IJCSC International Journal of Computer Science & Communication Vol. 1, No. 2, July-December 2010, pp. 399-403

Various Issues in Vehicular Ad hoc Networks : A Survey

Shinde S. S.[1] **& Patil S. P**[2]

[1,2]Annasaheb Dange College of Engineering & Technology, Ashta 416301, India
Email: [1]shindesunita@yahoo.co.in, [2]sanj22ony@yahoo.co.in

ABSTRACT

Vehicular Ad Hoc Networks is a kind of special wireless ad hoc network, which has the characteristics of high node mobility and fast topology changes. The Vehicular Networks can provide wide variety of services, ranges from safety and crash avoidance to Internet access and multimedia applications. So a lot of work and research is being conducted to study problems related to the vehicular communications. These problems include network architecture, protocols for physical and link layers, routing algorithms, as well as security issues. In this article we provide a review for the researches related to Vehicular Ad Hoc

Keywords: Vehicular Ad Hoc Networks, Mobility, Vehicular Communication, Protocols

1. INTRODUCTION

Nowadays, communications become essential in the information society. Everyone can get information anywhere, even in mobility environments, using different kinds of devices and communication technologies. Vehicles are other places where the people stay during long periods too. Millions of people around the world die every year in vehicle accidents and many more are injured. Implementations of safety information such as speed limits and road conditions are used in many parts of the world but still more work is required. Vehicular Ad Hoc Networks (VANET) should, upon implementation, collect and distribute safety information to massively reduce the number of accidents by warning drivers about the danger before they actually face it. Such networks consist of sensors and On Board Units (OBU) installed in the vehicle as well as Road Side Units (RSU). The data collected from the sensors on the vehicles can be displayed to the driver, sent to the RSU or even broadcasted to other vehicles depending on its nature and importance. The RSU distributes this data, along with data from road sensors, weather centers, traffic control centers, etc to the vehicles and also provides commercial services such as parking space booking, Internet access and gas payment. The network makes extensive use of wireless communication to achieve its goals but although wireless communications reached a level of maturity, a lot more is required to implement such a complex system. Most available wireless systems rely on a base station for synchronization and other services; however using this approach means covering all roads with such infrastructure which is impractically too expensive. Ad hoc networks have been studied for some time but VANET will form the biggest ad hoc network ever implemented, therefore issues of stability, reliability and scalability are of concern. VANET therefore is not an architectural network and not an ad hoc network but a combination of both.

This paper is organized according to following structure: Section 2 explains the history of VANET systems. The main characteristics and applications of Vehicular Ad Hoc Networks are described in section 3. Section 4 describes IEEE WAVE standard for vehicular communications. The fifth part presents the review of the routing algorithms for VANET. A discussion about security issues in section six, and then finally the paper is concluded.

2. HISTORY OF VEHICULAR COMMUNICATION

The original motives behind vehicular communications were safety on the road, many lives were lost and much more injuries have been incurred due to vehicle crashes. A driver realizing the brake lights of the vehicle in front of him has only a few seconds to respond, and even if he has responded in time vehicle behind him could crash since they are unaware of what is going at the front. This has motivated one of the first applications for vehicular communications, namely cooperative collision warning which uses vehicle to vehicle communication [1]. Other safety applications soon emerged as well as applications for more efficient use of the transportation network, less congestion and faster and safer routes for drivers. These applications cannot functions efficiently using only vehicle to vehicle communications therefore an infrastructure is needed in the form of RSU. Although safety applications are important for governments to allocate frequencies for vehicular communications, non-safety applications are as important for Intelligent Transportation Systems (ITS) [2].

Besides road safety, new applications are proposed for vehicular networks, among these are Electronic Toll Collection (ETC), car to home communications, travel and tourism information distribution, multimedia and game applications just to name a few. However these applications need reliable communication equipment which is capable of achieving high data rates and stable connectivity between the transmitter and the receiver under high mobility conditions and different surroundings.

3. VANET COMPONENTS & FEATURES

A VANET consists of vehicles and roadside base stations that exchange primarily safety messages to give drivers the time to react to life-endangering events [3]. A vehicle in a VANET is equipped with processing, recording and positioning features and is capable of running wireless security protocols [4] as shown in Fig.1.

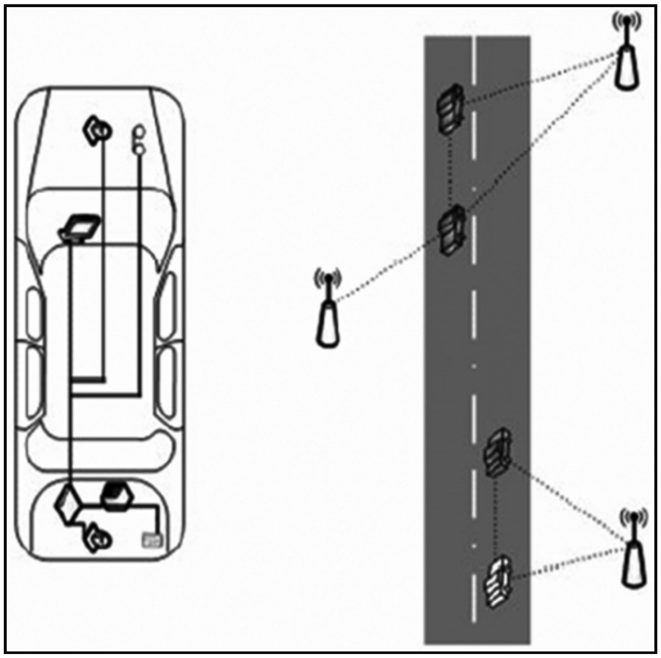

Fig.1: VANET,s Architecture

3.2. Features

Though vehicular ad hoc networks share general features with conventional ad hoc networks, VANETs have individual characteristics that are decisive in the design of the communication system [6], these include:

(i) Dynamic topology, *(ii)* Mobility models, *(iii)* Infinite energy supply and *(iv)* Localization functionality.

3.3. Applications

VANETs enable vehicle-to-vehicle *(v2v)* and vehicle-to infrastructure *(v2i)* communication, thus communicating nodes are either vehicles or base stations that can exchange information about traffic issues, road conditions and added value information. According to several authors: [3], [5], [6]) VANET's applications are commonly classified as follows:

- Warning: to prevent detected risky situations.
- Traffic management: to inform about traffic events.
- Added value: to provide numerous services (i.e. Internet).

4. IEEE STANDARDS

While ASTM E2213 standard is being developed, the IEEE standards IEEE P1609.1, P1609.2, P1609.3 and P1609.4 were prepared for vehicular networks. P 1609.3 is still under further development but the other three were recently released for trial use. P1609.1 is the standard for Wireless Access for Vehicular Environment (WAVE) Resource Manager. It defines the services and interfaces of the WAVE resource manager application as well as the message and data formats. It provides access for applications to the rest of the architecture. P1609.2 defines security, secure message formatting, processing, and message exchange. P1609.3 defines routing and transport services. It provides an alternative for IPv6. It also defines the management information base for the protocol stack. P1609.4 covers mainly how the multiple channels specified in the DSRC standard should be used. The WAVE stack uses a modified version of IEEE 802.11a for its Medium Access Control (MAC) known as IEEE 802.11p [7, 8]. The protocol architecture defined by IEEE is shown in Fig. (2) and the WAVE standards in Fig. (3) [8].

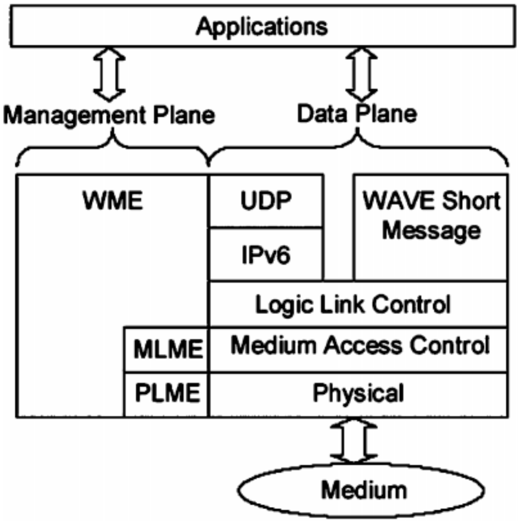

Fig.2: IEEE Architecture

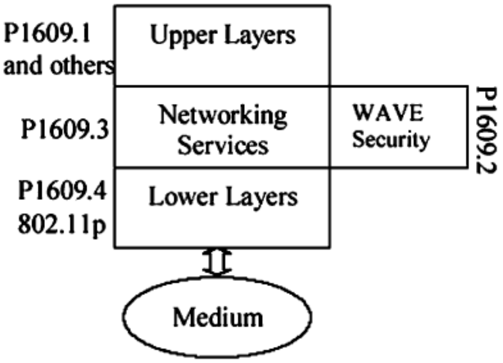

Fig. 3: WAVE Standards

5. ROUTING ALGORITHMS

Routing has always been a challenge in ad hoc networks (MANET). Moreover the movement in VANET is constraint by the road and highly predictable which is not the case in MANET where the mobility is random and in two dimensions.

Broadcasting and routing algorithms for VANET were studied in FleetNet project. Their focus was on using the positioning information provided by GPS for routing and broadcasting. Three routing protocols were considered,

- Position Based Forwarding (PBF),
- Contention Based Forwarding (CBF)
- Ad hoc On Demand Distance Vector (AODV).

All these protocols are reactive protocols. Reactive protocols discover the route to a destination only when a message is to be delivered counter to proactive protocols which tend to store routing tables for every destination and update these routing tables continuously.

As the topology of VANET changes frequently, the signaling messages of proactive protocols can result in a large overhead load.

- PBF and CBF use location service algorithms to find the position of the destination, based on this position PBF selects one of the surrounding nodes to forward the message. This process is repeated till the message reaches it destination.
- In CBF the source transmits the message with the position of the destination; every node receiving the message sets a timer proportional to the difference between its position and the destination. If the timer expires and no other node has broadcasted the message, the node forwards the message to the destination.
- In AODV the source floods the network with a route request for the destination. Nodes receiving the request calculate a distance vector and forward the message, this process is repeated till the destination is reached which sends a route reply. Once the reply is received the route is ready for sending the data. To reduce the flooding effects maximum hop count and Time To Live (TTL) fields are used in route messages.

Simulations show that CBF performs better than the other algorithms and it adapts to changes in the topology which interrupt routes in the other two protocols. CBF, however, requires the assistance of maps in cities when multiple roads intersect and run in parallel, its performance in congested areas also requires more investigation since several cars might have the same distance to the destination which might cause collisions [9, 10]. A broadcasting algorithm based on CBF has also been suggested for safety applications. A car encountering an accident broadcasts a safety message and its current position. Other cars receiving this position. Other cars receiving this message set a retransmission timer inversely proportional to their distance from the source and rebroadcast the message if no other node broadcasts first and keeps rebroadcasting till it receives a message from another node or the message is no longer relevant [11].

Another routing algorithm known as Greedy Traffic Aware Routing (GyTAR) has also been proposed in [12]. The algorithm targets the routing problem in cities. It works with the aid of maps and traffic density information to calculate the best direction in junctions the packet should take to reach its destination. The calculation is based on the distance, number of cars within that distance, their movement and speed. The paper also proposed a system for collecting and distributing information about the road and traffic conditions which can be used with GyTAR as well as other algorithms.

Although these algorithms, and others, provide a solution to the routing problem in VANET, still more research is required to examine their performance, applicability and overhead. A major issue of concern is the achievable throughput of the system. This has been examined in [13]. According to their results the throughput decreases considerably with the number of hops and can be as low as 20kbps in 2Mbps links with 6 hops.

6. SECURITY ISSUES

Most of the critical messages in VANETs are broadcast oriented safety messages that should have a deep penetration and should be delivered in a short time. Additionally these messages must be secure and must not leak personal, identifying, or linkable information to unauthorized parties, as the owners of the vehicles involved in the communication have a right to privacy.

Attacks can be sending bogus information, cheating with position information, tracking a location of a vehicle, jamming the channel for Denial of Service and pretending to be another vehicle [14]. A security system in VANETs must have the following features:

- *Authentication:* There can be malicious and genuine sources for messages in VANETs. Authentication is the ability to distinguish between these sources.
- *Data Integrity:* The data received are exactly as sent by the authorized entity without any modification. Senders can be legitimate while the message contains false data.
- *Anonymity:* The physical identity of the originator of a message should not be easily identifiable from the message.
- *Availability:* Availability of the channel should be supported when the system is under Denial-of-Service attacks like channel jamming.
- *Low Overhead:* The messages being time critical, the security overheads should retain the usefulness of the message.
- *Privacy:* The privacy of drivers against unauthorized observers must be guaranteed unless there is a judge order.
- *Real-time Constraints:* A slow security system should not harm the real-time constraints of VANETs.

In addition, general security architectures without specific protocols are proposed in literature [15-16]. The use of digital signatures in the vehicular environment is discussed in [17]. Methods to detect and correct malicious data are proposed in [18].

7. CONCLUSION

As a result of the substantial advances in the wireless technology, vehicles are becoming a part of the global network. In this paper we have provided an overview of the development of the communication standards and ongoing research for vehicular networks. 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 a reality. Vehicular networks will not only provide safety and life saving applications, but they will become a powerful communication tool for their users.

REFERENCES

[1] "ITS Applications Overview," http://itsdeployment2.ed.ornl.gov/technology overview/.

[2] K. Matheus, R. Morich, and A. Lübke, "Economic Background of Car to Car Communication," http://www.network–on–wheels.de/documents.html, 2004.

[3] M. Raya and J.-P. Hubaux, "The Security of Vehicular Ad hoc Networks," in SASN '05, (New York, NY, USA), pp. 11–21, ACM, 2005.

[4] J. Hubaux, S. Capkun, and J. Luo, "The Security and Privacy of Smart Vehicles," *Security and Privacy, IEEE*, **2**, No.3, pp. 49–55, May-June 2004.

[5] A. Zanella and E. Fasolo, "Inter-vehicular Communication Networks: a Survey," *in 2nd Internal NEWCOM Workshop*, 2006.

[6] K. Plossl, T. Nowey, and C. Mletzko, "Towards a Security Architecture for Vehicular Ad hoc Networks," *in ARES'06*, p. 8, 20-22 April 2006.

[7] "IEEE Draft P802.11p/D2.0, November 2006".

[8] "IEEE Draft P1609.0/D01, February 2007".

[9] M. TorrentMoreno,A. Festag, and H. Hartenstein, "System Design for Information Dissemination in VANETs," *in 3rd International Workshop on Intelligent Transportation(WIT)*, Hamburg, Germany, March 2006, pp. 2733.

[10] M. TorrentMoreno,F. Schmidt Eisenlohr, H. Füßler, and H. Hartenstein, "Packet Forwarding in VANETs, the Complete Set of Results," Dept. of Computer Science Universität Karlsruhe (TH) 2006.

[11] M. Meincke, P. Tondl, M. Dolores, P. Guirao, and K. Jobmann, "Wireless Adhoc Networks for InterVehicle Communication," in Zukunft der Netze-Die Verlezbarkeit meistern, 16. DFNArbeitstagung\über Kommuni kationsnetze: GI, 2002.

[12] M. Jerbi, S.-M. Senouci, and Y. GhamriDoudane, "Towards Efficient Routing in Vehicular Ad Hoc Networks," in UBIROADS 2007 Workshop, GIIS Marrakech, Morocco:IEEE, July 2007.

[13] M. Mabiala, A. Busson, and V. e. V'eque, "On the Capacity of Vehicular Ad Hoc Networks," *in UBIROADS 2007 Workshop*, GIIS Marrakech, Morocco: IEEE, July 2007.

[14] J.P. Hubaux, S. Capkun, and J. Luo, "The Security and Privacy of Smart Vehicles.," *in Proc. of the IEEE Security and Privacy Magazine*, **2**, May-June 2004, pp. 49-55.

[15] M. Raya and J.P. Hubaux, "The Security of Vehicular Ad hoc Networks," *Proceedings of the SASN05*, November 2005.

[16] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security Issues in a Future Vehicular Network.," *in Proc. of the European Wireless Conference*, 2002.

[17] L. Gollan and C. Meinel, "Digital Signatures for Automobiles?!," *Wireless and Optical Communications*, 2002.

[18] P. Golle, D. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in Vanets," in *Proc. of the 1st ACM International Workshop on Vehicular Adhoc Networks*, ACM Press, 2004, pp. 29-37.