

A Comprehensive Survey on Vehicular Ad Hoc Networks and Its Access Technologies

Manoj Goyal

Assistant Professor

Dept. of Electronics and Comm Engineering, KCT College of Engg. & Tech, Sangrur, Punjab

Abstract: VANETs, or Vehicular Ad-Hoc Networks have recently gained scientific and commercial interest. In fact, they have drawn many people from Mobile Ad-Hoc Networks (MANETs) field. In this paper we discuss the Vehicular Ad-Hoc Networks from our perspective. In detail, we will discuss the characteristics, routing and security of vehicular ad-hoc network and also look after the MANET/VANET comparison.

I. INTRODUCTION

Vehicular Ad-Hoc Networks (VANETs) are wireless networks between vehicles. Recently, they have attracted increasing scientific interest from the wireless networking community. This is, on one hand, due to the car manufacturing industry's determination to roll out vehicle to vehicle communication in the near future and, on the other, to the increasing disillusionment concerning the need for the vast number of protocols developed for general Mobile Ad-Hoc Networks (MANETs) in the past few years. In the case of VANETs, industry pressure has created a situation in which an overwhelming interest in solutions to problems leads to a preference for real-world research as opposed to fancy theory. the potential achievement of VANETs research lies on the development of vehicular communication system that enables convenient, stable and economical distribution of data to benefit the safety and comfort "on the road". Among various communication applications in VANETs, there is a wide range of important applications involving traffic safety, traffic monitoring and unpiloted vehicles applications demand time restraint communication in Ad Hoc wireless networks. In this paper, we talk about the history of Vehicular Ad-Hoc Networks.

II. MANET Vs VANET

When we entered VANET research with the FleetNet project in mid-2001, ad-hoc research was largely dominated by efforts to standardize MANET protocols in the same-named IETF working group. Consequently, these protocols were tailored to transporting IP unicast datagrams, enabling the variety of IP applications to be run transparently over these networks. A MANET is a mobile ad-hoc network based on a wireless network. It is self-configuring which means that the network is built up by the nodes of the network themselves without a super ordinate instance. This also means that all the information about the topology has to be collected and stored by the nodes themselves. Two examples for ad-hoc networks are shown in Figure. The nodes in such networks can be every kind of wireless-equipped device. These nodes thereby function as sender and receiver as well as routers - intermediate nodes -for packets sent by other nodes. The data flow between sender and receiver is controlled by special routing protocols, which are able to handle the movement of nodes and topology changes, which is typical for MANETs. Therefore those protocols build up so called routing tables, in which the information collected by the protocol is stored.

VANET is a special class of Mobile Adhoc Networks (MANET), in which the nodes are the vehicles which communicate with other vehicles or with the base station which acts as a roadside infrastructure for using security and services application. Though the nodes are mobile in VANETs as well as MANETs, the mobility in VANET is constrained to the boundaries of the road unlike the nodes in MANETs, where movement is more random in nature. Nodes in VANET are also characterized by high node mobility and fast topology changes. Unlike MANET, power is not of great concern in VANETs as the vehicle batteries have sufficient and rechargeable power. The concept of network vehicle was first proposed by a team of engineers from Delphi Delco Electronics Systems and IBM corporation in the year 1998. The central characteristics of VANETs are the higher amount of nodes and the fact, that the routing protocols have to handle much higher velocities, which results in much more frequent topology changes. As a result, the routing tables have to be updated much more frequently than in ordinary MANETs. A VANET consists of vehicles and roadside base stations that exchange primarily safety messages.

III. CHARACTERISTIC OF VANET

With the development of Intelligent Transportation System (ITS), Vehicular Ad-hoc Networks (VANETs) become an emerging research area. As a specific type of MANETs, VANETs have some similar characteristics to MANETs, e.g. short radio transmission range, low bandwidth, omni-directional broadcast and limited storage capacity.

In addition to these similarities the communication in VANETs has some particular characteristics.

- i) Rapid topology changes;
- 2) Frequent network partition;
- 3) Small effective network diameter;
- 4) Limited redundancy in time and in function.
- 5) Position predictability
- 6) Relatively sufficient power

Position predictability and relatively sufficient power may be utilized to give support to intervehicle and vehicle-to-roadside communication, with rapid topology changes, frequent network partition, small effective network diameter and limited redundancy in time and in function aggravate the difficulties to communication in VANETs.

IV. ROUTING IN VANET

Routing is used forward data or information in a network. In the area of VANETs, special routing protocols have to be applied to handle the typical characteristics of those types of networks, these include the lack of a central control instance, movement of the nodes and frequent changes of the topology. To be able to handle those problems, several routing strategies

have been developed. They can be classified into two main types of routing protocols i. e. position-based routing and topology-based routing.

Position-Based Routing

Position-based routing protocols function by means of node positions which are provided by a so called location service - for example the grid location service . To retrieve the node positions, a location service in general uses the global positioning system (GPS). Based on this information the route between sender and receiver is determined.

Topology-based routing

Topology-based routing protocol use the neighborhood of the nodes in the network to find a route from the sender to the receiver. Therefore, in addition to the routing tables, neighbor tables are built up to collect and store this neighborhood information. The main difference compared to position-based routing strategies is that the routes are determined before the data packet is finally sent. Topology-based routing protocols can be further divided into:

Proactive routing strategies

A proactive routing protocol determines the routes between two nodes in advance and even if they may not be needed. The advantage is that there is no delay before sending a data packet - but the negative side is that there is much overhead needed to determine all the routes and to store routes which may never be used, because the nodes on this route never send or receive anything. Examples of proactive routing strategies are distance-vector routing and link state routing.

Reactive routing strategies

Reactive routing protocols in contrast determine the route to a certain node if and only if it is needed. The advantage is that the overhead to store routes is kept minimal because there are no routes which are determined to no purpose. The disadvantage however is that there is a delay before the first packet on this route can be sent, because the route has to be determined first, for all subsequent packets this delay is missing. A sample protocol is AODV.

Hybrid routing strategies

This third type of topology-based routing protocols combines the two strategies mentioned above with the intention to combine the advantages of both.

V. THREATS V/S SECURITY

The prime concern that has plagued many VANET researchers is the security of these networks. Take an example of two cars moving on a single lane on a road. The car that is trailing behind can send a false message saying that there is a jam ahead due to a crashed car. The car in front on receiving this message may believe this message to be true and take a decision to leaving a less-traffic road for the malicious driver behind. This is one possible misuse of the several applications talked about here. Similar misuse can create in systems where safety is of primary concern. An obvious solution that has been looked into is asymmetric key based authentication. Few other possible attacks that have been considered as a threat to these networks are bogus information attack or disruption of network operation by jamming the wireless channel which leads to denial of service (DoS). There can also be attacks like cheating attack where identities, speed or position can be faked. Identity disclosure attack can be performed by a global observer who has an access to all the data gathered through these networks.

Security: The main challenge in providing security in VANET depends on privacy, trust, cost and gradual deployment. Some existing security tools in some countries include electronic licenses plates (ELP), which are cryptographically security issues of the network like key distribution, certificate revocation etc., event data recording by which important parameter can be registered during abnormal situation like accidents etc. Tamper proof hardware is essential for storing the cryptographic material like ELP and VPKI keys for decreasing the possibility of information leakage. To keep a tap on bogus information attack, data correlation techniques are used. To identify false position information, secure positioning techniques like verifiable multi alteration is commonly used.

VI. VANET'S APPLICATIONS

The three major classes of applications possible in VANET are safety oriented, convenience oriented and commercial oriented which can be discussed as below.

Safety Application: Safety applications will monitor the surrounding road, approaching vehicles, surface of the road, road curves etc. They will exchange messages and co-operate to help other vehicles out under such scenario. Though reliability and latency would be of major concern, it may automate things like emergency braking to avoid potential accidents. Safety applications would be Slow/Stop Vehicle Advisor in which a slow or stationary vehicle will broadcast warning message to its neighborhood. Another similar type of application is emergency electronic brake-light . In Post Crash notification a vehicle involved in an accident would broadcast warning messages about its position to other vehicles so that it can take decision with time in hand as well as to the highway patrol for tow away support. Road Hazard Control Notification deals with cars notifying other cars about road having landslide.

Convenience Application: Convenience application will be mainly of traffic management type. Such as Congested Road Notification (CRN) detects and notifies about road congestions which can be used for route and trip planning. TOLL is yet another application for vehicle toll collection at the toll booths without stopping the vehicles. Parking Availability Notification (PAN) helps to find the availability of slots in parking lots in a certain geographical area. The ultimate goal of these application to be enhance traffic efficiency by boosting the degree of convenience for drivers.

Commercial Application: Commercial applications will provide the driver with the entertainment and services as web access, streaming audio and video. Such as Remote Vehicle Personalization / Diagnostics helps in downloading of personalized vehicle settings or uploading of vehicle diagnostics from/to infrastructure. Service Announcements would be of particular interest to roadside business like petrol pumps, highways restaurants to announce their services to the drivers within communication range. Content Map Database Download acts as a portal for getting valuable information from mobile hotspots or home stations.

VII. CONCLUSION

VANET is definitely something to lookout for in the future. A lot of theoretical work has been put into realizing these networks and few experiments has been performed to validate this theory as cost of setting up this architecture is high, but more such efforts can be expected in near

future. A successful vehicular network will open a lot of services to a huge number of audience which will turn out to be life saving as well as fun.

REFERENCES

- [1] “The FleetNet Project Homepage”<http://www.et2.tu-harburg.de/fleetnet>
- [2] Holger Füßler ,Sascha Schnauffer ,Matthias Transier, Wolfgang Effelsberg “Vehicular Ad-Hoc Networks: From Vision to Reality and Back” 4th Annual IEEE/IFIP Conference on Wireless On Demand Network Systems and Services (WONS), Obergurgl, Austria, January 2007
- [3] Mainak Ghosh & Sumit Goswami, “Intelligent Transportation using VANET ”.
- [4] Yizhou Zhang,” Real-time Communication in Vehicular Ad Hoc Networks (VANETs) ” Trinity College, Sept. 2006.
- [5] Sze-Yao Ni, Yu-Chee Tseng, Yuh-Shyan Chen, and JangPing Sheu.. "The broadcast storm problem in a mobile ad hoc network." In: Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp 151162, Aug 1999.