Review in Trust and Vehicle Scenario in VANET

Sudha Dwivedi[1], Rajni Dubey[2]
[1, 2] Department of CSE
[1, 2] SRCEM, Banmore, India

Abstract- *VANET is a special type of MANET, where in vehicles act as nodes. Not like MANET, vehicles move on predefined roads, vehicles speed is determined by the velocity signs and additionally these vehicles additionally must comply with road traffic signs and road traffic signals. There are numerous challenges in VANET which can be wanted to be solved to be able to provide reliable offerings. Steady & reliable routing in VANET is likely one of the fundamental disorders. Accordingly more study is needed to be carried out in an effort to make VANET more relevant. As vehicles have dynamic conduct, excessive velocity and mobility that make routing much more difficult. In this paper, presenting a brief study on VANET its characteristics, types of routing protocols, Trust models and its security.*

Keywords- VANET; Trust; Security

I. INTRODUCTION

Vehicular Ad hoc Networks (VANET) is the subclass of Mobile Ad Hoc Networks (MANETs). VANET is without doubt one of the influencing areas for the improvement of intelligent Transportation system (ITS) with a view to provide protection and alleviation to the avenue customers. VANET assists automobile drivers to keep up a correspondence and to coordinate amongst themselves in order to restrict any vital quandary by means of automobile to auto verbal exchange e.G. Street facet accidents, visitors jams, speed manipulate, free passage of emergency vehicles and unseen boundaries etc. Besides security functions VANET also provide comfort functions to the road users [1]. Fig 1 shows the overall working structure of VANET.

VANET belongs to wireless communication networks discipline. VANET is the emerging field of MANETs in which vehicles act because the nodes inside the network. The elemental goal of VANET is to increase security of road customers and relief of passengers. VANET is the wireless community wherein communication takes location through wireless hyperlinks set up on every node (automobile) [2].

Each node within VANET act as each, the participant and router of the network as the nodes communicates through different intermediate node that lies within their own transmission range. VANET are self organizing network. It does now not rely on any constant community infrastructure.

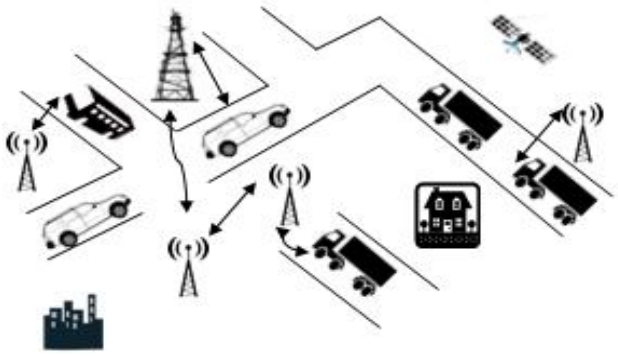

Fig.1. Vehicular Ad Hoc Network overview

Despite the fact that some fixed nodes act as the roadside models to facilitate the vehicular networks for serving geographical knowledge or a gateway to web etc [3]. Higher node mobility, velocity and fast sample movement are the most important characteristics of VANET. This also reasons speedy changes in network topology [4].

II. VANET ROUTING PROTOCOLS

VANET inherits similar characteristics as MANET. Because of excessive mobility, common changes in topology and limited life time are such characteristics of this network that make routing selections more difficult [6]. A number of other reasons equivalents to avenue layout and unique environments such as city and highway make routing more difficult in VANET.

Table.1 Routing Protocols

Routing Protocols		
Position Based Routing	Greedy Perimeter Stateless Routing- GPSR	Geographic Source Routing- GSR
Position based routing assumes that each node has advantage about its physical/ geographic position through GPS or via any other position opting for services. In it each and every node also has the abilities of source, destination and other neighbouring nodes.	Greedy Perimeter Stateless Routing (GPSR) [7] is among the satisfactory examples of function established routing. GPSR makes use of closest neighbour's information of destination with the intention to forward packet. This approach is sometimes called greedy forwarding.	Due to deficiencies of GPSR in presence of radio boundaries, network demanded new routing procedures that can compete with challenges occurred because of radio limitations. As a result, Geographic Source Routing (GSR) is proposed [8]. It deals with excessive mobility of nodes on one hand, on the other hand it uses roads layout to realize routes.

III. CHARACTERISTICS OF VANET

The unique characteristics of VANETs include:

a. High Mobility:
The nodes (vehicle) in VANETs usually are moving at high speed. The node motion is constrained by the road topology and layout

b. Rapidly Changing Network Topology:
Due to high node mobility, the network topology in VANETs tends to change frequently.

c. Unbounded Network Size:
VANETs could involve the vehicles in one city, several cities, or even a country. So the VANETs network should not be dependent on the number of the nodes.

d. Anonymous Naming:
Most applications in VANETs require identification of the vehicles in a certain region, instead of the specific vehicles. So, anonymous naming system should be followed to protect the privacy of the driver.

e. Delay-sensitive Data Exchange:
In the VANETs network the message transfer should be transfer without delay because security related applications need message delivery without any delay [9].

IV. SECURITY REQUIREMENTS OF VANET

VANET must fulfill some security prerequisites before they are transferred. A security system in VANET should fulfill the following necessary condition [9]:

a. 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.

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

c. 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.

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

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

V.TRUST IN VANET

Trustee (or the holding of a trusteeship) is a legal term which, in its broadest sense, can allude to any individual who holds property, power, or a position of trust or obligation regarding the advantage of another; additionally a trustee can be a man why should permit do certain assignments yet not ready to pick up wage.

Trust and reputation in VANET we define as derives from the notion of trust among human beings and is a subject of social science, the degree of subjective belief about the behaviors of a particular entity; trust is context dependent, dynamic and non-monotonic. Reputation defines as Building trust relations are a key part of todays distributed systems. They increase the efficiency without having to improve the detection or actuator parts, whereas they are critical to avoid bad behaved users to stay in the system with impunity. There is an extensive literature on those systems, but for our scope, we will focus on the hybrid-decentralized reputation ones. This is due to the fact that VANETs systems need reputation regarding inter-vehicles relationships (which can be reported to a coordinator) and also because wireless systems make impossible to request others' reputation for all and each announcement. The trustee can be anything from a man, association or physical substance, to digest ideas, for example, data or a cryptographic key [10].A trust relationship has an example, implying that it applies to a specific reason or space of movement, for example, "being authentic" on account of an a specialists' trust in a cryptographic key, or "giving reliable information" if there should arise an occurrence of a man's trust in the accuracy of a section in Wikipedia1. Mutual trust is when both parties believe one another with the same extension, yet this is clearly just conceivable when both sides are thinking elements. Trust impacts the tractor's states of mind and activities, yet can likewise have consequences for the trustee and different components in nature, for instance, by fortifying equal trust [11].

VI. TRUST MODELS IN VANET

Just a few trust models have as of late been proposed for implementing honest data sharing in vehicular systems. These models can be assembled into three classifications, element situated trust models, information arranged trust

models, and joined trust models. Entity-oriented trust models concentrate on the demonstrating of the dependability of peers. Data oriented trust models put more accentuation on assessing the dependability of information.

Table.2 VANET trust models

Trust Models		
Entity-oriented Trust Model	Data-oriented Trust Model	Combined Trust Model
Two typical entity-oriented trust models are the sociological trust model proposed by Gerlach [12] and the multi-faceted trust management model proposed by Minhas et al. [13]. The sociological trust model is proposed in light of the standard of trust and certainty labeling. The multi-faceted trust administration model of Minhas et al. [13] highlights in the part based trust and experience-based trust as the assessment metric for the coordinated reliability of vehicular substances.	Raya et al. [14] suggest that data-oriented trust may be more suitable in the area of Ephemeral Ad-hoc Networks, for example, VANETs. Data-centric trust establishment manages assessing the dependability of the information reported by different elements instead of trust of the substances themselves.	Three combined trust models have been proposed to model dependability of companions and utilize the demonstrating results to assess the reliability of information. Dotzer et al. [15] have recommended constructing a dispersed repudiated model that endeavors an idea called opinion piggybacking

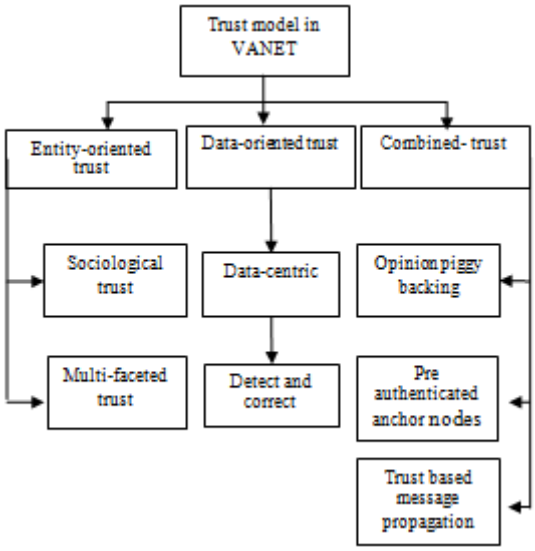

Fig.2 Trust Model in VANET

VII. LITERATURE SURVEY

Ming et al [16], proposed a decentralized light-weight authentication scheme referred to as crew to protect legitimate users in VANETs from malicious assaults. The quantity of cryptographic calculation under staff was once appreciably not up to in present schemes because it handiest used an XOR operation and a hash perform. Additionally, crew is based on the proposal of transitive believe relationships to support the performance of the authentication method. In addition, group has a number of storage spaces to store the authentication parameters

Xiaoping et al [17], presented a Reputation-based Global Trust Establishment scheme (RGTEs). The plan acquaints an answer with offer the trust information in VANET securely by applying statistical laws, which makes it more utilized and exact to build up trust in quickly evolving environment. Additionally, we distinguish an awful node of the element edge as per constant notoriety status of the network. Analysis shows that RGTEs is more powerful in confidence-building, security affirmation and versatility.

M Raya et al [18], proposed a data driven trust establishment system and connected it to the traffic safety application in VANET. Nonetheless, the creators did not consider the impact presented by the flow of movement occasions. A vehicle may not recognize a happened movement occasion or may gather loose information because of its sensor constraint when passing the event area of this activity occasion; therefore, for a vehicle, the assessment result on the trustiness of created information (or got messages) with respect to the watched (or reported) movement occasion may not be completely precise and dependable.

Schmidt et al [19], proposed a structure for vehicle behavior investigation in [19]. A vehicle's behavior alludes to all detectable data, including its development and position in the over a wide span of time. A getting vehicle aggregates an arrangement of messages from a TV vehicle, and these may give adequate data to conduct examination. The consequence of this examination will decide a vehicle as reliable, impartial, or conniving. In this methodology, vehicles are required to settle on perceptions before a choice can be made. This may not be attractive in VANETs, since vehicles are not ready to act rapidly upon the messages received.

Picconi et al [20], proposed a solution for validating a aggregated message with probabilistic signature checking mechanism. The proposed plan is utilized to confirm vehicle related data, for example, the present rate and geographic area, not activity occasions happened along the road. Also, a suspicious vehicle may have the capacity to go around the checking plan if its false messages are far not exactly all transmitted messages in a VANET. By and large, it is troublesome for a vehicle to decide the credibility of a reported movement event singularly.

Raya et al [21], applied message aggregation and

gathering communication to approve a reported movement event. The fundamental thought is to give a vehicle more proof around a reported movement event by gathering and investigating numerous approaching messages from diverse vehicles. The principle test of this paper is the manner by which to powerfully frame and keep up a vehicle bunch with the normal for high versatility.

In the below given table.3 a brief review on the work that has been conducted on VANET trust is depicted.

Table.3 Literature Survey

Author	Paper Title	Description
Ming	TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks	proposed a decentralized light-weight authentication scheme referred to as crew to protect legitimate users in VANETs from malicious assaults. The quantity of cryptographic calculation under staff was once appreciably not up to in present schemes because it handiest used an XOR operation and a hash perform. Additionally, crew is based on the proposal of transitive believe relationships to support the performance of the authentication method. In addition, group has a number of storage spaces to store the authentication parameters [16]
Xiaoping	RGTE: A Reputation-based Global Trust Establishment in VANETs	presented a Reputation-based Global Trust Establishment scheme (RGTEs). The plan acquaints an answer with offer the trust information in VANET securely by applying statistical laws, which makes it more utilized and exact to build up trust in quickly evolving environment. Additionally, we distinguish an awful node of the element edge as per constant notoriety status of the network. Analysis shows that RGTEs is more powerful in confidence-building, security affirmation and versatility [17]
M Raya	On data-centric trust establishment in ephemeral ad hoc networks	proposed a data driven trust establishment system and connected it to the traffic safety application in VANET. Nonetheless, the creators did not consider the impact presented by the flow of movement occasions. A vehicle may not recognize a happened movement occasion or may gather loose information because of its sensor constraint when passing the event area of this activity occasion; therefore, for a vehicle, the assessment result on the trustiness of created information (or got messages) with respect to the watched (or reported) movement occasion may not be completely precise and dependable [18]
Schmidt	Vehicle behavior analysis to enhance security in VANETs	proposed a structure for vehicle behavior investigation in [19]. A vehicle's behavior alludes to all detectable data, including its development and position in the over a wide span of time. A getting vehicle aggregates an arrangement of messages from a TV vehicle, and these may give adequate data to conduct examination. The

		consequence of this examination will decide a vehicle as reliable, impartial, or conniving. In this methodology, vehicles are required to settle on perceptions before a choice can be made. This may not be attractive in VANETs, since vehicles are not ready to act rapidly upon the messages received.
Picconi	Probabilistic validation of aggregated data in vehicular ad-hoc networks	proposed a solution for validating a aggregated message with probabilistic signature checking mechanism. The proposed plan is utilized to confirm vehicle related data, for example, the present rate and geographic area, not activity occasions happened along the road. Also, a suspicious vehicle may have the capacity to go around the checking plan if its false messages are far not exactly all transmitted messages in a VANET. By and large, it is troublesome for a vehicle to decide the credibility of a reported movement event singularly [20]
Raya	Efficient secure aggregation in VANETs	applied message aggregation and gathering communication to approve a reported movement event. The fundamental thought is to give a vehicle more proof around a reported movement event by gathering and investigating numerous approaching messages from diverse vehicles.
		The principle test of this paper is the manner by which to powerfully frame and keep up a vehicle bunch with the normal for high versatility [21]

VIII. PROMBLEM STATEMENT

Existing work is not very secure because every time XOR operation perform to find out the private key or user information which is easily modified or access same as happen with login procedure and authentication procedure. In this work if always XOR operation perform key size will be increase which is not good.

IX. CONCLUSION

VANETs are a promising communication scenario. Numerous novel applications are envisioned, which will recover traffic supervision and security. However, those applications have rigid security prerequisites, as they influence road traffic security. Besides, VANETs face a number of security threats. As VANETs present certain distinctive characteristics conventional security mechanisms are not constantly appropriate. In this paper presented a review on VANET and Trust in VANET, its characteristics, security requirements and VANET routing protocol.

REFERENCES

[1] T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato, and Y. Nemoto, “A stable routing protocol to support its services in vanet networks” IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3337–3347, November 2007.

[2] Manvi, S.S., Kakkasageri, M.S., Mahapurush, C.V., “Performance Analysis of AODV, DSR, and Swarm Intelligence Routing Protocols In Vehicular Ad hoc Network Environment” In International conference on future Computer and Communication., pp. 21-25, April. 2009.

[3] Bernsen, J. Manivannan, D., “Routing Protocols for Vehicular Ad Hoc Networks That Ensure Quality of Service” In the fourth international confernce on Wireless and Mobile Communications., pp.1-6, Aug. 2008.

[4] Wex, P. Breuer, J. Held, A. Leinmuller, T. Delgrossi, L., "Trust Issues for Vehicular Ad Hoc Networks" IEEE,VTC Spring 2008., pp. 2800-2804, May.2008.

[5] Blum, J. J., Eskandarian, A., and Hoffman, L. J. Challenges of intervehicle ad hoc networks. IEEE Trans. Intelligent Transportation Systems 5, 4 (Dec. 2004), 347–351

[6] Zhang, M.; Wolff, R., "Routing protocols for vehicular Ad Hoc networks in rural areas", Communications Magazine, IEEE , vol.46, no.11, pp.126-131, November 2008

[7] Karp, B. and Kung, H. T., "GPSR: greedy perimeter stateless routing for wireless networks", In Proceedings of the 6th Annual international Conference on Mobile Computing and Networking (Boston, Massachusetts, United States, August 06 - 11, 2000). MobiCom '00. ACM, New York, NY, pp. 243-254.

[8] C. Lochert, H. Hartenstein, J. Tian, D. Herrmann, H. Füßler, and M. Mauve, "A routing strategy for vehicular ad hoc networks in city environments," in Proceedings of IEEE Intelligent Vehicles Symposium (IV2003), pp. 156–161, June 2003..

[9] José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda." Overview of security issues in Vehicular Ad-hoc Networks".

[10] Saurabh Kumar Gaur, S.K.Tyagi, Pushpender Singh; "VANET" System for Vehicular Security Applications". International Journal of Soft Computing and Engineering (IJSCE), 2013

[11] R. Falcone and C. Castelfranchi. How trust enhances and spread trust. In Proceedings of the 4th Int. Workshop on Deception Fraud and Trust in Agent Societies, in the 5th International Conference on Autonomous Agents (AGENTS'01), May 2001.

[12] M. Gerlach, "Trust for vehicular applications," in Proceedings of the International Symposium on Autonomous Decentralized Systems 2007.

[13] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," International Journal of Computational Intelligence Theory and Practice (IJCITP) vol. 5, no. 1, 2010.

[14] M. Raya, P. Papadimitratos, V. Gligor, and J. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," Technical Report, LCA-REPORT-2007-003 , 2007

[15] F. Dötzer, L. Fischer, and P. Magiera, "VARS: A vehicle ad hoc network reputation system," in Proc. 6th IEEE Int. Symp. World Wireless Mobile Multimedia Netw., 2005, vol. 1, pp. 454–456.

[16] Ming-Chin Chuang and Jeng-Farn Le "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks" 1932-8184/$31.00 c 2013 IEEE.

[17] Xiaoping Li;" RGTE: A Reputation-based Global Trust Establishment in VANETs". IEEE, 2013

[18] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P.Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM '08), pp. 1238–1246, April 2008.

[19] R. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in VANETs," in Proc. 4th Workshop V2VCOM, Eindhoven, The Netherlands, 2008.

[20] F. Picconi, N. Ravi, M. Gruteser, and L. Iftode, "Probabilistic validation of aggregated data in vehicular ad-hoc networks," in Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET '06), pp. 76–85, Los Angeles, Calif, USA, 2006.

[21] M. Raya, A. Aziz, and J.-P.Hubaux, "Efficient secure aggregation in VANETs," in Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET '06), pp. 67– 75, Los Angeles, Calif, USA, 2006.