International Journal for Research in Applied Science & Engineering Technology (IJRASET)

# A Review: VANET

Piyush Anand[1], Apurva Sharma[2]
[1]Master of Computer Application , Institute of Engineering and Technology Bhaddal, Ropar, Punjab, India
[2]Master of Computer Engineering, Punjabi University Patiala, Punjab, India

***Abstract-VANET is a technology which is used to move cars as joint in network to make transportable network. VANET is a form of mobile ad hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as roadside equipment. Participating cars become a wireless connection or router through VANET and it allows the cars almost to connect 100 to 300 meters to each other and in order to create a wide area network, other vehicles and cars are connected to each other so the mobile internet is made. In this paper we will discuss the characteristics, applications of VANET.***

***Keywords: VANET, Road traffic information, Ad-Hoc Network , Routing Protocols.***

## I. INTRODUCTION

Work on the ad hoc network begins from 1970s when network were originally called packet radio networks. Inter-Vehicle Communications (IVC) and Roadside-toVehicle Communication (RVC) are becoming one of the most popular research topics in wireless communications. Capability of VANET has to provide safety and traffic management: vehicles can notify other vehicles of hazardous road conditions, traffic jamming, or rapid stops. In 1999, the Federal Communication Commission allocated a frequency spectrum for IVC and RVC. Studies in [1, 3] have demonstrated that communications among vehicles can exploit the short-range IEEE 802.11 based radio interface technology. IEEE, 802.11p group specifying the new physical layer and MAC (Medium access control) layer for inter- vehicular communication [2, 3].

In a VANET, vehicles will rely on the integrity of received data for deciding when to present alerts to drivers. Further in the future, this data may be used as the basis of control decisions for autonomous vehicles. If this information is corrupted, vehicles may present unnecessary or erroneous warnings to their drivers, and the results of control decisions based on this information could be even more disastrous. Information can be corrupted by two different mechanisms: malice and malfunction. Similarly, vehicles have two defense mechanisms: an internal filter and external reputation information. The former defense mechanism can consist of filters based on physical laws (e.g., maximum braking deceleration, maximum speed, physical space constraints) [4]. The latter defense mechanism can consist of reports from other vehicles or entities on the validity or trustworthiness of data originating from certain [5].

Information received from corrupted nodes should be disregarded or not trusted by legitimate vehicles, otherwise, a malicious vehicle could, for example, obtain a less congested route for itself by overstating the number of vehicles on its desired roadway. As a Second example, a corrupted node could trigger erroneous driver warnings to be displayed in other vehicles by falsifying its position information. IEEE 1609.2, the trial-use standard concerning security services for vehicular environments, stipulates that vehicles will be authenticated using certificates issued by a Certificate Authority (CA) in a Public Key Infrastructure (PKI) setup [6]. Illegitimate vehicles should have these certificates revoked, and the identity of the revoked certificates (although ideally not the identity of the associated driver) should be published and distributed to legitimate vehicles. Whatever mechanism that is used for distributing this revocation information should distribute the info information securely, quickly, and broadly in order to limit the amount of damage illegitimate vehicles can do. First we discuss the general architecture and security architecture of vanet.

Volume 3 Issue XII, December 2015
ISSN: 2321-9653


## II. LITERATURE SURVEY

| Sr. No | Name | Author | Objective | Drawbacks |
|---|---|---|---|---|
| 1. | Design and analysis of lightweight evocation mechanism for vanet[5] | Jasson j.hass kenneth p.laberteux ACM | 1. Reduced certificate revocation lists size 2. Lightweight mechanism for exchanging CRL updates | 1.CRLs can be very long due to the large number of vehicles and their high mobility. 2.Performance would be low when we use the protocol in high traffic area. |
| 2 | Security Certificate revocation list distribution for VANET. [8] | (Kenneth P. Laberteaux, J.J. Haas, and Y.C.Hu). In VANET '08 Proceedings of the fifth ACM international workshop on VehiculAr InterNETworking | 1.Improves distribution speed and distribution of CRLs by using vehicles in an epidemic fashion. | 1. Performs methods that only employ RSUs(Road Side Units) distribution points. 2. VANET nodes must confirm to the Bandwidth and Hardware restrictions. |
| 3. | Eviction of misbehaving and faulty nodes in vehicular networks [9 | (M. Raya, P. Papadimitratos, I. Aad, D.jungels, and J.P. Habaux) IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks, vol. 25, num. 8, p. 1557-1568 | 1. Infrastructure based Revocation protocols (RTPD, RCCRL). 2. MDS, enabling the neighbours of misbehaving or faulty nodes to detect its deviation from normal behavior. 3. LEAVE protocol to safeguard the system operation | Bloom fiter's false positive rate. |
| 4. | A Novel Defense Mechanism against Sybil Attacks in VANET. [10] | (Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi) , SIN '10 Proceedings of the 3rd international conference on Security of information and networks | 1.Proposed the parameter ANGLE for RSUs, to detect Sybil nodes. 2.ANGLE value remains unique for each node at any instant of time. 3.Results shows 99% accuracy and approximate of 0.5% error rate. | Processing time, Storage capacity and number of RSUs units are not well defined to achieve 100% detection accuracy. |
| 5. | A Scalable Robust Authentication Protocol for Secure Vehicular Communications. | (Lei Zhang, Qianhong Wu, Agusti Solanas) | The protocol efficiently exploits the specific features of vehicular mobility, physical road limitations, and properly distributed RSUs. | 1.Performance rate decreased, as load increases performance decreases. 2.If any RSU collapsed than working will be lost for that network. |
| 6. | Special issues on Inter-Vehicular Communication[11] | (M. Raya, Panos Papadimitratos, and Jean-pierre Habaux) | Vehicular Communication exhibits unique security challenges, induced by the high speed and sporadic connectivity of the vehicles | 1.Secure positioning is an open problem. 2.VC exhibits Short-Lived certification (CRLs). |

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

| | | | | |
|---|---|---|---|---|
| 7. | Securing Vehicular ad hoc networks. [12] | ( M. Raya, and J.P Habaux) | 1.Proposed a model that identifies the most relevant communication aspects. 2.Proposed a security architecture along with the related protocols. 3.Digital Signatures showed to be the most suitable approach despite their seemingly high overhead. | 1. Existing network security solutions cannot be readily applied to VANETs (due to radically different nature of this new type of networks). |

## III. GENERAL VANET ARCHITECTURE

The communication may be of 3 types-1.inter-vehicle communication i.e vehicle to vehicle communication 2.vehicle to roadside communication i.e communication between roadside unit(RSU) and vehicles 3.inter-roadside communication i.e communication between roadside unit and the base station. Applications based on vehicular communication range from simple exchange of vehicle status data to highly complex, large-scale traffic management including infrastructure integration.

Although exact operation details are not yet standardized for most applications and in spite that such a collection can never be completely finished, the overview delivers basic mechanisms, components and constraints involved in the system.

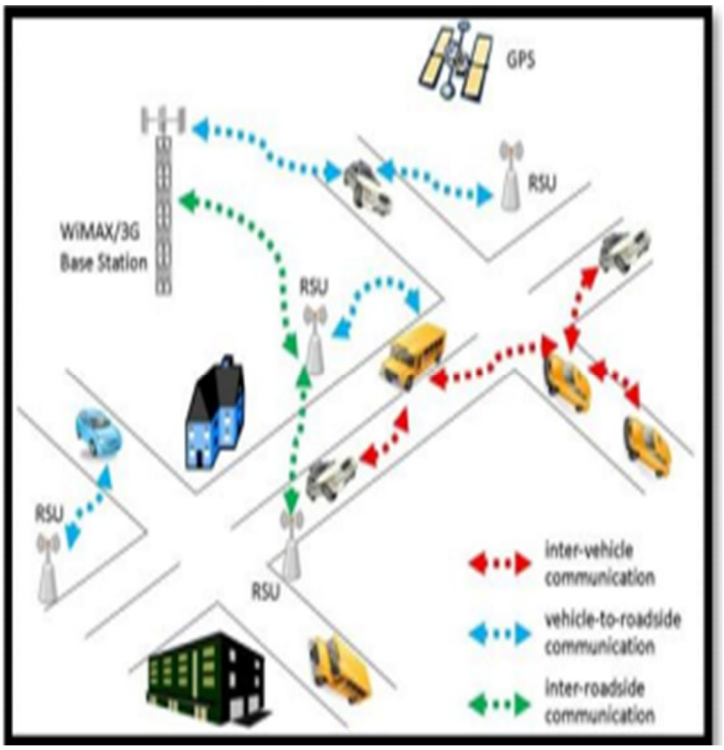


Fig.1: General Architecture[7]

## IV. SECURITY ARCHITECTURE

All Generally includes use of public key signatures. In a public key infrastructure, certificate authorities(CAs) binds between public keys and the nodes.

Security and privacy are two critical concerns for the designers of VANETs that, if forgotten, might lead to the deployment of vulnerable VANETs. Unless proper measures are taken, a number of attacks could easily be conducted, namely, message content modification, identity theft, false information generation and propagation, etc. The following are examples of some specific attacks .

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

If message integrity is not guaranteed, a malicious vehicle could modify the content of a message that is sent by another vehicle to affect the behavior of other vehicles. By doing so, the malicious vehicle could obtain many benefits while keeping its identity unknown. Moreover, the vehicle that originally generated the message would be made responsible for the damage caused.

If authentication is not provided, a malicious vehicle might impersonate an emergency vehicle to surpass speed limits without being sanctioned.

A malicious vehicle could report a false emergency situation to obtain better driving conditions (e.g., deserted roads), and if non-repudiation is not supported, it could not be sanctioned even if discovered.

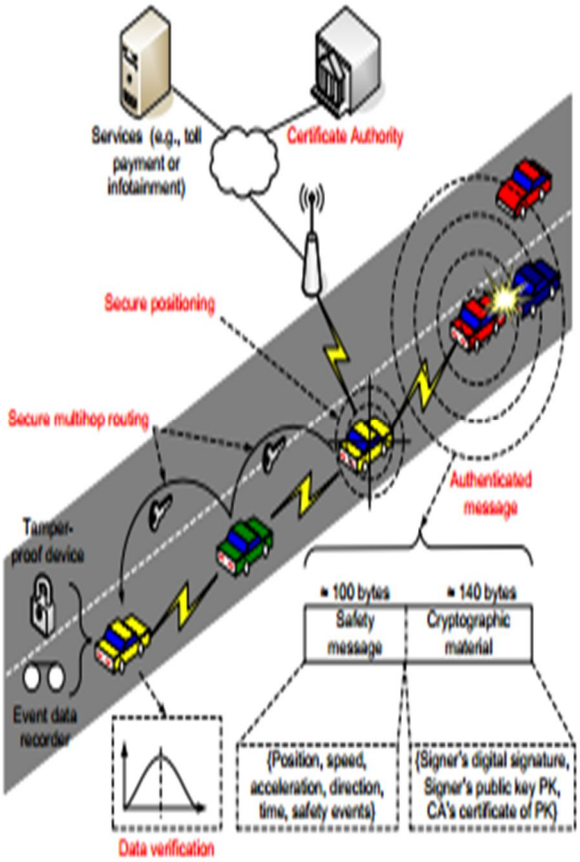


Fig.2: General Security Architecture [8]

## V. VANET APPLICATIONS

### A. *Safety Applications*

Safety Applications Safety applications include monitoring of the surrounding road, approaching vehicles, surface of the road, road curves etc. The Road safety applications can be classified as:

*1) Real-Time Traffic:* The real time traffic data can be stored at the RSU and can be available to the vehicles whenever and wherever needed. This can play an important role in solving the problems such as traffic jams, avoid congestions and in emergency alerts such as accidents etc.

*2) Co-Operative Message Transfer:* Slow/Stopped Vehicle will exchange messages and co-operate to help other vehicles. Though reliability and latency would be of major concern, it may automate things like emergency braking to avoid potential accidents. Similarly, emergency electronic brake-light may be another application.

*3) Post Crash Notification:* A vehicle involved in an accident would broadcast warning messages about its position to trailing vehicles so that it can take decision with time in hand as well as to the highway patrol for tow away support as depicted in Figure.

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

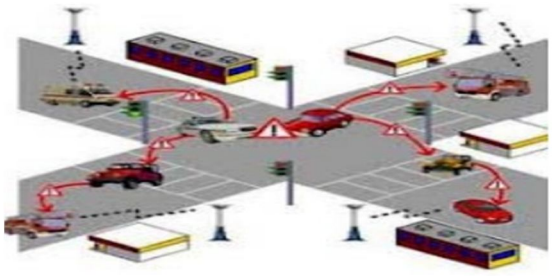

Fig3. Emergency Situation Notification

*4) Road Hazard Control Notification:* Cars notifying other cars about road having landslide or information regarding road feature notification due to road curve, sudden downhill etc.

*5) Cooperative Collision Warning:* Alerts two drivers potentially under crash route so that they can mend their ways [12].

*6) Traffic Vigilance:* The cameras can be installed at the RSU that can work as input and act as the latest tool in low or zero tolerance campaign against driving offenses [13].

*B. Commercial Applications*

Commercial applications will provide the driver with the entertainment and services as web access, streaming audio and video. The Commercial applications can be classified as:

*1) Remote Vehicle Personalization/ Diagnostics:* It helps in downloading of personalized vehicle settings or uploading of vehicle diagnostics from/to infrastructure**.**

*2) Internet Access:* Vehicles can access internet through RSU if RSU is working as a router.

*3) Digital Map Downloading:* Map of regions can be downloaded by the drivers as per the requirement before traveling to a new area for travel guidance. Also, Content Map Database Download acts as a portal for getting valuable information from mobile hot spots or home stations.

*4) Real Time Video Relay:* On-demand movie experience will not be confined to the constraints of the home and the driver can ask for real time video relay of his favorite movies.

*5) Value-Added Advertisement:* This is especially for the service providers, who want to attract customers to their stores. Announcements like petrol pumps, highways restaurants to announce their services to the drivers within communication range. This application can be available even in the absence of the Internet.

*C. Convenience Applications*

Convenience application mainly deals in traffic management with a goal to enhance traffic efficiency by boosting the degree of convenience for drivers. The Convenience applications can be classified as:

*1) Route Diversions:* Route and trip planning can be made in case of road congestions.

*2) Electronic Toll Collection*: Payment of the toll can be done electronically through a Toll Collection Point as shown in Figure 3. A Toll collection Point shall be able to read the OBU of the vehicle. OBUs work via GPS [14] and the on-board odometer or techograph as a back-up to determine how far the Lorries have travelled by reference to a digital map and GSM to authorize the payment of the toll via a wireless link. TOLL application is beneficial not only to drivers but also to toll operators.

*3) Parking Availability:* Notifications regarding the availability of parking in the metropolitan cities helps to find the availability of

slots in parking lots in a certain geographical area.

*4) Active Prediction:* It anticipates the upcoming topography of the road, which is expected to optimize fuel usage by adjusting the cruising speed before starting a descent or an ascent. Secondly, the driver is also assisted [15]. Figure 3. Electronic Toll Collection in India.

Fig 4. Electronic toll collection in india

*D. Productive Applications*

We are intentionally calling it productive as this application is additional with the above mentioned applications. The Productive applications can be classified as:

*1) Environmental Benefits:* AERIS research program [16] is to generate and acquire environmentally-relevant real-time transportation data, and use these data to create actionable information that support and facilitate "green" transportation choices by transportation system users and operators. Employing a multi-modal approach, the AERIS program will work in partnership with the vehicle-to-vehicle (V2V) communications research effort to better define how connected vehicle data and applications might contribute to mitigating some of the negative environmental impacts of surface transportation.

*2) Time Utilization:* If a traveler downloads his email, he can transform jam traffic into a productive task and read on-board system and read it himself if traffic stuck. One can browse the Internet when someone is waiting in car for a relative or friend.

*3) Fuel Saving:* When the TOLL system application for vehicle collects toll at the toll booths without stopping the vehicles, the fuel around 3% is saved, which is consumed when a vehicles as an average waits normally for 2-5 minutes.

## VI. OVERVIEW OF ROUTING PROTOCOLS [17]

| Type of Protocol | Topology Based | Position Based | Cluster Based | Geocast Based | Broadcast Based |
|---|---|---|---|---|---|
| Forwarding Technique | Wireless multi hop Forwarding | Heuristic Technique | Wireless multi Hop Forwarding | Wireless multi Hop Forwarding | Wireless multi Hop Forwarding |
| Strategy of Recovery | Multi Hop Forwarding | Carry & Forward approach | Carry & Forward approach | Flooding | Carry & Forward approach |
| Digital Map Requirement | No | No | yes | No | No |
| Virtual Infrastructure Requirement | No | No | yes | No | No |
| Realistic Traffic Flow | yes | yes | No | Yes | Yes |
| Scenario | Urban | Urban | Urban | Highway | Highway |

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

## VII. CONCLUSION

We have performed an extensive survey of various inter-vehicle communication applications and systematically classified them. This organizational approach permitted us to identify the communication requirements unique to each application type and focus on the most important protocol design issues that the developers are facing. We carefully reviewed these issues and illuminated the options using protocol examples taken from the past decade of research on IVC. Various applications were highlighted and used to analyze a representative set of protocols, which were classified by their architectural as well as relevance. Additional details on selected protocols appropriate to each of the defined application types are presented. We have also discussed some important strengths and weaknesses of current research.

## REFERENCES

[1] M. Wellens, B. Westphal P. Mahonen, Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios, IEEE Vehicular Technology Conference, VTC, 2007, pp 1167-1171.
[2] Spring, (2007) Status of Project IEEE 802.11p, http://grouper.ieee.org/groups/802/11/Reports/tg p_update.htm [Cited on: Sept. 2007], (2007).
[3] K. D. Wong, K. Tepe, W. Chen, M.Gerla, Inter vehicular communication, IEEE Wireless Communications, vol. 13, issue no. 5, October 2006, pp-6-7.
[4] P. Golle, D. Greene, and J. Staddon, ―Detecting and correcting malicious data in vanets,‖ in VANET ’04: Proceedings of the 1st ACM international workshop on Vehicular Ad hoc networks, (New York, NY, USA), pp. 29–37, ACM, 2004.
[5] Jason J. Haas, Yih-Chun Hu, Kenneth P. Laberteaux ―Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET‖ in VANET’09, September 25, 2009, Beijing, China. 2009 ACM.
[6] IEEE, IEEE 1609.2-Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages, available from ITS Standards Program.
[7] Ankita Agrawal , Aditi Garg , Niharika Chaudhiri , Shivanshu Gupta , Devesh Pandey , Tumpa Roy-Security on Vehicular Ad Hoc Networks (VANET) : A Review Paper , (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013.
[8] Kenneth P. Laberteaux, J.J. Haas, and Y.C.Hu, ―Security Certificate revocation list distribution for VANET‖. In VANET '08 Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking.
[9] M. Raya, P. Papadimitratos, I. Aad, D.jungels, and J.P. Habaux), ―Eviction of misbehaving and faulty nodes in vehicular networks‖, in IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks, vol. 25, num. 8, p. 1557-1568.
[10] Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi,‖ A Novel Defense Mechanism against Sybil Attacks in VANET‖, in Proceeding SIN '10 Proceedings of the 3rd international conference on Security of information and networks.
[11] M. Raya, Papadimitratos and J.P Habaux‖ Special issues on InterVehicular Communication.
[12] X. Yang, L. Liu and N. Vaidya, “A vehicle-to-vehicle communication protocol for cooperative collision warning,” 1st Annual International conference on Mobile and Ubiquitous Systems: Networking & Services, MOBIQUITOUS’04, pp. 114-123.
[13] http://www.teletrafficuk.com/products-concept-ii.htm.
[14] R. B. Thompson, “Global Positioning System (GPS): The Mathematics of Satellite Navigation,” MathCAD library, http://www.mathsoft.com/appsindex.html. 1998.
[15] www.scania.com.
[16] www.its.dot.gov/aeris.
[17] Pei, G., Gerla, M., and Chen, T.-W. (2000), “Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks,” Proc. ICC 2000, New Orleans, LA, June 2000.