A Summary of VANET Advances and Research

Renan Greca

***Abstract*—Vehicular Ad-hoc Networks (VANETs) are a growing field of research due to their potential of decreasing the number of accidents on the road. They can also make traffic more efficient and more comfortable. However, the development of functional VANETs in the real world still faces challenges when it comes to wireless communications, routing protocols, applications, security and simulation. This paper provides a summary of a recent meta-survey on the topic by briefly introducing readers on the concept and importance of VANETs and presents each of the five areas of research in the field. Finally, we show our conclusions on both the studied topic and on the aforementioned meta-survey.**

***Index Terms*—VANET, ad-hoc, V2X, wireless networks, protocols.**

I. Introduction

THIS paper is a summary of a recent meta-survey regarding Vehicular Ad-hoc Networks (VANET) [1]. The original article provides a broad overview of the history, technology, applications and challenges of VANET. In this summary, we will cover the basic meaning of VANET and the differences between it and traditional networking models, as well as a slightly more detailed look at the research currently being made to find useful technologies and applications for VANET.

A. What Are VANETs?

In recent years, we have witnessed both an increase in the number of vehicles on the road and a radical shift in how we perceive computers and their applications for communication. However, vehicles are rather unsafe: thousands of accidents occur every day on roads around the world. Meanwhile, the paradigm shift regarding the mobility of computers and the advance of wireless communication methods allow many vehicles to come equipped with on-board units (OBU), computers that have access to a variety of information about the vehicle. These OBUs can input and output data from and to the driver and passengers, and are often equipped with a networking module.

Therefore, it is now possible to think of vehicles as nodes in a network, by allowing them to communicate with other vehicles (vehicle-to-vehicle communication, or V2V) and with static nodes in a city's infrastructure (vehicle-to-infrastructure communication, or V2I). The static nodes are called road-side units (RSUs). By sharing information about traffic conditions, vehicle parameters and other data, it is possible to make roads safer, more efficient and more enjoyable.

RSUs have separate network interfaces to communicate with OBUs, other RSUs or Internet service providers (ISPs). By acting as bridges between ISPs and OBUs, it is possible to provide Internet access to traveling vehicles. Meanwhile, OBUs can exchange safety and efficiency messages with each other, either with single-hop transmissions or multi-hop ones to reach distant vehicles.

R. Greca is with the Department of Informatics, Universidade Federal do Paraná, Curitiba, PR, Brazil e-mail: rgreca@inf.ufpr.br.

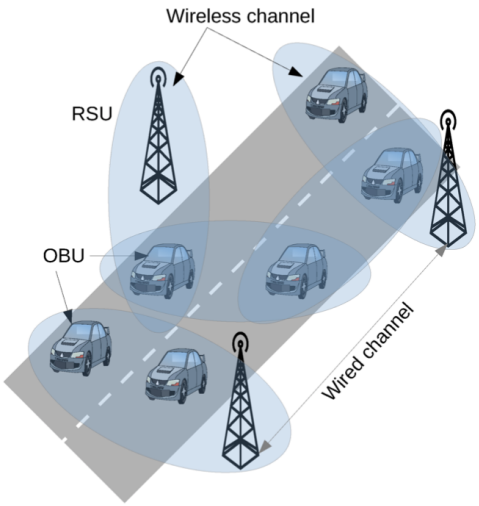

Fig. 1. Mockup of VANET showing OBUs and RSUs.

VANETs are different from mobile ad-hoc networks (MANET) because vehicles move much faster than humans carrying mobile devices, but are constrained to move in specific patterns (determined by the roads) [2]. Consequently, standards and protocols have been developed for vehicular networks taking in consideration these peculiarities.

B. Paper Organization

In the section above, we have familiarized readers with the basic concept of VANETs and their importance. In the following section, we brief readers on each of the five types of research currently being performed with VANETs. Section III presents our conclusions regarding the subject and the meta-survey this paper is based on.

II. Research being made on VANET

Research on VANET is generally divided into five categories: wireless technologies, routing protocols, applications, security and trust, and simulation. In this paper, we'll cover aspects of each one of these.

A. Wireless Technologies

There are several wireless communication technologies currently in use and widely available in mobile devices, such as

Bluetooth, Wi-Fi and LTE, that can be potentially useful in the realm of vehicular networks. However, each of those technologies have notable drawbacks in a vehicular environment: Bluetooth is designed for low battery use and therefore has severe limitations in range and bandwidth; Wi-Fi functions primarily using an access point model and, although it can be used for MANETs, its range would have trouble keeping up with the mobility of vehicles; LTE and other cellular technologies may be useful for RSU-to-OBU communication, but are not suitable for ad-hoc networks and add latency which would diminish the utility of safety applications [3].

Therefore, a new suite of standards and protocols has been devised called WAVE (Wireless Access in Vehicular Environments), as defined by IEEE 802.11p [Morgan 2010]. WAVE resembles Wi-Fi the most, but it operates in the 5.86-5.92 GHz frequency bands and provides longer range. Additionally, the WAVE model is closely based on the OSI model, but with a few key differences: (1) it adds a multichannel cooperation layer (IEEE 1609.4) which is necessary to integrate V2V and V2I communications; (2) it adds security services protocols (IEEE 1609.2) to all layers; and (3) the networking and transport layers are complemented by WSMP (Wireless Short Message Protocol), which handles time-critical safety messages instead of TCP/IP like most messages [4].

Although WAVE appears to be a promising technology for vehicular technologies, it still lacks extensive testing both in simulations and real testbeds. This issue will be covered further later in this section.

B. Routing Protocols

One of the greatest challenges with VANETs is routing. Routing is already a challenging task in MANETs, and the vast increase of mobility only makes it more difficult. Routing protocols used in VANETs are divided into *broadcast* (sends a message to all possible nodes), *multicast or geocast* (sends a message to a group of nodes in a certain location), and *unicast* (sends a message to one specific node). Furthermore, they are classified as topology-based, which are often adaptations of MANET protocols, and location-based, which take into consideration vehicular parameters such as GPS coordinates, speed and direction.

Despite over fifty protocols suggested for VANETs, none of them has stood above others in all relevant situations. Therefore, routing protocols are a field of much debate amongst researchers. Not only do these protocols have to find routes to a message's recipients, but also take into consideration the priority of safety messages, delay and the ever-changing network topology.

C. Applications

VANET applications are usually divided into *safety* and *non-safety* applications. As is implied, safety applications aid drivers to avoid collisions and other accidents. These applications have the highest priority in VANET communications. Meanwhile, non-safety applications include those directed towards traffic efficiency, comfort and entertainment. Safety applications only tolerate delays of some milliseconds, efficiency ones can't tolerate much more to be truly useful. Comfort applications, such as information about nearby points of interest, can tolerate a few seconds, but must still be delivered in a timely fashion. Entertainment applications might need a lot of bandwidth to function, but are generally the most delay-tolerant.

Most research currently being made here is on how to build and deliver messages to provide useful applications, as well as how to best present gathered information to the driver and passengers. Additionally, there are novel applications that can be developed using the relatively recent paradigm of VANETs.

D. Security and Trust

It is crucial that the integrity of messages sent through VANET is not compromised, especially in safety and efficiency applications. Malicious nodes in a network can eavesdrop or manipulate messages traveling between other nodes, and incorrect data might lead to drivers taking bad decisions for themselves or for others [5]. Furthermore, a malicious node might even forge traffic data for its own advantage — for example, one vehicle might falsely report a congestion so other nodes might consider different routes.

VANET security is generally divided in *authentication-based* and *reputation-based*. In the former, nodes are verified through authentication and all data originating from them are considered valid. Meanwhile, the latter method uses distributed reputation schemes so nodes are deemed more or less trustworthy over time.

E. Simulation

The most challenging aspect of VANET research is proper testing of proposed solutions. Therefore, a number of models have been created to simulate VANETs, and some of these models have been integrated with existing networking simulators. These models must take into consideration the movement patterns, traffic conditions, incidents and communication channels that would affect a real-life vehicular network.

Many of the proposed simulation models cover the constrained and high-speed movements of vehicles, but none of them cover all the situations that may occur in real traffic scenarios. At the very least, an ideal model would be able to cover all safety situations and preferably most efficiency ones. Furthermore, all existing simulators are modified versions of simulators made for traditional ad-hoc networks; none were developed from scratch with VANETs in mind.

III. Conclusion

In this brief summary, we have looked at the importance of VANETs plus the recent developments and research being made in the field. We notice that there is still a long way to go before VANETs become fully operational in real world conditions. However, the necessity for that operation will only grow larger as we make the transition from human-driven vehicles to fully autonomous vehicles.

The meta-survey that we summarized proved to be a valuable introduction to the study of vehicular networks and its vast

list of references will no doubt prove to be useful. Although the paper's objective was not to cover any one aspect of VANETs in detail, we noticed it came across lacking in some aspects, especially when it came to comparing new solutions to already existing ones (for example, despite the inclusion of a comparison chart, the text did not clearly explain the advantages of WAVE over other wireless technologies).

ACKNOWLEDGMENT

The author would like to thank professors Luiz Carlos P. Albini (UFPR) and Anelise Munaretto (UTFPR) for their instruction and guidance during the writing of this paper.

REFERENCES

[1] M. Saini, A. Alelaiwi, and A. E. Saddik, "How close are we to realizing a pragmatic vanet solution? a meta-survey," *ACM Computing Surveys (CSUR)*, vol. 48, no. 2, p. 29, 2015.

[2] F. K. Karnadi, Z. H. Mo, and K.-c. Lan, "Rapid generation of realistic mobility models for vanet," in *2007 IEEE Wireless Communications and Networking Conference*. IEEE, 2007, pp. 2506–2511.

[3] T. Mangel, T. Kosch, and H. Hartenstein, "A comparison of umts and lte for vehicular safety communication at intersections," in *Vehicular Networking Conference (VNC), 2010 IEEE*. IEEE, 2010, pp. 293–300.

[4] M. Bechler, S. Jaap, and L. Wolf, "An optimized tcp for internet access of vehicular ad hoc networks," in *International Conference on Research in Networking*. Springer, 2005, pp. 869–880.

[5] P. Papadimitratos and J.-P. Hubaux, "Report on the secure vehicular communications: results and challenges ahead workshop," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 12, no. 2, pp. 53–64, 2008.

Renan Greca received the B.Sc. degree in computer science from the Universidade Federal do Paraná (UFPR) in 2016. During his undergraduate studies, he studied abroad for a year at Pomona College in California.

Currently, he is working on getting his M.Sc. degree in computer networks also at UFPR, focusing his research on using vehicular networks to improve the safety of drivers and pedestrians.