COMMUNICATION TECHNOLOGIES TO DESIGN VEHICLE-TO-VEHICLE AND VECHILE-TO-INFRASTRUCTURES APPLICATIONS

A. REYES†, C. BARRADO† and A. GUERRERO‡

† *Computer Architecture Department. UPC. BarcelonaTech. Esteve Terradas 6.Castelldefels, Spain.*
mreyes, cbarrado@ac.upc.edu
‡ *School of Telematics, UDC, Av. Universidad 333, Colima, Mexico. antonio_guerrero@ucol.mx*

***Abstract*—— Intelligent Transport Systems use communication technologies to offer real-time traffic information services to road users and government managers. Vehicular Ad Hoc Networks is an important component of ITS where vehicles communicate with other vehicles and road-side infrastructures, analyze and process received information, and make decisions according to that.**

However, features like high vehicle speeds, constant mobility, varying topology, traffic density, etc. induce challenges that make conventional wireless technologies unsuitable for vehicular networks. This paper focuses on the process of designing efficient vehicle-to-vehicle and vehicle-to road-side infrastructure applications.

***Keywords*—— Vehicle-to-vehicle applications, mobile communication systems.**

I. INTRODUCTION

The Deployment of Intelligent Transport Systems in Europe (DGMTEC, 2011) deals with the integration of the information and communications technologies in vehicles and in infrastructure. An example of the European Commission interest is ensuring a sustainable urban mobility where new research focuses on next generation vehicles. Particular attention is paid to non-pollution, information and communication strategies, services and infrastructures (Popescu, 2010).

An application to find a suitable free parking slot in an urban area is an example of this priority area. Studies show that every person living in Madrid (Spain) wastes an average of 15.7 minutes every day searching for a valid parking slot (ASESGA, 2014). The lost of time and the generated pollution can be quantified in thousands of dollars a day.

A parking application is a clear example of the use of a collaborative network of sensors located within vehicles. This is known as a Vehicle ad hoc Network or VANET. Designing a VANET application is a complex process, in part because it is necessary to have a communication system with a convenient, stable, secure and economic distribution of data over high mobile nodes. It requires a reliable location mechanism and also a communication capability able to distinguish between critical and informative messages. In this paper, we will present a methodology to design applications for VANETs that will lead developers to a quality solution and will reduce development time of applications.

II. VEHICULAR AD HOC NETWORKS

VANETs are ad hoc networks that have predictable nodes' movements due to the existing infrastructures (roads, motorways, etc) and traffic laws. However, vehicle high velocities and density are some clear characteristics that make VANETs very distinct from other ad hoc networks. Also, context awareness gets difficult because the immediate context changes very fast. The same occurs with message dissemination and security mechanisms that have to deal with highly unstable network topologies.

In the physical layer, the 802.11p wireless standard is the most generalized protocol for VANETs (Jiang and Delgrossi, 2008). This standard, also called Wireless Access in Vehicular Environments uses the multi-hop technique for routing within a range between 300 and 1000 meters.

Network routing protocols for VANETS are analyzed in several researches: Menouar *et al.* (2007) proposes a proactive routing where movement of vehicles is expected and considered for improving performances. Fracchia (2006) considers the current location of vehicles to reduce the number of signal collisions in broadcast messages. In Menouar *et al.* (2006) the use of Directional MAC protocol to reduce the collisions rate is proposed. This protocol takes advantage of the vehicles predictable movements because of the roads and driving rules.

At the application level there are different ways for classifying VANET applications. For example Schoch *et al.* (2008) mention four application categories: Active Safety, Public Service, Improved Driving and Business/Entertainment. In contrast, CAR2CAR (2007) classifies applications based on their requirements of security and types of information: Vehicle-to-Vehicle Cooperative Awareness, Vehicle-to-Vehicle Unicast Exchange, Vehicle-to-Vehicle Decentralized Environmental Notification, Infrastructure to Vehicle (One-Way), Local Road Side Unit (RSU) Connection, and Internet Protocol RSU Connection. In Do *et al.* (2008), applications have three main categories: safety, traffic monitoring/optimization and infotainment. In Qian and Moayeri (2008) there is a classification based on six groups: Life-Critical Safety Applications, Safety Warning, Electronic Toll Collection, Internet Access, Group Communication and RSU Service Finder. In this research we use this last classification (see Section IV).

III. TECHNICAL ASPECTS INVOLVED IN VANET APPLICATIONS

VANET applications may require different sensing capabilities, communication abilities, security, etc. Different research projects focus only in one or maximum two of these aspects. For example Schoch *et al.* (2008) analyses only characteristics of VANETs, Boukerche *et al.* (2008) outlines the localization requirements of the main VANETs applications or Qian and Moayeri (2008) provides a guideline on security of VANETs.

Our proposal to design VANET applications considers five technical aspects: Transmission, Routing and Data Dissemination, Quality of Service, Security and Location.

A. Aspect 1: Transmission

The Dedicated Short Range Communication (DSRC) standard (Qian and Moayeri, 2008) provides a robust transmission for vehicular networks. Figure 1 shows the reserved bands of the radio electric spectrum. The spectrum was divided into seven 10MHz wide channels. Channel Ch178 is the control channel and it is restricted to safety communication. Channels Ch172 and Ch184 are reserved for accident avoidance applications and public safety communications. The rest, (Channels Ch174, Ch176, Ch180 and Ch182) are used for both safety and non-safety applications.

The standard 802.11p supports the dynamic nature of VANET environments. This standard contemplates the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol to access the medium. Another available family of protocols to access a shared medium in VANETS could be the Self-organizing Time Division Multiple Access (STDMA) which is specially designed for position messages (Sjöberg *et al*., 2010).

B. Aspect 2: Routing and Data Dissemination

Data dissemination in vehicular networks refers both to disseminating data that drivers are interested in and data that are used to keep connections established between nodes such as vehicle location, event notifications, etc.

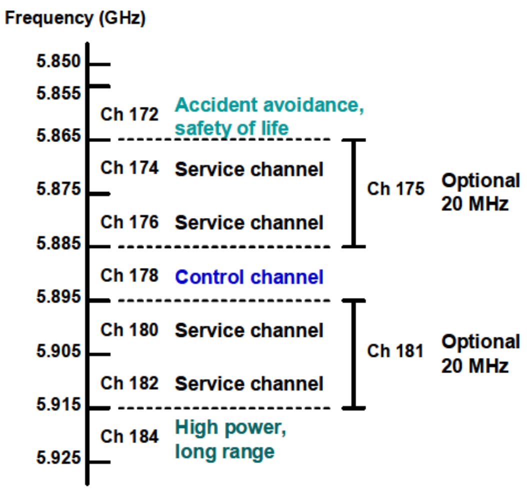

Figure 1. DSRC Channel assignment in North America (Quian and Moayeri, 2008).

Existing routing protocols have to be adapted in order to be used in vehicular networks. Depending on the type of road, density of vehicles, speed, etc. the kind of communication would not be the same. In cities traffic is less ordered than in highways, where there is only one road. The type of road is correlated with node density, in other words, there is not the same density on highways, than in cities or rural roads.

The speed of the vehicles may produce a partition in the network which currently is still an open challenge for the connectivity, and therefore, for the routing protocols. Moreover, because of the high mobility of VANETs, routing and data dissemination cannot be easily based on group addresses as ad hoc networks do but rely on the locations of nodes to determine the nodes in the delivery group. Data dissemination must consider a topology where node velocities may range from zero kilometres per hour, for stationary vehicles, to over 200 on highways.

Various attempts have been made to enhance routing and data dissemination by leveraging direction prediction and vehicle heading to improve performance. Chen *et al.* (2009a) presents a survey of geocast, broadcast and multicast technologies which can be applicable to Vehicle-to-vehicle (V2V) networks. Most of these methods use location techniques instead of topology-based approaches to predict route breakages and to take pre-emptive actions.

Critical safety applications require that geocast techniques disseminate data with high priority because the relevance of this information decreases with the distance to that location. In the same way, routing protocols do not have to lose time calculating the route. Thus, proactive protocols for VANETs, and more concretely for safety applications, are preferably used.

C. Aspect 3: Quality of Service

VANET applications require different classes of information priority. The sender specifies the priority parameters of messages (delay, jitter, bandwidth, loss rate, error rate). So, the VANET should act according to the priority parameters of the messages.

In road traffic scenarios, when an emergency event appears, the number of vehicles that will approximate to the accident may increase dramatically. This might create a mass of emergency messages in the VANET if they are broadcasted by every vehicle, leading to a collapse in the channel. To solve this problem in Menouar *et al.* (2006) the authors adapt the number of emergency messages that are going to be sent to the transmission rate. Some QoS requirements for VANET applications are presented in Chantaksinopas *et al.* (2012), Chen *et al.* (2009) and Qian *et al.* (2008b).

D. Aspect 4: Security

Intentional attacks can disturb the system either by jamming or overloading the channel with messages. Injecting false messages or rebroadcasting an old one are also possible attacks. The attacker can also steal or tamper with a car on-board unit or destroy an infrastructure.

Any malicious user behaviour could be fatal to other users. The attacker can also compromise the privacy of drivers by tracking and revealing their positions. Moreover, VANETs have to establish the liability of drivers and protect their privacy as much as possible.

In Qian and Moareri (2008) there is a classification of VANET security requirements. Some of them are:

Message authentication and integrity: Messages must be protected from any alteration and the receiver of a message must be able to corroborate the sender of the message.

Message Non-Repudiation: The sender of a message cannot deny having sent a message.

Access Control: Control the access to specific services which are provided by the infrastructures establishing what each node is allowed to do.

Message Confidentiality: The content of a message is kept secret from those nodes that are not authorized to access it.

Privacy and Anonymity: Conditional privacy must be achieved (driver's name, license plate, speed, position and travelling routes along with their relationships, has to be protected) while the authorities should be able to reveal the identities of message senders in case of a dispute such as a crime/car accidents, etc.

Liability Identification: As part of the "conditional privacy" above, the authorities should be able to reveal the identities of message senders in the case of a dispute.

E. Aspect 5: Location

VANET applications require different levels of accuracy regarding localization. Some applications can work with errors from 10 to 30 meters, while others, for example security distance warnings, require errors to be lower than 1 meter. Localization techniques for VANETS are detailed in Boukerche *et al.* (2008). We mention the main techniques:

Global Positioning System (GPS) is the easiest solution. However, as well as with other satellite-based systems, it is not always available. GPS receivers have an accuracy of 10 to 30 meters. A variant of GPS is *Differential GPS (DGPS)* which improves GPS calculating position with a known physical one. This difference will be broadcasted and this way, the other GPS receivers can correct their computed positions. Localization errors can be corrected to sub-meter precision, which will be suitable for most VANET applications.

Map matching technique combines roads databases with the actual position of the vehicle. It is able to estimate a trajectory by obtaining several position changes periodically. The possibilities are limited to roads or other places with vehicle access, getting a more accurate position.

Dead reckoning calculates current position by knowing the initial position and data such as speed, acceleration, time, distance and direction, which can be obtained by sensors placed in the vehicle. According to Boukerche *et al.* (2008) in 30 seconds, at a speed of 100km/h, the accumulated positioning error will be from 20 to 30 meters.

Cellular localization uses mobile cellular infrastructure to estimate the position of vehicles moving in the coverage area. Localization errors are up to 50 meters as it depends on factors such as the environment, the weather, the speed, etc. In indoor environments such as tunnels or parking lots, the signal from the base stations is more available as the one coming from satellites.

Relative position maps can be constructed with the information of a group of vehicles, exchanging the information between them and spreading the information with a multihop communication.

Data-fusion technique combines different techniques to end up with more reliable information. Data-fusion technique has been widely used for example in the SAFESPOT project (Menouar *et al.* where it is able to calculate the lane on which a vehicle is driving using neighbour messages. Figure 2 shows a data-fusion technique based on Boukerche *et al.* (2008).

IV. DESIGNING VANET APPLICATIONS

The proposed methodology support VANET applications: From the static ones to those that deal with dynamic and changing scenarios as weather changes, accidents, changes of driver's decisions, etc. We based our research in the six groups of applications presented in Qian and Moareri (2008): Life-Critical Safety Applications, Safety Warning, Electronic Toll Collection, Internet Access, Group Communication and RSU Service Finder.

Next, we present the proposed five main technical aspects (detailed in Section III) that should be specifically controlled for each group of applications. A specific table summarizes the proposed decisions for each group of applications. The values were obtained from an analysis of the references presented in Section III.

A. Life-Critical Safety Applications

Safety messaging is the most important aspect of VANETs, where the passive safety (accident readiness) in vehicles was reinforced with the idea of active safety (accident prevention). This group of applications includes: Intersections Warning, Collision Warning/ Avoidance, Cooperative Collision Warning, pre-crash sensing, lane change, etc. (Table 1).

B. Safety Warning Applications

This group includes applications like: Work Zone, Warning, Transit Vehicle Signal Priority, etc. (Table 2).

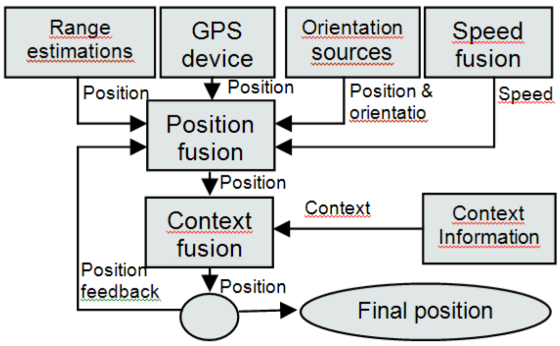

Figure 2 Data-fusion model.

Table 1: Technical aspects involved in Life-Critical Safety VANET applications

Transmission	Channel 172 Accident avoidance, safety of life
Routing and Data Dissemination	- Geocast - High priority data packets are sent continuously and periodically - Response time not applicable - Bidirectional protocols are not involved
QoS	- Delay < 250 ms - Jitter <100 - BW < 52 Mb/s (only messages with high priority should be sent at a time) - Loss and error rate =0 (retransmission is allowed)
Security	- Message authentication and Integrity - Message non-repudiation - Entity authentication - Liability Identification
Location	Differential GPS

Table 2 Technical aspects involved Safety Warning VANET applications

Transmission	Service Channels 174, 176,180, 182
Routing and Data Dissemination	- Geocast (the sender of the message determines a destination region for the message to be sent and attaches it to the message) - Response time not applicable - Bidirectional protocols are not involved
QoS	- Delay < 250 ms - Jitter <100 - BW < 52 Mb/s (Messages should indicate their priority to adapt forwarding accordingly) - Loss and error rate =0 (retransmission is allowed)
Security	- Message authentication and Integrity Message non- repudiation - Entity authentication - Liability Identification
Location	Differential GPS

Table 3: Technical aspects involved in Electronic Toll Collection and e-commerce VANET applications

Transmission	Service Channels 174, 176,180, 182
Routing and Data Dissemination	- Unicast - Data in the packets is generated by the sender. - Response time 2 - 4 seconds - bidirectional protocols are involved - Communication is single-hop - Information in packets is not forwarded
QoS	- Delay < 400 ms - Jitter has little impact - BW < 24 Mb/s (it increases according to the security measures) - Loss and error rate =0 (retransmission is allowed)
Security	- Access Control - Message Authentication and Integrity - Message non-repudiation - Message Confidentiality - High privacy requirements - Liability Indentification
Location	Local infrastructured location techniques

C. Electronic Toll Collections, e-commerce

This group of VANET applications allows that each vehicle can pay the toll electronically when it passes through a Toll Collection Point or make e-commerce operations in a RSU (Table 3).

D. Internet Access

These applications enable passages of the vehicles to connect to the Internet (Table 4).

E. Group Communications

Many drivers may share some common interests when they are on the same road and on the same direction, so they can use the VANET Group Communications function (Table 5).

F. RSU Services Finder

This group involves applications such as: find restaurants, gas stations, etc., in the nearby area along the road. A road side services database will be installed in the local area that connected to the corresponding RSUs (Table 6).

Table 4. Technical aspects involved in Internet Access VANET applications.

Transmission	Service Channels 174, 176,180, 182
Routing and Data Dissemination	- Unicast - Response time < 5 second - Bidirectional protocols are involved
QoS	- Delay < 400 ms - Jitter has little impact - BW < 30.5 Mb/s - Loss and error rate =0 (retransmission is allowed)
Security	- Access Control - Confidentiality for unicast - Symmetric key between vehicles and RSU through public key cryptography
Location	Data-fusion techniques

Table 5: Technical aspects involved in Group Communication VANET applications.

Transmission	Service Channels 174, 176,180, 182
Routing and Data Dissemination	- Broadcast - Continuous update of information among all neighbouring nodes (position, speed, heading) - Location-based routing approaches are suitable
QoS	- Response time 1 second - Delay < 200 ms - Jitter has little impact - This group of applications transmit plain character so the BW requirement is quiet small < 1Mb/s - Loss and error rate =0 (retransmission is allowed)
Security	- Access Control - Authentication requirements - Liability Identification - Message confidentiality - Message non-repudiation - Message authentication and Integrity
Location	Data-fusion techniques

Table 6: Technical aspects involved in Roadside Service finder VANET applications

Transmission	Service Channels 174, 176,180, 182
Routing and Data Dissemination	- Unicast - Communication may consist of a single hop, or route messages over multiple hops toward the destination - Location-based routing approaches are suitable
QoS	- Response time < 5 seconds - Delay < 400 ms - Jitter has little impact - BW < 30.5 Mb/s - Loss and error rate =0 (retransmission is allowed)
Security	- Access Control - Message Confidentiality - Message Authentication and Integrity
Location	- GPS+ Map matching

V. EXAMPLE OF A VANET APPLICATION DESIGN

As an example of the proposed method we design an application to deal with the common issue of finding parking in a city. The application reduces searching time for parking. When the driver arrives to destination, he/she will push the "search-parking" button, and will start receiving information about the parking lots that are near to his/her position, giving him/her the chance to decide and park in the nearest free lot. The information required in this application contains the coordinates of the free parking lot and its length, since it is not the same parking a truck than a small car.

The proposed parking application has basically two ways of being executed depending on where the received information is coming from.

Modality "A" if near vehicles driving through provide the data (see Fig. 3). Vehicles communicate -via geocast- with each other to notify the availability of a parking lot. This modality is classified as a "Group Communications" application (see Table 5). It involves vehicle-to-vehicle communications.

Modality "B" if data is coming from the infrastructures (see Fig. 4). Vehicle requests a parking to the "RSU service finder" (see Table 6) involving vehicle-to-road side communications.

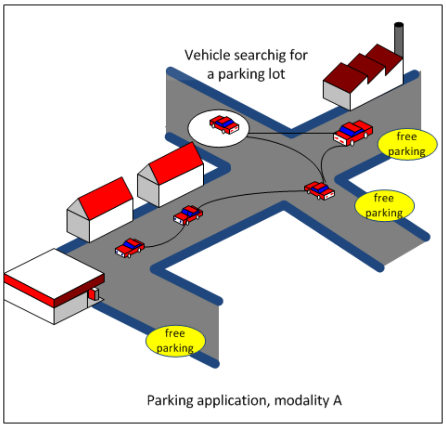

Figure 3. Parking application. Modality A

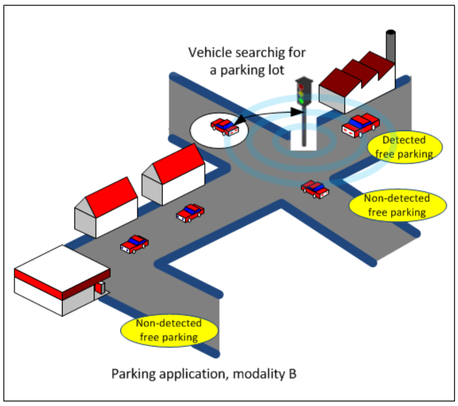

Figure 4. Parking application. Modality B

Next, we summarize the technical aspects required by the parking application:

A. Aspect 1. Transmission

Both modalities should use the channels for non safety applications, this is, Channels Ch174, Ch176, Ch180 and Ch182.

B. Aspect 2. Routing and Data Dissemination

The parking application in the modality A requires that the coordinates of the free parking lot not to be broadcast through big areas. For the user, it is useful to know where to park near his/her destination. This could be controlled by limiting the life of every packet or using a geographical protocol. Fracchia (2006) estimated location-based protocol that limit the coverage area of the node that finds a parking lot by knowing its neighbour vehicles' speed and direction.

On the other hand, in the modality B, depending on the capabilities of the RSU, infrastructural nodes may simply emit data to the network or have complete ad hoc functionality and thus may be used for forwarding like other vehicles. This modality requires unicast protocol. The vehicle requesting a free parking lot location determines a geographical region (in the message request) that is sent to the RSU. The RSU uses fusion location techniques to get location information about the free parking lots in the geographical requested area and communicate it to the vehicle that requested the parking lot.

C. Aspect 3. QoS

The parking application does not have any QoS requirements to work properly and due to delay in the transmission is not critical, either a proactive or a reactive protocol can be used. Still, using a proactive protocol means problems with bandwidth and table maintenance. So, we suggest using an active protocol or a geographical protocol, where the positions of the nodes' one-hop neighbours are known.

D. Aspect 4. Security

Authentication is needed in order to avoid the introduction of false free parking lots that would collapse the system or completely tarnish its functionality. Instead of saving time to park, we would waste more time going to the false free lots, and the application would lose its reliability.

For the modality A, privacy requirement is necessary because other users should not know which vehicle has parked or which one is sending the information Tracking of vehicles should be avoided, at least at user level. On contrast, for the modality B, the RSU are stationary nodes that do not have any relation with people or companies, so the application does not need to protect their privacy.

E. Aspect 5. Location

We propose to use GPS techniques to solve the location problem because our requirements of accuracy would be around a precision of 10 meters in the given coordinates of the free parking lot. This is enough for the user to find the free space in the streets.

GPS efficiency is rather low in tunnels, subways, etc. as the direct view to the satellites may be lost. This would not represent a problem due the application is thought to be working in the street, where the GPS has a good coverage. However, it could be useful to have a combination of the GPS together with a specific map of the city.

F. Simulation and Results

We perform a simulation study to analyse parameters of the parking application in both modalities A and B. See Fig. 3 and Fig. 4.

We carried out several simulations in a discrete-event simulator developed in C++ (Omnet, 2014). The simulation model is based on the average of a set of 30 replications, and the adopted confidence level for the mean was 95%. Each replication represents a simulation of 15 minutes of operation of the network.

In order to evaluate the performance of the application we analyzed the packet end-to-end delay and packet loss rate. The aim of these variables is to quantitatively determine the packet loss average and the average end-to-end delay produced since a vehicle requests a parking space until it receives an answer.

We define a 1km zone where we put several traffic lights representing Road-Side-Units and several fixed devices representing parking spaces located on roadsides. We study the impact of the number of vehicles on the performance of the application. Speed limit for vehicles is 50 km/h. We considered vehicles spawned from two directions and the number of vehicles varies from 20 to 100.

Figure 5 shows the end-to-end delay obtained by both modalities. We can observe that when the number of vehicles is small, modality B obtains better results in comparison with Modality A. However as the number of vehicles is increasing, the modality A obtains a better delay, reducing the average latency almost 28% in comparison with Modality B. Due to the number of request is increased, the response time from traffic lights considerably increases. However, as we can observe from the results, both modalities accomplish the limits of maximum delay to provide QoS.

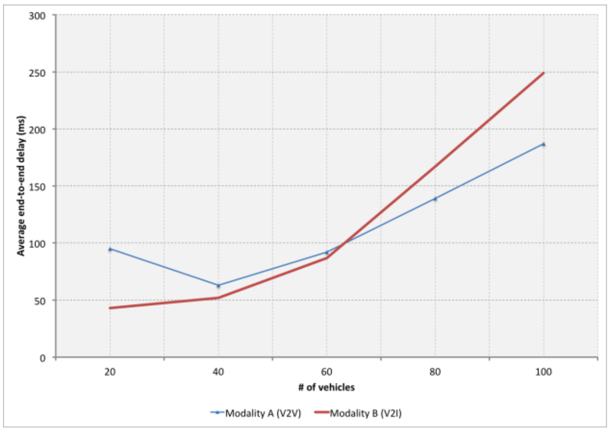

Figure 5. End-to-end delay

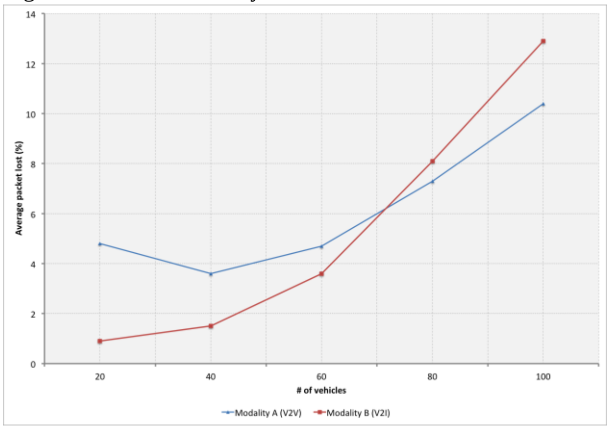

Figure 6. Packet loss rates.

Figure 6 shows the average packet lost obtained by both modalities. When the number of vehicles is small, modality B obtains better results, reducing the average packet lost almost 75% in comparison with modality A. However as the number of vehicles is increasing, the modality A obtains a better result, reducing the average packet lost almost 20% in comparison with Modality B. Due to the number of request is increased, the response time from traffic lights considerably increases.

VI. CONCLUSIONS

We analysed which protocols and tools of VANETS would fit best for user applications. We discussed advantages and shortcomings of five main technical aspects from the VANETs (Transmission, routing and data dissemination, QoS, security and location). This analysis was made for 6 different groups of VANETs applications (Life-Critical Safety Applications, Safety Warning, Electronic Toll Collection, Internet Access, Group Communication and RSU Service Finder).

Finally we detailed an example of a VANET design application in charge of notifies all interested drivers about free parking lots in some specific area.

REFERENCES

ASESGA, Spanish association of car parks and garages. http://www.asesga.org, Accessed December 2014 (2014).

Boukerche, A., H. Oliveira, E.F. Nakamura and A.F. Loureiro, "Vehicular Ad Hoc Networks: A New

Challenge for Localization-Based Systems," *Computer Communications*, **31**, 2838-2849 (2008).

CAR 2 CAR, *Communication Consortium Manifesto. Overview of the C2C-CC System*, http://elib.dlr.de/48380/1/C2C-CC_manifesto_v1.1.pdf, [Accessed December 2014] (2007).

Chantaksinopas, I., W. Lee, A. Prayote and P. Oothongsap, "Delay-Sensitive Applications in VANET and Seamless Connectivity: The Limitation of UMTS Network," *International Journal of Computer Science and Network Security*, **12 (**2012).

Chen, W., R.K. Guha, T.J. Kwon, J. Lee and Y.-Y. Hsu, "A survey and challenges in routing and data dissemination in vehicular ad hoc networks," *Wireless Communications and Mobile Computing*, **11**, 787-795 (2009a).

Chen, R., D. Ma and A. Regan, "TARI: Meeting Delay Requirements in VANETs with Efficient Authentication and Revocation," *2nd IEEE International Conference on Wireless Access in Vehicular Environments (WAVE)* (2009b).

DGMTEC, *Intelligent transport systems in action*, Directorate-General for Mobility and Transport of the European Commission (2011).

Do, Y., S. Buchegger, T. Alpcan and J.P. Hubaux, *Centrality Analysis in Vehicular Networks*, Technical report T-Labs/EPFL (2008).

Fracchia, R., "Knowing Vehicles Location HELPs Avoiding Broadcast Packets Storm," *Fourth IEEE International Conference on Pervasive Computing and Communications Workshops*, 118-123 (2006).

Jiang, D. and L. Delgrossi, "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments," *IEEE Vehicular Technology Conference*, 2036-2040 (2008).

Menouar, H., F. Filali and M. Lenardi, "A survey and qualitative analysis of mac protocols for vehicular ad hoc networks," *IEEE Wireless Communications*, IEEE , **13**, 30-35 (2006).

Menouar, H., M. Lenardi and F. Filali, "Improving Proactive Routing in VANETs with the MOPR Movement Prediction Framework," 7th International Conference on ITS Telecommunications, 1-6 (2007).

Omnet, *Discrete event simulation system,Omnet ++ Community Site*, Omnet ++ 4.1 http://www.omnetpp.org/ (2014).

Popescu, C., "Case study: project CIVITAS-SUCCESS", *International conference on Mathematical models for engineering science* (2010).

Qian, Y. and N. Moayeri, "Design of Secure and Application-Oriented VANETs," *IEEE Vehicular Technology Conference*, 2794-2799 (2008).

Qian, Y., K. Lu and N. Moayeri, "A secure vanet mac protocol for dsrc applications," *IEEE Global Telecommunications Conference,* New Orleans, LO. 1-5 (2008).

Schoch, E., F. Kargl, T. Leinmüller and M. Weber, "Communication Patterns in VANETs," *IEEE Communications Magazine*, **46**, 2-8 (2008).

Sjöberg, K., E. Uhlemann and E.G. Ström, "Medium Access Control in Vehicular Ad Hoc Networks," *IEEE VTS Workshop on Wireless Vehicular Communications*, Halmstad University, Sweden (2010).

Received: April 11, 2014.

Accepted: January 30, 2015.

Recommended by Subject Editor: José Guivant.