19th ITS World Congress
Vienna, Austria
22 to 26 October 2012
smarter on the way

Architecture and development of a networking stack for secure and continuous service access in vehicular environments

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

1.Computer Science Faculty, Regional Campus of International Excellence "Campus Mare Nostrum", University of Murcia, Spain. +34 868 88 8771. josesanta@um.es

Abstract

After a cycle of research efforts focused on pure and applied research on vehicular communications, recent ITS work in cooperative systems is now oriented to the next step: field operational tests (FOT). Thus the current paper proposes a communication stack for vehicular services that includes essential middleware features to be integrated on the future first generation of networked cars. A set of commercially available communication technologies is used to provide a continuous and secure IPv6 connectivity to an in-vehicle network through Network Mobility (NEMO), Internet Protocol Security (IPsec) and Extensible Authentication Protocol (EAP). On the top of this enhanced IPv6 basis, the IP Multimedia Subsystem (IMS) is used as an overlay network for vehicular services. Additionally, acting as a software lifecycle manager, an Open Service Gateway Initiative (OSGi) framework hosts an extensible human-machine interface and facilitates the installation of applications. The proposal presented in this paper conforms with ISO TC 204 and ETSI TC ITS specifications, integrates IETF protocols, and it is being continuously improved in frames of the EU ITSSv6 project and tested on the Spanish FOT OASIS project.

Keywords: communication stack, cooperative vehicles, vehicular services, IPv6, secure communications, IMS, OSGi, intelligent transportation systems.

Introduction

It was several years ago when the importance of vehicular communications rapidly grew. The research community on Intelligent Transportation Systems (ITS) had been working for years on autonomous systems focused on either the infrastructure or the vehicle side. This fact is still evident in current systems for traffic monitoring, safety or entertainment integrated in commercial vehicles. Nonetheless, this market inertia is planned to gradually change in the short term, due to the vast amount of research in vehicular communications and cooperative systems that has appeared in the last years. According to new schemes, infrastructure and vehicle subsystems will not be independent anymore. 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 [15]. 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 [5]. 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 standardising 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 that based on the results of the COMeSafety European project. The architecture of the current European ITS communication stack [9], summarised in Figure 1, should be instantiated totally or partially on vehicles, nomadic devices, roadside units and central points. As can be seen, the Management and Security planes surround four horizontal layers based on the well-known OSI communication stack. The work presented in the current paper proposes a communication stack that follows this approach, which is being tested on 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 among currently deployed traffic centres 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 algorithm that can be parameterised according to preferences; an IPv6 network mobility solution is provided to support the change of network attachment point when the communication stack is running on a vehicle; Secure IPv6 communications and network access control; Next Generation Network (NGN) advances have been integrated as facilities, to make easier the operation of applications while accessing to remote services; and, finally, it is proposed a modular software architecture framework for managing ITS station software, which also integrates an extensible human-machine interface (HMI).

The paper first presents the architecture of the communication stack and the overall testbed and then details each layer of the stack. Finally, several related works are followed by most important remarks in the conclusions.

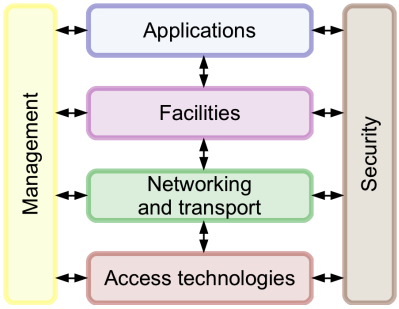

Figure 1. ISO/ETSI ITS communication stack

Stack architecture

The designed communication stack follows the guidelines given by ISO/ETSI, as can be seen in Figure 2. According to the ISO/ETSI ITS communication architecture, the basic stack provided in Figure 1 should be instantiated in the form of ITS station nodes in vehicles, nomadic devices (mobile hosts), roadside units and central systems. The design showed in Figure 2 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 according to the scenario later described, only the border router feature should be added to the stack on the right, to enable the central ITS station accessing Internet.

The mobile router (stack on the right of Figure 2) 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 following a set of preferences that dictate when to perform a handoff. The Extensible Authentication Protocol (EAP) works on both the access and networking layers, since it is used to authenticate the

vehicle in a new visited network in two phases: first, against the access point of a roadside unit, at link level and, second, against the central ITS station, at networking level. In this final stage, the vehicle is provided with IPv6 connectivity and, for authentication purposes, a set of cryptographic material is necessary, as it is also showed in Figure 2.

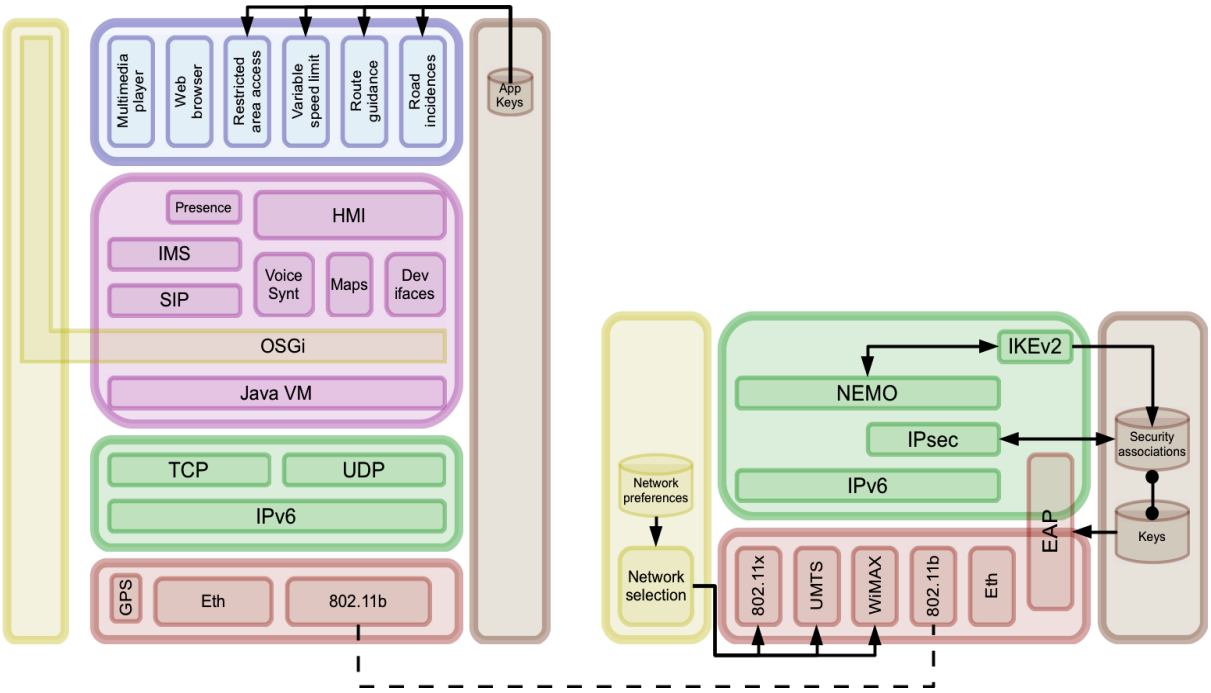

Figure 2. Communication stack design

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 Internet Protocol Security (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 Figure 2 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 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 the facilities layer. As can be seen in Figure 2, 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) is used by the IP Multimedia Subsystem (IMS) client as an enabler for signalling communications; the IMS client is directly used by applications to access remote services in a normalized way; and the Presence Service, also described in IMS specifications, 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, and some of them require an extra authentication stage at application level.

Scenario and testbed setup

The set-up scenario has been summarised in Figure 3 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, a 6over4 tunnel has been created between the mobile router and an access router within the central ITS station. On the contrary, 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 Figure 3 execute a common communication stack with IPv6 features. Additionally, the one included in the Central ITS Station also serves as the ending point of the 6over4 tunnel when 3G is used. The Border Router element uses both 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 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 1.

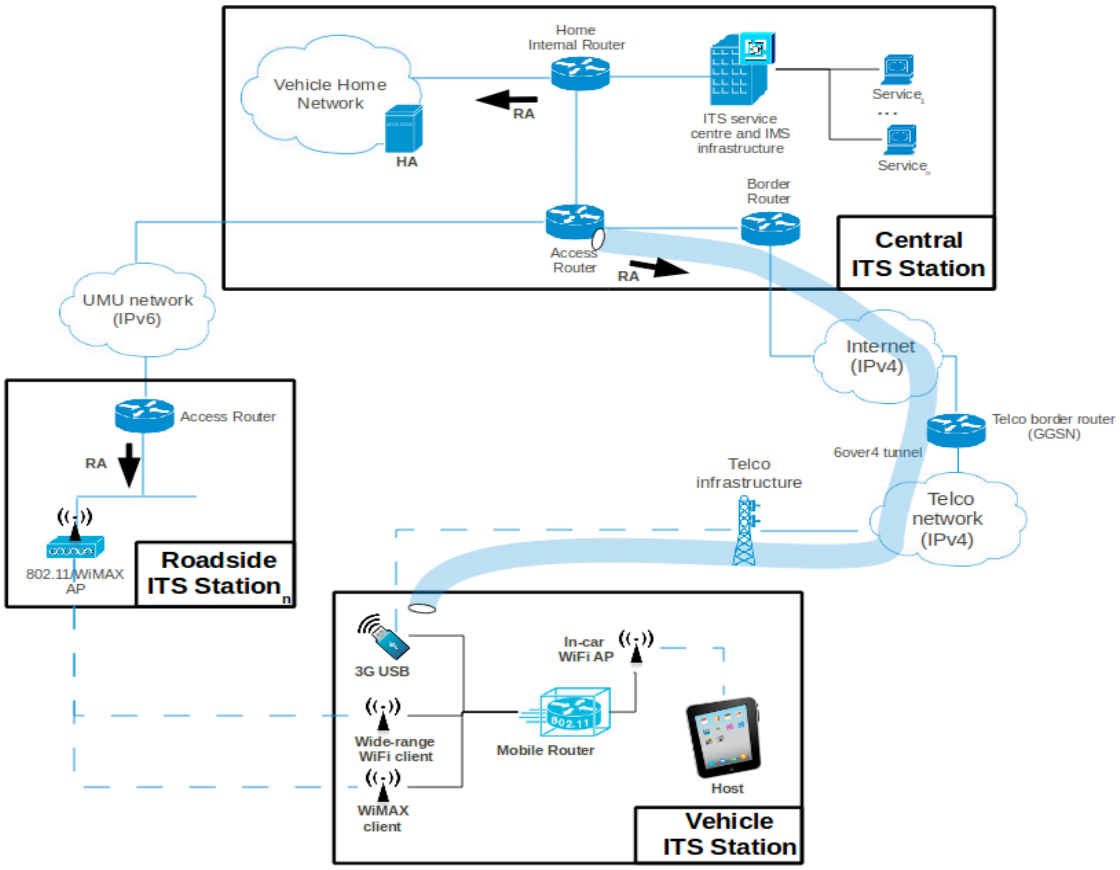

Figure 3. Deployed scenario

Table 1. 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 transceiver		
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		

Secure network mobility provisioning

Previous researches treat the security and privacy of wireless communications in vehicular environments, identifying security threats [8] and even proposing solutions based on well-known approaches, such as public key infrastructure [12]. Nevertheless, mobility issues and its optimization have been treated separately [2], but an integrated approach for both mobility and security in vehicular environments has not been tackled yet.

The problem of network mobility and security arises when both services are required at the same time, since their integration presents several interoperability issues. An interoperation approach has been identified in the IETF RFC4877 document [3], which explains how to protect the mobility traffic between the home agent and the mobile router by using IPsec and IKEv2. However, to cope with this design, software daemons that implement both NEMO and IKEv2 need to cooperate and how to do this is not well defined yet. In addition, in order to comply with the current RFC 4877 standard, some modifications have to be made in both daemons. The IPsec security associations to protect mobility traffic should be established using the address assigned within the home domain. This lets these associations survive upon a possible change of the locally assigned care-of address (CoA). However, current IKEv2 security associations, built to protect IPsec association establishments, use CoAs as end-point, so IKEv2 needs to update this CoA in its security policies every time a handover occurs. Two possible solutions have been identified to perform this CoA update [4]:

- The mobility daemon makes the changes by itself. In this case no IKEv2 daemon modification is needed. Furthermore, the IKEv2 daemon does not need to be notified because the security associations will be established in the presence of new traffic matching the new policies. Complete security associations must be performed in this case.
- The mobility daemon requests these changes to the IKEv2 daemon. In this case IKEv2 daemon could use IKEv2 Mobility and Multihoming (MOBIKE) protocol to update the policies taking into account the new CoA, and thus avoiding a renegotiation of the established security association from scratch.

Any of the previous solutions could be valid, but in both of them it is also needed an interface between these daemons in order to notify IKEv2 about the CoA to be used in security negotiations. Concretely, in our case, the first solution has been implemented for the moment, and the second one, which proposes to leave security association tasks to IKEv2, is on the way, since University of Murcia is the developer of an open IKEv2 implementation.

IMS-based service access middleware

Nowadays, many disparate services coexist in the field of ITS, from a simple video call to an advanced service for traffic monitoring. Therefore, a common framework for the provision

and access to these services is needed. IMS appears to be an efficient solution in this frame and a couple of previous works demonstrate its potential on the ITS field [6,11]. 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 vehicle hosts, will have a permanent IPv6 address, independently of the IMS domain in which the user is registered.

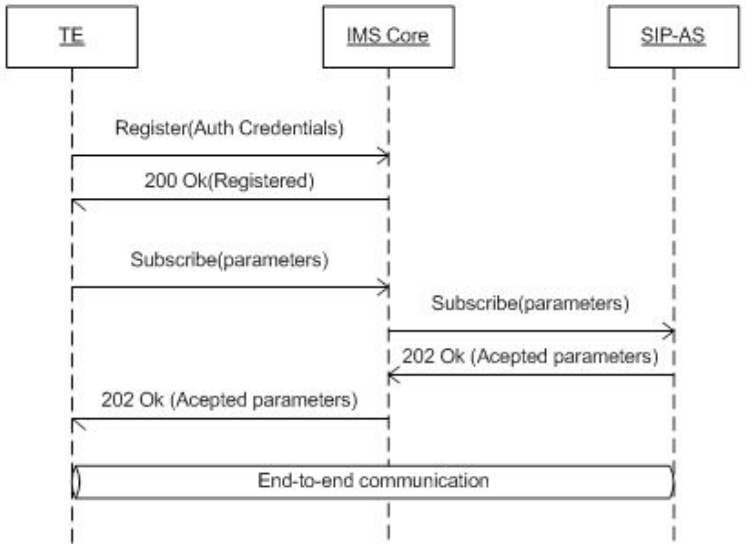

Figure 4. IMS negotiation process for service connection

The process of host registration in the IMS domain and the subscription to a service is depicted in Figure 4. 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 he wants to use, for instance, the quality of service (QoS) or the duration of the session. The IMS core entities forward this request to the corresponding SIP application server (SIP-AS), 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 TE and the service edge executed in the SIP-AS starts.

Host software management

OSGi is a framework oriented to manage software units in a gateway, which give us several advantages to provide modularity, deploy new applications and deal with inter-module dependencies. 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). Among other data, this meta-information lists the exported packages (visible packages by other bundles) and the imported ones (packages needed for the current bundle). With this information the framework manages the dependencies automatically. Thanks to this, it is possible to build a module hierarchy, from the most basic middleware to user applications. The vehicle host integrates software modules to use different devices, e.g. a GPS receiver or a video camera, which feed other software bundles.

Another important resource to deal with is the screen and how applications can gain access to it in a homogeneous manner. For this purpose and because of the several requirements that an HMI must accomplish [1,7], we have built a modular HMI service. This OSGi service shows a main interface in which are integrated all applications installed in the vehicle host. This service has three fundamental aims. First, it is in charge of drawing interface objects for all installed applications. Each application must define an XML description of its interface, which is provided to the HMI service as an argument to paint the graphical elements (buttons, labels, etc.). Second, the HMI module provides the unique input/output channel with the user and it is in charge of distributing interface information among all applications. Finally, the developed HMI provides accessibility features to host applications, such an on-screen keyboard, a speech synthesizer or mapping capabilities. The map OSGi service integrated in the platform is powered by *openstreetmap.org*, whereas the speech synthesizer is the based on the Java Speech API and it is used to give spoken alerts from applications, such as incoming incidences or asynchronous events, in order to avoid distractions.

Two screenshots of the HMI can be seen in Figure 5. 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 informative purposes) or the status of the voice synthesiser. 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 (only for demo 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 of the OASIS project: 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.

Figure 5. Screenshots of the developed HMI

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 [11], 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 for UMTS-based communications for management and testing. A similar work about the simTD project is presented in [15], 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.

Conclusions

This works proposes a networking stack that follows current ESO/ETSI trends towards a common ITS communication architecture. The stack has been defined and developed, and it supports several communication technologies that can be automatically selected to provide connectivity to the vehicle. 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, and the IKEv2 extension to support a dynamical care-of-address. All these tasks, together with extended security features to solve the privacy issues briefly presented in [10], 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. Amditis, A., L. Andreone, K. Pagle, G. Markkula, E. Deregibus, M. Romera, F. Bellotti, A. Engelsberg, R. Brouwer, B. Peters, A. De Gloria (2010). Towards the Automotive HMI of the Future: Overview of the AIDE-Integrated Project Results, *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 3, pp. 567-578.

2. Céspedes, S., X. Shen, C. Lazo (2011). IP Mobility Management for Vehicular Communication Networks: Challenges and Solutions, *IEEE Communications Magazine*, vol. 49, no. 5, pp. 187-194.

3. Devarapalli, V., F. Dupont, 'Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture' , *IETF RFC 4877*.

4. Fernandez, P. F., F. Bernal, C. Nieto, A. F. Gomez-Skarmeta, "Mobility and security in a real VANET deployed in a heterogeneous networks", *Security and Communication Networks*.

5. Festag. A., L. Le, M. Goleva (2011). Field Operational Tests for Cooperative Systems: A Tussle Between Research, Standardization and Deployment. In Proceedings *Eighth ACM international workshop on Vehicular inter-networking*, Las Vegas.

6. Foschini, L., T. Taleb, A. Corradi, D. Bottazzi (2011). M2M-Based Metropolitan Platform for IMS-Based Road Traffic Management in IoT, *IEEE Communications Magazine*, vol. 49, no. 11, pp. 50-57.

7. Giuli, T., D. Watson, K. Venkatesh (2006). The Last Inch at 70 Miles Per Hour, *IEEE Pervasive Computing*, vol. 5, no. 4, pp. 20-27.

8. Hubaux, J., S. Capkun, J. Luo (2004). The Security and Privacy of Smart Vehicles, *IEEE Security and Privacy*, vol. 2, no. 3, pp. 49-55.

9. Kosch, T., I. Kulp, m. Bechler, M. Strassberger, B. Weyl, R. Lasowski (2009). Communication Architecture for Cooperative Systems in Europe, *IEEE Communications Magazine*, vol. 47, no. 5, pp. 116-125.

10. Lee, J., T. Ernst (2011). Security Issues of IPv6 Communications in Cooperative Intelligent Transportation Systems. In Proceedings *2011 IEEE Vehicular Networking Conference*, Amsterdam.

11. Pinart, C., I. Lequerica, I. Barona, P. Sanz, D. García, D. Sánchez-Aparisi (2008). DRIVE: a reconfigurable testbed for advanced vehicular services and communications. In Proceedings *4th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities*, Innsbruck.

12. Raya, M., P. Papadimitratos, J. Hubaux (2006). Securing Vehicular Communications, *IEEE Wireless Communications*, vol. 13, no. 5, pp. 8-15.

13. Stahlmann, R., A. Festag, A. Tomatis, I. Radusch, F. Fischer (2011). Starting European Field Tests for Car-2-X Communication: The Drive C2X Framework. In Proceedings *18th ITS World Congress and Exhibition 2011*, Orlando.

14. Tsukada, M., J. Santa, O. Mehani, Y. Khaled, T. Ernst (2010). Design and Experimental Evaluation of a Vehicular Network Based on NEMO and MANET, *EURASIP Journal on Advances in Signal Processing*, vol. 2010, article ID 656407, pp. 1-18.

15. Weib, C. (2011). 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.