# Providing Privacy Preserved and Trusted Location Services in Location based Services

Amit Kumar Tyagi
Research Scholar

N. Sreenath
Professor

T.Frederick Fernanzdez
Assistant Professor

A. Rajeswari
Software Engineer

## ABSTRACT
Technological advances are changing the face of our society dramatically. New technology affects individuals countless ways, including the manner in which they interact with each other, with businesses, and with the government. Today's technology makes possible to accomplish many tasks more efficiently, i.e, providing various location based services to vehicle users over road network. Vehicles used location based services (LBSs, during their journey/ in road) to find the nearest location, point of interests etc. But these services do not come without costs, i.e., service providers request a little amount for that, plus some sensitive information of vehicles users. Due to its centralised and open nature to all, comes with a trust, priavcy and security issues. To communication with service provider, we need a secure, authentic and trusted infrastructure. The target of Vehicle Ad-hoc Network (VANET) is achieving higher level of safety (i.e., to provide secure, trusted and privacy preserved communication) in the road network. The main aim of this paper is to propose a trust model for vehicular environment with desired level of privacy protection. This work contains two different modules. First, this work proposed a location privacy protection algorithm (for preserving privacy protection of moving objects during accessing location services), procedure of this algorithm; simulation results in detail. Second, it provides an algorithm to update trust value (in term of trust levels) for VANET users during acessing LBSs inside a mix zone. The results show that proposed method outperforms the existing privacy preservation method by effectively enhances privacy and trust against various adversaries. This work clearly explained the answer of following question "How to gain maximum location privacy preservation with positive trust in location based services?"

## Keywords
Location Based Services; Privacy Protection; Trust Level; Vehicle Ad hoc Network; Location Privacy.

## 1. INTRODUCTION
Due to enhancement in mobile position technologies/ wireless communication, lives/ safety of human being is a becoming an important issue. Thousands of people die in road accidents over the globe every year. Several people using own mobile devices with positioning capabilities use various location-based services (LBSs) to obtain all kinds of information about their surroundings (communication with neighbor vehicle users also). During communication, Privacy concerns have emerged as a challenging issue because many of location services enable by design, i.e., service providers collect detailed location information about their visited users. LBSs provide users with valuable information about their surroundings such as traffic status (e.g., Beat the Traffic, or INRIX Traffic Maps, Routes & Alerts), nearby POI (points of interest, e.g., Google Maps), or friends' activities (e.g., Foursquare or Google Latitude). Market research firm ABI Research forecasts, the global number of people to enjoy location-based services from 1.2 million in 2006 increases to 31.5 million in 2011 and will cross one billion mark till 2020. Basically location services can be trust and non-trusted types. Trusted location services, i.e., provides guaranteed privacy by a third party like Hippocratic databases while Non-Trusted location services are where thirst party is not trusted, i.e., chances of revealing of personal/ location information are more in this case. In this, users 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. In vehicular network, their role (attacker) is more prominent because they can potentially change the life critical information on the road, for example, giving wrong information about congestion/ jam, fire accidents etc. So here biggest is "How to find trusted location services and users over road in instant time"?

VANET over road can be used to reduce death rate and improves traffic safety system [2, 3]. In VANET, vehicles can send and receive safety messages to each other on the road to ensure safety of human life. Devices using wireless devices are easily traceable/ provide to their personal accurate position or any other relevant information anytime and anywhere. In LBSs, mobile (wireless) users widely had known about serious privacy threats. These important threats are due to the leak of service content and position privacy. Service content threat is the potential exposure of service uses [3, 10]. During accessing location services user has disclosed her location/ information in her service request. But this information can be passed by a central party to a third party user. It may reveal sensitive private information such as political/religious affiliations, health conditions, alternative lifestyles, habits and so on. Ultimately, privacy is about feeling, and it is awkward for one to scale her feeling using a number [3, 4]. A very coarse location will make it difficult to provide meaningful LBS. There are several (popular first three) important metrics for measuring the level of location privacy guarantee, discussed in [1, 3]. Privacy Quantification can be done based on user preferences, anonymity, context constraints, interaction history and feedbacks etc. Additionally, to maintain trust in LBSs, author discussed event and data centric models. In event centric case, high mobility of vehicles leads to failure to collect enough information about the neghbors/ sender. While in sparse traffic density, it does not perform well (in data centric). In location based services, trust can be differentiating according to location services or based on based on user queries.

### 1.1 Privacy and Trust challenges in LBSs
Today's Mobile devices are increasingly being used by different types of people. With this, "Right to privacy as a fundamental right is implied in right to life and personal

liberty". Privacy is generally the information that you don't want others to know [1, 3]. Privacy matter person to person, i.e., for VVIPs, it requires privacy most while a normal person requires privacy less in metrics. Actually, normal or maximum people in India (or in all over the world) do not even care about their privacy. Privacy can be in terms of location, data, identity etc. Here, we focused only on location privacy. Location privacy is defined as "the ability to prevent other unauthorized (or malicious) parties from learning one's current or past location" [11, 13, and 14]. A user is only responsible person for losing his privacy. Maximum protection of privacy covers huge cost while less privacy protection covers nothing. Additionally, Trust can be described as the expectation and belief about future behavior, based on experiences and evidences collected in the past, either direct or indirect [5]. Trust may be human to human, machine to machine, human to machine, or machine to human. Trust is a vitally important part of human being. Maximum people are unaware about their actions which are influencing trust among them. Every relationship is depend on belief, i.e., on trust. Together, every relation among consumer and company is also depending on trust. Today "secure system" or "trust me" words do not work for company/ location service providers. Specially, till when we don't provide better results to users than others. It develops as early as the first year of life and continues to shape our interactions with others until the day we die. Today's Privacy, Trust and Security have become a serious concern for vehicle users who used location services like; acquire geographical location, coffee shop etc. Privacy breach is equal to positive membership disclosure for vehicle user. The relation between trust and privacy can be shows like;

$$\text{Trust} \rightarrow \text{Privacy} \rightarrow \text{Security}$$

Trust and Privacy are the two key parts of Security and it is undoubtedly a necessity to develop certain level of trust for moving objects. Trust isn't as asymmetric, i.e., hard to gain but easy to lose, as previously thought is good news for many but perhaps not so surprising after all. Once trust is lost in relationships, it can be recovered easily with a word "sorry" but among companies and customers; it cannot recover with a word "sorry". To avoid this problem and adequately preserve the privacy of the users when requesting LBSs, sophisticated algorithms have to be devised. After reading so many research articles, some of the questions arise in author's mind like:

a) How to protect user's privacy against compromised LBS providers and attackers are of vital to exiting systems"?
b) Which data is more sensitive to preserve private/ protect from user's point of views?
c) Who is trusted client and How to find it?
d) What are the methods used in the proposed trust models?
e) What are the trust metrics used to measure trust in the existing trust model?
f) What are the properties of the trust model?

Moreover this, a centralized model for providing certain level of privacy for LBSs is discussed in figure 1.

## 1.2 Leaking of Location Privacy and Trust during accessing LBSs

During accessing location services, location privacy of an user leaked in three ways (i.e., using Restricted Space Identification (RSI), Observation Identification (OI), and linking attack discussed in [3]) and two types of possible attacks (Homogeneity and Background Knowledge) on k-anonymity. An attacker use some threat model to perform any attacks, i.e., Weak Adversary Attack Model (in this weak adversary has little knowledge about the participators) and Strong Adversary Attack Model (in this strong adversary can launch the time attack such as FIFO (First In First Out) by gathering entering time and exiting time intervals). The most popular technique for designing privacy-preserving LBSs consists in obfuscating the actual location from which a query is made by constructing cloaking regions that contain the locations of k anonymous users. According to the k-anonymity metric, a user's level of location privacy directly depends on the number of other users that expose their location to the LBS using the same cloaking region and at the same time as the considered user does, while identity-wise they are indistinguishable from each other. Several other attacks are also possible on location privacy like; Message suppression attack, Jar copy attack, Disassembling attack, Localization attack, Sporadic attack, Transition attack, Timing attack, Continuous query/ range query attack and Misleading attack.

Hence to protect privacy of users, we also require trust as essential component. Trust and Privacy are co-related to each other. We want to protect user's privacy in such a way that trust among users also should be improved. Without privacy guarantee, lack of trust will cripple the promise. Providing 100% privacy preservation and trust is clearly impossible among human beings till communication takes place among them [1]. But we hope that, the proposal will help create a secure, trustworthy, and privacy preserved environment for vehicle users over road.

Finally the organization of the rest of the paper is followed as: Section 2 discusses about related works to this paper. Following that, in Section 3, proposes an algorithm for offering privacy in LBSs and then discuses simulation results. In addition, Section 4 presents a novel idea for offering trust in LBSs to moving objects. Section 5 discusses future works related to our work. Finally, Section 6 concludes this work in brief. This work interchangeably uses 'mobile users', 'VANET users' or vehicle users' words with respect of moving objects.

# 2. RELATED WORKS

As discussed, protecting user's location privacy in LBSs has received considerable attention over recent years by severe researchers. Today's various Location Privacy Protection Mechanisms; location perturbation and obfuscation methods have been widely used and explained to protect user's location privacy. Protecting location privacy through various methods like pseudomyzation, perturbation, adding dummies and reducing precision is not efficient. While privacy, security based on trust, for example, if a user losing her identity/ data in a hospital, i.e., she lost her privacy, i.e., loss her trust also among hospital's staffs. This type of cases occurred only due to some security weaknesses or by human error. In order to solve the problem of location privacy leakage, privacy protection and trust enhancement are essential one issue. 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. Several existed privacy protection methods are discussed in [1, 3]. We have also proposed a novel approach against Sybil attack in [7].

Here location privacy protection is the method that sends the false location information or anonymous identity and location

information to the authentic server. These methods can be divided into two categories: (a) protect the user's ID information (conceal anonymity or pseudonym), making the server service [7] does not know the requestor true ID; and (b) protect the location information of the user by submitting a region instead of true location of the user [3]. The proposed privacy protection method in this paper makes improvement as compared with the existed methods mentioned above. It combines the advantage of Pseudonym Method; Silent Period (SP); and Swing and Swap (SS) method [12] that suggests a location privacy protection method based on pseudo game including anonymity, diversity to realize the protection.

In vehicular communications, the way in which a user discloses his information that contains his privacy (personal/ location information) can be categorized into three classes (from the viewpoint of privacy protection patterns): direct mode, confusing mode and indirect mode. In direct mode, an entity discloses its privacy information directly to another interactive entity. In Confusing mode, privacy information is disclosed with some ambiguity (noise). And in Indirect mode, the information owner may need some help from a trusted third party in order to complete the interactions. This mode incurs the highest level of complexity of interactions which can occur when the information owner has a low level of trust on the information requester. On other side for trust, we 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 trust management. Various models to establish 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 data centric trust establishment (RATE) [3]. Raya et al. [8] proposed a framework for data-centric trust establishment where trust in each individual piece of data is computed. The basic idea is to suggest a vehicle to trust a message that has been evaluated to be trustworthy by various trusted peer vehicles [9]. Various existed methods (criteria) for trust management have been covered in [3]. In summary, existing solutions for the location privacy model can be classified into four categories, i.e., *Query enlargement* techniques, *Dummy-based* techniques, *Progressive retrieval* techniques and *Transformation-based* techniques.

This section discussed about related work done in this concern areas. Now next section will discuss the proposed algorithm in detail.

# 3. PROPOSED PSEUDO-GAME ALGORITHM TO PROTECT LOCATION PRIVACY

A good privacy-trust relationship can increase the rate of successful interactions and consequently the level of satisfaction of the communicating entities. Severe Researchers have published different-2 work to protect location privacy for LBS. Table 3 and table 4 in [1], provide summary of various privacy protection schemes in detail. As summary, [1] discussed about personalized k-anonymity, p-sensitivity, location spatial cloaking [11], pseudo location method, Spatio-temporal cloaking, and Mix-zone etc. approaches. Author concludes in [1], still there is no single framework for preserve the privacy of vehicles users during accessing location services.

Basically 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, i.e., based on trust third party (TTP) model (Refer figure 1). Here pseudo-game based *location privacy protection* method is based on the centralized model.

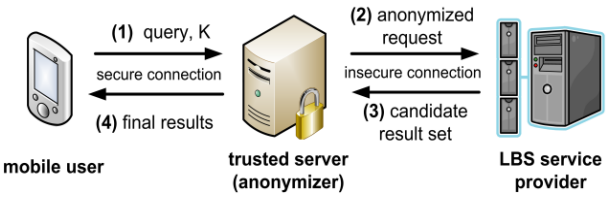


**Fig. 1 The centralized model for privacy in LBSs**

In this, it collects several type of information, i.e., identity anonymous, users footprints; service requests and response anonymous and feedback sent to the user will be kept secured (i.e., maintaining confidentiality, integrity and availability property) by the third trust party, who works as a secure and privacy protected communication bridge to the user and LBS provider.

## 3.1 Proposed Algorithm to Protect Location Privacy

To protect the location privacy of vehicle users, we need a secured communication channel between user and LBS service provider. There are two kinds of approaches for attacker to acquire user's location when communication established between user terminal and LBS, i.e., directly achieving query information from user terminal (Note-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) and achieving query information of user from LBS (Note- in this attacker can speculate user's location directly). Moreover this, attacker can acquire enough information about a particular user based on information collected from journey travelled over road and visited location by a user/ her (e.g., a person daily goes to his clinic at 2:00pm through NH-24 highway via dropping his son for tuition on a location M). Following proposed algorithm provide a certain level of privacy protection to such type of problems.

**Proposed Algorithm: preserving privacy of users while accessing location based services**

Input: number of n user over the road network

Output: number of p attackers (privacy preserved of users q= n-p)

**Begin**

1. If (at least one neighbor) and (not in silent period) then
2. Broadcast initiation message to change pseudonyms
3. Maximum gain = $\log_2$(number of neighbors)
4. If (at least one neighbor) and (current location privacy< maximum gain) and (not in silent period)
5. Then go to step 2
6. If (receive initiation message ) or (initiated change) then
7. If a < b then
8. Change pseudonym and comply with silent period

(SPmax)

9. Else
10. Quit
11. Else
12. Keep pseudonym
13. M ← estimate (n) // (number of neighbors)
14. Calculate b*
15. If a ≤ b* then
16. Play c
17. Comply with silent period (SPmax)
18. Else
19. Play d
20. Else
21. Follow step 12
22. Follow step 6
23. Follow step 13
24. Last N=n
25. For t=0 to SPmax do
26. If a ≥ $\log_2$ (n) then
27. Follow step 19
28. Quit
29. If n=last N then
30. Play c
31. Follow step 17, and last N=n then
32. Follow step 12
33. Follow step 6
34. Throw a coin
35. If heads then
36. Follow step 8
37. Else
38. Follow step 12

**End**

This algorithm used concept of being silent and changing pseudonyms to protect her location privacy. Basically, human being very much attracting with visual data, i.e., with movies, playing video games etc. Various games can be played orally. In this work, authors define the concept of pseudo-game due to huge attraction of vehicle users with playing games. Results are showed here according to utility and taking decisions related to play that game to make communication with others vehicle users. Here b is fixed threshold, and a is current location privacy of node/ user. Result with proposed algorithm mention in fig. 2. With proposed algorithm, the LBS provider is unable to link users with their visited locations, and thus is capable of inferring sensitive private information. (Note-This work can be used in VANET's applications like carpooling, parking of vehicles over a journey).

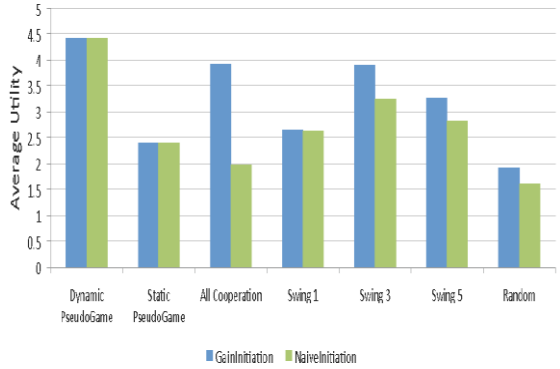


**Fig. 2 Average utility with each decision and initiation protocols**

Because this approach preserves privacy [15, 16] based on requirements, i.e., identify the requirements of mobile users based on information (i.e., information can be top secret, secret, confidential and unclassified), i.e., based on preferences of sensitive information. While existing approaches preserve privacy based on user's location preferences while in LBSs attacker can be anywhere. This is the only reason maximum existing privacy preserving algorithms fail to protect the privacy of vehicle users.

## 3.2 Experiment Simulation

To simulate the automobile over road network moving object generator is used. The service request is sent according to the location information of moving object generator. The map and configuration uses here like used in [3]. In [3], results are discussed with this requirements, i.e., k-anonymity and pseudonyms method. But in this proposed work, results are discussed with pseudonym using swing and swap and silent period methods. This work provides similar results like in [3]. Fig.2 shows that, randomly we get less naïve initiation and gain initiation values than any other cases.

Hence the aim of the presented methodologies is to protect the location of the requesters of LBSs in both static and continuous queries. This section discusses about experimental results derived through combination of pseudonyms, silent period and swings and swap methods to protect user's privacy. We believe that our proposed method provide a certain level of privacy to moving objects in LBSs. Now next section discussing a trusted computing flow diagram to enhancing trust level among vehicle users

# 4. TRUSTED VEHICULAR COMPUTING MODEL

As discussed, Trust is essential key element in creating a trustable vehicular ad-hoc networks (VANETs) environment which would help promote a safer road environment. The basis of VANET is the exchange of data between entities, and making a decision on received data (or event/ information) is usually based on information provided by other entities, trusted or not. Trust is a part of all significant relationships: friends, parents, siblings and the person you are dating. Regarding scientific texts existed in different fields; a widely accepted definition about trust can be mentioned as; "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another". Further as accepted definition of trust, "Trust is a subjective assessment of

another's influence in terms of the extent of one's perceptions about the quality and significance of another's impact over one's outcomes in a given situation, such that one's expectation of, openness to, and inclination toward such influence provide a sense of control over the potential outcomes of the situation" [3, 17].

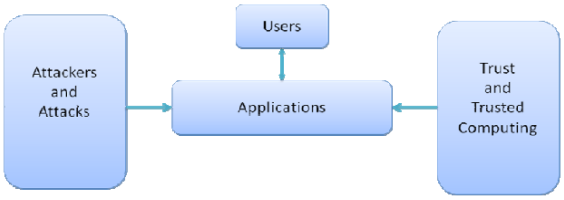


**Fig. 3 Trust Model [3]**

Trust is a vital ingredient of any successful interaction between individuals, among organizations and/or in society at large. Basically the kind of trust we are talking about here is not the kind of trust we have in friends and family (i.e., interpersonal trust) or in other people in general (i.e., social trust), but trust in specific individuals whose role it is to assess, manage and communicate information about risk. Such trust has been referred to as "role-based trust" since "it is not the person in the role that is trusted so much as the system of expertise that produces and maintains role-appropriate behaviour of role occupants". In marginal trust, bad information is stronger than good one (negative bias). Trusted in one system can be different in another system, but the goal remains the same, i.e., to improve relationship.

Trust is the key element in creating a trusted vehicular environment which promotes security in vehicular networks. Now days, there are various tools and technologies exist to measure trust include surveys, focus groups, before and after polls/feedbacks, model building, multivariate analysis projects etc., i.e., several researchers have developed mathematical methods such as Bayesian probability, Beta probability, maximum likelihood, game theory, weighted arithmetic means, and average of weighted recommendations to measure the degree of belief or recommended trust. Today's computing Trust for VANET users is a relatively new technology which will attract more researchers from auto-industries and academia in future. Figure 3 and 4 shows that "How trusted computing communication can be maintained between all entities of the network?" Figure 3 can be useful to build/ increase trust value among users like in figure 4. This is an ideal condition that we want to achieve in real vehicular network to provide positive trust.

## 4.1 Trusted Model for Vehicle Users

Trust models such as belief, organizational trust, dispositional trust, recommended trust, and direct trust have been proposed for pervasive systems. A trust is typically based on the trustor's characteristics such as ability, integrity, and benevolence and should not be a blind guess. It is expressed either by value, rating, or ranking or as probability or belief. Trust attributes such as integrity, motivation, competence, and predictability are proposed to measure the confidence level. Here we used five basic entities of trust and when all these entities work together then we can develop a chain of trust in the vehicular network. Equation 3 discussed in [3] explains that all modules are trusted and worked together for achieving chain of trust in system. Trust degree (value) can also be measured from interaction frequencies between trustor and trustee or from context-dependent direct and indirect recommendations collected from selected users. Figure 4 provides a certain trust value to mobile users based on received feedbacks from other existed users in the vehicular environment. This work receives trust feedback values from other users and updates it according to received responses. Basic concept is that collect information about a user 'A' form other several users and compute trust value for that user 'A'. (*Note*-Disadvantage of decentralized system: conflict, not proper contact between users, more financial burden, not following of unique policies etc.). This work is totally different form existed models like, it does not communicate provide V2V communication, so misleading, linking attacks etc. are not possible here. And in this model, vehicle can communicate directly with TA (centralised structure) not RSU to reduce the response time and various transition, timing or DoS (denial of service), Sybil attack etc.

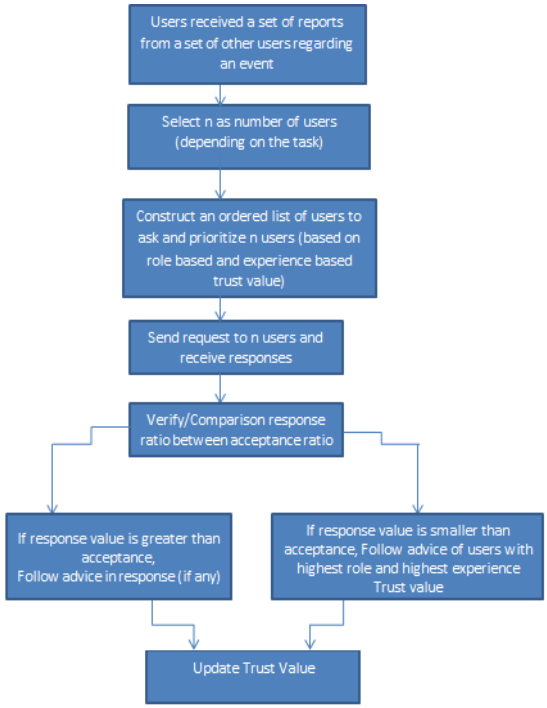


**Fig. 4 Proposed Trusted Flow Diagram**

Note that a little difference with our proposed algorithm with an algorithm discussed in [17] is that, here we are collecting reports from n users, whereas in latter algorithm, authors receive n different reports, from n different users. Generally, attackers are those people, who knows "How change the behavior of the entity and break the trust"? So first of all we should study about the attackers and attacks because it is directly related to change the behavior of a vehicle user. All attackers do not harm to a user, but some have intention to harm. If we want to achieve the trust and develop the trusted computing environment then we should uses feedback (ask) from other users about any user using LBSs. More number of vehicle users in LBSs (also in a mix zone) create more problems, i.e., the chance of revealing user's identity and loosing of trust is also too high during accessing location services. (In [3], authors discussed more about Level 1 attackers (L1) and level 2 attackers (L2) in detail).

## 4.2 Trust Levels

A trust (among person) or belief can be measured in different levels, i.e., can be notified as:

- **Zero Trust:** in this, the attacker is active and is able to use all kinds of entities in the network and create problem by launching different types of attacks (passive/ active) [3]. An entity which trust level cannot be validated or that, actually posses a zero trust value. Hence there is no communications in network, which means that the trust value for sending and receiving is zero due to specific attacks.
- **Weak (Low) Trust**: in this (First level), the attacker is able to launch different kind of attacks and scopes of the attacks are within some specific region. It can be assigned by default to private vehicles.Some entities are effected with these attacks whereas other entities of the network performing their task properly and serve the users. In this, 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.
- **Medium Trust: (TL = 2),** Second level trust that can be assigned by default to regional authorities such as police vehicles or traffic authorities.
- **Semi-full Trust: (TL = 3),** Third level trust, that can be assigned by default to emergency vehicles, and other related authorities.
- **Strong Trust:** in this (Fourth level), all entities of the network are trusted and work properly. There are no attackers in the network and this is a very ideal condition and every entity performing their task properly. In this, trust assigned either to enforcing law authorities in liability cases, or manually assigned by the driver to an entity which is well known and strongly trusted.

Clearly speaking, bad news had a larger (negative) impact on trust than good news but this was moderated by prior attitudes towards the hazard and the risk manager, by the amount of information conveyed and the exact nature of the error/ correct decision. Moreover, we would be surprised if there weren't further psychological processes that could shed additional light on these issues. Trust can be discussed further as "The trust of a particular node is a subjective assessment by an agent (user)/ other peer node on the reliability and accuracy of information received from or traversing through that node in a given context. Trust reflects the belief or confidence or expectations on the honesty, integrity, ability, availability and quality of service of target node's future activity/ behaviour. It also reflects the mutual relationships where a given node behaves in a trustworthy manner and maintains reliable communications only with nodes which are highly trusted by the given node".

Trust in a VANET is viewed in this way, "all components (User, Vehicle, and RSU) of network should behave in an expected manner and serve the user". "The trustor entity not only believes the trustee will behave in an expected manner but also is willing to be vulnerable for that belief in a specific context, i.e., trustor is willing to assume the risk that the trustee may not behave as expected". There are the two basic options for establishing trust, i.e., statically (by the static dependence on a security infrastructure) and dynamically (by the dynamic build-up of trust in a way that is self-organizing). 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 behavior, i.e., Positive Behaviour (Trusted users and non-trusted users) and Negative Behaviour (Non-trusted users) discussed in [3]. Some of the properties and metrics required for a trust model also discussed in [3]. In last, trust level for vehicle users (in an area) can be compute as:

**Trust level=Total number of neighbor in a zone/Total no of vehicle users existed in a zone (1)**

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 (2)**

From equation 1 and 2, we can derive that role of neighbor node or total negative trust, which has an important role to maintain a certain level of trust including privacy protection. Table 4 in [3] provides the complete description about existing methods to provide a certain level of trust to vehicle users. We see that, Trust can also be computed based on reputation based ranking, i.e., based on previous records of vehicles, direct ranking, i.e., based on person Frobenius theorem based on message strength (i.e., each participant vehicles can compute trust value based on message received from other vehicles), i.e., based on message strength, and last one is indirect ranking, i.e., it evaluated based on the number of authentication certificate exchange at the certain time of vehicles with in communication range.

Hence as discussed in vehicular environment, the role of vehicle user and infrastructure is most important for building the chain of trust. Chain of trust would be affected if user or trusted authority (TA) is not performing their task accurately. In their respective Vehicles, user communicates with application unit (AU)/ Road Side Unit (RSU) and sends messages to other Vehicle's users over road network. Now next section will deal with future work related to presented work in section 3 and 4.

## 5. FUTURE WORKS

The role of privacy as an attribute in trust is well understood in human relationships. However much of the technical work in protecting privacy has been addressed from a security standpoint, i.e., assuring confidentiality of data or providing complex access control models. Trust and Privacy are in practice softer technologies that provide reinforcement that privileged information given is enacted on within the bounds of a mutually agreed policy. The problem of protecting privacy of individual data used for research is not new. A breach of privacy occurs when individuals are not aware that the data have been collected in the first place, have been passed onto other companies and organizations, or have been used for purposes other than the one for which they were originally collected. Even when individuals approve of use of their personal records for data mining and statistical analysis, for example, in medical research, it is still assumed that only aggregate values will be made available to researchers and that no individual values will be disclosed.

Privacy and Trust concerns have emerged because many of such services enable, by design, service providers to collect detailed location information about their users [3]. Human model to maintain/ compute trust is complex, slow, and expensive, but it is also ultimately resilient. This compares quite badly to the normal trust models used in computing

systems where the model is often reduced to trust for a single transaction with third parties brought into the loop to give validation. For this, we can create masked micro-data that satisfy *p*-sensitive *k*-anonymity using the existing anonymity algorithms with some necessary metrics, and we will compare the running time of these modified algorithms against our existed algorithms. As an extension of this work, we can provide location privacy protection in term of user interface like alert message, in checkbox etc. But we cannot protect a system which is internally damaged, i.e., if a user like our friend is travelling with us and leaking our privacy to an adversary then for such types of problems we need strong trust and we cannot protect such types of challenges/ problems. So to provide a certain level of privacy, trust from (or in) external world, first we assume that, we are internally trusted or secured. For future work, we can focus on questions mentioned in section 1.1. Proving trust to users inside location services using new privacy principles also a challenging (future) task. Hence as summary, there are a number of further important research issues for continuous LBSs, which we omit due to space constraints. Now next section concludes this work in brief.

# 6. CONCLUSION

Recently privacy of VANET was an important issue to be addressed by designers of VANET infrastructure security. Today's several attackers have changed their attacking behavior to reveal the identity/ location of moving objects. Attackers always try to tamper the information and create troubles in the network, which creates the problem of leaking of information and loss of trust. In this work, a privacy preserved algorithm is proposed which provide a trusted communication with other users during accessing location services. We show that, this algorithm can effectively anonymize all service requests with shorter execution time, which will realize the position privacy protection more efficiently. Further, to improve the certain level of trust during accessing LBSs, we discussed an algorithm to update trust value of vehicle users' after receiving feedback from other vehicle users. The level of trust develops in the network if the system is able to control attackers from distracting the information. In last, we can say, this work maintains trust and certain level of privacy among vehicular users without revealing her identity in LBSs. For future research, there is needed to build a generic architectural framework towards addressing the trust, security and privacy issues/challenges in a holistic manner. 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 we are in a new era where providing security and privacy issues will help us to discover new knowledge that no one has discovered before. So everybody is warmly invited to provide a safe and secure and privacy preserved environment (with required trust) to the vehicle users (when requesting services in LBSs).

# 7. CONFLICT OF INTERESTS

The authors declare no conflict of interest regarding the publication of this paper.

# 8. REFERENCES


[1] Amit Kumar Tyagi, N. Sreenath, A Comparative Study on Privacy Preserving Techniques for Location Based Services, BJMCS, July, 2015 10(4): 1-25, 2015.

[2] Irshad Ahmed Sumra,Halabi Hasbullah et al., Trust and Trusted Computing in VANET, Computer Science Journal, Volume 1, Issue 1, April 2011.

[3] Amit Kumar Tyagi, N. Sreenath, Providing together Security, Location Privacy and Trust for moving objects, IJHIT Vol.9, No.3 2016, March, 2016.

[4] http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=2594&context=etd

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

[6] Amit Kumar Tyagi, N. Sreenath, Future Challenging Issues in Location Based Services, IJCA, March, (0975 – 8887) Volume 114 – No. 5, 2015.

[7] Amit Kumar Tyagi, N. Sreenath, Preserving Location Privacy in Location Based Services against Sybil Attacks, IJSIA Vol.9, No.12 2015, pp.189-210, December, 2015.

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

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

[10] D¨urr, F., Skvortsov, P., Rothermel, K., "Position sharing for location privacy in non-trusted systems", In: Proceedings of the 9th IEEE International Conference on Pervasive Computing and Communications, Seattle, USA, March 2011.

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

[12] 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.

[13] Skvortsov, P., D¨urr, F., Rothermel, K., "Map-aware position sharing for location privacy in non-trusted systems", In: Proceeding of the 10th International Conference on Pervasive Computing, Newcastle, UK, and June 2012.

[14] ChiYinet. al., "ChowTrajectory- Privacy in Location based Services and Data Publication," SIGKDD Explorations, Volume 13, Issue 1, page 19, 2011.

[15] Chow, Chi-Yin, Mokbel, Mohamed F., "Trajectory privacy in location-based services and data publication", ACM SIGKDD Explorations Newsletter, 2011.

[16] XinxinLiu et al., "Privacy Preserving Techniques for Location Based Services in Mobile Networks", IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012.

[17] Amit Kumar Tyagi, N.Sreenath, "Ensuring Trust and Privacy in Large Carpooling Problems", in proceeding of International Conference on Computational Intelligence and Communication (CIC), Vol. 14. International Journal of Computer Science and Information Security (IJCSIS), Pondicherry, India, pp. 1-11, 2016.