

Proxy Usage for Vehicular Networks Interconnection

Alfredo Matos, Justino Santos and Rui Aguiar
Instituto de Telecomunicações
Universidade de Aveiro

Andreas Festag and Roberto Baldessari
NEC Europe Ltd.
Network Laboratories

Abstract—This paper discusses the introduction of a new network element - MIPv6 Proxy - to act on behalf of registering nodes on a moving car network. The new element allows increased performance, while reducing communication costs and enhancing communication in general.

I. INTRODUCTION

Communication capabilities in vehicles is one of the main trends in development of future automobiles. When used for extending the driver's range of recognition, they offer a wide range of new applications for active traffic safety, such as collision warning, road obstacle warning, cooperative driving or intersection collision warning [1]. These safety applications are typically based on wireless Ad-Hoc networks, where vehicles exchange data by means of vehicles that relay data over multiple wireless hops [2], [3]. In these vehicular Ad-Hoc networks (VANET) data is transmitted through the shortest path from the source to the destination vehicle(s) without crossing any infrastructure.

For Mobile IPv6 [4] and Ad-Hoc routing integration, several technical problems exist such as efficient distribution of router advertisements, selection of Internet gateways, and movement detection of the mobile node. For solution of these problems different proposals exist [6], [7], [8], [9] but none of them address the specific problems of VANETs.

A solution for VANETs, resorting to Position Based Routing for vehicular Ad-Hoc networks (PBRV), has been presented in [10]. It defines an architecture for VANETs, integrating Ad-Hoc Networks and multiple communication modes. This includes MIPv6 integration with PBRV mechanisms. In the presented solution it is assumed that VANETs are sustained by automobiles, which have no power or size requirements, meaning that can be equipped with larger hardware, with no power consumption restrictions or bandwidth limitations. Also vehicles participate in Ad-Hoc networks with other vehicles, and form in-car networks, based on the devices of the occupants (or other devices located inside the car). These devices can have limitations in terms of power consumption, range amongst others. Another limitation is the fact that these devices should be MIPv6 enabled, requiring infrastructure access for Home Address (HoA) to Home Address communication, even if they are inside the same car, or within the same Ad-Hoc domain.

Another problem posed by VANETs is how to handle the vehicle networks connection to other networks. One possible solution to the problem is to use NEMO [5] integrated with an Ad-Hoc routing protocol. The main problem of this solution

is that it assumes that communication to the infrastructure is always possible, although that might not be true. Our approach to the problem tries to address this problem, enabling usage of Vehicle to Vehicle communication using Home Addresses if the communicating nodes are reachable in the Ad-hoc domain, but not connected to the infrastructure.

This paper proposes a Mobile IPv6 Proxy (MIPP) to enhance VANET communication, within a specific architecture and discusses different approaches for the design of the MIPP. The remaining sections of the paper are structured as follows: In Sect. II we present the underlying architecture that serves as basis for this work. In Sect. III we analyse all the available options reasonable to consider for a Mobile IPv6 Proxy. In Sect. IV we propose two possible solutions for the MIPP and finalise with a comparison between them. In Sect. V we present the general conclusions of our work.

II. VEHICULAR AD-HOC NETWORK ARCHITECTURE

In [10] an architecture is described that integrates VANETs relying on position information for routing with infrastructure access and MIPv6 for hierarchical access to the Internet. The assumed VANET architecture is depicted in Fig. 1. The network consists of three distinct domains: *in-vehicle*, *Ad-Hoc*, and *infra-structure domain*.

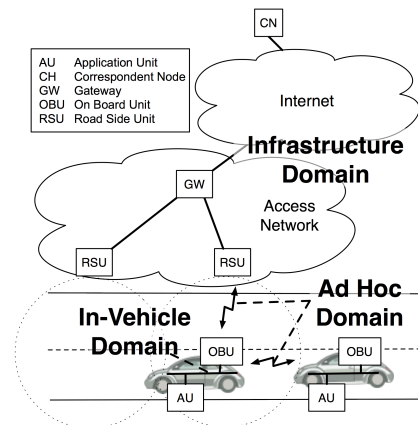


Fig. 1. High-Level Architecture View

The *in-vehicle domain* is a network composed of an *on-board unit* (OBU) and *application units* (AU). AUs are typically portable devices such as laptops, PDAs, game pads or any type of handheld device attached to an OBU and can be

connected by either wired or wireless connection to the on-board unit. It is assumed that application units do not connect directly to the Ad-Hoc domain, but rather through an OBU.

The *Ad-Hoc domain* is composed of vehicles equipped with OBUs and stationary units along the road, termed *road-side units* (RSU). RSUs are responsible for interconnection between the Ad-Hoc and the infrastructure domain. The units (OBUs and RSUs) can directly communicate if direct wireless connectivity exists. In case of no direct connectivity, multi-hop communication is used, where data is forwarded from one OBU to another, potentially via road-side units, until it reaches its destination. Road-side units allow on-board units to access the infrastructure domain. This allows application units registered with an OBU to communicate with *correspondent nodes* in the Internet, when at least one RSU is available.

The infrastructure domain is clearly divided into *access networks* and the *Internet*. The access networks are composed by a gateway which provides communication with Internet with several down link interfaces that connect to one or more RSUs. The previously mentioned domains lead to three distinct communication modes:

- **Direct in-vehicle (DIV)** AUs in the same vehicle communicate with each other using the in-vehicle network.
- **Vehicle-to-vehicle (V2V)** AUs in different vehicles communicate with each other using OBU to OBU communication potentially including RSUs. The data packets are routed inside the ad hoc domain without using the infrastructure domain.
- **Vehicle-to-roadside (V2R)** In this mode of communication the infrastructure is used. Communication peers can be CNs in the Internet or other AUs not accessible via V2V communication.

For further information on the integration of VANETs with position based routing and connectivity management and integration, please refer to [10].

III. PROXY USAGE IN A VEHICULAR ENVIRONMENT

As seen in Section II the architecture comprises three different domains, each with its own set of features. This causes a strong need for integration, since these domains should cooperate to provide a seamless connectivity environment. The VANET environment is assumed to be very mobile, and it is fair to assume that in many occasions infrastructure access will not be possible. Since the integration between domains is closely coupled to MIPv6, when there is no accessible RSU, there is no usable Home Agent (HA), and therefore communication through a Home Address is not possible. But this can be accomplished by introducing a MIPv6 proxy. When using a proxy, it is possible to enable communication between AUs using their Home Address even when there is no connection to the infrastructure. This can happen on two separate situations:

- **Using DIV Communication:** In this case the communication is established between AUs in the same vehicle. Data should be routed without resorting to Home Agents

or going outside of the DIV network. This must be transparent to the AUs and can be done knowing all the AUs in the DIV network and their respective HoA.

- **Using V2V Communication:** In V2V, the communication is established between AUs in nearby vehicles. Just like in DIV communication, all data can be routed without usage of the infrastructure, i.e. it's possible to relay the data packets through the ad-hoc domain. In this case, a vehicle should have means of querying nearby vehicles for the location of the required destination address on their DIV network. Again, this kind of operation is supposed to be transparent to the MIPv6 instance in the AU, and the proxy element should know which HoA are currently on its DIV network.

Supporting HoA to HoA communication is only possible if an isolated in-vehicle network is used alongside the support for surrogate AU registration. Both of these items are discussed in the design options (Sections III-A and III-B).

Using a mobile fixed network is becoming an increasingly common scenario, where nodes connect to an infra-structured network that in fact is connected to a MANET. This is the case of the DIV network, provided by the OBU. The DIV is supported by vehicles, i.e. cars, which is where the OBU resides. Vehicles are assumed to have no power limitations. Furthermore, the nodes connecting to the DIV network usually share a common profile: they have low power and low battery capabilities. The two before mentioned facts lead to the idea that an enhanced environment should be provided, integrating specific nature of both elements. For this we consider that a paging solution should exist (discussed in Section III-C).

The presented issues lead to introducing a new network element. The new element should solve the identified problems, taking advantage of the environment's special conditions. We introduce a Mobile IPv6 Proxy (MIPP), co-located with the on-board unit, that enables mobility support for the AUs in the vehicles. There are several factors that need to be analysed due to the introduction of a new element that will influence the outcome of the MIPP. We perform a deeper analysis of the different kinds of approaches that are relevant for the MIPP design and their impact on the end functionality provided:

A. In-Vehicle Network Isolation

One possibility is to consider the in-vehicle network an independent IP network from the PBRV domain. The usage of an isolated in-vehicle network implies that the MIPP acts as the access router for that network. In this case the MIPv6 Proxy is responsible for the routing to/from the in-vehicle network. Also, with this option it is easier to provide security if we introduce in the MIPv6 Proxy filtering and location privacy mechanisms. If the in-vehicle network does not represent an independent IP network, the MIPP acts as a bridge between the two physical networks. So in this case, it is much more difficult to provide enhancing mechanisms, such as location privacy and security, because the proxy operates at the lower level.

B. Support for Surrogate AU Registration

Another issue is to decide which identity executes the signalling: the AU or the MIPP. The design choice of using the MIPv6 instance in the AU trigger all MIPv6 signalling messages means that MIPv6 only has to change the AU IP address to the MIPP CoA and forward the packet. No state of AU registration is maintained in the MIPP, simplifying software complexity. This means that every signalling message received in the MIPP is forwarded to the application unit or the Home Agent, depending on the sender.

If we support surrogate AU registration, the MIPv6 signalling on behalf of the AU would be generated in the MIPP. First the AU registers with the MIPP using Normal Binding Update Messages. The MIPP then registers an AU, creating an internal state, and sends a Binding Acknowledgement message on behalf of the Home Agent to an AU. The AU now believes it is attached to network and correctly bound in the Home Agent, even when it is possible that this is not truth. There is not always connection between the RSU and an OBU so using PBRV information the MIPP is able to provide more efficient signalling. It is important to notice, that due to the AU registration internal state in the MIPP, the signalling between the AU and MIPP is completely independent from the signalling between the MIPP and the Home Agent.

C. Paging Scenarios

Due to the nature of the moving network (sustained by a car with no power limitations) a paging scenario would be very useful. This must be considered when introducing a new network element, because it allows MNs that have no ongoing communications to enter a dormant state. If the MIPP can allow this behaviour, then the usage of the car capabilities are being maximised.

IV. MIPV6 PROXY SOLUTIONS

Having the options referred in Sect. III in mind, there can be two different approaches to the MIPP design, which may have different implications:

- **Lightweight Approach** The main idea behind this approach, is to keep it as simple as possible, but still providing to the AUs the basic mobility scenarios. This design is most likely stateless.
- **Heavyweight Approach** It is possible to enhance the MIPP with a more complex design allowing the MIPP to not only providing the basic mobility scenarios to AUs, but also extra functionality (discussed in IV-B). This obviously implies a stateful approach.

A. Lightweight Proxy

In this approach we consider the In-Vehicle Network a different network from the Access Network. This change makes the MIPP the entity that detects movement and because of that, the entity responsible for triggering the AU to register in the HA. This can done through MIPP controlled Router Advertisements from which the AU retrieves its IPv6 address and detects handovers. It is important to notice that all the mobility

related signalling messages are automatically forwarded from the AU to the Home Agent and vice versa as they succeed, but with one slight modification: the Care-of Address registered in the HA is the one that the MIPP acquires and not the one from the AU. So the MIPP has only to process all the packets to and from the AU and change the IPv6 address of AU to the MIPP Care-of Address, and vice versa, without creating any internal state regarding AUs in vehicle.

B. Heavyweight Proxy

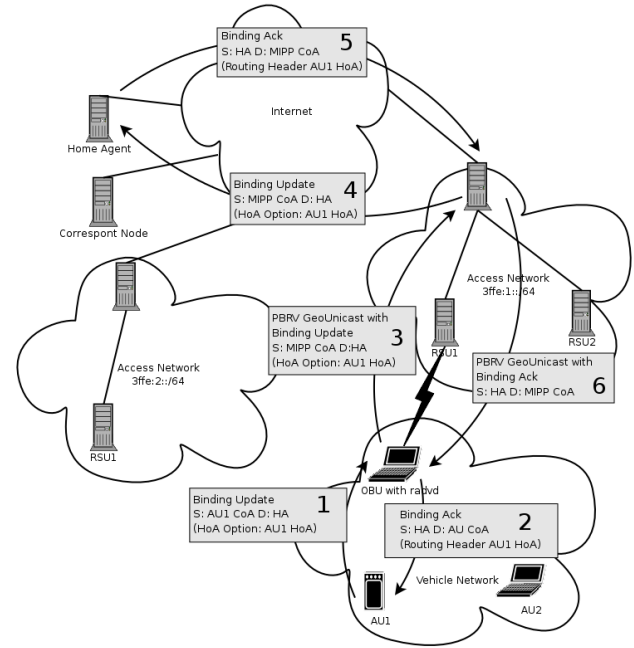


Fig. 2. Heavyweight MIPv6 Proxy solution

This solution is similar to the previous one, but it implements an independent state of registration between AU-MIPP and MIPP-HA. Since the MIPP the entity responsible for movement detection, we try to put all mobility management in the MIPP, by means of a stateful proxy design.

Basically, when a AU powers up or attaches to an OBU it sends a initial Binding Update. This message is automatically processed and replied by the MIPP on behalf of the the Home Agent. By doing this, the MIPP makes the AU believe that it is connected to the infra-structured network and consequently to its home agent. The MIPP is the entity responsible for dealing with lack of connection to the infrastructure. This registration, called AU Registration, is soft state and reuses normal MIPv6 operation messages. While an AU is registered in an OBU, the MIPP is responsible to perform all mobility signalling on behalf of the AU. This means that when the MIPP detects movement (i.e. when it acquires a new Care-of Address) it is required to send a Binding Update to the Home Agent and handle the response, and also for updating the binding for each application unit. This means the MIPP needs to perform all mobility operations a MIPv6 mobile node performs, but for all the AUs.

C. Solution Comparison

In terms of functionality, the lightweight solution provides basic MIPv6 support with no AU registration, which puts aside support for AU communication using Home Addresses with V2V communication only. The main advantage of this solution is its simplicity, although at the cost of flexibility. On the other hand, the heavyweight solution keeps track of the AUs registered. If the MIPP is capable of resolving the Home Address of a registered AU to which it is trying to connect, then we are able to provide the right environment for implementing AU communication using Home Addresses without infrastructure access.

TABLE I
MESSAGE COUNT FOR AN AU WITH BOTH PROXY APPROACHES.

	Message Count
Lightweight Approach	$2 * (1 + N_{handovers})$
Heavyweight Approach	2

In terms of message overhead, the heavyweight proxy also reveals better performance. As we can see from table I, with a lightweight proxy the message requirements for the AU grows at a linear rate with both node and handover number. With a heavyweight proxy, the message requirements for the AU are always fixed, since the only required step for an AU is the registration procedure with the proxy.

The number of processed messages (sent and received) in the AU is explained by the initial two message registration (Binding Update and Binding Acknowledgement) plus the two message (same as in registration) update for each handover.

With a heavyweight proxy, the message counts drops to two per node because all procedures are handled by the proxy. This means the heavyweight approach causes less signalling overhead in the In-Vehicle Network. If the registration lifetime with the MIPP is increased, the signalling overhead is even more reduced.

In the same line with the aforementioned, the heavyweight proxy allows paging scenarios with no extra cost for two reasons: 1) the mobile nodes are always reachable with no messaging from them. 2) They do not perform messaging besides the initial registration, allowing them to enter sleep mode while not in usage. These features are not available with a lightweight proxy.

V. CONCLUSIONS

The introduction of a MIPv6 Proxy poses several advantages, specially if we consider a heavyweight proxy scenario. By introducing a new element, we introduce an in-vehicle network, and potentially better ways of handling mobility while moving signalling load from the mobile nodes to the introduced MIPP. But, considering the benefits of introducing a heavyweight versus a lightweight proxy, we conclude that it is better to follow the heavyweight approach since the car can support it at no additional cost. With the heavyweight

proxy, application units are only required to do a one time registration, reducing the total number of messages exchange and also allowing nodes to enter sleep mode. This behaviour is particularly useful if we consider that all environments of VANET scenarios are highly mobile, i.e. we can expect a car moving along a high way to be performing handovers between road-side units every 2 km, which would give at least a handover every minute, forcing application units to update their current position. Also, if a lightweight proxy was to be used, the advantages of having a car (which as exceptionally good power capabilities), that harbours a network, would not be fully exploited, since for instance Home Address to Home Address communication would not be available.

Ongoing research is directed at including two important scenarios in the proxy operation: First, introduce IPSec communication while still enabling the MIPP to perform readdressing without breaking IPSec consistency, and in a secure way. Second, introduce Route Optimization, supported by normal MIPv6 operation. This means that it is the MIPP that performs route optimization with correspondent nodes.

Concluding, the introduction of a network element is useful, considering that the on-board unit (located within a car) has no limitations in terms of power consumption. Certain requirements are then moved from the mobile nodes to the MIPP (co-located with the on-board unit), that presents no disadvantages on handling these requirements and presents several advantages over its lightweight counterpart.

VI. ACKNOWLEDGMENTS

The authors acknowledge the support of German Ministry of Education and Research (BMB+F) for 'Network on Wheels' project under contract number 01AK064F.

REFERENCES

- [1] S. Tsugawa, Inter-Vehicle Communications and Their Applications to Intelligent Vehicles: An Overview, In *Proc. of IEEE Intelligent Vehicle Symposium*, vol. 2, pages 564-69, 2002.
- [2] B. N. Karp and H. T. Kung. GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. In *Proc. of MobiCom '2000*, pages 243-254, Aug. 2000.
- [3] M. Mauve, J. Widmer, and H. Hartenstein. A Survey on Position-Based Routing in Mobile Ad Hoc Networks. *IEEE Network*, 15(6):30-39, Nov./Dec. 2001.
- [4] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. Internet RFC 3775, June 2004.
- [5] V. Devarapalli, R. Wakikawa, A. Petrescu and P. Thubert. Network Mobility (NEMO) Basic Support Protocol. Internet RFC 3963, January 2005.
- [6] M. Corson, J. Macker, and G. Cirincione. Internet-Based Mobile Ad Hoc Networking. *IEEE Internet Computing*, 3(4):63-70, Aug. 1999.
- [7] U. Jönsson, F. Alriksson, D. Johnson, and G. Maguire. MIPMANET: Mobile IP for Mobile Ad Hoc Networks. In *Proc. of 1st ACM International Symposium on Mobile AdHoc Networks & Computing (MobiHoc)*, pages 75-85, 2000.
- [8] H. Lei and C. Perkins. Ad Hoc Networking with Mobile IP. In *Proc. of 2nd European Personal Mobile Conference (EPMCC)*, pages 197-202, Sept. 1997.
- [9] P. Rantachandani and R. Kravets. A Hybrid Approach for Internet Connectivity for Mobile Ad Hoc Networks. In *Proc. of Wireless Communication and Networking Conference (WCNC 2003)*, March 2003.
- [10] A. Matos, J. Santos, A. Festag, R. Aguiar and R. Baldessari. Flexible Connectivity Management in Vehicular AdHoc Networks In *Proceedings of 3rd International Workshop on Intelligent Transportation (WIT)*, pages 211-216, March 2006.