Asian Journal of Information Technology 12 (11-12): 387-390, 2013
ISSN: 1682-3915

Vehicular Ad Hoc Networks: Characteristics, Application and Standards

[1]S. Prabhadevi and [2]A.M. Natarajan
[1]Department of Computer Science and Engineering, Nandha Engineering College, Erode, India
[2]Bannari Amman Institute of Technology, Sathyamangalam, India

Abstract: Vehicular networks or Vehicular Ad Hoc Networks (VANETs) are likely to become the most relevant form of mobile ad hoc networks. Vehicular ad hoc networks are one of the most interesting research areas due to high node mobility and fast topology changes. They can provide a wide variety of services ranging from safety-related warning systems to improved navigation mechanisms as well as information and entertainment applications. These diversified applications give rise to a lot of challenges including network architecture, vanet communication protocol, routing mechanisms as well as security issues. In this study, researchers review the standardization work and researches related to vehicular networks and discuss the challenges facing future vehicular networks.

Key words: Vehicular ad hoc networks, IEEE 802.11, WAVE, VANET security, network architecture

INTRODUCTION

Vehicular 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. It is a cornerstone of the envisioned Intelligent Transportation Systems (ITS). By enabling vehicles to communicate with each other via Inter-Vehicle Communication (IVC or V2V) as well as with roadside base stations via Roadside to Vehicle Communication (RVC or R2V), vehicular networks will contribute to safer and more efficient roads by providing timely information to drivers and concerned authorities.

VANETs share some common characteristics with general Mobile Ad Hoc Network (MANET). Both VANET and MANET are characterized by the movement and self-organization of the nodes. But they are different in some ways. Because of the high nodes mobility and unreliable channel conditions suggested by Abdalla *et al*. (2007). VANETs have unique characteristics which pose many challenging research issues such as data dissemination, data sharing and security issues (Fig. 1).

Advancing trends in ad hoc network scenarios allow a number of deployment architectures for nearby vehicles and between vehicles and nearby fixed roadside equipment. Vehicular ad hoc networks are expected to implement a variety of wireless technologies such as Dedicated Short Range Communications (DSRC) which is a type of Wi-Fi. Other wireless technologies are cellular, satellite and WiMAX. Vehicular ad hoc networks can be viewed as component of the Intelligent Transportation Systems (ITS) given by US DOT 2012.

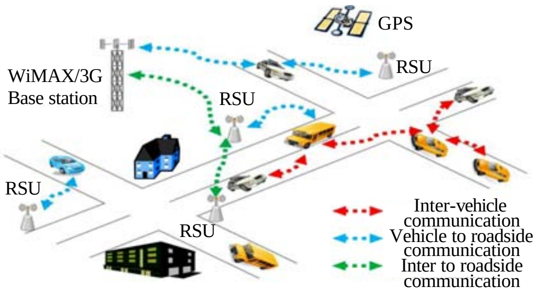
GPS
RSU
WiMAX/3G
Base station
RSU
RSU
RSU
Inter-vehicle communication
Vehicle to roadside communication
Inter to roadside communication

Fig. 1: Typical VANET scenario

CHARACTERISTICS OF VANETs

Drive behavior, constraints on mobility and high speeds create unique characteristics in VANETs. These characteristics distinguish them from other mobile ad hoc networks and the major characteristics are given.

High mobility and rapid changing topology: Vehicles move very fast especially on highways. Thus, they stay in the communication range of each other just for few seconds hence links are established and broken fast. When the vehicle density is low or existing routes break before constructing new routes, it has higher probability that the vehicular networks are disconnected. So, the previous routing protocols in MANET are not suitable for VANETs.

Corresponding Author: S. Prabhadevi, Department of Computer Science and Engineering, Nandhu Engineering College, Erode, India

Geographic position available: Vehicles can be equipped with accurate positioning systems integrated by electronic maps. For example, GPS receivers are very popular in cars which help to provide location information for routing purposes.

Mobility modeling and prediction: Vehicular nodes are usually constrained by prebuilt highways, roads and streets, so given the speed and the street map, the future position of the vehicle can be predicated. Vehicles move along pre-defined paths, this provides an opportunity to predict how long routes would last compared to arbitrary motion patterns like the random waypoint model recommended by Kosch (2004).

Hard delay constraints: In VANETs applications such as the collision warning or pre-crash sensing, the network does not require high data rates but has hard delay constraints and the maximum delay will be crucial.

Unlimited transmission power: The node (vehicle) itself can provide continuous power to computing and communication devices.

Potentially unbounded network size: VANETs could involve the vehicles in one city, several cities or even a country. Thus, it is necessary to make any protocols for VANET scalable in order to be practical.

Time-sensitive data exchange: Most safety related applications require data packet transmission in a timely manner. Thus, any security schemes cannot harm the network performance of VANETs.

Potential support from infrastructure: Unlike common MANETs, VANETs can actually take advantage of infrastructure in the future. This property has to be considered to make any protocol scheme for VANET.

Abundant resources: VANET nodes have abundant energy and computation resources. This allows schemes involving usage of resource demanding techniques such as ECDSA, RSA, etc.

Better physical protection: VANET nodes are better protected than MANETs. These tamper-proof nodes are more difficult to compromise enabling good security provisioning in VANETs.

Partitioned network: Vehicular networks will be frequently partitioned. The dynamic nature of traffic may result in large inter vehicle gaps in sparsely populated scenarios and hence in several isolated clusters of nodes.

Challenges in securing vehicular ad hoc networks: The unique characteristics of VANETs leave it particularly challenging from the design perspective and security issues. The provision of robust security for vehicular networks must overcome a set of technical, economic and social challenges. Some of the challenges faced by the vehicular networks are outlined in Raya *et al*. (2006).

Network volatility: The connectivity among the nodes can often be highly transient and a one-time event. Hence, a password based security channel establishment becomes impractical.

Liability vs. privacy: IVC provides a strong source of legal investigation in the case of accidents. In similar situations, the vehicle identity and the driver biometrics are considered, exploiting privacy to a great extent.

Delay-sensitive applications: Most of the safety and driver-assistance applications are time-sensitive. Hence, the protocol must be lightweight and robust against DoS attack.

Heterogeneity: The heterogeneity in VANET technologies and the supported applications are added challenges, especially taking into account their gradual deployment.

According to Parno and Perrig (2005), the cost of development and deployment of vehicular networks is another inhibiting factor for IVC solutions.

Quite often the fundamental building block for security protocols is key distribution. In vehicular ad hoc networks, key distribution poses several significant challenges implied by Raya and Hubaux (2005). Without a system for key distribution, applications like traffic congestion detection may be vulnerable to spoofing.

Applications of VANETs: Vehicular ad hoc network applications range from road safety applications to entertainment and commercial applications for passengers, making use of a plethora of cooperating technologies. Thus, researchers have divided the applications into two major categories.

Safety-related applications: These applications contain safety related applications such as collision avoidance and cooperative driving (e.g., for lane merging). The common characteristic of this category is the relevance to life-critical situations where the existence of a service may prevent life-endangering accidents. Hence, the security of this category is mandatory, since the proper operation of any of these applications should be guaranteed even in the presence of attackers.

Other applications: It includes traffic optimization, payment services (e.g., toll collection), location-based services (e.g., finding the closest fuel station) and entertainment information (e.g., Internet access). Obviously, security is also required in this application category especially in the case of payment services. The main focus is on the security aspects of safety-related applications because they are the most specific to the automotive domain because they raise the most challenging problems. Li *et al*. (2009) discussed the security of safety-related applications. VANET would support life-critical safety applications, safety warning applications, electronic toll collections, Internet access, group communications, roadside service finder, etc.

Electronic Toll Collections (ETCs): Each vehicle can pay the toll electronically as figured out by Dotzer *et al*. (2005) when it passes through a toll collection point without stopping. The toll collection point will scan the electrical license plate on the OBU (On-Board Unit) of the vehicle and issue a receipt message to the vehicle including the amount of the toll, the time and the location of the toll collection point. In the MAC layer, the electronic toll collections priority should be a direct one-hop wireless link between the toll collection point and the vehicle.

Internet access: Future vehicles can be equipped with the capability so that the passages on the vehicles can connect to the Internet. In the MAC layer, the internet access applications can use DSRC service channels except the control channel with the lowest priority comparing with the previous applications. In the network layer, it is used to support VANET Internet access, a straight forward method is to provide a unicast connection between the OBU of the vehicle and a RSU, which has the link towards the internet.

Vision enhancement: Drivers are given a clear view of vehicles and obstacles in heavy fog conditions and can learn about the existence of vehicles hidden by obstacles, buildings or by other vehicles.

Automatic parking: Parking Availability Notification (PAN) helps to find the availability of space in parking lot in certain geographical area as per the weather conditions. Automatic parking is an application through which a vehicle can park itself without the need for driver intervention.

Group communications: Many drivers may share some common interests when they are on the same road to the same direction, so they can use the VANET group communication functions. In the MAC layer, the group communications can use DSRC service channels except the control channel with the lowest priority comparing with the safety related applications and ETCs.

Life-critical safety applications: It provides intersection collision warning/avoidance, cooperative collision warning, etc. In the MAC Layer, the life-critical safety applications can access the DSRC control channel and other channels with the highest priority.

Safety warning applications: Safety warning applications contain work zone warning, transit vehicle signal priority, etc. The differences between life-critical safety applications and safety warning applications are the allowable latency requirements while the life-critical safety applications given by Li *et al*. (2009) usually require the messages to be delivered to the nearby nodes within 100 msec, the safety warning applications can afford up to 1000 msec. In the MAC layer, the safety warning applications can access the DSRC control channel and the other channels with the 2nd highest priority.

Both life-critical safety applications and safety warning applications messages are broadcasted to the nearby vehicles. In short, the application layer requirements must be addressed in the MAC layer and network layer design. This study provides a network design framework to satisfy the above applications while providing sufficient security.

DAHNI (Driver Ad Hoc Networking Infrastructure): DAHNI proposed by El-Zarki *et al*. (2002) provides numerous possibilities to revolutionize the automotive and transportation industry of the future. For example, data captured by DAHNI when properly aggregated can be fed into the traffic monitoring and flow control system for real-time traffic management. Alternatively, such information can be archived for off-line analysis to understand traffic bottlenecks and devise techniques to alleviate traffic congestion.

Standards and IEEE drafts: Many automobile manufacturers and researchers using vehicular ad hoc networking technologies are working towards overcoming the challenges and achieve the future envisioned networks.

C2C-CC: The Car to Car Communication Consortium (C2C-CC) from Car to Car Communication Consortium, 2013 has been initiated in Europe by car manufacturers and automotive OEMs (Original Equipment Manufacturers) with the main objective of increasing road traffic safety and efficiency by means of inter vehicle communication (Fig. 2).

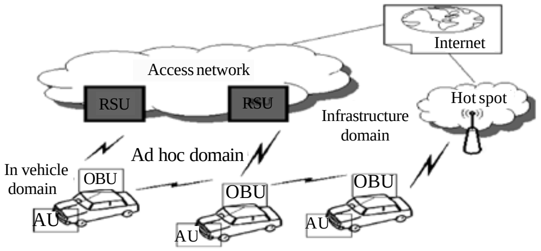

Fig. 2: C2C-CC reference architecture

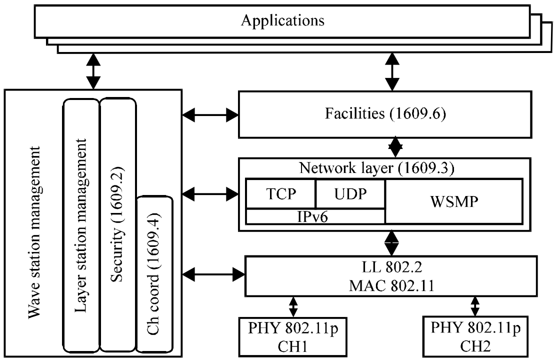

Fig. 3: IEEE 1609 WAVE protocol stack

IEEE (WAVE): IEEE from IEEE Standards, 2013 has also advanced with the IEEE 1609 family of standards for Wireless Access in Vehicular Environments (WAVE). Wireless ACEESS IN Vehicular Environments (WAVE) is a radio communications system intended to provide interoperable wireless networking services for transportation. These services include those recognized for Dedicated Short-Range Communications (DSRC) by the US National Intelligent Transportation Systems (ITS) Architecture. The system enables vehicle to vehicle and vehicle to roadside infrastructure communications. The Physical layer (PHY) and Network layer use elements of IEEE 802.11 PHY and MAC (Fig. 3). The IEEE 1609 suite of standards:

- IEEE P1909.1 defines the resource manager that uses the network stack for communication
- IEEE P1609.2 specifies security services for the WAVE networking stack and for applications that are intended to run over those stack
- IEEE P1609.3 specifies upper layers of the network stack
- IEEE P1609.4 specifies the channelization

CONCLUSION

VANET is a promising wireless communication technology for improving highway safety and information services. In this study, researchers propose a secure and application oriented network design framework in which the requirements of potential VANET applications are taken into account. This study represents an overview and tutorial of various issues and challenges in vehicular ad hoc network. Various types of challenges in vehicular network has been identified and addressed. Researchers also study several applications as a promising tool for monitoring the physical world with wireless sensor that can sense, process and communicate. VANET applications range from safety and crash avoidance to Internet access and multimedia. Researchers believe that the study can provide a guideline for more practical VANET.

REFERENCES

Abdalla, G.M.T., M.A. Abu-Rgheff and S.M. Senouci, 2007. Current trends in vehicular Ad Hoc networks. Proceedings of the IEEE Global Information Infrastructure Symposium, July, 2007, Morocco.

Dotzer, F., F. Kohlmayer, T. Kosch and M. Strassberger, 2005. Secure communication for intersection assistance. Proceedings of the 2nd International Workshop on Intelligent Transportation, March 15-16, 2005, Hamburg, Germany.

El-Zarki, M., S. Mehrotra, G. Tsudik and N. Venkatasubramanian, 2002. Security issues in a future vehicular network. Symp. Q. J. Mod. Foreign Literatures, 35: 270-274.

Kosch, T., 2004. Local danger warning based on vehicle Ad Hoc networks: Prototype and simulation. Proceedings of the 1st International Workshop on Intelligent Transportation, March 23-24, 2004, Hamburg, Germany.

Li, Z., Z. Wang and C. Chigan, 2009. Security of Vehicular ad Hoc Networks for Intelligent Transportation Systems in Wireless Technologies. Nova Science Publishers, USA.

Parno, B. and A. Perrig, 2005. Challenges in securing vehicular networks. Proceedings of the 4th ACM Workshop on Hot Topics in Networks, November, 2005, College Park, Maryland, USA.

Raya, M. and J.P. Hubaux, 2005. Security aspect of inter-vehicle communications. Proceedings of the 5th Swiss Transport Research Conference, March 9-13, 2005, Ascona, Switzerland.

Raya, M., P. Papadimitratos and J.P. Hubaux, 2006. Securing vehicular communications. IEEE Wireless Commun., 13: 8-15.