A Survey of All Existing Trust Models in Vehicular Ad Hoc Network

Neha Jain[1], Krishna Kumar Joshi [2]
[1, 2] Department of Computer Science And Engineering
[1, 2] MPCT, Gwalior, M.P, India

Abstract- *VANET or Vehicular Ad-Hoc Network is a sub form of Mobile Ad-Hoc Network or MANET that provides communication between vehicles and between vehicles and road-side base stations with an aim of providing efficient and safe transportation. A vehicle in VANET is considered to be an intelligent mobile node which is capable of communicating with its neighbours and other vehicles in the network. VANET introduces more challenging aspects as compare to MANET because of high mobility of nodes and fast topology changes in VANET. Various routing protocols have been designed and presented by researchers after considering the major challenges involved in VANETs. This paper provides a survey of routing protocols for VANET. This paper covers application areas, challenges and security issues occurred in VANETs.*

Keywords- RSU, V2V, V2I or VRC, ITS, VANET

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) have grown out of the need to support the growing number of wireless products that can now be used in vehicles [Raya, 2005] [Harsch, 2007]. These products include remote keyless entry devices, personal digital assistants (PDAs), laptops and mobile telephones. As mobile wireless devices and networks become increasingly important, the demand for Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (VRC) or Vehicle-to-Infrastructure (V2I) Communication will continue to grow [Harsch, 2007]. VANETs can be utilized for a broad range of safety and non-safety applications, allow for value added services such as vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based services like finding the closest fuel station, restaurant or travel lodge [Gerlach,2006] and information based applications such as providing access to the Internet.

Over the last few years, we have witnessed many research efforts that have investigated various issues related to V2I or VRC and V2V areas because of the crucial role they are expected to play in Intelligent Transportation Systems (ITSs). In fact, various VANET projects have been executed by various governments, industries, and academic institutions around the world in the last decade or so.

II. OVERVIEW OF VANET

A. Intelligent Transportation Systems (ITSs)

In intelligent transportation systems, each vehicle takes acts like a sender, receiver and router [Jinyuan, 2007] to broadcast information to the vehicular network or transportation agency, which then uses the information to ensure safe, free-flow of traffic. For communication to occur between vehicles and Road Side Units (RSUs), vehicles must be equipped with some sort of radio interface or On Board Unit (OBU) and this On Board Unit enables short-range wireless ad hoc networks to be formed [Stampoulis, 2007]. Vehicles must also be fitted with hardware that allows detailed location information such as Global Positioning System (GPS) or a Differential Global Positioning System (DGPS) receiver. Fixed RSUs are connected to the backbone network, must be in place to make easy communication. The distribution of roadside units and the number of RSUs is dependent on the communication protocol is to be used. For example, some of the protocols need roadside units to be distributed evenly throughout the whole road network; some of them need roadside units only at intersections, while others need roadside units only at region borders.

Though it is safe to assume that infrastructure exists to some extent and vehicles have access to it intermittently, it is unrealistic to require that vehicles always have wireless access to roadside units. Figures 1, 2 and 3 depict the possible communication configurations in intelligent transportation systems in VANET. These include inter-vehicle, vehicle-to-roadside, and routing-based communications. These communications are based on very accurate and up-to-date information about the surroundings and environment, which, in turn, requires the use of accurate positioning systems and smart communication protocols for sending and retrieving information. In a network environment in which the communication medium is shared, highly unreliable, and with limited bandwidth [Balon, 2006], smart communication protocols must guarantee fast and reliable delivery of information to all vehicles in the vicinity. It is worth mentioning that Intra-vehicle communication uses technologies such as IEEE 802.15.1 (Bluetooth), IEEE 802.15.3 (Ultra-wide Band) and IEEE 802.15.4 (Zigbee) that can be used to support wireless communication inside a vehicle but this is outside the scope of this paper and will not be discussed further.

B. Inter-Vehicle Communication

The inter-vehicle communication configuration (Figure 1) uses multi-hop multicast/broadcast to forward traffic related information over multiple hops to a group of receivers.

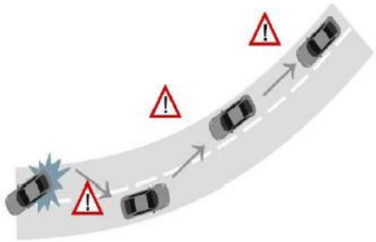


Fig.1. Inter vehicle communication

In intelligent transportation systems, vehicles require only be concerned with activity on the road ahead and not behind (an example of this would be for emergency message dissemination about an imminent collision or dynamic route scheduling). There are two types of message transmission in inter-vehicle communications: naïve broadcasting and intelligent broadcasting. In naïve broadcasting, vehicles send broadcast messages periodically and at regular intervals. Upon receipt of the message, the vehicle ignores the message if it has come from a vehicle behind it. If the message comes from a vehicle in front, the receiving vehicle sends its own broadcast message to vehicles behind it.

This ensures that all enabled vehicles moving in the forward direction get all broadcast messages. The actual limitations of the naïve broadcasting method is that large numbers of broadcast messages are generated, therefore, increasing the risk of message collision resulting in lower message delivery rates and increased delivery times [Bickel, 2008]. Intelligent broadcasting of messages with implicit acknowledgement addresses the problems inherent in naïve broadcasting by limiting the number of messages broadcast for a given emergency event. If an event-detecting vehicle receives the same message from behind, it assumes that at least one vehicle in the back has received the same message and ceases broadcasting. The assumption is that the vehicle in the back will be responsible for moving the message along to the rest of the vehicles. If a vehicle receives a message from more than one source it will act on the first message only.

C. Vehicle-to-roadside Communication

The vehicle-to-roadside communication configuration (Figure 2) represents single hop broadcast where the roadside unit sends a broadcast message to all equipped vehicles in the network.

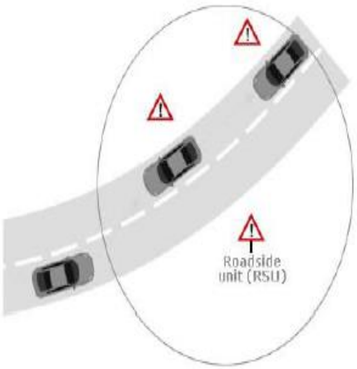


Fig.2.Vehicle to roadside communication

Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside units. The RSUs may be placed every kilometer or less, enabling high data rates to be maintained in heavy traffic. For example, when broadcasting dynamic speed limits, the roadside unit will determine the appropriate speed limit according to its internal timetable and traffic conditions. The roadside unit will perform periodically broadcast a message containing the speed limit and will compare any geographic or directional limits with vehicular data to find if a speed limit warning applies to any of the vehicles in the vicinity. If a vehicle in the network violates the desired speed limit, a broadcast message will be delivered to the vehicle in the form of an auditory or visual warning, requesting to the driver to reduce his speed.

D.Routing-based Communication

The routing-based communication configuration (Figure 3) is a multi-hop or unicast scheme where a message is propagated in a multi-hop fashion until the vehicle carrying the desired data is reached.

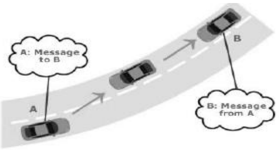


Fig.3.Routing based communication

When the request is received by a vehicle owning the desired piece of information, the application at that vehicle immediately sends a unicast message containing the information to the vehicle it received the request from, which is then charged with the task of sending it to the requesting source [1].

III. CHALLENGES IN VANET

VANET supports almost all kind of dissimilar range of on road applications and thus needs efficient and effective radio resource management strategies. [2] This includes QOS control, capacity enhancement, interference control, bandwidth reservation, packet loss reduction, packet scheduling and fairness assurance. The existing approaches designed for MANETs are ineffective and/or inefficient and cannot be directly applied in VANET. To accomplish various applications in a vehicular environment, new and effective strategies are required to be tailored specifically meant for VANET. Following are the key research challenges in VANET:

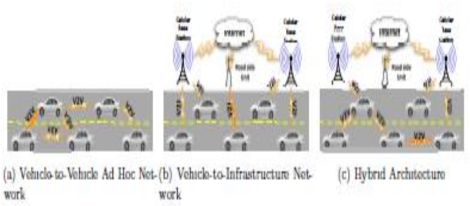
Frequent Link Disconnections: As discussed in the previous section that unlike nodes in MANETs, vehicles are highly mobile and generally travel at higher speeds, especially on highways (i.e., over 100 km/hr) and thus changes the topology of a network which causes intermittent communication links between a source and a destination. Moreover, the network resources allocated to vehicles go in vain due to frequent link disconnections. Node Distribution: In the real world, vehicles are not uniformly distributed in the given region [3]. Hot spots like commercial region and shopping centre's can attract more people, which outcomes in higher node densities in these areas. The heterogeneous distributions of vehicles raise a great challenge for design of routing algorithms.

Inter-contact time and duration time: Inter-contact time [3] characterizes the sharing of the interval between two inter-vehicle contacts. The network connectivity is better if the inter-contact time is smaller. The duration time of a contact decides the amount of data can be transmitted within a contact, which is typically small, in the scale of seconds.

IV. CHALLENGES IN VANET

The advances in mobile communications and the existing trends in ad hoc networks allow different deployment architectures for vehicular networks in rural, urban and highways environments to support many applications with different QoS requirements. The goal of a VANET architecture is to allow the communication among nearby vehicles and between vehicles and fixed roadside equipments leading to the following three possibilities (as shown in Figure 4):

- Vehicle-to-Vehicle (V2V) ad hoc network: allows the direct vehicular communication without relying on a fixed infrastructure support and can be mainly employed for safety, security, and dissemination applications;
- Vehicle-to-Infrastructure (V2I) network: allows a vehicle to communicate with the RSI mainly for information and data gathering applications
- Hybrid architecture: include both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). In this scenario, a vehicle can communicate with the roadside infrastructure either in a single hop or multi-hop fashion, depending on the distance, i.e., if it can or not access directly the roadside unit. It enables long distance connection to the Internet or to vehicles that are far away.



(a) Vehicle-to-Vehicle Ad Hoc Network (b) Vehicle-to-Infrastructure Network (c) Hybrid Architecture

Fig 4. VANET Architecture

A VANET has some particular features despite being a special case of a MANET and presenting some same characteristics like low bandwidth, short transmission range and omnidirectional broadcast:

- Highly dynamic topology: VANET is highly dynamic due to two reasons:
  a) Speed of the vehicles and
  b) Characteristics of radio propagation. Vehicles have high relative velocities in the order of 50 km/h in urban environments to more than 100 km/h in highways. They may also move at different directions. Thus, vehicles can quickly join or leave the network in a very short period of time, leading to frequent and fast topology changes.
- Frequently disconnected: the highly active topology results in frequent changes in its connectivity, thus the link between two vehicles can quickly disappear while they are transmitting information;
- Geographical communication: vehicles to be reached typically depend on their geographical location. This differs from other networks in which the target vehicle or a group of target vehicles are defined by an ID or a group ID;

- Constrained mobility and prediction: VANETs present highly active topology, but vehicles usually follow a certain mobility pattern constrained by roads, streets and highways, traffic lights, speed limit, traffic conditions, and drivers' driving behaviors. Thus, given the mobility pattern, the future position of the vehicle is more feasible to be assumed;
- Propagation model: typically, VANETs operate in three environments: highway, rural, and city. In a highway, the propagation model is usually understood to be free-space, but the signal can suffer interference by the reflection with the wall panels around the roads. In a city, its surroundings make the communication complex due to the variable vehicle density and the presence of buildings, trees, and other objects, acting as obstacles to the signal propagation. Such obstacles cause shadowing, multi-path, and fading effects. Usually, the propagation model is assumed to not be free-space due to those characteristics of the communication environment. In rural environments, due to the complex topographic forms (fields, hills, climbs, dense forests, etc.), it is important to consider the signal reflection and the attenuation of the signal propagation. Therefore, in this scenario, the free-space model is not appropriate. As in any other network, the propagation model in a VANET must consider the effects of potential interference of wireless communication from other vehicles and the existence of largely deployed access points. All these features bring new challenges to the design of communication protocols in VANETs. The spatial-temporal constraints of this type of network and the heterogeneity of vehicles in terms of speed and mobility are design factors to be considered in the development of algorithms and protocols for VANETs. For illustration, taking into account cars and trucks versus buses and trams: cars and trucks have different speeds and tend to follow an unpredictable mobility model, whereas buses and trams have a regular, slower speed and a predictable mobility model [4].

V. TRUST MODELS IN VANETs

Only a few trust models have recently been proposed for enforcing honest information sharing in vehicular networks. In this section, we summarize them and point out their issues. Note that great efforts, for example the work in [5], [6], have been spent by researchers in security and privacy on trust establishment in VANETs that relies on a security infrastructure and most often makes use of certificates. A more extensive summary of this kind of trust systems can be found in [7]. We focus on trust models that do not fully rely on the static infrastructure and thus can be more easily deployed. In these models, peers may form trust relationships with each other based on, for example, past interaction experience. They may also gather environmental information about messages sent by other peers to determine the correctness of the data. These models can be grouped into three categories, entity-oriented trust models, data-oriented trust models, and combined trust models. Entity-oriented trust models focus on the modeling of the trustworthiness of peers. Data-oriented trust models put more emphasis on evaluating the trustworthiness of data. In these models, normally, no long-term trust relationships between peers will be formed. Combined trust models make extensive use of peer trust to evaluate the trustworthiness of data, but at the same time maintain peer trust over time.

A. Entity-oriented Trust Model

Two typical entity-oriented trust models are the sociological trust model proposed by Gerlach [8] and the multi-faceted trust management.

The sociological trust model is proposed based on the principle of trust and confidence tagging. Gerlach has identified various forms of trust including situational trust – which depends on situation only, dispositional trust – which is the level of trust based on a peer's own beliefs, system trust – depends on the system and finally belief formation process – which is the evaluation of data based on previous factors. Additionally, they have presented architecture for securing vehicular communication and a model for preserving location privacy of the vehicle. However, Gerlach does not provide formalization of the architecture about how to combine the different types of trust together. The multi-faceted trust management model. Features in the role-based trust and experience-based trust as the evaluation metric for the integrated trustworthiness of vehicular entities. This model also allows a vehicular entity to actively inquire about an event by sending requests to other entities but restrict the number of reports that are received. For this purpose, the authors introduce in the research the concept of priority-based trust, which provides for an ordering of the value of an information source within a role category, using the influence of experience-based trust. The limit on the number of sources consulted is sensitive to the task at hand. In the end, the trust of information sources and the contextual information about the event such as time and location are integrated into a procedure for gauging whether majority consensus has been reached, which ultimately determines the advice a vehicular entity should follow. The above two trust models have some components in common, for example, situational trust can be compared with event/task specific trust, and similarly dispositional trust can be compared to experience or role-based trust. One problem about the multi-faceted trust management is that robustness has not been extensively addressed.

B. Data-oriented Trust Model

In contrast to the traditional view of entity-oriented trust, propose that data-oriented trust may be more appropriate in the domain of Ephemeral Ad-hoc Networks such as VANETs. Data-centric trust establishment deals with evaluating the trustworthiness of the data reported by other entities rather than trust of the entities themselves. In their model, they define various trust metrics of which a priori trust relationships in entities is just one of the default parameters and depends on the attributes associated with a particular type of node. Using Bayesian inference and Dempster-Shafer Theory, they evaluate various evidences regarding a particular event taking into account different trust metrics applicable in the context of a particular vehicular application. Finally their decision logic outputs the level of trust that can be placed in the evaluated evidences indicating whether the event related with the data has taken place or not. Raya et al. also propose the use of task/event specific trust metrics as well as time and location closeness. One of the shortcomings of their work is that trust relationships in entities can never be formed, only ephemeral trust in data is established, and because this is based on a per event basis, it needs to be established again and again for every event. This will work so long as there is enough evidence either in support of or against a specific event, but in the case of data sparsity their model would not perform well. Present a technique that aims to address the problem of detecting and correcting malicious data in VANETs. The key assumption of their approach is in maintaining a model of VANET at every node. This model contains all the knowledge that a particular node has about the VANET. Incoming information can then be evaluated against the peer's model of VANET. If all the data received agrees with the model with a high probability then the peer accepts the validity of the data. However, in the case of receiving data which is inconsistent with the model, the peer relies on a heuristic that 107 tries to restore consistency by finding the simplest explanation possible and also ranks various explanations. The data that is consistent with the highest ranking explanation(s) is then accepted by the node. The major strength of this approach is that it may provide security against adversaries that might even be highly trusted members in the network or might be colluding together to spread malicious data. However, one strong assumption of this approach is that each vehicle has the global knowledge of the network and solely evaluates the validity of data, which may not be feasible in practice.

C. Combined Trust Model

Three combined trust models have been proposed to model trustworthiness of peers and use the modeling results to evaluate the reliability of data. suggested building a distributed reputation model that exploits a notion called opinion piggybacking where each forwarding peer (of the message regarding an event) appends its own opinion about the trustworthiness of the data. They provide an algorithm that allows a peer to generate an opinion about the data based on aggregated opinions appended to the message and various other trust metrics including direct trust, indirect trust, and sender based reputation level and Geo-Situation oriented reputation level. This last trust metric allows their model to introduce some amount of dynamism in the calculation of trust by considering the relative location of the information reporting node and the receiving node. Additionally, the situation oriented reputation level allows a node to consider certain situational factors e.g. familiarity with the area, rural or metropolitan area etc. again introducing some dynamism in trust evaluation based on context. One problem is that the authors did not provide sufficient and complete details about the approach. Although they mention that sender based reputation information is managed, they did not describe its formalization or how reputation information can be updated. A more important problem about this approach is that it repeatedly makes use of the opinions from different nodes. The nodes that provide opinions about a message earlier will have larger influence than the nodes generated opinions later, because the earlier nodes' opinions will be repeatedly and recursively considered by later nodes. propose an approach in which the reputation of a node is determined by data validation. In this approach, a few nodes, which are named as anchor nodes here, are assumed to be pre-authenticated, and thus the data they provide are regarded as trustworthy. Data can be validated by either agreement among peers or direct communication with an anchor node. Malicious nodes can be identified if the data they present is invalidated by the validation algorithm. One problem about this scheme is that it does not make use of reputation of peers when determining the majority consensus. The majority consensus works well only when a sufficient number of reports about the same event are provided. However, this scheme only passively waits for reports from other peers. Overcoming some problems of the above two models, propose a trust-based message propagation and evaluation framework in vehicular ad-hoc networks where peers share information regarding road condition or safety and others provide opinions about whether the information can be trusted. More specifically, the trust-based message propagation model collects and propagates peers' opinions in an efficient, secure and scalable way by dynamically controlling information dissemination. The trust-based message evaluation model allows peers to evaluate the information in a distributed and collaborative fashion by taking into account others' opinions. This model is demonstrated to promote network scalability and system effectiveness in information evaluation under the pervasive presence of false information, which are the two essentially important factors for the popularization of VANETs.

VI. LITRATURE SURVEY

Marc Torrent Moreno [9] presented mechanism that was aimed at investigating broadcasted messages to a neighbour by another neighbour node in VANETs.

Sascha et. al .[10] presented Modern decision support systems (DSS) for transportation management that store huge amounts of decision-relevant data, as well as intend at assisting decision-makers to explore the meaning of that particular data, and to obtain decisions based on understanding this architecture.

Nabeel Akhtar [11] has presented realistic analysis of the VANET topology characteristics over time and space for highway . In this analysis, Author integrate real-world road topology and real-time data extracted from the Freeway Performance Measurement System (PeMS) database into a microscopic mobility model to generate realistic traffic flows along the highway.

Umar Farooq Minhas [12] introduced multi-faced trust model that is an intelligent agent based scheme for vehicular Ad-hoc network. In this scheme drivers exchange information with other drivers regarding road and traffic conditions.

Christian Adler et. al [13] presented the concept of self-organized and context-adaptive information diffusion in VANETs. Christian Lochert et. al [14] presents information dissemination in vehicular ad-hoc networks (VANETs) in city scenarios.

Zhou Wang et. al [15] examined the cooperative packet forwarding schemes in VANETs. VANET insists cooperative communication with peer nodes below its operation environment of high mobility, quickly changing topology and low associatively redundancy. Mingliu Zhang et. al [16] reviewed the routing protocols for VANETS.

Francesco Lupi et. al [17] evaluate the performance of broadcast routing protocol in a VANET presented and also presented the employment of RSUs inside the vehicular network.

P. Suresh [18] proposed an analytical model for warning messages through collision avoidance (CA) system.

VII.CONCLUSION

VANET is an area of research that holds promising future and for vehicular users. However, it has its own challenges in the security prospect. VANET aims at reducing the accidents on our roads and increasing the flow of information among vehicle and the road users. The unique nature of VANET springs up issues like illegal tracking and jamming of the network. In this paper, we introduced VANET, its architecture, components, communication pattern and issues in its security.

ACKNOWLEDGMENT

The preferred spelling of the word ―acknowledgment‖ in American English is without an ―e‖ after the ―g.‖ Use the singular heading even if you have many acknowledgments.

REFERENCES

[1] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan " Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges"2012.

[2] Rakesh Kumar and Mayank Dave "A Review of Various VANET Data Dissemination Protocols" International Journal of u- and e- Service, Science and Technology, Vol. 5, No. 3, September, 2012

[3] Yanmin Zhu1, Chao Chen1 and Min Gao "An evaluation of vehicular networks with real vehicular GPS traces"EURASIP Journal onWireless Communications and Networking 2013,pp.190, 13 July 2013

[4]Felipe Domingos da Cunha, Azzedine Boukerche, Leandro Villas, Aline Carneiro Viana, Antonio A. F. Loureiro "Data Communication in VANETs: A Survey, Challenges and Applications" RESEARCH REPORT N° 8498 March 2014.

[5] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," in Proceedings of VANET, 2009, pp. 89–98.

[6] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, “Eviction of misbehaving and faulty nodes in vehicular networks,” IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1557– 1568, Oct. 2007.

[7] P. Wex, J. Breuer, A. Held, T. Leinmuller, and L. Delgrossi, “Trust issues for vehicular ad hoc networks,” in Proceedings of the 67th IEEE Vehicular Technology Conference (VTC Spring), 2008.

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

[9]. Torrent-Moreno, Marc, Daniel Jiang, and Hannes Hartenstein, ‘Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks’, Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, vol. 15, pp. 39-68, 2004.

[10]. Ossowski, Sascha, ‘ Decision support for traffic management based on organisational and communicative multiagent abstractions’, Transportation Research part C: emerging technologies, vol. 13, Issue 4,pp. 272-298, 2005.

[11]. Akhtar, Nabeel, S. Coleri Ergen, and Oznur Ozkasap, ‘Vehicle mobility and communication channel models for realistic and efficient highway VANET simulation’, (2014).

[12]. Umar Farooq Minhas,’ Intelligent Agents in Mobile Vehicular Ad-Hoc Networks: Leveraging Trust Modeling Based on Direct Experience with Incentives for Honesty’, International Conference on Web Intelligence and Intelligent Agent Technology, pp. 4191-4, 2010.

[13]. Adler, Christian,’Self-organized and context-adaptive information diffusion in vehicular ad hoc networks’, International Symposium Wireless Communication Systems, 2006.

[14]. Lochert, Christian,’ The feasibility of information dissemination in vehicular ad-hoc networks’, Wireless on Demand Network Systems and Services, Fourth Annual Conference , 2007.

[15]. Zhou Wang, and Chunxiao Chigan,’ Countermeasure uncooperative behaviors with dynamic trust-token in VANETs’, IEEE International Conference, 2007.

[16]. Zhang, Mingliu, and R. S. Wolff, ’Routing protocols for vehicular ad hoc networks in rural areas’, Communications Magazine, IEEE 46.11, pp.19-131, 2008.

[17]. Lupi, Francesco, Veronica Palma, and Anna Maria Vegni, ’Performance Evaluation of Broadcast Data Dissemination over VANETs,’ A Case Study in the City of Rome, pp. 1-4, 2012.

[18]. Suresh, P., and M. Ramya,’Collision Avoidance System for Safety Vehicular Transportation in VANET’, Asian Journal of Technology & Management Research, 2014.