Continuous IPv6 Communications in a Vehicular Networking Stack for Current and Future ITS Services

José Santa[1], Fernando Bernal[1], Pedro J. Fernández[1], Antonio Moragón[1], Andrés S. García[1] and Antonio F. Skarmeta[1]

Abstract— **The Intelligent Transportation System (ITS) community and road transport stakeholders are nowadays seeking for practical solutions in the area of vehicular communications and telematics. It is the time to provide real implementations that can be tested and evaluated in field operational tests. The work presented in this paper follows this line and a communication stack based on the well-known IPv6 protocol is described in detail. The main aim in the design of this stack has been providing an integral management of IPv6 mobility. For this reason, the proposal is based on Network Mobility (NEMO) to support eventual point of attachment changes at IPv6 level but, additionally, an authentication/authorization mechanism is added to automate the access to secured domains, and extended capabilities to support handovers have been added. The IEEE 802.21 standard is used to enhance vertical and horizontal handovers by publishing and centralizing access information of available wireless networks. Moreover, on the top of this access and networking layer, which also provides extra security features, a set of OSGi modules are given as facilities to make easier the implementation of applications. As it is noted in the rest of the paper, the proposal presented in this paper conforms with ISO TC 204 and ETSI TC ITS specifications and proposes new extensions for improving security and handover support, integrates IETF protocols, and it is being continuously improved in frames of the EU ITSSv6 project and tested on the Spanish FOT OASIS project.**

I. INTRODUCTION

According to the vast amount of research in vehicular communications and cooperative systems that has appeared in the last years, infrastructure and vehicle subsystems will not be independent in the future. Communication networks should interconnect infrastructure processes (I2I - infrastructure to infrastructure); they should make easier the provision of services to vehicles (V2I/I2V - infrastructure to vehicle); and they should be the seed of future cooperative services among vehicles (V2V - vehicle to vehicle). As a result of the great research efforts on vehicular communications we are now immersed in the phase of developing previous theoretical or simulated advances and getting preliminary results [1]. The European Union is aware of this necessity and the Sixth and, above all, the Seventh Framework Program calls have been especially focused on field operational tests (FOT) projects. Initial founded projects, such as EuroFOT, have given way to a new set of national and international initiatives. The German simTD, the French SOCOR@F, the Spanish OASIS, or the recent European DRIVE C2X and FOTsis are some examples. Although these initiatives start from the basis of previous research projects, such as CVIS or Coopers, it has been noted that there is a gap between the preliminary developments made on those projects and the more complete communication stack necessary to perform a wide set of tests in FOTs [2]. Due to that, the European Union agreed to found a project like IPv6 ITS Station Stack for Cooperative ITS FOTs (ITSSv6), whose main aim is to conform an IPv6-based communication stack ready to be used by FOT projects.

In parallel to the progress on vehicular communications in research projects, additional efforts have been put on standardizing a communication architecture that assures the future compatibility among different providers. First, the ISO TC 204 released the Communications Access for Land Mobiles (CALM) concept, but the recently created group ETSI TC ITS has improved CALM based on the results of the COMeSafety European project. The architecture of the current European ITS communication stack [3] should be instantiated totally or partially on vehicles, nomadic devices, roadside units and central points. Two management and security planes surround four horizontal layers based on the well-known OSI communication stack in this proposal, although they have not been completely defined by standardization bodies yet. The work presented in the current paper proposes a communication stack that extends, above all, these parts, which is being tested in the OASIS project and that integrates features from the ITSSv6 European project.

According to the current deployment of communication technologies on transport systems, it is envisaged that the first cooperative ITS segment to be exploited is the V2I/I2V one. Pure V2V services will require a great penetration, and I2I communications between currently deployed traffic centers would require huge efforts. It is in the V2I/I2V segment where novel traffic efficiency, comfort services and relaxed safety applications can be first efficiently tested and deployed. This is the reason why the networking stack developed in this work is especially interested on providing a useful solution for V2I/I2V IPv6 communications, given that IP is the basis of Internet and the new version, IPv6, is a must nowadays.

The communication stack presented in this paper comprises a set of proposals that are distributed among the protocol layers of the ISO/ETSI ITS communication stack: 802.11, WiMAX and 3G/UMTS communication technologies have been integrated with a network selection system that can be parameterized according to user preferences and integrates IEEE 802.21 concepts. A key part of the work is

[1]José Santa, Fernando Bernal, Pedro J. Fernández, Antonio Moragón, Andrés S. Garca and Antonio F. Skarmeta are with Faculty of Computer Science, University of Murcia, 3100 Murcia, Spain

ISBN: 978-84-695-3472-4

providing continuous IPv6 communications and, to achieve this objective, it is necessary to reduce the handover latency and obtain seamless transitions, if possible. To achieve this goal, the use of IEEE 802.21 standard [4] enables optimizations to improve handovers between heterogeneous wireless networks and provides mechanisms to perform such changes in a secure way. Moreover, since the network access could not be a direct process when the domain is secured or the terminal must be authorized, a AAA (Authentication, Authorization and Accounting) approach based on the Extensible Authentication Protocol (EAP) is presented. In the network layer, an IPv6 network mobility solution is provided to support the changes of network attachment point, which has been enhanced with Internet Protocol Security (IPsec) to secure communications. Additionally, Next Generation Network (NGN) advances have been integrated as facilities, to make easier the operation of applications while accessing remote services, and a modular software architecture framework for managing ITS station software has been added.

The paper first presents handover basics in Section II and then details the architecture of the communication stack proposed in Section III. The overall scenario considered and the testbed deployed is presented in Section IV. Next, a separated description of the 802.21-based adds in the communication stack are described in Section V, and the various facilities for application support are presented in Section VI. Finally, several related works in Section VII are followed by the most important conclusions in Section VIII.

II. THE HANDOVER PROBLEM

Mobility is one of the main research topics in wireless networks, due to the benefits offered to end users. For the case of vehicular communications, wireless infrastructures must provide efficient mobility capabilities along the road to maintain vehicles moving at high speed connected to the network. In order to cope with this, a vehicle connected to a wireless network should be able to move freely, using different access points that are available along its path. These access points could belong to different domains and different wireless technologies, like 802.11a/b/g, 80.11p, WiMAX or 3G. As a consequence of using more than one communication technology and differentiated network domains, several types of handovers should be taken into account:

a) Intra-domain and intra-technology handover: This is the least complex type of handover from the network engineering point of view, since only the link layer is involved. The IP address does not change and neither mobility nor AAA mechanisms are needed in this case.

b) Inter-domain and intra-technology handover: A domain change usually implies an IP address reassignment. For this to happen, both the link-layer and network-layer are involved. Mobility and AAA mechanisms should be used in this case.

c) Intra-domain and inter-technology handover: In this case, a change of communication technology implies a more complex interaction, since a transition between two different communication interfaces must be provided, however, the same IP address could be maintained. AAA mechanisms at link-level could be needed.

d) Inter-domain and inter-technology handover: This is the most complex type of handover, and both mobility and AAA processes are involved, since it implies a domain/technology change.

An inter-domain and intra-technology handover is usually called as horizontal handover, whereas a vertical handover usually denotes an inter-domain and inter-technology handover. In vehicular communications, each roadside unit with an attachment point could be provided with an access router that manages a network domain with its own addressing scheme. In this way, changing the network attachment point would imply entering a new domain. Furthermore, when a handover occurs extra security mechanisms should be executed to maintain communication channels trough IPsec, for instance, as it is further discussed in a previous work [5].

III. STACK ARCHITECTURE

The designed communication stack, illustrated in Fig. 1, follows the guidelines given by ISO/ETSI communication architecture and, hence, it should be instantiated in the form of ITS station nodes in vehicles, mobile hosts, roadside units and central systems. The design showed in Fig. 1 gives such instantiation for the case of the vehicle, splitting the whole stack functionality in two nodes: vehicle host (on the left) and mobile router (on the right). For the sake of simplicity, the rest of ITS stations are not showed, but most of the functions are showed with these two instantiations.

The mobile router (stack on the right of Fig. 1) includes the needed functionalities to hide networking tasks to in-vehicle hosts. An unlimited number of hosts could connect with the ITS network by means of the access router through a common WiFi or Ethernet connection. Up to now, three external communication technologies are supported: 3G/UMTS, WiMAX and 802.11a/b/g/p. A network selection module manages these interfaces considering a set of user preferences about them. Moreover, IEEE 802.21 has been embedded in the stack in the management plane, in order to improve the handover and provide useful network information to the network selection module. The IEEE 802.21 support is provided by adding different modules to the stack: MIES (Media-Independent Event Service), which informs about different events (i.e. link up/down); MICS (Media-Independent Command Service), which allows commands to be sent between higher and lower layers or to a remote entity; and MIIS (Media-Independent Information Service), which provides information about networks in the vicinity of the mobile router location. This last component provides the network parameters needed by the network selection module to take the handover decision. Further details about these modules are given in Section V.

The EAP protocol is used in different layers: link, network and management. The management plane needs EAP because the IEEE 802.21a standard is used. This provides security and handover optimization features to IEEE 802.21. Moreover, for authentication purposes, it is assumed that the

ISBN: 978-84-695-3472-4

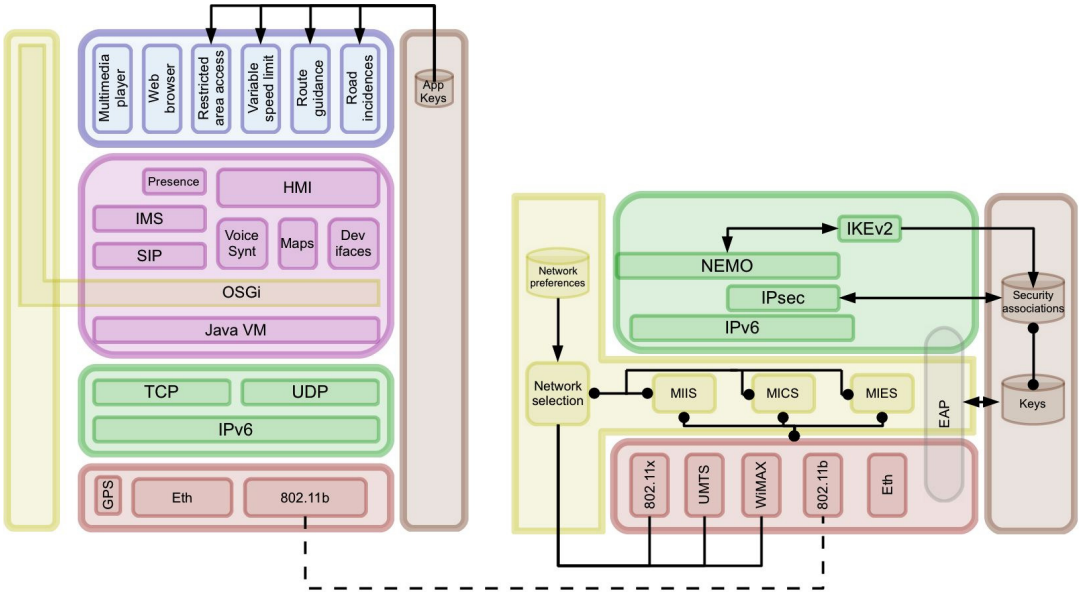


Fig. 1. Communication stack design

mobile router has valid pre-installed credentials. In general, the authentication of the in-vehicle network is performed following two steps: first, at link level, the mobile router authenticates against the access point of a roadside unit, and second, at network level, the mobile router authenticates against the roadside access router or the central ITS station, depending on the AAA capabilities delegated to each roadside unit. Upon a successful authentication, the vehicle is provided with IPv6 connectivity, and for authentication and/or handover optimization purposes, keying material is stored in the mobile router, as it is also showed in Fig. 1.

IPv6 connectivity is supported by the set of elements included within the networking and transport scope of the mobile router. The core feature of this part is the Network Mobility (NEMO) module, which is in charge of maintaining a continuous IPv6 addressing for the whole in-vehicle network. Moreover, communications are secured by means of IPsec, which takes a set of security associations previously negotiated by Internet Key Exchange version two (IKEv2) when a new network is accessed.

The stack on the left in Fig. 1 belong to the vehicle host, which is in charge of executing final applications that could access remote services. A GPS device in the lower layer enables the host to be geo-located, although this is sometimes included in the mobile router. Additionally, a common networking middleware includes Transport Control Protocol (TCP) and User Datagram Protocol (UDP). An essential part of the host protocol stack is, however, the facilities layer. As can be seen in Fig. 1, a Java virtual machine is used as the basis for the Open Service Gateway Initiative (OSGi) framework. OSGi acts as the manager of the lifecycle of middleware parts and applications, and makes easier the communication among software modules installed in the host. Above OSGi, the most relevant facilities are: the Session Initiation Protocol (SIP), which is used by the IP Multimedia Subsystem (IMS) client as an enabler for signaling communications; the IMS client, which is directly used by applications to access remote services in a normalized way; and the Presence Service, also described in IMS specifications, which could be directly used by applications that depend on the terminal status (location, temperature, vehicle in emergency state, etc.). Finally, a set of tested applications in frames of the OASIS project has been included inside the top layer, some of them require an extra authentication stage at application level.

IV. SCENARIO AND TESTBED SETUP

The set-up scenario has been summarized in Fig. 2 with one vehicle, one roadside station and the home central ITS station for the vehicle. By means of the three communication interfaces of the mobile router, the vehicle ITS station can be connected with 802.11x or WiMAX access points and the 3G/UMTS network. In the last case it is necessary to provide an IPv4 to IPv6 transition solution, since most of the 3G providers (including the used one) still offer IPv4 Internet. In this case, OpenVPN is used between the mobile router and an access router within the central ITS station. Communications through our 802.11a/b/g/p and WiMAX access points is directly performed using IPv6, since the University of Murcia (UMU) infrastructure supports this protocol natively.

Home Internal Router and the access routers in Fig. 2 execute a common communication stack with IPv6 features. Additionally, the router included in the Central ITS Station also serves as the ending point of the OpenVPN tunnel when 3G is used. The Border Router element uses an IPv4/IPv6 dual stack, since it provides Internet connectivity to the ITS network. Additionally, this border router offers network address translation from IPv6 to IPv4 (NAT64) and a domain name system for getting IPv6 addresses of external IPv4 services. In this way, it is possible to provide access to

ISBN: 978-84-695-3472-4

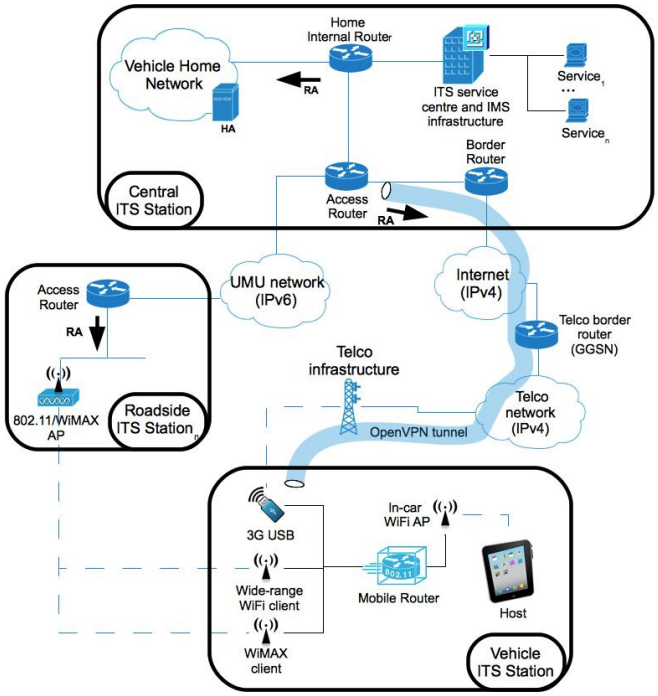


Fig. 2. Deployed scenario

IPv4 resources on the Internet. The Vehicle Home Network comprises the domain in which the vehicle maintains its home addressing. In other words, when any computer outside this domain communicates with the vehicle host, it uses the home IPv6 address and packets follow the route towards the home network (within the central ITS station), and the NEMO Home Agent (HA) will redirect these IPv6 packets to the current IPv6 address of the vehicle, which is assigned to the mobile router by each visited roadside station. The other important part of the central ITS station is the service centre, which is in fact distributed in a set of nodes that run the IMS core network. Connected with the IMS core, an application server hosts the various services offered to vehicles. The list of hardware and associated software used for each node can be found in Table I.

V. EXTENDED HANDOVER SUPPORT IN VEHICULAR COMMUNICATIONS

There are several critical points in vehicular communication performance, but one of the most important is the handover time when the mobile router perform a change in the attachment point. During that time services could suffer from a poor network performance or even communication loss. For that reason, the time spent performing a handover should be reduced to the maximum. To achieve this objective it is necessary to take into account users' preferences, as it has been considered in the communication stack presented above, and collect information about the surrounding networks. For the latter, IEEE 802.21 is used as a mechanism that provides network information to perform the right network selection in each moment.

The main purpose of IEEE 802.21 is to enable handovers between heterogeneous technologies without service interruption. Concretely, IEEE 802.21 provides a framework that allows higher levels to interact with lower layers to provide session continuity without dealing with the specifics of each technology. This is of paramount importance in communication architectures where a vast number of networks and technologies are present, such as the case of vehicular communications. To achieve this, IEEE 802.21 defines a media-independent entity that provides a generic interface between the different link layer technologies and the upper layers. To handle the particularities of each technology, 802.21 maps this generic interface to a set of media-dependent services access points (SAPs) whose aim is to collect information and control the link behavior during handovers. Moreover, 802.21 allows to get network environment information in order to perform the correct network selection.

Apart of the previous 802.21 features, a set of secondary goals make easier and more efficient handovers in our vehicular communication stack proposal:

- Handover-aware applications. Applications can participate in handover decisions. This allows the management plane to easily contribute in the network selection.
- Quality of service (QoS)-aware handovers. Provides the necessary functions to make handover decisions based on QoS criteria.
- Network discovery. 802.21 provides the mobile router with capabilities to easily receive information about new networks in the surroundings.
- Power management, which could be specially useful when the communication stack works on mobile devices (Personal ITS Station).

IEEE 802.21 architecture is based in a central entity called media-independent handover function (MIHF). The MIHF acts as an intermediate layer between the upper and lower layers, whose main function is to coordinate the exchange of information and commands between the different devices involved in making handover decisions and executing handovers. From the MIHF perspective, each node has a set of MIHF users, typically mobility management protocols and, in our case, the network selection module in the management plane of the stack, that use the MIHF functionality to control and gain handover-related information. IEEE 802.21 defines three MIHF services, the ones included as modules in Fig. 1:

- Media-Independent Event Service (MIES). This service provides the network selection logic in the stack of notification upon the detection of significant events, such as when a handover to another network is possible.
- Media-Independent Command Service (MICS). This part processes commands sent from higher layers, in our case the network selection management, to determine the status of physical links or control and configure the terminal.
- Media-Independent Information Service (MIIS). This provides a framework through which the management layer of the mobile router is able to acquire network information within a geographical area.

ISBN: 978-84-695-3472-4

TABLE I
LIST OF HARDWARE EQUIPMENT

Networked nodes			
Node	**Model**	**CPU/Mem**	**Operating System**
Vehicle Host	PC Viliv X70	Atom 1.3Ghz/1GB	Windows 7
Mobile Router	PC Asus EB150U	Atom 1.8Ghz/2GB	Ubuntu 10.4
HA and roadside AR	mini-ITX PC	Via 532Mhz/476MB	Ubuntu 10.4
Central ITS AR	PC	i5 3.1Ghz/3GB	Ubuntu 10.4
IMS core x 4	Xen virtual machine	PentiumD 2Ghz/256MB	Ubuntu 10.4
IMS Apps Server	Xen virtual machine	PentiumD 2Ghz/1GB	Ubuntu 10.4
Network interfaces			
Technology	**Hardware**		
3G/UMTS	Ovation MC950D modem		
802.11p (WAVE)	802.11p-capable Laguna LGN-00-11 client and access points		
802.11b/g (Wi-Fi)	ALFA AWUS036 client and Lobo 924TS access point		
802.16e (WiMAX)	Alvarion Breeze Max 5000 client and base stations		
Relevant software			
Node	**Description**		
Vehicle Host	OSGi Equinox framework 3.6		
MR / HA	NEMO (UMIP 0.4) and IKEv2 (OpenIKEv2 0.96)		
IMS core	Fraunhoffer Open IMS		
IMS Apps Server	Kamailio 3.1.2		

Thanks to the 802.21 support, the communication stack can perform optimized handovers due to the fact that, above all, the MIIS can provide a big amount of information about the networks in its traffic area. Concretely, the MIIS service provides network parameters about network security and load, number of points of attachment, etc. The network selection logic of the communication stack can request all the extra information needed to MIIS, in order to decide which network will be the most suitable to initiate a handover. Moreover, the mobile router could use IEEE 802.21 to prepare the handover in the target network, for example, by performing a pre-authentication with the chosen point of attachment to reduce the handover time. This comprises an ongoing research line, in which our previous work in this context [6] is being ported and adapted for the case of vehicular communications.

VI. FACILITIES FOR APPLICATION SUPPORT

Several software modules have been implemented over the network and transport layer. The most representative ones are the IMS service access layer and the OSGi middleware to host all software modules (including facilities and applications). Both provide high-level functionalities to implement final applications that, hence, validate the networking capabilities over real cases of study.

A. IMS-Based Service Access Middleware

A common framework for the provision and access the many disparate telematic services that can be available in vehicular platforms is needed. IMS is an efficient solution in the ITS frame, as it is also demonstrated in previous works [7], [8]. This work proposes a service access middleware based on the 3GPP IMS, which is located in the facilities layer of the proposed communication stack. This feature provides mechanisms for session establishment and negotiation of capabilities between client applications and services.

IMS provides a mobility solution at service level, but it is important to notice that, since network mobility is used for the in-vehicle network, the mobility support of IMS is obviated. With NEMO, each IMS Terminal Equipment (TE), included in the vehicle host as a facility, maintains a permanent IPv6 address, independently of the IMS domain in which the user is registered. How IP mobility and IMS can integrate for enhanced service mobility support is out of this work for the moment, but further details on this issue can be found in [9], [10].

The process of host registration in the IMS domain and the subscription to a service is summarized next. First, the TE, which usually comprises the in-vehicle host, needs to register in the IMS domain. This is carried out by an initial SIP exchange with the IMS core, indicating the identity of the subscriber, the authentication method, and the user credentials. In the current proposal, we have chosen the challenge-response algorithm for user authentication. Once the subscriber is registered, the host TE is able to subscribe to IMS services, by means of a new SIP transaction with the service parameters that he or she wants to use; for instance, the quality of service or the duration of the session. The IMS core entities forward this request to the corresponding SIP application server, which decides whether it is able to accept these parameters. In this way, a negotiation is maintained between the TE and the service edge. If the negotiation is successful, the service session is established and the data flow between the application, local to the in-vehicle host,

ISBN: 978-84-695-3472-4

and the remote service edge, executed in the SIP-AS, starts.

B. Host Software Management

OSGi is a framework oriented to manage software units in a gateway that offers us several advantages to provide modularity, easiness of application deployment and deal with inter-module dependencies, within the vehicle host. Each application is implemented as one or more OSGi modules, called "bundles", which are deployed together with extra meta-information on a *manifest* file, inside a compressed Java Archive (jar). In this proposal, OSGi is used as the basis for installing facilities and applications, according to the communication stack illustrated in Fig. 1.

One of the reference OSGi-based facilities already implemented is the human-machine interface (HMI), which offers an homogeneous screen access to all applications installed in the vehicle host. For this purpose, and because of the several requirements that an HMI must accomplish [11], [12], we have built a modular HMI service. This module has three fundamental aims. First, it is in charge of drawing interface objects for all installed applications, which define their aspect through an XML descriptor. Second, it provides the unique i/o channel with the user and it is in charge of distributing interface information among all applications. And third, the developed HMI provides accessibility features to host applications, such an on-screen keyboard, a speech synthesizer or mapping capabilities. Two screenshots of the HMI can be seen in Fig 3. On the left part, the root interface is divided in three main areas. First, the upper bar includes general functions, such as the name of the active application, the available communication interfaces in the mobile router (only included for testing purposes) or the status of the voice synthesizer. The second main part on the middle contains the icons of the installed applications, and the third one provides an on-screen keyboard and information about the communication interface used by the mobile router (also for demonstration purposes). On the right part of the figure, the application "Servicios integrados" is active. This application integrates in a unique map view the information that comes from three different services: route guidance, variable speed limit and incidence warning. As can be seen, the HMI capabilities enable the integration of applications in a friendly and low-distractive way.

VII. RELATED WORK

Practical proposals for vehicular communications similar to the one presented in this paper are not frequent in the literature, due to the tough design and development efforts needed. The work presented in [8], for instance, proposes 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 develop a generic communication stack to be instantiated on the different elements of an ITS network.

More related solutions can be found on recent proposals from FOT projects, since they offer the needed framework for implementing integral communication modules. Authors of [13] present the Drive C2X ITS station proposal, which is similar to the one presented in this paper, also offering an OSGi-based software platform for applications and dealing with communication issues at network level. What is noticeable in this work is that IP networking has been left out only for management and testing through UMTS-based communications. A similar work about the simTD project is presented in [1], but a special mention is given to security and privacy, and a public key infrastructure is added to the architecture. As has been explained before, it is the authors' opinion that IPv6 communications are the key to ITS cooperative systems deployment, and this paper defends a combined solution for IPv6-based network mobility and security for non-critical vehicular services. In this line it is the work presented in [14], although a constrained and non-autonomous communication stack is used for experimental evaluation of concrete routing and flow management subsystems.

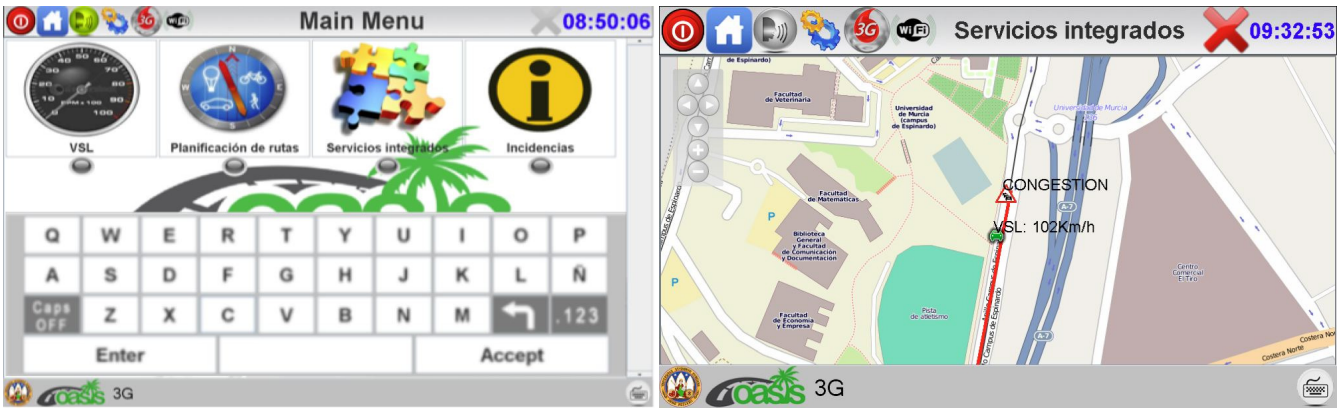
Regarding extended support for mobility, IEEE 802.21 is an emerging technology and it is being adopted by in several proposals to enhance handover in mobile terminals. For instance, in [15], a framework for integrating an adaptive lifetime-based vertical handover using IEEE 802.21 is presented, which is useful for video streaming applications. More related with the context of the current paper, in [16], 802.21 is used to improve the transition time by means of Fast Handover for Mobile IPv6 (FMIPv6) in vehicular networks. In [17] authors present an initial proposal for implementing a MIIS service in vehicular ad-hoc networks, with the aim of assisting vehicles in handovers.

VIII. CONCLUSION

This works proposes a networking stack that follows current ESO/ETSI trends towards a common ITS communication architecture, but proposing new extensions for handover and security support. The stack has been defined and developed, and it supports several communication technologies that can be automatically selected in an intelligent way thanks to the 802.21 features. This improves the handover support capabilities towards a seamless transition between attachment points. A secure IPv6 network mobility solution is proposed, first requiring the network access through authentication and then using NEMO and an IPsec/IKEv2 combination to secure control and data traffic. Moreover, as part of the stack facilities and management features, OSGi is used as a framework for middleware and applications. IMS is used as a facility for making easier the service access to on-board applications. Finally, an extensible HMI is provided to integrate application interfaces and offer a friendly interface to users.

Current lines at IPv6 level comprise an exhaustive testing of the IPv6 networking part, above all considering communications over the recently integrated 802.11p devices. Nevertheless, the communication stack has been successfully validated in frames of the final tasks of the FOT OASIS project, through a set of real applications tested on real traffic conditions. Furthermore, extended security features

ISBN: 978-84-695-3472-4



(a) Main view

(b) Service operating in the map view

Fig. 3. Screenshots of the developed HMI

to solve the privacy issues briefly presented in [18] are being carried out in frames of the ITSSv6 European project. Regarding facilities, speech recognition is being provided to the HMI and new IMS services are almost finished, such as a novel radio-equivalent system based on 3GPP Push-to-Talk functionality.

ACKNOWLEDGEMENT

This work has been sponsored by the European Seventh Framework Program, through the ITSSv6 Project (contract 270519); the Ministry of Science and Innovation, through the OASIS (CENIT-2008 1016) and Walkie-Talkie (TIN2011-27543-C03) projects; and the Seneca Foundation, by means of the GERM program (04552/GERM/06).

REFERENCES

[1] 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, <ce:title>Deploying vehicle-2-x communication</ce:title>. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128611001198

[2] A. Festag, L. Le, and M. Goleva, "Field operational tests for cooperative systems: a tussle between research, standardization and deployment," in *Proceedings of the Eighth ACM international workshop on Vehicular inter-networking*, ser. VANET '11. New York, NY, USA: ACM, 2011, pp. 73–78. [Online]. Available: http://doi.acm.org/10.1145/2030698.2030710

[3] T. Kosch, I. Kulp, M. Bechler, M. Strassberger, B. Weyl, and R. Lasowski, "Communication architecture for cooperative systems in europe," *IEEE Commun. Mag.*, vol. 47, no. 5, pp. 116 –125, may 2009.

[4] M. I. H. W. Group, "Ieee 802.21." [Online]. Available: http://ieee802.org/21/

[5] P. Fernandez, F. Bernal, C. Nieto, and A. F. Gomez-Skarmeta, "Mobility and security in a real vanet deployed in a heterogeneous networks," *Security and Communication Networks*, vol. In Press, 2012.

[6] F. Bernal-Hidalgo, R. Marin-Lopez, and A. F. Gomez-Skarmeta, "Key distribution mechanisms for ieee 802.21-assisted wireless heterogeneous networks," in *Mobile Networks and Management*, K. Pentikousis, R. Agüero, M. García-Arranz, and S. Papavassiliou, Eds. Springer, 2011, pp. 123–134.

[7] L. Foschini, T. Taleb, A. Corradi, and D. Bottazzi, "M2m-based metropolitan platform for ims-enabled road traffic management in iot," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 50 –57, november 2011.

[8] 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. [Online]. Available: http://dl.acm.org/citation.cfm?id=1390576.1390595

[9] L. Le and G. Li, "Cross-layer mobility management based on mobile ip and sip in ims," in *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*, sept. 2007, pp. 803 –806.

[10] D. S. Nursimloo, G. K. Kalebaila, and H. A. Chan, "A two-layered mobility architecture using fast mobile ipv6 and session initiation protocol," *EURASIP J. Wirel. Commun. Netw.*, vol. 2008, pp. 24:1–24:8, January 2008. [Online]. Available: http://dx.doi.org/10.1155/2008/348594

[11] A. Amditis, L. Andreone, K. Pagle, G. Markkula, E. Deregibus, M. Rue, F. Bellotti, A. Engelsberg, R. Brouwer, B. Peters, and A. De Gloria, "Towards the automotive hmi of the future: Overview of the aide-integrated project results," *IEEE Trans. Intell. Transp. Syst.*, vol. 11, no. 3, pp. 567 –578, sept. 2010.

[12] T. Giuli, D. Watson, and K. Prasad, "The last inch at 70 miles per hour," *IEEE Pervasive Comput.*, vol. 5, no. 4, pp. 20 –27, oct.-dec. 2006.

[13] 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.

[14] 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.

[15] L. Chen, A. Zahran, and C. Sreenan, "Ieee 802.21-enabled alive-ho for media streaming in heterogeneous wireless networks," in *Local and Metropolitan Area Networks (LANMAN), 2010 17th IEEE Workshop on*, may 2010, pp. 1 –6.

[16] Q. Mussabbir, W. Yao, Z. Niu, and X. Fu, "Optimized fmipv6 using ieee 802.21 mih services in vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 56, no. 6, pp. 3397 –3407, nov. 2007.

[17] L. A. Flétscher and A. F. Gómez-Skarmeta, "Proposal for implementation of 802.21 information services (miis) as handover support in vanet networks," *Revista Científica Ingeniería y Desarrollo*, vol. 28, no. 28, 2011. [Online]. Available: http://rcientificas.uninorte.edu.co/index.php/ingenieria/article/view/1447/1043

[18] J.-H. Lee and T. Ernst, "Security issues of ipv6 communications in cooperative intelligent transportation systems (poster)," in *Vehicular Networking Conference (VNC), 2011 IEEE*, nov. 2011, pp. 284 –290.