Nemo Using IPv6 for Real time Communications

A.Manikandan

Department of computer science, Vels University, India

Abstract
In this paper may deals with the problems that may faced during intelligent transporting vehicular networks. Here using internet key exchange, telecommunications,ipv6 and network mobility. he use of multicast addressing is expanded and simplified, and provides additional optimization for the delivery of services. Device mobility, security, and configuration aspects have been considered in the design of the protocol. 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 Network mobility 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.

Keywords:
IPV6, NEMO, Internet key exchange.

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 hard-ware, 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 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, pro-posing standards more focused on a particular communication stack including IEEE technologies.

Manuscript received April 5, 2026
Manuscript revised April 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.4.18

2. Related Works

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, 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 and a high-level security framework has been envisaged, 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. reviews in more detail particular works in the literature about security and experimentation in vehicular networks. overviews the IPv6-based communication architecture in which the security solution has been implemented and tested, while details the security subsystem and the new contributions to the design issues found in standards. Later, a real test bed 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,concludes the paper summarizing the main contributions and addressing future lines of work

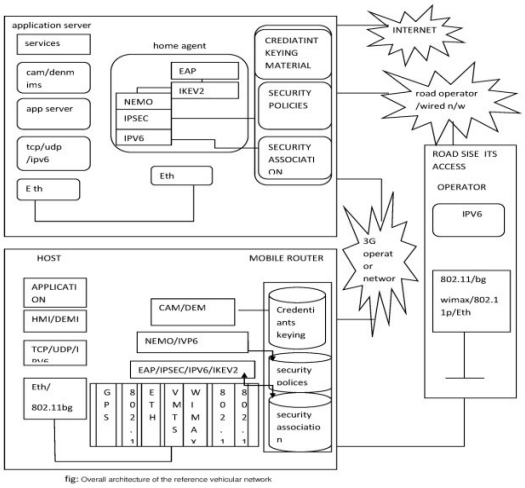

fig: Overall architecture of the reference vehicular network

3. Real Time Architecture

Figure 1: overall performance architecture

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 net-work 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 the set of elements included within the networking (NEMO) 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 Reg istration (MCoA). Regarding security, the mobile router is equipped with the needed elements to secure mobility-related traffic by means of Internet Protocol Security, although this part is extended in the next section.

The stack on the Vehicle ITS-S Host is in charge of execut ing final applications that could access remote services. As observed, this stack includes a common networking middle-ware 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 we can see the commu nication 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

4.General Proposal

It can be noted that the main target of the research in this paper is addressing (secure) vehicle to infrastructure com munications using an IPv6-compliant solution. In this line, NEMO is an IP technology inherently designed for support ing 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 commu nication is completely feasible, given that all communica tion 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.

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.

Table1:hardware component

TABLE 1
Hardware Components Used in the Testbed

Network Nodes		
Node	Hardware	Software
MR	Laguna LGN-0011	ITSSv6 stack
Host	Laptop, Intel i7, 4 GB	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	

and IKEv2. Nevertheless, we have real-ized some important lacks in the standard that should be considered in a practical implementation.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 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.

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. MR with three avail-able 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.

5. 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 illus-trated 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.

6. Setting Up the Test

The testbed depicted in As can be seen, the three types of ITS sta-tion presented in Section 3 are included. In the diagram, it is showed the two available communication rou tes, the one supported by means of a 802.11p access, using the control channel of the ETSI G5 profile, 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).

7. Plan path

The purpose of the test is assessing the operation of the mobil-ity 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 MurciaSolution. 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 config-ured.

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 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. 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 and the vehicle roof-mounted antenna are used to improve the communication performance in terms of gain and radiation pattern. 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 HA addr 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 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 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.

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, 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.

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.

8. 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. Internet 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 over-load 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 notice-able impact when driving slowly, due to the time an unstable data path is maintained at locations with a poor communication coverage in zones where a handover is required.

9. Future Works

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 and Internet standardization..

REFERENCES

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

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

[3] 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.

[4] 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.

[5] C. Weib, “V2X communication in Europe: From research projects towards standardization and field testing of vehicle communica-tion technology,” Comput. Netw., vol. 55, no. 14, pp. 3103–3119, 2011.

[6] J.-C. Lin, C.-S. Lin, C.-N. Liang, and B.-C. Chen, “Wireless com-munication performance based on IEEE 802.11p R2V field trials,” IEEE Commun. Mag., vol. 50, no. 5, pp. 184 –191, May 2012.

[7] V. Devarapalli and F. Dupont, “Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture,” RFC 4877 (Proposed Standard), Apr. 2007