ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 1, 387-402 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Trust and Reputation Mechanisms in Vehicular Ad-Hoc Networks: A Systematic Review

Amit Kumar Tyagi[1,2,*], A. Mohan Krishna[3], Shaveta Malik[4], Meghna Manoj Nair[2], Sreenath Niladhuri[1]

[1]*Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry-605014, India*

[2]*School of Computing Science and Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, 600127, Tamilnadu, India*

[3]*Department of Computer Science and Engineering, Lingaya's Vidyapeeth, Faridabad, Haryana, India*

[4]*Department of Computer Science and Engineering, Terna Engineering College, Navi Mumbai, Maharashtra, India*

ARTICLE INFO

Article history:
Received: 23 October, 2019
Accepted: 25 January, 2020
Online: 20 February, 2020

Keywords:
Vehicular Ad hoc Networks (VANETs),
Vehicle User,
Trust and Reputation
Security
Privacy in Vehicles

ABSTRACT

An emerging trend has been observed in the Trust and Reputation (T & R) systems in field of decision-making support for a majority of the provisions propagated by the Internet. It is the extreme importance that peers (users) are able to trust each other and rely on them for file sharing and for services. This paper provides the reader an apprehensive and completely true information and details on a large number of the present conceptions, proposals, issues, and the key to those problems in VANETs and other fields to enhance the eminence of the data in transportation through a systematized literature review. Trust and reputation have also been discussed gravely in this paper. After the scrutinized analysis of more than 90 articles related to trust in a plethora of fields, extracted from few of the apt scientific sources ((i.e., SIEEE Computer Society, ACM Digital Library, Springer Link, Science Direct, and Wiley Online Library), and hence, succeeds to bring about the major hurdles and necessities for trust in real world and future research.

1. Trust and Reputation (T&R) – A Detailed Discussion (Introduction)

In the past decade, trust has received a great attention in the field of psychology, sociology, economics, political science, anthropology and recently in wireless networks. Mundane life find trust to be at the zenith of priority and everything goes by accordingly [1]. After all, when you run into a communal society, trust proves to be a foundation for desired decision making and efficient rating strategies. There is no universal definition for trust and reputation. In this work, authors defined Trust as "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" [1]. Reputation is the opinionized version of an individual regarding another person or an object. In Oxford dictionary, reputation is said to be an opinion or belief held on someone about something.

*Corresponding Author: Amit Kumar Tyagi, amitkrtyagi025@gmail.com

Abdul Rahman et al. [2] define reputation as "an expectation about an agent's behavior based on information about its past behavior". Chang et al. [3] define reputation as "an aggregation of the recommendations from all of the third-party recommendations agents and their first, second and third hand opinions as well as the trustworthiness of the recommendation agent in giving correct recommendations to the trusting agent about the quality of the trusted agent". Trust have been invented an essential term in human-beings life, so it should be maintained in vehicle applications (for example, during carpooling, parking) to encourage the vehicle users to perform transactions with the other users over road network.

1.1. Trust

Trust is the old word and came into existence along with human being evolved on this earth. It plays a significant role in the survival of human beings. As we experience trust on daily basis, it is not an objective property but subjective to the degree of belief shown on a person, process or objects. The degree of trust varies over situation, person and opinion. It is not a blind guess or a game of chance, but it is blind guess based on the

knowledge and experience acquired over a period of time. The basic understanding of trust is list as follows:

a. The development of a bonding between two or more individuals aimed towards a particular target of action or goal is referred to as trust, such that they trust and rely on each other for the smooth and successful fulfilment of the action. The first specimen is the subject, while the other is the agent. Hence, we can see that subject, agent and action can be used to define trust.
b. Uncertainty and doubtfulness are ways to measure trust. Consider the following three situations: (a) The case when the subject has cent percent trust on the agent and strongly believes that the agent can and will fulfil the action. (b) The case when the subject highly despises the trust worthiness of the agent and hence there is no possibility of uncertainness here as well, but in a different perspective when compared to the previous case. (c) The case when the subject has an extremely vague idea about the agent, leading to the rise of large levels of uncertainty as he doesn't trust the agent at all.
c. Trust is not symmetric in most of the cases. The thin line of trust between two entities A and B does not have to facilitate the very same feeling for either of them.

In general, trust can be a personal experience between the partners based on the context, reputation and on recommendations. It is the presence of uncertainty and depends on the expected risk among the partners while interaction. Further, we recall some characteristics of trust as follows [1]:

- Binary, Directed Relation: Trust is a binary directed relation linking two entities. It is considered as the confidence of an entity called trustor towards another entity referred to as trustee.
- Asymmetry: If entity A trusts entity B, it does not imply that entity B trusts entity A. Trust is not necessarily reciprocal between a pair of entities.
- Contextual: Trust is considered in the context of particular actions which the target entity may perform.
- Subjectivity: Trust is the level of the subjective probability with which the trustor assesses that the trustee entity will perform a particular action.
- Non-transitivity: If entity A trusts entity B, and B trusts C, it does not necessarily imply that entity A trusts entity C.
- Composability: Trust relations can be constructed between not directly connected entities. Entity A may query for trust of entity B. Many entities in the community can provide different ratings, i.e., reputation scores of trusts for B. Thereafter, entity A can aggregate the received information to assign a trust level for B based on its own trust assessment method.
- Self-reinforcing: Entity tends to act honestly with trusted entities and to abstain with untrusted ones. Thus, this behavior reinforces the trust relation among trusted entities along the time.
- Dynamicity: The trust score of an entity may change over time. It may increase or decrease depending on the current performance of the entity. If its current interaction has a better quality than the last ones, its trust level could increase, and vice versa.

Properties of Reputation based Trust Systems are Complexity, Decentralization, Dynamics, Scalability, Privacy, Security level, Sparsity and Robustness, etc. A comparison among trust properties can find in table 4.

Trust Parameters: The certainty of agents being capable enough of doing an action at par excellence. This has a the two-tiered definition: Firstly, agents must develop the habit of believing their peers; secondly, its completely in the hands of the agent to delegate actions to the peer. In a social environment, trusty nature can often be defined as the facilities handed over to the other earlier irrespective of their relationship in the present. Content storage and exchange are the seemingly leading areas in the field of trust within P2P technology. With advancement in modern ways of living, most of the models, focus on malicious behaviors and capacity to complete the transactions.

The five factors for evaluation of trust are as follows:

- The feedback obtained between peers.
- The final and all in all dealings happening between the peers.
- The certainty of the source of feedback
- The framework for distinction of important transactions from the less important ones.
- The social factor for addressing the corresponding issues.

The word 'trust' describes that belief and expectation about future behavior based on past experiences and evidences collected either directly or indirectly.

1.1.1 Belief (or faith)

Belief is the essential and important to make trust and reputation among people. Trust is "a peer's belief in another peer's capabilities, honesty and reliability based on its own direct experiences". Reputation is "a peer's belief in another peer's capabilities, honesty and reliability based on recommendations received from other peers". The decision by agent X to delegate a take to agent Y is based on belief and this belief is called 'trust'. To build a mental state of trust, the basic beliefs that an agent need are:

- Motivation belief- X believes that Y has some motivation to help X and this motivation over long-term help X to achieve his goal. If y believes to be motivated, then x tends to trust him.
- Competence belief: The optimistic mindset of the agent to assure himself that the task can be accomplished by agent Y. Else, the feeling of trust would be of utter waste.
- Dependence belief: The agent believes that better to rely on y to complete the task successfully.
- Self-confidence belief: X strongly believes in y for completing his task.
- Disposition belief*:* Though it may not be necessary that Y could do the task, articulation of disposition belief and support would gather great help along with two more beliefs:
    - Willingness belief: The agent is assured about Y doing α *(*the action that leads to the goal g). X is confident about doing the required proposal as suggested by Y. If Y feels uninterested in doing the task, they might as well end up masking themselves saying that they intend to do so. However, this

would immensely decrease the bond of trust between them.

- Persistence belief: The agent acquires a positive approach and a touch of stability in Y about the task completion of *α.* If Y's stability seems to dwindle, there are chances of risks being produced when they interact with Y, due to which there's just mere belief existing between the two.

These two beliefs together refer to what is called soul trust and reliance. Along with these, the following also arises:

- Fulfilment belief: If the agent believes that Y has the potential to complete g, the agent would decide

i) not to drop the plan of the goal ii) Not to bring about changes or modifications to it iii) to encourage Y to complete it.

In short, we can prove that trust revolves around a mentalistic feature which would showcase the agents mind (X) who prefers the work to be done by Y, Y being the intellectual agent. So, in short, X is completely assured of Y doing the action and Y continues.

Kinds of Trust

Trust and faith are complementary to each other and revolve around the sense of confidence. The only thing that distinguishes the two is nothing but the fact that trust consists of a risk of element but confidence does not. We often notice trust to be used in common geek speak, when people have a spark of feeling inside them, i.e., an internal emotion that keeps oscillating, on the basis of the situation. Trust is also considered to have phenomenal feeling of trusting or being trusted. Figure 1 discusses the kind of trust in term of computation (refer figure 1 after Appendix A).

Basically trust (among human being) can be positive, negative, global, local or based on recommendation or reputation value. In other words, based on the reputation or recommendation, trust can be positive, negative, global or local. The contravention of trust leads to mental fluctuations between the agent and the source. Hence, on the grounds of creative design agents open systems, trust can be summarised as shown:

- Basic Trust: It is a general trust disposed independently on the agent based on the good experience accumulated by the agent.
- General Trust: Without taking any specific situation into consideration, one agent will trust another agent.
- Individual-level Trust: The agents has some belief on their partners
- System-level Trust: By the rules of the regulatory bodies in the system, the agents are forced to be trustworthy.

There seem to be three different forms of trust on the basis of a societal research. This includes dispositional trust [1, 4], system trust [5], etc. There are numerous perspectives and takes on trust and it's not practical to furnish each one of them. Several Type of Trust discussed in [4]. Further, Trust Classes discussed as: For specificity on trust semantics, distinction between a large number of different trust cases on the basis of Grandison and Sloman's classification (2000) [6] has also been analysed..

- Provision Trust: It talks about the trust values of the dependent party and is to be looked into when they seem to acquire coverage from harmful and disloyal service providers. Business trust [7] is commonly used to showcase the communal interactions between the companies which emerge from the contract agreements that keeps a track of the trust relations between them. For example, when a contract mentions a qualified delivery service, business trust would act aa a provision trust in our language.
- Access Trust: It talks about the trust with respect to a principiated dimension wherein the dependent party's resources are being targeted at. This relates to the centralised component of any computer which is the access control paradigm. Grandison & Sloman (2000) [6] provides an excellent perspective of access trust systems.
- Delegation Trust: It personifies trust as an agent (delegate) and decides on behalf of the dependent party. It has been well pointed out by Grandison and Sloman [6] that one of the specific service provisions would be to act on one's behalf.
- Identity Trust: It portrays belief to be a claimed identity. X.509 and PGP are the trust systems which produce their very own identity [8]. This is a topic of interest in the information security society, of whose overview can be found in in Reiter and Stubblebine (1997) [9].
- Context Trust: It tags the limit up to which any dependent party trusts the necessary systems and machinery to facilitate safe and sound transactions. These can be keenly affected by critical architectural framework, insurance, legal system, etc.
- Experience Trust: It refers to the trust that an agent has obtained on the previous and past interactions with a client. The interactions are called as transactions and the trust thus obtained is transaction trust.
- Similar Trust: This is the trust than an agent acquires by reasoning with respect to a client with other clients. A client is considered to be well known if there's an active conversation existing between the client and the agent and both of them have their own experience trust about each other.

Trust Models in VANET: The trustworthy nature of peers is the key focus in entity-oriented trust models. On the contrary, data-oriented trust models focus on the loyal nature of the peers. Data-oriented trust models depend on evaluating the trustworthiness of the transmitted data. In such models, there is no long-term trust relationships between nodes are formed. The combination of a number of trust models use node's trust to evaluate the aptness of data. Figure 2 defines this concept/ picture clearly (refer figure 2 after Appendix A). Basically, trust depends on friendship-not money, not power, not education. Only if there is trust, will there be friendship. Whenever we got friendship, we got feedbacks or recommendation for future to maintain our trust among other person. A Detail description about various trust establishment models existed in VANET network discussed in table 3.

Trust Calculation

If two nodes want to communicate each other, the level of trust worthiness of two nodes must be high enough to continue the communication process. Before the initialization of a connection, nodes refer to the local table and seek help from the adjacent

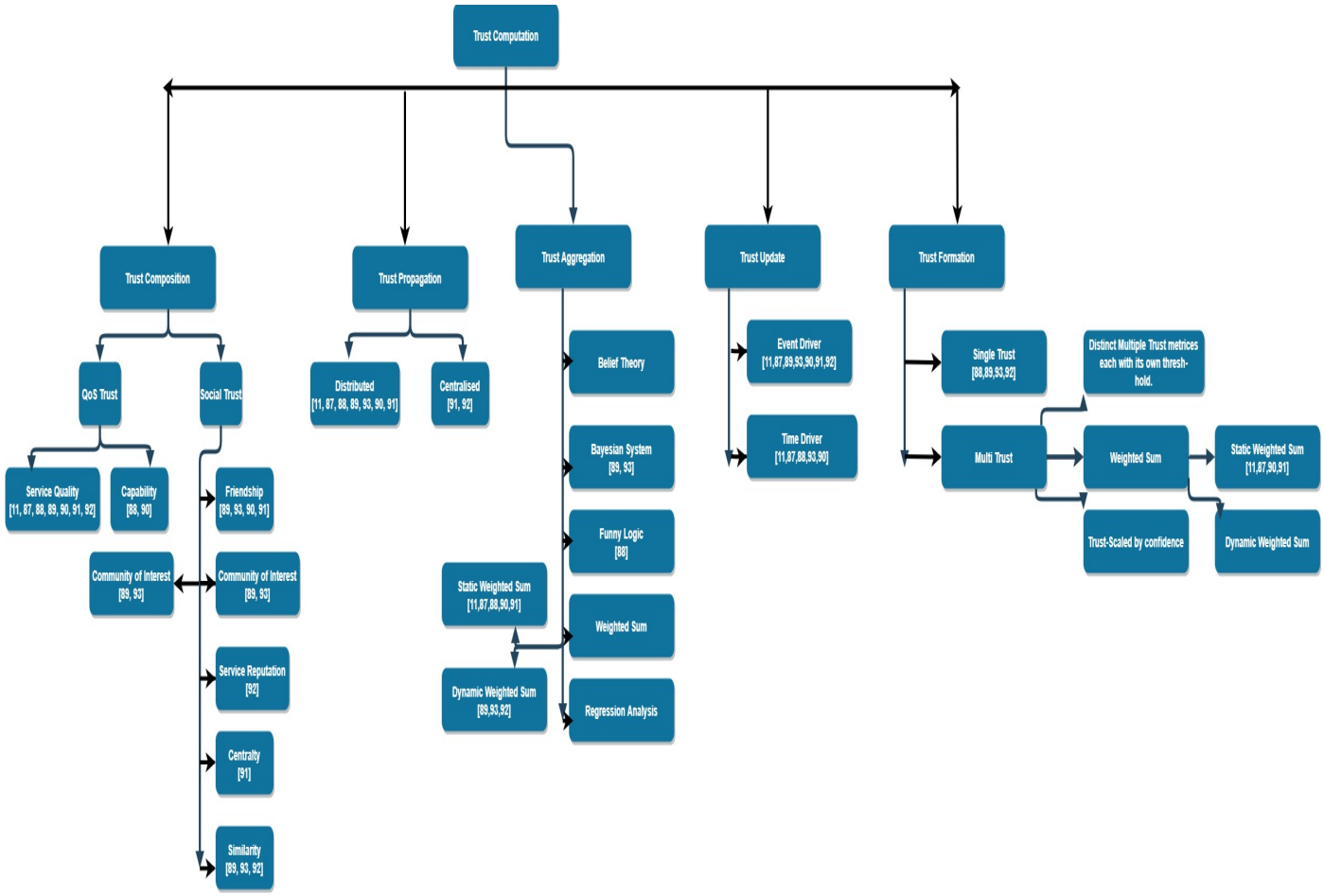

Figure 1: Classification Tree of Trust

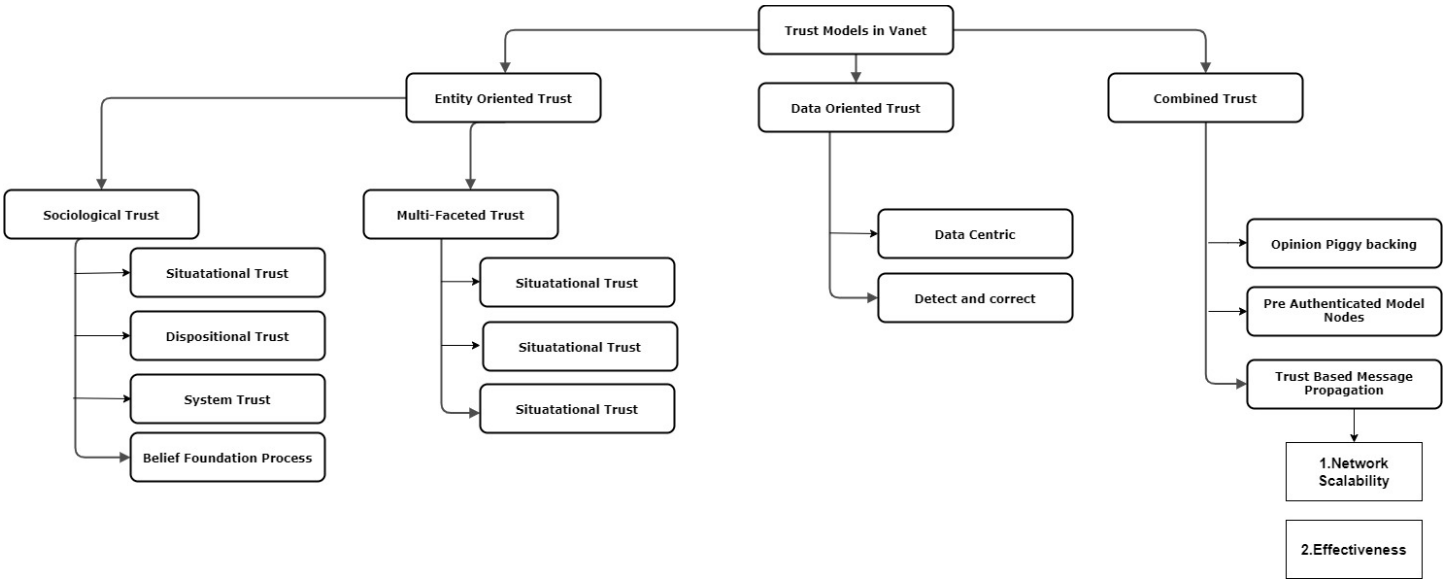

Figure 2: Trust Models in Vehicular Ad-hoc Network (VANET)

nodes to identify the trustworthy nature of the colleague. “Small World Problem” is a new approach to ease out and enhance the reach of the nodes to its neighboring nodes for trust evaluation. The decision made by every node is highly dependent on the prioritization given by them to the array and the minimum value too accepts them as per the “Trust Array” approach [10].

Some of the critical node accepts the communication request whereas few of them will reject it. Trust array values should be maintained somewhere on application level and recalculation of the values are required whenever the node initiate a new communication. Here trust model defines three important metrics: service, recommendation and reputation (see figure 3). Figure 3

represents variation of trust values when user starts a new interaction.

- Service trust metric is essential not only for evaluating the trustworthiness of the neighbor but also for the selection of the best service provider.
- Recommendation and reputation used to Measuring the trustworthiness of the new node. Recommendation trust metric include the number of recommendations for the stranger from various neighbor nodes.
- Reputation is required during the preliminary stages of communication. Later the number of acquaintances increases and hence the importance of reputation is less.

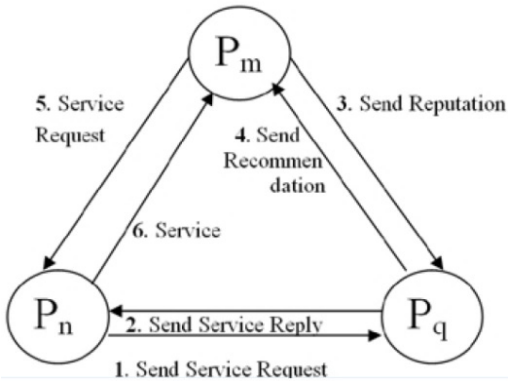

Figure 3: Interaction between the Peers

Computational Trust: Figure 4 shows that, Trust can be compute based on direct evidence (direct availability trust, direct integrity trust and direct competence trust) and indirect evidence (indirect availability trust, indirect integrity trust and indirect competence trust). The work on trust computations can be broadly classified into the following categories:

- Distributed trust computations: Each individual node creates its analysis on its peers through neighbor sensing, trust systems based on recommendation, and hybrid method.
- Centralized trust computations: It is a centralized form of computation and manipulation of the evaluations.

The central controls and manipulates the trust evaluations. In section 2, this work is provided in detail, i.e., advantages or disadvantages about each trust models (centralized, decentralized and partially decentralized). Through stringent sieving and combination of sophisticated technologies, around seven critical elements can be shortlisted in figure 4. Furthermore, through filtering combining the duplicated terminologies used in the different trust models, seven critical compositional elements can be summarized in figure 4. Further, dimension is to study what the sources of the trust values are:

- The syntax mainly focuses on the actual definition of trust if the outcome is a combined product.
- The model inculcated for the calculation of trust is called trust computation engine.
- Trust network includes the study on the pattern set up of the agents and the host agents.
- Uncertainty involves efficient risk management which supervises the occurrence of incidents and reliability which assures the reliability of the agent.

Values of trust are often classified into one or multi dimensions. A very specifically bound context limiting itself to the description of trust is found in a single dimensional approach. On the contrary, a multidimensional approach inculcates a feeling of unassured trust. The framework of trust values revolves around: rating, ranking, probability, belief, fuzzy value, etc. The rating is often related to numerical numbers of natural type. For example, on a scale of [11, 1], 1 is used for representing “Highly Untrustable”, while 4 is linked to “Highly Trustable”. Discrete tag-names are used for the labelling of the levels of trust, namely “Very Trustworthy”, “Trustworthy”, “Untrustworthy”, and “Very Untrustworthy” for direct which is mainly used for direct trust while “Very Good”, “Good”, “Bad”, and “Very Bad” are used for the recommenders’ trust. Local and Aggregate are the two types of rating [12]. Ratings based on the personal interactions with the second peer is called Local Rating and is produced whenever an interaction takes place. Ratings which are computed with the local ratings and validations from witnesses as a base is called Aggregate Rating. This is mainly used for computing if the peer is faithful or loyal and if they are worthy enough to be propagated to other peers.

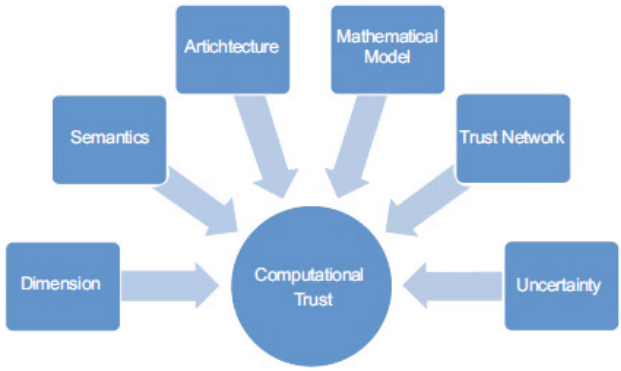

Figure 4: The Compositional Elements of Computational Trust

The authors of [13] seem to have classified trust into three tiers, i.e., Credential Base Trust Management Systems (all service providers along with the services are reliable but those requesting for it are not necessarily trust worthy), Reputation Baes Trust Management Systems (Both the providers of trust and the services are unreliable and the requesters choose the providers based on the values of reputation to provide the desired services) and Social Network Based Trust Management Systems (social networks form a foundation for these and reputation is analyzed on the basis of societal relationships). A variety of these types are intricately described in [1].

1.2. Reputation

Reputation can be defined (an accepted definition by several researchers) as: the subjective cumulative value, as identified by the requester, with the help of the judgment by others, about the non-familiar characteristic or capability of a particular node with whom the requester has never communicated before. Reputation of a vehicle can be treated as the measure of faith which other vehicles have about the sender, based on the reliability of previously transmitted data. Basically, Reputation is an old human notion: The Romans named it “reputatio”: “reputatioest vulgaris opinioubi non estveritas” [14]. Reputation, often treated as a social control mechanism [15], involves the process of telling

the truth rather than faking ones' reputation. Since reputation is not bound to specific location, the change of region has less impact on the reputation information. That is reputable people will get their value even if they change the location. Another example is that the reputation of an individual is simply rumored.

The reputation information need not be authentic all the time as it may be biased or plagiarized by malicious recommender who wishes to destroy the recommender. The above Latin quote translates to "reputation is a vulgar opinion where there is no truth" [14]. The term reputation and recommendation are used in different context. Reputation value is used to access a stranger entity but recommendation used for known familiar entity. Reputation can be categorized as centralized and decentralized. In centralized category the reputation value is computed by a trusted third party where as in later it can be computed independently each node. Since trust depends on many factors, peers need to develop differentiated trust in multiple aspects of other nodes capability. Reputation systems if used efficiently with a positive approach, can be used to nurture humble behavior and to influence persistence to contacts in ad hoc networks. The key function of the system involves gathering, distribution, and clustering of feedbacks about the behaviors of peers and colleagues. These mechanisms seem to provide incentives for the benevolent behavior aiding people to be decisive about the people they trust. Prior experience with transaction partners can be induced into the forthcoming world in order to measure their status on trust and honesty and this is very often referred to as the "Shadow of the Future". However, they can be easily invaded unrelatable and misguided ratings. And this when done on purpose, is Recommendation-Based Attack. Note that the first Web sites to introduce reputation schemes were on-line auction sites such as eBay.com.

Classification of Reputation

In an ad hoc network reputation are viewed at two levels: local and network reputation. As reputation, it can be local or global. Local reputation, the reputation of a fellow peer based on direct conversations and relationships, and global reputation, which involves local reputation along with witnesses received from other, are the two types of reputations present. They often come in handy when it is necessary to decide whether peers should be propagated for further recommendations and to check their level of trustworthy nature. These reputations can be acquired directly or indirectly [16] (refer figure 4):

a. Direct Reputation: The witness is required to directly interrogate the peer to form a reputation about him or her. For example, if peer C had already conversed with peer D, it advises peer A regarding its intuitive feeling of trust reputation of peer D. And this kind of transfer of reputational information is called Direct Reputation [16].
b. Indirect Reputation: This involves the witness peer being interrogated by a middle peer (s) instead of direct interaction by the peer who requires the reputational feedback. For example, if peer A is unaware of the creditable nature of peer D, then he/she would infer about this to his/her fellow peer B to get a feedback in order to proceed accordingly and peer B may be required to further take this to his/her colleague peer D and then its reported back to peer A and the cycle is complete.

Generally, we identify three main types of reputation here:

- Positive Reputation
- Negative Reputation
- Neutral Reputation

Here, we define positive reputation as "Reputation of the reputation queried peer obtained from a witness peer that advises that the reputation queried peer be trusted" We define negative reputation as "Reputation of the reputation queried peer obtained from a witness peer that advises that the reputation queried peer not to be trust" We define neutral reputation as "Reputation of the reputation queried peer obtained from a witness peer that is unsure about the trustworthiness of the reputation queried peer". A newcomer or to a peer who has decided to use a brand-new identity are corresponds to zero reputation, as the case may be to avoid being admitted as someone who previously misbehaved. Non trivial is also known as characterizing good reputation. A possible approach lies in the identification of a threshold which permits to discriminate the outcome of the poll as representing a good or bad reputation. It is necessary to keep in mind that the possibility of providing or obtaining a perfectly apt and matching value is a rare chance. This is because its often characterized based on a collection of responses, if its positive opinions by a number of users, it will lead to a positive reputation which takes shape from a certain mixture of responses, producing a value higher than the threshold. The same applies to negative opinions as well.

Reputation based Trust System

An interesting and challenging research can be done/ performed in Reputation based trust management in peer-to-peer systems. The soul use of trust would be to develop trust among the colleagues, ensure safe and sound transactions to increase the satisfaction. There are four main varieties of reputation-based trust systems [17]: 1) gathering of details 2) data mapping for trust evaluation 3) broadcasting and 4) decision making. In a sensing campaign, a number of tasks are produced by the main server, one of which is then chosen by a participant. The participant, for example Pi, then would preserve his/her observations for a given task J on the basis of which he/she generates a sensing report RPi for the task. These are then sent to the server for verification. The server, on the other hand, combines the reports from a plethora of such sources and produces a detailed analysis. Some of the Properties of Reputation based Trust Systems are discussed as follows:

One can identify the main properties of reputation-based trust systems on the following basis:

- Traceability: It is suitable for participants whose past behavior is made use of for the tracking and analysis of the nature and mannerism of the person. It is a key source to predict the behavior of the person in the near future.
- Freshness: The reputational value which is being assigned to an individual participant which modulates and fluctuates the faithful and loyal qualities of the person.
- Separability: The individuals do not have any control on the updation of their reputation scores. They would have no rights to maliciously interfere or forge their reputation scores.

- Exposure: Dangerous and harmful participants should be portrayed and ejected or at the least, the hostile participants should be avoided. Unknown reputation-based trust systems are well known to acquire their previous goals and targets while masking the credentials and identity of the participants. A few of them have been mentioned in [18].
- Anonymous login: The participant must have the right to login and provide the reports in an unacknowledgeable manner or in incognito mode.
- Non-associative: The report shouldn't include the participants credentials or identification details which would reveal his/her persona. Therefore, the server wouldn't be allowed to link the report to any specific individual.
- MSR unlink ability: The server shouldn't be allowed to link Multiple Sensing Reports from the same individual.
- Anonymous demonstration: The service of giving demos and reports to the server without having to reveal their original identities to it must also be facilitated [18]. The fulfilment of these goals and preventive measures against the earlier mentioned attack revolves around the efficiency of the system. Participant should be active enough to elucidate their reputation values to the server anonymously [18]. The strength of the system determines the fulfilment of these targets and resilience to the earlier mentioned attacks.

Hence, the rest of this paper is organized as follows: Section 1 discusses the definitions of trust and reputation, trust models in VANET, parameters, and their characteristics, reputation mechanisms in Peer to Peer (P2P) networks, etc. Section 2 introduces trust and reputation model comparison in detail. Section 3 discusses about open issues in trust and reputation models. In section 4, this work argues about trust and reputation mechanisms. Finally, in section 5, we conclude with a summary of contributions. In the following sections, we do not differentiate terms "vehicle," "object," "users "and "moving object". Additionally, "Trust" and Reputation" are often used interchangeably in a network trust or reputation model.

2. Trust and Reputation Infrastructure Models

A variety of mechanisms related to trust and reputation have been proposed the longer run which ids applicable to different perspectives of life like e-commerce, peer-to-peer, etc. Trust is a feeling an individual possesses when he/she believes that the other agent will handle a given task. Trust is defined as "the belief that allows individuals to be willing to react after having taken the characteristics of the providers and the underlying Internet infrastructure into consideration". Trust should be substantially based on evidence. Trust (dimensions of trust) include confidentiality, authentication, integrity, authorization, technical security and non-repudiation. In spite of its simplicity, it captivates few of the highly targeted properties of trust (found in [19] and table 4): Trust is a two-way relation between the agent and his/ her peer.

- It is a kind of decisive statement- trust or distrust
- Trust revolves around a final aim or target which is to be achieved by the trustor after relying on the trustee.
- Trust is very often descriptive and personalized. Different trustors may make differed decisions when relating to the same goal and trustee.
- Trust is uncertain and highly cloudy.

This type of work is bound to produce modularized models combining different ways of trust and reputation.

- Trust based on conversations and meetings with people in the past,
- Trust based on the roles payed among the agents,
- Trust based on the reports sent in by the witnesses regarding the attitudinal behavior of a person, and
- Authorized reputation formed from third party references.

This type of work has been known to propose a novel and innovative peer-to-peer trust model in ad hoc network systems. In the model which we have proposed [1, 20], trust is a logical connects of emotions: trustor, trustee, and goal. The predicate turns out to be true when the trustor believes the trustee for completion of the task, else it is false. Each subject is expected to possess a set of policies on the grounds of trust. These policies reflect the trustors analyzing criteria and builds up a few traits for the trustee and the environment. However, the degree of trust varies from one person to another. The accreditation for a trust relationship is as follows:

- If T's value of a trusted relationship lies between 0 and 1, then it's trust.
- If T's value of a trusted relationship lies between -1 and 0, then it is distrust.
- If T's value is equivalent to 0, then it is not trust and not distrust.

The models follow the given steps for a systematic and efficient working [21]:

a. Gathering and sorting out information related to a specific participant with the help of others opinions and recommendations.
b. Putting together all the bits and pieces of the received notification in order to compute a matching score for each peer.
c. Choosing the highly reliable and professionalized entity in the community to carry on the task smoothly and assessing the satisfaction of the user.
d. Based on the received feedback, the final step of rewarding or punishment is put forth.

Trust ratings are updated based on the compatibility of second-hand reputation information with prior reputation ratings. For more comparison and survey regarding about trust and reputation mechanisms, refer Table 1 and table 2 (refer appendix A). Three distinctive levels have been used to classify trust and reputation models from this perspective according to what was observed in trust and reputation models [19,22]:

- Level 0: Behaviors which involve cheating and plagiarism isn't considered and it mainly focuses on a massive number of agents who provide honest opinions and ratings to condemn the response from malicious agents.
- Level 1: The model perceives the agents to hide or opinionize the details though they never lie.
- Level 2: The model includes particular mechanisms to handle liars.

Though trust and reputation differ quite a lot, they're closely related and are also used to assess a persons' trustworthy nature. The common features they share are:

- Context specific: Trust and reputation both are liable on some or the other context. For example, Mike believes in John in the form of a doctor but not as a person who can fix his car. So, with respect to the case of a doctor, John is trustworthy and with respect to a mechanic, he clearly isn't.
- Multi-faceted: With reference to the same topic, it is of prime importance to generate a varied trust in varied perspectives of the potential of a person. The same goes for reputation as well. Consider this example, a customer is likely to analyze a hotel on a number of categories like food quality, cost, service, etc. The context-specificity of trust highlights that trust depends on the situation and can be characteristic, multi-faceted, etc.
- Dynamic: Trust along with reputation may deteriorate or accelerate with experience and is likely to decay with time.

1.2 Advantages and Drawbacks of different types of Trust and Reputation Management Infrastructures

The points discussed below describe the pros and cons of different varieties of trust and reputation management frameworks:

Centralized systems:

They use a reliable federal server for handling the reputation details.

Advantages:

- Flexible and simple usage
- Simplified design structure
- Ensures efficiency as all the details received by the peers are handed over to the corresponding peer.
- Keeps data together and persistent.

Drawbacks:

- Hard to attain if all peers can't trust a single entity.
- Points out even a single failure point and blockages as a large number of peers can send queries to the same entity.
- Points out even a single attack point like DoS (denial of service) attacks, Sybil attacks [8,23], sabotage and subversion.
- Costly to acquire efficient performance and strength
- Not scalable
- Not resilient to lawsuit

1.2.1 **Completely decentralized systems:** The details pertaining to the reputation is stored at their level itself and the information is scattered throughout the network.

Advantages:

- No individual failure points
- No requirements for an all-trust subject
- Provides strength and scalability
- Resistant to lawsuit

Drawbacks

- Many overhead messages are generated to maintain and handle the data
- Flooding is a necessity to acquire the required details from peers to cumulate different trust values
- The layout fluctuates often because of the momentary behavior of the peers' dude to which data loss is often existing.
- The data can be easily tampered or modified.

1.2.2 **Partially Decentralized Systems**

Advantages:

- Efficient search hacks for data
- Easily manageable and scalable
- Resilient to lawsuit
- Require a smaller number of super nodes to handle data
- Super node can easily access data from each other
- Empowering peers from the pressure of answering unnecessary doubts as peers are contacted by the respective super nodes on request alone.
- Efficient implementation of service distinction

Drawbacks:

- Super nodes should be blindly rusted to take over the details
- A burden on the nodes

Hence this paper discusses several trust and reputation computational models that attempts to address the concerns raised in table 1-4. This section discusses about the characteristics, advantages, and disadvantages of different types of trust and reputation systems. The next section contrasts several open issues in trust and reputation mechanisms in detail.

3. Open Issues

The work concludes with trust being linked to multi-agent systems by bordering the prime concerns to be tackled so as to create a complete model for an open system:

a. **Strategic Lying:** While the problem is being dealt by a few reputation models problem (such as Schillo et al. (2000) [24]; Sen & Sajja (2002) [25]; Zacharia & Maes (2000) [26]), a majority of them don't give a deeper in sight of strategized lying. It involves belittling the agents to find a trustworthy character in a liar which is then exploited for selfish deeds.

b. **Collusion Detection:** A small count of the interactive mechanism has been trained to comply with collusion (Brandt, 2002 [27]; Sen & Sajja, 2002) [25]. Furthermore, they've failed to explain how they can learn to collude though they were successful in showing how the agents could counter good deeds over time. This is the same as passing about false information to take advantage of others. We can expect agents to schematize and collude in an unrestricted environment, but if the system is expected to be efficient and well-functioning, collusion must be prevented. Or else, the agents might as well trust people who are complete liars and would take full advantage of them. In our research work, firstly, we are keen towards approaching it in a perspective which would make the system efficient and resilient to malicious mannerisms like collusion. Simultaneously, we also penetrate into the depths of combining trust control long with attack detection to suppress sudden attacks. The next concern is to detect peers as time passes

and link their past history with them. We are also continuing developing an extensive set of adaptive metrics, using the test bed to evaluate them, and finally testing the approach with real workload data.

c. **Context:** A large number of the models fail to consider the important fact that interactions often happen in an organizational context. It is absolutely wrong to label an agent dishonest or as a liar just because an agent has performed poorly, as it may be due to certain professional environment changes. Instead, the environmental variable is to be taken into consideration for this very purpose. This calls for a better risk analysis in the environment (Yamagishi et al. 1998 [28]; Molm et al. 2000 [29]). The absence of stern rules may lead to increased risk factors, which in turn will result in the analysis of an honest agent to be considered extremely trustworthy than his actual nature. Thus, if rules hinder dishonesty, there will be no requirement to increase trust related conversations among partners (Molm et al. 2000 [29]).

d. **Expectations:** Hardly any of the models surveyed are capable of conveying their expectations to one another (consider the case of data exchange regarding the quality of goods or delivery time). In an unrestricted environment, agents are free to possess different view-points and approaches which would intimate the type and form of interaction. For example, "High quality service" can mean "exact timed delivery" for one person and it may mean "good pricing" for another one. REGRET has put forth a transcendental dimension trust rating [30, 31] but this one doesn't show the conversation between the peers to comprehend each other's expectation. Once the expectation has been analyzed, the agent can satisfy the other side of the party easily. Or else, they may feel deemed to be untrustworthy with an agent.

e. **Social Networks:** Most of the security models presume a lot of scenarios which is built on the previous interactions and conversations or which are given by the agents (Schilloet al. 2000 [24]; Sabater & Sierra, (2001, 2002) [30, 32]; Yu & Singh, 2002b [33]). The semantic of the connections should be clearly defined within the network. (for example: as collaborators, partnerships in coalitions, or members of the same organizations)

f. **Coping with Peer Abuses and Selfishness:** To secure P2P system application a thorough investigation is needed for various behavior models. New mechanisms should be proposed to deal with intrusions, free riders, black mouths, collusions, and selfishness of peers. More focus should on game theoretic studies and benchmark.

g. **Reputation System for Unstructured Peer to Peer (P2P) System:** DHT (Distributed Hash Table) overlay network provides the foundation for Power Trust [34], Eigen Trust [35], and Peer Trust [36]. But, a majority of the P2P systems formed on the internet platform are unstructured and is in high demands. The major challenge faced in this field is the speedy performance of the reputation aggregation while forbidding the use of fast searching or hashing mechanism. To cross this hurdle, we are mainly focused on a gossip-based mechanization.

h. **Explore New Killer Peer to Peer (P2P) Applications:** The analysis of modern P2P applications for structured and unstructured P2P systems are a necessity. Most of the current P2P applications don't seem to have a strong and interactive bond between the users and hence, cooperation between the users should be apprehended.

i. **Others:** There are some other important concern yet to be focused are as follows:

- Impact of network dynamics on trust: The intricate analysis and description of the impact is yet to be looked into in the case of trust dynamics. The best example is that flexibility often affects the trust propagations and other modules and the clarified relationship is yet to be studied.
- Computations of trust in cooperative and non-cooperative games: In a self-organized distributed network, nodes may result in positive or negative suggestions in a straightforward or malevolent manner. These perspectives are a subdivision to a variety of scenarios in the complicated systems combined with game theoretic interactions, of which the games may be non-cooperative but are controllable using Nash equilibrium. It is to be noted that every node indulges in the games individually or in a compound manner wherein, a group of nodes form smaller groups to play games with each other and against the remaining ones. However, this field hasn't been studied to great depths.
- Impact of heterogeneous nodes on trust: Using wireless networks prove to be highly ununiform. Here, uniformity refers to the roles played by the nodes, their capacity and refuge. When trust takes form, varied evaluations ensure that not all of the nodes or their contents are treated the same. Hence, the very same descriptive pattern cannot be applied to monitor the trust levels of all nodes and their details. However, this field requires extensive knowledge and induction of network dynamics and heterogeneity in the trust evaluation functions.
- Security paradigms to enhance trust in the network: The capacity of data delivery and security concerns complements the amount of trust a recipient is likely to put forward on the data handed over. For example, the piece of information we've received can't be trusted completely if the sender or its path seem to be malicious. Furthermore, if the authenticity legalization system isn't functioning in full swing, it would be our call whether to trust the data or not. Deep dwelling into the subject would give further clarity on these issues.
- Social and context dependent trust: In the modern era, social relationships and content-based trust have been in the limelight. However, this is an area not often touched by Mobile Ad-hoc Network (MANET) because the dependence between the networks, be it social or communications, and their application are yet to be explored by MANET. Since validation of trust is a prime area for future research, they can be aided from the social communities.

This section discusses various open issues with respect to trust and reputation systems for further research. The next section arguing about trust and reputation and also provides some views to respective models.

4. Arguing about Trust and Reputation

We have discussed about trust and reputation in above sections and finally, this work made a conclusion that trust is an essential entity which is needed to be maintained in centralized system or decentralized and distributed systems. So now we discuss or arguing all possible ways to enhance trust and reputation in people and organizations.

4.1. Arguing about Trust

As definition of Trust "it is the belief the trusting agent has in the trusted agent's willingness and capability to deliver a mutually agreed service in a given context and in a given time slot". As we can be seen, trust pervades multi-agent interactions at all levels. Instead of trying hard to apprehend a translation between each other for trust evaluation, a versatile approach would be to convince others about how and why our very own evaluation seems to be apt. Arguments related to trust are mainly focused on whether an evaluation or analysis should be accepted or not. For contemplating among the models, we need to develop a new approach of looking at trust. Current models are highly colossal: input refers to the evidence which is further processed and then the output produced is the trust report. T argue about the betterment of one trust model over that of another, every agent should have a clear-cut perspective of why his very own model is the best (Pinyol et al. 2008 [37]; Castel franchi and Falcone, 2010 [38]). We consider an agent based on multi-context systems as in Pinyol et al. work (2008) [37] and have taken up the case further in a reflective manner as in [20]. Our target is to implement this in an optimized manner, allowing agents to allow for adapting to its trust model. With this, our next step is to lay down a protocol that enables agents to convince each other of the benefits of the model, limited by a specific domain in order to acquire this alignment. Gradually, the methods can be combined to provide an agent with multiple options to analyze another agents' model. In the long run, we intend to explore the interplay of the various alignment methods.

4.2. Arguing about Reputation

As deliberated earlier, reputation is the opinionized perspective of a person or an object. Oxford dictionary defines reputation to be the beliefs that are generally held about someone or something. Abdul Rahman et al. [2] define reputation as "an expectation about an agent's behavior based on information about its past behavior". Chang et al. [3] define reputation as "an aggregation of the recommendations from all of the third-party recommendations agents and their first, second and third hand opinions as well as the trustworthiness of the recommendation agent in giving correct recommendations to the trusting agent about the quality of the trusted agent". As discussed, we find out that, Trust is must needed element in human being to make love or better relationship with other human being, i.e., nothing can be operate without it (operable otherwise). Once you become trusted to someone, then you can be good for that user (in future). It is difficult to gain/maintain in case of product/organization but easy to lose. Actually, once if we lose trust among our family, it can be regained but it takes time. But if we lose our trust among any company/ corporation, it is hard to build. Once it is gone, it is difficult to recover/ build. Hence, this section provides and argues with trust and reputation models. Now next section concludes this work in brief.

5. Conclusions

Due to enhancement in Peer-to-Peer (P2P) ad hoc networking technology, Trust Mechanism has emerged to be the talk of the town. In a peer- to-peer system, trust worthiness and reputation identification play a vital role. The importance of these factors is increasing in peer-to-peer communication, since it can protect unreliable, malicious peer. Here we talked about these mechanisms in different context. And in each context different methods were used. That is there is no unique solution suitable for all scenarios. All type of constraints and input information has to be taken into account while implementing a new system. We find throughout this work, there is no single mechanism which suits for all scenarios. We have tried to showcase the different methods to identify the apt computation model to analyze the worth of the existing T&R systems across VANETs domains in this paper. Although there has been a significant number of works in T&R systems (refer table 1 and 2, in appendix A). As conclusion, a fair amount of work has been done in the area of computing reputation-based trust ratings but not sufficient according to human being's life. We need to focus in those issues and want to provide reliable experiences to human beings that no one has provided before.

Acknowledgement

This research work is funded by the Anumit Academy's Research and Innovation Network (AARIN), India. The authors would like to thank AARIN, India, a research network for supporting the project through its financial assistance.

Conflicts of Interests

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

References

[1] Amit Kumar Tyagi, N.Sreenath, "Never Trust Anyone: Trust-Privacy Trade-Offs in Vehicular Ad hoc Network", British Journal of Mathematics & Computer Science (BJMCS), Vol. 19, no. 6, 2016.

[2] A. Abdul-Rahman, S. Hailes, "Supporting Trust in Virtual Communities," Proc. 33rd Hawaii International Conference on System Sciences, 2000.

[3] Chang, E.,Dillon, T.,Hussain, F.K.,"Trust and Reputation for Service-Oriented Environments". Wiley, 2006.

[4] D. H. McKnight and N. L. Chervany, "What is Trust? A Conceptual Analysis and an Interdisciplinary Model", in Proceedings of AMCIS, 2000.

[5] D. McKnight and N. L. Chervany, "The Meanings of Trust." MISRC 96-04, University of Minnesota, Management Informations Systems Research Center, 1996.

[6] T. Grandison and M. Sloman,"A Survey of Trust in Internet Applications". IEEE Communications Surveys and Tutorials, 3, 2000.

[7] Zhang, J. "A survey on trust management for VANETs", In Proceedings of the 25thIEEE International Conference on Advanced Information

Networking and Applications, AINA 2011, Biopolis, Singapore, pp. 105–112, march 2011.
[8] Amit Kumar Tyagi, N. Sreenath, "Preserving Location Privacy in Location Based Services against Sybil Attacks", International Journal of Security and Its Applications (IJSIA), Vol.9, No.12, pp.189-210, December, 2015.
[9] M.K. Reiter and S.G. Stubblebine, "Toward acceptable metrics of authentication". In Proceedings of the 1997 IEEE Symposium on Research in Security and Privacy, Oakland, CA, 1997.
[10] Mauro Stocco, Thomas Engel, Uwe Roth, "Trust Arrays: Allowing P2P nodes to "personally" evaluate trustworthiness of potential partners", Advances in Intelligent Systems - Theory and Applications, In cooperation with the IEEE Computer Society, Luxembourg, November, pp. 15-18, 2004.
[11] F. Bao and I.R. Chen, Dynamic Trust Management for the Internet of Things Applications, International Workshop on Self-Aware Internet of Things, San Jose, USA, September, 2012.
[12] Yu, Bin Yu Bin Singh, M.P. Sycara, K."Developing Trust in Large-Scale Peer-to-Peer Systems",IEEE First Symposium on Multi-Agent Security and Survivability, 2004.
[13] Suryanarayana, G. Taylor, R.N. "A Survey of Trust Management and Resource Discovery Technologies in Peer-to-Peer Applications". Tech. rep. ISR, 2004.
[14] Bouvier M. "Maxims of Law", Law Dictionary, 1856.
[15] Kuwabara K. "Reputation: Signals or incentives?", In The annual meeting of the American sociological association, 2003.
[16] Patel, Nirav J Jhaveri, and Rutvij H, "Trust based approaches for secure routing in VANET: A Survey", International Conference on Advanced Computing Technologies and Applications, 2015.
[17] K. J. Hoffman, D. Zage, C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems", ACM Computing Surveys (CSUR), Vol. 42, no. 1.
[18] X. O. Wang, W. Cheng, P. Mohapatra, T. F. Abdelzaher, "Artsense: Anonymous reputation and trust in participatory sensing", in: INFO- COM, IEEE, pp. 2517–2525, 2013.
[19] Amit Kumar Tyagi, N. Sreenath, "Providing together Security, Location Privacy and Trust for moving objects", International Journal of Hybrid Information Technology (IJHIT) Vol.2, No.3, pp. 221-240, March, 2016.
[20] Amit Kumar Tyagi, N.Sreenath, "Providing Trust Enabled Services in Vehicular Cloud Computing (extended version)", in proceeding of ACM/International Conference on Informatics and Analytics (ICIA), pp. 25-26 August, Pondicherry, India, 2016. DOI: http://dx.doi.org/10.1145/2980258.2980263.
[21] Marti, S. and Garcia-Molina, H. "Taxonomy of trust: categorizing P2P reputation systems", Computer Networks, Vol. 50 No. 4, pp. 472-484, 2006.
[22] Sabater, Jordi Sierra, Carles, "Review on computational trust and reputation models", Artificial Intelligence Review, Springer, Vol. 24, Issue 1, pp 33-60,September 2005.
[23] Amit Kumar Tyagi, N. Sreenath, "Providing Safe, Secure and Trusted Communication among Vehicular Ad hoc Networks' Users: A Vision Paper", International Journal of Information Technology and Electrical Engineering, Vol. 5, Issue 1 February 2016.
[24] Schillo, M. Funk, P.&Rovatsos, M."Using trust for detecting deceptive agents in artificial societies", Applied Artificial Intelligence, Special Issue on Trust, Deception, and Fraud in Agent Societies, Vol. 14, no. 8, pp. 825-848, 2000.
[25] Sen, S.& Sajja, N."Robustness of reputation-based trust: Boolean case", In Castelfranchi, C.& Johnson, L.(eds.), Proceedings of the First International Joint Conference on Autonomous Agents and Multi-Agent Systems, Vol.1, pp. 288-293, 2002.
[26] Zacharia, G.&Maes, P. "Trust through reputation mechanisms", Applied Artificial Intelligence 14, pp.881–907, 2000.
[27] Brandt, F. "A verifiable bidder-resolved auction protocol", In Workshop on Deception, Fraud and Trust in Agent Societies, AAMAS, Bologna, Italy, pp.18–25, 2002.
[28] Yamagishi, T. Cook, K. & Watabe, M."Uncertainty, trust, and commitment formation in the United States and Japan", American Journal of Sociology, 104, pp. 165-194, 1998.
[29] Molm, L. D. Takahashi, N.& Peterson, G."Risk and trust in social exchange: an experimental test of a classical proposition", American Journal of Sociology 105, pp. 1396-1427, 2000.
[30] Sabater J. and Sierra C. "REGRET: a reputation model for gregarious societies". In 4th Workshop on Deception, Fraud and Trust in Peer Societies, 2001.
[31] Sarvapali D. Ramchurnet. al. "Trust in multi-agent systems", The Knowledge Engineering Review, Vol. 19, no. 1, pp. 1-25, Cambridge University Press,2004.
[32] Sabater, J.& Sierra, C."REGRET: a reputation model for gregarious societies", In Castelfranchi, C.&Johnson, L.(eds.), Proceedings of the 1stnternational Joint Conference on Autonomous Agents and Multi-Agent Systems, pp. 475-482 (Extended work of 2001), 2002.
[33] Yu, B.& Singh,M. P."An evidential model of reputation management", In Castelfranchi, C.& Johnson, L.(eds.), Proceedings of the 1st International Joint Conference on Autonomous Agents and Multi-Agent Systems, Vol. 1, pp. 295-300, 2002b.
[34] Zhou, R. and Hwang, K. "PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing", IEEE Transactions on Parallel and Distributed Systems, Vol. 18 No. 4, pp. 460-473, 2007.
[35] Kamvar, S. Schlosser, M. and Garcia-Molina, H. "The Eigen-Trust algorithm for reputation management in P2P networks", WWW03: Proceedings of the 12thinternational conference on World Wide Web, pp. 640-651, 2003.
[36] Xiong, L. and Liu, L. "PeerTrust: supporting reputation-based trust in peer-to-peer communities", IEEE Transactions on Knowledge and Data Engineering, Vol. 16 No. 7, pp. 843-857, 2004.
[37] Pinyol et al. I. Pinyol, J. Sabater-Mir, and P. Dellunde, "Cognitive social evaluations for multi-context bdi agents". In CCIA'08, 2008.
[38] Castelfranchi and Falcone, C. Castelfranchi and R. Falcone,"Trust Theory: A Socio-cognitive and Computational Model", Wiley, 2010.
[39] Go´mez, F. and Martı´nez, G. "Providing trust in wireless sensor networks using a bio-inspired technique", Telecommunications Systems Journal, Vol. 46, no. 2, 2010.
[40] Go´mez, F. and Martı´nez, G. "TRMSim-WSN, trust and reputation models simulator for wireless sensor networks", paper presented at IEEE ICC09: International Conference on Communications, 2009a.
[41] Anupam Das and Mohammad Mahfuzul Islam, "SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems", IEEE Transactions on Dependable And Secure Computing, Vol. 9, no. 2, March/April 2012.
[42] Yonghong Wang, Munindar P. Singh, "Evidence-Based Trust: A Mathematical Model Geared for Multiagent Systems," ACM Transactions on Autonomous and Adaptive Systems, Vol. 5, No. 3, pp. 1-25, September 2010.
[43] Justin Manweiler et al., "SMILE: Encounter-Based Trust for Mobile Social Services," CCS'09, November 9-13, Chicago, Illinois, USA, 2009.
[44] Heba A. Kurdi, "HonestPeer: An enhanced Eigen-Trust algorithm for reputation management in P2P systems," Journal of King Saud University-Computer and Information Sciences, 27, pp. 315-322, 2015.
[45] Marsh, S.P. "Formalising trust as a computational concept", PhD thesis, Department of Computing Science and Mathematics, University of Stirling, Stirling, 1994.
[46] Go´mez, F. and Martı´nez, G. "State of the art in trust and reputation models in P2P networks", in Shen, X. Yu, H. Buford, J. and Akon, M. (Eds), Handbook of Peer-to-Peer Networking, Springer, New York, NY, pp. 761-784, 2009b.
[47] Mui, L. "Computational models of trust and reputation: agents, evolutionary games, and social networks", PhD thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, 2002.
[48] Sun, Y.L. and Yang, Y. "Trust establishment in distributed networks: analysis and modelling", IEEE ICC07: International Conference on Communications, pp. 1266-1273, 2007.
[49] Lam, S.K. and Riedl, J. "Shilling recommender systems for fun and profit", WWW '04: Proceedings of the 13thInternational Conference on World Wide Web, 2004.
[50] Go´mez, F. and Martı´nez, G. "TRMSim-WSN, trust and reputation models simulator for wireless sensor networks", paper presented at IEEE ICC09: International Conference on Communications, 2009a.
[51] Moloney, S. "Simulation of a distributed recommendation system for pervasive networks", SAC05: Symposium on Applied Computing, pp. 1577-1581, 2005.
[52] Chen, X. Zhao, K. and Chu, X. "SepRep: a novel reputation evaluation model in peer-to-peer networks", Proceedings of the 5thInternational Conference on Autonomic and Trusted Computing, pp. 86-99, 2008.
[53] Wang, Y. Tao, Y. Yu, P. Xu, F. and Lu, J. "A trust evolution model for P2P networks", Proceedings of the 4thInternational Conference on Autonomic and Trusted Computing, pp. 216-225, 2007.
[54] Gui, C. Wu, Q. and Wang, H. "Towards trustworthy resource selection: a fuzzy reputation aggregation approach", Proceedings of the 4thInternational Conference on Autonomic and Trusted Computing, pp. 239-248, 2007.
[55] Gui, C. Wu, Q. Wang, H. and Qiang, J. "Towards trustworthiness establishment: a D-S evidence theory based scorer reliability tuned method

for dishonest feedback filtering", Proceedings of the 5thInternational Conference on Autonomic and Trusted Computing, pp. 444-454, 2008.
[56] Chen, R. Zhao, X. Tang, L. Hu, J. and Chen, Z. "CuboidTrust: a global reputation-based trust model in peer-to-peer networks", Proceedings of the 4th International Conference on Autonomic and Trusted Computing, pp. 203-215, 2007.
[57] Azzedin, F.Ridha, A. and Rizvi, A. "Fuzzy trust for peer-to-peer based systems", Proceedings of World Academy of Science, Engineering and Technology, Vol. 21, pp. 123-7, 2007.
[58] Hao Hu, Rongxing Lu, et al. "REPLACE: A Reliable Trust-based Platoon Service Recommendation Scheme in VANET", IEEE Transactions on Vehicular Technology, 2016.
[59] Serna, Jetzabel, Jesus Luna, and Manel Medina, "GeolocationBased Trust for Vanet's Privacy", In Information Assurance and Security, ISIAS'08, Fourth International Conference on, pp. 287-290. IEEE, 2008.
[60] LinkeGuo, Member, Chi Zhang et al., "A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks", IEEE Transactions on Dependable And Secure Computing, Vol. 12, no. 4, July/August 2015.
[61] Fe´ lix, Go´mez Ma´rmol et al., TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks", Journal of Network and Computer Applications 35, pp. 934–941, 2012.
[62] Huynh et al. et al., "An integrated trust and reputation model for open multi-agent systems". Journal of Autonomous Agents and Multi-Agent Systems, Vol. 13, no. 2, pp. 119-154, September 2006.
[63] B. Yu and M. P. Singh, "Detecting deception in reputation management", in Proceedings of the 2ndInternational Joint Conference on Autonomous Agents & Multiagent Systems, Melbourne, Australia, ACM, pp. 73-80, 2003.
[64] W. T. L. Teacy, J. Patel, N. R. Jennings, and M. Luck, "TRAVOS: Trust and reputation in the context of Inaccurate information sources, Autonomous Agents and Multi-Agent Systems", Vol. 12, no. 2, pp. 183-198, 2006.
[65] A. Jøsang, and R. Ismail, "The beta reputation system", in Proceedings of the 15th Bled Conference on electronic Commerce, Bled, Slovenia, 2002.
[66] Hong, Xiaoyan, Dijiang Huang, Mario Gerla, and Zhen Cao, "SAT: situation-aware trust architecture for vehicular networks", In Proceedings of the 3rdinternational workshop on Mobility in the evolving internet architecture, pp. 31-36, ACM, 2008.
[67] Wang, Zhou, and ChunxiaoChigan, "Countermeasure uncooperative behaviors with dynamic trust-token in VANETs", In Communications, ICC'07, IEEE International Conference on, pp. 3959-3964, IEEE, 2007.
[68] Biswas, Subir, JelenaMisic, and Vojislav Misic, "ID-based safety message authentication for security and trust in vehicular networks", In Distributed Computing Systems Workshops, 31st International Conference on, pp. 323-331. IEEE, 2011.
[69] Wei, Yu-Chih, and Yi-Ming Chen, "An efficient trust management system for balancing the safety and location privacy in VANETs", In Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11thInternational Conference on, pp. 393-400, IEEE, 2012.
[70] Amit Kumar Tyagi, N. Sreenath, "A Comparative Study on Privacy Preserving Techniques for Location Based Services", British Journal of Mathematics & Computer Science (BJMCS), Vol. 10, no. 4, pp. 1-25, Article no.BJMCS.16995, ISSN: 2231-0851, July 2015.
[71] Dhurandher, Sanjay K. et al., "Securing vehicular networks: a reputation and plausibility checks-based approach", In GLOBECOM Workshops (GC Workshops), IEEE, pp. 1550-1554, 2010.
[72] Gazdar, Tahani et al."Secure clustering scheme based keys management in VANETs", In Vehicular Technology Conference (VTC Spring), IEEE 73rd, pp- 1-5. IEEE, 2011.
[73] Ding, Qing, Xi Li, Ming Jiang, and XueHai Zhou, "Reputation-based trust model in vehicular ad hoc networks", In Wireless Communications and Signal Processing (WCSP), International Conference on, pp- 1-6, IEEE, 2010.
[74] Wang, Jian, Yanheng Liu, Xiaomin Liu, and Jing Zhang, "A trust propagation scheme in VANETs", In Intelligent Vehicles Symposium, IEEE, pp. 1067-1071, 2009.
[75] Serna, Jetzabel, Jesus Luna, and Manel Medina, "GeolocationBased Trust for Vanet's Privacy", In Information Assurance and Security, ISIAS'08, Fourth International Conference on, pp. 287-290. IEEE, 2008.
[76] Gazdar, Tahani, AbderrahimBenslimane, et al., A trust-based architecture for managing certificates in vehicular ad hoc networks", In Communications and Information Technology (ICCIT), International Conference on, pp.180-185,IEEE, 2012.
[77] Chen, Yi-Ming, and Yu-Chih Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs", Communications and Networks Journal, Vol. 15, no. 2 pp- 153-163, 2013.
[78] Chen, Chen, Jie Zhang, Robin Cohen, and Pin-Han Ho, "Secure and efficient trust opinion aggregation for vehicular adhoc networks", 72nd Conference Fall in Vehicular Technology (VTC 2010-Fall), pp. 1-5, IEEE, 2010.
[79] Sahoo, RashmiRanjan, Rameswar Panda, et al., "A trust based clustering with Ant Colony Routing in VANET", In Computing Communication & Networking Technologies (ICCCNT) Third International Conference on, pp. 1-8, IEEE, 2012.
[80] M. Raya, P. Papadimitratos, V. Gligor, and J. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in Proceedings ofIEEE Infocom, 2008.
[81] F. Dotzer, L. Fischer, and P. Magiera, "Vars: A vehicle ad-hoc network reputation system," in Proceedings of the IEEE International Symposiumon a World of Wireless, Mobile and Multimedia Networks, 2005.
[82] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in Proceedings of VANET, 2004.
[83] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," InternationalJournal of Computational Intelligence Theory and Practice (IJCITP), Vol. 5, no. 1, 2010.
[84] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust-based message propagation and evaluation framework in VANETs," in Proceedings of theInt. Conf. on Information Technology Convergence and Services, 2010.
[85] M. Gerlach, "Trust for vehicular applications," in Proceedings of the International Symposium on Autonomous Decentralized Systems, 2007.
[86] Patwardhan,A.; Joshi,A.; Finin, T.; Yesha, Y. "Adata intensive reputation management scheme for vehicular ad hoc networks", In Proceedings of the 3rdAnnual International ICST Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MOBIQUITOUS 2006, San Jose, CA,USA, pp. 1–8, 17-21 July 2006.
[87] F. Bao and I.R. Chen, "Trust Management for the Internet of Things and Its Application to Service Composition", IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, San Francisco, USA, pp. 1-6, June 2012.
[88] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang "TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things." Computer Science and Information Systems, Vol. 8, no. 4, pp. 1207-1228, 2011.
[89] F. Bao, I.R. Chen and J. Guo, "Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems", 11th International Symposium on Autonomous Decentralized System, Mexico City, Mexico, March 2013.
[90] Z. Chen, R. Ling, C.M. Huang and X. Zhu, "A scheme of access service recommendation for the Social Internet of Things," International Journal of Communication Systems, February 2015.
[91] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness Management in the Social Internet of Things," IEEE Transactions on Knowledge and Data Management, Vol. 26, no. 5, pp. 1253-1266, 2014.
[92] Y.B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," Computers and Security, 2014.
[93] I.R. Chen, J. Guo, F. Bao, "Trust Management for SOA-based IoT and Its Application to Service Composition", IEEE Transactions on Service Computing, 2015.

Appendix A

Table 1 Trust and Reputation Model Comparison (based on Proposed Model in [20])

Trust and /or Reputation model steps		**Selected Trust/or Reputation models**								
		BTRM-WSN [39]	**TRM Sim WSN [40]**	**EIGEN TRUST [35]**	**PEER TRUST [36]**	**POWER-TRUST [34]**	**SECURED TRUST [41]**	**EVIDENCE- TRUST [42]**	**SMILE-TRUST [43]**	**HONEST PEER [44]**
	Gather information	Ants leave pheromone trace during their expedition.		$C=\{c_{ij}\}$, is the matrix form built by a node.	Every client gathers responses from every other client to analyse their credibility Cr(v).	Each server i collects r_{ji} and v_j from each interacted client j	$F\ Cret\ n\ (p, q) = (1-ln(Simt\ n(p,q))/\ ln\ \theta$, *if* $Simt\ n(p, q) > \theta$ $=0$, *else*	$F_{p^1}{}^{p^2}f(p)dp.$	Number of recipients $= n/2^l = z \cdot k/(p \cdot (1-c)\ r \cdot d)$	
	Score and ranking	Every path is scored in the following manner: $Q(S_k)$.		Vector $\vec{t}_i(k)$ is computed for each node i	Every client Audits T(u) for each server-u.	Each server i, computes v_i		$c(r, s) = 0.5*f_0{}^l\ (x^r (1-x)^s / f_0{}^l\ (x^r(1-x)^s\ dx$	Overhead reception rate *(score)* $= z \cdot k/p \cdot (1-c) \cdot d) - r$	Score=*#(valid files received by good peers)/#(transactions attempted by good peers)*
	Entity selection	The highest quality path makes it to the top of the chart.		Probabilistic with probability $\frac{t_i}{\sum_j t_j}$	The server which satisfies $\max_u\{T(u)\}$ is chosen.	Server k with $max_k\{V_k\}$ is picked.				
	Transaction	The client computes her responses with the services obtained.		The client analyses her remarks with the reserved space.	The client analyses her remarks with the reserved space.	The client assesses her satisfaction with the received services.				
	Punish and reward	Pheromone evaporation		Not applicable	Not applicable	Not applicable	$DT^t{}_n\ (p, q) = Sat_n{}^t\ (p, q)$			

Note- Empty Space- Not Sure

Table 2 Review of Existing Trust and Reputation Model Literature

Category	Authors	Description
Trust and reputation management theory	Marsh (1994) [45]	The very first work related to this subject. It's a thesis bringing out bases of trust and reputation.
	Go´mez and Martı´nez (2009b) [46]	This work is mainly related to the P2P networks and doesn't implement any model or provide any surveyed comparison.
	Mui (2002) [47]	An age old work in the same field related to multi-agent systems.
	Sun and Yang (2007) [48]	An amazing piece of work formalizing the perspectives of trust and reputation management.
	Lam and Riedl (2004) [49]	The work takes us through the vulnerabilities based on the recommendation systems.
	Go´mez and Martı´nez (2009a) [50]	This paper portrays the security threats in the trust and reputation systems along with ways to overcome them.
	Marti and Garcia- Molina (2006) [21]	This work defines the general steps to be kept in mind in P2P networks.
Trust and reputation models simulation frameworks	Moloney (2005) [51]	A paper which portrays the simulations of a simple recommendation system for persistent networks.
	Go´mez and Martı´nez (2009a) [50]	It describes about the open source models like TRMSim-WSN.
Trust and/or reputation models	Chen et al. (2008) [52]	It talks about the reputation models for a P2P network.
	Wang et al. (2007) [53]	This paper puts forth a trusted model for P2P networks considering the direct experiences.

	Kamvar et al. (2003) [35]	Aiming to develop P2P network, this paper has proposed EigenTrust which is the highly used model.
	Go´mez and Martı´nez (2010) [39]	BTRM-WSN is a part of the paper, which is a rare piece making use of ant colony system to handle trust and reputation in wireless networks.
	Gui et al. (2007) [54]	This work proposes an aggregate of the reputation by using fuzzy sets and logics.
	Gui et al. (2008) [55]	It shows methods for filtering of dishonest and malicious feedbacks using Dempster-Shafer theory.
	Xiong and Liu (2004) [36]	One of the highly cited papers, it's based on peer trust in P2P networks in the field of e-commerce systems and gives two ways in the form of credibility measures. It also satisfies community context factors in trust measurement, employing a camouflaging design for the peer location. It supports a single-rating system.
	Chen et al. (2007) [56]	CuboidTrust is portrayed in this paper which is handy for P2P networks. It build strong bonds and ties between contribution, trustworthiness and qulity of resources, applying power to analyse the global trust value of each peer.
	Zhou and Hwang (2007) [34]	PowerTrust is presented in this paper and is considered to be an enhancement of EigenTrust receiving international attention.
	Azzedin et al. (2007) [57]	This paper uses uncertain logics and reasonings to handle ambiguous details of trust in P2P networks.
	Abdul-Rahman and Hailes (2000) [2]	It is one of the first few works and describes the general properties of trust and reputation systems.
	TassosDimitriou, et al., (2007) [58]	SuperTrust, which is not a centralised approach, is based on K-redundant peer networks and guarantees a complementary support to the proposed models for developing trust.
	Hao Hu,RongxingLu , et al., (2016) [58]	REPLACE, a reputation system, has been designed for the team headed vehicles by gathering and prototyping the users' feedback. This is a scure and sound method against frequent attacks, belittling, etc.
	Anupam Das, Mohammad Mahfuzul Islam (2012) [41]	SecuredTrust, which identifies the malicious alterations in behavior along with striking a balance of work among the service providers is introduced here. It keeps in mind a variety of factors to determine the trust of an individual like similarities, feedback and responses, previous trust issues, etc. and hence remains more effective amidst a large number of agents.
	Jetzabel Serna, Jesus Luna and Manel Medina (2009) [59]	Geolocation-Based Trust passes on the details related to a vehicles' location.
	LinkeGuo, Member, Chi Zhang et al., (2015) [60]	This paper, introduces a new field, i.e., trust with privacy. It's a trust-based privacy preserving friend recommendation scheme for OSN's. The OSN users use their traits to identify matching peers so as to develop a social relationship with the unknown through a trust-chain.
	Fe´ lix Go´mezMa´rmol et al., (2012) [61]	TRIP, a quick, scalable model, is used for resolving on whether to accept a traffic input dropped in by another vehicle or not by analysing the loyal nature of the issuer of the message.
	Xinlei, Wei Cheng, et. al (2014), [33]	ARTSense is a skeletonised system to overcome the issue of trust without identity in mobile sensing. There's no need for the presence of a trusted third party and both positive and negative reputational messages can be applied. a framework to solve the problem of "trust without identity" in mobile sensing. In this, no require of trusted third party and both positive and negative reputation updates can be enforced.
	(T.D Huynh, N.R. Jennings, N.R.Shadbolt, 2006)[62]	FIRE focuses on the multi-agent system with the help of four information reservoirs and deals with the problems of freshers and eradicates the unnecessary details along with distinguishing between dishonest and mistaken agents. It also provides reliability measures by using an overrated rating system approach to complement MAS.
	(JordiSabater and Carles Sierra, 2002) [19]	REGRET is meant for sophisticated e-commerce platforms and is into the development of sociogram and modelized social relationships. It complements system reputation and provides a huge dimension to bring together different perspectives of behavior in terms of reputation. It evaluates honesty through unambiguous rules and provides a measure of reliability to employ an advanced rating system.
	(B. Yu, M.P. Singh,2003) [63]	This work is highly useful for the MAS (multi-agent system) as it provided novel trust and reputed network and is capable of identifying three models of description. It helps in distinction of agents who have good or no reputation at all with the Dempster-Shafter theory and it highly suffices dynamism in MAS.
	(W. T. L. Teacy, J. Patel, et al,2006) [64]	TRAVOS has been created for a huge scale open system, providing two sources for information. It takes good advantage of the probabilistic approach to obtain the credibility of the witnesses and provides confidence and reliability measures for apt conversations between the information sources. It makes use of a single rating system.
	(A.Jøsang,, 2002) [65]	Beta Reputation System (BRS), which is highly advised for a dynamic surrounding, supports binomial rating systems and comprehends the bootstrapping issues by keeping in mind the quality of the society in the marketplace, provide repeated filtration algorithms which is capable of unveiling malicious intentions if majority of the participants act loyally, exploit the longevity factor to discount the ratings with time, allow participants to fluctuate their mannerisms to increase their own profits.

Table 3 Summary of Trust Establishment Techniques in VANETs

Topic Name	Description	Mechanism / Algorithm	Methodology	QoS / Performance
SAT: Situation-Aware Trust architecture for vehicular Networks [66]	It's the middle layer forming a strong relation among the nodes consisting of SAT and STL.	SAT architecture (Situation-Awareness Trust)	Developing trust which revolves around cryptographic methods like data integrity and authentication.	Managing policy, trust improvement, Social network
Analyzing the credibility of the guards in VANETs [6] for safety.	Watchdogs keep an eye on the neighboring nodes and observe the behavioral values.	Watchdog algorithm with intrusion detection	Neighboring nodes carry on the packets forward and guard the nodes.	Detection potential, false negative and false positive
Counter the Unacceptable behaviors with dynamic trust-token in VANETs [67]	DTT puts forth a carefully calculated trust at real time functioning of the node spontaneously	Dynamic Trust-Token (DTT)	A variety of Symmetric and asymmetric cryptographic methods for veracity and watchdog is used for creating trust tokens.	Protect packet integrity, potential degradation
ID-based safety message authorization for safety in Vehicular Networks [68]	ECDSA is useful for the RSU unit authorization and for verification purpose	ID-based proxy signature and ECDSA	For message authentication and trust control, certificates are made less public.	Message transfer with authentication throw trusted RSU
A structured and systematic trust management system for maintain safety and location privacy in VANETs [69, 70]	RSU makes an instantaneous decision to identify the trust worthiness of the message being sent by the vehicle and it also prevents internal attacks.	Road-side unit (RSU) and Beacon-Based Trust System (RABTM)	Event-based trust systems are used for developing trust and beacon message and event message to govern the value of trust for that event.	Safety and location privacy of vehicles
TRIP, a trust and reputation Infrastructure based proposal for vehicular ad hoc networks [61]	Predict the destructive and harmful nodes which are likely to broadcast unwanted data. This is achieved by developing an update in the central database in a recurring fashion.	Trust and Reputation Infrastructure based Proposal (TRIP)	Anomalous sets divide trust and categorized servity of past trust	Recognizing spoilt and destructive nodes which spread false details.
Securing vehicular networks: a reputation and possibility checks-based approach [71]	Opinion generation, opinion piggybacking and provision of node reputation which can be trusted or not. False message creation identifies with PVM.	Vehicular Security produces Reputation and Plausibility check (VSRP), VARs algorithm	VARs algorithm showcases indirect and direct trust, reputation-based algorithm	Event Modification, false event production, data aggregation and data Dropping
Secure clustering scheme-based keys management in VANETs [72]	VDDZ popularises filter certificate request which is provided by CA in the group and protects direct interaction and destroys attacks.	VANET Dynamic Demilitarized Zone (VDDZ)	Divide cluster head (CH) of neighbor node and Registration authority (RA) provides the confidence to neighbors	Prevent destructive and anomalous vehicles within cluster
Reputation-based trust model in vehicular ad hoc Networks [73]	All vehicles come across same traffic issues and differentiate the roles occurred in the event.	Event based reputation algorithm	Random way point scheme to adopt for identify bogus information	Filter bogus and false warning message, enhance trust
A trust propagation scheme in VANETs [74]	Creating a serene relation between the past and current trust status, analyzing trust on the grounds of attributes and processing the similarity between the two nodes.	Novel scheme for enhancing trust management	Attributes comparison with trust value	Enhancing trust propagation, reliable packet delivery
Geolocation-Based Trust for VANET's Privacy [75]	Strict access management provides trust verification among nodes. New techniques result in valid trust geographical areas.	Geolocation based establishment	Pseudonyms used for privacy and MAC trusted location	Privacy mechanism
A trust-based architecture for managing certificates in vehicular ad hoc networks [76]	Certificate authority (CA) provides authorization legitimately to vehicles and uncertain distinguee honest node and clusters broadcasts the trust values to its neighbors.	Fuzzy algorithm, Certification Authority (CA)	Fuzzy based solution and certificate authority (CA) and PKI scheme	CA within cluster only Co-operation with vehicles and legitimate broadcast data
A beacon-based trust management system for advancing user centered location privacy in VANETs [77]	BTM generates and verifies the position of the vehicles and its direction. Message transmission is used for cryptography and pseudo identity scheme	Beacon-based Trust Management (BTM), Dempster Shafer evidence	Beacon establishes trust relationships, FSP and RSP along with location privacy enhancement scheme	internal attacks, bogus message and privacy enhancement

Secure and efficient trust opinion aggregation for vehicular ad hoc networks [78]	A mixture of a lot of message signs into a single one is forwarded to the vehicle	Identity based Aggregate algorithm	Trust opinion aggregate scheme	Space efficiency and time complexity
A trust-based clustering with Ant Colony Routing in VANET [79]	CH roots the networks in a group and calculates the indirect trust on the nodes	Trust dependent Ant Colony Routing (TACR), Mobility aware Ant Colony Optimization Routing (MARDYMO)	MAR-DYMO used for routing overhead in the network. CH calculates the indirect trust value, MAR-DYMO, for optimized routing technique	Scalability, real time updated position and trust value of vehicles

Table 4 Properties of the Existing (Some) Trust Model for VANETs

Approaches	Raya et al. 2008 [80]	Dotzer et al. 2005 [81]	Golle et al. 2004 [82]	Minhas et al. 2010b [83]	Chen el al. 2010 b [84]	Gerlach 2007 [85]	Pawardhan et al. 2006 [86]	Fe´ lix Go´mezMa´rmol et al. 2012 [61]	Hao Hu, et al. 2016 [58]
Decentralized	Y	Y	Y	Y	Y		Y	Y	Y
Sparsity			Y	Y	Y	Y	Y		
Dynamics	Y	Y		Y	Y	Y	Y		
Scalability				Y	Y				Y
Confidence	Y			Y	Y	Y			
Security	Y		Y	Y	Y	Y	Y	Y	
Privacy		Y	Y	Y		Y			
Robustness			Y						

Note:Y-Yes, Empty Space - Not Sure