British Journal of Mathematics & Computer Science
19(6): 1-23, 2016; Article no.BJMCS.27737
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Never Trust Anyone: Trust-Privacy Trade-offs in Vehicular Ad-Hoc Networks

Amit Kumar Tyagi[1*], Sreenath Niladhuri[1] and R. Priya[2]

[1]Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry-605014, India.
[2]Department of Information Technology, RAAK College of Engineering and Technology, Puducherry 605110, India.

Authors' contributions

This work was carried out in collaboration between all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJMCS/2016/27737
Editor(s):
(1) Doina Bein, Applied Research Laboratory, The Pennsylvania State University, USA.
(2) Qiang Duan, Information Sciences & Technology Department, The Pennsylvania State University, USA.
(3) Paul Bracken, Department of Mathematics, The University of Texas-Pan American, Edinburg, TX 78539, USA.
Reviewers:
(1) Vaishali D. Khairnar, Mumbai University, India.
(2) Olatunji Sylvester, Federal University of Technology, Nigeria.
(3) A. Robertsingh, Kalasalingam University, India.
(4) Anonymous, Amity University, India.
Complete Peer review History: http://www.sciencedomain.org/review-history/17019

Opinion Article

Received: 16th June 2016
Accepted: 27th October 2016
Published: 24th November 2016

Abstract

Due to the rapid development of networking and communications technologies, it has made more convenient for consumers to interact with each other to exchange information in Location Based Services (LBSs) and to share digital contents, making privacy and trust protection one of the primary concerns in history of information security. Therefore, in such applications like carpooling, parking no one is trusted (i.e. applications of Vehicular Ad hoc Network (VANET)). In VANET before a genuine communication starts, certain level of trust must be set up among the cooperating substances, which may require that some data that may contain privacy about the entities which is to be shared among the entities. Thus, privacy protection and trust establishment are inter-related issues that ought to be legitimately adjusted to guarantee both a smooth correspondence and for appropriate security insurance or privacy protection. A service request typically reveals the identity (for example, IP address or caller ID) of the user but may incorporate other individual data, for example, area, time, and the kind of the service on demand. This

**Corresponding author: E-mail: amitkrtyagi025@gmail.com;*

data empowers a Location Service Provider (LSP) to construe after some time a thorough client profile with a high level of accuracy, which thus makes a huge potential for privacy invasions. The exchange of such information can be result of loss of privacy and trust among users and infrastructure. To protect such privacy, several efforts have made in past including Mix Zones. This work discusses maximum facts to improve trust, preserved privacy (with proposing a new design in spite of mix zone which has not been proposed before,), and trade-offs among them, in result this proposal saves time, fuel and cost of vehicle users. Finally, this work concludes that to gain a higher level of trust just, be self–secured i.e. not to disclose everything to someone else, because in this current world, we cannot trust perfectly on anyone.

Keywords: Trust; privacy; feedback; recommendation; Vehicular Ad hoc Network; applications, location based services.

1 Introduction

Trust is a phrase (word) that men and women (livings) regularly use to intend distinctive matters in distinctive circumstances and in different scenarios (for illustration: trust among parties, trust in the underlying infrastructure, etc.). Largely speaking, trust (believe) means an act of faith; confidence and reliance in something that's anticipated to behave or supply as promised [1,2]. When you trust someone implicitly you gain two things – either a friend for life or a lesson for life. Basically, a trust cannot be put on non-living things. This work talks about trust relationship among vehicle users i.e. among human being. Trust is the confidence between two or more human place in each other. It entails faith in users like that the other user will be honest, loyal, and consistent [3]. You could trust your acquaintances to maintain your secrets and techniques. Your significant can be faithful to others (to you, your family and friends) to defend you. When you trust anyone, you consider that you would be able to inform them about something that you are feeling or ask them for support and they will be there for you, without resentment or judgement. But whenever we discussed our some secrets to our friends or others then we have chance (possibility) of losing our trust with revealing our secrets. For example; a person does a business of diamond and one day, he told about delivery of his diamonds to his friend. Now if that friend reveals this information (or to others) to rob him over road network. As another example, if one person is scientist/professor and he discussed some issue/secrets/information about his laboratory work/research information with other users. Then "How can we say that, this person will not share these secrets with anyone". So here, two solutions comes: First do not reveal your secrets/about your work with anyone. Secondly provide or tell your secret with others in encrypted/with some misleading information. So especially here, we come with the issues of trust including privacy in road network.

Generally, Trust has received a higher attention in last few years (around the world) in a few literary works: brain science, human science, financial matters, political science, human studies and some more. Every literature approaches the issue with its own particular disciplinary focal point and channels [4]. In recent, trust got consideration in remote systems by few scientists. For instance, while sociologists tend to see trust (peer trust) as relationship in nature, a few analysts consider it as an individual view/attribute. Social psychologists will probably consider trust as an interpersonal phenomenon while Economists are additional inclined to view trust as an objective decision component to extend its possess utility. Trust is an initial step to love and an essential element for each strong relationship. Trust is a piece of critical connections among several entities like companions, guardians, siblings and the person you are dating. Trust can be characterized in various courses with the primary attributes of being asymmetric, subjective and context-dependent. But with respect to VANET sense, these definitions can be classified as:

a) Trust as risk factor
b) Trust as belief
c) Trust as subjective probability
d) Trust as transitivity relationship.

Trust is (a popular accepted definition) define as; “Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another” [5,6]. Trust is must needed term in human being i.e. nothing can be operate without it (or operable otherwise). An another 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" [7]. Trust will also be based on expertise and experiences of an entity about actors and approaches involved in personal knowledge, on laws established for ruling actors’ behavior and processes, and on laws binding actors and imposing processes (law enforcement) [8]. Trust can be present in human to human, machine to machine, human to machine, or machine to human. Trust can be created or destroyed through personal perceptions and behaviors. Trust means different meanings and definitions to different people. Sometime it is in term of belief, or faith or confidence in others. It’s predicated ‘who we are’ and ‘how we were raised’ and is shaped by our experiences and perceptions of other’s behavior. Sometimes lack of trust creates cynicism, doubt, and anxiety that lead to “time off-task” speculation and generally low energy and productivity [9]. Trust defines the individual’s expectations in the context of collection, processing, communication, and use of private information. It makes it possible for acceptance of threat and balances privacy need against advantages. Trust will also be regarded on account of growth closer to protection or privacy objectives. Trust is an improved thought of safety (security) which entails mental and sensible standards. Apart this, some researchers argue that there is no relation among privacy, security and trust. But for example, the people, who have more intention to invest on E-commerce, are assured their credit-card number [10]. Then leaking of customer’s personal/card details can be a reason of decreasing trust among end users. Leaking of customer details can be a reason of breaching privacy of the customers. Breaking of privacy or leaking of customer details may be a fault of security (see Fig. 1). Fig. 1 shows the relationship between security, trust and privacy. In that, one thing is clear; Trust, Privacy and Security are co-related and essential issues in road network. Trust is a socially based paradigm and privacy is directly proportional to trust. Trust and Privacy are strongly related to Security (see Table 1). Here we talk about only trust and privacy, because providing security to vehicle user/their location/confidential information in road network is a long-term task, this work already have done by A K Tyagi et al. in [11]. (Note-The relation between trust and privacy can be shows like; Trust→Privacy→Security).

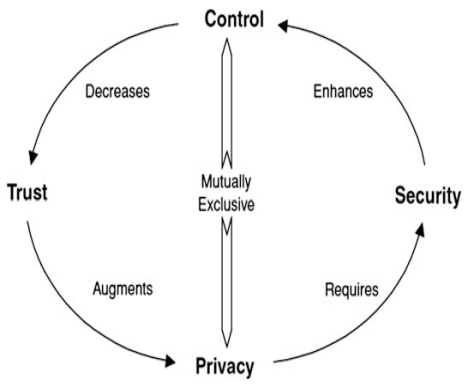

Fig. 1. Relationship between control, trust, privacy, and security

Privacy isn't nearly whether or now not you share stuff - it's whether or not or now not you have got any control over what you share, and who you have shared it with. Privacy is a foremost consideration in the design procedure (process); it could be worth the hassle to seek out a deeper local understanding of what this concept for a certain person/population and how it's normally completed in day-to-day lifestyles [12]. Besides that, it doesn't matter whether owner of an organisation believes in privacy. Sometimes even owners of an organisation do not believe in privacy [13]. For example; Millions of users are using an/any organisation’s application like Facebook, Twitter etc. In these applications, every user needs to share some

personal or identity or location information. Some users share a lot of information with these social/online applications. Every user shares his information with these organizations with some trust. But what happens, if organizations (or a hacker steal this personal information and sold to other party) misuse it against respective users. Losing of privacy comes in result of losing trust. A good Privacy-Trust relationship can increase the rate of successful interactions and consequently the level of satisfaction of the communicating entities. Without privacy guarantee, lack of trust will cripple the promise. Privacy loss is affected by the order of disclosure (your information) results in loss of trust. Trust and Privacy are inter-related constructs-the more we trust, the more information we are prepared to reveal about ourselves. Privacy on its own is about protecting users' personal information. According to Alan Westin [14] "privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information is communicated to others". So losing the credentials of users is always results in loss of privacy and trust. Throughout the approach of trust establishment, an entity may just request for some expertise information [15] that will incorporate some privacy from one or more other entities, leading to the loss of privacy to the inquiring entity. Meanwhile, the exchange of such knowledge can help in establishing beliefs (trust) among the entities for future communication. With privacy more suitable credentials, trust negotiation has the knowledge to increase its success rate and efficiency. A human may select to trade their privacy for a corresponding gain in another's trust.

For example; if some vehicle users are accessing some LBSs inside a mix zone then these service providers charge some amount plus collect some valuable information of users to provide accurate and efficient services, which can be reason of breaching privacy and losing of trust for vehicle users if this information is shared with unauthentic users. Sharing of information with in LBSs can be from following categories: Unclassified, Restricted, Confidential, Secret, Top secret [16,17] i.e. information (in reverse order for example top secret etc.) requires more security with higher trust. Further, provided information to LBSs can be top secret or sensitive or just a normal one. Information in VANETs (can be public i.e. emergency, traffic management, collaborative, and private i.e. personal, or emergency) that is public to its participants, and that it is no precisely stored in the vehicle, but in turn it is represented by commonly exchanged messages with the main objective of informing vehicles in various situations, such as, traffic management, emergency warnings, or nodes misbehaviour. Meanwhile this exchanged information among vehicle users in LBSs can be trusted or not. Moreover this, Leaking of one day information/privacy of any vehicle user's does not matter [18] but what happens if it is for a long term like month, year etc. In this case, several users care for their privacy and raises concerns to protect their sensitive/location information (which is related to privacy). But somewhere, somehow, third party service providers (or hackers) used tracked data for their use or against user's policy. It breaches the privacy of users and raises concerns to protect it. Similarly, maximum users do not care about their previous tracking but they care about their future tracking i.e. schedules etc. Especially, normal (poor) people do not care about their privacy, but rich people do.

Trust can be built among human as higher or lower one. In higher one, people trust each other a lot for example, there is always a higher trust among brother and sisters living in a family, but it can be lower among their parents. Lower trust leads to isolation and leak of collaboration i.e. lower privacy, and higher trust leads to higher privacy protection. This work aims to provide lower results to threats of privacy and trust violations. To provide efficient results, Trust must be established before a privacy disclosure (for an application). Trust is sometime asymmetric and sometimes not (refer Table 1, in appendix A). For example, I trust you more than you trust me. Trust isn't as asymmetric. it is difficult to acquire (gain) however easy to lose [19], as previously thought is good information for a lot of many users, however perhaps not so surprising after all. That is, baseline stage of belief may also be influenced via the accuracy of exact earlier judgements (decisions). If you wish to construct trust, it might be better to stipulate the implementation of confident (positive) policies that effectively constrain behaviour over a sequence of events rather than seeking to provide individuals with information about particularly positive constructive instances of efficiency (performance). Trust, as with confidentiality is dynamic and evolves (increase or decrease) interaction after interaction. Relying on what human being can get based on their trustworthiness, they may be willing to disclose extra of their private information with the intention to broaden belief (trust) [20]. There is a need for contextual privacy-trust trade-offs. There are two types of users existed in this real world i.e. trusted and non-trusted users, discussed as in [18];

- **Trusted Users (TUs):** Those are who received messages from other Vehicles/Infrastructure (RSU), perform task according to message (safety or non-safety) and pass this message to other Vehicles/ infrastructure (RSU) in the network.
- **Non Trusted Users (NTUs**): Those are those users that do not possess the trusted credentials and could perform (various) kind of attacks (like Man in Middle, Sybil, Continuous Query, Sematic Attacks etc.) which create problems directly to users available over road network. In VANET, their role is more prominent because they can potentially change the life critical information on the road. NTUs can be classified in positive and negative types (i.e. based on behavior). In Positive Behavior, a user behave just normal one and did not make any reply/attack but he is not trusted to other users also. While in Negative Behavior, a user behaves like an attacker i.e. attacker, who intentionally create problems for users in a network by launching different types of passive/active attacks [18]. In VANET, they (attackers) become more prominent because they can potentially change a critical message or broadcast a wrong message to other vehicles.

A non-trusted user can make fool to other user for example, provided information i.e. "Accident at Location X" can become "Road is clear" to other users in road network. But in this case, trust issue become an essential issue among drivers or users and service providers i.e. provide information by service provider/users is trustable or not, if trustable then "how much", "how to quantify it"? As discussed above, a trust relationship can be symmetric or asymmetric. In an asymmetric trust relationship, one of the interacting partners is stronger and other one is weaker. The weaker partner will get a high level of trust through disclosing his private (or confidential) information to other users (stronger or weaker). Basically weaker or poor people even do not care about trust. They believe in trust which is made or dependent on some previous decisions or recommendations provide by other people. basically, Trust is suffering from a large quantity of system factors, including [21]: (a) excellent and integrity information; (b) trustworthiness of end-to-end communication, together with sender authentication, message integrity, etc. and (c) protection of community routing algorithms, including dealing with malicious friends, intruders, protection assaults, and many others. [21]. Recalling the procedure of trust formation makes apparent the fact that privacy is at stake in trust-based systems [20,22]. There may be an inherent conflict between trust and privacy because each relies on abilities about an entity, however in reverse ways [22]. Privacy is crucial when dealing with trust management. For a privacy-trust trade-offs, the users could be interested in answers to various privacy and trust related questions, such as:

- How much privacy is lost by disclosing the given data?
- How much does a user benefit from a particular trust gain?
- How much privacy should a user be willing to sacrifice for a certain amount of trust gain?
- How much trust lost during a sacrifice/loss of privacy?
- How to quantify the perfect trust established between/in other users?

This section started as introduction about trust and privacy in detail. Further, it discusses need of trust, privacy in real world, also provides several definitions given to trust in various literatures. Finally this work is carried as; Section 2 discusses about trust characteristics, its types. Section 3 discusses privacy and trust issues arise in real word. Section 4 discusses about quantification of Trust and Privacy. Trust, Privacy trade-offs (to preserve location privacy and gain in trust among users using LBSs services) discussed in Section 5. Section 6 concludes this work and draws road ahead for future.

2 Trust Characteristics and Types

A researcher wishing to make use of trust in computing systems need to take care of the difficult option of the most fulfilling subset of trust characteristics. A significant style of exclusive trust based systems can influence from settling on distinct subsets [21]. One of the crucial picks will make systems based on them ineffective/inefficient. Trust is based on knowledge in regards to the other party, which directly contradicts the prevention of linkability of knowledge to users. So for ultimate privacy protection, i.e., preventing moves to be linked to users prevents the formation, evolution and exploitation of trust in the actual (i.e. On-line)

world [20]. Trust is computed by direct (linking interactions over time/past transactions) and indirect (recommendations) communication. In order to be able to make the decision to trust another entity, the first step is to establish the level of trust in that entity, which is the result of an analysis of the existing knowledge and evidence [22]. If full knowledge is available, it is true that the need of trust vanishes because no uncertainty and no risk available there. There must be a mechanism that can dissociate users from their actions. Basically, Trust will also be divided into hard (rough) trust (security-oriented) and delicate (soft) (non-security) oriented trust. The rough trust entails parts and operations comparable to validity, encoding and safety in methods (processes) nevertheless the delicate trust covers dimensions like human psychology [10], loyalty to alternate mark (manufacturer or brand loyalty) and user-friendliness. In a similar fashion, privacy will also be individual as hard privacy and soft privacy [23]. Reputation (fame) is an instance of soft privacy which is a component of online trust and can be most valuable asset of a company/organization. A corporation's brand is preferred with trust or faith. If it cannot participate in effectually in matters like trust and privacy, it is going to fail and be defeated. Nonetheless, human being still have less self-assurance to the services offered on-line in assessment with the offline ones due to the lack of physical cues in digital world. So the infield of online service supplying, lack of belief or trust in them can have a poor influence in getting into and competitive competence of the companies and old organization which were trustworthy for an extended-time into the digital world [10,18].

To compute trust, several authors define several basic trust parameters/characteristics (refer Table 1) to compute or notify it. Among those, two important characteristics of trust (or distrust) are as follows:

- The primary is the dynamic nature of trust. Trust changes over time. Even if there is not any change in the underlying motives that affect trust over a time period, the value of trust on the finish of the interval isn't the equal as that at the establishing of the period. Irrespective of our preliminary trust or distrust selection, over a period of time we steadily grow to be non-decisive or uncertain about the trust decision. This leads us to claim that trust (and alternately distrust) decays over time - each tends closer to a non-decisive price over time.
- The second is what is often called the *propensity* to trust. Giving same set of values for the factors that influence trust, two trusters may come up with two different trust values for the same trustee. It happened because of two main reasons; first, during evaluation of a trust value, a truster may assign different weights to the different factors that influence (affect) trust. The weights will depend on the trust evaluation policy of the truster. Second, a truster used same weight to different factors to compute trust. So if two different trusters assign two different sets of weights, then the resulting trust value will be different. (Note-The second reason is applicable only when the truster is a human being and is completely subjective in nature).

2.1 Other trust characteristics

a. Symmetric and Asymmetric Trust: The former assumes that "A trusts B" implies "B trusts A," which (in general) is not true [21]. A trust relationship is usually asymmetric. Therefore, asymmetric trust is more general. Symmetric trust can be viewed as its special case, which can be assumed only in very special circumstances or applications. In symmetric property, a trust relation R on a set of users X is *symmetric* when: $\forall a,b \in X$ $(aRb \rightarrow bRa)$. An example of symmetric relation: "... is trusted to ___". A binary relation R on a set X is *asymmetric* when: $\forall a,b \in X$ $(aRb \rightarrow \neg (bRa))$. Figs. 3b, 3c show the sharing of privacy and trust among several users in a LBSs environment.

b. Degrees of Trust vs. Binary Trust: The previous is more exact, taking into account degrees of trust (from multi-level to constant trust), while the last mentioned, is all or nothing trust, which strengths to determine a solitary trust threshold above which full trust can be expected. Binary trust is inadequate in general, and can be expected just for extremely uncommon and constrained settings in type of 0 to 1 value where 1 means 'a highly trusted user' and 0 is 'neutral user'. Neutral user means does not take part in any process i.e. feedback, recommendation, relationship etc.

c. Implicit or Explicit Trust: Implicit trust is utilized by either insensible or gullible or naïve connection parties for instance, a user, who downloads a document from an unfamiliar webpage, trusts it verifiably by not even considering trust deliberately. The outcomes may incorporate

infiltration by malware. Explicit trust takes into account its reasonable determination, guaranteeing that trust contemplations are not overlooked. Explicit trust might be gained offline. For example, a people who chooses to purchase an Internet service from an Internet Service Provider (ISP) may construct her trust in disconnected form by approaching her companions for dependable ISPs or trust. As simple example, trust on Judges in court (about justice) consider as explicit trust.

d. Direct or Indirect Trust: Direct trust (developed based on past transactions, feedbacks) between user A and user B (as in: "user A trusts user B") is limited to cases when user A has gained a degree of trust in user B from previous interactions (i.e. feedbacks). This may, but does not mean that user B gained any degree of trust in user A. It is obvious that the domain of trust can be significantly extended by relying not only on direct trust but also on indirect trust. **Direct relationship (for example: mother–son relationships) is like that**, as one user's trust increases, together this, the other's trust also increases, or as one's trust decreases, the other's trust decreases. In indirect trust (developed based on recommendation), user A does not need to trust user B to be willing to interact with it. It is sufficient that user A finds an intermediary user C such that user A has a sufficient degree of trust in user C and user C trusts user B (transitive property). To be more precise, in this case, user A needs to trust to a sufficient degree in user C's recommendations about trustworthiness of B. A recommendation can be completely true (trusted) either semi-true. Some recommendation from malicious users can change the global trust value among people. Now user C becomes a Trusted Third Party (TTP). A TTP can be any entity accepted by Entity or user A, in particular, it can be an institution set up to provide indirect trust, also on a commercial basis. In **indirect relationship (for example: relatives/neighbors relationships)**, user x has an inverse relationship with y if y = (some constant) / x.

e. Type of Trusted Entities: Should trust be lavished just on people? The answer is clearly "no". We believe or trust on our coolers, autos, phones, PDAs, or RFID labels accessible our house (future smart houses) or available in various stores/shops. Just like the case with people, this trust can be ruptured if the gadgets are faithful to other parties than their owners or essential users. Reliability (loyalty) chooses who the entrusted party works for. For instance, sensors and recorders in a vehicle can work not only for driver but also for an insurance organisation also for a back-up plan. a program can work for a business promoter, and a sensor system in one's home can be seized or hijacked by a nosy or malicious neighbor or—in the most pessimistic scenario—by the Big Brother.

f. Number of Trusted Entities: The most of the basic refinement is between believing someone and believing no one. The last one prompts to paranoid behavior, with to great degree negative outcomes on framework performance. We believe in that "You can't trust everyone except you need to trust some individual." Trusting more accomplices enhance performance the length of trust is not manhandled. Any rupture of trust causes performance punishments. An ideal number of trusted substances ought to be resolved.

g. Responsibility for Breaches of Trust: If there is no TTP is included in an infrastructure, is the trustor (who exposes a vulnerability to the other party, in a desire for picking up an advantage from this) or the trustee (who could conceivably give such an advantage to the trustor) in charge of settling on the level of trust required to offer or accept a service. In result, this is the trustor or the trustee eventually for conceivable ruptures of trust. In commercial relationships, (at the time of buying a product) mostly a buyer always have a confusion i.e. particular seller is trusted or not or vender is sufficiently reliable or not. And after that—once the guarantee time frame for that particular product is over—bears the expenses of broken trust. There are situations when vender pays for misuses by the purchaser (as in the case when terrorists are not prevented from boarding a plane). Now if a TTP is included in a trust relationship, it might be considered in charge of maintain the degree permitted by its legitimate commitments.

2.2 Types of trust

Trust is a powerful paradigm that enables smooth operation of social systems, also under conditions of uncertainty (or incomplete information). Trust becomes solidified when words consistently back up by deeds. Trust him with little who, without proofs, trusts you with everything. He who mistrusts most should be trusted least. Today's everyone wants to share secrets/failures with others to improve their performance

(in their life). But in result, it creates trust and privacy issues to preserve their secrets. The state of trust is so dire, we cannot afford to build trust one manager/person, one relationship at a time. Basically, in social research, there are three main types of trust have been identified: interpersonal trust, dispositional and Impersonal trust. Trust, existed in various organisation can be discussed as;

a. **Interpersonal Trust:** This describes trust between two people based on your own and the other's characteristics and the risk we are prepared to take by entering in a relationship (business or otherwise) [24]. Interpersonal trust is requesting entity and context specific. Many people believe that interpersonal trust is the foundation of all other relationships. That if you like and trust the salesperson of a company, then you will trust their company also (symmetric property) (but not necessary always, asymmetric property). And that trust in and between organizations has to with stand turnover and has to be greater than just a relationship between two people. Inter-personal trust is important in inter-firm relations**.** However, trust about friends and relatives consider as 'interpersonal trust'.
b. **Dispositional Trust:** It describes an internal state of the trustor i.e. a basic trusting attitude. This is "a sense of basic trust, which is a pervasive attitude towards oneself and the world". This trust is extremely open-ended and independent of any party or context. This trust has been further divided into two; i.e. type A and type B. Type A concerns the truster's belief on others' benevolence, type B is the "disposition that irrespective of the potential trustee's benevolence, a more positive outcome can be persuaded by acting "as if' we trusted her".
c. **Impersonal trust:** It refers to trust on perceived properties or reliance on the system or institution within which the trust exists.
d. **Organizational Trust:** This includes trust among individuals inside an association (organization). It can incorporate trust between a worker and her administrator; a representative and the general authority group; the worker (i.e. employee) and a particular pioneer, or trust between gatherings and so forth. It can likewise consider trust created and supported by impersonal measures, for example, HR (human resource) approaches equipped towards fairness, procedures and distributive justice (compensation, opportunities, etc.). In light of "How it treats its people, its cultures, its way of life and standards (norms) etc.". Leaders sign to their staff what sorts of practices will be compensated to make their future bright.
e. **Inter-organizational Trust:** This is "trust placed in the partner organization by the members of a focal organization based on reliability, predictability, and fairness" [24]. It's the dependability "score" you would create if you could consider in your survey everybody in Company A, who is included in an association with Company B (in legal, executive, front-line, marketing, accounting, etc.). What might the general recognition be of Company B's reliability (or trustworthiness)? The precarious part is that it can't just be a total score of everybody's observations (perceptions), emotions (feelings) or activities (action) because the trust factors may be different as well. This trust as a method for organizing "desires and communications in relationships between individual on-screen characters (i.e., supervisors) and/or aggregate performing artists (i.e. associations)". Inter-organizational trust develops in hierarchical form among as the superseding driver of exchange performance, negotiation, and decreasing clashes (conflicts).
f. **Technical Trust:** With security considerations, layers of trust have been identified namely technical trust, that is, trust in the components of the underlying technical infrastructure, and trust in the interacting entities. Static and Dynamic evidence-based means to compute the level of technical trust in Entity Recognition (ER) schemes have been proposed and evaluated. The levels of technical trust can be used for threat analysis, especially concerning identity usurpation attacks. When dynamic evidence-based means are used, technical trust is changed from system trust to inter-personal trust in the technical components. Technical trust existed in the infrastructure taken into account to compute trust (refer equation (i)).
g. **Decision Trust:** Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible.
h. **Reliability Trust:** Trust is the subjective probability by which an individual 'A' expects that another individual 'B' performs a given action on which its welfare depends.

i. **Computational Trust:** However, with full knowledge and no privacy, the need of trust vanishes. In high privacy setting, there is a high need of trust called computational trust. It is based on interpersonal trust and trust values rather than system trust is a means for trust in privacy protected environments.
j. **Situational trust:** This is the amount of trust that one agent has in another taking into account a specific situation. The *utility* of the situation, its importance and the 'General trust' are the elements considered in order to calculate the 'Situational Trust'.

Trust term is extensively used when discussing about social judgments/sharing of information. It is major to distinguish this kind of 'role-based trust' which pertains to the target's capabilities to fulfill precise hazard (risk) management roles [19], from the kind of interpersonal believe we have preserve with our friends and household. *The type of trust, we are discussing in this work,* is not the trust we've got with our neighbors and loved ones i.e. with family members (interpersonal trust) or with different individuals generally (social trust). however trust in certain participants whose role it is to examine, control and be in contact information about risk (chances) known as "role based trust", because "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" [16, 19, 25]. Hence this section discussed about trust, characteristics, and its types etc. Next section will discuss about in privacy and trust issues with respect to VANETs application.

3 Privacy and Trust Issues in VANET's Applications

Today's Current technologies are depending on wireless services. It means everything is far away from a central device or works on decentralised structure. Due to this openly nature, several privacy and trust issue arises among users and service providers. As discussed above, "Privacy is a non-renewable resource," McSherry said. "Once it gets consumed, it is gone." Privacy is a fundamental human right which concerns the expression of various legal and non-legal norms regarding the right to private life [26]. In general, privacy talks about the protection and appropriate use of the personal data. Privacy can be classified based on location, data, identity and differential [18]. The privacy concern typically will make most people uncomfortable, especially if systems cannot guarantee that their personal information will not be accessed by the other people and organizations. As discussed in introduction section, providing information (about your location, vehicle, credit card etc.) to service providers to access reliable services is trust-based. Now there are chances (probability) of losing this information to non-trusted servers/users. This issue can be controlled with stricter privacy policy maintain by organizations. If someone violates this policy, it should be punished. Moreover, privacy, trust issue among vehicle users emerged. Trust is a primary factor in "How people work together, listen to one another, and build effective relationships [27]"? Maximum people are unaware about their actions which are influencing trust among them. It 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. Once it's gone, it is difficult to gain again, especially in organizational, human-being relationships.

Trust is also related with security which includes mental and practical criteria (see Fig. 1). For example, forwarding credit-card number, PIN, and password by e-commerce companies to third (unknown) parties is a result of breaching trust and security. Together, privacy issue also has become an essential issue with trust and security because using data mining, higher security tools and other analysis technologies tool, attackers/service providers can reveal user's personal information easily. This stole information is used by attacker for their financial use or for third party use. Although all the gathered information for shop behavior are unknown for example, buying some personal items like diamond rings for his fiancé from a shop in LBSs/mix zone. But this information can be effectively gathered by various gadgets and systems (for instance, area of the shop and age of the purchaser etc.) using a data mining algorithm easily find out that who purchased this ring and from which shop. More precisely, the data analytics is able to reduce the extent of the database because location of the shop and age of the buyer provide the information to help the system find out possible persons. Therefore, any sensitive or confidential data should be deliberately secured. The unknown, impermanent distinguishing proof, and encryption are the delegate innovations for privacy of data analytics, but the critical factor is "how to use", "what to use", and "why to use" the collected data on big

data analytics. Privacy issues in VANETs application (in Carpooling) are Safety, Security and Trust. Further, Trust issues in VANETs application (in Carpooling) are Privacy, Cost and Waiting time. While in Parking, some mitigated issues are like Privacy, Safety and Reliability. Some of the Privacy and Security Issues are in LBSs are; Access to Location Information Versus Privacy Protection; Location Privacy Protection; Social Challenges and Trade-Offs; Personal Safety and Physical Security; Applications in the Marketplace; Risks Versus Benefits of LBS Security and Safety Solutions; Safety of "Vulnerable" Individuals; National Security and Proportionality: National Security Versus Individual Privacy.

Big data analytics also perform an essential role to revealing and protecting of users information to end users. This section discussed about privacy and trust issues arises in road network. Next section will measure trust and privacy among users/infrastructures using some relevant (top) techniques.

4 Quantification of Trust and Privacy

Basically Trust relies on profiling, where more information is better, because it allows the likely behaviour of the other entity to be more accurately estimated. Trust cannot be built or verified/improved without having measures of trust, which can be determined in many levels like zero, average, strong [16] etc. Low level of trust has lower responsibility i.e. higher privacy risk. Similarly, High trust levels lead to a greater sense of self responsibility, greater interpersonal insight, and more collective action toward achieving common goals. Trust is situation specific, reflects the belief or confidence or expectations on the honesty, integrity, ability, availability and quality of service of target node's future activity/behaviour [4]. It is in one environment does not directly transfer to another environment. In order to adequately negotiate privacy for trust or trust for privacy, there is a need of quantification of the trade-off between privacy, trust and utility. So a notation of context is necessary represent trust and privacy.

4.1 Trust quantification

Computational trust is an innovative mechanism towards the prediction of behaviour. We comprehend trust regarding the *probability of the probability* of results, and embrace his concept of a trust space of triples of belief (in a decent result), disbelief (or faith in a terrible result), and uncertainty. Trust in this sense is unbiased (neutral) with regards to the result and is reflected in the certainty assurance (certainty = 1-uncertainty). Consequently the accompanying three circumstances are recognized:

- Trust being set in a party (i.e., seeing the gathering as being great): conviction (belief) is high, mistrust (disbelief) is low, and uncertainty is low.
- Distrust being set in a party (i.e., viewing the gathering as being terrible): conviction is low, mistrust is high, and uncertainty is low
- Lack of trust being set in a party (pro or con): conviction is low, mistrust is low, and uncertainty is high

To compute trust, a trust metric consists of the different computations and communications which are carried out by the trustor (and his/her network) to compute a trust value in the trustee. It is y resistant if more than y nodes must be compromised for the attacker to successfully drive the trust value. It is used to choose the most trustworthy user among the all selected users who claim to have the sought-after file. Trust can be reflected by reliability, utility, availability, reputation, risk, confidence, quality of services and other concepts.

4.1.1 Trust by levels

First determine multilevel trust metrics with n trust levels, measured on a numeric scale from 1- n, where n could be an arbitrarily large number. Such metric is generic, applicable to a broad range of applications, with the value of n determined for a particular application or a set of applications [21]. The case of $n = 2$ reduces multilevel trust to the simplistic case of binary trust (it might still be useful in simple trust-based

applications), with trust levels named, perhaps, *full_service* and *no_service*. Selecting $n = 5$ results in having 5 trust levels that could be named: *no_service*, *minimal_service*, *limited_service*, *full_service*, and *privileged_service* uses as the lowest to the highest level. Refer [16,18] to know more about trust levels.

4.1.2 Trust by recommendation

The trust of a particular node is a subjective assessment by an agent/other peer (user) node on the reliability and accuracy of information received from or traversing through that node in a given context [28]. Trust can be established using collected recommendations about a user from known or unknown entities. But getting recommendation is not that much easier. For this, a user should know to recommended user and should know about his behavior/experience/attitude in society. It (recommendation) 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 [29]. It can be figured with the assistance of alerts i.e. providing alarms. If there is a light and they accurately distinguish its presence, refereed as a True Positive or Hit [19]. In the event that a light was really present however they neglected to recognize it this is alluded to as a False Negative or Miss. At last, if a light was not present but rather they claim it, known as a False Positive or False Alarm i.e. three expectations made here. Compute trust value like;

- First tally or count right decisions (Hits and All Clears); it will be connected with more positive changes in trust than incorrect decisions (False Alarms and Misses).
- Secondly tally decisions demonstrating cautions danger response bias (Hits and False Alarms), it will be connected with more positive changes in trust than decisions demonstrating a risky response bias (All Clears and Misses).
- Finally while Risk administrators who are "open" about their choices or decisions will be connected with more positive changes in trust than risk managers who are ‘closed’'.

4.1.3 Trust by value

Trust can be established using previous decisions/feedbacks. It can be develop based on past transactions or collected feedbacks and reputation about users. It is the total trust values in all contexts in all virtual identities with whom the trustor has interacted so far. Risk is used in a threshold for trusting decision making (see equation (iv)). Risk is a major factor to believe someone or quantifying trust and privacy. (*Note*-Trust categories are not strictly independent but they are influencing each other i.e. based on risk value, previous decisions etc.). Trust value is based on direct observations or recommendations of the count of event outcomes from one specific entity (reputation from a number of unidentified entities and credentials as in trust management [16,30]. It has been noted in various literature that there are issues “with trusting recommenders to recommend arbitrarily deep chains”. They argue that trust at level n is independent of trust at level $n+1$.

4.1.4 Trust by entity recognition

Further, a computational model of Entity Recognition (ER) has been developed and integrated in a trust engine as a replacement for the authentication process [22]. When the level of trust is based on counts of interaction outcomes [31], the techniques of fusionym and trust transfer address both accurate computation of the level of trust in spite of self-recommendations and identity multiplicity. They address the issue of “identity proliferation”.

4.1.5 Trust by trust transfer

A trustor should be able to increase/decrease the influence of the recommenders according to his/her goals (to protect trust value). The mechanism used to control the recommender’s influence must achieve this goal [30]. This mechanism called as *Trust Transfer*. Trust transfer corresponds to a local decentralised scalar metric and is evaluated with simulations of a real social network of email users extracted from online data. It implies that recommendations cause trust on the trustor (T) side to be transferred from the recommender (R)

to the subject (*S*) of the recommendation (refer Fig. 2). A second effect is that the trust on the recommender side for the subject is reduced by the amount of transferred trustworthiness [30,32]. If it is a self-recommendation, then the second effect is moot, as it does not make sense for a real-world entity to reduce trust in his/her own pseudonyms. Even if there are different trust contexts (such as trustworthiness in delivering on time or recommending trustworthiness), each trust context has its impact on the single construct trust value: they cannot be taken separately for the calculation of the single construct trust value. A transfer of trust is carried out if the exchange of communications/information between users is successful. A local entity's *Recommender Search Policy (RSP)* dictates which contacts can be used as potential recommenders. Its *Recommendation Policy (RP)* decides which of its contacts it is willing to recommend to other entities [32], and how much trust it is willing to transfer to an entity. Trust Transfer [30,32] (in its simplest form, among all components) can be decomposed into 5 steps (depicted in Fig. 2):

i. The subject demands an activity (or action), requiring an aggregate sum of trustworthiness (TA) in the subject, all together for the solicitation to be acknowledged by the trustor; the real estimation of TA is dependent upon the risk acceptable to the client [31], and additionally dispositional trust and the connection of the solicitation [30-35]; so the risk module of the trust engine assumes a role in the computation of TA.
ii. The trustor queries its contacts, which pass the RSP, with a specific goal to discover recommenders willing to exchange some of their positive event results/criticisms or feedbacks count to the subject. Recall that trustworthiness is based on event outcomes count in trust transfer.
iii. If the contact has specifically collaborated with the subject and the contact's RP permits it to allow the trustor to exchange a sum (A_TA) of the recommender's trustworthiness to the subject, the contact consents to suggest (recommend) the subject [30,32,34]. It queries the subject whether it consents to lose A of trustworthiness on the recommender side.
iv. The subject returns a marked statement, demonstrating whether it concurs or not.
v. The recommender sends back a marked recommendation to the trustor, demonstrating the trust value. It is set up to exchange to the subject. This message incorporates the signed agreement of the subject [33,35].

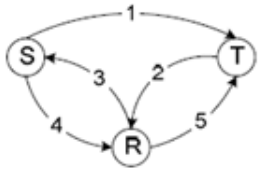

Fig. 2. Trust transfer process

In trust transfer, Trustor is the entity that ascertains the reliability i.e. trustworthiness among peers or users. Trustee is the substance whose trustworthiness is computed. Trustworthiness is demonstrated with a trust value. Trust value expresses the subjective degree to which the Trustor has a legitimate conviction (beliefs) that the Trustee will follow the trust scope. Trust is "functional, such that trusting behaviours are attempts to attain desirable outcomes by protecting one's interests through actions that either increase or decrease influence in accordance with one's assessment of such influence" [30]. When somebody suggests or recommend someone else (i.e. a person), he/she has impact over the potential result of communication between this individual and the trustor. The inclination of the trustor as to this impact "provides a goal-oriented sense of control to attain desirable outcomes". In this way, the trustor ought to likewise have the capacity to build/diminish the impact of the recommenders as per his/her objectives. Trust is not multiple constructs that vary in meaning across contexts however a solitary build that changes in level across contexts [30]. In general, overall trustworthiness relies on upon the complete arrangement of various areas of trustworthiness. This general trustworthiness must be placed in context: it is not adequate as far as possible the domain of trustworthiness to the present trust context and the trustee; if recommenders are included, the decision and the outcome ought to affect their overall trustworthiness as indicated by the impact they had [30,32].

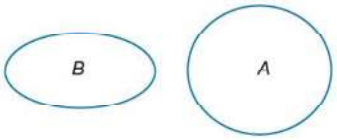

Fig. 3a. Represent of user A and B in an environment

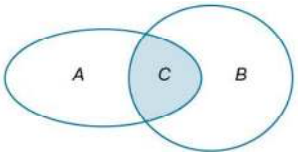

Fig. 3b. Sharing and losing of privacy, trust between user A and user B

Fig. 3a shows that how user A and B are stranger. Figs. 3b and 3c discusses "how user A and B share their information with other users and how it becomes a serious concern i.e. sharing of information means sharing your privacy".

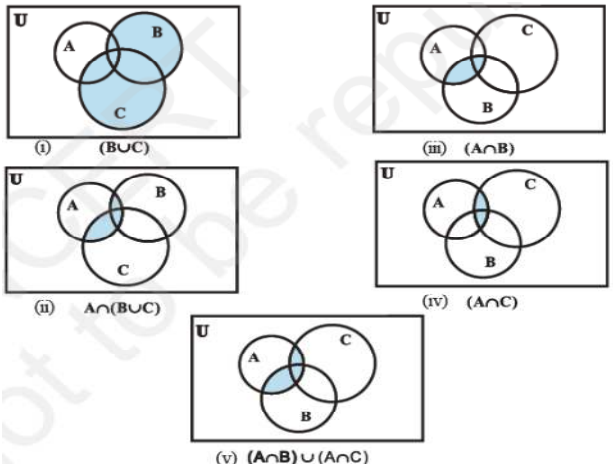

Fig. 3c. Sharing and losing of privacy, trust in an environment (among users A, B and C).

To computer trust, first consider (taken into account) Technical trust (existed in the infrastructure):

End to End Trust Value = f (Technical Trust Value, Virtual Identity Trust Value) (i)

We combine some important variables into the following equation to compute trust:

Trust = (Credibility+Reliability+Intimacy)/Self-Orientation = Trustworthiness (ii)

Equation (ii), can also be define as;

Trust = (Ability + Benevolence + Integrity) (iii)

Trust can be relates to risk and its correspondents as define in eq. (iii).

Risks = Threats * Vulnerabilities * Impact (iv)

A risk is directly related to improve or decrease trust. While risk in eq. (iii) directly related to threats i.e. based on security. Further to improve trust, we should focus to improve privacy i.e. minimum loss of privacy results in minimum loss of trust. Eq. (v) computes minimum loss of privacy as:

$$\text{Min } \{\text{Pr}\textit{ivacy Loss } (N_c\text{UR}(s)) - \text{Pr}\textit{ivacy Loss}(R(s)) \mid N_c \textit{ satisfies trust requirements}\} \quad \text{(v)}$$

Total trust gain in a relationship can be shows as in equation (vi):

$$\text{Trust gain} = G\,(\textit{new\_trust\_level}, \textit{old\_trust\_level}) = B(\textit{new\_trust\_level}) - B(\textit{old\_trust\_level}) \quad \text{(vi)}$$

As discussed, Trust is a measure of uncertainty; as such trust values can be measured by entropy. From this understanding, we developed axioms that address the basic rules for establishing trust through a third party (concatenation propagation) and through recommendations from multiple sources (multipath propagation). Trust is a binary relation between two subjects: the trustor and the trustee. Trust partly depends on context. With multiple wrongs attempts and experience, it can be change dynamically. Trust is subjective. For the same trustee and goal, different trustors may make a different decision. Like privacy policy, trust also can be improved among human beings. A trust policy is displayed as Trust {(trustor, trustee, objective) →policy}, where the policy body is a conjunction of predicates. The trustor believes (trusts) the trustee for an objective if and only if the trust policy body is valid (true). Trust policies catch the subjectivity of trust. In outline, there are two fundamental choices accessible for setting up (establishing) trust: statically (by the static reliance on a security infrastructure) and dynamically (by the dynamic develop of trust in a way that is self-organizing). To establish the certain level of trust among users in road network, all entity/all components (User, Vehicle, and RSUs) require to behaving in expected manner and serving the user in trusted manner".

4.2 Privacy quantification

Privacy is a concept that combines law, sociology and psychology, so the dimension of privacy includes multiple decision factors. Privacy is about if it is possible for the system to restore or infer personal information from the location service providers, even though the collected information are anonymous. Therefore, all the factors should be considered in privacy quantification. For privacy quantification, requester (who request user's information to provide LBSs services), data handler (who handle user's data like administrator) etc. factors are concerned. For privacy metric, anonymity set size and entropy is used by most of reported work [18,36]. A tuple requester ID, information handle, information content is characterized to depict data that an associate has when information is procured. Fig. 4 is a representation of security estimation. Information handle is utilized to distinguish the asked for information (for example: file/user name and the segment index etc.).

In Fig. 4, for each tuple component, "0" implies that the user knows nothing about requested query, while "1" implies that it knows everything. For instance, a supplier's vector is (x, 1, 1) ($x\varepsilon[0,1]$) because it knows all details of the requested information. A state in which a requester's privacy is compromised can be notify as a vector (1, 1, y) ($y\varepsilon[0,1]$), from which one can interface the identity of the requester with information that it is interested in. Significant choice elements in privacy measurement [37] incorporate such attributes: user preferences, context constraints, trust on communicating entities, privacy interaction history and feedback of privacy interaction, anonymity and unlinkability etc. Each entity can be discussed in brief as:

4.2.1 User preferences

Typical user preferences (set by a user entity) ought to at any rate incorporate into privacy data, kind of service and objectives of interaction. A user can characterize privacy preferences as far as the kind of every service. For instance, the user can indicate that credit-card information be unveiled for online web shopping (or for that span) only but not for any other types of services.

4.2.2 Context constraints

Usually, context constraints can be in terms like temporal and spatial. Since privacy is a context-dependent i.e. a privacy disclosure decision may not always be the same in different temporal and spatial situations.

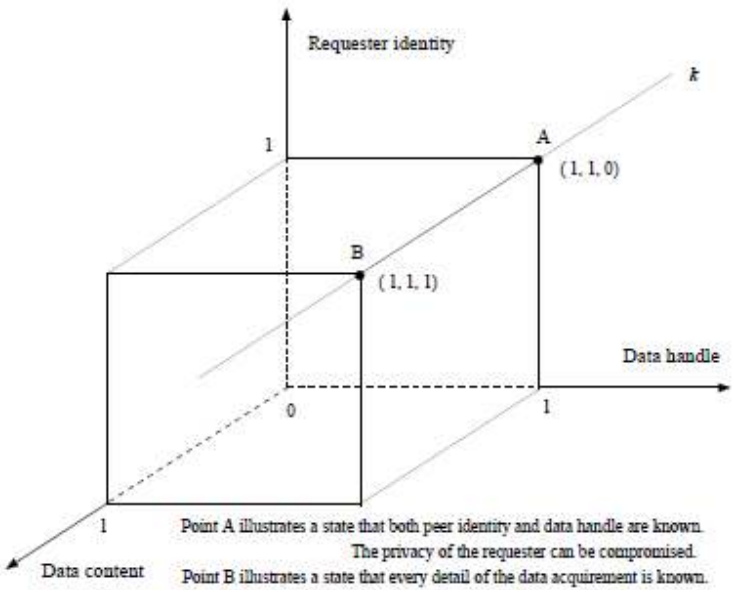

Fig. 4. Privacy Measurement

4.2.3 Trust on communicating entities

In user communications, a user (entity) may cooperate with a variety of other user. Intuitively, an entity's privacy disclosure decision is identified with the trust on the conveying element to some degree. Hypothetically, in any case, trust can be seen as a likelihood (probability) of a trusted substance accomplishing something that would profit the trusting element. Subsequently, trust permits a substance to settle on a few choices (decisions).

4.2.4 Privacy interaction history and feedbacks

If two users have shared some privacy data before and thus satisfied with each other's behaviour or feedbacks, they are presumably more than willing to exchange some more privacy information as indicated by psychological studies. Therefore, after the entities have exchanged some privacy information, there should be a feedback function to check whether one entity has disclosed the other entity's privacy (without user's proper consent) to other users or not. So for privacy evaluation, security, privacy connection history and criticisms ought to likewise be considered.

4.2.5 Anonymity

Providing anonymity to k user with k-1 users to protect each user's privacy. The more complex structure of anonymity will be, more privacy will be preserved.

4.2.6 Unlinkability

Maximum unlinkability to the collection of user's information provides also sufficient level of privacy.

4.2.7 Privacy policy

With more strict privacy policy, more privacy of users will be preserved for example; HIPPA (Health Insurance Portability and Accountability Act of 1996) privacy policy used in medical applications to protect user's information form online/outside world/any other application.

This work discussed "How trust can be quantify among human beings using some metrics like intimacy, credibility and feedback etc. Similarly privacy can be quantified using hop count, anonymity, unlinkability and unobservability methods. Protecting user's privacy is an assumption to increase trust among users. There are several feedback techniques (textual, colour, sound, avatars etc.) to improve and complain about trust change. For establishing trust using recommendation process refer [23]. Next section will deal with trade-offs among trust and privacy.

5 Trust-privacy Trust-offs

In order to increase trust within a community one would like to import good feedback (or reputation) values and good credentials from other communities. However, these may expose the details of the reputation values and thus impair the user's privacy [38]. However, when privacy protection is high, the need of trust is far greater that when full knowledge is available. In some cases, a user (or a community) may be willing to report only the aggregated values of reputation. In other cases, users may be willing to disclose the data (collected or stored) behind the aggregated values, such as individual ratings (for example, most hotel recommendation sites disclose only individual ratings). Several users made different queries to access different services in location based services (provided by various organisations). For that, they need to provide some basic/personal information to service provider. Several organisations did not disclose about their users or their preferences/habits individually to other users (unauthorized or non-trusted) due to implementation of some strict policy. But some organisation violates these policies. An attacker stole user's credential from these non-trusted organisations and sold it to other party or uses it against respective user. The privacy/trust trade-off is a major issue in real time/LBSs/Cross-Community Reputation (CCR) systems. A computational trust engine must take into account that humans need (or have the fundamental right to) privacy [22]. However, depending on what benefits can be reaped through trustworthiness; people may be willing to trade part of their privacy for increased trustworthiness. Hence, contextual privacy-trust trade-off is needed. Although, trust allows us to accept risk and engage in actions with potentially harmful outcome.

Due to the division of trust evidence between many pseudonyms, it takes more time for the entities behind these pseudonyms to reach the same trustworthiness than for a unique virtual identity [20]. The privacy-trust trade-off model allows the requester of an interaction to relinquish some privacy in order to increase trust evidence to be able to reap the benefit of being trustworthy [31]. Privacy is really in danger when identities point to real world users. In this case, it becomes Personally Identifiable Information (PII). For example, two entities interact and information about the outcome of their interactions is recorded. Depending on the outcome, the trust between each entity is increased or decreased. The trusted information may be forwarded to other (malicious) entities as recommendations for further use. Even if trust has only been built with direct observations, PII information stored in another entity may still have to confirm to directives. When trust built due to direct observations is used for further recommendations (or reputation/feedbacks), the new trust values created in other entities for further use (see Fig. 5). This direct observation can be used in VANET applications like parking or carpooling for building a correct, exact trust value. This trust can be used to preserve privacy till a certain level.

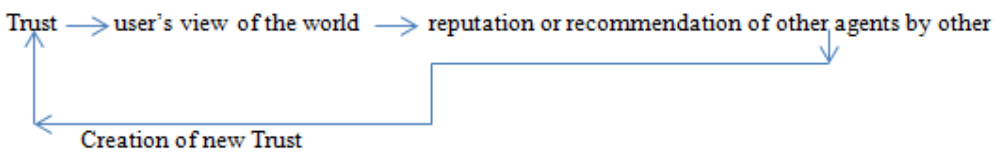

Fig. 5. Reputation-based trust management

Several problems are mitigated in recently in preserving privacy or implementing/computing trust among vehicle users. This work proposes a traffic free signal to preserve privacy and improving trust among people (see Fig. 6) which is not discussed in any previous work before. As discussed in section 1, Privacy protection and trust establishment have received a great deal of attention in network security research. Trust and Privacy can be in a symbiotic or in an adversarial relationship [21]. Both Privacy and trust relate to the information subject and include knowledge (or assumptions) about interacting entities (users). Data disclosure means loss of privacy, but an increased level of trustworthiness reduces the need for privacy. The more evidence is known; the more accurate trustworthiness is reached; the less privacy is left. The privacy expectations of a user vary across time and depend on contexts. The interest of the Data Subjects (DS) is to minimize loss of privacy at an acceptable level of trust.

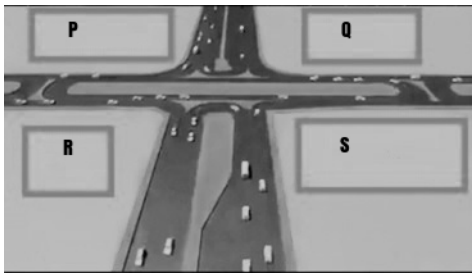

Fig. 6. Proposed scenario to managed vehicle without (using) traffic signals

In past, several researches have been made on breaking the continuity of location exposure by utilizing mix-zones to change users' identification. A mix-zone is a region (not a physical region) where the attackers cannot eavesdrop the vehicular communications. Among the all exited approaches to persevering privacy of vehicle users, in [36], authors consider multiple factors in the placement of mix zones, such as the statistical behavior of the user population. However, it pays no consideration to the network updating, which may lead to system unavailability in the long run (a weakness in MobiMix approach). This work proposes an idea which is that, provide a traffic free signal where no need of change any pseudonyms anymore. Some of advantages of proposed traffic free signal schemes are as follows:

- Provide parking to vehicle user near the square because at square, people always in hurry to cross the road, so problem of mix zone can be sort out providing parking facility at square at the side of road like P, Q, R and S (with providing pseudonym id and pseudonym location to service provider).
- There is no need of centralized authority to carry on or handle request of vehicle users.
- Total time, fuel and cost reduced.
- Certain of privacy are preserved, because one parking slot's users do not know other parking slot users (For example, user form a parking slot P do not know about parking slot Q or R's users etc.).

Depending on what location services users are accessing, it may be willing to divulge some of their private data. However, business must also be considered along with technology, legislation and social norms. Social norms are cultural phenomena that prescribe and proscribe behaviour in specific environments, the emergence of which are key to trust formation and privacy concerns. There is definitely an intrinsic relationship between trust, privacy, legislation, technology, social norms and markets. Further, knowledge is composed of evidence. A piece of evidence may be any statement about some entity, especially: a transaction, a direct observation (i.e., evaluated outcome of a transaction), or a recommendation. The anonymity of evidence is the amount of information about the identity of the entity that is revealed. The *trustworthiness assessment impact*, called '*tai'* of evidence, is the amount of information that can be used for assessing the trustworthiness of the entity, which is represented as a trust value. Moreover, the salutogenic (the Sense Of Coherence (SOC)) concept is a deep personal way of thinking, being and acting [39], a feeling of an inner trust that things will be in order independent of whatever happens. We agree that only passing the trust value may improve performance and may be better from a privacy point of view than all evidence information [33]. However, it may also decrease interoperability as highlighted here, and may show "how

another entity computes trust [20,33] from evidence"? Trust can be computed quantifying of a piece of evidence from a privacy disclosure point of view or a trust assessment impact point of view. There is also the issue of the sequencing of pieces of evidence: the combination of a new piece of evidence subsequent to the release of a first different piece of evidence may be worse from a privacy point of view than if the initial piece of evidence had been different. This may help to mount attacks and may reveal feelings towards other entities, which may not be welcome. In other words, decreasing confidence in someone leads to strength of privacy level towards him or her, as presented in equation (1) or following formula:

$$\begin{cases} privacy \propto (1 - trust) \\ trust \rightarrow [0,1], \quad privacy \rightarrow \{0, 0.1, \dots, 1\} \end{cases} \tag{1}$$

Recommendation (indirect trust) also is part of trusting behaviour i.e. trust transfer. It has not just an effect on the recommender's general trustworthiness, additionally on the general level of trust in the network of the involved parties. *A social network formed by trusting behaviours is intricate and a model assuming independence of any of its parts appears to be unlikely to result favourably.* When somebody prescribes another user, they ought to know that the result of their recommendation will reflect upon their trustworthiness and reputation since they are partly responsible for this result [34, 35]. A recommendation that is made by a user about other user, his recommending trustworthiness was impacted: "in consequence of my crediting such recommendations, my own are out of credit". Nonetheless, his letter underlines that still he needed to make recommendations about not extremely understood parties since they made the solicitation and not making recommendations could have disturbed them. In results, any communication alters the measure of trust between the interacting parties [35] and can be seen as support or disapproval (disfavour) – deposit or withdrawal. Further, inferred privacy rating of node s from point of view of node u can be processed by following formula:

$$privacy(s,u) = \begin{cases} \alpha(1 - trust(s,u)) + \beta\, p_s & ,if\ \ trust(s,u) \geq Min_{trust} \\ \gamma(1 - trust(s,u)) + p_s & ,else \end{cases} \tag{2}$$
$$0 < \gamma < 1,\ 0 \leq \alpha, \beta < 1,\ \alpha + \beta = 1,$$

In equation (2), Mintrust indicates the trust threshold for considering user u as trusted individual and trust(s,u) represents inferred trust value from node *s* to node u to be registered and computed utilizing the recommendations algorithms [25]. Now if *w* represents a service then rating of composer user *u* over service *w* is denoted by $t_c(w)$. Let us be a set of all individuals in the road network who rated service *w*. Subsequently, the reputation of service w from the user c viewpoint can be processed as:

$$t_c(w) = \frac{\sum_{u \in U}\ \rho_u(w)\, trust(c,u)}{|U|} \tag{3}$$

In equation (3), *tc(w)* indicates the reputation (feedabcks) of service *w* with respect to user *c* and *trust(c,u)* denotes trust of composer user *c* to individual user *u* in set *U* of users who has provided ratings over service *w* in their profile and their inferred privacy level allows exploitation of their ratings by user *c*. The final trustworthiness of service *w* is considered as the average of its reputation across all users in set *U*. Further, we limit the policies to simple ones based on trust values. The recommender could make requests to a number of recommenders until the total amount of trust value is reached [30]. A recommender chain in trust transfer is not explicitly known to the trustor. As summary, in case of trust transfer real distributed systems can be stated as follows:

- The trustor must know the recommender's trust attitude.
- The trustor must believe the recommender is honest.
- The trustor must be willing to acquire beliefs from the recommender.
- The trustor must know the recommender's trust policy.
- The recommender's trust policy must be more stricter than the trustor's.

The trustor only needs to know his/her contacts who agree to transfer some of their trustworthiness. This is useful from a privacy point of view since the full chain of recommenders is not disclosed. This is in contrast to other recommender chains such as public keys web of trust [30]. If the full list of recommenders is revealed to an attacker then he is able to check the independence of recommender chains i.e. the privacy protection is lost. Fig. 5 shows that, Trust can be improved through reputation mechanism. Initially trust can change dynamically and flow from one user to another and in results; it comes in form of new trust for a user, which concerns some privacy issues regarding that user also.

Now as summary of this section, the trade-off between privacy and trust (in LBSs) is well explained with some clear goals. Of course, there is no blanket solution to convince users that a service provider/other users are trustworthy or not. We discuss some valuable assumptions for privacy and trust trade based on linkability of pieces of evidence. At a point, when genuine information around an entity increases. The assessment of its trustworthiness is more exact and in the event that this substance is to be sure really trustworthy, its trustworthiness likewise increases. Also, when its security or privacy abatements and as discussed, it is almost a one-way function. Since protection of privacy and security i.e. recovery such issues in human being, difficult to accomplish [20]. If privacy or trust is lost, privacy took more time to recover than trust. The importance of trust varies organization to organization, depending on data's value. This work concentrates on the accompanying privacy- trust trade-offs measurements: right of informational self-determination, data security, information privacy including privacy (protection) of individual conduct, freedom from observation, communication privacy, and data privacy etc. Next section concludes this work in brief with some relevant future directions.

6 Conclusion and Future Works

Now days, several LBSs are offered by several Service Providers (SPs). Accessing such services is becoming an essential part of our daily life's activities. With these services location privacy and trust issues raised. A good health is necessary for everything. Aspects of social capital like; trust, social support and social networks are also important determinants of the mental health of individuals. Strong ties within the group may lead to less trust and reciprocity to those outside the group. In this world, a person who trusts everybody is a fool and who trusts nobody is a bigger king. Because todays one person just want to take advantage from another. So as soon as you trust yourself (then you will find yourself), you will know "how to live"? Trust is an extremely important commodity to any relationship, personally or organizationally. The good news is that if trust and privacy has been broken among any relationships, your professional or personal relationship can recover with a word "sorry". It takes hard work (a long term) to build certain level of trust, especially after it has been betrayed, but it can be recovered. But it is hard to gain in case of relationships among buyer, seller and producer. Similarly, once privacy is leaked by member of your family, it can recover in some time. But it cannot be recovered, if it leaked by service provider like; a hospital. In an analysis of ecological factors, societies with low trust levels exhibited higher rates of violent and property crime, such as homicide, assault, robbery and burglary. In case of providing trust–privacy trade-offs, "Most people can be trusted". This work discusses the concept of trust transfer. Trust transfer is still limited to scenarios where there are many interactions with the recommenders. Trusted in one system can be different to another system, but the goal remains the same i.e. to improve relationship.

This work provides maximum facts to improve trust among vehicle users and also provides a new proposal that no one has discussed before i.e. a traffic free signal which can be reduced the necessity of mix zones to change their pseudonyms (to preserving their privacy travelling on road and even with using parking services near/sides of road network). A final open research issue concerning privacy concerns the possibility to negotiate the ER schemes without compromising privacy. Further, one may contend that it is unfair for the recommender to lose the same measure of belief (trust) as indicated in his/her suggestion (recommendation), moreover if, the results are really trustworthy or not trustworthy. It is imagined that a more intricate grouping of messages can be set up in place in order to revise the decline of trustworthiness after an effective result. This work is still left concerning as for future work, since it can prompt vulnerabilities (for instance, taking into account Sybil Assaults with cautious cost/advantage examination). Measuring user's location

privacy and trust also is a non-trivial task. During this work, we find out that, there is no unique standard for this. As future work, there should be an unique framework which mitigates all these privacy, trust problems, together validate our model/framework and enforcement mechanism for preserving location privacy with certain level of trust using real world data. Now we are in a new era where providing trust and privacy to passengers and drivers which will help us to protect many of lives and will provide different experiences to human beings that no one has provided before.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Costa C, Bijlsma-Frankema K. Trust and control interrelations, Group and organization management, 2007;32(4)392–406.

[2] Lund M, Solhaug B. Evolution in relation to risk and trust management, Computer. 2010;49–55.

[3] Available: http://us.reachout.com/facts/factsheet/trust-issues

[4] Govindan K, Mohapatra P. Trust computations and trust dynamics in mobile adhoc networks: A survey, IEEE Communications Surveys and Tutorials. 2012;14(2):279–298.

[5] Matt Twyman, Nigel Harvey, Clare Harries. Trust in motives, trust in competence: Separate factors determining the effectiveness of risk communication. Judgment and Decision Making. 2008;3(1):111-120.

[6] Available: http://syd.ungetalenter.dk/sites/default/files/aktiviteter/trust_definitions.pdf

[7] Abdul Rahman A, Hailes S. Supporting trust in virtual communities. Proc. 33rd Hawaii International Conference on System Sciences; 2000.

[8] Pekka Sakari Ruotsalainen, et al. A conceptual framework and principles for trusted pervasive health. Journal of Medical Internet Research; 2012.

[9] Available: www.kenblanchard.com/img/pub/blanchard-building-trust.pdf

[10] Sajjad Hashemi, Cloud computing technology: Security and trust challenges. International Journal of Security, Privacy and Trust Management (IJSPTM). 2013;2(5).

[11] Amit Kumar Tyagi, Sreenath N. Preserving location privacy in location based services against sybil attacks. International Journal of Security and Its Applications (IJSIA). 2015;9(12):189-210.

[12] Available: http://www.ijdesign.org/ojs/index.php/IJDesign/article/view/67/30

[13] Available: http://www.cauce.org/2010/05/facebook-privacy-and-the-loss-of-trust.html

[14] Westin Alan, Privacy and freedom. New York: Atheneum; 1967.

[15] Available: ojs.academypublisher.com/index.php/jnw/article/viewFile/jnw0702322328/4366

[16] Amit Kumar Tyagi, Sreenath N, et al. Providing privacy preserved location and trust enabled services for location based services. In proceeding of Springer/International Conference on Soft Computing, Intelligent Systems and Applications, Bangalore, India; 2016.

[17] Olatunji SO, et al. Integrating a secured access control policy on wireless sensor networks. British Journal of Mathematics & Computer Science. 2016;16(6):1-12.

[18] Amit Kumar Tyagi, Sreenath N. Providing together security, location privacy and trust for moving objects. International Journal of Hybrid Information Technology (IJHIT). 2016;2(3):221-240.

[19] Richard Eiser J, Mathew White P. A Psychological approach to understanding how trust is built and lost in the context of risk. Presented at SCARR conference on Trust, LSE; 2005.

[20] Jean-Marc Seigneur, Christian Damsgaard Jensen. Trading privacy for trust, Second International Conference, iTrust 2004, Oxford, UK; 2004 (Proceedings).

[21] Available:https://www.cs.purdue.edu/homes/bb/CLEAN--z--SHORTEST--Privacy-Trust_Tradeoff.pdf

[22] Seigneur Jean-Marc, Jensen Christian D. The role of identity in pervasive computational trust. Dublin, Trinity College Dublin, Department of Computer Science, TCD-CS-2004-48. 2004;13.

[23] Amit Kumar Tyagi, Sreenath N. Future challenging issues in location based services. International Journal of Computer Applications 2015;114(5):0975 –8887.

[24] Available:https://accoladecommunications.wordpress.com/2012/04/22/15-facts-about-trust-definition-types-perspectives-week-2-of-twelve-weeks-to-trust/

[25] Amit Kumar Tyagi, Sreenath N. Providing trust enabled services in vehicular cloud computing (extended version). In proceeding of ACM/International Conference on Informatics and Analytics (ICIA), 25-26 August, Pondicherry, India; 2016.
DOI: http://dx.doi.org/10.1145/2980258.2980263

[26] Rama Krishna Kalluri, Guru Rao CV. Addressing the security, privacy and trust challenges of cloud computing. International Journal of Computer Science and Information Technologies. 2014;5(5): 6094-6097.

[27] Available:http://atwtraining.com/trainers-toolbox/whitepapers/trust-works-four-keys-to-building-lasting-relationships/

[28] Irshad Ahmed Sumra, et al. Trust levels in peer-to-peer (P2P) vehicular network. International Journal of Information Technology and Electrical Engineering. 2014;3(5).

[29] Available:spirit.cs.ucdavis.edu/pubs/journal/kannan_survey.pdf

[30] Jean-Marc Seigneur, Alan Gray, et al. Trust transfer: Encouraging self-recommendations without sybil attack. Third International Conference on Trust Management iTrust; 2005.

[31] Jean-Marc Seigneur. Trust, security and privacy in global computing. Thesis submitted to the University of Dublin, Trinity College; 2005.

[32] Peter Herrmann, Valerie Issarny, Simon Shiu. Trust management. Third International Conference, ITrust 2005, Proceedings. Paris, France. 2005;3:23-26,.

[33] Jennifer Golbeck. Computing with social trust. Springer Science & Business Media. 2008;16.

[34] John Vacca R. Morgan kaufmann. Computer and Information Security Handbook; 2009.

[35] Seigneur Jean-Marc. Online e-reputation management services survey. In: Morgan Kauffman. Computer and Information Security Handbook; 2013.

[36] Palanisamy B, Liu MobiMix L. Protecting location privacy with mix-zones over road networks. In: 2011 IEEE 27th International Conference on Data Engineering (ICDE). 2011;494–505.

[37] Fei Xu, Jingsha He, et al. Toward trust-based privacy protection in consumer communication, International Journal of Security and Its Applications. 2013;7(3).

[38] Nurit GalOz, Tal Grinshpoun, et al. Privacy issues with sharing and computing reputation across communities. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2010;1(4):16-34.

[39] Available:http://www.salutogenesis.hv.se/eng/Salutogenesis.5.html

Appendix A

Table 1. Comparison of trust and privacy characteristics

Trust characteristics	Privacy characteristics with respect to Security
▪ Trust is a relationship. It involves risk. ▪ Trust is based on beliefs (human being) and it change dynamically ▪ Trust has a positive expectation. Trust is a binary decision: trust or distrust. ▪ Trust is fuzzy since trust is imprecise and vague. ▪ Trust is a relativistic, complex, and dynamic concept. ▪ Trust involves goodwill or benevolence. ▪ Trust is freely given, dynamic and ever-changing. ▪ Trust factors change at different organizational levels. ▪ Trust moves among interpersonal & intergroup levels. ▪ Trust is generative. It creates more trust. ▪ Trust is bidirectional i.e. multi-dimensional and Trust isn't as asymmetric. ▪ Trust is a very complex and multi-faceted notion. ▪ Trust varies by type of relationship. ▪ Trust evolves over time, or does it? ▪ Trust can be a cause, an outcome or a mediating variable. ▪ Trust is a confidence in someone's competence and his or her commitment to a goal. ▪ Trust as "reliance on the integrity, ability, or character of a person or thing. ▪ Trust is truly ubiquitous and beneficial in social systems. ▪ Trust essentially is and should be based on knowledge – knowledge is brought by evidence. ▪ Trust in a virtual identity cannot be accurate if the information used at the recognition level is imprecise or simply invalid.	▪ Security is a process, privacy is a consequence. ▪ Security is action; privacy is a result of successful action. ▪ Security is the sealed envelope; privacy is the successful delivery of the message inside the envelope. ▪ Security is a tactical strategy; privacy is a contextual strategic objective. ▪ Privacy is a state of existence, security is the constitution supporting the existence ▪ Security is a condition, privacy is the prognosis. ▪ Security is action, and privacy is a result of successful action ▪ Security is the strategy, privacy is the outcome. ▪ The main characteristics of privacy are also diverse, subjective and context-dependent. ▪ Privacy is "the ability to prevent other parties from learning one's current or past location. ▪ Privacy can control through policies.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/17019