Design and Performance evaluation of a PMIPv6 solution for geonetworking-based VANETs

Victor Sandonis[a], Maria Calderon[a], Ignacio Soto[b], Carlos J. Bernardos[a]

[a]*Departamento de Ingeniería Telemática, Universidad Carlos III de Madrid, 28911 Leganés, Spain*
[b]*Departamento de Ingeniería de Sistemas Telemáticos, Universidad Politécnica de Madrid, 28040 Madrid, Spain*

Abstract

Vehicular Ad hoc NETworks (VANETs) are considered as the most suitable technology to provide vehicles with communication capabilities as a mean to improve road safety. Additionally, VANETs also open the market to non-safety applications where Internet connectivity is the main focus. Internet access from VANETs can be provided with the support of gateways located at the side of the roads, such that vehicles change their point of attachment to the Internet maintaining ongoing communications while they move. In this paper we tackle the problem of providing Internet access from VANETs combining the Proxy Mobile IPv6 (PMIPv6) with the ETSI TC ITS GeoNetworking (GN) protocols. We study how to adapt PMIPv6 to the multi-hop ETSI TC ITS architecture. A key contribution of this work is the design and analysis of different mechanisms that can be applied to the solution to improve the overall performance. A detailed performance evaluation of the solution and the different mechanisms assessing their influence is conducted by means of simulation under real traffic traces of an important orbital highway of Madrid.

Keywords: VANET, ETSI ITS, geonetworking, PMIPv6

1. Introduction

In recent years, significant attention has been paid to Vehicular Ad hoc NETworks (VANETs) because they are considered as the most suitable technology to provide vehicles with communication capabilities as a mean to improve road safety. Applications that inform drivers about road hazards (e.g., the sudden breaking of

Email addresses: vsandoni@it.uc3m.es (Victor Sandonis), maria@it.uc3m.es (Maria Calderon), isoto@dit.upm.es (Ignacio Soto), cjbc@it.uc3m.es (Carlos J. Bernardos)

the vehicle ahead) could be deployed in order to avoid traffic accidents and decrease road casualties. In addition to improving road safety, VANETs can also open the market to non-safety applications where Internet access has become the main focus. This is so because, on the one hand, drivers could use common Internet services and, on the other hand, it makes possible the appearance of new Internet applications oriented to drivers.

A VANET is a type of ad hoc network, formed by vehicles that can communicate among them through wireless interfaces in a decentralized way, i.e., with no infrastructure support. Nodes can communicate with other nodes out of its direct coverage range through a multi-hop path between source and destination. A key distinct characteristic of VANETs – when compared to other flavors of ad-hoc networks, is their high level of node mobility (due to vehicles' speed) causing links among nodes to break down continuously. Nodes' mobility pattern is typically restricted as vehicles move on roads with a given topology. Additionally, VANET nodes may have large memory and processing capabilities. These important properties have to be taken into account when designing protocols for VANETs.

The European Telecommunications Standards Institute Technical Committee Intelligent Transport System (ETSI TC ITS) [1] is the technical committee that is in charge of standardizing the architecture and the communication protocols for an intelligent transport system. The ETSI TC ITS takes into consideration input from automobile manufactures and industry recommendations, such as those proposed by the Car to Car Communications Consortium (C2C-CC) [2]. The ETSI TC ITS system architecture [3] is based on the use of a geographic based routing protocol: the GeoNetworking protocol (GN) [4]. Geographic based routing protocols assume that every node can obtain its geographical location using a location service mechanism such as Global Positioning System (GPS). Packets are forwarded through the network following the direction where the destination node is located, sending the packets via the neighboring node that is the closest to the destination.

In order to provide Internet connectivity to vehicles of the VANET, gateways connected to the fixed infrastructure are placed at the side of the roads. Therefore, vehicles have to be able to change their point of attachment to the Internet while maintaining ongoing communications. In the ETSI TC ITS specification for Internet Integration [5], mobility support is addressed by means of the Network Mobility Basic Support (NEMO BS) protocol [6] by default, but other mobility support approaches can be applied such as Proxy Mobile IPv6 (PMIPv6) [7].

In this article, we tackle the problem of providing Internet access from VANETs combining PMIPv6 with the ETSI TC ITS architecture [3] and its GeoNetworking protocol (GN) [4]. The main motivation for adopting PMIPv6 to provide mobility support in the VANET is that it allows efficient handovers in a local domain.

PMIPv6 is a Network-based Localized Mobility Management (NetLMM) solution where all the functionalities regarding to IP mobility support reside in the network side. The NetLMM approach has been promoted by network operators because it offers them more control to manage mobility in their networks. Mobility support is provided without Mobile Node (MN) intervention at the IP layer, avoiding the need for special software and/or complex configurations in the MN, whereas other mobility approaches (e.g., MIPv6) require in the MN mobility specific security configuration and signaling. Additionally, due to the progressive adoption of PMIPv6 as mobility support approach by network operators, this brings the opportunity of integrating the mobility solution selected for VANETs with the one existing in other regions of their network (e.g., with other access technologies, for instance 3G) where they provide mobility support also by means of PMIPv6. In this way, vehicles could access the Internet through different technologies without changing their IP addresses, so they would not be restricted to move inside the VANET domain to maintain their ongoing sessions.

However, PMIPv6 is designed for single-hop scenarios, so it has to be adapted to a multi-hop environment to integrate it with the ETSI TC ITS architecture. In this paper we propose a set of procedures to integrate PMIPv6 with the ETSI TC ITS architecture. We also identify several mechanisms that can be applied to the ETSI TC ITS GeoNetworking specification [4] and analyze their behavior when used within the integrated PMIPv6 and ETSI TC ITS architecture. Some of these mechanisms are already proposed in the ETSI specification while others are new. Finally, we provide a thorough simulation analysis of the performance of the integration of PMIPv6 with the ETSI TC ITS architecture using the different mechanisms to optimize the Internet access from vehicles. In the simulation analysis we have used real traffic traces of an important orbital highway of Madrid.

The rest of the paper is organized as follows. In Section 2, related work is reviewed. Section 3 briefly describes the ETSI TC ITS architecture and PMIPv6. In the following section, we present the solution to integrate PMIPv6 with the ETSI TC ITS, presenting also some mechanisms for improving the performance of the solution. In Section 5 the simulation scenario is described. Section 6 analyzes the feasibility of the solution evaluating the influence of the described mechanisms on the performance. Section 7 concludes the paper and presents our future workplan.

2. Related Work

The problem of connecting a mobile ad-hoc network (MANET) to the Internet has been extensively researched in recent years [8]. However, existing MANET solutions cannot be directly applied to VANETs because of their special characteristics, particularly the high speed of vehicles. We next briefly introduce existing solutions for providing Internet connectivity to vehicles.

An experimental study about the performance of radio connectivity provided by residential Wi-Fi access points to vehicles is presented in [9]. Authors describe the results of several experiments where a few cars driving on metropolitan areas, collect information about the connectivity between cars and home Wi-Fi hot-spots. Although the presented results are limited to single-hop connection between cars and Wi-Fi hot-spots, they show the feasibility of developing VANET applications.

Authors of [10] present an architecture for WLAN-based Internet connectivity from vehicles. The proposal focuses on single-hop connectivity between vehicles and WLAN hot-spots located along the road. The problem of intermittent connectivity and mobility is managed at application layer introducing two entities: Drive-Thru client and Drive-thru proxy. These entities interact to keep connections during disconnection periods between hot-spots by means of the Persistent Connection Management Protocol. The main drawback of the proposal is that it is limited to single-hop connectivity between vehicles and WLAN hot-spots.

In [11], authors consider the multi-hop Vehicle-to-Infrastructure scenario, enabling seamless connectivity to the infrastructure network while vehicles perform handovers between roadside access points maintaining their IP addresses. Routing and mobility support is handled at layer-2 by means of an enhanced version of the BATMAN protocol [12]. However, managing mobility at layer-2 poses the drawback of potential scalability problems due to the high number of vehicles a VANET is usually comprised of. Besides, authors assume that roadside access points operate at different frequency channels and vehicles are equipped with two radio interfaces. This would introduce more complexity allocating frequency channels in real deployments. On the other hand, the experimental evaluation is limited to urban scenarios where vehicles move at low speed.

An efficient way of supporting IPv6 over VANETs with geographic routing based on the C2C-CC [2] system architecture is proposed in [13]. Using standard unmodified Neighbor Discovery and Stateless Address Autoconfiguration protocols [14, 15] in a VANET is challenging because these protocols assume the existence of a multicast capable layer below IP. The authors solve this problem by defining C2C and virtual point-to-point links and making the IPv6 layer aware of C2C location management information. In this way, the Neighbor Discovery protocol does not depend on link-local multicast messages at the expense of introducing modifications to the IPv6 protocol that can cause interoperability problems with standard IPv6 protocol implementations. Additionally, the solution does not deal with IP mobility support.

One of the few research works that addresses the challenges and solutions of IP mobility management for vehicular networks can be found in [16]. Authors analyze the requirements of IP mobility mechanisms when applied to the vehicular scenario due to its special features. Although PMIPv6 [7] is mentioned as a possible approach for roaming between heterogeneous access networks, authors mainly focus on a comparison among different existing optimization solutions for Network Mobility Basic Support protocol (NEMO BS) in vehicular scenarios.

In [17], authors propose a MANET-centric solution to integrate NEMO BS and geographic routing in VANETs taking as reference the C2C-CC system architecture. A geonetworking-based sub-IP layer hides the multi-hop nature of VANETs to IPv6, avoiding the need for changes to standard IPv6. This way, NEMO mobile routers are connected to the Internet via a multi-hop path. The proposal is validated by means of laboratory tests. Our proposal is however focused on the integration of a network-based mobility management protocol (i.e., PMIPv6) in VANETs, instead of a client-based global mobility approach like the NEMO BS.

A global mobility management solution combining Host Identity Protocol (HIP) and PMIPv6 to provide seamless connectivity to the Internet in urban vehicular scenarios is proposed in [18]. The solution allows legacy nodes (nodes without mobility support) and HIP-enabled nodes to perform handovers between Road Side Units (RSUs) of the same (intra-domain handover) or different PMIPv6 domains (inter-domain handover). However, the proposal requires correspondent nodes in the Internet to be HIP-enabled or to be behind a HIP proxy.

Authors in [19] propose a quality-driven routing scheme for video streaming in VANETs that minimizes packet loss. In order to provide mobility support, the routing scheme is integrated with an adaptation of PMIPv6 to multi-hop VANETs with a handover prediction mechanism. Their approach to adapt PMIPv6 to the multi-hop environment is similar to our proposal, however their solution uses the Neighbor Discovery mechanism and Neighbor Unreachability Detection [14] to predict handovers and this is costly in VANETs because produces signaling overhead. In our approach, we avoid the use of the Neighbor Discovery mechanism completely because the address resolution is done directly since the link layer address is part of the GN address according with the GN protocol specification [4]. Besides, we do not only study the integration of PMIPv6 with the ETSI TC ITS GeoNetworking protocol in multi-hop VANETs, but also propose and deeply analyze different mechanisms to improve the performance of the solution. To the best of our knowledge, there are no existing detailed studies on the performance evaluation of the integration of PMIPv6 and the ETSI TC GeoNetworking protocol to provide Internet connectivity from VANETs as the work presented in this article.

3. Background

3.1. ETSI TC ITS Architecture

The ETSI TC ITS is standardizing an architecture [3] for an intelligent transport system based on the C2C-CC recommendations. The ETSI TC ITS has adopted the Geographically Scoped stateless Address Configuration (GeoSAC) [20] mechanism for automatic IPv6 address configuration in its specification for transmission of IPv6 packets over GeoNetworking protocols [5].

In the ETSI TC ITS architecture, vehicle ITS stations are equipped with the Communication & Control Unit (CCU) and Application Units (AUs). The CCU executes the ETSI communication protocol stack and can be seen as the gateway (optionally with NEMO extensions) that provides communication capabilities to the AUs. The CCU has in-vehicle interfaces for communications with AUs and external short-range wireless interfaces for communications with other ITS stations of the vehicular ad hoc network. An AU is a device (e.g., a passenger smart phone) with a standard IPv6 protocol stack which is attached – via a wired or wireless technology – to the CCU, and that executes a set of applications which benefit from the connectivity provided by the CCU.

On the other hand, the ITS ad hoc network is also formed by roadside ITS stations or Road Side Units (RSUs) that are located at the side of the road and also execute the ETSI communication protocol stack. CCUs and RSUs form a VANET that allows decentralized inter-vehicle communications. Besides, RSUs can be connected to the infrastructure of a network operator, thus they not only increase network connectivity but provide Internet connectivity to vehicles of the VANET acting as access routers.

The ETSI TC ITS has adopted a geographic routing scheme to forward packets in its system architecture. The ETSI GeoNetworking protocol (GN) [4] is based on greedy forwarding and is situated between the link and the IPv6 layer of the communication protocol stack (see Figure 1(a)). Greedy forwarding is based on the assumption that all nodes know their own geographical position and the one of their direct neighbors (nodes that are one hop away). With that information, an intermediate node can forward packets to the closest neighbor to the geographic position of the destination. In this way, packets travel from source to destination through a multi-hop path. In order for the nodes to know neighbors' position, each node periodically broadcasts beacon messages including its identifier, actual position, heading, speed, etc. Thereby, nodes store a location table with information about neighbors' position and final destination's position. The location of the destination is obtained by means of a location service.

The GN protocol defines two kinds of packet deliveries: geo-unicast and geo-broadcast. In geo-unicast, the packet is forwarded hop by hop following greedy forwarding and delivered to a specific destination node located in a particular position. In geo-broadcast, the packet is geo-routed to a target geographic area, and then delivered to all nodes located inside the destination area by simple flooding.

The ETSI TC ITS specification for transmission of IPv6 packets over GeoNetworking protocols [5] relies on GeoSAC [20] mechanism for automatic IPv6 address configuration. GeoSAC adapts the IPv6 SLAAC [14, 15] mechanisms to geographic addressing and networking defining a new concept of multicast link. From the point of view of IPv6, the GN layer plays the role of sub-IP layer. The GN layer receives IPv6 datagrams from the IPv6 layer, encapsulates them into a GN packet adding the GN header and routes them as mentioned above. Thereby, the GN layer offers to the IPv6 layer a flat network topology. This means that two IPv6 neighbors can be separated more than one GN hop away from each other, but the GN layer makes this transparent so they are in the same link from the point of view of the IPv6 layer. In Figure 1(a), vehicle A and the RSU are neighbors at the IPv6 level, but actually the GN layer of vehicle B acts as a forwarder and establishes a multi-hop path between them. Following this approach a new concept of multicast link is defined as the restricted geographical zone where the GN protocol distributes packets to all nodes inside it using geo-broadcast delivery. This allows to define multicast links as non-overlapping geographic areas. All the nodes inside an area belong to the same IPv6 link, including an RSU in charge of the area.

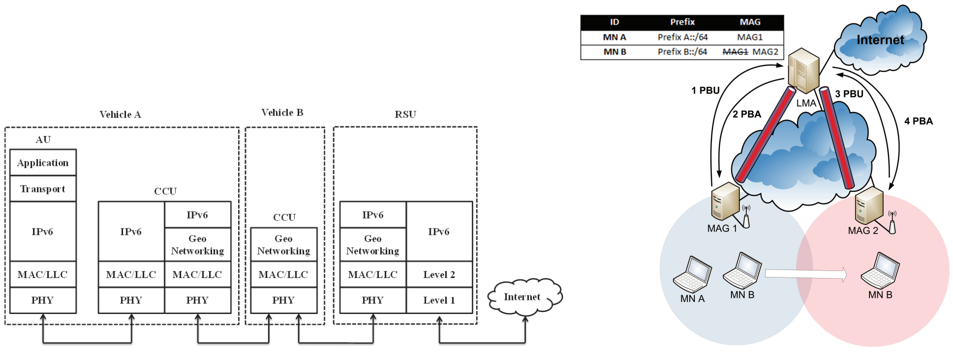
As mentioned above, an RSU can be connected to the infrastructure of a network operator, acting as access router for nodes located inside its influence region. These RSUs issue Router Advertisements (RAs) that are delivered by the GN layer to all nodes situated inside its geographic area using geo-broadcasting.

Routing of packets in the VANET is performed as follows (see Figure 2). Suppose that an AU of vehicle G wants to send a packet to a node in the Internet. Since RSU 2 is the access router for the IPv6 layer of vehicle G and they are attached to the same IPv6 link (although they are not directly connected, i.e. vehicle G is out of the radio coverage of RSU 2), vehicle G uses RSU 2 as the IPv6 next-hop to route the packet towards the Internet. Thus, for the packet to reach RSU 2, the GN layer of vehicle F acts as a forwarder between vehicle G and RSU 2. Once the packet gets to RSU 2, it is sent to the Internet. But, if vehicle G wants to send a packet to a vehicle of the same geographic area, for example vehicle E, the packet is not routed to RSU 2, because vehicles G and E are in the same IPv6 link (i.e., vehicle E is the IPv6 next-hop) and the GN protocol routes packets between them.

Note that vehicles' CCU can learn the geographical area they belong to and the geographic position of the RSU while they move along different zones because the RAs issued by the RSUs include these parameters in the GN header.

3.2. Proxy Mobile IPv6

A new trend has recently appeared in IP mobility that proposes to support mobility of nodes within a local domain without the intervention of mobile nodes. That is, all functionalities regarding to IP mobility support reside in the network side. This approach is called Network-based Localized Mobility Management (NetLMM). Proxy Mobile IPv6 (PMIPv6) [7] follows this idea.



(a) IPv6 over GeoNetworking.

(b) Operation of PMIPv6.

Figure 1: IPv6 over GeoNetworking and operation of PMIPv6.

PMIPv6 uses some of the concepts of Mobile IPv6 (MIPv6) [21], but relocating the mobility management functionality of the Mobile Node (MN) to network nodes. The main advantage that provides PMIPv6 is that an MN can move inside a localized area called Localized Mobility Domain (LMD) where handovers are more efficient, maintaining its IP address without participating in any IP layer mobility signaling. An MN can move inside the LMD without changing its IP address and without the necessity of informing about its location because the network tracks MNs' movement without their involvement. To achieve this functionality, PMIPv6 introduces new entities and reuses some of the concepts of MIPv6:

Mobile Node: it is a moving IPv6 node that can communicate through (most likely wireless) network interfaces. In PMIPv6, the MN is not involved in any IP mobility signaling.

Mobile Access Gateway (MAG): it is a network entity that is responsible for mobility management on behalf of MNs connected to its access links and is in charge of maintaining the localization of an MN inside the LMD. Besides, the MAG is usually the access router of these MNs.

Local Mobility Anchor (LMA): it is a local version of the Home Agent (HA) of MIPv6 with some extended functionalities. The LMA is the anchor point of the prefixes assigned to MNs in the LMD. Thus, all packets originated in the Internet and addressed to prefixes belonging to the PMIPv6 domain will be routed to the LMA. Besides, the LMA keeps routes to all MNs by means of tunnels between the LMA and the MAGs where the MNs are attached to.

Next, we briefly explain how PMIPv6 works. When an MN appears in the LMD, it attaches to a MAG. The MAG, after checking if the MN is authorized to use the mobility service, sends a Proxy Binding Update message (PBU) to the

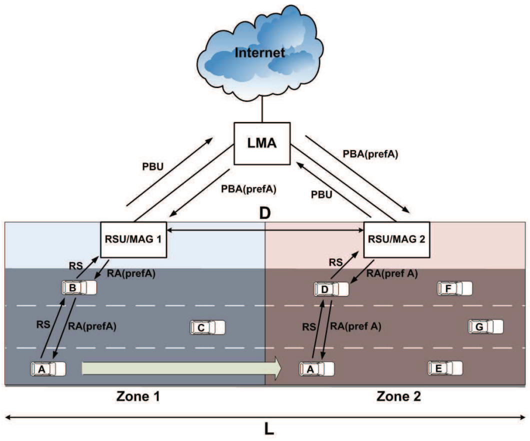


Figure 2: PMIPv6 in VANETs.

LMA to report that the MN is under its influence. Upon reception of the PBU, the LMA allocates a prefix to the MN and sends a Proxy Binding Acknowledgment (PBA) to the MAG carrying the allocated prefix. Then, the MAG sends Router Advertisement (RA) packets to the MN, so the MN can configure an IPv6 address using the prefix allocated by the LMA (e.g., using stateless autoconfiguration mechanism). In this process, a bidirectional tunnel is established between the LMA and the MAG where the MN is attached to.

While moving inside the LMD, the MN can disconnect from an old MAG and connect to a new MAG. PBU/PBA signaling is used to keep updated the tunnel between the LMA and the MAG providing service to the MN. Besides, to make the IP mobility transparent to the MN, the new MAG sends RAs to the MN advertising the same prefix which was allocated by the LMA. Thus, the MN can maintain its IP address while changing its point of attachment between MAGs. Hence, the LMD is a single link from MNs point of view. This is called the home network emulation. Figure 1(b) shows all this process in a schematic view.

Traffic is routed as follows. Packets from the Internet directed to the MN are received by the LMA and forwarded to the MAG where the MN is attached to through the bidirectional tunnel. Finally, the MAG delivers the packets to the MN. When the MN is the source of the traffic, packets are routed to the MAG and then to the LMA through the bidirectional tunnel. After that, the LMA forwards packets to the destination.

4. PMIPv6 in vehicular scenarios

4.1. Integration of PMIPv6 with the ETSI TC ITS architecture

In this section we describe a solution to provide Internet access from VANETs combining PMIPv6 [7] with the ETSI TC ITS architecture [3] and its GeoNetworking protocol (GN) [4]. PMIPv6 allows vehicles to perform efficient handovers between RSUs if the LMA is placed close to the RSUs. As compared to client-based mobility approaches (like Mobile IP), with PMIPv6 vehicles do not need to have complex security configurations, as the IP mobility signaling is performed by the network. Last but not least, if the network operator had PMIPv6 deployed in other parts of its network (with other access technologies like 3G), the solution allows for inter-access mobility using PMIPv6. This enables vehicles to get Internet connectivity and keep their IP addresses while moving across different technologies (i.e., not being limited to mobility within the VANET). These three aspects (efficient handovers, no complex mobility related security configuration required in the MN, and integration with the operator's mobility management allowing inter-access mobility) justify our choice of PMIPv6 as mobility protocol.

PMIPv6 is designed to single-hop scenarios where the MN is directly connected to the MAG. Thus, PMIPv6 has to be adapted to a multi-hop environment in order to integrate it with the ETSI TC ITS architecture. The basic operation of the proposed solution is shown in Figure 2. RSUs play the role of MAGs in PMIPv6 and are located at the side of the road in order to extend the coverage range of the VANET and to provide Internet connectivity to vehicles. Since RSU/MAGs act as access routers, they periodically geo-broadcast RA messages within their managed geographic area. These RAs are the only messages that are broadcast in the VANET, being delivered to all vehicles inside the RSU/MAG's geographic area. The RA messages include information about the geographical position of the RSU/MAG and its associated geographic area. This enables vehicles to detect when they change of geographic area and learn the position of the new RSU/MAG.

We take the scenario depicted in Figure 2 to explain the adaptation of PMIPv6 to multi-hop VANETs. When vehicle A gets connected to the VANET, it learns the geographic position of the RSU/MAG 1 and its associated geographic area from a received geo-broadcast RA. In order to let the RSU/MAG 1 detect the arrival of vehicle A to the zone, vehicle A sends a geo-unicast Router Solicitation (RS) to the RSU/MAG 1. Note that this is possible because RAs include RSU/MAG 1 geographic position. Then, the RS packet is routed by the GN protocol towards RSU/MAG 1 through a multi-hop path. This way, RSU/MAG 1 becomes aware of vehicle A's arrival, which triggers sending a PBU message to the LMA to report the vehicle A presence. Upon reception of this PBU, the LMA allocates a prefix for vehicle A and sends a PBA message to RSU/MAG1 which carries the prefix allocated for vehicle A. After PBA processing, RSU/MAG 1 sends the prefix to the vehicle A by means of a RA message carried inside a geo-unicast packet which is delivered via a multi-hop path (note that RSU/MAG 1 obtains vehicle A position from the previous geo-unicast RS). Thus, vehicle A can configure a global IPv6 address using the prefix allocated by the LMA. Besides, a bidirectional tunnel is created between the LMA and the RSU/MAG 1. In order to assure the success of this procedure, vehicle A keeps transmitting geo-unicast RSs to the RSU/MAG 1 periodically until it receives the geo-unicast RA with the allocated prefix.

Once the mobility signaling is complete, routing of subsequent data packets is performed as follows. When a vehicle sends a data packet, it is sent to the RSU/MAG, which acts as the gateway of the geographic area. After that, the RSU/MAG forwards the data packet to the LMA through the bidirectional tunnel. Then, the LMA forwards the packet to the destination: if the destination is inside the LMD, the packet is tunneled again to the appropriate RSU/MAG; otherwise, the packet is routed to destination through the Internet. In the opposite direction, packets coming from the Internet get to the LMA, which then forwards them to the RSU/MAG where the destination vehicle is attached to, through the right tunnel. After that, the RSU/MAG routes the packets to the destination vehicle using the GN protocol.

Due to the mobility of vehicles in the VANET, they may change of geographic area. Handovers between RSU/MAGs are also illustrated in Figure 2. When vehicle A enters into area 2, it detects the area change because of the reception of a geo-broadcast RA from RSU/MAG 2. Then, vehicle A sends a geo-unicast RS to the RSU/MAG 2. Thereby, RSU/MAG 2 notices that vehicle A has entered into its geographic zone and sends a PBU message to the LMA to inform about the vehicle A arrival. Then, the LMA sends a PBA message with the prefix of vehicle A to RSU/MAG 2 and updates the bidirectional tunnel used to forward traffic to the vehicle A, which now is terminated by the RSU/MAG 2. Since RSU/MAG 2 sends the same prefix allocated by the LMA to vehicle A, it can maintain its IPv6 address despite the change of point of attachment.

4.2. Optimization mechanisms

The procedures presented above allow the integration of PMIPv6 with the ETSI TC ITS architecture and its GN protocol enabling Internet access from vehicles. Additionally, several mechanisms can be used within the GeoNetworking protocol to improve the resulting performance. Next we describe and analyze the use of several of those mechanisms. Some of the mechanisms have been proposed and are already described in the ETSI TC ITS GeoNetworking specification [4], while others are new proposals to optimize the performance when accessing Internet from vehicles using the proposed integration of PMIPv6 and the ETSI TC ITS architecture.

4.2.1. Mechanisms of the ETSI GeoNetworking protocol

Aggressive Independent Beacon Sending: In the ETSI GeoNetworking protocol [4], nodes periodically broadcast beacon messages including their identifier, current geographic position, heading direction, speed, etc. This beaconing algorithm causes additional network overhead (that depends on the beacon interval), but it is needed to maintain location tables updated for the appropriate operation of the GN protocol. With the goal of decreasing the network overhead produced by the beaconing algorithm, the ETSI GN specification [4] states that “a beacon packet shall be sent every beacon interval except another GN packet is sent”. In other words, the beacon timer is reset upon the transmission of any GN packet because it piggybacks beacon information inside the GN header.

A concern with this optimization mechanism is that when a node sends a geo-unicast packet, the packet is only received by the next-hop node and this neighbor is the only one that processes the GN header information, so other neighbor nodes do not process the GN header and miss the updated location information. Therefore, we modify the mechanism so that vehicles send beacons independently of the transmission of other GN packets (aggressive independent beacon sending).

Geo-broadcasting delay: In the ETSI GN protocol [4], geo-broadcasting is managed by means of the *Simple GeoBroadcast forwarding algorithm with line forwarding*. So, a geo-broadcast packet is directed to the target geographic area following greedy forwarding until it reaches the target zone. Once the packet reaches the target region, it is delivered to all nodes located inside the destination area by means of simple flooding. However, when the density of vehicles in the VANET is quite high, simple flooding can generate collisions at the Media Access Control (MAC) layer. In our proposal, RAs are sent using geo-broadcast in the RSU area, but this can generate collisions because upon reception of the geo-broadcast RA packet, vehicles within RSU/MAG’s radio coverage try to re-transmit the RA packet at the same time. In order to avoid this behavior, we propose to introduce a geo-broadcasting delay mechanism such that vehicles wait for a random interval before re-transmitting a geo-broadcast packet by means of simple flooding.

GeoNetworking Buffering: The ETSI GN protocol [4] keeps packets in a forwarding packet buffer when the greedy forwarding algorithm fails finding a valid neighbor as next hop. This GeoNetworking buffering avoids discarding packets, by storing them in a buffer until a valid next hop neighbor is found. The GeoNetworking buffering mechanism is useful when there are not reachable neighbors closer to the final destination due to disconnections among zones of the VANET.

4.2.2. New optimization mechanisms

Cross-Layer Based Neighbor Loss Detection: Cross-layer optimizations have been shown to be useful in VANET protocol architectures (see for example [22]). This mechanism is such a cross-layer optimization. When nodes process beacons or GN packets, they store or update information about the identifier, actual position, heading, speed, etc. of the sender in their location table. This information is considered valid for a specific lifetime, therefore it is possible that a node routes a packet to a neighbor that is not reachable any more (because of the high mobility of VANET nodes) until its entry in the location table expires. We propose the following cross-layer based neighbor loss detection mechanism: when a packet is discarded at link layer because the next hop at the GN level is not reachable (after seven failed send attempts), the neighbor information is erased from the location table of the GN layer. In this way, packets are routed through other available neighbors avoiding packet losses.

Neighbor Position Prediction: Following the idea of avoiding to send packets to neighbors that became unreachable because of their movement, we propose to select the next hop for greedy forwarding taking into account a predicted position of neighbors instead of the position stored in the location table. The predicted position is calculated from the stored position, speed, heading and the interval of time between the actual moment and the time-stamp of location table entry (moment at which the position, speed and heading of the neighbor was acquired). Therefore, neighbors that are predicted to be outside of the radio coverage of the node are not selected as next hop.

Handover Detection & Bicasting: As mentioned above, authors of [19] have proposed a handover prediction scheme that relays on the Neighbor Discovery mechanism and Neighbor Unreachability Detection [14] that are costly in VANETs because produce signaling overhead. Note that according with the GN protocol specification [4] the link layer address is part of the GN address, thus address resolution is direct avoiding the use of the Neighbor Discovery mechanism.

We propose a handover detection scheme based on the analysis of the GN header of data packets instead of Neighbor Discovery messages. Since RSU/MAGs are the gateways of vehicles within their area, when a vehicle is communicating with a node in the Internet, the RSU/MAG receives data packets sent by the source vehicle. Thus, the RSU/MAG can extract from the GN header the actual position of the source vehicle. By doing so, the RSU/MAG can detect when the vehicle has changed of geographic zone. If the RSU/MAG detects that a vehicle has entered into a new geographic area, it informs the LMA about that. Then, the LMA starts bicasting data packets coming from the Internet and addressed to the concerned vehicle towards the RSU/MAG of the previous geographic zone and the RSU/MAG of the new area. Thereby, packet losses in the handover between two RSU/MAGs are avoided. The LMA finishes bicasting data packets when receives a PBU from the new RSU/MAG informing about the vehicle attachment.

5. Simulation scenario

In this section we report on the scenario used to conduct an experimental evaluation of the solution based on simulation. This experimental evaluation has two main goals: *i)* to validate the feasibility of the general solution, and, *ii)* to assess the performance impact of each of the different optimization mechanisms described before. With the aim of obtaining results close to real scenarios we run simulations using our own implementation of the ETSI TC ITS GeoNetworking protocol [4] and PMIPv6 [7], integrated with the INETMANET framework[1] for the OMNeT++ simulator[2]. The PMIPv6 implementation is based on xMIPv6[3]. Next we describe the simulation scenario that is depicted on Figure 2.

The simulation scenario is an L meters long highway stretch with three lanes. There are two RSU/MAGs separated by a distance of D (meters), each of them managing a geographic area of length D/2 meters (see Figure 2). Vehicles are generated in the simulation from real traffic traces of an important orbital highway of Madrid called M-40. These traces have been collected in the kilometer point 12.7 of the M-40 from 8:30 to 9:00 in the morning. The vehicular density is 54 veh/Km and the average speed is 95 Km/h. To obtain realistic driver's behavior during the simulation we use the SUMO traffic simulator[4]. Following this approach, vehicles enter in the highway stretch in a specific lane, time point and speed obtained from the real traces, move along the highway performing a handover between RSU/MAGs changing from geographic area 1 to geographic area 2, and finally, they exit the highway stretch. The maximum speed of vehicles is limited to 100 Km/h, which is the speed limit of the M-40. Vehicles and RSU/MAGs are equipped with IEEE 802.11g link layer operating at 54Mbps. The transmission power is configured to obtain a radio coverage of 200 meters.

RSU/MAGs periodically send RA messages using an inter-message interval uniformly distributed between $RA_{min} = 0.75$ seconds and $RA_{max} = 1.25$ seconds. When the geo-broadcasting delay optimization is enabled, vehicles wait for a ran-

[1] INETMANET Framework for OMNEST/OMNeT++ 4.x (based on INET Framework): https://github.com/inetmanet/inetmanet/wiki

[2] OMNeT++ Network Simulator Framework: http://www.omnetpp.org/

[3] Extensible Mobile IPv6 (xMIPv6) Simulation Model for OMNeT++: http://www.kn.e-technik.tu-dortmund.de/ obs/content/view/232/lang de/

[4] SUMO Simulation of Urban MObility: http://sumo.sourceforge.net/

dom interval between 0 and 50 milliseconds before re-transmitting a geo-broadcast packet. Vehicles may send up to 7 geo-unicast RS each separated by 0.75 seconds when they want to attach to an RSU/MAG.

Regarding the lifetime of the entries in the location table, we have experimentally realized that when the beaconing interval is too short (e.g., 0.5 seconds) and the location table lifetime is also short, the overall performance degrades. This degradation may be caused by collisions of beacon messages so that the location table information is not updated timely. Therefore, the location table lifetime has to be increased when the beacon interval is short to mitigate the problem caused by beacon losses. On the other hand, the use of long location table lifetimes also produces performance degradation because old entries in the location table can be considered as valid even though the neighbors might not be reachable. Based on this rationale, we have set up a lifetime value equal to 3 times the beaconing interval, with a minimum of 2.5 seconds.

In order to experimentally assess the performance of the solution and the impact of the different optimization mechanisms, the characteristics of the data traffic used in the experiments is very important. We have used in our simulation different scenarios in terms of traffic patterns. In one scenario, two independent UDP CBR flows are established between a vehicle in the VANET and a Correspondent Node (CN) in the Internet (Internet-VANET and VANET-Internet directions), with both sending a 20-byte data packet each 10 milliseconds. This traffic pattern (i.e., frequent small packets) allows to sample the behavior of the solution with accuracy. The vehicle is randomly selected once the highway stretch is populated with vehicles to recreate a real scenario where the vehicle has other vehicles ahead and behind of it. Since this traffic generation pattern does not model a realistic one in the Internet, we also consider a UDP traffic pattern of 512-byte packets sent each 30 milliseconds. Last but not least, we also consider the case in which not only one vehicle communicates with the CN, but a 10% of vehicles of the VANET do.

Two basic configurations of RSU/MAGs deployment have been considered: *i)* a highway stretch of L = 2000 m. with RSU/MAGs separated D = 1000 m., and *ii)* a highway stretch of L = 4000 m. with RSU/MAGs separated D = 2000 m.

Multiple simulations, varying the beaconing interval, have been run using the previous simulation scenarios. Each simulation is repeated 30 times using different seeds (95% confidence intervals are provided). These simulations have been used to obtain the following performance metrics:

Beacons per second that a vehicle sends. Note that this depends on the use of the beacon piggybacking strategy.

Packet delivery ratio measured from the moment a vehicle configures its IPv6 address until it exits the highway stretch.

Number of hops traversed by data packets transferred between the MAG and the vehicle.

Configuration time defined as the time that elapses from the moment a vehicle changes of geographic area (from area 1 to area 2) until it receives a geo-unicast RA message from the RSU/MAG with the prefix allocated by the LMA.

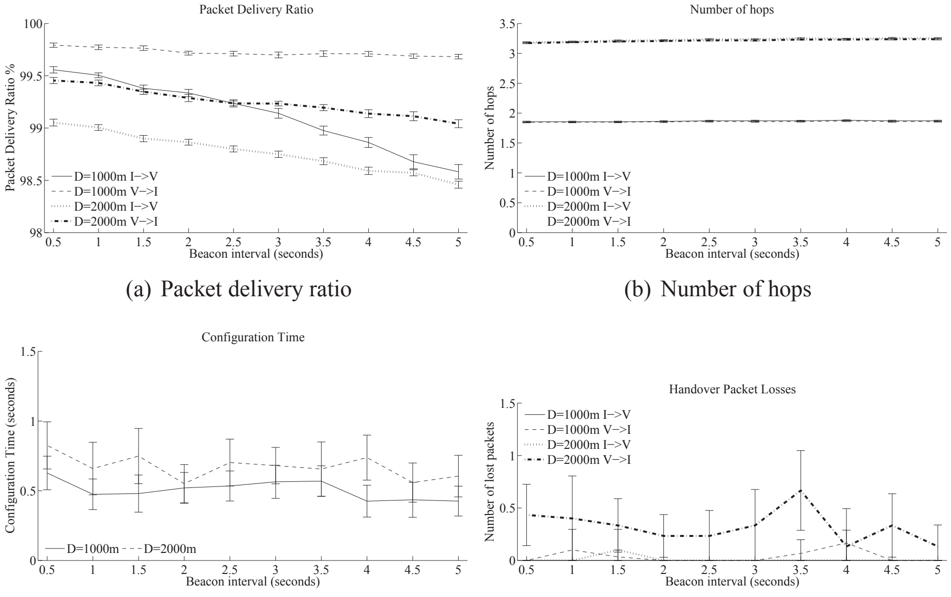
Handover Packets losses during handovers.

6. Performance Evaluation

In this section we conduct an extensive performance evaluation of the solution by means of simulation. A very important contribution of this section is assessing and understanding the impact of each of the optimization mechanisms. In order to do so, we follow a 2-stage approach. First, we analyze the results obtained when all the optimization mechanisms are enabled. Afterwards, taking these results as reference, we selectively disable each mechanism to analyze its influence on the overall performance of the solution. The goal of this analysis is to identify the mechanisms that can be disabled without a noticeable degradation on the performance. There may happen that mechanisms disabled together cause a significant loss of performance even if disabling each one individually does not. In order to avoid this, we compare the results of the final candidate solution (i.e., the resulting one after disabling all the mechanisms that did not seem to add any significant performance gains when disabled) against the reference solution results.

For the following tests we use the first traffic generation scenario, namely two UDP CBR flows of 20-byte data packets sent every 10ms between a vehicle and a node in the Internet. Figure 3 shows the performance obtained with the reference solution. Figure 3(a) presents the packet delivery ratio of the two CBR flows (Internet-VANET and VANET-Internet directions) as a function of the beaconing interval. It can be seen that the packet delivery ratio decreases when the beaconing interval increases, which is an expected behavior as the accuracy of the neighbor position information depends on the beaconing interval. In terms of packet delivery ratio, the VANET-Internet flow obtains a better result than the Internet-VANET one. This is due to the fact that the RSU/MAG is a fixed node, so the vehicles always know its location very accurately. On the other hand, in the Internet-VANET direction, the destination might be moving, and therefore the forwarding nodes need to have an accurate view of the destination's position, as the packet delivery may fail otherwise. Besides, the packet delivery ratio is higher when the distance between RSU/MAGs is shorter, which is also an expected result, since the longer the VANET path is, the higher the chances of losing packets are.

Figure 3(d) shows that the packet losses due to handovers are close to zero for all simulated cases. Only for the VANET-Internet flow, packet losses slightly in-



(a) Packet delivery ratio

(b) Number of hops

(c) Configuration time

(d) Handover packet losses

Figure 3: Performance evaluation of PMIPv6 over ETSI GeoNetworking (Reference solution).

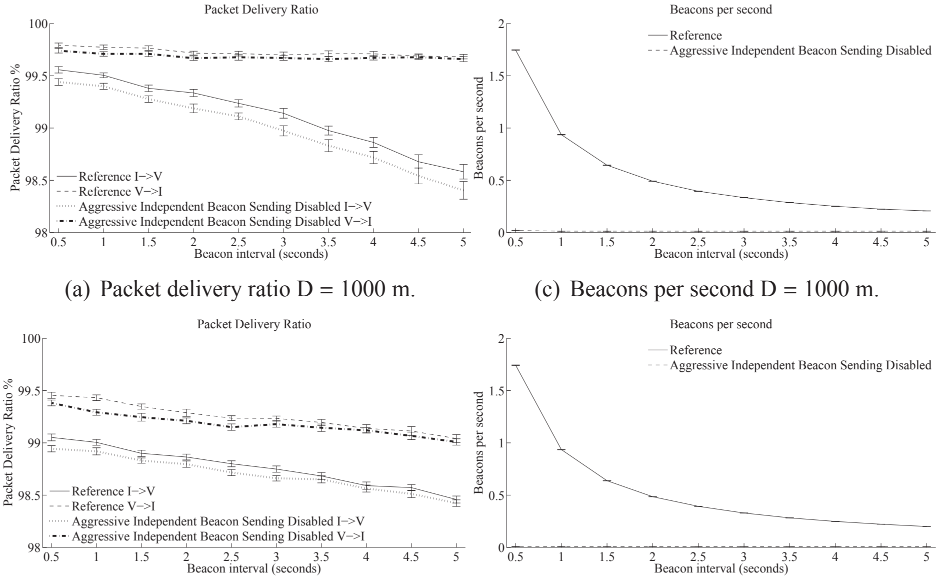
crease with the distance between RSU/MAGs is longer, because of the higher probability of losing a packet when the geographic area gets bigger (see Figure 3(b)).

We measured the average number of hops and configuration time, obtaining the expected results (see Figures 3(b) and 3(c)).

The next step after obtaining the reference solution results is to selectively disable one by one the different optimization mechanisms, analyzing their impact on the overall performance, by comparing the results obtained with the ones of the reference solution.

Aggressive Independent Beacon Sending: We present in Figures 4(a) and 4(b) the packet delivery ratio when aggressive independent beacon sending is disabled versus the reference solution (with aggressive independent beacon sending enabled). It can be seen from the results that the packet delivery ratio only slightly decreases when aggressive independent beacon sending is disabled in both scenarios (D = 1000 meters and D = 2000 meters).

Although we believed that aggressive independent beacon sending could help to improve the performance, obtained results do not support this assumption. In addition, the signaling control overhead significantly increses (see Figures 4(c) and 4(d)). Therefore, we decide to disable aggressive independent beacon sending



(a) Packet delivery ratio D = 1000 m.

(c) Beacons per second D = 1000 m.

(b) Packet delivery ratio D = 2000 m.

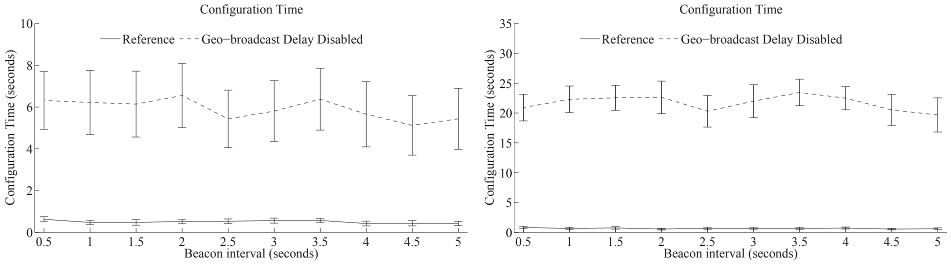
(d) Beacons per second D = 2000 m.

Figure 4: Analysis of Aggressive Independet Beacon Sending.

in the final solution.

Geo-broadcasting Delay: Figure 5 presents the impact of the geo-broadcasting delay optimization on the configuration time. When geo-broadcasting delay mechanism is disabled the configuration time is too high due to the collisions produced at the MAC layer when all vehicles inside RSU/MAG's radio coverage try to retransmit geo-broadcast RA packets at the same time. When geo-broadcasting delay mechanism is enabled, the configuration time is the expected one, as shown before in Figure 3(c). From the results shown in Figures 5(a) and 5(b), we can observe that the configuration time gets higher with the distance between RSU/MAGs when geo-broadcasting delay is disabled. This is because as vehicles get farther than one hop from the RSU/MAG, it becomes more likely that geo-broadcast RAs are lost due to the wireless collisions. Therefore, based on the obtained results, we decide to keep the geo-broadcasting delay mechanism in the final solution.

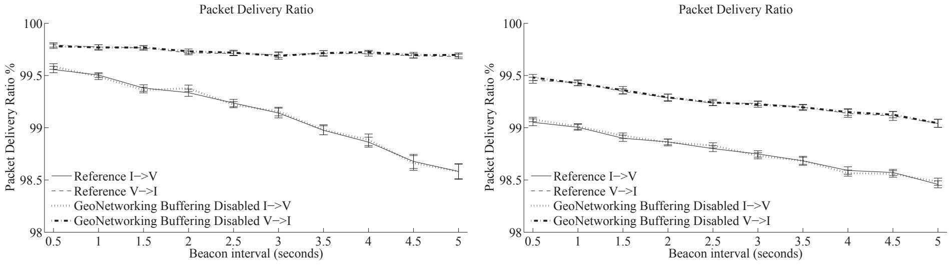
GeoNetworking Buffering: Figure 6 illustrates the impact of the GeoNetworking buffering optimization mechanism. The GeoNetworking buffering prevents discarding a packet when greedy forwarding does not find a valid next hop neighbor, by keeping the packet in a buffer for a certain amount of time. In this way, the GeoNetworking buffering is useful in scenarios with low vehicle density where disconnections between parts of the VANET are frequent. However, ex-



(a) Configuration time D = 1000 m.

(b) Configuration time D = 2000 m.

Figure 5: Analysis of Geo-broadcasting Delay.



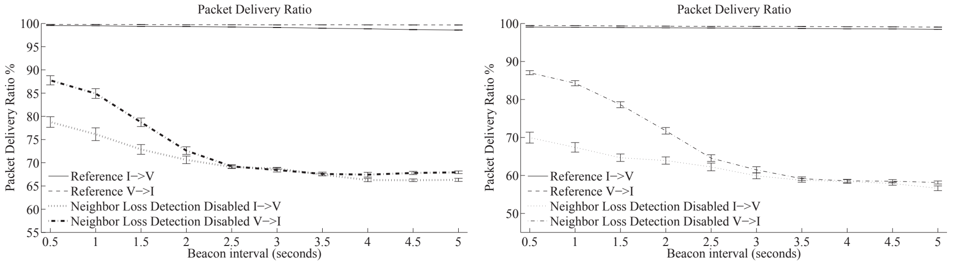
(a) Packet delivery ratio D = 1000 m.

(b) Packet delivery ratio D = 2000 m.

Figure 6: Analysis of GeoNetworking Buffering.

perimental results show that the GeoNetworking buffering deactivation does not produce any degradation on the packet delivery ratio. This can be explained because vehicles in our simulations are generated from real traffic traces of a busy highway. Hence, vehicles can find a path to other nodes of the VANET because the density of vehicles in the simulation is high. On the other hand, GeoNetworking buffering mechanism introduces extra complexity in network nodes. Therefore, in high density scenarios like ours, the GeoNetworking buffering mechanism can be disabled without any noticeable degradation of the performance.

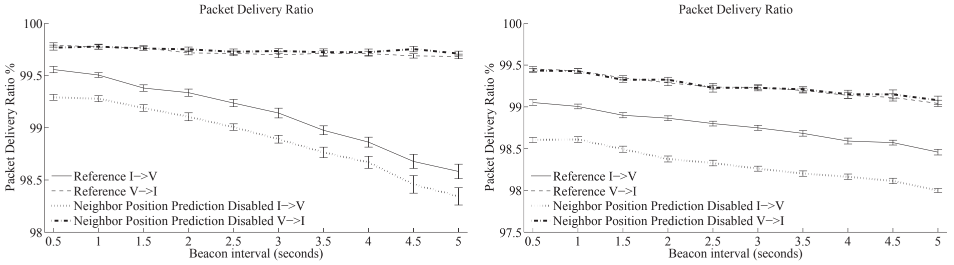
Cross-Layer Based Neighbor Loss Detection: In Figure 7 we analyze the influence of the cross-layer based neighbor loss detection optimization in the packet delivery results. It can be seen that the cross-layer based neighbor loss detection mechanism produces great improvements on the packet delivery ratio for both D = 1000 meters and D = 2000 meters. When forwarding packets with cross-layer based neighbor loss detection enabled, the node detects at the link layer that a next hop neighbor is not reachable anymore, and therefore that neighbor is removed from the location table so it is not used as next hop for future packet transmissions. The longer the distance between RSU/MAGs, the bigger the obtained gain.



(a) Packet delivery ratio D = 1000 m.

(b) Packet delivery ratio D = 2000 m.

Figure 7: Analysis of Cross-Layer Based Neighbor Loss Detection.



(a) Packet delivery ratio D = 1000 m.

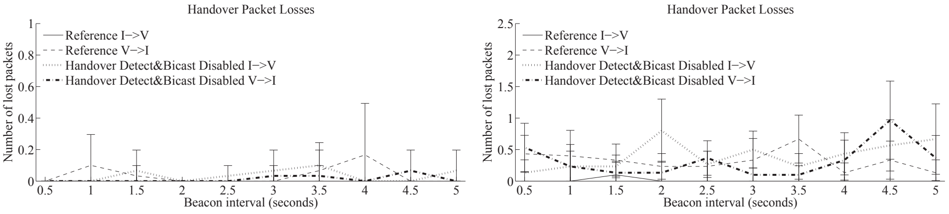
(b) Packet delivery ratio D = 2000 m.

Figure 8: Analysis of Neighbor Position Prediction.

This can be explained because as the distance between RSU/MAGs increases, the length of the chain of vehicles traversed by packets also increases, making more likely that a node selected as the best neighbor to forward a packet is no longer reachable. Of course, this effect depends on the beaconing interval, as it has a direct effect on the freshness of the position information. Therefore, cross-layer based neighbor loss detection is enabled in the final solution because it produces significant enhancements on the packet delivery ratio.

Neighbor Position Prediction: Next we analyze the impact of the neighbor position prediction optimization. Neighbor position prediction deactivation (see Figure 8) produces a slight decrease of the packet delivery ratio in the Internet-VANET flow because it is the most vulnerable flow: packets are directed to a destination that is moving so when the packet reaches the intended destination, it can happen that the node is not there anymore, whereas in the VANET-Internet flow, packets are addressed to the RSU/MAG which is a fixed node.

From the obtained results, we conclude that we can disable the neighbor position prediction mechanism in the final solution since the performance improvement is not significant and it introduces extra complexity in the network nodes. Note that,



(a) Handover packet losses D = 1000 m.

(b) Handover packet losses D = 2000 m.

Figure 9: Analysis of Handover Detection & Bicasting.

the cross-layer based neighbor loss detection mechanism could be hiding the positive effect of the neighbor position prediction mechanism because they deal with the same problem in different ways, but the former mechanism is more effective.

Handover Detection & Bicasting: As we can see in Figure 9, the number of lost packets in the handover is low regardless of whether the handover detection & bicasting optimization mechanism is enabled or not for both D = 1000 meters and D = 2000 meters. This is so because nodes do not need to lose connectivity with previous RSU/MAG before getting connectivity through the new one and therefore we have a make-before-break handover.

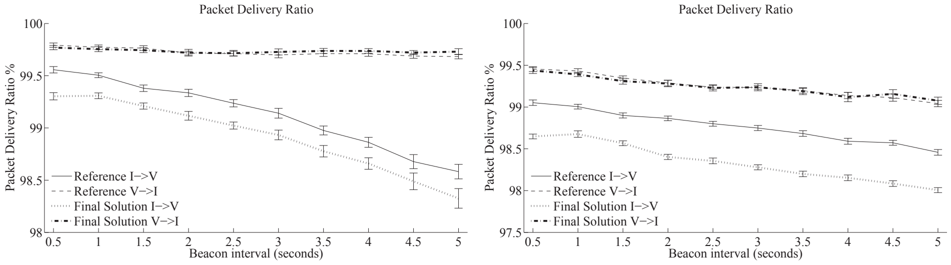
Taking into account that handover packet losses are low when the handover detection & bicasting mechanism is disabled and the overhead produced by the bicasting of packets, we decide to disable this optimization mechanism.

6.1. Final configuration of the GeoNetworking mechanisms

Based on the previous analysis, the final solution has the next configuration in terms of activated optimization mechanisms: independent beacon sending disabled, geo-broadcasting delay enabled, GeoNetworking buffering disabled, cross-layer based neighbor loss detection enabled, neighbor position prediction disabled and handover detection & bicasting disabled. The next step is to cross-check that the deactivation of some mechanisms has not produced a degradation effect that was not noticeable when analyzing each of the optimization independently.

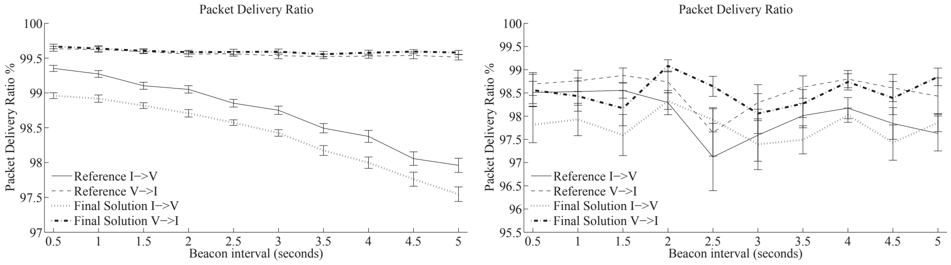
Figure 10 shows the packet delivery ratio of the two simple UDP CBR flows (Internet-VANET and VANET-Internet) as a function of the beaconing interval for both the final solution and the original reference solution. As expected, the packet delivery ratios for both solutions are very similar, with high values close to 100 %. Based on these results, we conclude that we can disable the previously identified optimizations as they do not provide a considerable performance gain.

After this detailed characterization of the different optimization mechanisms, as well as the complete solution, we were also interested in assessing the performance under more realistic traffic patterns. Packet delivery ratio results using



(a) Packet delivery ratio D = 1000 m. (b) Packet delivery ratio D = 2000 m.

Figure 10: Final and reference solutions comparison: packets of 20Bytes each 10 ms.



(a) Packet delivery ratio, 1 vehicle, D=1000m. (b) Packet delivery ratio, 10% vehicles, D=1000m.

Figure 11: Final and reference solutions comparison: packets of 512Bytes each 30 ms.

UDP flows of 512-byte data packets sent each 30 milliseconds are shown in Figure 11. Figure 11(a) represents the case where only one vehicle communicates with a CN in the Internet, whereas Figure 11(b) shows the results for the case in which 10% of vehicles are communicating with the CN. A first conclusion that we can derive from Figure 11(a) is that the packet delivery ratio decreases respective to Figure 10(a), due to the bigger packet size. Regarding the impact of a higher number of vehicles generating traffic (Figure 11(b)), the packet delivery ratio seems to be now independent of the beaconing interval. In any case, the packet delivery ratio is still very high, validating the feasibility of the solution to provide Internet connectivity from VANETs in more realistic scenarios.

7. Conclusion

In this paper we have tackled the problem of Internet connectivity provision in VANETs by combining the ETSI TC ITS architecture and its GeoNetworking protocol (GN) with PMIPv6 to provide mobility support. Since PMIPv6 was originally designed for single-hop scenarios where the MN is directly connected to the MAG, a solution for the adaptation of PMIPv6 to a multi-hop environment in order to integrate it with the ETSI TC ITS architecture has been presented. In addition to the generic integration design, we have described and analyzed different mechanisms that can be applied to the GeoNetworking protocol to improve the performance. An important contribution of this article is the performance and feasibility analysis of the general solution and the impact of the different proposed optimization mechanisms by means of simulation taking real traffic traces of an orbital highway in Madrid. A summary of the main conclusions obtained from this analysis is included next:

- The solution to provide Internet connectivity in VANETs combining the ETSI TC ITS architecture [3] and its GeoNetworking protocol (GN) [4] with PMIPv6 [7] proves to be feasible. Obtained results show a packet delivery ratio close to 100%.
- The beacon piggybacking optimization mechanism decreases the signaling control overhead on the VANET without degrading the performance.
- The geo-broadcasting delay optimization mechanism greatly reduces the configuration time.
- The GeoNetworking buffering optimization mechanism can be valuable for scenarios with low vehicle density, where disconnections between parts of the VANET can be frequent. The cost of the mechanims is introducing extra complexity in the network nodes. We however could not evaluate the influence of the mechanism because in our simulations we use real traffic traces where the density of vehicles is high.
- The cross-layer based neighbor loss detection optimization greatly improves the packet delivery ratio.
- The neighbor position prediction optimization mechanism can be disabled because it does not produce a noticeable enhancement on the performance of the solution and it introduces extra complexity in the network nodes.
- The handover detection & bicasting optimization mechanism can be disabled because handover packet losses are close to zero regardless of its activation.

As future work, we plan to analyze the influence of the location table lifetime on the performance because we have experimentally observed that its impact is considerable. Furthermore, we are interested in studying the applicability of PMIPv6 in vehicular scenarios considering other families of routing protocols, e.g. reactive or proactive routing protocols, instead of a geographic protocol like the ETSI GeoNetworking protocol [4].

Acknowledgment

This work has been funded by the Spanish MICINN through the I-MOVING project (TEC2010-18907) and by the EC FP7-ICT-2009-5 through the MEDIEVAL project (grant agreement n.258053). Authors would like to thank the Spanish DGT for providing us with the traffic traces used in this work.

References

[1] European Telecommunications Standards Institute Intelligent Transport System: http://www.etsi.org/website/Technologies/IntelligentTransportSystems.aspx.

[2] CAR 2 CAR Communication Consortium: http://www.car-to-car.org/.

[3] Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture (Mar. 2010).

[4] Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality (Jun. 2011).

[5] Intelligent Transport Systems (ITS), Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols (Mar. 2011).

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

[7] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, Proxy Mobile IPv6, RFC 5213 (Proposed Standard) (Aug. 2008).

[8] F. Abduljalil, S. Bodhe, A survey of integrating IP mobility protocols and mobile ad hoc networks, Communications Surveys Tutorials, IEEE 9 (1).

[9] V. Bychkovsky, B. Hull, A. K. Miu, H. Balakrishnan, S. Madden, A Measurement Study of Vehicular Internet Access Using In Situ Wi-Fi Networks, in: 12th ACM MOBICOM Conf., Los Angeles, CA, 2006.

[10] J. Ott, D. Kutscher, The ”drive-thru” architecture: WLAN-based Internet access on the road, in: VTC 2004-Spring. 2004 IEEE 59th.

[11] S. Annese, C. Casetti, C.-F. Chiasserini, N. Di Maio, A. Ghittino, M. Reineri, Seamless Connectivity and Routing in Vehicular Networks with Infrastructure, Selected Areas in Communications, IEEE Journal on 29 (3).

[12] A. Neumann, C. Aichele, M. Lindner, S. Wunderlich, Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.), Internet-Draft draft-openmesh-b-a-t-m-a-n-00, IETF, work in progress (Apr. 2008).

[13] J. Choi, Y. Khaled, M. Tsukada, T. Ernst, IPv6 support for VANET with geographical routing, in: ITS Telecommunications, 2008. ITST 2008. 8th International Conference on, 2008, pp. 222 –227.

[14] T. Narten, E. Nordmark, W. Simpson, H. Soliman, Neighbor Discovery for IP version 6 (IPv6), RFC 4861 (Draft Standard) (Sep. 2007).

[15] S. Thomson, T. Narten, T. Jinmei, IPv6 Stateless Address Autoconfiguration, RFC 4862 (Draft Standard) (Sep. 2007).

[16] S. Cespedes, X. Shen, C. Lazo, IP mobility management for vehicular communication networks: challenges and solutions, Communications Magazine, IEEE 49 (5) (2011) 187 –194.

[17] R. Baldessari, W. Zhang, A. Festag, L. Le, A MANET-centric solution for the application of NEMO in VANET using geographic routing, in: TridentCom ’08, ICST, Brussels, Belgium, 2008, pp. 12:1–12:7.

[18] S. Cespedes U., X. Shen, An Efficient Hybrid HIP-PMIPv6 Scheme for Seamless Internet Access in Urban Vehicular Scenarios, in: GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference, 2010, pp. 1 –5.

[19] M. Asefi, S. Cespedes, X. Shen, J. Mark, A Seamless Quality-Driven Multi-Hop Data Delivery Scheme for Video Streaming in Urban VANET Scenarios, in: Communications (ICC), 2011 IEEE International Conference on, 2011.

[20] R. Baldessari, C. Bernardos, M. Calderon, GeoSAC - Scalable address autoconfiguration for VANET using geographic networking concepts, in: PIMRC 2008. IEEE 19th International Symposium on, 2008, pp. 1 –7.

[21] C. Perkins, D. Johnson, J. Arkko, Mobility Support in IPv6, RFC 6275 (Proposed Standard) (Jul. 2011).

[22] H. Füßler, M. Torrent-moreno, M. Transier, A. Festag, H. Hartenstein, Thoughts on a protocol architecture for vehicular ad-hoc networks, in: 2nd Int. Workshop on Intelligent Transportation (WIT, 2005).

*Author Biography

Victor Sandonis received the telecommunication engineering and the M.Sc. in telematics engineering in 2009 and 2011, respectively from the Universidad Carlos III de Madrid (UC3M), Leganes, Spain where he is currently working toward the Ph.D. degree in telematics engineering. His current work focuses on vehicular networks and IP-based mobile communication protocols.

Maria Calderon is an associate professor at the Telematics Engineering Department of University Carlos III of Madrid. She received a computer science engineering degree in 1991 and a Ph.D. degree in computer science in 1996, both from the Technical University of Madrid. She has published over 40 papers in the fields of advanced communications, reliable multicast protocols, programmable networks and IPv6 mobility. Her current work focuses on vehicular networks and IP-based mobile communication protocols.

Ignacio Soto received a telecommunication engineering degree in 1993, and a Ph.D. in telecommunications in 2000, both from the University of Vigo, Spain. He was a research and teaching assistant in telematics engineering at the University of Valladolid from 1993 to 1999. In 1999 he joined University Carlos III of Madrid, where he was an associate professor since 2001 until 2010. In 2010, he joined Universidad Politécnica de Madrid as associate professor. His research activities focus on mobility support in packet networks, heterogeneous wireless access networks, and automatic network management and operation.

Carlos J. Bernardos received a Telecommunication Engineering degree in 2003, and a PhD in Telematics in 2006, both from the University Carlos III of Madrid (UC3M), where he worked as a research and teaching assistant from 2003 to 2008 and, since then, has worked as an Associate Professor. His Ph.D. thesis focused on route optimization for mobile networks in IPv6 heterogeneous environments. His current work focuses on vehicular networks and IP-based mobile communication protocols. He has published has published over 30 scientific papers in prestigious international journals and conferences, and he is also an active contributor to the Internet Engineering Task Force (IETF). He served as TPC chair of WEEDEV 2009 and as TPC co-chair of the Mobility track of NTMS 2011. He has also served as guest editor of IEEE Network.