Chapter 4

Deploying ITS Scenarios Providing Security and Mobility Services Based on IEEE 802.11p Technology

Pedro Javier Fernández Ruiz,
Fernando Bernal Hidalgo, José Santa Lozano and
Antonio F. Skarmeta

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/55285

1. 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 [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, such as the German simTD, the French SCORE@F, the Spanish OASIS, or the recent European DRIVE C2X and FOTsis. Although these initiatives start from the basis of previous research projects, such as CVIS or Coopers, preliminary developments made on those projects should be further extended to obtain more complete communication stacks 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 comform an IPv6-based communication stack ready to be used by FOT projects. Part of the work presented in this chapter has been carried out inside ITSSv6 and it has been in this frame where we have realized the great lack of security countermeasures currently available for FOT-equivalent evaluations.

Standardization efforts in ISO TC 204, based on the Communications Access for Land Mobiles (CALM) concept, and ETSI TC ITS, based on the recent European ITS Communication Architecture, have paved the way towards vehicular cooperative systems. The ETSI proposal presents a more refined view of a communication stack that should be instantiated on Personal, Vehicle, Roadside and Central ITS Stations, where common OSI layers are surrounded by two planes for stack management and security. While the first one has been more or less exploited in terms of software lifecycle and interface management, above all in the CVIS project, the specification and implementation of the security plane is still a pending issue.

In current researches security is not taken into account in the communication stack development. Our proposal is a first attempt to integrate mobility services usually provided in vehicular scenarios with security mechanisms. This integration will result in a communication stack that also provides integrity and confidentiality to the transmitted traffic. Also, an extensible access control mechanism based on EAP [16] is part of this set of proposals that are distributed among the protocol layers of the ISO/ETSI ITS communication stack.

At link-layer level, Wi-Fi, 802.11p and 3G/UMTS communication technologies have been integrated with a network selection algorithm that can be parameterised according to preferences. At network-layer level, an IPv6 network mobility solution is provided to support the change of network attachment point when the communication stack is running on a vehicle. Also at network-layer level, secure IPv6 communications are achieved by means of standardized IETF protocols, such as Internet Protocol Security (IPsec) and Internet Key Exchange Version two (IKEv2). The final solution obtained gives a ready-to-use IPv6 communication stack provided with security mechanisms, which can be currently integrated in the ITS communication segment envisaged to be the first in being exploited: the vehicle to infrastructure (V2I) one or vice versa (I2V). Moreover, these capabilities have been validated by a suitable software platform and applications, and tested through performance tests obtained in real evaluations, whose main results are presented later.

It is worth noting that all the research has been developed using open source, and in particular, Linux distributions like Ubuntu and Busybox.

The outline of the rest of the chapter is as follows. Section 2 describes the concept of "Intelligent Transport System" (ITS), how the standard organizations like the International Organization for Standardization (ISO) and the European Telecommunications Standards Institute (ETSI) are working to develop the Reference ITS Communication Architecture, adding some arguments of how important is the IPv6 protocol for this architecture and ITS in general. An overview of the most common access technologies used in ITS scenarios can be found in Section 3, focusing on their suitability for ITS communications. Section 4 and 5 describe the ITS scenarios from the security and mobility point of view respectively. In Section 6 is discussed

http://dx.doi.org/10.5772/55285

the interoperability between security and mobility mechanisms. Finally, a set of evaluation results are presented in Section 7 followed by the conclusions in Section 8.

2. Intelligent Transport System (ITS)

Intelligent Transport System (ITS) applies advanced technologies of electronics, communications, computers, control and sensing and detecting in all kinds of transportation system in order to improve safety, efficiency and service, and traffic situation through transmitting real-time information.

Next subsection describes the Reference ITS Communication Architecture to be used in part of the FOTs scenarios. This architecture is mainly motivated by the works carried out by the International Organization for Standardization (ISO) and the European Telecommunications Standards Institute (ETSI) in the frame of Cooperative ITS. Its design and implementation has been done within the European IPv6 ITS Station Stack (ITSSv6) project, inside the 7TH Framework Program. As can be read in the rest of this section, it comprises a communication stack that can be instantiated into different roles that cover the key elements of a communication architecture based on the concept of ITS Station, from ETSI [5]. The communication stack implementation is totally based on IPv6 and offers capabilities especially focused on the network layer, also supporting a set of communication technologies and providing a common and simple IP view to facilities or final applications.

2.1. Reference ITS communication architecture

In an effort towards harmonization, the international ITS community agreed on the definition of a common ITS communication architecture suitable for a variety of communication scenarios (vehicle-based, roadside-based and Internet-based) through a diversity of access technologies (802.11p, 2G/3G, etc.) and for a variety of application types (road safety, traffic efficiency and comfort / infotainment) deployed in various continents or countries ruled by different policies.

This common communication architecture is known as the ITS station reference architecture and is specified by ISO [4] and ETSI [5]. This architecture is illustrated in Figure 1. Both ISO and ETSI architecture standards are based on the same terminology and tend to converge, although there are still remaining differences between the two. This lack of consistency shall disappear as standards are being currently revised.

It is divided in functional modules, each one with a defined and concrete functionality. The most important for our research are:

- IPv6 mobility management module: this module comprises mechanisms for maintaining IPv6 global addressing, Internet reachability, session connectivity and media-independent handovers (handover between different media) for in-vehicle networks. Nothing new, this module combines NEMO Basic Support [20] and Multiple Care-of Address Registration [21].

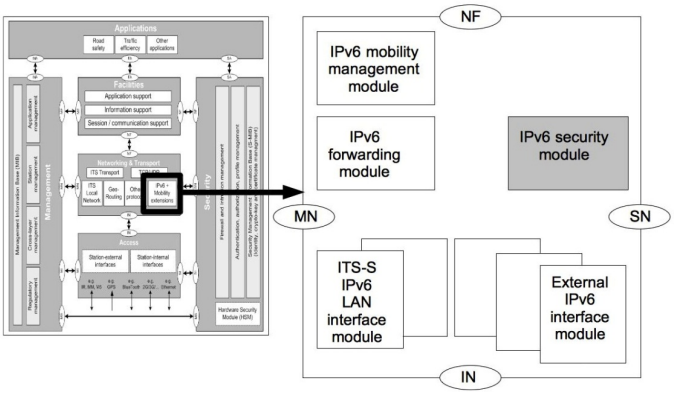

Figure 1. IPv6 functional modules in ISO 21210

It must only be present in ITS station IPv6 nodes performing functions to maintain Internet reachability and session continuity.

- IPv6 security module: the need for a module in charge of securing IPv6 communications is acknowledged in ISO 21210 [7], but the required features are not yet defined. In our case, it is assumed that this module comprises the functionality offered by IPsec [18], IKEv2 [15] and EAP [16].

One distinguishable feature of this architecture is the ability to use a variety of networking protocols in order to meet opposite design requirements i.e. fast time-critical communications for traffic safety versus more relaxed communication requirements for road efficiency and comfort / infotainment. However, for the majority of anticipated ITS applications and services, IPv6 is ideally suited. A particular emphasis was thus put on the use of IPv6 as the convergence layer ensuring the support of the diversity of access technologies, the diversity of applications and the diversity of communication scenarios. This resulted into the FP6 CVIS (Cooperative Vehicle-Infrastructure Systems) European Project taking a leadership on the specification and implementation of IPv6 Networking as defined by ISO [7], the FP6 SeVeCom (Secure Vehicular Communication) European Project investigating IPv6 security issues (IPv6 addresses based on pseudonyms), the FP7 GeoNet (IPv6 GeoNetworking) European Project specifying and implementing the concepts linking IPv6 networking and geographic addressing and routing, and the launch of IPv6-related work items at both ETSI TC ITS and ISO TC204. In addition, ETSI is going to provide test suites related to IPv6 and GeoNetworking.

2.2. ITS and IPv6

2.2.1. IPv6 basics

The first widely deployed protocol allowing packet-based communications between computers located in various networks was the Internet Protocol version 4 (IPv4) [8]. This protocol

http://dx.doi.org/10.5772/55285

defines addresses of a fixed 32-bit length. This allows approximately 4 billion IP addresses to be used on the Internet. This figure appeared sufficient for the expected use of the protocol at that time. But the emergence of the commercial use of the Internet in the 90's decade led to an exponential use of IP addresses. To prevent the shortage of IP addresses, the IETF decided two measures: the specification of private IPv4 address spaces [9], to be used with Network Address Translation (NAT) and the design of a new version of the IP protocol: IP version 6 (IPv6).

The specification of this new protocol was finalized in 1998 [10]. This protocol defines addresses of a fixed 128-bit length. This allows a very large address space that is considered sufficient for most ambitious deployment scenarios (there would be enough addresses to identify every grain of sand on Earth). In addition to the address space, IPv6 defines new protocols to ease the management of the layer-3 protocol stack, such as Neighbour Discovery [11] that allows auto-configuration of IPv6 addresses.

While IPv6 is entering in its deployment phase, the depletion of the IPv4 address space is on going, despite the measures taken by the IETF. The global IPv4 address pool is exhausted since February 2011 and several regions such as Asia and Europe are facing shortage of IPv4 addresses. The exhaustion for the European region may happen in August 2012. After this date, Internet Service Providers (ISPs) and hosting services will not be able to get new IPv4 addresses. The deployment of IPv6 is therefore critical to ensure the future growth of the services of these stakeholders.

2.2.2. IPv6 for ITS

By the time ITS services requiring the use of the public IP addresses appear on the market, there will not be enough public IPv4 address available. The use of this version of IP scales to meet the addressing needs of a growing number of vehicles and connected devices, and provides the added functionality necessary in mobile environments. By relying on IPv6 in their ITS communication architectures, ISO, followed by ETSI, COMeSafety and the Car-to-Car Communication Consortium, have thus taken the right decision to guarantee sustainable deployment of Collaborative ITS.

Furthermore, IPv6 has the potential to decrease accident rates by enabling transmission of safety critical information. This chapter is not envisaged to demonstrate that this would be the case for real time applications, since the automotive industry and the SDOs(Standard Developing Organizations)at this time are not considering IPv6 for fast V2V communications. However, it is simple to note that not all data is time critical. There is no question that IPv6 could be a media-agnostic carrier of such non-time critical but safety essential information. FP7 GeoNet has demonstrated an example of the benefit of IPv6 for time critical application in the traffic hazard detection and notification scenario during its final demonstration [12]. Once the safety benefit of IPv6 is acknowledged, there are classical ways of calculating the economic impact of reducing road fatalities. E.g. the Safety Forum 2003 Summary Report estimated the cost of accidents at 160 billion euros. A 1% reduction would reduce these costs by 1.6 billion euros annually. And of course, this does not take into account the reduction of pain and suffering experienced by surviving family members and friends of accident victims

that may not be adequately reflected in the method used to estimate the economic costs of traffic fatalities.

3. Access technologies

In order to provide access to a wide set of networks, the current distribution of the communication stack supports three key technologies in vehicular networking: 2G/3G, 802.11a/b/g (WiFi) and 802.11p. The communication stack is able to manage communication transceivers of many manufactures and it can exchange the data flow among them in a transparent way for the upper layers. All used frequencies have similar physical attributes, however their middle layer properties differ.

In the current work these interfaces have been provided by means of Laguna boxes from Commsignia (see Figure 2). The Laguna's firmware is ready to support these interfaces, providing an easy and unified way to configure them using the UCI (Unified Configuration Interface) from OpenWrt project [13].

Figure 2. Laguna box form Commsignia company

There are other wireless communication technologies considered for ITS communication like satellite, infra-red, WiMAX, microwave, millimetre wave; but they will not be evaluated during these tests.

3.1. GSM, 3G and UMTS

3G networks are wide area cellular telephone networks which have evolved to incorporate high-speed internet access. It has greater network capacity through improved spectrum efficiency. 3G technology supports around 144 Kbps, with high speed movement, i.e. in a vehicle, 384 Kbps locally, and up to 2Mbps for fixed stations, i.e. in a building. 3G technology uses CDMA, TDMA and FDMA, and the data are sent through packet switching.

http://dx.doi.org/10.5772/55285

3G has the best overall coverage or range of the three technologies and may serve as the easiest way of communication. Its range is 4-6 km at medium data throughput with the highest latency of the mentioned technologies. Response times can exceed 1 second.

The next generation technology is LTE (3GPP Long Term Evolution project) with speeds of 100/50 Mbit/s using orthogonal frequency-division multiplexing. The mobility support is also more robust, speeds up to 350-500 Km/h are supported depending on the frequency.

GSM also has the possibility to fall back to previous technologies below 3G (like EDGE) if no other types of services are present or are of low quality. This results in limited data throughput, but gives a higher technological reliability.

3.2. 802.11a/b/g/n

IEEE 802.11a/b/g/n protocols are supported by the Laguna's firmware and the compat-wireless open source project. Requirements of these standards are extremely and extensively complex, thus the implementations contain multi-level collaboration among device drivers, MAC layer modules, configuration and interface modules. Nevertheless, existing implementations support a wide range of wireless communication devices including upper layer functionalities. Summarizing, the existing solutions cover all the requirements against the IEEE 802.11a/b/g/n standards such as carrier frequencies, band width specifications, data rates, modulation schemes, authentication modes and security.

Operation and communication modes need to be supported according to the standards. One of these modes is the ad-hoc mode which is used for decentralized self-organizing connections between individual nodes. The implementation supports other, centralized modes: access point (ap) and station (sta). For these modes, authentication and encryption services are available as well, which are implemented by the Linux kernel and compat-drivers project [28].

High level configuration and management tools which are also integrated into the system prove a high level abstraction for device drivers and modules of the wireless framework. These user space applications provide a full scale management platform and most of them are integrated from the wireless-tools package e.g., iw, iwlib, etc. applications and libraries. Usually called as common WLAN (wireless local area networks), the a/b/g/n standards use the 2.4 and 5 GHz frequency bands with DSSS or OFDM modulation. It is a widely used technology with a range of 100-200 m. Response time calculation (using ad-hoc mode) supposes that several packets need to be transferred, before a link's status can be treated as set up.

An established connection may have a response time below 100ms either in ad-hoc or infra-structure mode.

In our test scenario, 802.11b is used for providing connectivity to the personal devices that use the car as point of attachment. It is capable of 11 Mbit/s maximum raw data throughput over the 2.4 GHz frequency band on 14 channels (split from 2.401 GHz to 2.495 GHz) using the original CSMA/CA protocol defined by the base standard. The common usage prefers the point-to-multipoint configuration. An access point communicates with one or more clients using an omni-directional antenna.

Common WiFi's latest amendment is 802.11n adding multiple-input multiple-output antennas used in both 2.4 and 5GHz to achieve net data rates up to 600 Mbit/s. The newest extension under development is 802.11ac, promising to better all parameters of the throughput.

3.3. 802.11p

The amendment modifies the 802.11 standard to add support for WLAN in a vehicular environment. It also proposes small modifications to the PHY and MAC layers in order to achieve a robust connection and a fast setup for moving vehicles. As 802.11a and g, the 802.11p is also based on the OFDM modulation method.

The 11p technology also differs by the fact that it is not as common as 802.11b or 3G and therefore has a limited hardware support, only a few companies offer transceivers capable of communicating with the required set of features and performance.

802.11p has the same range as WLAN, but uses a dedicated frequency (the licensed ITS band of 5.85-5.925 GHz) and an optimized set of protocols to reach a latency under all other listed technologies. Communication does not require a classic link to be set up and this results that high-priority traffic latency may be kept under tens of milliseconds at most. This attribute is essential for time-critical safety messages of ITS applications.

The implementation of the 802.11p feature is completely missing in the current open source world; therefore it cannot be imported from any known open source repository. Though there are several driver initiatives, a complete standard compliant version is yet to be found. The feature is newly developed to support the latest Linux kernel interfaces while focusing on the compliance of the latest communication standards.

4. IPv6 communication security

The main modules identified for providing security to the reference ITS communication architecture are IPsec and IKEv2. The latter is used to negotiate the security channels created by IPsec. A brief description of these technologies is included next.

4.1. IPsec

The IPsec software is present in Linux releases. The implementation supports both Encapsulated Security Payload (ESP) for both encryption and authentication and Authentication Header (AH) for authenticating the remote peer, which can be used together or separately to secure IPv4 or IPv6 traffic. The IPsec support is mandatory in IPv6 stack. The core implementation includes utilities for manual keying, while dynamic key management is implemented by other software components, using the IKE [14] and IKEv2 [15] protocols.

The main concept in IPsec is the Security Assiciation (SA), that establishes a secure channel to protect traffic. For selecting which traffic is going to be protected exists the concept of policy. This IPsec policies are stored in the Secure Policy Database (SPD). Every policy should be

http://dx.doi.org/10.5772/55285

linked with a SA that determines the protocol (AH or ESP), cryptographic algorithm and keying material to be used to protect the traffic determined by the policy.

These SAs have to be established by hand by the networks administrators. As the keying material has to be refreshed with a determined frequency in order to ensure the traffic protection, administrators have to perform this task every time by hand, that becomes this in a bit tedious or even impossible task in large networks. For automate this task, IKE and IKEv2 protocols appeared, solving this scalability problem.

4.2. IKEv2

The Internet Key Exchange (IKE) protocol was designed in order to automate the IPsec Security Association (SA) establishment. The first version of IKE (IKEv1) [14] that was released in 1998, suffered some limitations and complexity, so that the IETF decided to propose a second version that was able to solve these limitations and simplified the protocol. The result was the IKEv2 protocol [15].

The IKEv2 protocol uses a non-reliable transport protocol (UDP using ports 500 and 4500) and it is performed between two parties: the initiator and the responder. As their names indicate, the initiator starts the IKEv2 communication, whereas the responder acts as server during the negotiation. The protocol is composed of a well-defined set of four main exchanges (request-response), namely: IKE_SA_INIT, IKE_AUTH, CREATE_CHILD_SA and INFORMATIONAL. Figure 3 shows the various IKEv2 message exchanges. These exchanges provides reliability to the IKEv2 protocol, since there is an expected and well defined response for each request.

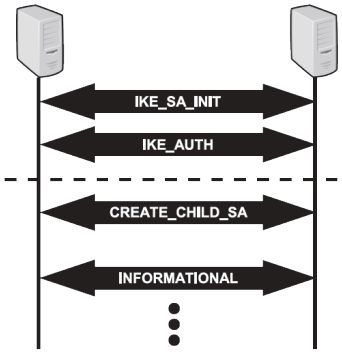

Figure 3. IKEv2 message Exchange.

The IKE_SA_INIT exchange establishes an SA at IKE level, named the IKE SA (IKE_SA), between the participant entities. This IKE_SA will protect all the following IKE exchanges. Once the IKE_SA is established, an IKE_AUTH exchange is performed in order to authenticate the parties and create the first IPsec SA (CHILD_SA) between them. These exchanges are denoted as initial exchanges and always must occur in this order.

There are two additional exchanges used for managing the SAs. The CREATE_CHILD_SA exchange allows creating additional SAs. The INFORMATIONAL exchange can be used for deleting SAs, notify events and manage configuration issues. When a SA expires a new one is created in order to replace the old one. This process is denoted as rekeying.

Additionally, IKEv2 introduces a good set of improvements with respect to IKEv1. For example, one of the main advantages of IKEv2 against IKEv1 is the inclusion of new features like NAT traversal, the transport of the Extensible Authentication Protocol (EAP) [16] for a flexible authentication mechanism and remote address configuration support.

4.3. EAP

Before establishing an IPSec based access control, the involved ITS station IPv6 nodes are required to authenticate each other. This mutual authentication is typically performed by means of the IKEv2 protocol [15], which in turn, relies on authentication mechanisms such as the Extensible Authentication Protocol [16], that allows the usage of a wide set interchangeable authentication methods.

5. IPv6 mobility in vehicular networks

Service continuity is a need when telematics services are offered in vehicles. Although it is possible to offer this feature at higher layers, maintaining communications at network level simplifies the implementation of facilities and applications in the ITS communication stack. The reference ITS station reference architecture described by ETSI and ISO includes, as part of its IPv6 support, Network Mobility Basic Support (NEMO) to accomplish the IPv6 communication continuity objective. The next parts of this section describe in more detail NEMO and some improvements that enhance the network connectivity of vehicles.

5.1. NEMO

5.1.1. IPv6 network mobility basic support (NEMO)

NEMO provides the necessary procedures within the ITS station networking & transport layer to allow an ITS station to maintain continuous IPv6 connectivity while changing its point of attachment to the network. The IPv6 mobility support module within the IPv6 protocol block ensures this. The IPv6 mobility support module comprises mechanisms for maintaining IPv6 global addressing, Internet reachability, session connectivity and media-independent handovers (handover between different access technologies) for in-vehicle networks. This module mostly combines Network Mobility Basic Support (NemoBS) [20]and Multiple Care-of Addresses Registration (MCoA) [21].

NemoBS is designed to maintain Internet connectivity between all the nodes in the vehicle and the infrastructure (network mobility support). This is performed without breaking the flows under transmission, and transparently to the nodes located behind the Mobile Router (MR), the

http://dx.doi.org/10.5772/55285

mobile network nodes (MNNs), and the communication peers, also call "correspondent nodes" (CNs). This is handled by mobility management functions in the MR and a server known as the Home Agent (HA) located in an IPv6 subnet known to the MR as the home IPv6 link.

The key idea of NemoBS is that the IPv6 mobile network prefix (known as MNP) allocated to the MR is kept irrespective of the topological location of the MR while a binding between the MNP and the newly acquired temporary Care-of Address (CoA) configured on the external IPv6 egress connecting the MR to the Internet is recorded at the HA. This registration is performed by the MR at each subsequent point of attachment to an AR. In order to do this, the MR uses its global address known as the Home Address (HoA). This allows a node in the vehicle to remain reachable at the same IPv6 address as long as the address is not deprecated. The HA is now able to redirect all packets to the current location of the vehicle. MNNs attached to the MR do not need to configure a new IPv6 address nor do they need to perform any mobility support function to benefit from the Internet connectivity provided by the MR. This mobility support mechanism provided by NEMO is thus very easy to deploy, at a minimum cost.

The tunnel between the MR and the HA may be implemented as a virtual IPv6 interface pointing to a physical egress interface (external IPv6 interface) where packets would be encapsulated. The routing module as the physical external IPv6 interface would then treat such an IPv6 virtual interface. The same rules would thus be applied to the selection of the MR-HA.

The earlier Mobile IPv6 mobility support specification [22] provides Internet connectivity to a single moving IPv6 host only (IPv6 host mobility support). Mobile IPv6 is therefore inappropriate for the most advanced ITS use cases which usually consider more than one in-vehicle embedded CPU. Network mobility support using RFC 3963 also supports situations where there would be only a single IPv6 node deployed in the vehicle. Indeed, the ability to support an entire network of n nodes includes the ability to support a network of one node only. So just considering NEMO Basic Support, and not Mobile IPv6, makes the ITS station architecture much simpler.

The operation of NEMO Basic Support is illustrated in Figure 4.

For a better understanding of NEMO, the terminology is specified in [23] and the design goals behind NEMO Basic Support are described in [24]. These documents are normative documents about how to apply NEMO Basic Support to the ITS station architecture.

5.2. MCoA

The specifications given in [25] are extensions to Mobile IPv6 [22] and NEMO Basic Support [20] and allows a MR to register multiple Care-of Addresses (CoA) with its HA.

As a result of the notification of the tunnel set-up from the IP mobility management module to the ITS station management entity, the ITS station management entity should notify the IPv6 forwarding module with new forwarding table entries.

The operation of MCoA is illustrated in Figure 5.

The NEMO and MCoA extension of the Mobile IPv6 protocol was implemented as part of the NAUTILUS6 project. The project extended the UMIP (USAGI-patched Mobile IPv6 for Linux)

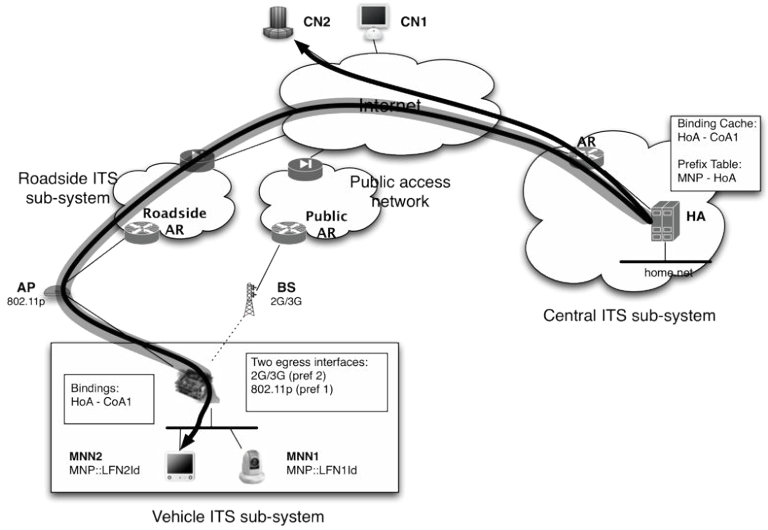

Figure 4. IPv6 session continuity with NEMO Basic Support.

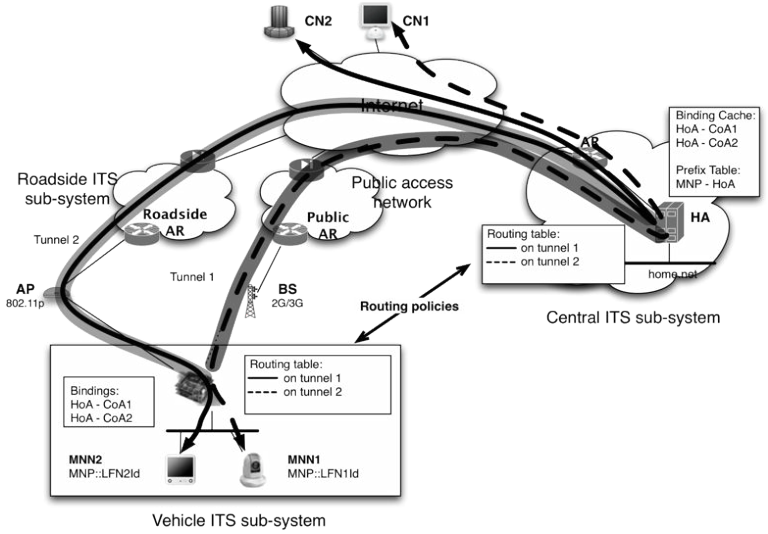

Figure 5. IPv6 mobile edge multihoming.

implementation with the NEMO, MCoA, DSMIPv6, HAHA, FMIPv6 protocols. After the project had ended an open source repository was opened on the UMIP.ORG website to continue the maintenance of the implementation with the help of the open source community. The MCoA protocol extension was not merged back into the code base because the standard

http://dx.doi.org/10.5772/55285

was not finished at the time of the original implementation. To fully integrate the NEMO and MCoA functionality into the communication software stack presented in this chapter the existing implementation had to be reviewed in scope of standard compliance, scalability and conformance with other features such as IKEv2.

Advanced mobility support of IPv6 is two-fold in modern Linux environments. Packet transformation and decoding of protocol signalling implemented in the Linux kernel, while the rest of the protocol stack is implemented in a user space binary called mip6d. The latest open source snapshot of mip6d does not contain Multiple Care-Of Address support as the proposed implementation of the feature does not comply with the final standard definition.

The implementation of the MCoA protocol uses separate internal mechanisms for protocol signalling and data transmission. The description of internal procedures for handling protocols messages can be distinguished by the following properties:

- Signalling packets: Signalling messages such as Binding Updates (BU), Binding Acknowledgements (BA), Mobile Prefix Solicitation and Mobile Prefix Advertisement are built in the user space application and sent to the network stack via the socket interface. In case of BU/BA messages the XFRM framework is called which insert the Home Address Option and Routing Header Type 2 option headers after the IPv6 header. When IPsec is used, the installed XFRM policies demand that after the final packet structure is created, the payload of the packet is encrypted in ESP transport mode.
- Data packets: Data packets could originate from two sources: from the Mobile Router (MR) itself or from a Mobile Network Node (MNN). As MCoA allows the presence of multiple tunnels between the MR and the HA, all sharing the same Home Address (HoA) which makes exact routing decisions impossible. To properly route the packets, another identifier called BID is needed which selects the appropriate tunnel interface. The implementation design of the policy based routing mechanism is shown in Figure 6.

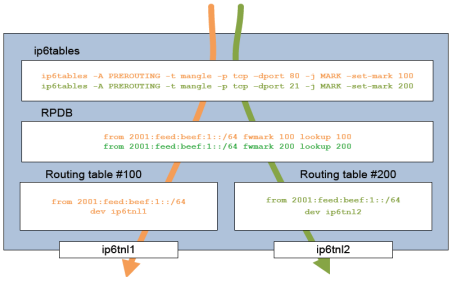

Figure 6. Policy routing used in MCoA.

Packet flows are marked by the Netfilter framework. Using the MARK target, all packets matching the rule are marked inside the kernel, so they can be later processed by the added mark value. Recent Linux implementations include a Routing Policy Database (RPDB), which allows the selection of routing tables based on a policy; in this case the routing table to use is

determined by the packet mark value previously applied by the Netfilter framework. Each routing table contains default-route entries for different tunnel interfaces, hereby completing the policy routing method by sending the packet on the appropriate tunnel interface. IPsec secured data flows are routed the same way, however the encapsulation of data packets is done by the XFRM framework, which transmit the packets in ESP tunnel mode, making the above introduced ip6tnl IPv6-in-IPv6 kernel interfaces obsolete.

6. Integration of security, mobility and access control services

One of the main contribution in this chapter is the integration between the presented services of access control, security and mobility. There is no problem on using each service on its own, but when more than one is required to be applied at the same time, some interoperation issues have to be addressed first.

Figure 7 shows the considered scenario where a vehicle ITS station changes to a new point of attachment (Roadside ITS station). Following the standard mobility procedures, the vehicle's MR receives a RA message from the AR containing the network prefix (NP), which is used by the MR to configure the new MR's CoA (Care-of-Address).

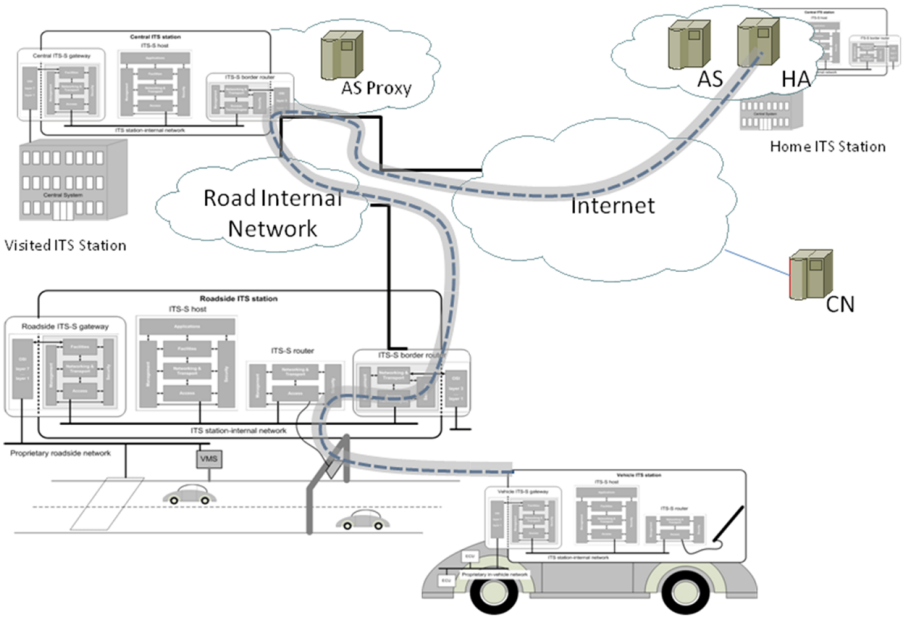

Figure 7. Authentication scheme for a vehicle ITS station accessing Internet through a roadside ITS station.

http://dx.doi.org/10.5772/55285

Before the use of the new configured CoA for IPv6 communications (e.g., to inform the home HA about the new vehicle's location), mobility signalling and data traffic are requested to be protected by means of IPsec. This protection has to be RFC4877 [26] compliant. This requires collaboration between security(IKEv2) and mobility(NEMO) services. First of all, IKEv2 has to manage the NEMO signalling traffic in a different and specific way. In addition, IKEv2 daemon needs to be aware of which of the available Care-of addresses is the one that has triggered the IKEv2 negotiation. For this reason, NEMO daemon has to notify this Care-of address to the IKEv2 daemon.

Before mobility negotiation could be performed, the MR must get authenticated against the AR to gain access to the network. This is performed by means of link-layer mechanisms like 802.1x [27]. Also, another authentication process has to be performed against the HA to gain mobility service. This authentication is performed jointly with the IPsec tunnel negotiation using IKEv2 protocol where EAP is used as authentication mechanism. While the MR acts as EAP peer, the HA implements the EAP authenticator functionality. The EAP authenticator may contact the home Authentication Server (AS) (acting as EAP server).

Once the EAP authentication is successfully completed, the IKEv2 protocol negotiates the parameters of the IPSec SA (keying material, algorithm, etc.). This IPSec SA is used to protect IPv6 packets transmitted between MR and HA through the ESP security protocol, thus satisfying the restriction on the HA for granting access to the mobility service to attached MRs.

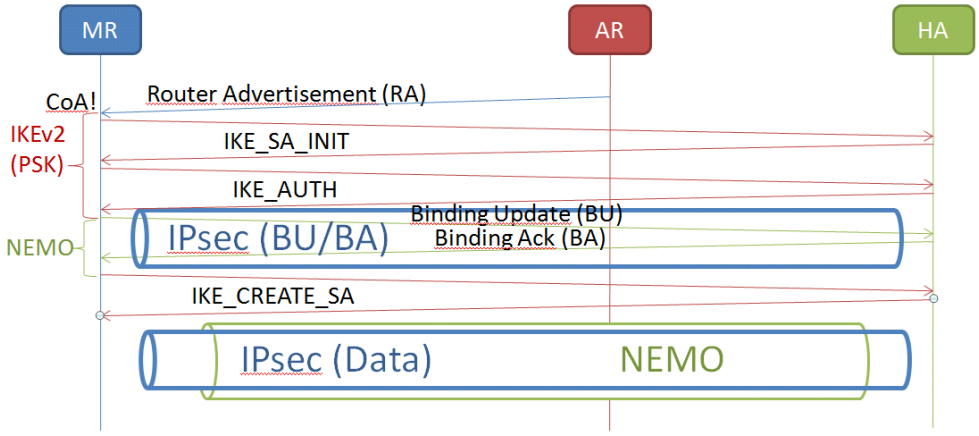

Figure 8. Sequence diagram of the IKEv2 and NEMO negotiation

In the Figure 8 can be seen that the negotiation is triggered by means of Router Advertisements (RA) presence, launching the IKEv2 negotiation to establish the IPsec tunnel that will protect the mobility control signalling, i.e., BU and BA messages. Once the mobility is also established, another IKEv2 negotiation is performed for the data traffic protection.

7. Performance evaluation of the secure network mobility solutions

The main purpose of the test is to evaluate the performance of the network when both mobility and security services are applied. Also, the performance of 802.11p wireless technology is measured, since it is aimed to be the next generation wireless technology designed for vehicular networks.

7.1. Description of the tests

In this scenario 3G and 802.11p can be used at the same time thanks to the MCoA capabilities of the mobility service.

As a transition mechanism for IPv4 support in a IPv6 network, an OpenVPN solution has been deployed, that creates IPv6 tunnels over IPv4 networks (3G networks), as it is depicted in Figure 9.

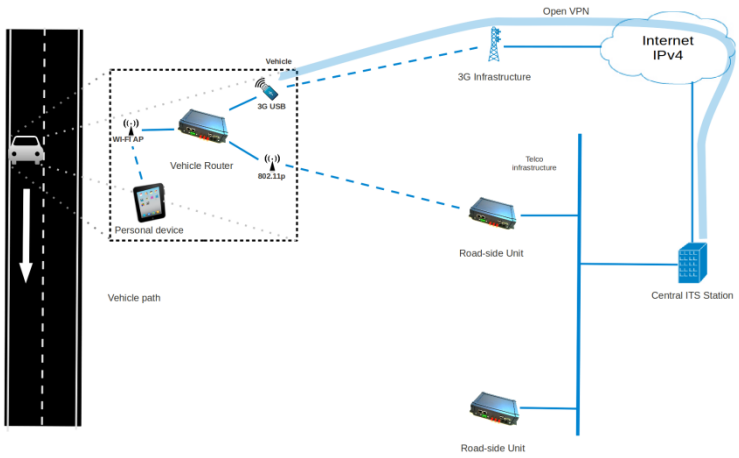

Figure 9. Test scenario using OpenVPN

In the test, the vehicle moves within the Espinardo Campus (University of Murcia) using the 3G connectivity and the 802.11p coverage to perform handoffs, as can be seen in Figure 10.

The next steps are carried out in the case of study considered for the tests:

1. The data flow start and the vehicle (MR) starts communicating through its home domain, through 802.11p at point A.
2. The vehicle (MR) moves towards a new (visited) domain, the one provided with the 3G infrastructure. An inter-domain and inter-technology handoff is necessary.
3. While the data connection is still maintained by the old data path through 802.11p, the vehicle (MR) connects to the 3G infrastructure, but it needs to gain network access

http://dx.doi.org/10.5772/55285

Figure 10. Test location

obtaining a new CoA. This is performed once the Router Advertisement message is received through the established OpenVPN tunnel.

4. The new MR CoA is registered in HA to change the data path used for both uplink and downlink communications.

5. The vehicle (MR) keeps moving and gains again 802.11p coverage. 802.11p is preferred and the MR changes its point of attachment. A new intra-domain and intra-technology handoff is necessary.

6. The vehicle (MR) keeps moving until point B and then stops.

The next metrics have been considered in the evaluations:

1. Bandwidth, measured in Mbps. It has been evaluated with a TCP flow maintained at the maximum allowable speed from the personal device to a correspondent node (CN) connected within the IPv6 UMU network.

2. Packet Delivery Ratio (PDR), measured in percentage of packets lost. It has been evaluated with a UDP flow in the downlink direction at 100 Kbps, 1Mbps and 5 Mbps, from the CN to the personal device.

3. Round-trip delay time (RTT), measured in ms. It has been evaluated with ICMPv6 traffic generated from the personal device to the CN. ICMPv6 Echo Request messages have been generated at a 1 Hz rate.

UDP and TCP traffics have been generated with the *iperf* utility, while the ICMPv6 traffic has been obtained from the common *ping6* Unix tool.

7.2. Results

The previous test plan has been executed enabling IPsec and IKEv2. Each of these round of tests considers one TCP trial, two UDP trials (100 Kbps and 1 Mbps), and one ICMP trial.

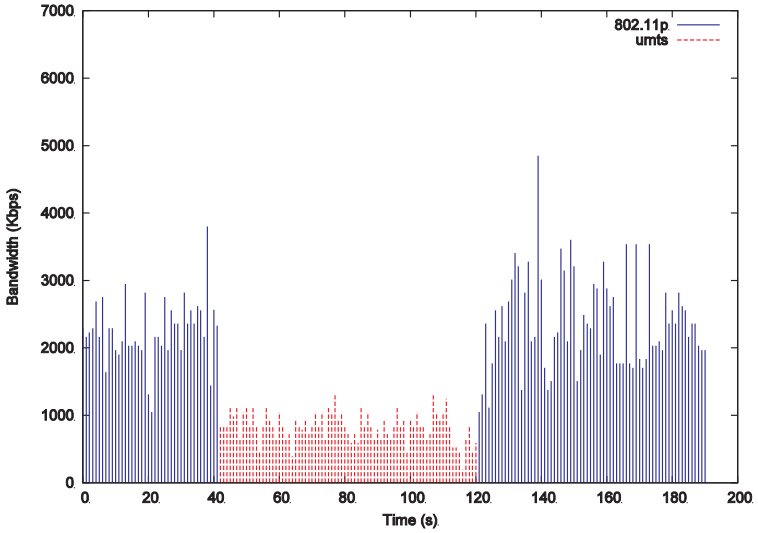

Figure 11. TCP bandwidth results

The bandwidth results obtained in the TCP tests are showed in Figure 11. As can be seen, the slow-start algorithm of TCP tries to adapt to the wireless medium in the whole test. This effect is even worse here if it is considered that tests have been carried out with a moving vehicle. Initially the vehicle is connected using 802.11p technology. The first handoff from 802.11p to 3G occurs just after time 40 sec, and the second one, from 3G to 802.11p at time around 120 sec. It is evident that the data rate using 802.11p is higher than 3G.

Although the achievable bandwidth is potentially higher in the 802.11p stretch than in any other part of the circuit, as it has been showed in the TCP case, the amount of packet losses is higher than when the 3G link is used as can be seen in Figure 12 and Figure 13. This is explained by the implementation of the 802.11p stack, which is in a very initial state where there are no improvements like Doppler effect mitigation. Changing the bit rate of the UDP transmission, we can appreciate that the packets are lost at the same locations in the path. It is worth nothing that in the handoff from 802.11p to 3G exists a gap where no transmission is possible, as you can appreciate in Figure 12 and Figure 13. This is due to the 802.11p coverage is gradually lost until the point that the transmission is not possible. The interface selector mechanism spends some seconds to realise that this interface is no longer usable and switches to the other one. This fact does not happen in the handoff from 3G to 802.11p because the 3G interface is not lost at anytime, so the interface selector mechanism switches seamlessly to 802.11p when this preferred interface is usable again.

http://dx.doi.org/10.5772/55285

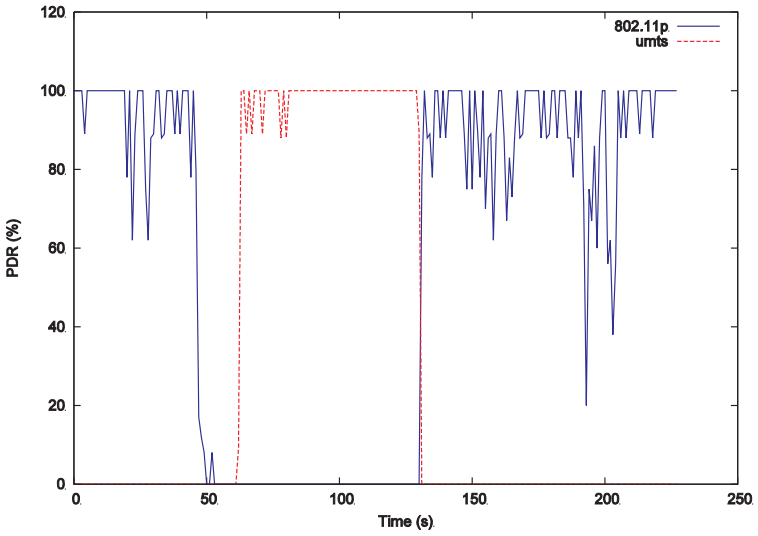

Figure 12. Packet delivery ratio at 100 Kbps

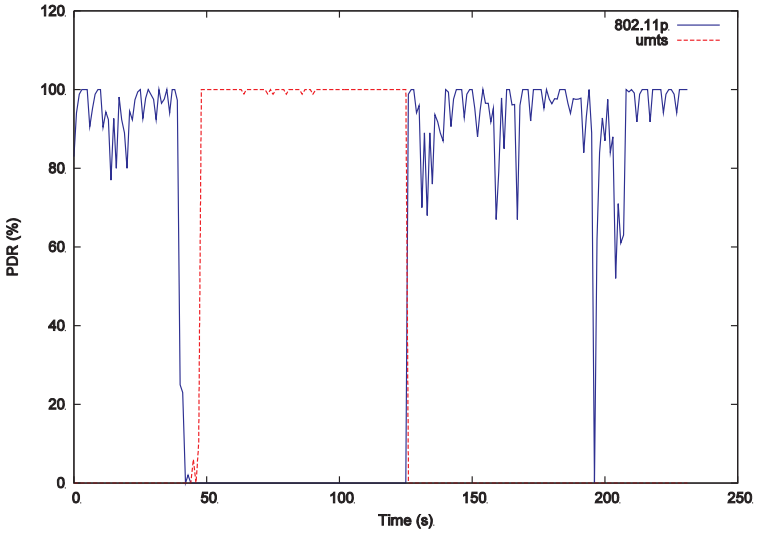

Figure 13. Packet delivery ratio at 1 Mbps

Finally, the network latency has been evaluated and results are given in Figure 14. These results have been obtained by generating ICMP traffic from the personal device inside the vehicle.

Regarding round-trip time (RTT), it is about twelve times better in 802.11p than in 3G. A low RTT is desirable for real-time applications, where the delay in packet delivery is crucial.

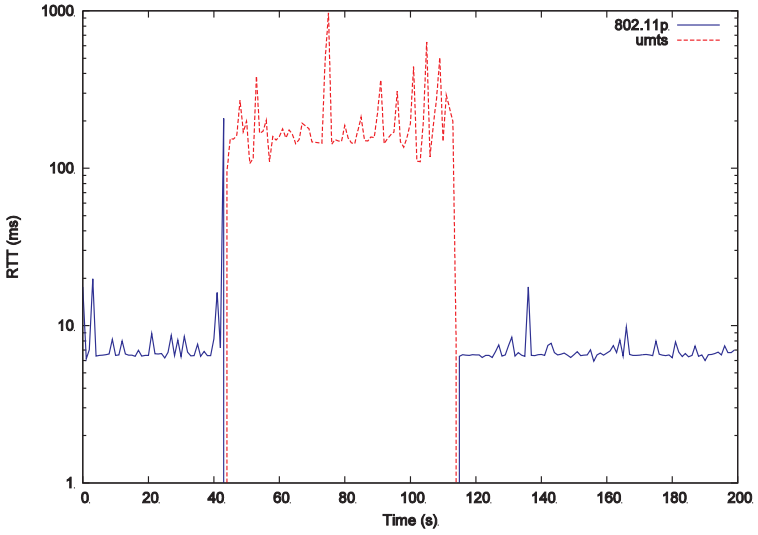

Figure 14. Latency evaluation with ICMPv6 traffic

8. Conclusion

This work presents 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 also presented, using NEMO and an IPsec/IKEv2 combination to secure control and data traffic.

Taking into account the results presented in this chapter, this secure IPv6 network mobility solution performs efficiently under real inter-technology handoffs, the most difficult to accomplish. The communication stack operates correctly, maintaining the in-vehicle network connectivity in all tests and showing performance results that enable the communication stack to be used in many vehicular services. Unless high-quality multimedia transmissions are required, the bandwidth results indicate that the data rate required by most of the traffic efficiency and comfort services can be covered, and, according to latency tests, even non-critical security services, which are not highly dependent on real-time response, could be implemented, such as emergency assistance, variable traffic signalling or kamikaze warning.

Acknowledgements

This work has been sponsored by the European Seventh Framework Program, through the ITSSv6 Project (contract 270519), FOTsis (contract 270447); the Ministry of Science and Innovation, through the Walkie-Talkie (TIN2011-27543-C03) project; and the Seneca Foundation, by means of the GERM program (04552/GERM/06).

Author details

Pedro Javier Fernández Ruiz, Fernando Bernal Hidalgo, José Santa Lozano and Antonio F. Skarmeta*

*Address all correspondence to: skarmeta@um.es

Department of Information and Communication Engineering, University of Murcia, Spain

References

[1] Weib, C. V2x communication in europe: From research projects towards standardization and field testing of vehicle communication technology," Computer Networks, (2011). Deploying vehicle-2-x communication. Available: http://www.sciencedirect.com/science/article/pii/S1389128611001198, 55(14), 3103-3119.

[2] Festag, A, Le, L, & Goleva, M. 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). Available: http://doi.acm.org/10.1145/2030698.2030710, 73-78.

[3] ISOIntelligent transport systems- Cooperative Systems- Terms, Definitions and Guidelines for Standards Documents- Part 1, April (2012). ISO/NP 17465:2012(E).

[4] ISOIntelligent transport systems- Communications Access for Land Mobiles (CALM)- Architecture, April (2010). ISO 21217:2010(E).

[5] Intelligent Transport Systems (ITS); Communications ArchitectureSeptember (2010). ETSI EN 302 665 , 1

[6] ISOIntelligent transport systems- Communications Access for Land Mobiles (CALM)- CALM using 2G Cellular Systems, April (2008). ISO/IS 21212:2008.

[7] ISOIntelligent transport systems- Communications Access for Land Mobiles (CALM)- IPv6 Networking, January (2011). ISO 21210:2011(E)

[8] Internet Engineering Task ForceRFC 791 Internet Protocol- DARPA Inernet Programm, Protocol Specification, September (1981).

[9] Rekhter, Y, Moskowitz, B, Karrenberg, D, De Groot, G. J, & Lear, E. Address allocation for private internets. RFC 1918 (Best Current Practice), February (1996).

[10] Deering, S, & Hinden, R. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460 (Draft Standard), December (1998). Updated by RFCs 5095, 5722, 5871.

[11] Narten, T, Nordmark, E, & Simpson, W. Neighbor discovery for ip version 6 (ipv6). RFC 2461 (Proposed Standard), (1998).

[12] GeoNetD7.1 GeoNet Experimentation Results. Public deliverable, June (2010).

[13] OpenWRT: Linux distribution for embedded deviceshttps://openwrt.org (accessed 27 July (2012).

[14] Harkins, D, & Carrel, D. The Internet Key Exchange (IKE). RFC 2409 (Standards Track),November (1998).

[15] Kauffman, C. Internet Key Exchange (IKEv2) Protocol. IETF RFC 4306, Dec. (2005).

[16] Aboba, B, Blunk, L, Vollbrecht, J, Carlson, J, & Levkowetz, H. Extensible AuthenticationProtocol (EAP). RFC3748, June (2004).

[17] Arkko, J, Kempf, J, Zill, B, & Nikander, P. Secure neighbor discovery (send). RFC 3971 (Proposed Standard), March (2005).

[18] Kent, S, & Seo, K. Security architecture for the internet protocol. RFC 4301, (2005).

[19] Jari Arkko, Vijay Devarapalli, and Francis Dupont Using IPsec to protect mobile ipv6 signalling between mobile nodes and home agents. RFC, June (2004).

[20] Devarapalli, V, Wakikawa, R, Petrescu, A, & Thubert, P. Network Mobility (NEMO) Basic Support Protocol. RFC 3963 (Proposed Standard), January (2005).

[21] Wakikawa, R, Devarapalli, V, Tsirtsis, G, Ernst, T, & Nagami, K. Multiple Care-of Addresses Registration. RFC 5648 (Proposed Standard), October (2009).

[22] Johnson, D, Perkins, C, & Arkko, J. Mobility Support in IPv6. RFC 3775 (Proposed Standard),June (2004). Obsoleted by RFC 6275.

[23] Ernst, T, & Lach, H-Y. Network Mobility Support Terminology. RFC 4885 (Informational), July (2007).

[24] Ernst, T. Network Mobility Support Goals and Requirements. RFC 4886 (Informational), July (2007).

[25] Wakikawa, R, Devarapalli, V, Tsirtsis, G, Ernst, T, & Nagami, K. Multiple Care-of Addresses Registration. RFC 5648 (Proposed Standard), October (2009).

http://dx.doi.org/10.5772/55285

[26] Devarapalli, V, & Dupont, F. Mobile IPv6 Operation with IKEv2 and the Revised IP-sec Architecture.RFC 4877 (Standards Track), (2007).

[27] IEEE 802x- Port Based Network Access Control- http://www.ieee802.org/1/x.htmlac-cesed by 30th July (2012).

[28] Compat-drivers project- http://linuxwirelessorg (accesed by 27th November (2012).