A Vehicular Network Mobility Framework: Architecture, Deployment and Evaluation

José Santa, Pedro J. Fernández, Fernando Pereñíguez, Fernando Bernal, Antonio F. Skarmeta

***Abstract*—Research on vehicular networks has increased for more than a decade, however, the maturity of involved technologies has been recently reached and standards/specifications in the area are being released these days. Although there are a number of protocols and network architecture proposals in the literature, above all in the Vehicular Ad-hoc Network (VANET) domain, most of them lack from realistic designs or present solutions far from being interoperable with the Future Internet. Following the ISO/ETSI guidelines in field of (vehicular) cooperative systems, this work addresses this problem by presenting a vehicular network architecture that integrates well-known Internet Engineering Task Force (IETF) technologies successfully employed in Internet. More precisely, this work describes how Internet Protocol version 6 (IPv6) technologies such as Network Mobility (NEMO), Multiple Care-of Address Registration (MCoA), IP Security (IPsec) or Internet Key Exchange (IKE), can be used to provide network access to in-vehicle devices. A noticeable contribution of this work is that it not only offers an architecture/design perspective, but also details a deployment viewpoint of the system and validates its operation under a real performance evaluation carried out in a Spanish highway. The results demonstrate the feasibility of the solution, while the developed testbed can serve as a reference in future vehicular network scenarios.**

***Index Terms*—V2I; vehicular networks; testbeds; IPv6; 802.11p; Intelligent Transportation Systems.**

I. Introduction

In the near future, computer communications are expected to be the cornerstone in vehicular cooperative systems. Current systems for traffic monitoring, route guidance or entertainment services for vehicles, are planned to be complemented with novel telematic proposals in the short term, due to the vast amount of research in vehicular communications and cooperative systems that has appeared in the last years.

As a result of the great research efforts in cooperative ITS, we are now immersed in the phase of developing previous theoretical or simulated advances and getting preliminary results prior to the real operation of commercial services over real platforms. The European Union has recently financed projects for Field Operational Tests (FOT), such as the recent DRIVE C2X [1] or FOTsis [2]. In parallel to these projects, additional efforts have been put on standardizing an interoperable communication architecture in vehicular cooperative systems. First, the ISO TC 204 released the Communications Access for Land Mobiles (CALM) concept, but the later created group ETSI TC ITS improved CALM based on the results of the COMeSafety European project [3].

Current lines of publicly founded projects are implementing communications stacks conforming with the previous standards. Many of these initiatives have shown an interest on IPv6 communications, since numerous ITS services will be based on current Internet standards. However, essential issues such as global addressing or network mobility of nodes (i.e. hosts on vehicles) have not been considered in implementations until recent days. The ITSSv6 project [4], concluded in 2014, worked on this line, proposing an implementation of a communications stack based on current standardized Internet protocols, which has been ported to several FOT initiatives such as FOTsis.

The maturity of 3G/4G and the more recent vehicular WiFi (IEEE 802.11p), together with the penetration issues that imply vehicle to vehicle (V2V) communications, implies that vehicle to infrastructure (V2I) communications are expected to be firstly exploited. It is in the V2I segment where novel traffic efficiency, comfort services and relaxed safety applications can be initially tested and deployed. For this reason, this research work is framed in this communication domain and presents a comprehensive vehicular communications stack compliant with the ISO/ETSI standards that integrates a secure mobility solution by means of well-known and standardized Internet technologies such as Network Mobility (NEMO), Multiple Care-of Address Registration (MCoA), IP security (IPsec) or Internet Key Exchange (IKE), which favors its potential adoption by car manufacturers or road operators. Unlike existing works, this proposal not only presents a conceptual design, but also validates the proper operation of the communications stack through a deployment architecture and its application in a real test site in the Spanish A2 highway, in frames of the FOTsis project.

The paper is structured as follows. Section II places this paper in the research context, taking as reference a set of related cites in the literature. Section III reviews the reference ISO/ETSI communication stack and the proposal developed in this work. The general network deployment model is presented in Section IV, which has been replicated in the reference test-site evaluated in Section V. Finally, Section VI concludes this work with a set of final remarks and presenting our future research lines.

José Santa is with the Department of Engineering and Applied Technology, University Centre of Defence at the Spanish Air Force Academy, San Javier, 30720 Spain, and with Department of Information and Communication Engineering, University of Murcia (UMU), 30100 Spain, email: jose.santa@cud.upct.es|josesanta@um.es

Pedro J. Fernández, Fernando Bernal and Antonio F. Skarmeta are with UMU, e-mail: (pedroj|fbernal|skarmeta)@um.es

Fernando Pereñíguez is with Catholic University of Murcia, 30107 Murcia, and with UMU, email: fpereniguez@ucam.edu|pereniguez@um.es

[1] http://www.drive-c2x.eu

[2] http://www.fotsis.com

[3] http://www.comesafety.org

[4] http://itssv6.eu

II. State of the Art

The integral, realistic and experimental dimensions of the proposal presented in this work are non-frequent aspects in the literature. In the context of FOT projects one could find some articles in the line of supplying frameworks for vehicular integral communication. The authors of [1], for instance, present the testing framework for the DRIVE C2X project that, unfortunately, is not concerned with the use of IP-based communications, which are left out for management and testing purposes. A similar work about the simTD project is presented in [2], but it is specially focused on security and privacy. The work conducted in frames of the ITSSv6 project is based on the usage of IPv6 technologies in vehicular communications. Research results achieved by this project have been published by authors in [3], [4] as well as by some colleagues in [5] where it is reported their experience performing packet delivery ratio tests using the 802.11p technology, which are in line with the results gathered in the work.

Apart from specific project proposals, the work presented in [6] develops an experimental testbed to validate an on-board solution for providing vehicular communications through a "car gateway", which is similar to the concept of mobile router. However, this solution is highly coupled with the vehicular platform and does not follow the ISO/ETSI guidelines. The work presented in [7] is nearer to the testbed presented in this paper, although a constrained communications stack is used for an experimental evaluation of a concrete routing and flow management subsystem using IPv6 with 3G and common WiFi. In [8] the Network Mobility (NEMO) protocol is evaluated in a real environment with two WiFi access points, however, the good results obtained in this work (no data looses during handovers) are attributed to the limited testbed where a trolley is used to move the "on-board" equipment. This scenario is far from the real evaluation carried out in this paper in a real highway environment.

Exclusively evaluating the usage of the 802.11p technology in testbeds, there are works in the literature such as in [9], which an exhaustive evaluation of roadside to vehicle communications is performed especially attending the vehicle speed, or in [10], this time carrying out a great testing campaign in a city. In this last case it is anlyzed the impact of the physical environment in the expected performance of the network. In our case, a great contribution of the work is using the 802.11p technology in real highways, as opposed to the common use in urban settings. This implies changes in the vehicle speed and issues regarding the installation of the access points along the road to improve the communication range.

III. IPv6-Based Vehicular Communications Stack

This section describes the vehicular communications stack used in this research work, which is an extended version of the ISO/ETSI one.

A. ISO/ETSI Station Reference Architecture

In an effort towards harmonization, the international ITS community agreed on the definition of a common ITS communication architecture suitable for a variety of communication scenarios (vehicle-based, roadside-based and Internet-based) through a diversity of access technologies (802.11p, infra-red, 2G/3G, satellite, ...) and for a variety of application types (road safety, traffic efficiency and comfort/infotainment) deployed in various continents or countries ruled by distinct policies. This common communication architecture is known as the *ITS station reference architecture* and is specified by ISO in [11] and by ETSI in [12]. As depicted in Fig. 1, the ITS station architecture follows an *Open Systems Interconnection* (OSI) like layered design: *access*, *networking & transport*, *facilities* and *applications*. Additionally, two cross-layer entities are defined: *ITS Station Management Entity* (SME) and *ITS station Security Entity* (SSE).

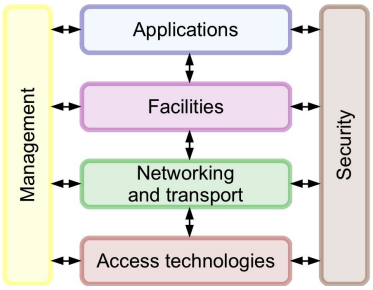


Figure 1. ISO/ETSI reference communications stack

There exists different types of ITS stations (ITS-S): *personal ITS-S* (e.g. smartphones), *vehicle ITS-S* (e.g. cars), *roadside ITS-S* (e.g. electric charging station) or *central ITS-S* (e.g. road operator control center). Each ITS station type implements a subset of the functionalities of the general ITS station reference architecture according to the played role. In the most general case, the functions of an ITS-S are split into a router (ITS-S router) and hosts (ITS-S host). The first one is a node comprised of routing functionalities that is used to connect two networks and forward packets, the ITS-S host is a final node executing specific ITS applications. ITS-S hosts are attached to the ITS-S router via some ITS station internal network.

B. IPv6-Extended Stack Design

The vehicular communication architecture used in this work is based on the previous ISO/ETSI reference stack, which has been extended with IPv6 technologies, as described in [3]. Fig. 2 shows a simplified view of this platform, including three of the previously described ITS-S: vehicle ITS-S, roadside ITS-S and central ITS-S.

In the vehicle the stack functionality is split into the vehicle ITS-S host and vehicle ITS-S router (also known as Mobile Router - MR). The MR includes the needed functionalities to hide networking tasks to in-vehicle hosts, which could connect to the network by means of the MR through WiFi or Ethernet. To maintain external communications with roadside equipment and the control centre, the following communication technologies are integrated: 3G/UMTS, WiMAX, WiFi and 802.11p (ETSI G5-compliant). IPv6 connectivity is supported by the set of elements included within the networking and transport layer of the MR. On one hand, Network Mobility (NEMO) [13] is in charge of maintaining reachability for the whole in-vehicle

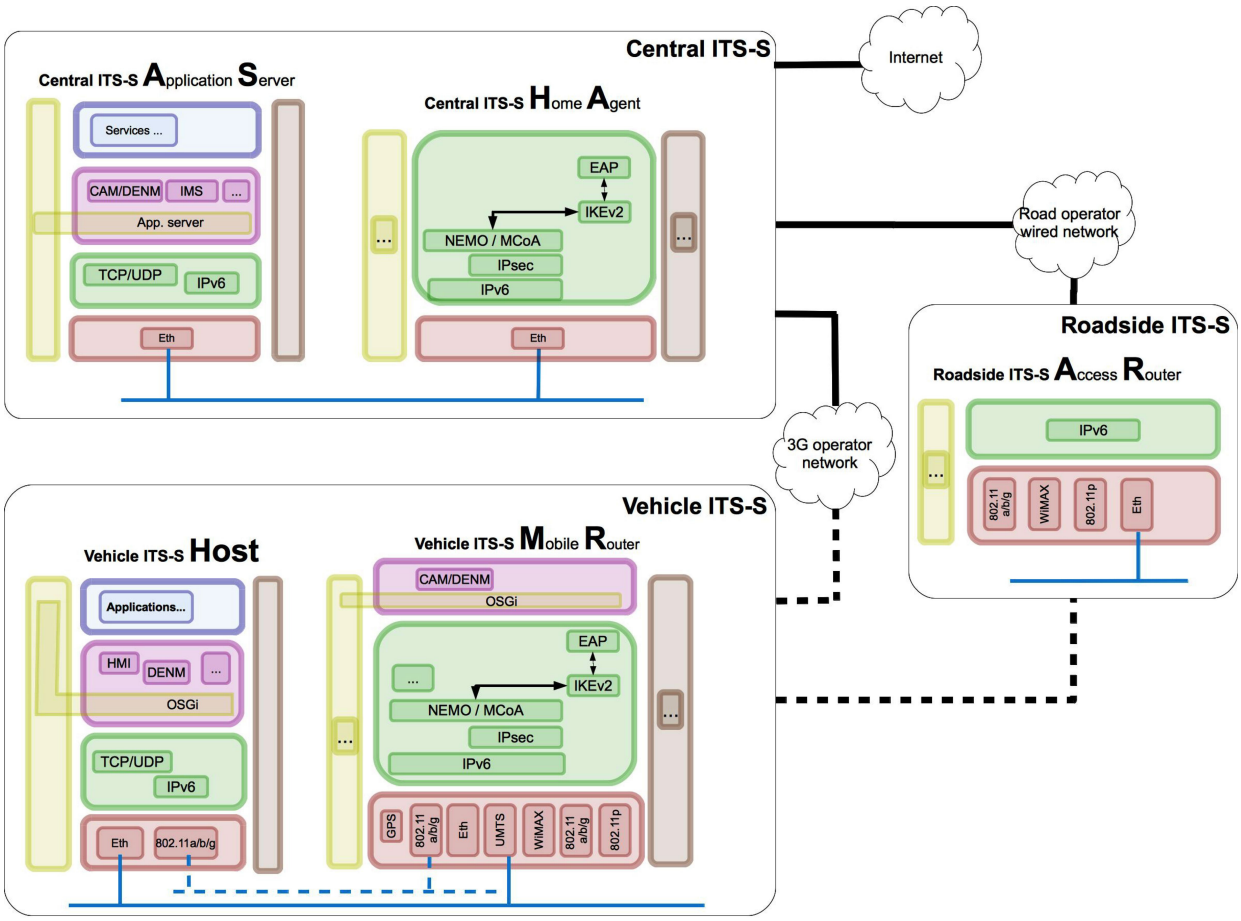


Figure 2. Overall design of the reference vehicular communications stack

IPv6 network. Additionally, to support the multi-homed configuration of the mobile router, the NEMO operation is assisted with Multiple Care-of Addresses Registration (MCoA) [14]. Regarding security, the mobile router is equipped with Internet Protocol Security (IPsec) [15].

The stack on the Vehicle ITS-S Host is in charge of executing final applications that could access remote services. As observed, this stack includes a common networking middleware based on the Transport Control Protocol (TCP) and User Datagram Protocol (UDP). The facilities layer, based on the Open Service Gateway Initiative (OSGi), includes CAM (Cooperative Awareness Message) and DENM (Decentralized Environmental Notification Message) messaging modules (apart from other functionalities) to make easier the implementation of applications.

The communications stack instantiated in the roadside ITS-S access router acts as network attachment point for vehicles using short/medium-range communication technologies. Similarly to the MR, the available wireless technologies to communicate with vehicles are WiFi, 802.11p and WiMAX.

Finally, in the upper part of Fig. 2 we can see the communications stacks for both the Central ITS-S Application Server (ITS-S AS) and the Central ITS-S Home Agent (Central ITS-S HA). The former hosts ITS services managed by the central ITS-S, while the latter is necessary for maintaining the connectivity of vehicles upon the change of point of attachment to the road, acting as NEMO Home Agent (HA). For this reason, the modules included in the network layer are equivalent to the ones included at the same layer in the MR. Since IPv6 security is applied between the MR and the mobility/security server, represented by the HA, equivalent security modules are used in both entities.

IV. Deployment Architecture

On the basis of the previous stack design for the different entities involved in our V2I scenario, it is now possible to create a deployment architecture using real modules. This is showed in Fig. 3. Initially, it is noticeable the direct mapping among the different entities included in this diagram and the communication nodes described in the previous section. For the sake of clarity, only two roadside ITS-S and one vehicle ITS-S are included. For a reference testbed it is not necessary to replicate the functionality of the central ITS-S Home Agent and Application Server in multiple servers.

Fig. 3 shows the two available communication routes between the vehicle and the central ITS-S: the 802.11p one, using the control channel of the ETSI G5 profile; and the one provided by using the 3G operator's infrastructure. A testing addressing scheme is also showed and, due to the 3G operator used does not provide IPv6 connectivity, an OpenVPN tunnel over IPv4 has been used. A wired connection is used between the roadside ITS-Ss and the central ITS-S, which is supposed

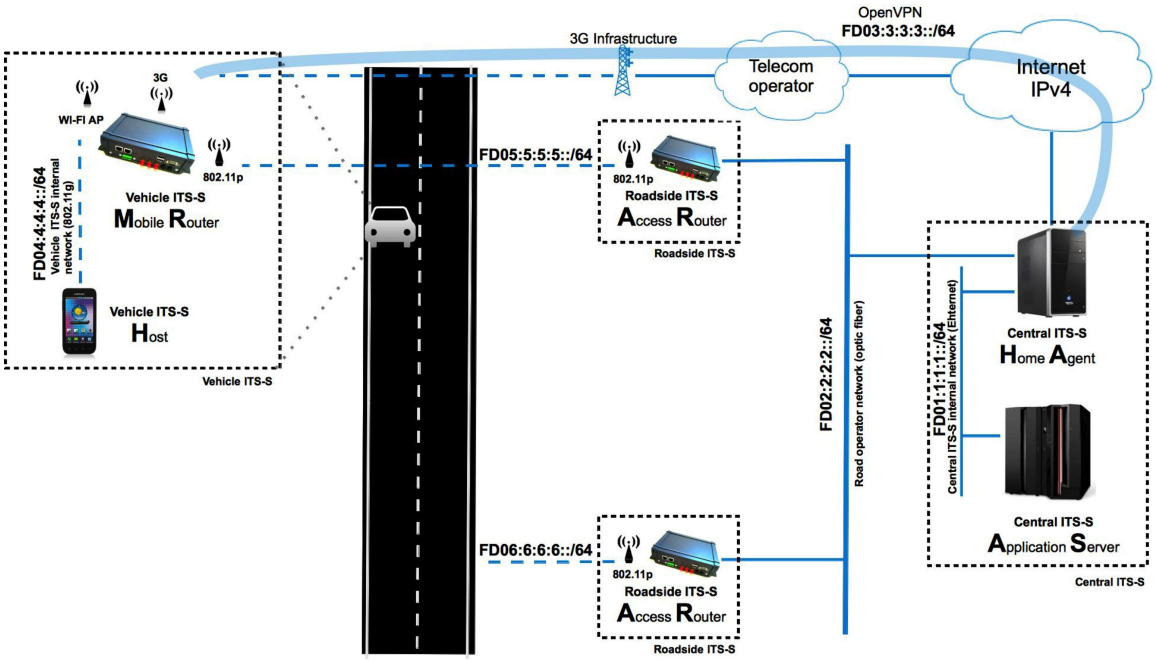


Figure 3. Deployment architecture of the vehicular network

to be installed in the control centre premises of the highway. Here, the central ITS-S Home Agent acts as a border router, interconnecting the roadside network segment with the whole central ITS and the Internet. The wired connection between each roadside ITS-S and the central ITS-S is supposed to be established over the communication infrastructure of the road operator, which is usually a fiber optic channel.

In the test-site later explained the roadside ITS-Ss are installed next to the road, using the available road infrastructure, while the vehicle ITSs are mounted in common vehicles. The 12-volts lighter connection is enough to connect the mobile router, which offers connectivity to in-vehicle hosts through a common WiFi connection based on IEEE 802.11g.

V. Testbed and Performance Evaluation

The previous deployment architecture has been used in several test-sites in frames of the FOTsis project. In this section it is describes the real deployment conducted in the Spanish A2 highway (3rd stretch), near Zaragoza.

A. Equipment Used

The equipment used in the test site is detailed in Table I. The same base hardware is used for both the MR and the AR, in which the ITSSv6 software stack has been installed. It integrates the mobility and security services previously described. A stick antenna is mounted in each roadside ITS-S for 802.11p communications, and a roof antenna is used in each vehicle ITS-S, supporting 802.11p/3G/GPS. Both antennas are designed to improve the communication performance in terms of gain and radiation pattern.

B. Test Site Preparation

The roadside ITS-Ss have been installed at KP 139+00 and KP 146+00 of the A2 highway, as showed in Fig. 4, while the central ITS-S equipment is installed in the highway control centre. The HA and AS are wired to the control centre local network, which has external connection with Internet and the roadside ITS-Ss. The two ARs have been installed in roadside cabinets used for electronic devices at the selected points of the road, where power supply and network connection is available. They are connected with an optic fiber to Ethernet switch also available in the cabinet. In order to enable IPv6 communications within the road operator network, a separated virtual local area network (VLAN) was set up with the switch ports used by each AR and the pair of terminating ports in a local switch available in the control centre.

Regarding the vehicle ITS-S, which can be seen in Fig. 5, it is installed in a common vehicle in the tests. The combined 3G/802.11p/GPS antenna is affixed on the vehicle roof, as can be seen in Fig. 6. The tests were also focused to validate

Table I
Hardware components used in the test-sites

Network Nodes		
Node	**Hardware**	**Software**
MR	Laguna LGN-00-11/LGN-20	ITSSv6 stack
Host	Laptop, Intel i7, 4GB	Ubuntu 12.4
Host	Samsung Galaxy Tab II	Android 4.0.3
HA	Asus eeBox EB1501P	ITSSv6 stack
AS	PC Intel i5, 3.1Ghz, 3GB	Ubuntu 10.4
AR	LGN-20	ITSSv6 stack
Communication hardware		
Item	**Model**	
802.11p transceiver	Unex DCMA-86P2 mini-PCI in AR/MR	
Vehicle antenna	Omni-combined 3G/ 11p/ GPS 7dBi	
Roadside antenna	Omni-stick 12dBi	
3G modem	Ovation MC950D (only for LGN-00-11)	

Figure 4. IRoadside ITS-S in the A-2 highway

the capability of the mobile network to route the packets generated by an independent on-board unit provided by the GMV company, which generates packets using the Point-to-Point Protocol (PPP) over a serial link.

Figure 5. Vehicle ITS-S used in the A-2 highway

Figure 6. Vehicle antenna

C. Performance Evaluation

The network was tested to check its performance in terms of the throughput and delay. For measuring the network throughput, a constant data rate of 250 Kbps was generated from the central ITS-S HA to the vehicle ITS-S host, connected to the MR. The data rate was fixed to this value due to the 3G limitations checked in the area, which is attributed to a poor network deployment of the telecom operator. It is important to consider that this test-site is quite far from big urban areas, and this could be the reason. The results can be seen in Fig. 7a. The vehicle has been driven at a speed between 80 and 100 Km/h, and the test starts at the control centre, far from both roadside ITS-Ss, and then passes the first roadside ITS-S (marked as "RSU1") and later the second roadside ITS-S (marked as "RSU2"). Although a low data rate is used, the limitations of the 3G network and the impact of mobility is noticeable in the results. However, in the segments where 802.11p is used the network throughput recovers.

A delay study was performed by using the *ping* tool in the host to generate ICMP Echo Request messages and receive the correspondent ICMP Echo Replay messages. The round-trip delay time (RTT) results are showed in Fig. 7b. Since the car passes two times the two roadside ITS-Ss, four 802.11p connectivity periods are visible in the RTT results. As can be seen, the delay here is around 10 ms, while the 3G technology could imply RTT values of one second. Attending to the results, it is also noticeable a lack of connectivity just after the pass near the AR. This is due to the time needed for carrying out the handover back to 3G, which is performed when AR advertisements do not arrive through this link for a period of time configured in the NEMO software.

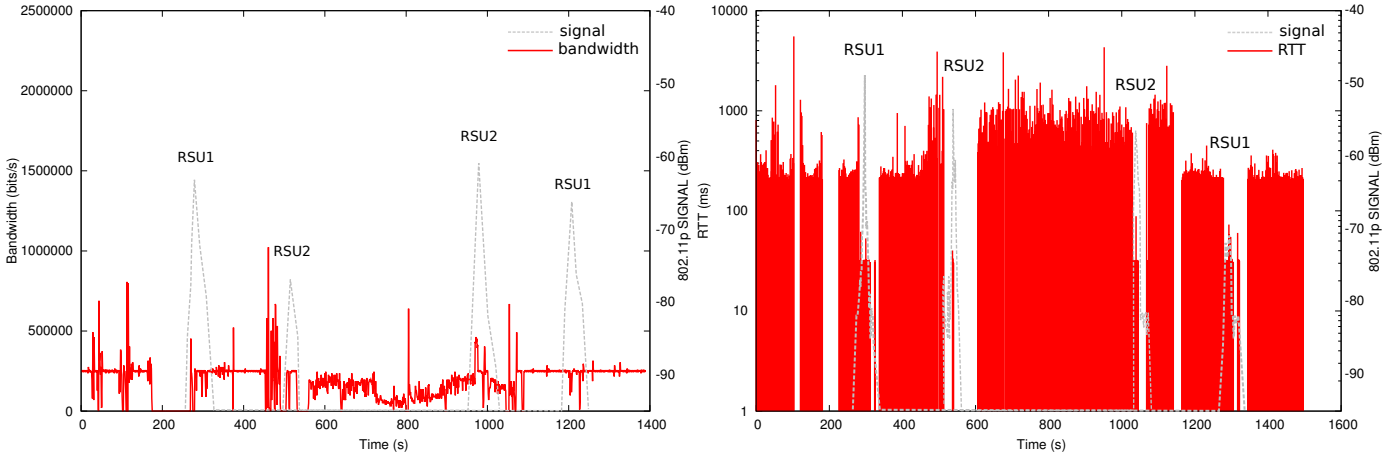
D. Discussion

In the road segments where 802.11p connectivity is available, it can be seen in the results how NEMO works correctly, by changing the data flow to use a proper communication channel. As expected, the throughput is better with 802.11p, covering the requested data rate, although the maximum achievable bandwidth can exceed 5 Mbps, according to our previous research [4]. The delay improvement is even greater than with throughput, as compared with 3G. RTT values bellow 10 ms have been gathered, which is a performance similar to common WiFi networks.

Considering the previous results, services deployed over a network like the one presented cover a wide range of possible traffic efficiency applications, such as route guidance, dynamic speed limit, congestion avoidance and mitigation, or road traffic monitoring. Moreover, in the area of comfort and entertainment, the possibility of accessing directly to the Internet offers many possibilities to our model. Regarding safety, delay-relaxed applications such as notification of road accidents, or incidents in general, could be supported, but others requiring direct low-delay communications among vehicles, such as forward collision avoidance, fall out of the network model analyzed. However, it is important to remark how V2V communications are possible in the network architecture exploited in this work, since all communication nodes in the network are IPv6-addressed.

VI. Conclusion

The work presented in this paper addresses three main objectives: first, describes a network architecture with a proper communications stack based on ISO/ETSI standards and IETF technologies to present an IPv6 access to future telematic



(a) UDP throughput from the host perspective

(b) Network delay

Figure 7. Network throughput in the A-2 test-site (Spain)

services; second, creates a deployment architecture of the proposal prepared to be installed in real scenarios; and third, sets up and evaluates a reference testbed in a highway.

The results gathered from the experiments validate the correct operation of the network architecture and allow us to assess the performance of the solution. The network has been able to route data packets using alternatively 3G or 802.11p thanks to the NEMO technology. This has been performed in a real highway with vehicles moving at realistic speeds. Nevertheless, we have checked that some parts of our system could be improved through several parallel research lines. The work described in [4] envisages how the IEEE 802.21 specification can improve the handover operation diminishing the network transition time, above all when passing from 802.11p to 3G. Another line is focused on the security aspects in IPv6 vehicular communications, further evaluating the use of IPsec and IKE. A third line is the authentication to access vehicular networks and, especially, the ones provided by road operators. A vehicular authentication framework is being designed and developed solving this issue, based on EAP (Extensible Authentication Protocol) and PANA (Protocol for Carrying Authentication for Network Access).

ACKNOWLEDGMENT

This work has been sponsored by the EU 7th Framework Program through the FOTsis, GEN6 and Inter-Trust projects (contracts 270447, 297239 and 317731).

REFERENCES

[1] R. Stahlmann, A. Festag, A. Tomatis, I. Radusch, and F. Fischer, "Starting European Field Tests for Car-2-X Communication: The Drive C2X Framework," in *18th ITS World Congress and Exhibition 2011*, ser. ITS World Congress '11, 2011.

[2] C. Weib, "V2X communication in Europe: From research projects towards standardization and field testing of vehicle communication technology," *Computer Networks*, vol. 55, no. 14, pp. 3103 – 3119, 2011.

[3] J. Santa, F. Pereñiguez, A. Moragón, and A. F. Skarmeta, "Experimental evaluation of CAM and DENM messaging services in vehicular communications," *Transportation Research Part C: Emerging Technologies*, vol. 46, no. 0, pp. 98 – 120, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0968090X14001193

[4] J. Santa, F. Pereniguez-Garcia, F. Bernal, P. Fernandez, R. Marin-Lopez, and A. Skarmeta, "A framework for supporting network continuity in vehicular ipv6 communications," *Intelligent Transportation Systems Magazine, IEEE*, vol. 6, no. 1, pp. 17–34, Spring 2014.

[5] O. Shagdar, M. Tsukada, M. Kakiuchi, T. Toukabri, and T. Ernst, "Experimentation towards IPv6 over IEEE 802.11p with ITS Station Architecture," in *Intelligent Vehicles Symposium (IV'12), 2012 IEEE*. Madrid, Spain: IEEE, jun. 2012, pp. 1–6.

[6] C. Pinart, P. Sanz, I. Lequerica, D. García, I. Barona, and D. Sánchez-Aparisi, "DRIVE: a reconfigurable testbed for advanced vehicular services and communications," in *Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities*, ser. TridentCom '08, 2008, pp. 16:1–16:8.

[7] M. Tsukada, J. Santa, O. Mehani, Y. Khaled, and T. Ernst, "Design and Experimental Evaluation of a Vehicular Network Based on NEMO and MANETS," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, no. 656407, pp. 1– 18, september 2010.

[8] M. Hossain, M. Atiquzzaman, and W. Ivancic, "Performance evaluation of multihomed nemo," in *Communications (ICC), 2012 IEEE International Conference on*, june 2012, pp. 5429 –5433.

[9] J.-C. Lin, C.-S. Lin, C.-N. Liang, and B.-C. Chen, "Wireless communication performance based on IEEE 802.11p R2V field trials," *IEEE Communications Magazine*, vol. 50, no. 5, pp. 184 –191, may 2012.

[10] J. Gozalvez, M. Sepulcre, and R. Bauza, "IEEE 802.11p vehicle to infrastructure communications in urban environments," *IEEE Communications Magazine*, vol. 50, no. 5, pp. 176 –183, may 2012.

[11] International Organization for Standardization, "Intelligent transport systems - Communications Access for Land Mobiles (CALM) - Architecture," ISO 21217, International Organization for Standardization, april 2013.

[12] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Communications Architecture," ETSI EN 302 665, European Telecommunications Standards Institute, September 2010.

[13] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," RFC 3963 (Proposed Standard), Jan. 2005.

[14] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, "Multiple Care-of Addresses Registration," RFC 5648 (Proposed Standard), Internet Engineering Task Force, Oct. 2009.

[15] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," RFC 4301 (Proposed Standard), Internet Engineering Task Force, Dec. 2005.