Securing Vehicular IPv6 Communications

Pedro J. Fernández, José Santa, Fernando Bernal, and Antonio F. Skarmeta, *Member, IEEE*

Abstract—A common practice is applying security after a network has been designed or developed. We have the opportunity of not committing this error in vehicular networks. Apart from particular works in the literature, ETSI TC ITS has defined general security services for (vehicular) cooperative systems. However, existent efforts do not pay the needed attention to the integration of IPv6 yet. The potential of IPv6 in the field is being described within ISO TC 204, above all, but further work is needed for a proper integration of security. This work follows this direction, and a reference vehicular communication architecture considering ETSI/ISO regulations, uses Internet Protocol security (IPsec) and Internet Key Exchange version 2 (IKEv2) to secure IPv6 Network Mobility (NEMO). A key advance is also the implementation and experimental evaluation of the proposal in a challenging vertical handover scenario between 3G and 802.11p. The performance of the secured NEMO channel is widely analyzed in terms of the movement speed, bandwidth, traffic type or signal quality, and it is concluded that the addition of IPv6 security only implies a slight reduction in the overall performance, with the great advantage of providing confidentiality, integrity and authenticity to the communication path.

Index Terms—Security, vehicular networks, IPv6, IPsec, communication stack, testbed, ITS

1 Introduction

The importance of vehicular networks within the Intelligent Transportation System (ITS) research field is evident if one considers the envisaged future cooperative cars and some of the current vehicular services, such as fleet management, road pricing or e-call, which already use computer communications to operate. However, each service usually provides its own communication architecture, different protocols (probably non standardized), specific hardware, and thus communication links cannot be shared. These issues lead to flexibility lacks in the hardware installed in the vehicle and extra costs to the final user. With the aim of solving this problem, ISO and ETSI have been working during the last years in a common communication architecture for (vehicular) cooperative systems. The resulting standards [1], [2] provide a common framework to implement interoperable vehicular networks. IEEE 1609 WG has also worked in parallel to achieve a similar aim, obtaining the wireless access for vehicular environment (WAVE) architecture, although its vision is narrower, proposing standards more focused on a particular communication stack including IEEE technologies. International projects like FOTsis,[1] Drive C2X[2] or ITSSv6[3] are already exploiting the ISO/ETSI architecture potential in real use cases and using particular protocols described by these standards.

1. http://www.fotsis.com
2. http://www.drive-c2x.eu
3. http://www.itssv6.eu/

- *P. J. Fernández, F. Bernal, and A. F. Skarmeta are with the Department of Information and Communications Engineering, University of Murcia (UMU), Murcia, Spain. E-mail: {pedroj, fbernal, skarmeta}@um.es.*
- *J. Santa is with the Department of Engineering and Applied Technologies, University Centre of Defence at the Spanish Air Force Academy, Spain, and the UMU Group. E-mail: jose.santa@cud.upct.es.*

Manuscript received 30 June 2014; revised 17 Oct. 2014; accepted 30 Dec. 2014. Date of publication 2 Feb. 2015; date of current version 20 Jan. 2016.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TDSC.2015.2399300

In the security plane, apart from particular research contributions (later analyzed in the paper), the standardized ISO/ETSI reference communication architecture provides a transversal layer with security services at different levels of the stack. This sets the bases for the design and integration of security protocols, key management, cyphering schemes, firewalling capabilities, etc. to appear in the next years. According to ETSI TC ITS [3], the security needs that should be considered in vehicular cooperative systems are confidentiality, integrity, authenticity, availability and non-repudiation. ETSI TC ITS has also identified the security services to cope with the previous security needs [4] and a high-level security framework has been envisaged [5], dealing, above all, with the first three security needs previously described. However, this approach is still too focused on message-level security for cooperative awareness message (CAM) and decentralized environmental notification message (DENM), which are defined as facilities to operate over a transport protocol.

The security models proposed by IEEE WAVE and ETSI TC ITS do not consider (up to now) session based security associations, and messages are usually routed using ITS-specific network protocols and then individually protected using a public key infrastructure (PKI). This provides a security scheme valid for broadcast scenarios and cases with low volumes of traffic, considering both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Although many services in vehicular networks can be served by this security approach, a number of traffic efficiency, infotainment and even notification-based safety services could use IPv6 unicast or multicast traffic that can be more efficiently transmitted using end-to-end security associations powered by symmetric cryptography. IPv6 is being more and more considered in the ITS research and standardization forums as a perfect media-agnostic carrier of new vehicular services, offering a large addressing space for ambitious deployment scenarios, easier support due to the well-known Internet standards, or an integral network-level solution for upper layers.

The focus of this work lies on the special case of vehicle to infrastructure communications, although the network model described allows an indirect communication path between vehicles. The work presented relies on IPv6 technologies such as internet key exchange version 2 (IKEv2) and internet protocol security (IPsec) to provide secure communication channels between a mobile router (MR), which provides connectivity to users and on-board devices, and the mobility server located in a wired remote point at the infrastructure side. The model presented in this paper is based on providing IPv6 continuity to the in-vehicles nodes through the usage of network mobility basic support (NEMO). All the traffic tunneled by NEMO is encapsulated by IPsec using the parameters given by a security association, which is composed by the keys to be used, IPv6 security headers to use, cyphering algorithms, etc. These security associations are created beforehand by IKEv2, which enables the mobile router and the mobility/security servers to negotiate the parameters of the secure channel.

The rest of the paper is organized as follows. Section 2 reviews in more detail particular works in the literature about security and experimentation in vehicular networks. Section 3 overviews the IPv6-based communication architecture in which the security solution has been implemented and tested, while Section 4 details the security subsystem and the new contributions to the design issues found in standards. Later, in Section 5, a real testbed that develops this architecture is presented and used to perform a wide testing campaign. In this part, the gathered results are presented and analyzed. Finally, Section 6 concludes the paper summarizing the main contributions and addressing future lines of work.

2 State of the Art

Previous investigations have addressed the provision of security and privacy of wireless communications in vehicular environments, identifying security threats [6], [7] and even proposing solutions based on well-known approaches, such as public key infrastructure [8], [9]. There are also works dealing with mobility management and its optimization in vehicular networks [10]. Nevertheless, to the best of our knowledge, the problem of achieving a secure mobility management taking into account the particularities of vehicular environments has not been tackled yet.

Authors of [11] 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 UMTS-based communications for management and testing. A similar work about the simTD project is presented in [12], 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 will play a key role in realistic ITS cooperative systems deployments, and this paper defends a combined solution for IPv6-based network mobility and security for non-critical vehicular services.

IPsec is used in a vehicular environment in the CVIS project [13], where Kerberos is used for establishing these IPsec security associations (IPsec SA) as well as for authentication purposes. However, this solution lacks of the flexibility provided by IKEv2 to negotiate the required security parameters, especially when using NEMO.

Another noticeable contribution of the present work relies on the development of an experimental validation of the secure IPv6 communication stack over a real vehicular network and using a handoff scenario between 3G and IEEE 802.11p technology (ETSI G5), which is especially adapted to the conditions that arise in vehicular communications. To the best of our knowledge, there exist a few works dealing with this issue at network level, and some of them are within our research line [14], [15]. However, these prior evaluations were minor IPv6 network mobility tests and security was not considered. Some works have recently appeared evaluating particularly the behavior of 802.11p at link level. The evaluations performed in [16] reveal that the packet delivery ratio (PDR) achieved by this technology is highly dependent on the distance between sender and receiver. These results are confirmed in [17], where it is also concluded that the vehicle speed does not imply a noticeable performance degradation in the communication. A similar evaluation is performed in [18], but this time carrying out a great testing campaign in a city. The most interesting analysis is the one attending to the impact of an environment with obstacles for the transmission of 802.11p signals. In the current work, these issues have also been demonstrated to play a key role in the expected performance of the considered secure and mobile IPv6 network.

3 Base Communication Architecture

The base communication architecture used in this paper for integrating IPv6 security features was initially presented in [15]. Fig. 1 shows a simplified view of this platform, which follows the ISO/ETSI reference architecture specifications [1], [2]. The IPv6 mobility and security modules are now especially remarked. In the diagram one can distinguish three main entities: Vehicle ITS Station (Vehicle ITS-S), integrating the on-board networked nodes; Roadside ITS Station (Roadside ITS-S), which provides local wireless connectivity and data processing; and Central ITS-S (Central ITS-S), which includes the necessary nodes for providing backend services. The communication stacks depicted for each node follow the ISO/ETSI layered scheme that considers, from bottom to top, the following layers: access technologies, networking and transport, facilities and applications. These layers are surrounded by two additional planes in charge of management and security tasks.

In the vehicle the stack functionality is split into two nodes: vehicle ITS-S host and vehicle ITS-S router (also known as Mobile Router). The MR includes the needed functionalities to hide networking tasks to in-vehicle hosts. An unlimited number of hosts could connect to the ITS network by means of the MR through a common wireless (e.g., IEEE 802.11a/b/g) or Ethernet connection. 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). A GPS device in the lower layer enables the vehicle to be geo-located. IPv6 connectivity is supported by

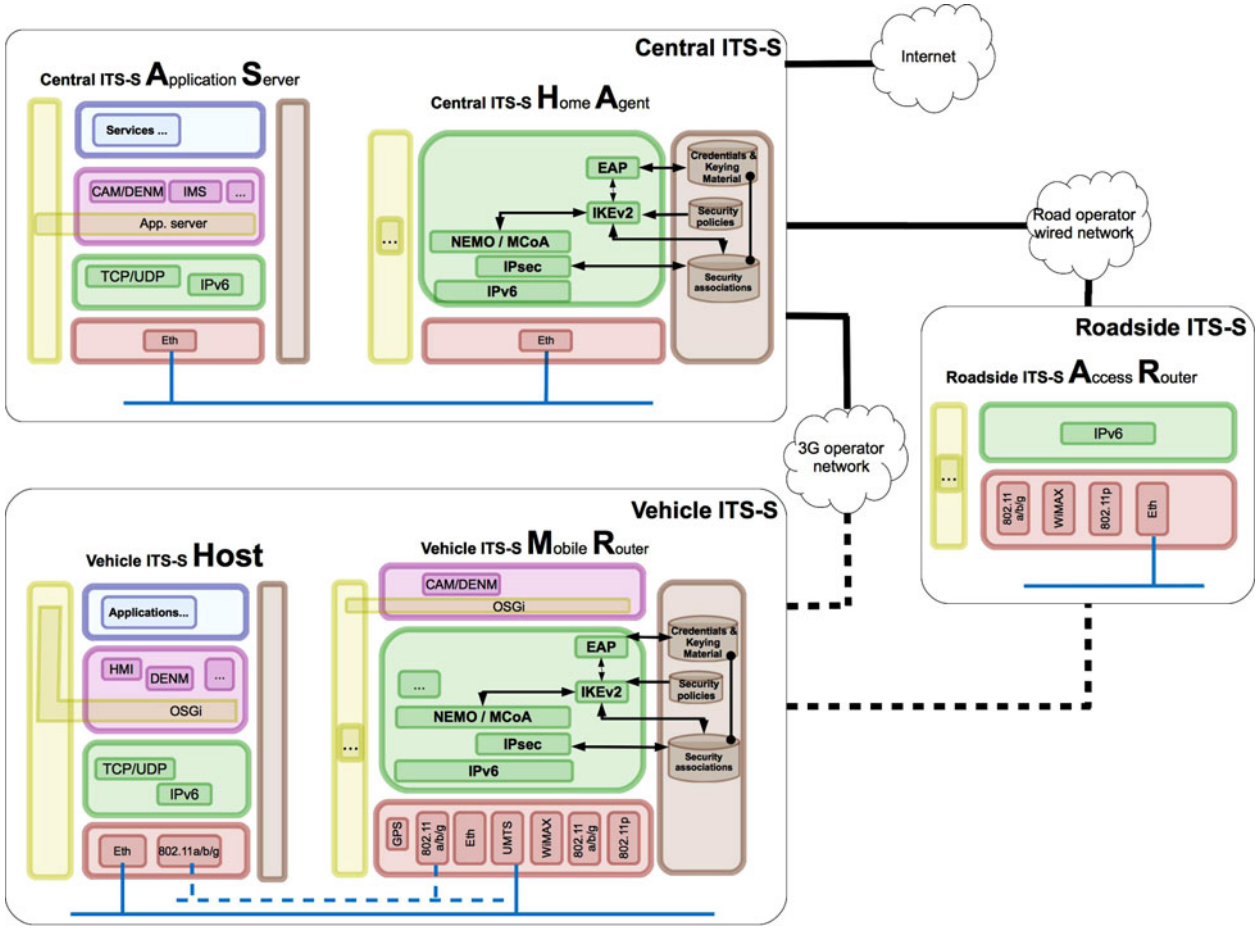


Fig. 1. Overall architecture of the reference vehicular network.

the set of elements included within the networking and transport layer of the MR. On one hand, Network Mobility (NEMO) [19] is in charge of maintaining reachability for the whole in-vehicle 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) [20]. Regarding security, the mobile router is equipped with the needed elements to secure mobility-related traffic by means of Internet Protocol Security [21], although this part is extended in the next section.

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 and DENM messaging modules (apart from other functionalities) to make easier the implementation of applications.

The communication stack instantiated in the roadside ITS-S access router (AR) 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 Wi-Fi (802.11 a/b/g), 802.11p (ETSI G5-compliant) and WiMAX.

Finally, in the upper part of Fig. 1 we can see the communication 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.

It can be noted that the main target of the research in this paper is addressing (secure) vehicle to infrastructure communications using an IPv6-compliant solution. In this line, NEMO is an IP technology inherently designed for supporting the mobility of nodes using a centralized entity located at the infrastructure side, as it is later detailed. Nevertheless, as one can figure out, an indirect vehicle-to-vehicle communication is completely feasible, given that all communication nodes are globally reachable through IPv6. This way, although safety services requiring strident communication delays between nearby vehicles are not the target of this work, both V2V and V2I applications can use the underlaying network detailed in the next sections.

4 IPv6 Security Subsystem

4.1 NEMO and MCoA Integration

In this study we have used the base communication stack developed in the ITSSv6 project for implementing the network architecture introduced above. This stack uses the

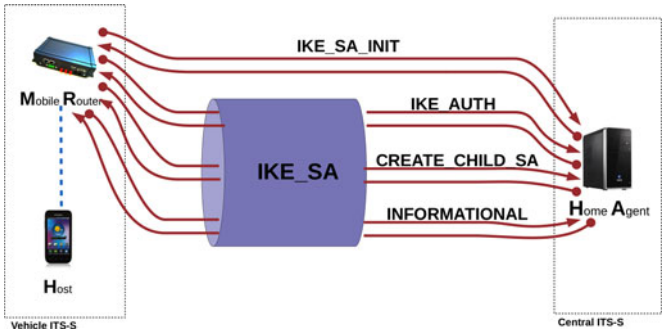


Fig. 2. IKEv2 exchanges.

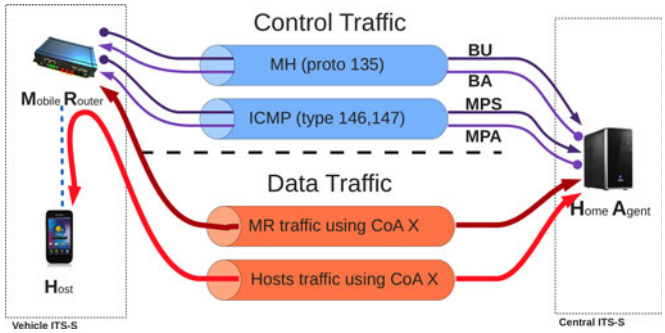


Fig. 3. IPsec tunnels established between MR and HA to provide security to mobility traffic.

NEMO protocol to provide mobility with MCoA capabilities, which allows a MR to be connected through several networks at the same time. A mobility software acting as daemon is necessary in both the MR and HA, which is in our case an adapted ITSSv6 UMIP version of NEMO. The MR always has a long-term IP address called Home Address (HoA), the one that it uses when it is connected to the home network. When the MR enters in a different network domain, a new IP address is generated, called Care-of Address (CoA). This CoA is only used to reach the HA. The MR forwards all the traffic from the in-vehicle devices to the HA, and the HA performs the same action in the apposite direction. Hence, the HA needs to correlate each HoA with one or more CoAs, given the MCoA capability. For this reason, the MR has to notify the HA about this new CoA. These notifications are performed using the Binding Update (BU) and Binding Acknowledgment (BA) messages, and maintain a binding cache up-to-date in the HA. Since no optimization is applied in this NEMO deployment, all the mobility traffic (data and control) passes through the MR and the HA. This fact is important for our security approach, as it is discussed later.

4.2 IPsec and IKEv2 Operation

In order to understand the following sections, first it is important to introduce IPsec and IKEv2. IPsec is a protocol designed to protect IP traffic between two endpoints. It uses two types of headers: IP Authentication Header (AH) and IP Encapsulating Security Payload (ESP). The support of these extension headers in IPv6 are mandatory for all network nodes. The traffic to be protected is defined using policies, stored in a database called Security Policy Database (SPD), which are normally defined by the network administrator. When one of these policies is matched, IPsec tries to find an IPsec Security Association stored in another database called Security Association Database (SAD). This IPsec SAs can be configured ad-hoc by the network administrator, but this method lacks of flexibility.

IKEv2 is the protocol implemented as a service used by IPsec to automate the creation of IPsec SAs. In order to achieve this, a set of message exchanges are used as showed in Fig. 2. It is implemented by a daemon that must be present in both endpoints, i.e., MR and HA. The considered IKEv2 distribution is OpenIKEv2, an open source implementation developed by the University of Murcia (UMU) that is also included in the ITSSv6 network stack. Every time IPsec requests the IKEv2 daemon for a new SA, in order to protect the required IKEv2 negotiation, a dedicated security association for IKEv2 messages has to be established before. This association is called "IKE Security Association" (IKE_SA), which is established in the first and non protected exchange called "IKE SA Initiation" (IKE_SA_INIT), as showed in Fig. 2. This IKE_SA is similar to a regular IPsec Security Association, using the same kind of cryptography methods, but it is only maintained by IKEv2 daemons and it is exclusively used to protect the rest of IKEv2 exchanges: the IKE Authentication (IKE_AUTH) exchange, the IKE Create Child SA exchange (CREATE_CHILD_SA) and the IKE Informational (INFORMATIONAL) exchange. The IKE_AUTH also creates the first IPsec SA. If the IKE_SA or any IPsec SA has to be refreshed, or a new IPsec SA is requested, then the CREATE_CHILD_SA exchange is used. The INFORMATIONAL exchange can be used for multiple purposes, like IPsec end of use.

4.3 General Proposal

As said before, all the mobility traffic is exchanged between the MR, in the Vehicle ITS-S, and the HA, in the Central ITS-S. The idea is to protect this channel, considering both data and control mobility traffic. It is important to be aware that before IPsec can be used, cryptographic algorithms and keying material has to be agreed between the edges of the communication (i.e., MR and HA). This agreement is performed by IKEv2 daemons just after an associated traffic policy is matched. Further details of these policies can be found in [22]. Fig. 3 summarizes the resulting IPsec associations, which are used to protect both control and data mobility traffic. All the traffic is considered as data traffic except the Mobility Header (MH) protocol, used for mobility control messages like BU and BA, and two subtypes of ICMPv6 messages: the Mobile Prefix Solicitations (MPS) and Mobile Prefix Advertisement (MPA).

Starting from scratch in a NEMO mobility scenario, as you can see in Fig. 4, the first message that appears is a Router Advertisement (RA) that the router installed in a near attachment point sends periodically to advertise its presence. The functionality of this attachment point is performed by the ITS-S Access Router, which allows the MRs to access the operator network. The MR takes the prefix from this RA and builds a CoA, assigning it to the interface that has received it. This is part of the IPv6 stateless address auto-configuration system, which is out of the scope of this study.

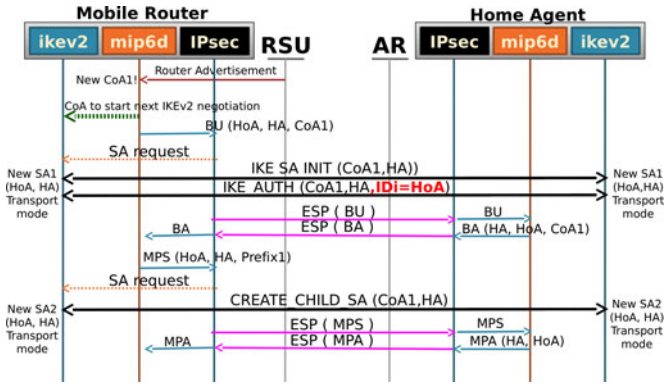


Fig. 4. Sequence diagram of the initial mobility and security bootstrap.

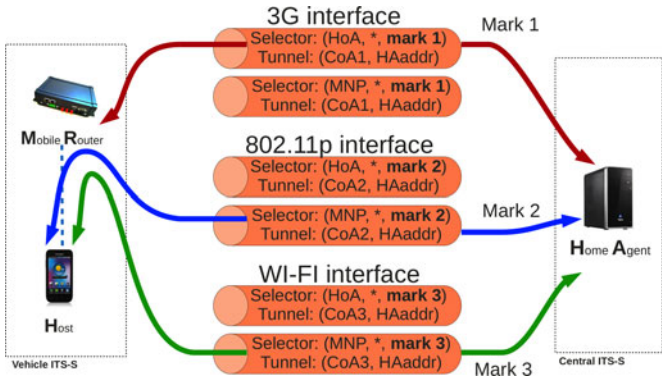


Fig. 5. Interface selection based on traffic marks.

After that, the NEMO daemon reacts by taking note of this CoA, notifying it to the HA using a BU message. This BU message matches with one of the installed IPsec policies so it has to be protected. Hence, IPsec requests the IKEv2 daemon to create the corresponding IPsec association. According to [22], in the matched policy it is stated that the resulting IPsec association must be established between the MR Home Address and the Home Agent address (HAaddr) in transport mode, using the ESP extension header. A similar IPsec association in transport mode is also created to protect MPS and MPA messages, which are also part of the mobility control traffic, as can be seen in Fig. 4. The transport mode is used to avoid an useless double header, since the sender and receiver addresses of this control traffic are the same as the tunnel endpoints.

For the data traffic, a different set of IPsec SAs, using the ESP header in tunnel mode, are created on-demand. The tunnel mode is required due to the selectors of the IPsec SAs are set in terms of HoA, but the tunnels are forced to use the associated CoA as endpoint. As a result, these IPsec SAs are CoA dependent. To have a better understanding of concepts like "selector" and "tunnel", the following section explains the different parts of an IPsec SA. As we are using the MCoA extension of the NEMO protocol, more than one CoA can be used at the same time. Due to this, two IPsec associations have to be established for the data traffic per CoA assigned to the Mobile Router. As you can see in Fig. 3, the first one is used to protect the traffic that goes form/to the Mobile Router itself to/from anywhere, while the second one is used to protect the traffic that goes to/from any host attached to the Mobile Network from/to anywhere. Hence, all attached hosts in the same Mobile Network share the same IPsec SA.

4.4 Flow Selection for Data Traffic

In order to understand how the data traffic is routed through a concrete flow, the parts of an IPsec SA are illustrated first. This is composed of the IPsec extension header to be used (ESP or AH); a selector, which is composed of a set of rules that define the traffic affected by the IPsec association; an algorithm selection for cyphering the traffic; keying material to generate keys to be used by the selected cyphering algorithms; and, finally, the address of the tunnel endpoints (if the tunnel mode is used).

Although all the resulting IPsec associations to protect data traffic have different endpoint addresses in their tunnels (using the corresponding CoA), all of them have the same traffic selectors. So the traffic by itself can not determine which IPsec association matches with. For selecting the CoA which is going to be used for transmitting each kind of traffic, it is necessary to add a different mark to each traffic and, of course, to the selectors of the IPsec SAs. In Fig. 5 it can be seen an example of this, with a MR with three available interfaces, and each one with its IPsec tunnels and its corresponding CoA. There are three traffic flows, each one marked with a different number, which allows the usage the desired IPsec association and its corresponding CoA. The NEMO daemon is the responsible for marking the mobility traffic and use a priority relationship between interfaces, in order to use the most suitable interface at each moment.

4.5 Low-Level Design Issues in a Practical Solution

The mobility service provided by the NEMO protocol and its MCoA extension works well when the traffic is not secured. Additionally, IPsec and IKEv2 protocols work well when no mobility service is required. However, when both services are used together (i.e. secure network mobility), an interoperation approach between these services is needed, as described in [22]. Here it is explained how to protect the mobility traffic between the home agent and the mobile router using IPsec and IKEv2. Nevertheless, we have realized some important lacks in the standard that should be considered in a practical implementation:

Issue 1. IKEv2 uses the MR HoA for the first negotiation, but it is not accesible in a visited network.

When the Mobile Router gains connectivity in one of its interfaces and the mobility control traffic must be secured with a new IPsec tunnel, as described in 4.3, IKEv2 in a normal fashion uses the MR HoA and the HAaddr to perform the IKEv2 negotiation, but the HoA is not directly accessible when the MR is out of its home network. The mobility service is in charge of allowing this communication using the assigned CoA, but there is no mobility service established yet.

Solution. Use the CoA instead of the HoA. In our solution the NEMO daemon provides the CoA that has triggered the process, since there could be more than one CoA configured. Fig. 4 shows this interaction between the NEMO and IKEv2 daemons. All the following IKEv2 negotiations will be also performed using this first CoA. If NEMO needs to change this CoA (due to mobility), the "K flag" is used in

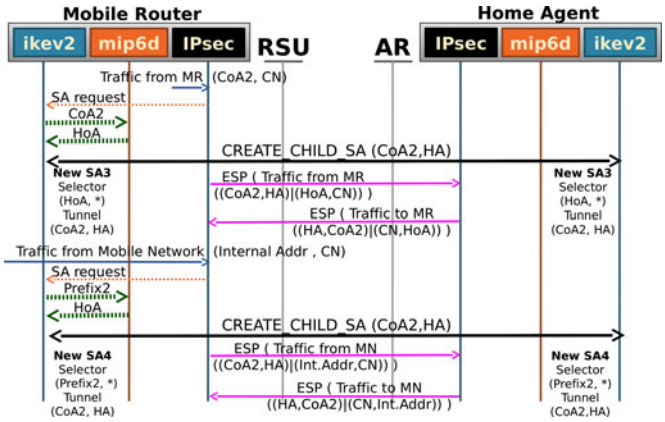


Fig. 6. Sequence diagram of IKEv2 negotiation for creating IPsec associations to protect data traffic with NEMO. MR as initiator.

the BU and BA messages to notify it. The "K flag" allows a peer to update the IKE_SA endpoints [23].

Issue 2. In the first IKEv2 negotiation, the HA cannot identify the MR, since it uses a CoA.

In the first IKEv2 negotiation for encapsulating the BU/BA messages in an IPsec tunnel, the resulting IPsec association has to be created in terms of HoA and HA addresses. However, the HA IKEv2 instance, upon the reception of the first message, does not know the MR, since the message source is the CoA.

Solution. Send the MR HoA for the interface within the Initiator Identification payload (IDi) of the IKE_AUTH request. This field is protected by the IKE Security Associatio established in the previous IKE_SA_INIT exchange, hence there is no security threat. In Fig. 4 this IDi field is marked in bold in the IKE_AUTH exchange. Further IPsec SA creations will not have this problem because IKEv2 will use the same IKE_SA to negotiate them, which is already associated with the HoA.

Issue 3. IKEv2 needs the HoA of the interface to search for the IKE_SA when a new SA for data traffic is needed.

The creation of IPsec associations for data traffic can be seen in detail in Fig. 6. The IKEv2 daemon indexes IKE_SAs using the endpoints of the negotiation. In this case, the MR (HoA) and the HA (HAaddr) addresses. However, the IKEv2 instance of the initiator of this process only knows the interface CoA.

Solution. IKEv2 daemon must ask the NEMO one for the HoA associated to the CoA, since HoAs are exclusively known by the NEMO daemon, which has a binding cache database with current CoA-HoA bindings. In the MR as initiator case, the HoA and HAaddr can be considered static, but this is not the case if the HA is the initiator, since the HA IKEv2 daemon has to maintain secure NEMO channels for several MRs at the same time.

Given the previous issues, a communication strategy between the IKEv2 and NEMO daemons is needed. Our implementation considers it by using inter-process communication using UNIX file descriptors.

5 Experimental Evaluation

The IPv6 mobility and security solution developed has been deployed in a testbed installed in a real driving area, with the aim of assessing the impact of security in the overall performance of the network. NEMO, MCoA, IPsec and IKEv2 are used in a scenario of vertical handover between two networks accesible through 802.11p and 3G technologies in this case. The testbed setup, planning and results are presented in this section.

5.1 Setting Up the Testbed

The testbed depicted in Fig. 7 has been deployed at the University of Murcia. As can be seen, the three types of ITS station presented in Section 3 are included. In the diagram, it is showed the two available communication routes, the one supported by means of a 802.11p access, using the control channel of the ETSI G5 profile [24], and the one provided by using the 3G operator's infrastructure. The addressing scheme is also showed, using IPv6 addresses for testing purposes. Due to 3G does not provide IPv6 connectivity, an OpenVPN tunnel over IPv4 has been used. A direct wired connection is used between the Roadside ITS-S and the indoor laboratory where the Central ITS-S is mounted. Here a high-end router (Border Router (BR)) interconnects the roadside network segment with the Home Agent. This router also acts as a Correspondent Node (CN).

Fig. 8 shows the equipment used. The Roadside ITS-S antenna has been placed in a window of the Faculty of Computer Engineering, while the Central ITS-S is set-up in a close laboratory inside the building. A common vehicle of the UMU fleet is used as Vehicle ITS-S. It is powered with a Mobile Router offering connectivity to in-vehicle hosts through a common WiFi connection based on IEEE 802.11g, which is provided by the same unit. The stick antenna mounted in the Roadside ITS-S showed in Fig. 8a and the vehicle roof-mounted antenna showed in Fig. 8c are used to improve the communication performance in terms of gain and radiation pattern.

For the sake of clarity, all the components used in the testbed are listed in Table 1. As can be seen in this table, the same base hardware is used for both the MR and the AR. The ITSSv6 stack has been used in both MR and HA, because this stack provides the base mobility and security services. The Roadside ITS-S uses the same ITSSv6 stack, but in this case because it is the default operating system in Laguna boxes. The rest of nodes use standard Linux distributions.

Additionally, a list of the most important configuration parameters used in several components of the testbed is provided in Table 2. The time between Router Advertisement messages have been reduced in the 802.11p interface with the aim of minimizing the time spent to detect the presence of a Roadside ITS-S. The rest of parameters remain with regular values.

5.2 Testing Plan

The purpose of the test is assessing the operation of the mobility and security procedures and observe the performance of a data channel maintained during the handoffs. Another goal of the test is to compare the 3G and 802.11p communication technologies and analyze the influence of applying security compared with the case where only mobility is used. The tests consist of a repeated trial in which a vehicle moves within the Espinardo Campus at the University of Murcia (see Fig. 9).

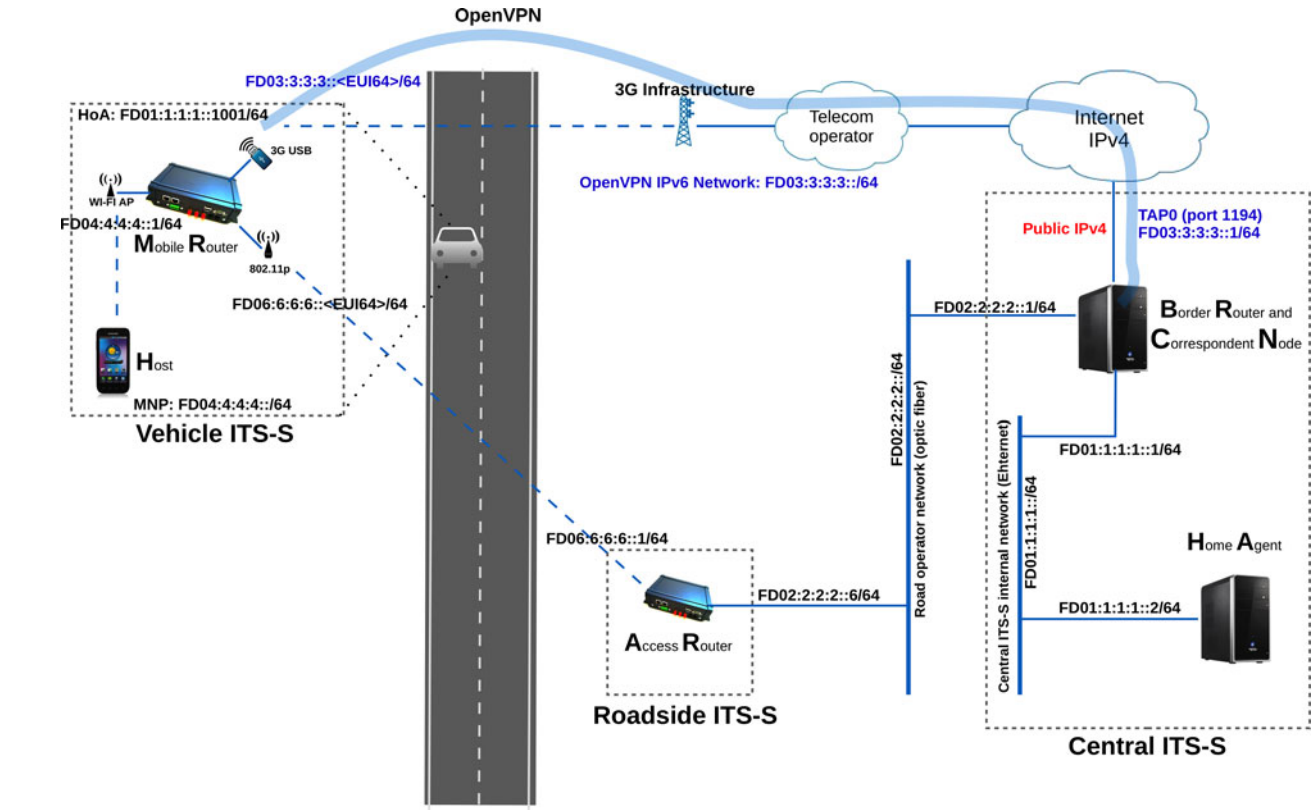
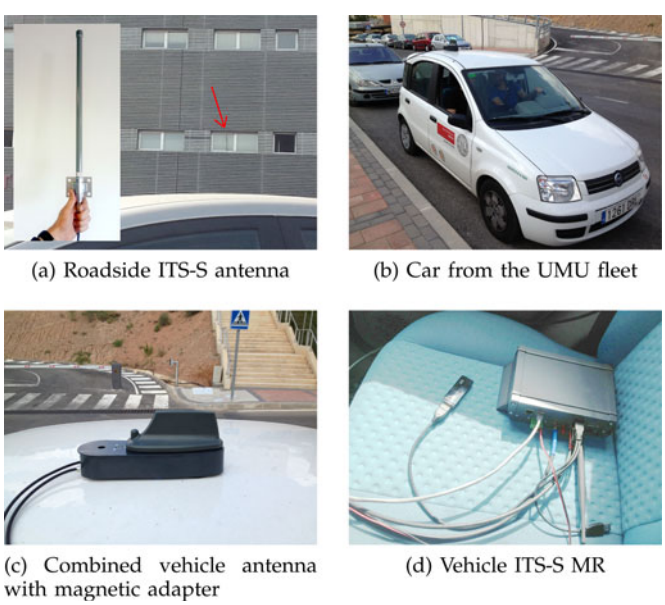


Fig. 7. ITS scenario deployed at University of Murcia.

The vehicle follows a traced path where the 3G coverage is always present, but the 802.11p coverage is limited to a part of the circuit. This can be seen in the image with a coverage plot on the map. Hence, the trial starts with 3G coverage and then a handoff occurs to 802.11p. Later, 3G is used again when 802.11p is not available.

The steps of an an individual trial (lap in the circuit) are detailed next. (1) In case security is applied, the MR uses IKEv2 to negotiate a secure IPsec tunnel to the HA. This first step is not taken into account for the test, since it is already carried out when the test starts. The MR starts communicating through a visited domain using 3G and an already assigned CoA and IPsec tunnels (if applicable). (2) The MR moves and leaves the first visited domain to reach another visited domain with a different communication technology (802.11p). While the data connection is still maintained though the old data path using 3G, the MR connects to the AR, once an RA message is received, and the MR gains access to the network by creating an additional CoA. Then, the mobility procedure is activated, and this new CoA is registered in the HA to change the uplink and downlink data path. An IKEv2 negotiation is required here only in the first lap to protect the data traffic for the 802.11p interface. Consider that all trials at the same speed have been



(a) Roadside ITS-S antenna

(b) Car from the UMU fleet

(c) Combined vehicle antenna with magnetic adapter

(d) Vehicle ITS-S MR

Fig. 8. Equipment used in the testbed.

TABLE 1
Hardware Components Used in the Testbed

Network Nodes		
Node	**Hardware**	**Software**
MR	Laguna LGN-0011	ITSSv6 stack
Host	Laptop, Intel i7, 4GB	Ubuntu 12.4
HA	PC Via 532Mhz, 476MB	ITSSv6 stack
BR/CN	PC Intel i5, 3.1Ghz, 3GB	Ubuntu 10.4
AR	Laguna LGN-0011	ITSSv6 stack
Communication hardware		
Item	**Model**	
3G USB	TP-LINK MA-180	
802.11p transceiver	Unex DCMA-86P2 mini-PCI in AR/MR	
Vehicle antenna	Omni-combined 3G/ 11p/ GPS 7dBi	
Roadside antenna	Omni-stick 12dBi	

TABLE 2
Configuration Parameters Used by Several Components

Node	Daemon	Parameter	Value
AR	radvd	Router Adv. rate (3G)	3-4s
AR	radvd	Router Adv. rate (11p)	0.2-0.6s
MR	mip6d	Max. Bind. Lifetime	12s
MR and HA	openikev2	ESP algorithm	3DES
MR and HA	openikev2	AH algorithm	SHA1
MR and HA	openikev2	DH group	2

performed consecutively. (3) The vehicle keeps moving, and leaves its current point of attachment (AR) and connects through 3G to the first visited domain (the 3G connection was already established before).

The tests have been performed using different protocols to maintain a data transmission:

- ICMPv6 protocol: A ping is performed every second from the in-vehicle host to the HA, sending 56 bytes of data in each packet. We have chosen the HA as a target of the ping because we are interested in the delay time when crossing the mobility tunnel.
- UDP protocol at 500, 1,000 and 2,000 Kbps: The UDP traffic is generated in the BR and sent to the in-vehicle host, sending 1,230 bytes of data in each packet. Both the packet delivery ratio and the link bandwidth are evaluated in this case.
- TCP protocol: the TCP traffic is generated in the in-vehicle host attached to the MR and sent to the Border Router. The maximum achievable bandwidth is evaluated.

The "iperf" tool is used to generate the UDP and TCP traffic. For the case of ICMPv6, the common "ping6" command line tool is used. Each data transmission has been carried out at different speeds with the aim of analyzing the effect of mobility on the network performance. In particular, speeds at 10, 20, 30 and 40 Km/h have been covered, and each particular configuration (traffic and speed) have been tested five times. To sum up, 200 tests were performed in total, 100 of them applying only mobility, and the rest considering also security. Such a number of trials provides statistical confidence to the results, allowing us to reach justified conclusions about the impact of mobility and security in a real scenario and thus minimizing the impact of temporal outliers due to 3G congestion, movement of vehicles and vegetation, or possible traffic jams that imply changes in the time spent at different locations.

5.3 Results

5.3.1 ICMPv6

In one of the laps of the ICMPv6 tests at 20 Km/h, the obtained values of Round-Trip Time (RTT) can be observed in Fig. 10, with and without security. The RTT when the 802.11p technology is used is very low, compared with the 3G RTT measurements. Table 3 shows in a numerical way this big difference by averaging the RTT values obtained in all the tests. Moreover, when the speed of the car increases, RTT values decrease. This is because at higher speeds the time that the car remains in a handover zone is smaller. In these zones, the 802.11p signal strength is not enough to ensure a good transmission and more packets are lost. Regarding the usage of IPsec, we can observe that the results are quite similar, and we cannot state that security implies a significant impact on the performance. This is explained by the small amount of messages sent and the low data load of the packets (the default length of an ICMPv6 Echo Request message is 64 bytes, taking into account the 8-bytes header).

5.3.2 UDP

The PDR values obtained with an individual configuration and different traffic rates can be observed in Fig. 11. Here

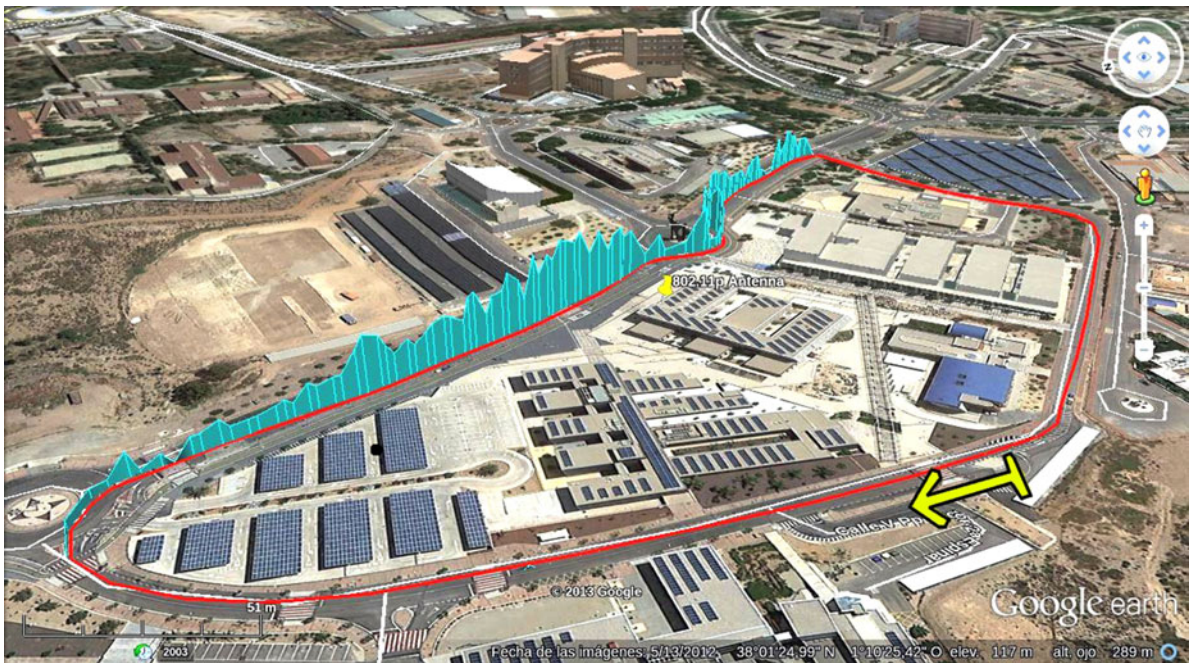
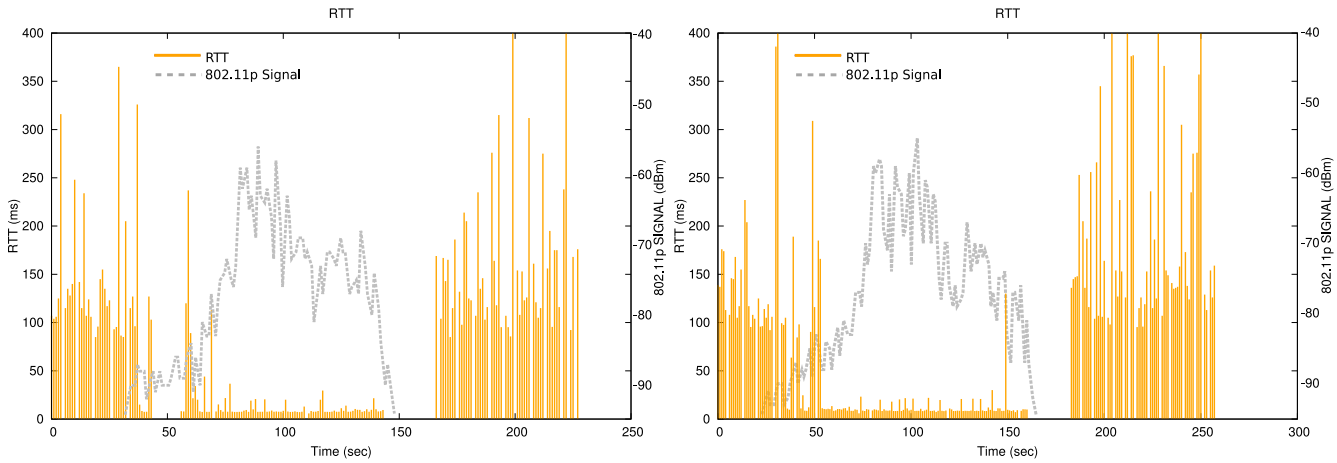


Fig. 9. Path followed in a single trial and 802.11p coverage.



(a) RTT without security (b) RTT with security

Fig. 10. ICMPv6 traffic evaluation (RTT).

one can see that PDR decreases when the traffic ratio increases. This is explained by the progressive congestion of the wireless channel, which is also affected by the mobility conditions. It is specially noticeable in the first handover, when the car spends a lot of time in a low 802.11p coverage area. This provokes a number of lost packets, in proportion to the sent ones. According to the averaged values showed in Table 4, we have not observed a significant influence of speed in the results. It should be taken into account that the car speeds are relatively low for obtaining here a clear conclusion.

Additionally, we have evaluated the communication bandwidth and how it changes during the test when increasing the traffic rate. These results are plotted in Fig. 12, where you can observe how the communication is harshly affected when 802.11p is used in zones where the signal strength is very low. In the 3G to 11p handover, the signal strength remains some seconds at a very low value, making the communication almost impossible. And in the 11p to 3g handover, the signal strength suddenly disappears, and the MR keeps trying to communicate using 802.11p until the next binding renovation. This time is configured to 12 seconds in this case, as we saw in Table 2. This means that in the worst case the communication is impossible during this whole time, as it is later explained in more detail in the handover analysis.

Regarding security, it can be seen in Table 4 that the PDR values are in general slightly worse in the test with security, but not enough to say that IPsec implies a significant overhead in the communication performance. In Figs. 11 and 12, for the cases where security is applied, it can be observed that mobility affects in a quite similar way.

TABLE 3
Statistics Resulted in ICMPv6 Tests

Speed (Km/h)	3G Mean (ms)	3G Mean IPsec (ms)	11p Mean (ms)	11p Mean IPsec (ms)
10	309.4	192.8	12.4	11.4
20	277.9	250.0	13.3	14.9
30	187.4	222.5	11.0	13.7
40	173.4	174.8	11.1	15.7

5.3.3 TCP

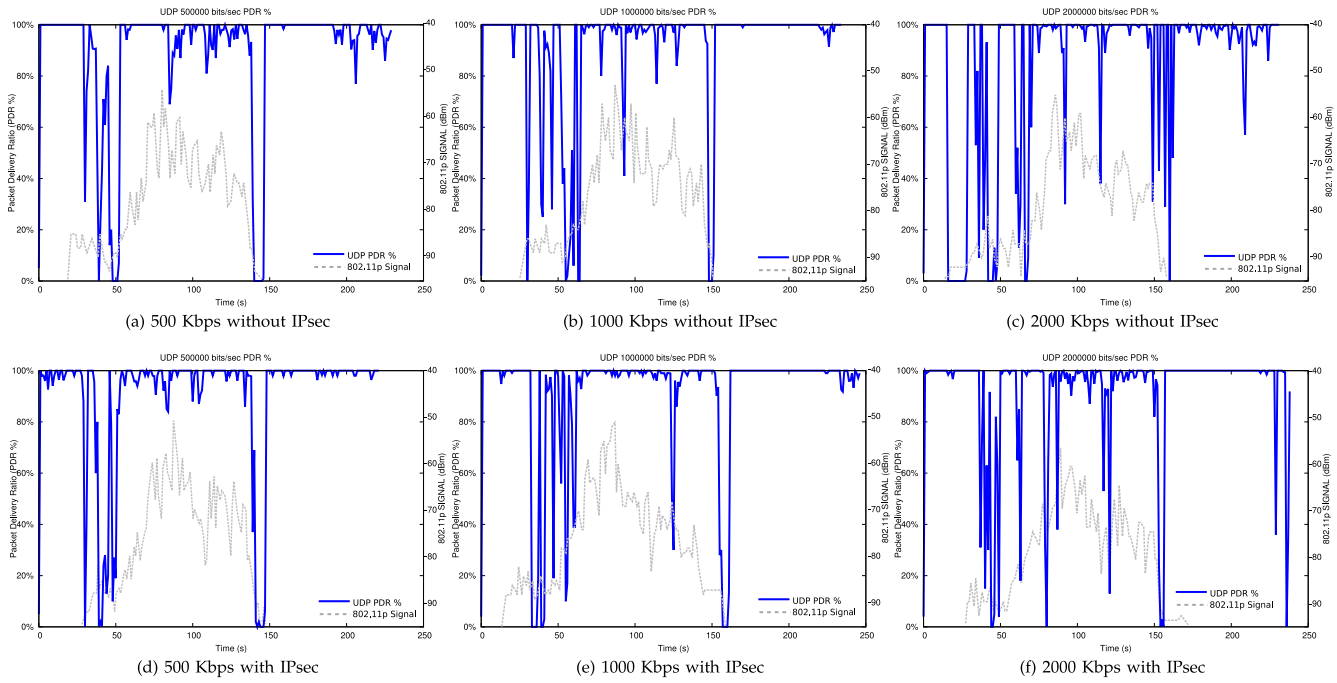
Fig. 13 shows in a graphical way that the maximum TCP bandwidth in zones where only 3G is available reaches values of around 1-2 Mbps. When 802.11p is also available, the maximum TCP bandwidth raises to around 4-5 Mbps. These values are similar in the cases with or without security. Table 5 compares the bandwidth tests performed with and without security. According to the results, there is not a noticeable impact in the usage of IPsec to protect communications. However, as expected, there is a slight reduction in the performance, due to a greater processing time of packets and a bigger packet overhead. When security is applied, more packets are needed to transport the same payload due to the extra IPv6 header used (ESP).

5.3.4 Handovers

One of the main goals of these tests is studying the handover operation and evaluate the tasks in which the time is spent during the process. This analysis helps us to improve the handover mechanism and formulate conclusions to be considered in future works. A comparison between the security/mobility case and the only mobility case is performed. The keying exchange and IPsec tunnel generation is performed before starting the tests, so the IKEv2 negotiation is initially out of this study.

On each lap there are two important handovers. The first one is triggered when the MR discovers the presence of the 802.11p-based AR while using 3G. The communication is carried out through 3G until the handover ends. The time spent in this handover is shown in Table 6, by averaging the results obtained in all the above tests with ICMPv6, UDP and TCP, and dividing the process into the following phases:

1) RA-Duplicate Address Detection (DAD): Form the Router Advertisement reception to the beginning of the Duplicate Address Detection process. In this phase a new CoA is generated.
2) DAD-BU: From the beginning of the Duplicate Address Detection process to the moment the Binding Update message is sent to the HA.
3) BU-BA: From the BU delivery to the BA reception.



(a) 500 Kbps without IPsec (b) 1000 Kbps without IPsec (c) 2000 Kbps without IPsec

(d) 500 Kbps with IPsec (e) 1000 Kbps with IPsec (f) 2000 Kbps with IPsec

Fig. 11. PDR (percent) at different traffic rates at 20 Km/h (UDP traffic).

At higher speeds the total time spent in this handover is clearly lower, due to the time that the MR stays in zones where the signal strength is low is shorter and the probability of loosing a packet is lower. Comparing these values with the values obtained when security is applied, also showed in Table 6, we can see how the results are slightly worse in all the cases, as it is illustrated in Fig. 14. This is due to the higher processing time of packets and the greater network overhead, above all.

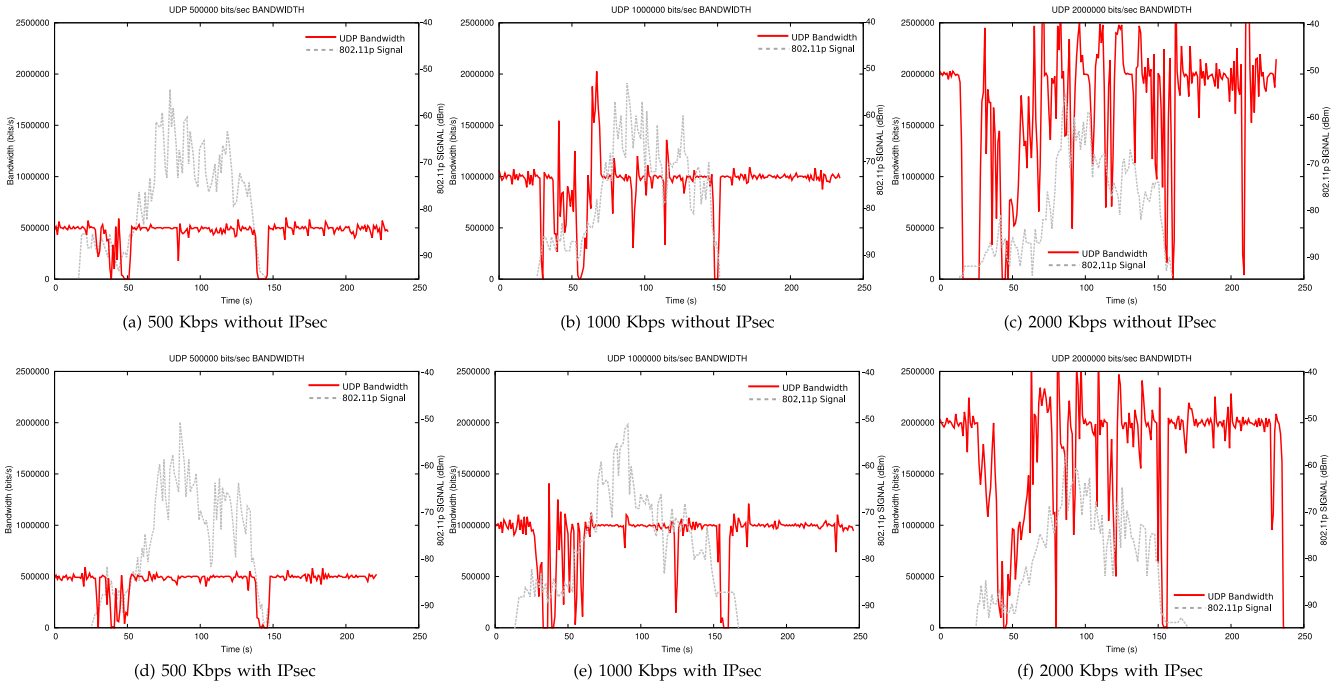
The second handover is triggered when 802.11p is being used and the mobility binding of the associated CoA expires because of a low or null coverage. Then, the traffic starts going throughout the 3G interface again. The 3G link was already established at the beginning of the test, so there is no need to renegotiate it. This procedure implies that the system needs some time to be aware that the 802.11p channel is lost. During this period the communication is not possible throughout 802.11p, but no change to another available interface (i.e., 3G) happens due to the binding entry associated with 802.11p interface is still present in the NEMO binding cache. The maximum lifetime of a CoA binding, as can be seen in Table 2, is about 12 seconds in our case. Hence, this handover can spend randomly a time between almost cero to about twelve seconds. This time could be reduced to a value close to zero if we anticipate the change of interface. This can be performed by establishing a minimum signal strength threshold that ensures enough quality in the wireless communication, and let us using as soon as possible other available interfaces in case the coverage is not enough. For this purpose, the NEMO daemon can cancel a binding entry by sending a BU message with a lifetime of zero for the binding. In almost all the figures one can appreciate the gap produced by this handover. A statistical analysis for this handover is useless because the transition time to 3G obtains random values in a quite large interval, and many more tests would be needed. The more interesting handover is found in the previously explained 3G to 802.11p case, since a new link is established in the communication stack in a vertical fashion.

TABLE 4
Statistics Resulted in UDP Tests

Speed (Km/h)	500 Kbps PDR Mean (%)	1,000 Kbps PDR Mean (%)	2,000 Kbps PDR Mean (%)
Without security			
10	88.373	88.542	78.978
20	87.997	91.553	86.109
30	90.992	91.360	86.701
40	88.155	91.525	86.886
With security			
10	83.265	78.261	76.826
20	80.189	85.393	78.185
30	88.364	88.734	82.326
40	87.662	87.398	84.559

5.4 Overall Impact of Security

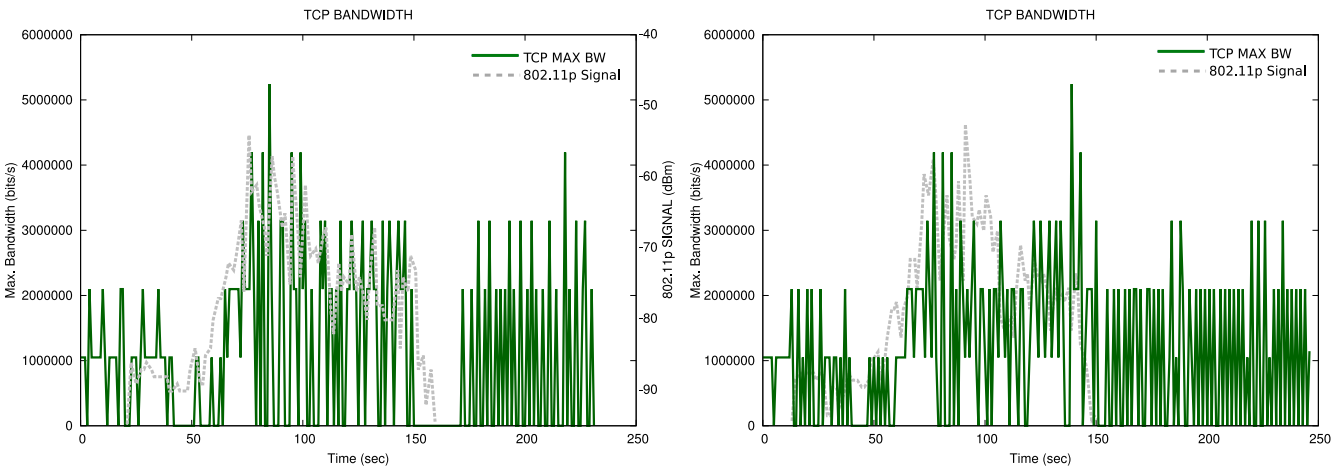
The results show a slight impact of security when the network overload is significant, due to the higher packet processing time, because of encryption/decryption tasks, and the extra packets needed to transport the same data load, because of the addition of extra security headers needed when applying IPsec. The differences in the ICMPv6 case are only attributed to outliers, however, in the UDP case, security reduces by 4.7 percent the PDR and, with TCP traffic, a reduction in performance of 5.3 percent is observed. Moreover, an increase of 15.5 percent for the handover time is noticeable when security is used, which is attributed again to the network overload and, hence, the contention in the mobility control traffic,



(a) 500 Kbps without IPsec (b) 1000 Kbps without IPsec (c) 2000 Kbps without IPsec

(d) 500 Kbps with IPsec (e) 1000 Kbps with IPsec (f) 2000 Kbps with IPsec

Fig. 12. UDP bandwidth comparison at different traffic rates at 20 Km/h.



(a) TCP bandwidth without security (b) TCP bandwidth with security

Fig. 13. Maximum bandwidth with and without security at 20 Km/h (TCP traffic).

which shares the communication channel with the data traffic. With these results it can be said that the IPv6-secured NEMO solution implies a low impact in communication performances, even when the communication channel is flooded, as compared with the confidentiality, integrity and authenticity benefits.

6 Conclusion

Through the pages of the paper the reader is introduced to security in vehicular networks and the proposal of applying state of the art IPv6 technologies to create a secure vehicular mobile network. The solution presented uses a mobile network based on NEMO, with the improvement of MCoA, to apply an IPv6 security scheme based on IPsec and IKEv2. IPsec security tunnels are established between an on-board Mobile Router, which provides connectivity (e.g., Internet Access) to in-vehicle hosts, and the NEMO Home Agent. This represents the most critical network segment to secure, involving a wireless channel operated by a road network provider or a telecom company. For designing such a system, amendments to already available standards have been proposed at the protocol design level. In this line, the

TABLE 5
Mean Bandwidth Obtained in TCP Tests

Speed (Km/h)	TCP BW Mean without IPsec (Mbits/sec)	TCP BW Mean with IPsec (Mbits/sec)
10	1.08	0.86
20	0.95	0.89
30	0.72	0.81
40	0.82	0.82

TABLE 6
Mean Values of Time Spent in Handover from 3G to 802.11p

Speed (Km/h)	RA to DAD (sec)	DAD to BU (sec)	BU to BA (sec)	Total (sec)
Without security				
10	0.4224	3.6462	1.9738	6.0425
20	0.5330	3.6554	0.8172	5.0057
30	0.5239	2.6731	0.4461	3.6432
40	0.4196	2.2944	0.6524	3.3665
With security				
10	0.4016	5.6353	1.4739	7.5109
20	0.3734	3.2836	1.8803	5.5373
30	0.4183	2.5722	0.9737	3.9643
40	0.5326	2.0787	1.2410	3.8525

negotiation of the IPsec security associations, which allow the establishment of secure IPsec channels, has received a great attention. An active cooperation between software entities for NEMO and IKEv2 at the edges of the mobility and security tunnels are necessary to achieve a correct operation of the solution, and already available protocols features for the cases of NEMO and IKEv2, have been chosen to provide a solution compliant with current standards.

One of the main contributions of the paper is the experimental assessment of the proposal with communication technologies relevant in the cooperative systems domain (i.e., 3G and 802.11p), attending the base network performance and the handover process. The results obtained from an extensive testing campaign reveal that the usage of the security proposal does not present a serious overload in the network. Only a slight performance degradation is observed when the traffic rate is increased to take the most of the network, because of higher packet processing times and the additional control data embedded in the IPv6 packets. The vehicle speed has presented a noticeable impact when driving slowly, due to the time an unstable data path is maintained at locations with a poor communication coverage, i.e., in zones where a handover is required.

Further research have been left for future work, such as the improvement of the data path selection to indicate NEMO to use an alternative link if a configured threshold is not met. This is particularly useful in our case, since a link already established and ready to be used thanks to MCoA could be exploited more effectively. The integration of IEEE 802.21 features in the ETSI/ISO reference communication architecture will provide essential improvements in the handover plane in our future works. Moreover, it is envisaged the contribution to the standards in the area of cooperative systems (ISO and ETSI) and Internet standardization (IETF).

Acknowledgments

This work has been sponsored by the EU 7th Framework Program through the ITSSv6, FOTsis, GEN6 and Inter-Trust projects (contracts 270519, 270447, 297239 and 317731), and the Ministry of Science and Innovation through the Walkie-Talkie project (TIN2011-27543-C03). José Santa is the corresponding author.

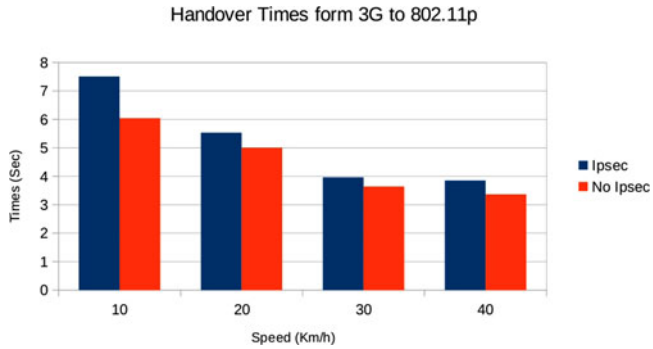


Fig. 14. Mean handover times from 3G to 802.11p with and without security.

References

[1] ETSI TC ITS, *Intelligent Transport Systems (ITS); Communications Architecture*, ETSI EN 302 665, Eur. Telecommun. Stand. Inst., Sep. 2010.

[2] ISO TC 204, *Intelligent Transport Systems-Communications Access for Land Mobiles (CALM)-Architecture*, ISO 21217, Int. Organ. Stand., Apr. 2013.

[3] ETSI TC ITS, *Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)*, ETSI TR 102 893, Eur. Telecommun. Stand. Inst., Mar. 2010.

[4] ETSI TC ITS, *Intelligent Transport Systems (ITS); Security; Security Services and Architecture*, ETSI TS 102 731, Eur. Telecommun. Stand. Inst., Sep. 2010.

[5] ETSI TC ITS, *Intelligent Transport Systems (ITS); Security; ITS Communication Security Architecture and Security Management*, ETSI TS 102 940, Eur. Telecommun. Stand. Inst., Jun. 2012.

[6] J. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security Privacy*, vol. 2, no. 3, pp. 49–55, May 2004.

[7] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 110–113, Jan. 2014.

[8] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[9] N. Alexiou, M. Lagana, S. Gisdakis, M. Khodaei, and P. Papadimitratos, "Vespa: Vehicular security and privacy-preserving architecture," in *Proc. ACM Workshop Hot Topics Wireless Netw. Secur. Privacy*, Apr. 2013, pp. 19–24.

[10] S. Cespedes, X. Shen, and C. Lazo, "IP mobility management for vehicular communication networks: Challenges and solutions," *IEEE Commun. Mag.*, vol. 49, no. 5, pp. 187–194, May 2011.

[11] 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 *Proc. 18th ITS World Congr. Exhib.*, 2011, pp. 1–9.

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

[13] S. Zrelli, A. Miyaji, Y. Shinoda, and T. Ernst, "Security and access control for vehicular communications," in *Proc. IEEE Int. Conf. Wireless Mobile Comput. Netw. Commun.*, Jan. 2008, pp. 561–566.

[14] J. Santa, F. Pereniguez, A. Moragon, P. Fernandez, F. Bernal, and A. Skarmeta, "IPv6 communication stack for deploying cooperative vehicular services," *Int. J. Intell. Transportation Syst. Res.*, vol. 12, pp. 1–13, 2013.

[15] 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," *IEEE Intell. Transportation Syst. Mag.*, vol. 6, no. 1, pp. 17–34, Spring 2014.

[16] O. Shagdar, M. Tsukada, M. Kakiuchi, T. Toukabri, and T. Ernst, "Experimentation towards IPv6 over IEEE 802.11p with ITS station architecture," in *Proc. IEEE Intell. Veh. Symp.*, Jun. 2012, pp. 1–6.

[17] 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 Commun. Mag.*, vol. 50, no. 5, pp. 184 –191, May 2012.

[18] J. Gozalvez, M. Sepulcre, and R. Bauza, "IEEE 802.11p vehicle to infrastructure communications in urban environments," *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 176–183, May 2012.
[19] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network mobility (NEMO) basic support protocol," RFC 3963 (Proposed Standard), Jan. 2005.
[20] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, "Multiple Care-of addresses registration," RFC 5648 (Proposed Standard), *Int. Eng. Task Force*, Oct. 2009.
[21] S. Kent and K. Seo, "Security architecture for the internet protocol," RFC 4301 (Proposed Standard), *Internet Eng. Task Force*, Dec. 2005.
[22] V. Devarapalli and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture," RFC 4877 (Proposed Standard), Apr. 2007.
[23] S. Decugis, "Key management mobility capability (K) flag in Mobile IPv6 BU/BA messages," RFC draft, Dec. 2007.
[24] ETSI TC ITS, *European Profile Standard for the Physical and Medium Access Control Layer of Intelligent Transport Systems Operating in the 5 GHz Frequency Band*, ETSI ES 202 663, Eur. Telecommun. Stand. Inst., Nov. 2009.

Pedro J. Fernández received the MSc degree in computer science engineering and the MSc degree in advanced information and telematics technologies in 2005 and 2007, both from the University of Murcia, Spain, where he is currently working toward the PhD degree. He is a researcher at the University of Murcia. His research interests include communication security protocols, intelligent transportation systems (ITS) and mobility.

José Santa received the MSc degree in computer engineering and the MSc degree in advanced information and telematics technologies in 2004 and 2008, respectively, and the PhD degree in computer science in 2009, all from the University of Murcia, Spain. He is currently an assistant professor in the University Centre of Defence at the Spanish Air Force Academy. His research interests include ITS and telematics.

Fernando Bernal received the MSc degree in computer science engineering and the MSc degree in advanced information and telematics technologies in 2008 and 2009, respectively, both from the University of Murcia, Spain. He is currently working as a researcher and developer at the same university. His main research interests include authentication and authorization aspects in mobile networks.

Antonio F. Skarmeta received the MS degree in computer science from the University of Granada, Spain, and the BS (Honors) and the PhD degrees in computer science from the University of Murcia. He is a full professor at the same university. Research interests include mobile communications, artificial intelligence, and home automation. He is a member of the IEEE.