IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

Vehicular Adhoc Network- Architecture and Operations

Ankur Jain[1], Ratnesh Dubey[2], Vineet Richariya[3]

LNCT Bhopal[1, 2, 3]

Abstract: Vehicular ad-hoc networks (VANETs) are the class of mobile ad-hoc network (MANET) applications that have the future chances in improving road safety and in giving travellers contentment. Now a day's many persons are adopting cars and other individual vehicles. The biggest hazard respect to increased use of private transport is the increasing number of victims of the accidents on the roads; the expense and associated dangers have been predictable as a serious problem being confronted by current society. In this paper we are going to consider the main features related to VANETs its characteristics and functions. This field is favourable for researchers and developers to percept and differentiate the main aspects neighbouring VANETs.

Keywords: Vehicular Ad hoc Network, RSU, OBU global position system (GPS), attacks.

1. INTRODUCTION

Vehicular adhoc Network (VANET) provides a means to the moving vehicles to communicate by a wireless communication using dedicated short range communication (DSRC). The DSRC is a IEEE communication having a standard IEEE 802.11a for low overhead operation to 802.11p. In VANET vehicles should be able to communicate with other vehicles that are vehicle to vehicle communication (V2V), with fixed unit along road termed as Road side unit (RSU) which comes under Vehicle to infrastructure communication (V2I). These types of communications permit vehicles to allocate different kinds of information, for instance, safety information for the use of accident avoidance, post-accident investigation or traffic jams. Other types of information are capable of disseminating like traveller related information that is measured as non-safety information. The objective behind distributing and contributing this information is to give a safety message to advise drivers about expected hazard with the purpose of decreasing the number of accidents and save people's lives, or to give passengers with happy journeys [3-4].

This area attracts researchers for different fields to develop VANET applications, protocols and simulation tools. Researchers and developer are facing several challenges. Hence, several papers and articles have attempted to cover these issues. The communication and networking aspects of this technology are to address the security and privacy issues that have been investigated by Hartenstein and Laberteaux [5]. But, the focal point on the routing protocols of VANET and their requirements to achieve better communication time with less expenditure of network bandwidth introduced by Li and Wang in 2007 [6]. Lin et al. investigated the categories of routing protocols in VANET and the idea behind each of them [7]. In this paper, we present a key document which is able to make available detailed information to researchers and developer to facilitate they can appreciate the main aspects and challenges related to VANET. It covers diverse issues such as network architecture, communication domains, challenges, applications and simulation tools [8].

2. VANET ARCHITECTURE

The communication between vehicles or between a vehicle and an RSU is accessed by using a wireless medium known as WAVE. These ways of communication provides a broad range of information to drivers and travellers, and enable safety applications to improve road safety and provide a secure driving [8].

The most significant system components are the application unit (AU), OBU and RSU. Generally the RSU hosts an application that provide services and the OBU is a peer device that uses the services provided. The application may reside in the RSU or in the OBU; the device that hosts the application is called the provider and the device using the application is called as the user. Each vehicle is able to with an OBU and a set of sensors to gather and process the information then send it on as a message to other vehicles or RSUs through the wireless medium; it also carries a single or multiple AU so as to use the applications provided by the provider using OBU connection capabilities. The RSU can also connect to the Internet or to another server which allows AU's from multiple vehicles to connect to the Internet [9-10].

3. ON BOARD UNIT (OBU)

An OBU is a wave device typically mounted on-board a vehicle used for exchanging information with RSUs or with other OBUs. It consist of a resource command processor (RCP), and resources in which a read/write memory used to store and recover information, a user interface, a specialised interface to connect to other OBUs and a network device for short range wireless

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

communication based on IEEE 802.11p radio technology. It may furthermore, include another network device for non-safety applications based on other radio technologies such as IEEE 802.11a/b/g/n. The OBU connects to the RSU or to other OBUs through a wireless link based on the IEEE 802.11p radio frequency channel, and is responsible for the communications with other OBUs or with RSUs. It also provides a communication services to the AU and forwards data on behalf of other OBUs on the network. The major functions of the OBU are wireless radio access, ad hoc and geographical routing, network congestion control, reliable message transfer, data security and IP mobility.

4. APPLICATION UNIT (AU)

The AU is the device capable of within the vehicle that uses the applications provided by the provider using the communication capabilities of the OBU. The AU be able to a dedicated device for safety applications or a normal device such as a personal digital assistant (PDA) to run the Internet, the AU can be connected to the OBU through a wired or wireless connection and can reside with the OBU in a single physical unit. The difference between the AU and the OBU is logical. The AU communicates with the network only via the OBU which takes task for all mobility and networking functions.

5. ROADSIDE UNIT (RSU)

The RSU is a wave device typically fixed along the road side or in dedicated locations such as at junctions or near parking spaces. The RSU is equipped with one network device for a dedicated short range communication based on IEEE 802.11p radio technology, and can also be equipped with other network devices ever since to be used for the intention of communication within the infrastructural network.

The main functions and procedures associated with the RSU are:

- By extending the communication range of the ad hoc network by reallocate the information to other OBUs and by transfer the information to other RSUs in order to forward it to other OBUs as shown in figure 1.1.

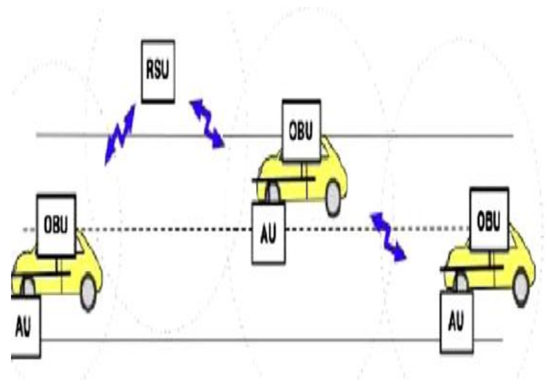

Fig.1.1 RSU extend the range of the ad hoc network by forward the data of OBUs

- Running safety applications such as a low bridge warning, accident warning or work zone, with the use of infrastructure to vehicle communication (I2V) and acting as an information source. The RSU work as information source as shown in figure1.2.

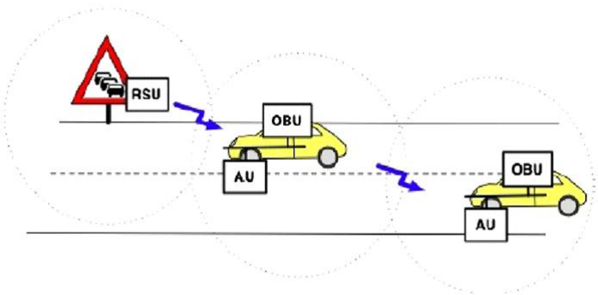

Fig.1.2 RSU work as information source (running safety applications)

- Providing Internet connectivity to OBUs: RSU provides internet connectivity to OBUs are shown in figure 1.3.

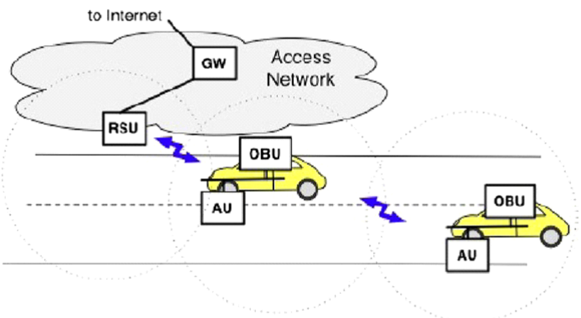

Fig.1.3. RSU provides internet connectivity to the OBUs

The communication among vehicles and the RSU and the infrastructure variety three types of domains:

Inter-vehicle communication

The inter-vehicle communication configuration adoption of multi-hop multicast/broadcast to transmit traffic related information over multiple hops to a group of receivers. In intelligent transportation systems, vehicles must only be concerned with activity on the road ahead and not behind (an example of this would be for emergency message dissemination about an imminent collision or dynamic route scheduling). There are two types of message forwarding in inter-vehicle communications: naïve broadcasting and intelligent broadcasting.

In naïve broadcasting, vehicles send broadcast messages periodically and at regular intervals. Upon receipt of the message, the vehicle ignores the message if it has come from a vehicle behind it. If the message comes from a vehicle in front, the receiving vehicle sends its own broadcast message to vehicles behind it. This ensures that all enabled vehicles moving in the forward direction get all broadcast messages. The boundaries of the naïve broadcasting method is that large numbers of broadcast messages are generated, therefore, increasing the risk of

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

message collision resulting in lower message delivery rates and increased delivery times [11].

Intelligent broadcasting with inherent acknowledgement addresses the effort inherent in naïve broadcasting by limiting the number of messages broadcast for a given tragedy event. If the event-detecting vehicle receives the same message from behind, it assumes that at least one vehicle in the back has received it and ceases broadcasting. The assumption is that the vehicle in the back will be responsible for moving the message along to the rest of the vehicles. If a vehicle receives a message from more than one source it will act on the first message only.

In-vehicle domain: This domain comprise of an OBU and one or multiple AUs. The connection could be wired or wireless using WUSB or UWB; an OBU and an AU are capable to reside in a single device [5]. The OBU provides a communication link to the AU so as to execute one or more of a set of applications provided by the application provider with the use of the communication capabilities of the OBU [10].

Vehicle-to-roadside communication
The vehicle-to-roadside communication configuration represents a single hop broadcast where the roadside unit sends a broadcast message to all equipped vehicles in the vicinity. Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside units. The roadside units can be placed every kilometre or less, enabling high data rates to be maintained in heavy traffic. For instance, when broadcasting dynamic speed limits, the roadside component will determine the appropriate speed limit according to its internal timetable and traffic conditions. The roadside unit will periodically broadcast a message containing the speed limit and will compare any geographic or directional limits with vehicle data to determine if a speed limit warning applies to any of the vehicles in the vicinity. If a vehicle violates the required speed limit, a broadcast will be delivered to the vehicle in the form of an auditory or visual warning, requesting that the driver decrease his speed[11-12].

Routing-based communication
The routing-based communication configuration is a multi-hop unicast in which a message is propagated in a multi-hop fashion until the vehicle carrying the desired data is reach. When the query is received by a vehicle owning the desired piece of information, the application at that vehicle immediately sends a unicast message containing the information to the vehicle it received the request from, which is then charged with the task of forwarding it towards the query source.

VANET CHARACTERISTICS

VANET has its individual unique characteristics when it compared with other types of MANETs, the only characteristics of VANET includes:

- **Predictable Mobility**

VANET differs from other types of mobile ad hoc networks that nodes move in a arbitrary way, as vehicles are constrained by road topology and layout and by the requirement to obey road signs and traffic lights and to respond to other moving vehicles leading to predictability in term of their mobility [13, 14].

- **Providing Safe Driving, Improving Passenger Comfort And Enhancing Traffic Efficiency**

VANET gives the potential of direct communications among moving vehicles, therefore allowing a set of applications, demanding direct communication between nodes to be applied over the network. Such applications are capable to afford drivers travelling in the same direction with warning messages about accidents, or about the require for sudden hard breaking; leading the driver to construct a broader picture of the road ahead. Moreover, additional kinds of applications could be applied via this type of network in order to recover passenger comfort and traffic efficiency by disseminating information about weather, traffic flow and point of interest information [13].

- **No Power Constraints**

The power in VANET is not a significant challenge, because vehicles have the capability to provide continuous power to the OBU by the long life battery [13,16,17].

- **Variable Network Density**

The network density in VANET varies depending on the traffic density, which can be very high in the case of a traffic jam, or very low, as in suburban traffic[15][17].

- **Rapid Changes In Network Topology**

High speeds distinguish moving vehicles, primarily at the highway leading to rapid changes in network topology. In addition, driver behaviour is exaggerated by the requirement for reacting to the data received from the network, which causes changes in the network topology. The life time of the link between vehicles is affected by the radio communication range and the direction of the vehicles; thus increasing the radio communication range leads to an increase in the life time of the link. The life time of the link between vehicles moving in opposite directions is very short lived compared with case in which vehicles move in the same direction. The fast changes in link connectivity cause the effective network diameter to be small, while many paths are disconnected before they can be utilised [13, 17, 7].

- **Large Scale Network**

The network scale could be large in dense urban areas such as the city centre, highways and at the entrance of the big cities [15, 16, 17].

- **High Computational Ability**

The nodes in VANET are vehicles that can be equipped with a adequate number of sensors and computational resources; such as processors, a large memory capacity,

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

advanced antenna technology and global position system (GPS). These resources move up the computational capacity of the node, which help obtaining reliable wireless communication and acquire accurate information regarding its current position, speed and direction [18, 19,20].

B. SECURITY IN VANET

VANET security is different from that of wireless and wired networks because of its unique characteristics of mobility constraints, infrastructure-less framework, and short duration of link between nodes. so, it is vital to develop security algorithms that help to guarantee the accurate and safe operation of VANETs [21,22,23].
The main cryptographic requirements to solve security issues in VANETs are:

• **Availability:** The network must be available at all times in order to send and receive messages. Two possible threats to availability are for instance DoS and jamming attacks. One more availability problem might be caused by selfish nodes which do not provide their services for the benefit of other nodes in order to save their own resources like battery power.

• **Confidentiality:** Secrecy must be provided to susceptible material being sent over the VANET, like in certain commercial applications.

• **Integrity:** Messages sent over the network should not be corrupted. Possible attacks that would compromise their integrity are malicious attacks or signal failures producing errors in the transmission.

• **Authenticity:** The identity of the nodes in the network must be ensured. Otherwise, it would be possible for an attacker to masquerade a legitimate node in order to send and receive messages on its behalf.

• **Non-Repudiation:** A sender node might try to deny having sent the message in order to avoid its task for its contents on-repudiation is particularly useful to sense compromised nodes.

6. CONCLUSION

The convergence of computing, telecommunications and a wide range of services are enabling the use of different kinds of VANET technologies. This paper provides a comprehensive survey on all the issues covering VANET, VANET architectures with their important components, VANET characteristics, challenges and requirements, VANET applications and imperative types of attacks on VANET.

REFERENCES

[1] S. Biswas, R. Tatchikou, F. Dion, Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety, IEEE Communications Magazine 44 (1), pp. 74–82, 2006.
[2] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan,"Vehicular ad hoc networks (VANETS): Status, Results, and Challenges", Telecommunication Systems, Volume 50, Issue 4, pp.- 217-241, 2012. DOI-10.1007/s11235-010-9400-5.
[3] J. Blum, A. Eskandarian, L. Hoffman, Challenges of inter-vehicle ad hoc networks, IEEE Transactions on Intelligent Transportation Systems 5 (4), pp.347–351, 2004.
[4] W. Kiess, J. Rybicki, M. Mauve, "On the Nature of inter-vehicle communication", In: WMAN 2007: Proceedings of the 4th Workshop on Mobile Ad-Hoc Networks, pp. 493–502, 2007.
[5] J. Luo, J.-P. Hubaux, "A Survey of Inter-Vehicle Communication", Tech. Rep. IC/2004/24, School of Computer and Communication Sciences, EPEL, 2004.
[6] J. Hubaux, S. Capkun, J. Luo, "The Security and Privacy of Smart Vehicles", IEEE Security and Privacy Magazine 02 (3), pp.49–55, 2004.
[7] Boukerche A., Oliveira H.A.B.F., Nakamura E. F. and Loureiro A. A.F., "Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems", Computer Communications, Volume 31, Issue 12, pp. 2838–2849, 2008.
[8] Lin Y, Chen Y, Lee S.,"Routing protocols in vehicular ad hoc networks: a survey and future perspectives", Journal of Information Science and Engineering 2010;26 (3), pp.913–32, 2010.
[9] Saif Al-Sultan, MoathM.Al-Doori, AliH. Al-Bayatti and Hussien Zedan "A Comprehensive Survey on Vehicular Ad Hoc Network", Journal of Network and Computer Applications Vol.-37, pp.380–392, 2014. http://dx.doi.org/10.1016/j.jnca.2013.02.036.
[10] Olariu S, Weigle MC, "Vehicular Networks: From Theory to Practice", 1st edition, Chapman & Hall/CRC, 2009.
[11] Zeadally S., Hunt R., Chen Y. S.,Irwin A., and Hassan A., "Vehicular Ad-hoc Networks (VANETS): Status Results and Challenges", Springer Journal of Telecommunication Systems Volume 50, Issue 4 , pp. 217-241,2010.
[12] Bickel,G.Inter/intra-vehicle wireless communication,2008. http://userfs.cec.wustl.edu/~gsb1/index.html#toc (accessed: May 29, 2010)
[13] Jakubiak J, Koucheryavy Y, "State of the Art and Research Challenges for VANETs", In: Consumer Communications and Networking Conference. CCNC 2008, 5th IEEE, pp. 912–6, 2008.
[14] Blum J, Eskandarian A, Hoffman L, "Challenges of Inter-vehicle Ad hoc Networks", IEEE Transactions on Intelligent Transportation Systems, pp.347–51, 5(4), 2004.
[15] Toor Y, Muhlethaler P, Laouiti A, "Vehicle Ad hoc Networks: Applications and Related Technical Issues", IEEE Communications Surveys Tutorials 10(3), pp.74–88, 2008.
[16] Yousefi S, Mousavi MS, Fathy M, "Vehicular Ad hoc Networks (VANET): Challenges and Perspectives", In Proceedings of the 6th International Conference on ITS Telecommunications, pp. 761–6, 2006.
[17] Nekovee M.,"Sensor Networks on the Road: The Promises and Challenges of Vehicular Ad -hoc Networks and Grids", In: Workshop on ubiquitous computing and e-Research, 2005
[18] Wischhof L, Ebner A, Rohling H, "Information Dissemination in Self-Organizing Intervehicle Networks", IEEE Transactions on Intelligent Transportation Systems; 6(1): pp.90–101, 2005.
[19] Moustafa H, Zhang Y.," Vehicular Networks: Techniques Standards and Applications", CRC Press; 2009.
[20] Rawashdeh Z, Mahmud S, "Intersection Collision Avoidance System Architecture", In:Consumer Communications and Networking Conference, CCNC 2008. 5th IEEE, pp.493–4, 2008.
[21] A. Aijaz, B. Bochow, F. Dtzer, A. Festag, M.Gerlach, R. Kroh, and T. Leinmuller, "Attacks on Inter-Vehicle Communication Systems Analysis", In Proceedings of the 3rd International Workshop on Intelligent Transportation (WIT), 2006.
[22] Farhan Aadil, Shahzad Rizwan, Adeel Akram, "Vehicular Ad Hoc Networks (VANETs), Past Present and Future: A survey", Springer-Verlag Berlin Heidelberg, 2011.
[23] P. Caballero-Gil, "Security Issues in Vehicular Ad Hoc Networks", Mobile Ad-Hoc Networks: Applications, University of La Laguna, Spain, 2012.