. Moreover this, between privacy and security, trust is also an important issue.In order to solve the problem of location privacy leakage, privacy protection is also required. Many researchers try to find the balance point between the service quality and privacy protection, which means the best service with least location privacy exposure. While most existing work focuses on how to minimize and protect the sizes of cloaking regions, and area travelled by moving objects. In that, the relation between cloaking regions and semantic locations is always unclear.

Now we have already made a number of privacy protection methods. Location privacy protection is the method that sends the false location information or anonymous identity and location information to the server in the location service. These methods can be divided into two categories: one is to protect the user's ID information (conceal anonymity or pseudonym), making the server service does not know the requestor true ID; the other is to protect the location information of the user by submitting a region instead of true location of the user.The author also discussed thread model which contain attacks such as Sybil attack [5, 30],Vehicle impersonation, sending false information and car tracking. Three security properties were presented. They include vehicle and it must have a unique identifier, ensuring the integrity of the messages which must be authentic with regards to vehicle identifier and lastly, to ensure the trustfulness of the content of the messages that must be verified.

Existing methods to provide privacy protection for vehicle user in LBSs, such as pseudo-location method, pseudonym method, k-anonymity method, mix-zone, slow, swing and swap [19] *etc*. Some other methods based on already existing methods, such as personalized k-anonymity(using the concept of k-anonymity), silent mix zone or silent period [18], and promix zone etc. (based on mixzone concept)have some defects which will reveal the location privacy [1, 3, and 8].Perceived k-value location privacy protection method in this paper makes improvement as compared with the existed methods mentioned above. It combines the advantage of pseudonym method; location k-anonymity; location *l*-diversity and road segment *s*-diversity method that suggests a location privacy protection method based on perceived k-value including diversity to realize the protection.

Here after, Trust describes the level to which an entity accepts the dependence on another one. Trust is a vitally important part of human existence. It develops as early as the first year of life and continues to shape our interactions with others until the day we die. Furtherwe have already made a number of trust management methods for mobile users', *i.e.,* entity-based trust management, data centric trust management, and combine based trustmanagement.In the entity-oriented trust model, trustworthiness of information is estimated based on the trustworthiness of the message sender [24]. Minhas, *et al.,* [25] and Gomez andMartinez [26] proposed two models of trust based on entity. The data-based trust model attempts to verify whether the reported information is reliable or not. Based on the trust value, the model decides how to react on the reported event. A few models of trust based on data have been proposed such as the data-centric, RMCV, intrusion-aware trust model, reputation-based trust model, event-based reputation system (ERS), and roadside-unit aided datacentric trust establishment (RATE). Raya, *et al.,* [5] proposed a framework for data-centric trust establishment where trust in each individual piece of data is computed. Combined based trust model, data trust evaluation is performed using entity trust. The combined trust model aims to determine trustworthiness of the messages based on opinions provided by other vehicles. The basic idea is to suggest a vehicle to trust a message that has been evaluated to be trustworthy by many other trusted peer vehicles [24].

Hence, existing methods for trust management (Refer Table 2, Table 3 And Table 4, in appendix A, in end of this work) in vehicular networks, such asTrust and Reputation Infrastructure-based Proposal (TRIP), RMCV, Event-based Reputation System (ERS), roadside-unit aided datacentric trust establishment (RATE), beacon-based trust management (BTM), Content reputation system (CoRS), Data-Centric Trust Establishment framework(DCTE), Distributed Emergent Cooperation through Adaptive Evolution (DECADE) *etc*.

This section discussed about related work done in this interested area i.e. to maintain a certain level of privacy and trust between vehicle users and third party entity during using services over road networks. Now next section analyses existing location privacy protection methods in brief.

4. Analysis of the Existing Location Privacy Preserving Method

Researchers have long been aware of the potential privacy threats associated with LBS, and a lot of promising work has been conducted concerning how to protect location privacy.Table 3 and table 4 in [1], provide summary of Privacy Protection Schemes in detail.As summary, [1] discussed about: the anonymity technologies, such as location cloaking techniques (personalized k-anonymity, p-sensitivity, location spatial cloaking, pseudo location method, and Spatio-temporal cloaking), then Mix-zone (like pro-mix, mini-mix, silent mix zone *etc*.,), Fake points, path confusion, location obfuscation and pseudonyms approaches.However, there arevarious location privacy protection methods exist based on the location service. In last, the merits and demerits of each approach are discussed in brief.

4.1 Pseudo-location Method

Pseudo-location method [9] (also called position dummy method) can realize the confusion effect. In this method, a user confuses an attacker to hide her real identity and location. Here two situations are created for pseudo-location method to realize the location privacy protection. The first one is that user forms some pseudo-location by himself and sends it with his real location to the LBS provider when user put forward the service request. So the attacker cannot discriminate the pseudo and real location, which protects the user’s location privacy. The second situation is that user only sends one specified pseudo-location when putting forward the service request. Then the server increases the resent adjacent inquiry according to this pseudo-location and sends the results to the client. So user can retrieve the requisite answer according to the results. Because attacker doesn’t acquire the real location of user, *i.e.,* the location privacy of user can still be protected. But the defect of this method is obvious. In this method, it is hypothesized that user only act in some restricted space. And in this method, the level of privacy protection is not fixed, which is proportional to the distance between the pseudo and real location.

4.2 Path Confusion

This approach similarly looks like fake positions, but in that consecutive location samples from a vehicle is temporally and spatially correlated, trajectories of individual vehicles can be constructed from a set of location samples with anonymized pseudonyms reported from several vehicles through target tracking algorithms [1]. The basic idea of false position is to either send one or more fake locations to attackerrelated to her location. This algorithm predict the position of a target vehicle based on the last known speed and direction information and then decide which next location sample to link to the same vehicle through Maximum Likelihood Detection.But this approach fails [1], if attacker predicts the position of vehicular user using some guessing methods like probability or last known identity, speed, location *etc*.

4.3 Pseudonym Method

Pseudonym method [1] changes the real ID to a pseudo-ID and then sends the service request to the anonymous server. Every user can realize the concealment of the real ID through the pseudo-ID. Even attacker obtain the accuracy position information from the server, the exact interconnection between user's position information and real ID information still can't be established, which realizes the location privacy protection. But the shortage of this method still exists. All information of user's request and corresponding IP address will be stored in the server, which will lead to the location privacy leak.

4.4 K-anonymity Method

K-anonymity method [1, 3, 6, and 12] was firstly proposed by Gruteser and Grunwald. In this, k-anonymity requires that every record in a released dataset is indistinguishable from at least k-1 other records with respect to a certain set of identifying variables. Before sending to the LBS provider, user deletes the personal information and publishes hypo-accurate data, which induces that every record has identical quasi-identifier value with other k-1 record in the data list to realize the location privacy protection. But the restriction of this method is that there is no protection mechanism for leak of sensitive attribute data, and there is no any constraint for sensitive attribute data in this method. It is easy for attacker to infer the individual corresponding sensitive attribute data and identify the relationship between data and individual through the background information, which leads to the location privacy leak.For example,an attacker can easily guess an user present's location based on some habits, and features of that user or an attacker can easily co-relate patient data according to their admit date in a particular hospital.

4.4.1 Personalized K-anonymity Method: This method was proposed by Gedik and Liu [8], in which every user can define the desired anonymous level and adjust the least anonymous level and maximum tolerable time and spatial resolution. This method can provide certain level of privacy protection to sensitive information, which will decrease the data lost from the unified anonymous. But the defect of this method is undefined information and the proportion of anonymous information will decrease when the k value increases.

4.4.2Other Methods based on the K-anonymity Method: Other methods have been proposed according to the defect of k-anonymity method.Firstly,l-diversity [1] model was proposed by A.Machanavajjhalato protect user privacy over road networks. But this method only suitable for handling classification sensitive attribute data instead of numerical sensitive attribute data. Further p-sensitive k-anonymity model proposed, but it may lost a lot of information usability in some data set and can't resist the skewed attack and similarity attack to the sensitive attribute data [10]. (α,k)-anonymous model [11] still can't avoid the skewed attack and similarity attack with the significant loss of data during the anonymous process. (k, e)-anonymous model [1] has similar defect. t-closeness [1, 3] frame can fix the skewed attack and similarity attack to the sensitive attribute data. But it reduces the usability of published data.

4.9 Other Privacy Protection Methods

CARAVAN approach [1, 5, 20] from Sampigethaya, is another scheme to create user-centric mix zones by using cluster-based communications. Due to vehicle mobility, vehicles tend to form clusters while driving, *i.e.,* several vehicles travel at same speed and keep same distance to each other, especially on highways [20]. The CARAVAN approach exploits this property by grouping vehicles into clusters and letting one of the vehicles in the group act as a proxy for the group members for anonymous communications with entities outside the group. Hence each group forms a virtual moving mix zone [1, 3, and 23]. This approach failed if group leader is malicious one or controlled by a malicious activity (for *e.g.,* botnet) [22]. Here after Buttyan et al., propose a different solution for the potentiallydangerous time frame where no beacons are broadcasted: in their proposal called *SLOW,* in thateach vehicle may stop sending messages when its speed is below a threshold of 30 kmph. Obviously, crashes at low speed [1].

Finally as conclude to this section, it covered almost all existed privacy protection techniques for LBSs users. Several privacy preserving methods for moving objects (for *e.g.,* vehicle, mobile *etc.,*) are discussed in [1]. Hence there is no single privacy preserving techniques that covers all of the privacy requirements to provide certain level of privacy to mobile users, due to some merits and demerits in respective privacy preserving schemes. For further location privacy methods, refer [1]. Todays it is an emerging area to do further research and provide convenient services to vehicle users. Now next section dealt with proposed algorithm to protect location privacy of vehicle users for LBSs.

5 k-value Algorithm to Protect Location Privacy

There are three main models used for achieving the privacy in LBS. The first one is non-cooperative model. The second one is a peer to peer cooperative model. The last model is a centralized trust third party (TTP) model (Refer Figure 1). Here perceived k-value location privacy protectionmethod is based on the centralized trusted third party (TTP) model. In this, it collect several type of information, *i.e.,* user location and identity anonymous; service request and response anonymous and feedback sent to the user will be kept secured by the third trust party, who works as a secure and privacy protected communication bridge to the user and LBS provider.

5.1 The Analysis of Location Privacy Protection Level

To protect the location privacy of vehicle users, we need a secured communication between user and LBS service provider. There are two kinds of approaches for attacker to acquire user's location when communication goes between user terminal and LBS, *i.e.,* achieving location information from user terminal and LBS. As in the first case,it is directly achieving query information from user terminal. As the user have control power on location information of herself, attacker can't directly communicate with the user and achieve his location information in un-cooperated model. The second one is achieving query information of user from LBS. On this occasion attacker can speculate user's location. Beside this, attacker can acquire information about a particular user based on information collected ontravelled on road and visited location by her. For example, a person daily goes to his clinic at 2 pm through NH-24 highway via dropping his son for tuition on a location M.

With the hypothesis of p for real position of user terminal, p' for location of query spot and $q_i$for thei^{th}query result acquired from terminal, the information received by attackerinclude query spot p' and orderly result set { q_1 , q_2 , q_3 ,...q_m } centered on the p' . Also the hypothesis is set that the known user employ incremental close neighbours query and the attacker take the q_j as expected query results of user. According incremental query ending condition, the supposed user location p may meet the equation as follows:

$$dis(p, p')+\ \overset{J}{\underset{1\le m\le n-1}{\min}} dis(p, q_m) > dis(p', q_{n-1}) \ldots\ldots\ldots\ldots \qquad ①$$

$$dis(p, p')+\overset{J}{\underset{1\le m\le n}{\min}}\ dis(p,q_m)\le dis(p',q_n)\ldots\ldots\ldots\ldots\ldots \qquad ②$$

Here in the equation1 and 2, $dis(.,.)$represents the distance between query spot of userand supposed user location of attacker. The solution of equation 1 and 2, represents the possible user location area/zone speculated by attacker. But attacker cannotget the real user query results saved in terminal. As there were many different solutions representing different possible user location for the defined equation above, the attacker still cannot make sure with the specific location of user. Attacker cannot reveal the identity and location of a user from terminal.

5.2 Algorithm and Procedure

Algorithm:

```
Set the minimum value of k is $k_{min}$ , set the maximum value of k is $k_{max}$($k_{min=2}$, $k_{max=6}$)
1. The user sends the service request
2. the trusted third party receives the service request
3. if k $\in$($k_{min}$, $k_{max}$)
4. if (k=$k_{min}$), the trusted third party process the privacy protection with k-anonymity method and l-diversity
5. (if k=$k_{max}$),the trusted third party process the privacy protection with k-anonymity method, l-diversity and road segment s-diversity

6. The trusted third party processes the privacy protection with k-anonymity method and pseudonym method.

7. else
8. if k>$k_{max}$

9.    the trusted third party process the privacy protection with pseudonym method
10.   else
11.   if k<$k_{min}$

12.       the trusted third party process the privacy protection with k-anonymity method

13.       end if
14.   end if
15.   end if
```

Procedure:

When k value is located in the set range, the certified trusted third party (TTP) will anonymize the user's location information with k-anonymity and pseudonym methods and sent service request to the LBS provider, who will answer this request and return the results to themobile terminal user. (*Note*- here maximum value of k is 6, because a large of nodes also creates problem, *i.e.,* more chances to revealing user's privacy, while minimum value of k is 2, because below 2 shows already a single user inside a zone/area). Here the real id will be replaced by pseudo-id which will be saved in the trusted third party list with the real id and other detailed information of the user. When the trusted third party sends the result from the LBS provider to the mobile terminal, pseudo-id is checked with corresponding real id of user in the list and then all primal data will be feedback to the mobile terminal user. But if value of k is equal to k_{min}, the TTP will anonymize user's location with k-anonymity and l-diversity and transmit the result to the LBS provider, who will send the feedback to the mobile terminal user. If value of k is equal to k_{max}, the TTP will anonymize user's location with k-anonymity, l-diversity and road segment s-diversity method and transmit the result to the LBS provider, who will send the feedback to the mobile terminal user. Now here, when the k-value is higher than k_{max}, the trusted third party will anonymize user's location with pseudonym method. Finally when the k value is lower than k_{min}, the TTP will anonymize user's location with k-anonymitymethod and transmit the result to the LBS provider, who will send the feedback to the mobile terminal user. (*Note*-The value of k can be increased and can get result on required values. But this work shows all results with the value of k=2 and 6 only).

5.3 Experiment Simulation and Analysis of Algorithm Efficiency

A number of interesting and desired applications of Intelligent Transportation Systems (ITS) have been stimulating the development of a new kind of ad hoc network. Here moving object generator is used to simulate the automobile over road network. The service request is sent according to the location information of moving object generator. The map used here is national mapping map provided by U.S. Geological Survey [13], which utilizes the spatial data transmission standards [14]. OPEN GL is used to simulate this map. Further, experiment circumstance is Inter(R) Core(TM) i3 2.26 GHz for CPU, 3GB for memory in Windows 7. Programming circumstance is MyEclipse+Hibernate+SQL Server 2005. In this experiment, 400 moving object generators were used to simulate the automobile along the road and 470 service request information were received. Here for experiment purpose, k-value was set as 2,3,5,6, which can be increases.

5.3.1. AnonymizedSuccess Rate: Different k-values are input so as to check the working of the algorithm in different contexts/formats for *e.g.,* success rate, complexity, anonymity, scalability etc. But here we discuss about only two contexts. Success rate is an important measure of performance evaluation. While entropy/unlinkability between mobile users used to determine the privacy protection level.Success rate is the ratio of the number of request anonymized by the TTP (trusted third party) to the total number of request send to the TTP [8].

According to the simulate experiment, it is discovered that most information is anonymized with k-anonymitymethodwhen k value is less.If the k value is set as 2, 290 information is anonymized with k-anonymitymethod while only 80 information by pseudonym method. *(Note- results with l-diversity and road segment s-diversity will be discussed in an enhancement work of this research).*But more and more information will be anonymized by pseudonym method with the enlargement of k-value. When k-value is set as 6, only 178 information is anonymized with k-anonymity method while 192 information by pseudonym method (Figure 2).That is, when the k-value is less (*i.e.,* less than maximum value), the k-anonymity method will be used more and as the k value increases the pseudonym method usage will get increased.

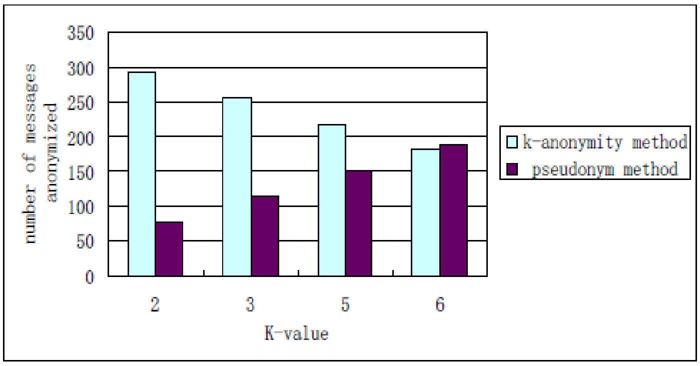

Figure 2. Number of Information Anonymized by K-anonymity Method and Pseudonym Method

5.3.2. Execution Time: Here another performance evaluation is execution time. It is the time of anonymous process for all inquiry requests from a certain scale of mobile users, which reflects the efficiency of anonymous algorithm. The execution time is shorter;the anonymous algorithm is more efficient.

When comparing the execution time of perceived k-value location privacy protection method and personal k-anonymitymethod, we realize that the execution time of latter is significantly longer, which is owing to its moredeeper refinement to the data and bigger searching space. After every refinement, personal k-anonymitymethod will calculate the restraint of every new anonymous group and undertake the sensitive attribute generalization, which induce longer execution time (Figure 3).

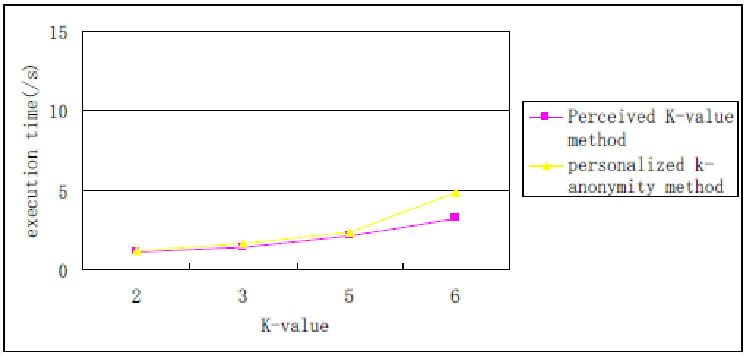

Figure 3. Comparison of Execution Time

Hence this Section discusses about experimental results derived through k-anonymity method and pseudonyms methods to protect user's privacy. While as discussed, results with l-diversity and road segment s-diversity will be discussed in an enhancement work of this research later. Now next section will start with proposing a trusted computing model for VANET users.

6. Vehicular Trusted Computing (VTC) Model

Trust is the key element in creating a trustable vehicular ad-hocnetworks environment which would help promote a safer road environment. The basis of vehicular ad-hocnetworks is the exchange of data between entities, and making a decision on received data/event/information is usually based on information provided by other entities, trusted or not. As discussed above, security and privacy are important issues in LBSs for VANET users. Moreover this, Trust is also an important issue between security and privacy. Security is one of the main issues in VANETs, and trust is a key element of security.

Trusted Computing Group (TCG) defines trust as:"An entity can be trusted if it always behaves in the expected manner for intended purpose" [15]. Putting "trust" definition in the context of VANET, it would mean that "all components of the network (vehicles and infrastructure) are behaving in an expected manner (trusted communication between the components) and serve the users and save human lives". Hence Trust is the key element in creating a trusted vehicular environment which promotes security in vehicular networks.

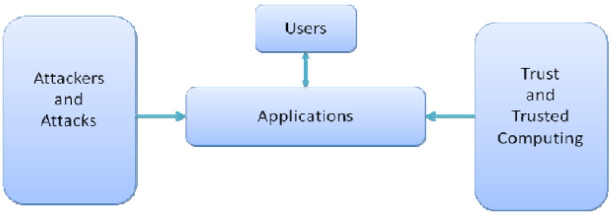

Figure 4. Proposed Trust Model

Today's computing Trustfor VANET users is a relatively new technology which will attract more researchers from auto-industries and university in future.Trusted Computing Group (TCG) [25] has been the main proponent/component of this technology. The main aim of TCG is to enhance security in computer network by using security hardware module (called Trusted Platform Module (TPM)), *i.e.*, via enhancing security; we can provide a certain level of trust to moving objects over road network. For implement TPM for enhancing security, some requirements have an important role for, *e.g.*, details of the module should be public; the module should be based on well-known techniques, and Diffie-Hellman certainly qualifies; the module should be compatible with laws and regulations on interception, the module should allow national and international operation *etc*.

Figure 4 and 5 shows "How trusted computing communication can be maintained between all entities of the network"?For, *e.g.*, Vehicle A to Vehicle F is doing their task in proper manner. Vehicle D communicates with RSU(road side unit) and RSU communicate with TOC and authenticates and provide valid information. Vehicle D shares this information with other Vehicles in the network. This is an ideal condition that we want to achieve in real vehicular network. Trust will be built in two different ways in vehicular trusted computing. Trusted computing requires that these two basic properties are fulfilled:

- The sender who sends the information in vehicle to vehicle or vehicle to infrastructure is accepted as a trusted entity.
- The contents of the message source is not changed during transmission, it meets the integrity requirement.

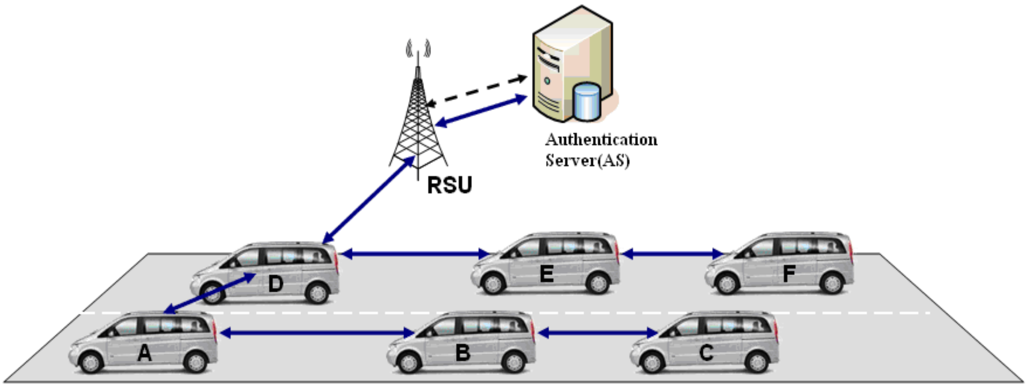

Figure 5. Vehicular Trusted Computing Communication

6.1. Trusted Entities of VANET: This Section explains five basic entities of trust and when all these entitieswork together then will develop a chain of trust in the vehicular network. Eq.3 explainsthat all modules are trusted and worked together for achieving chain of trust in system.Detail discussions of all these entities are given below:

- Trusted User (TU)
- Trusted Vehicle (TV)
- Trusted Applications (TA)
- Trusted Routing (TR)
- Trusted Medium (TM)
- Trusted Infrastructure (TIF)

Chain of Trust (COT) = $\Sigma_{i= 0}$(TU + TV + TA + TR +TM + TIF)………………………. (3)

So attackers are those people how change the behavior of the entity and break the trust. So first of all we should studies the attackers and attacks because it is directly change the behavior of the vehicle. If we want to achieve the trust and develop the trusted computing environment then we should keep remind following three steps. For respective trust level, no attacker should be present there. More number of vehicle users in LBSs create more problems i.e. the chance of revealing user’s identity and loosing of trust is too high inside the LBSs. Refer Table 1 (in appendix A),to know about Level 1 attackers (L1) and level 2 attackers (L2) explanation.

6.2. Levels of Trust

- **Zero Trust** is the first trust level in which the attacker is active and is able to use allkinds of entities in the network and create problem by launching different types ofattacks (passive or active). Eq.4 describes that first and second level attackers are activeand chain of trust in this condition will be zero.
  Zero Trust = Σ (L1.Attackers + L2.Attackers) – (Chain of Trust: = 0)……………(4)
- Second level of trust is called **Weak Trust**, in which the attacker is able to launchdifferent kind of attacks and scope of the attacks are within some specific region. Someentities are effected with these attacks whereas other entities of the network performingtheir task properly and serve the users. In Eq.5 we represent a situation where all entitiesof the chain of trust and only trusted infrastructure (TIF) are affected due to attacks.
  Weak Trust = Σ (TU + TV + TA +TR +TM) – (TIF)……………………………….. (5)
- **Strong Trust** is a third level of trust is which all entities of the network are trusted andwork properly. There are no attackers in the network and this is a very ideal conditionand every entity performing their task properly. In Eq.6. Here, this work assigns zero value to both types of attackers.
  Strong Trust = Chain of Trust – Σ (L1.Attackers:=0 + L2.Attackers:= 0)………… (6)

Moreover this, a user has a dynamic behaviour and changes his/her behaviour according to the information received from other users or from the roadside unit (RSU). There are two types of user behaviour.

- **Positive Behaviour- Trusted users and non-trusted users**
- **Negative Behaviour- Non trusted users**

Positive Behaviour: A user receives a warning message from another user or from the RSU, and then changes his/her behaviour according to the content of the message and also forwards this message to other users of the network. **Trusted users** have following qualities.

- Receive messages from other Vehicles, perform task according to message (safety or non-safety) and pass this message to other Vehicles in the network.
- Receive messages from infrastructure (RSU) and execute it and pass this message to Vehicles of the network.
- Messages are generated by users according to situation, *e.g.*, if an accident has occurred in some specific place, messages are past to other Vehicles and as well as to the infrastructure in the network.

Non Trusted Users (NTUs) are those users that do not possess the trusted credentials and could potentially be the kind of attackers who create problems for legitimate users by launching of some attacks. Non-Trusted Users could potentially be an active attacker and launches attacks that can be of high intensity. Non-Trusted Users can break the integrity of messages sent through the communication in vehicular environment. Attackers could change the content of the message, for example, **“**Accident at Location X” can become “Road is clear”.

Negative Behaviour of Non-Trusted Users (Attackers): Attackers are those who intentionally create problems for users in a network by launching different types of attacks (passive or active). In a vehicular network, they become more prominent because they can potentially change a critical message or broadcast a wrong message to other vehicles. As defining problem, the *attacker can use two basic mechanisms to link transmissions from a vehicle: (1) linking pseudonyms or other identifiers between heartbeat messages (syntactic linking), and (2) using the position and velocity information in the heartbeat messages to reconstruct the trajectory of the vehicle (semantic linking).*

6.3. Properties of Trust Model

- Complexity
- Decentralization
- Dynamics
- Scalbility
- Privacy
- Security level
- Sparsity
- Robustness etc.

6.4. Trust Metric based on Properties

- Distance
- Time
- Type of vehicle
- Type of event
- Experience
- Direction of vehicle
- Velocity of vehicle
- Position of vehicle
- Recommendation by RSU
- Recommendation by vehicle

- Type of event *etc*.

In last, trust level for vehicle users (in an area) can be defined as:

Trust level=Total number of neighbor in a zone/Total no of vehicle users existed in a zone ….(7)

As discussed, negative users create more problems than non-trussed users. Negative user generates negative trust for other users. So negative trust can be computed as,

Total Negative Trust = Total Trust - Positive Trust …………………………………………… (8)

From equation 7 and 8, we can derive that role of neighbor node or negative trust has an important role to maintain a certain level of trust including privacy protection. Equation 3 to 6, provide trust level in respect of weak, average and strong. Table 2, 3 and Table 4 (refer appendix A), provides the complete description about existing methods to provide a certain level of trust for Vehicle users.

Hence as discussed in vehicular environment, the role of user and infrastructure is most important for building the chain of trust. Chain of trust would be affected if user or certified authority is not performing their task accurately. In their respective Vehicles, user communicate with application unit (AU) or road side unit (RSU) and send messages to other Vehicles in network. Now next section will deal with future work related to work presented in this paper.

7. Future Works

An increasing number of people own mobile devices with positioning capabilities, and use various location-based services (LBSs) to obtain all kinds of information about their surroundings. Information interaction is a crucial part of modern transportation activities. Privacy and Trust concerns have emerged because many of such services enable, by design, service providers to collect detailed location information about their users. Ultimately, privacy is about feeling, and it is awkward for one to scale her feeling using a number. Further as discussed above, in human-being relationships, a lack of trust means that there is also no bonding, no giving, and no risk-taking i.e. without trust, there can be no meaningful connection to another human being. And without connection to one another, we literally fall apart. We get physically sick and get highly depressed. And our minds run away with themselves. We will create masked microdata that satisfy *p*-sensitive *k*-anonymity using the existing algorithms for *k*-anonymity with the addition of the two necessary conditions, and we will compare the running time of these modified algorithms against the existing algorithms that searches for *k*-anonymity only. For further research, we can try to find exact trust level matching (define in equation 7) with proposed algorithm protect privacy for LBSs. Hence as summary, there are a number of further important research issues for continuous LBSs, which we omit due to space constraints. However, research into location privacy is a relatively young field and many of the research issues outlined above are likely to be addressed in the near future. Now next section concludes this work in brief.

8. Conclusion

Security of VANET is an important issue to be addressed by designers of VANET infrastructure security. Attackers change their attacking behavior and they launch different attacks at different times. Attackers always try to tamper the information and create troubles in the network. In this paper, the merit and demerit of existing location privacy protection is analyzed. Then an effective perceived k-value location privacy protection algorithm is discussed and its efficiency is validated through simulation. This method can effectively anonymize all service requests with shorter execution time, which will realize the position privacy protection more efficiently. Further, discuss a phenomenon to maintain certain level of trust in LBS among vehicle users. The aim of the presented methodologies is to protect the location of the requesters of LBSs in both static and continuous queries. The level of trust develops in the network if the system is able to control attackers from distracting the information.Hence a lot of attentions have been drawn on location privacy and trust protection in location-based services and trajectory data publication from the viewpoint of industry and academia.We believe that future work in this research direction will lead to more robust and thorough methodologies that better protect the privacy (with required trust)of the vehicle users when requesting services in LBSs.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Appendix-A

Table 1. Example of Location Privacy Attackers [1]

Attacker Types	Description
Insider (L1)	An employee at Transportation Management Center (TMC) with access to floating car data (FCD).
Intentional (L1)	These types of attacker intentionally disturb the network operation and create problems for legitimate users to gain access the network.
Independent	This type of attacker has an unique identity and nature of the attacker is independent in the network.
Outsider (L2)	Someone outside the TMC without legitimate access to FCD data.
Malicious (L1)	A teenage obtains the whereabouts of renowned person and posts it on Internet.
Rational(L2)	A white-collar criminal seeks particular location information and sells it to a bidder.
Active(L1)	A hacker poses as authority and queries a vehicle about its position.
Passive(L2)	An eavesdropper deploys receivers along the road to collect beacon messages.
Local(L2)	An attacker with limited coverage of a few blocks in the city.
Dependent (L2)	The group of attackers intentionally wants to attack the network as a coordinated group in launching the attacks. In the group attack, the attackers are dependent on each other and share the same interest.
Unintentional(L2)	The attackers do not intentionally want to get involved in the network and to create some problems for the network users. This can be the case where errors occur due to some network operations and transmission in the network.
Extended(L1)	An attacker with global coverage of the whole network in a region.

L1- level 1 attacker, L2- level 2 attacker

Table 2. Comparision of Trust Provided in VANET (Based on Properties)

Approaches	Metrics					
	Complexity	Decentralization	Dynamics	Scalbility	Privacy	Security level
A multifacted approach	Simple (medium)	Y	Y	NC	NC	NC
TRIP	Simple	Y	NC	NC	N	N
On data centric	Simple (medium)	Y	Y	NC	N	NC
RMCV	Complex	Y	Y	NC	N	N
Intrusion aware trsut model	Simple (medium)	Y	Y	Y	NC	N

Reputation based trust model	Simple	Y	Y	NC	N	NC
ERS	Simple (medium)	Y	Y	Y	N	N
RATE	Complex	Y	NC	NC	N	Y
BTM	Simple (medium)	Y	Y	Y	Y	Y
RaBTM	Simple	Y	NC	Y	N	N

Note: Y-YES, NC-NOT COMPLETELY

Table 3. Comparison of Trust Provided in VANET (Based on Metrics)

	Metrics										
Approaches	**Time**	**Distance**	**Rec. by vehicle**	**Rec. by RSU**	**Exp.**	**No. of sender**	**Velocity**	**Vehi-cle position**	**Vehicle direction**	**Type of vehicle**	**Type of event**
A multifacted approach	Y	Y		Y	Y					Y	
TRIP			Y	Y	Y						
On data centric	Y	Y								Y	Y
RMCV						Y					
Intrusion aware trsut model	Y	Y				Y					
Reputation based trust model			Y			Y				Y	
ERS			Y			Y					Y
RATE		Y									
BTM	Y	Y	Y				Y	Y	Y		
RaBTM	Y	Y	Y	Y			Y	Y	Y		

Note: Y-YES, EMPTY SPACE- CAN NOT SAY

Table 4. Criteria for Trust Models in Moving objects

Feature	**Pending**	**In progress**	**Covered**	**CoRS**	**TRIP**	**DCTE**	**DECADE**
				Existed Approaches			
Low complexity		No		P	P	T	T
Scalability			No	T	T	T	P
Sparsity	No			T	P	P	P
Security and privacy level		No		T	P	P	P
mobile patterns independent			No	P	P	P	P
Trust and reputation decentralization			No	P	P	T	T
Confidence measure	No			F	T	T	P
Event and spatio-temporal specification			No	T	T	T	T

Note: P-Partially, F-Fail, T-Total

References

[1] A. K. Tyagi and N. Sreenath, “A Comparative Study on Privacy Preserving Techniques for Location Based Services”, BJMCS, vol. 10, no. 4, **(2015)** July, pp. 1-25.

[2] P. Zacharouli, A. Gkoulalas-Divanis and V. S. Verykios, “A K-anonymity model for spatiotemporal data”, In Proceedings of the IEEE Workshop on Spatio-Temporal Data Mining (STDM), **(2007)**, pp. 555-564.

[3] A. K. Tyagi and N. Sreenath, “Location Privacy Preserving Techniques for Location Based Services over road networks”, ICCSP, **(2015)** April 2-4, India.

[4] A. K. Tyagi and N. Sreenath, “Future Challenging Issues in Location Based Services”, IJCA, (0975 – 8887), vol. 114, no. 5, **(2015)** March.

[5] M. Raya, P. Papadimitratos, V. D. Gligor and J.-P. Hubaux, “On data-centric trust establishment in ephemeral ad hoc networks”, in the 27th Conference on Computer Communications, INFOCOM, IEEE, Phoenix, AZ, USA, **(2008)**.

[6] M. Gruteser and D. Grunwald, “Anonymous usage of location-based services through spatial and temporal cloaking”, In Proc. of MobiSys, **(2003)**, pp. 31-42.

[7] M. F. Mokbel, “Privacy in location-based services:start-of-the-art and research directions”, Proceeding of 8th International Conference on Mobile Data Management (MDM); Mannheim, Germany, **(2007)**.

[8] B. Gedik and L. Liu, “Protecting location privacy with personalized k-anonymity: Architecture and algorithms”, IEEE Trans. Mobile Computing, vol. 9, no. 1, **(2008)**, pp. 1–17.

[9] H. Kido, Y. Yanagisawa and T. Satoh, “Protection of location privacy using dummies for location-based services”, Proc. the 25th International Conference on Distributed Computing Systems (ICPS), **(2005)**.

[10] T. M. Truta and B. Vinay, “Privacy protection: p-sensitive k-anonymity property”, Proceedings of the 22nd International Conference on Data Engineering Workshops (ICDEW), IEEE Computer Society, Washington, DC, USA, **(2006)**.

[11] C. R. Wong, J. Li and A. Fu, “(α, k)-anonymity: an enhanced k-anonymity model for privacy preserving data publishing”, Proceedings of the 12th ACM SIGKDD Conference, PA: ACM Press, Philadelphia, **(2006)**.

[12] L. Sweeney, “Achieving k-anonymity privacy protection using generalization and suppression”, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, vol. 10, no. 5, **(2002)**, pp. 571-588.

[13] “U. D. of the Interior, Us geological survey web page”, **(2003)**, [Online] Available: http://www.usgs.gov/.

[14] M. C. M. Center, “Spatial data transfer format”, **(2003)**, [Online Available]: http://mcmcweb.er.usgs.gov/sdts/.

[15] I. A. Sumra, H. Hasbullah, *et al.,* “Trust and Trusted Computing in VANET”, Computer Science Journal, vol. 1, Issue 1, **(2011)** April.

[16] https://www.abiresearch.com/pages/about-abi-research/.

[17] https://en.wikipedia.org/wiki/Augmented_reality.

[18] L. Huang, K. Matsuura, H. Yamane and K. Sezaki, “Towards modeling wireless location privacy”, in Proceedings of Workshop on Privacy Enhancing Technologies, **(2005)**, pp. 59-77.

[19] M. Li, K. Sampigethaya, L. Huang, *et al.,* “SWING & SWAP: User-centric approaches towards maximizing location privacy”, in Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, **(2006)**, pp. 19-28.

[20] K. Sampigethaya and L. Huangy, “CARAVAN: Providing Location Privacy for VANET”, In Proc. of Embedded Security in Cars, **(2005)**, pp. 0710.

[21] N. Bibmeyer, S. Mauthofer, B. Kpatcha and F. Kargl, “Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters”, IEEE, Seoul, Korea, **(2012)**, pp. 78–85.

[22] A. K. Tyagi and G. Aghila, “A Wide Scale Survey on Botnet”, International Journal of Computer Applications, vol. 34, no. 9, **(2011)** November.

[23] J. Freudiger, M. Raya, *et al.,* “Mix-zones for location privacy in vehicular networks”, In Proc. of ACM Workshop on Wireless Networking for Intelligent Transportation Systems, **(2007)**.

[24] S. Gurung, D. Lin, A. Squicciarini and E. Bertino, “Information-oriented trustworthiness evaluation in vehicular ad-hoc networks”, in Network and System Security. Springer, **(2013)**, pp. 94–108.

[25] U. F. Minhas, J. Zhang, T. Tran and R. Cohen, “multifaceted approaches to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks”, IEEE Trans. Syst. Man Cybern.C Appl.Rev., vol. 41, no. 3, **(2011)**, pp. 407–420.

[26] F. G. Mármol and G. M. Pérez, “TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks”, J. Netw. Comput.Appl., vol. 35, no. 3, **(2012)**, pp. 934–941.

[27] L. Liu, “Privacy and Location Anonymization in Location-based Services”, SIGSPATIAL, **(2009)**.

[28] J. P. Daries, *et al.,* “Privacy, anonymity and big data in social sciences”, ACM, vol. 57, no. 9, **(2014)** September.

[29] J. A. Perolle, “Computer-supported cooperative work, in Computers, Surveillance and Privacy”, D. Lyon and E. Zureik, Eds., Minneapolis, MN: Univ. of Minnesota Press, **(1996)**, pp. 47-59.

[30] A. K. Tyagi and N. Sreenath, "Preserving Location Privacy in Location Based Services against Sybil Attacks", IJSIA, vol. 9, no. 12, **(2015)** December, pp. 189-210.

Author

Amit Kumar Tyagi, He is currently working as Ph.D Research Scholar (Full-Time) in Pondicherry Engineering College, Puducherry. He has completed his M.Tech in Computer Science and Engineering from **Pondicherry University, Puducherry**, in 2012. His research interests include Smart and Secure Computing, Network and Information Security, Theoretical Computer Science, Privacy (including Genomic Privacy), Evolvable Hardware, Parallel Algorithms, Cloud Computing.

N. Sreenath, is currently working as Professor in Pondicherry Engineering College, Puducherry. He completed his PhD in Computer Science and Engineering from **Indian Institute of Technology, Madras**, in 2003. His primary research interest lies in WDM Optical Networks, High Speed Networks.