International Journal of Grid and Distributed Computing
Vol. 9, No. 4 (2016), pp.325-334
http://dx.doi.org/10.14257/ijgdc.2016.9.4.29

A Review on Trust Model in Vehicular Ad Hoc Network

Pallavi Agarwal[1] and Neha Bhardwaj[2]

[1]Research Scholar, CSE & IT Dept., Madhav Institute of Technology & Science, Gwalior, India
[2]Assistant Professor, CSE & IT Dept., Madhav Institute of Technology & Science, Gwalior, India
[1]pallaviagarwal015@gmail.com, [2]bhardwaj.neha08@gmail.com

Abstract

In vehicular ad hoc network (VANETs), the applications mainly focused on the road and making their journey safe and comfortable to fulfill the users' requirements. It is a challenging subclass of Mobile Ad-hoc Network, which empowers smart transmission among vehicles and between vehicles and roadside frameworks. It is an optimistic methodology for the Intelligent Transport System (ITS). There are numerous difficulties to be tended while utilizing VANET. It is flexible and has a high dynamic topology and flexibility which makes the conventional MANET protocols unacceptable for VANET. Trust is a principal element which is used to create a trustful environment to improve the security in vehicular networks. Trust can be calculated by observing the human behavior which creates a trusted communicating environment. In this paper, we define the architecture of VANET, then the communication establishment and various challenges. Some trust models had been defined in this paper to enforce honest information sharing between communicating nodes. Trust establishment is compulsory among communicating vehicles to build a secure messages exchange and reliability.

***Keywords**: VANET, V2V, V2I, Challenges, Trust models, Security*

1. Introduction

Vehicular ad-hoc network (VANET) is a newly emerged technology, which is utilized to set up a communication among the vehicles. It provides the communication among vehicles to vehicles and vehicles to roadside units within the short range of 100 to 300 m. In a VANET every node communicates by sharing data of traffic jam and accidental alerts while driving. It put an extra effort to enhance the condition of road related system like collision detection & avoidance, traffic visibility system, message sharing and crash reporting, all these bodily functions must be done safely. The primary intention of made system is to satisfy reliable delivery of the entire message among the nodes (vehicles). Vehicles should follow traffic pattern and road limit to avoid accident. The malicious node can create many problems which can generate false messages like wrong information of traffic jam and an accident.

2. Architecture of VANET

Current vehicles are frequently planned as LAN, with the capacity to unite different implanted PCs, which can impart among themselves and in addition with different vehicles by means of various remote associations. The VANET is accordingly being utilized as a part of numerous business applications like giving efficient direction of data to alternate vehicles, advising the drivers about the activity conditions, mischance, street conditions, *etc*. For this reason the VANET utilizes sensor gadgets to monitor the network conditions, for example, vibration, weight, movement, temperature and sound. Each

ISSN: 2005-4262 IJGDC

sensor is prepared for social event huge information and transmits the data to others. These sensor devices are very little, ease and can be sent in a substantial number on the network. In VANET, such type of radio communication vehicles to vehicles is complex [1].

The two main reasons are:

1. The atmosphere in which the vehicles move has numerous radio reflective surfaces.
2. Vehicles go at a high range of speeds, bringing about disturbance of radio communication.

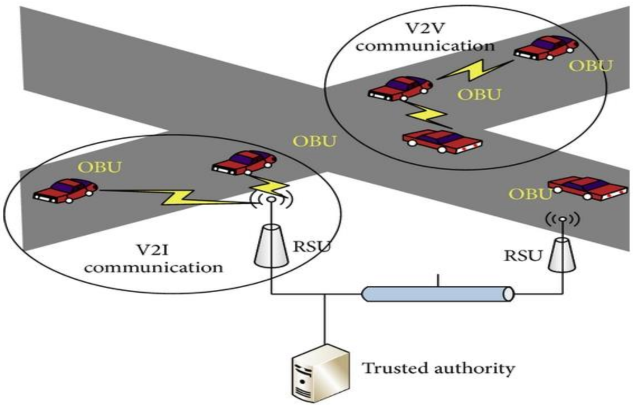

Figure 1. Architecture of VANET

VANETs consist of Road-Side unit (RSU), On-Board unit (OBU) and Trusted Authority (TA). RSU is based on infrastructure which is fixed node and all the messages are transferred by the RSU to all the vehicles within its range. It also helps the vehicles to connect to the internet. OBU is a sensor which is located in the vehicles to collect all the data from the surroundings. Its main function includes reliable message transfer and routing information. Trusted Authority is a third party which provides security to the network. Certificate authority provides the keys and certificates to the vehicles or RSUs and authenticates the vehicles for the secure communication. All the messages are encrypted with the keys provide which is generated by the TA and also identify an attack performed.

2.1. Communication

Basically, in VANET vehicular communication are three types:

2.1.1. Vehicle-to-Vehicle Communication (V2V): In V2V, vehicles can communicate to exchange the information within the range. It includes the information regarding the number of people in vehicles, steering angle, brake status, speed and vehicle’s position. There is no need of any roadside unit and allow vehicles to communicate directly.

2.1.2. Vehicle-to-Infrastructure Communication (V2I): In V2I, vehicles can communicate with the roadside unit which is fixed. RSU is placed within the specified range at the corner of the road and enables higher data rates. RSU is connected to the internet which provides various facilities related to the entertainment.

2.1.3. Infrastructure-to-Infrastructure Communication (I2I): In I2I or Hybrid communication, it offers communication between RSUs or RSU and Base Stations. It mainly increases the communication range and connects all the vehicles in the network [2] [3].

2.2. Roles of Vehicle

There are different roles that are played by the vehicles:

2.2.1. Event reporter (ER): The vehicle senses the surrounding and then transmits the alarm messages to other neighboring vehicles. It should be trustful, so that every vehicle can trust them.

2.2.2. Event Observer (EO): The behavior of the event messages of ER is observed by the vehicles within one hop.

2.2.3. Event Participant (EP): All the vehicles beyond one hop of an event reporter can receive and forward the event messages. The behavior of the event participants are not possible to identify.

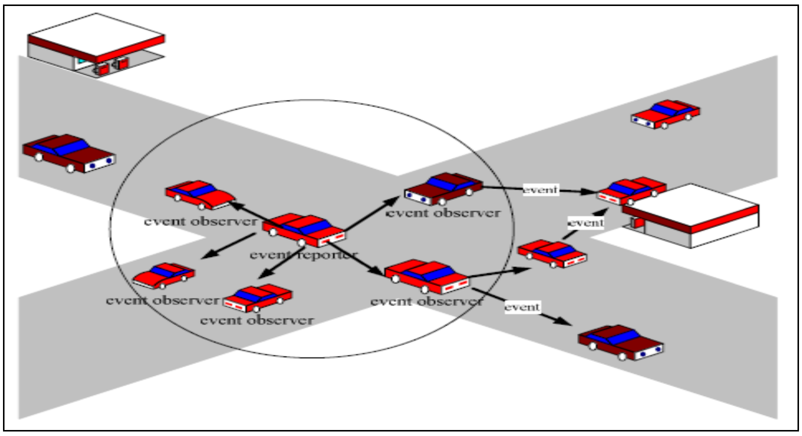

Figure 2. Role of Vehicles

3. Challenges in VANET

There are numerous difficulties that should be tended to while making such system. One of the difficulties confronting unarranged systems is the topology of the system changes quickly. Vehicles in a VANET have a high level of versatility. The average time of direct communication of two vehicles is approximately one minute. Another drawback restricting the widespread adoption of ad hoc networks is many of the protocols used for 802.11 are centralized and new distributed algorithms must be developed.

The 802.11 standard provides a limited ad hoc mode with the independent basic service set (IBS) configuration but it is sufficient for vehicular ad hoc networks. Furthermore, wireless communication is unreliable. The error rate in a wireless network is much higher than Ethernet. All of the issues make implementing a VANET difficult. Although the attributes of VANET recognize it a different network, however a few qualities forces a few difficulties to convey the VANET [4].

3.2. Technical Challenges

The technical difficulties manage with the technical snags which should to be determined before the deployment of VANET. A few difficulties are given below:

Network Management: The network topology and channel condition change quickly due to high mobility. Because of this, we cannot set up and manage the structure as quickly as the topology change. It also makes difficult to predict the vehicle's location.

Congestion and Collision Control: The unlimited size of a network creates a major challenge. In rural area, the traffic load is low and also at night in the rural area. Because of this, the network segments as often as possible happens while in surge hours the activity burden is high and thus the network is congested and a collision happens in the network.

Environmental Impact: VANETs use the electromagnetic waves for transferring the messages from one to another. These waves are controlled by the earth. Hence the environmental impact must be examined to deploy the VANET.

MAC Design: VANET for the most part utilize the shared medium to convey hence the MAC outline is the key issue. Numerous methodologies have been given like TDMA, SDMA, and CSMA and so on. IEEE 802.11 embraced the CSMA based Mac for VANET.

Decentralized: The network has no centralized infrastructure and the vehicles can enter or exit the network at any time. There are also less possibilities of not interacting with the previous vehicles in future again.

Cost: New communication standards have been introduced for the vehicular communication. It requires extra hardware modules on vehicles which increase the cost for the consumers.

Security: As VANET gives the road safety applications which is life basic in this manner security of these messages must be fulfilled.

3.3. Social and Economic Challenges:

Apart from the technical difficulties to convey the VANET, social and economic challenges should to be considered. It is hard to persuade producers to fabricate a system that passes on the activity signal infringement on the grounds that a purchaser may reject such kind of checking. Then again, purchaser values the notification message of a police trap. So to persuade the maker to convey VANET will get short incentive.

3.4. Security in VANET:

VANET must fulfill some security prerequisites before they are transferred. A security system in VANET should fulfill the following necessary condition [5]:

Authentication: Authentication guarantees that the message is produced by the honest to legitimate client. In VANET a vehicle responds upon the information originated from the other vehicle consequently authentication must be fulfilled.

Availability: Availability obliges that the data must be accessible to the real clients. It blocked the entire network to affect the services. DOS Attacks can cut down the network and hence information can't be shared.

Non-Repudiation: Non-repudiation implies a node can't deny that he/she doesn't transmit the message. It might be pivotal to focus the right arrangement in accident reproduction.

Privacy: The privacy of a node against the unauthorized node should be ensured. This is obliged to eliminate the message delay attack.

Data Verification: A generally confirmation of data is obliged to take out the false messaging.

4. Applications in VANET

The aim of VANET is to improve driving experience and the safety of transportation. By frequently broadcasting and receiving messages, vehicles are aware of their surrounding road situations. The drivers can react to events happen on the road by these messages in advance. Even in some urgent cases, the OBU can make the decision (stop or change the lane) automatic. There are many applications used in VANET, which are mainly classified into two parts: safety-related and user application.

4.1. Safety-Related Applications

This type of application can significantly decrease the number of accidents. Normally, vehicles travel at very high speed, especially on the highways. Drivers have very short time to react to the car crashes in front. If an accident occurs, then the vehicles behind it often crash before they stop on the highway. Safety applications should give warning to drivers in advance, so that they can change the lanes or stop, thus avoiding accidents. The application should supply driver, the road situation and choose the best path for the driver. This could prevent road congestion, saving people’s time and fuel consumption. It can be noticed that the security for this type of application is mandatory; even a tiny mistake can cause serious consequences.

4.2. User Applications

User application provides drivers with information (*e.g.*, gas station), online-payment, entertainments and advertisements. For instance, if a driver wants to know the location of the cheapest price gas station, he/she can get the information by sending a request to the nearby RSU. After receiving this request, RSU checks from Internet and echoes it to the vehicle. Security is also required but not as much important as in safety-related application.

5. Trust

Trust is the key element in creating a trusted vehicular environment which promotes security in vehicular networks. Trust is either in human behavior or in the deployed hardware, where both form a trusted communicating environment. Few trust models had been introduced to enforce honest information sharing between communicating nodes [8] [6]. Current trust management schemes for VANETs establish trust by voting on the reports received. This is time consuming for time critical applications and not practical in real life especially in dense areas.

5.1. Trust Models in VANET

As shown in Figure 3, [6] there are three main trust models: entity-oriented trust models, data-oriented trust models, combined trust models.

Entity-oriented trust models focus on the trustworthiness of peers. It is divided into sociological trust model and multifaceted trust management model. The sociological trust model is based on the principle of trust and confidence tagging. 1) Situational trust depends on the node's situation. 2) Dispositional trust is the peer’s own beliefs. 3) System trust depends on the system security level. 4) Belief formation process is the evaluation of data based on the previous factors. The multi-faceted trust management model allows vehicles to inquire the event by requesting other entities. 1) Role based trust depends on the role a node plays in society, *e.g*. police car. It gives higher priority to vehicles which is having lower roles. 2) Experience-based trust is built between nodes after several interactions. 3) Priority based trust gives a higher priority to vehicles with a higher experience value.

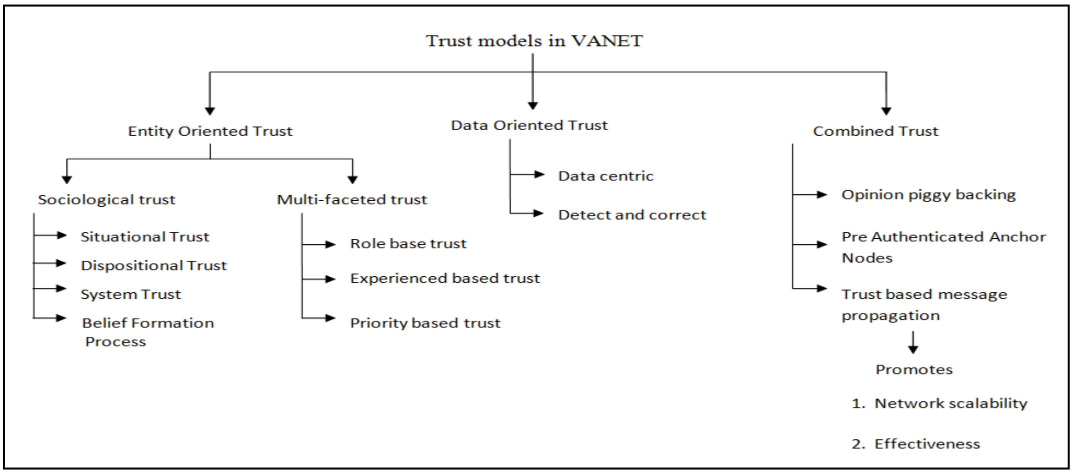

Figure 3. Trust Models in VANET

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. 1) Data-centric trust establishment evaluates the trustworthiness of the reported data rather than the trust of the entities. 2) Detect and correct is based on detecting and correcting the malicious data in VANETs.

Combined trust models make use of the node's trust to evaluate the trustworthiness of data, where node's trust is maintained by them. 1) Opinion piggybacking is when each node appends its opinion to the message before forwarding it. 2) Pre Authenticated anchor nodes are previously predefined nodes and are regarded as trustworthy. 3) Trust-based message propagation and evaluation framework in vehicular ad-hoc networks [8], is when nodes share information regarding road condition or safety messages and others provide their opinions.

6. Literature Survey

Jorge h. *et al.* [9], proposed a watch dog algorithm with an interruption identification system for building the trust administration. In that source node sends messages to the neighbor's node and shows that node with ids. It forwards those messages and keeps its trust value in trust table generally that diminishing trust estimation of that node. The disadvantage of this strategy is to make crash in the system, and show that node until that forward or drop. It has contained the huge checking history of the neighbor's node in the event that it has expanded the number of neighbor nodes.

Cong. *et al.* [11], proposed Crowed sourcing capacities which take into account occurrence reports in V2V correspondence and forward to those vehicles. It is used in assessing the dependability value for vehicles. Worldwide perspective can telecast for the individual vehicles trust value in CSC. Future work incorporates security, protection and overhead issues.

Subir b. *et al.* [10], proposed an id-based proxy signature techniques by using ECDSA for security. An ID-based technique offers a verification of a certificate-less public key, while a proxy signature provides message authentication flexibilities. This strategy is good for authentication and trust management in VANET which is highly dynamic and untrustworthy as it is able to avoid potential security threats.

Tahani g. *et al*. [12], proposed a Markov chain model for setting up trust administration. This model considers not just the conduct of hub in the element trust metric yet that screenings all imperatives movement of that hub. Every vehicle regarded as checking upgrading trust metric tables of its neighbor nodes has a place that conduct. Making trouble and childish vehicles related to this system. It utilizes time interim and number of moves with different hubs in trust administration. This framework utilizes stretch and a trust, an advanced framework for trust model. In this worldwide trust ought not be set up which is future extent of this component.

Yu-Chih w. *et al*. [13], proposed roadside unit (RSU) and guide based trust administration framework to enhance well being and security area. This procedures maxim is a speedy message conclusion and keep sending and sending from the inner vindictive hub. This method takes choice rapidly and gives supposition in less time. The downside of this system is not ready to contrast, trust, esteem and another node.

Felix g. *et al*. [14], proposed a view of TRIP (Trust and Reputation base based proposition) calculation for activity dissecting. TRIP distinguishes malevolent and childish hub, which spreading fake or false data in the system. The message and movement are cautioning message sent to another hub that checks notoriety and reliable estimation of that hub. On the off chance that hub is noxious than reject and drop bundles from those hubs/autos. Fluffy rationale arranges and sorts trust esteem according to operational and commercial messages. Notoriety score is registers with three information's: past experience, encompassing vehicles and suggestion of the focal power. Three sorts of trust qualities: Not trust-dismiss all bundles, +/ - trust-acknowledge yet not forward and trusted-acknowledge and forward. The disadvantage of this instrument is difficult to keep up trust esteem and the conduct of hub and we can't recognize the hub is straightforward or vindictive.

Qing d. *et al*. [15], proposed repudiation based filtering model for bogus messages. The role based notoriety component is utilized to decide approaching message is critical and dependable to the drivers/autos. It improves trust for vehicular system. This method incorporates arbitrary way point which is not an adequate strategy for notoriety. In future we can infer fluffy rationale for figuring notoriety esteem for an occasion.

Tahani g. *et al*. [16], proposed hybrid trust model for decides trust metric. Two terms utilized for checking trust: participation with different vehicles in the system and telecast true blue information. Fluffy based calculation used to choose the genuineness of vehicles and sift through vindictive vehicles. One trusted neighbor to issue CA in the PKI is disseminated among number of vehicles. Reliable quality is ascertained through checking helpfulness of screen vehicles and forward computed trust to neighbor vehicles.

Yi-Ming c. *et al*. [17], proposed Beacon-based trust administration (BTM) systems keep the inside aggressors from sending false or fake messages in protection upgrade in the system. Secure reference point based trust convention is utilized to assess immediate and backhanded trust administration plan. Direct trust in dependability esteem and round about trust sentiment transmitted from various vehicles. Dempster Shafer proof hypothesis are utilized for numerical calculation.

Chaung *et al*. [18], the first mistrustful node becomes trustful and authenticated, it obtains the sufficient authorized parameter, so it can authorize other mistrustful nodes. The problem is, if an adversary node was authenticated as trustful, it may misuse this trust gained to authorize and authenticate other misbehaving nodes. A user is allowed more than one identity in the network.

Sumra *et al*. [19], states that if trusted node A communicates with node B safely, then node B becomes trusted. Thus it provides chain of trust between the communicating groups of nodes. The drawback of this protocol is the first communicating node with the new comer node will always be the victim. Moreover, in vehicular environment nodes are highly dynamic, continuously leaving a group and joining a new group. Thus a malicious node can join a new group that has no idea about its bad history and deceive nodes in this new group.

Sumra *et al*. [20], it depends on a 16 digit secret code to ensure a secure key renewal. The main drawback of this solution occurs at the entry point where client and service provider authentication task is performed, the channel could be congested when the number of users increases, *e.g.* in a highway.

Kapil *et al*. [21], proposed a trust based scheme for location finding in VANETs using DST. The technique is able to evaluate the trust based location finding when evidence is less. The simulation and results show that the proposed work can effectively find the trustworthy location. It proved the efficacy of the proposed scheme and makes it attractive and viable for VANET. Future work aims to perform experiments to evaluate its performance in other message categories in a realistic environment for VANET.

Ming *et al*. [22] in this paper proposed a decentralized lightweight authentication scheme called TEAM to protect valid users in VANETs from malicious attacks. The amount of cryptographic calculation under TEAM was substantially less than in existing schemes because it only used an XOR operation and a hash function. Moreover, TEAM is based on the concept of transitive trust relationships to improve the performance of the authentication procedure. In addition, TEAM has a few storage spaces to store the authentication parameters.

7. Conclusion

In Vehicular Ad Hoc Networks (VANET), trust establishment among communicating vehicles is important to be built to secure messages exchange and reliability. We clearly presented an application of VANET and identify the many challenges in this environment. It is very dynamic network so it is vulnerable to attacks which should be taken into consideration in the security section. In this survey, we mention some existing trust models for different contexts, and point out their issues when being taken to the VANET domain. We present a list of important properties that should be archived by trust management for VANET, setting a specific outcome for researchers in this area.

References

[1] Dzmitry Kliazovich, Michael Devetsikiotis and FabrizioGranelli, “Networking and Telecommunications: Concepts, Methodologies, Tools, and Applications”, **(2010),** pp. 410-436.

[2] K. Tanuja, T.M. Sushma, M.Bharthi, K.H. Arun, “A Survey on VANET technologies”, International journal of computer applications, vol. 121, **(2015)** July.

[3] Hannes Hartenstein, “A Tutorial Survey on Vehicular Ad Hoc Networks”, IEEE Communication Magazine, **(2008)** June, pp. 164-171.

[4] Maxim Raya, “The Security of Vehicular Ad Hoc Networks”, SASN, Alexandria, Verginia, USA, **(2005)** November 7, pp. 11-21.

[5] Ram Shringar Raw, Manish Kumar, Nanhay Singh, “Security challenges, issues and their solutions for VANET”, International Journal of Network Security & Its Applications (IJNSA), vol.5, **(2013)** September.

[6] J. Zhang, “A survey on trust management for VANETs”, International Conference on Advanced Information Networking and Applications, **(2011)**, pp. 105-112.

[7] C. Chen, J. Zhang, R. Cohen, and P. Han Ho, “A trust-based message propagation and evaluation framework in VANETs”, International Conference on Information Technology Convergence and Services, **(2010)**.

[8] J. Zhang, “Trust management for VANETs: challenges, desired properties and future directions”, International Journal of Distributed Systems and Technologies, **(2012)**, pp. 48-62.

[9] Hortelano, Jorge, Juan Carlos Ruiz, and Pietro Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs", Communications Workshops (ICC), IEEE International Conference, **(2010),** pp. 1-5.

[10] Biswas, Subir, JelenaMisic, and Vojislav Misic, "ID-based safety message authentication for security and trust in vehicular networks", 31st International Conference on Distributed Computing Systems Workshops (ICDCSW), IEEE, **(2011),** pp. 323-331.

[11] Liao, Cong, Jian Chang, Insup Lee and Krishna K. Venkatasubramanian, "A trust model for vehicular network-based incident reports", Wireless Vehicular Communications (WiVeC), IEEE 5th International Symposium on IEEE, **(2013),** pp. 1-5.

[12] Gazdar, Tahani, AbderrezakRachedi, AbderrahimBenslimane, and AbdelfettahBelghith, "A distributed advanced analytical trust model for VANETs", Global Communications Conference (GLOBECOM), IEEE, **(2012),** pp- 201-206.

[13] Wei, Yu-Chih, and Yi-Ming Chen, "An efficient trust management system for balancing the safety and location privacy in VANETs", Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th International Conference, **(2012),** pp. 393-400.

[14] Gómez Mármol, Félix, and Gregorio Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for Vehicular ad hoc networks", Journal of Network and Computer Applications, Springer, **(2012),** pp- 934-941.

[15] Ding, Qing, Xi Li, Ming Jiang, and XueHai Zhou, "Reputation-based trust model in Vehicular ad hoc networks", Wireless Communications and Signal Processing (WCSP), International Conference on IEEE, **(2010),** pp. 1-6.

[16] Gazdar, Tahani, AbderrahimBenslimane, AbderrezakRachedi, and AbdelfettahBelghith, "A trust-based architecture for managing certificates in Vehicular ad hoc networks", International Conference on Communications and Information Technology (ICCIT), IEEE, **(2012)**, pp. 180-185.

[17] Chen, Yi-Ming, and Yu-Chih Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs", Journal of Communications and Networks, **(2013)**, pp- 153-163.

[18] M. Chuang and J. Lee, “TEAM: Trust extended authentication mechanism for Vehicular ad hoc networks”, Consumer Electronics, Communications and Networks (CECNet), IEEE International Conference, **(2011)**, pp. 1758-1761.

[19] I. AhmedSumra, H. Hasbullah, I. Ahmad, and J. BinAbManan, “Forming vehicular web of trust in VANET”, Electronics, Communications and Photonics Conference (SIECPC), IEEE, **(2011)**, pp. 1-6.

[20] I. AhmedSumra, H. Hasbullah, I. Ahmad, and J. BinAbManan, “New card based scheme to ensure security and trust in Vehicular communications”, Electronics, Communications and Photonics Conference (SIECPC), IEEE, **(2011)**, pp. 1-6.

[21] Kapil Sharma, Brijesh Kumar Chaurasia, “Trust Based Location Finding Mechanism in VANET using DST”, Fifth International Conference on Communication Systems and Network, IEEE, **(2015).**

[22] Ming-Chin Chuang and Jeng-Farn Le, “TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks”, IEEE, **(2013).**