VANETs (Vehicular Adhoc Networks): Introduction, Imperatives and Challenges

Dr. Rajesh Gargi, Sumit Goyal

***Abstract*— The integration of communication technology in state-of the art vehicles has begun years ago: Car phones and Internet access based on cellular technologies as well as Bluetooth adapters for the integration of mobile devices are popular examples. This paper presents an insight into the VANETs (Vehicular Ad-hoc NETworks) technology.**

This technology integrates WLAN/cellular and Ad Hoc networks to achieve the continuous connectivity. Vehicular Ad hoc Network (VANET), a subclass of mobile Ad Hoc networks (MANETs), is a promising approach for future intelligent transportation system (ITS). These networks have no fixed infrastructure and instead rely on the vehicles themselves to provide network functionality. However, due to mobility constraints, driver behavior, and high mobility, VANETs exhibit characteristics that are dramatically different from many generic MANETs. This paper provides a comprehensive study of challenges in these networks.

Index Terms*— *MANET, VANET.

I. INTRODUCTION

VANETs can be considered as a special case of MANETs (Mobile Adhoc networks) except that in VANETs the nodes present are basically vehicles which strictly follow the traffic rules and have highly complex and dynamic topology. The mobility of vehicles on road is restricted by factors like driving behavior of the driver as well as surrounding people, traffic jams, traffic signals, road-side mishap, unseen obstacles, free passage of emergency vehicles etc., thus the mobility patterns in vehicular network is restricted and is frequently changing. VANETs provide a tremendous potential for low latencies which means communication delay for message or packet transmission is quite low and hence helps in increasing the performance of system by allowing the network connection to remain active even if vehicles are moving at fast speeds and in dynamic topologies. Driving means changing location constantly. This means a constant demand for information on the current location and specifically for data on the surrounding traffic, routes and much more. This information can be grouped together in several categories. A very important category is driver assistance and car safety. This includes many different things mostly based on sensor data from other cars. One could think of brake warning sent from preceding car, tailgate and collision warning, information about road condition and maintenance, detailed regional weather forecast, premonition of traffic jams, caution to an accident behind the next bend, detailed information about an accident for the rescue team and many other things. One could also think of local updates of the cars navigation systems or an assistant that helps to follow a friend's car. Another category is entertainment for passengers. For example internet access, chatting and interactive games between cars close to each other. The kids will love it. Next category is local information as next free parking space (perhaps with a reservation system), detailed information about fuel prices and services offered by the next service station or just tourist information about sights. A possible other category is car maintenance. For example online help from your car mechanic when your car breaks down or just simply service information.

Figure1: Vanet Scenario

To realize communication in VANETs, the Federal Communications Commission (FCC) dedicated 75MHz of the frequency spectrum in the range 5.850 GHz to 5.925 GHz to be used for V2V and V2I communication. The 5.9 GHz spectrum was termed Dedicated Short Range Communication (DSRC) and uses IEEE 802.11p. VANET applications must share the allocated bandwidth, making it a scarce resource that should be managed very carefully.

II. DIFFERENCE BETWEEN VANET (IVC) AND MANET

MANETs are wireless multihop networks that lack infrastructure, and are decentralized and self-organizing while IVC systems satisfy all these requirements, and are therefore a special class of MANETs. While most MANET articles do not address specific applications, the common assumption in MANET literature is that MANET applications are identical (or similar) to those enabled by the Internet. In contrast, IVCs have completely different applications. An important consequence of the difference in the applications is the difference in the addressing modes. MANET applications

Dr. Rajesh Gargi Director, Geeta Engineering College, Naultha, Panipat,

Sumit Goyal Pursuing the M.tech degree in computer science Engineering from the Geeta Engineering College.

require point-to-point (unicast) with fixed addressing that is, the recipient of a message is another node in the network specified by its IP address.IVC applications often require dissemination of the messages to many nodes (multicast) that satisfy some geographical constraints and possibly other criteria (e.g., direction of movement). The need for this addressing mode requires a significantly different routing paradigm. In MANETs, the nodes are assumed to have *moderate mobility*. This assumption allows *MANET* routing protocols (e.g., Ad Hoc On Demand Distance Vector, AODV) to establish end-to-end paths that are valid for a reasonable amount of time and only occasionally need repairs. In IVC applications due to the high degree of mobility of the nodes involved, even multi-hop paths that only use nodes moving in the same direction on a highway have a lifetime comparable to the time needed to discover the path. In MANETs, the random waypoint (RWP) is (by far) the most commonly employed mobility model. However, for IVC systems, most existing literature recognized that RWP would be a very poor approximation of real vehicular mobility; instead, detailed vehicular traffic simulators are used. While in MANETs a significant body of literature is concerned with power-efficient protocols, IVC enjoys a practically unlimited power supply.

III. VANET: Imperatives & Challenges

A. *Applications Of VANET*

The three major classes of applications possible in VANET are safety oriented, convenience oriented and commercial oriented.

a) ***Traffic Application*** This application intends to improve the driving efficiency and comfort on roads by means of communications. Driving efficiency applications intend to optimize the traffic flow on roads, i.e. minimizing the travel time by disseminating information about traffic flow conditions on roads. By this the packet delivery ratio and throughput can be increased due to which the driving efficiency is increased.

b) ***Safety Application*** Safety applications represent one of the most important groups of VANET applications. The goal of these applications is to reduce the number of injuries and fatalities of road accidents. To achieve this goal, safety applications disseminate information about hazardous situations (e.g. about abnormal road conditions or post-crash warning) to vehicles which can benefit from such information to avoid an accident. Security of message content is one issue in vehicle to vehicle communication. Authentication service is concerned with communication between different vehicles. The integrity service concerned with security deals with stability of a stream of messages. An important feature of VANET security is digital signature.

c) *Commercial Application* Commercial applications provide communication services like entertainment, web access and advertisement. Examples are remote vehicle diagnostics, video streaming, and map download for the navigation system. In contrast to the previously discussed types of applications, commercial applications mostly rely on unicast communication and require a much higher bandwidth than the two other application groups.

B. *Unique VANET Characteristics:*

a) Potentially high number of nodes Regarding VANETs as the technical basis for envisioned intelligent transportation system (ITS) we expect that a large portion of vehicles will be equipped with communication capabilities for vehicular communication. Taking additionally potential roadside units into accounts, VANET needs to be scalable with a very high number of nodes.

b) High mobility and frequent topology changes Nodes potentially move with high speed. Hence in certain scenarios such as when vehicles pass each other, the duration of time that remains for exchanging of data packets is rather small.

c) High application requirement on data delivery Important VANET applications are for traffic management to avoid road accidents, potentially including safety of life. These applications have requirements with respect to real time and reliability. An end-to-end delay of seconds can render safety information meaningless.

d) No confidentially of safety information For safety application, the information contained in a message is of interest for all road users and hence not confidential.

C. *Challenges In VANET*

Vehicular traffic is a major problem in developed societies. Every day huge amounts of time and resources are wasted due to traffic congestion. Traffic management improves the driving efficiency and comfort on roads by means of communications. In vehicles, navigation is also one of the traffic applications that are designed to reduce the driving time and fuel consumption by exchanging real time information about traffic conditions in driving route. Also applications like traffic jam detection or travel time estimation for road segments can be utilized for example information about traffic jam in advance and then by knowing this information alternate route can be choose. This can reduce the travel time. Thus a successful use of traffic application could greatly reduce the fuel consumption of vehicles which in turn reduce the cost and CO2 emission. Parking lot payment is an OBU to RSU non-safety application that provides benefit to parking lot operators, simplify payment for customers, and reduce congestion at entrance and exits of parking lots. A challenging issue in VANET is congestion control. The network is based on end to end transfer of packet data but sometimes in vehicle to vehicle contact congestion problem arises. In the case of congestion, the source reduces its data rate during delivery of packet. However in VANET the topology changes within seconds and a congested node used for forwarding a few seconds ago might not be used at all at the point in time when the source reacts to the congestion. Thus, some schemes must be proposed where each node locally adapts to the available bandwidth. VANET is one of the best approaches to improve the traffic efficiency and to improve the travel comfort for drivers and passengers. Different protocols are introduced by researches to optimize the traffic management applications. All the protocols show the good performance by utilizing the vehicle location and traffic information to forward messages. However some protocols need to be modified for better results. Hence different aspects related with traffic like congestion control, traffic efficiency, travel time, route

mapping, fuel consumption are considered while designing the new protocol or during modification of existing protocol. Also in VANET, the route for sending data may often be changed due to VANET topology that is changed all the time and can be highly dynamic. Every node in the same area will use the same access channel, causing the congestion due to sending a large amount of various packets (both Control packet and Data packet) within the network, which causes communication efficiency to decrease Therefore, finding the route in the area where the high congestion exists could be efficient. The shortest route could be found out to overcome this problem that is economical, fastest and efficient.

a) ***Mobility*** The basic idea from Ad Hoc Networks is that each node in the network is mobile, and can move from one place to another within the coverage area, but still the mobility is limited, in Vehicular Ad Hoc Networks nodes moving in high mobility, vehicles make connection throw their way with another vehicles that maybe never faced before, and this connection lasts for only few seconds as each vehicle goes in its direction, and these two vehicles may never meet again. So securing mobility challenge is hard problem.

b) ***Volatility*** The connectivity among nodes can be highly ephemeral, and maybe will not happen again, Vehicles traveling throw coverage area and making connection with other vehicles, these connections will be lost as each car has a high mobility, and maybe will travel in opposite direction. Vehicular networks lacks the relatively long life context, so personal contact of users device to a hot spot will require long life password, and this will be impractical for securing VC.

c) ***Network Scalability*** The scale of this network in the world approximately exceeding the 750 million nodes, and this number is growing, another problem arise when we must know that there is no a global authority govern the standards for this network, for example: the standards for DSRC in North America is deferent from the DSRC standards in Europe, the standards for the GM Vehicles is deferent from the BMWone.

d) ***Bootstrap*** At this moment only few number of cars will be have the equipment required for the DSRC radios, so if we make a communication we have to assume that there is a limited number of cars that will receive the communication, in the future we must concentrate on getting the number higher, to get a financial benefit that will courage the commercial firms to invest in this technology.

e) **Authentication** In VC every message must be authenticated, to make sure for its origin and to control authorization level of the vehicles, to do this vehicles will assign every message with their Private Key along with its Certificate, at the receiver side, the vehicle will receive the message and check for the key and certificate once this is done, the receiver verifies the message. Signing each message with this, causes an overhead, to reduce this overhead we can use the approach ECC (Elliptic Curve Cryptography), the efficient public key cryptosystem.

f) **Availability** Vehicular Network must be available all the time, for many applications Vehicular Networks will require realtime, these applications need faster response from Sensor Networks or even Ad Hoc Network, a delay in seconds for some applications will make the message meaningless and maybe the result will be devastating. Attempting to meet real-time demands makes the system vulnerable to the DoS attack. In some messages, a delay in millisecond makes the message meaningless; the problem is much bigger, where the application layer is unreliable, since the potential way to recover with unreliable transmission is to store partial messages in hopes to be completed in next transmission.

g) **Non-repudiation** Non-repudiation will facilitate the ability to identify the attackers even after the attack happens. This prevents cheaters from denying their crimes. Any information related to the car like: the trip rout, speed, time, any violation will be stored in the TPD, any official side holding authorization can retrieve this data

h)**Privacy** Keeping the information of the drivers away from unauthorized observers, this information like real identity, trip path, speed etc.The privacy could be achieved by using temporary (anonymous) keys, these keys will be changed frequently as each key could be used just for one time and expires after usage ,all the keys will be stored in the TPD, and will be reloaded again in next time that the vehicle makes an official checkup .For preserving the real identity of the driver, an ELP (Electronic License Plate) is used, this license is installed in the factory for every new vehicle, it will provide an identification number for the vehicle, to identify the vehicle in anywhere , with the RFID technology to hold the ELP.

i) **Confidentiality** The privacy of each driver must be protected; the messages should be encrypted to prevent outsiders from gaining the drivers information.

IV. Conclusions and Future Perspectives

This paper presents a state of the art survey in networking challenges in vehicular ad hoc network which is a promising technology for intelligent transportation system (ITS). Although many problems are not yet solved, the general feeling is that vehicles could benefit from spontaneous wireless communications in a near future, making VANETs (Vehicular Ad-Hoc Networks) a reality. For being practical, it is needed that research and industry community come to agreement about a MAC technology. The trend is toward an extension of IEEE 802.11 called DSRC. Because of the emergency of safety messages and their strict QOS requirement, there is a severe need to optimum methodologies for service differentiation and admission control. Due to limited bandwidth of channel, there is need for some techniques for controlling the amount of data sent to the network. This problem addressed as congestion control. Since the mobility of VANETs cannot be captured by general mobility models of MANETs, special mobility models by making use of traffic flow theory should be proposed. So the simulation results could be trustable .Since experimental evaluation of VANETs is expensive, simulation technique should be improved. There are some works attempting to conduct co-simulation. In this case two or three simulators,

simulate network and traffic characteristics and driver behavior.

REFERENCES

[1] Carlos de morais corderio and Dharma P.Agarwal "Mobile Adhoc Networking",OBR research center for distributed and mobile computing,University of Cincinnati, USA.

[2] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester "An Overview of Mobile Ad Hoc Networks: Applications and Challenges"

[3] Mobile Ad-hoc Networks (MANETs) Working Group,http://www.ietf.org/html.characters/MANETs-character.html, 2004.

[4]Lars Wischhof and Hermann Rohling, "Congestion Control in Vehicular Adhoc Networks", IEEE International conference on Vehicular Electronics and Safety, pp 58-63, 2005.

[5]Car-to-Car communication consortium http://www.car-2-car.org/

[6] Saleh Yousefi, Mahmoud Siadat Mousavi, Mahmood Fathy, " Vehicular Ad Hoc Networks (VANETs):Challenges and Perspectives",2006 6th international Confrence.

[7] M Raya, P Papadimitratos, JP Hubaux, " Securing Vehicular Communications ", IEEE Wireless Communications.

[8] Ahren Studer, Fan Bai, Bhargav Bellur, Adrian Perrig, March 14, 2008 "Full Paper: Flexible, Extensible, and Efficient VANET Authentication"

[9] Kusum Dalal Prachi Chaudhary Dr. Pawan Dahiya, "Performance Evaluation of TCP and UDP Protocols in VANET Scenarios using NCTUns-6.0 Simulation Tool", International Journal of Computer Applications Volume 36– No.6, December 2011

[10] www.wikipedia.com

[11] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges"

[12] GMT Abdalla, SM Senouci " Current Trends in Vehicular Ad Hoc Networks".

Sumit Goyal Pursuing the M.tech degree in computer science Engineering from the Geeta Engineering College**.**