ITSSv6 - IPv6 ITS Station Stack
for Cooperative ITS FOTs
http://www.itssv6.eu/

ICT-2009.6: ICT for Mobility,
Environmental Sustainability
and Energy Efficiency

ITSSv6 Deliverable

ITSSv6 STREP Grant Agreement 210519

D4.1 Initial Validation & Evaluation Results

DATE	22nd May 2012
CONTRACTUAL DATE OF DELIVERY TO THE EC	M12 (31.01.2012)
ACTUAL DATE OF DELIVERY TO THE EC	M13 (1.3.2012)
EDITOR, COMPANY	José Santa, UMU
DOCUMENT CODE	ITSSv6-D4.1-InitialValidation&EvaluationResults-v1.1
SECURITY	Public

Project Coordinated by Thierry Ernst - Mines ParisTech / Inria
E-mail: thierry.ernst@mines-paristech.fr

Document History

Release	Date	Reason of change	Status	Distribution
1.0	01/03/12	Final consolidated version	Final	Internal
1.1	01/05/12	Alignment with other deliverables	Final	EC

Contents

List of Figures

List of Tables

Executive summary

This is the first of the two expected deliverables in Work Package 4 (Validation and Evaluation). The main contributions of this first WP4 deliverable is the description of the validation/evaluation methodology which is going to be used in the project tests, the presentation of the essential cases of study for testing the communication stack developed and integrated in Work Package 3, and the report of main results obtained in the first tests.

This document identifies those technologies and subsystems that will be evaluated in three essential cases of study, although these could slightly change during the project. For the moment, it is found of core importance to assure the basic operation of the ITSSv6 communication stack, which is based on, first, supporting IPv6 mobility following the NEMO model; second, providing a route optimisation solution to the well-known performance problem of the mobility tunnel, by means of direct communication with correspondent nodes, that could be in near cars, for instance; and, third, exploiting multi-homed capabilities of mobile routers mounted in vehicles through flow selection techniques, which provide both performance and reliability improvements in data transfers.

Contributors

The following ITSSv6 members have contributed to this deliverable:

- José Santa, from University of Murcia.
- Jozsef Kovacs, from SZTAKI.
- Andras Varadi, from Lesswire.
- Antonio F. Skarmeta, from University of Murcia.
- Pedro J. Fernández Ruiz, from University of Murcia.
- Fernando Bernal Hidalgo, from University of Murcia.
- Manabu Tsukada, from INRIA
- Benjamin Cama, from Institut Télécom.
- Fernando Pereñiguez, from University of Murcia.
- Rafael Marín, from University of Murcia.

CHAPTER 1

Introduction

1.1 The ITSSv6 project

ITSSv6 (IPv6 Station Stack for Cooperative Intelligent Transportation Systems (ITS) Field Operational Tests (FOTs) is an European Project (STREP) from the 7th Programme Framework (Grant Agreement 270519), Call 6 (ICT-2009.6: ICT for Mobility, Environmental Sustainability and Energy Efficiency) started in February 2011 and lasting until January 2014. The project is coordinated by Institut National de Recherche en Informatique et en Automatique (Inria) and gathers Universidad de Murcia (UMU),Institut Mines Telecom (IT), lesswire (LW), Magyar tudomanyos akademia szamitastechnikai es automatizalasi kutato intezet (SZTAKI), Schalk & Shalk OG (IPTE) and Bluetechnix Mechatronische Systeme GmbH (BT) (Bluetechnix in short).

The objective of the ITSSv6 project is to deliver an optimized IPv6 implementation of ETSI / ISO ITS station reference architecture. ITSSv6 builds on existing standards from ETSI, ISO and IETF and IPv6 software available from the CVIS and GeoNet projects. The IPv6 lTS station stack provided by ITSSv6 supports at least 802.11p and 2G/3G media types and is configured differently according to the role played by the ITS station (roadside, vehicle, central). The tasks of ITSSv6 are to:

- Gather third party users into a common User Forum to collect user's requirements;
- Enhance existing IPv6-related ITS station standards and specification of missing features;
- Implement IPv6-related ITS station standards;
- Validate the implementation and assess its performance;
- Port the IPv6 ITS station stack to selected third party platforms;
- Support third parties in the use of the IPv6 ITS station stack.

Publishable material of the ITSSv6 project (public deliverables, newsletters, presentations made at conferences or workshops, information about events) are made available on the project's web site (http://www.itssv6.eu) as it becomes available.

1.2 Purpose of this deliverable

Validating and evaluating the communication stack that is being developed in ITSSv6 is an essential part of the project. Since one of the objectives is to port the communication stack to third parties (mostly field operational test projects - FOTs), an extensive validation and evaluation of the implementations carried out in the project must be performed before that moment. Moreover, testing the communication stack will provide visibility to the project and, in the medium/long term, could assure the continuity of the prototypes/implementations developed in frames of ITSSv6. The project Description of Work points out that two deliverables have to be released within Work Package 4, which must describe the validation and evaluation tests performed over the ITSSv6 communication stack. The first of these two deliverables, which is the present one, is focused on the description of the evaluation platform (Task 4.1) and the first tests carried out of those essential parts of the communication stack (Tasks 4.2 and 4.4).

1.3 Objectives and contributions

As it is described in Work Package 2 (System Specification) and Work Package 3 (Implementation and Integration) deliverables, the core components of the stack are focused on providing basic IPv6 network mobility for an in-vehicle network, which is provided of the necessary capabilities to efficiently use multiple network paths simultaneously, by means of one or more physical communication interfaces. This document describes, in general, the methodology used to validate and evaluate the communication stack implemented in ITSSv6 and, particularly, presents a set of cases of study and first results obtained in the evaluation of these core features required of the stack at this moment.

1.4 Structure of the document

The present document is structured as follows:

- Chapter 2 describes the technological features that have been tested in this first set of evaluations and the testing methodology that will be maintained during the work package lifetime.
- Chapter 3 gives an overview of the general scenario considered in tests, describing main nodes, communication means and roles.
- Chapter 4 describes the data gathering and processing environment used to collect communication logs and obtain relevant figures of merit of the network performance.
- Chapter 5 includes the cases of study that have been considered at this stage to test the core functions of the stack, together with the results obtained in first tests.
- Chapter 6 concludes the document revisiting main outputs of this first round of tests and identifying the next tasks to be performed within this Work Package.
- Appendix B provides the list of acronyms;
- References are provided at the end of this document.

CHAPTER 2

Testing methodology

This chapter describes the methodology that will be used for both the first set of tests included in this ITSSv6 deliverable and further tests carried out during the project lifetime. As indicated in the Description of Work, deliverable 4.2 will provide a final report of the final tests carried out on a real and overall testbed.

2.1 ITSSv6 features to be tested

According to WP2 deliverable [ITSSv6-D2.2], the set of technologies involved in the ITSSv6 communication stack design is divided into three groups (classes): technologies to be implemented and integrated (class-1), technologies to be implemented and probably integrated (class-2) and technologies to be analysed (class-3). For the first evaluation of the communication stack, a set of core class-1 technologies are considered, since they are understood to provide the essential operation of the system regarding mobility support and efficient routing. These technologies are listed next.

Regarding mobility management the technologies considered are:

- NEMO, since basic IPv6 mobility capabilities are essential in the project.
- MCoA, because testing the operation of the stack under multi-homed conditions is of interest.

Regarding routing, the next protocol is used:

- Geonetworking, since geographical V2V dissemination of messages over a concrete area can be essential for some ITS services.

For IPv4-IPv6 transition, the next technologies are used:

- L2TP, which is necessary to encapsulate IPv6 traffic over IPv4 networks. This solution is used to create a tunnel between Roadside ITS Stations and a Central ITS Station.
- OpenVPN, which is also used to encapsulate IPv6 packets, but in this case it is used to create a tunnel between Vehicle ITS Stations and a Central ITS Station.

- 6o4 tunneling, which is a more simple tool to create an IPv6 tunnel over IPv4. This technology has been used in the same scenario than OpenVPN in some tests, but it will be replaced with this last technology in further tests.

Finally, the next communication media are used:

- 802.11a/b/g, as a support of legacy networks for the in-vehicle network or roadside stations. 802.11p will be gradually integrated in the testing scenarios, and it will be used as 802.11 communication technology in next tests.
- 2G/3G, to provide a quasi-global connectivity to the in-vehicle networks.

2.2 General testing methodology

The general testing methodology which will be used in ITSSv6 comprises the next steps:

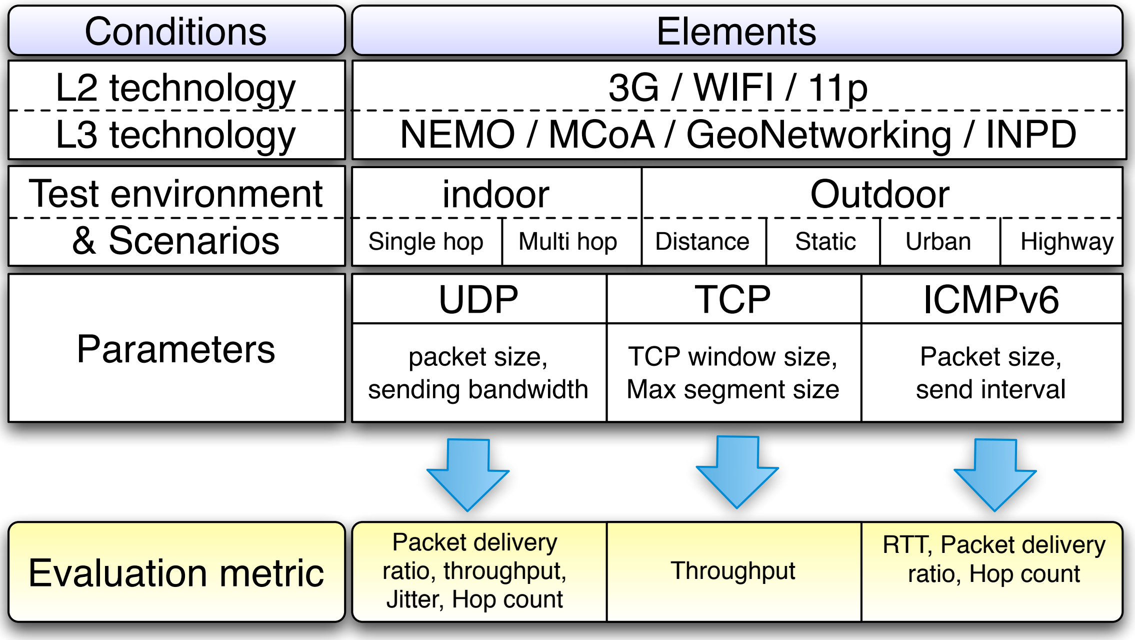
1. Testing platform specification.
   (a) Definition of the scenario for the case of study, taking into account the technologies to be tested and the expected capabilities.
   (b) Detailed description of the tests to be done, considering data flows, movement of terminals, physical conditions, etc.
   (c) Definition of the performance metrics to be analysed during tests, in order to save relevant dumps.
   (d) Specification of the needed software tools to both log performance metrics during tests and carry out post-processing tasks.
2. Indoor tests.

   A first round of tests in order to debug future problems or more extensive cases of study can be interesting before performing realistic outdoor tests.
   (a) Validation of the integrated stack (conformance tests).
   (b) Preliminary tests emulating outdoor trials.
   (c) Tests.
   (d) Evaluation of results.
3. Outdoor tests.
   (a) Infrastructure and vehicle set-up.
   (b) Preliminary outdoor tests, before involving extra human resources (for driving, etc.).
   (c) Tests.
   (d) Evaluation of results.
4. Global assessment of results.

   In this stage conformance evaluations carried out in 2a and results collected in 3d will be essential to create a final validation/evaluation report for each case of study.

In this deliverable, the previous methodology is adopted partially, considering a set of preliminary tests which have been obtained both in laboratory (indoor) and outdoors, although in this last case only considering tests which could cover step 3b in the previous plan. Final evaluations to be reported in the deliverable D4.2 will consider the whole testing roadmap.

All evaluation parameters and evaluation metrics are summarized in Table 2.1. Initially, L2 and L3 technologies defined in deliverable [ITSSv6-D2.2] as class-one features will be tested under identical conditions (network configuration, vehicles, location, test scenarios and so on) in text steps of WP4. Main test environments and parameters that will be taken into account are also specified in Table 2.1.



<table>
<tr><th>Conditions</th><th colspan="6">Elements</th></tr>
<tr><td>L2 technology</td><td colspan="6">3G / WIFI / 11p</td></tr>
<tr><td>L3 technology</td><td colspan="6">NEMO / MCoA / GeoNetworking / INPD</td></tr>
<tr><td rowspan="2">Test environment & Scenarios</td><td colspan="2">indoor</td><td colspan="4">Outdoor</td></tr>
<tr><td>Single hop</td><td>Multi hop</td><td>Distance</td><td>Static</td><td>Urban</td><td>Highway</td></tr>
<tr><td rowspan="2">Parameters</td><td colspan="2">UDP</td><td colspan="2">TCP</td><td colspan="2">ICMPv6</td></tr>
<tr><td colspan="2">packet size, sending bandwidth</td><td colspan="2">TCP window size, Max segment size</td><td colspan="2">Packet size, send interval</td></tr>
<tr><td>Evaluation metric</td><td colspan="2">Packet delivery ratio, throughput, Jitter, Hop count</td><td colspan="2">Throughput</td><td colspan="2">RTT, Packet delivery ratio, Hop count</td></tr>
</table>

Table 2.1: Evaluation Parameters and Evaluation metrics

The **indoor test environment** is designed to evaluate the pure performance of ITSSv6 protocols avoiding interferences due to unexpected radio perturbations and difficulties to trace the movements of the mobile routers (MRs). The tests will be performed in laboratory, without any vehicle as shown in Figure 2.1. The Global Positioning System (GPS) information used will not be taken from a real GPS device but from a log previously recorded while driving a real vehicle. The advantage of this method is that the same test scenarios can be repeated several times with various parameters.

To evaluate the performance in more realistic scenarios, we have considered for integral WP4 tests an **outdoor field test environment** with four vehicles equipped with an MR, a mobile network node (MNN), a GPS receiver and a WiFi antenna, as shown in Figure 2.2. The topology of the network will dynamically change during the test depending on the location of the vehicles. The performance of the implementations will also depend on the radio propagation, which is influenced by obstacles. Network performance also depends on other factors such as the distance or the movement of vehicles. We have therefore developed the AnaVANET evaluation tool (described in Section **??**) to perform the evaluation taking into account all of these factors.

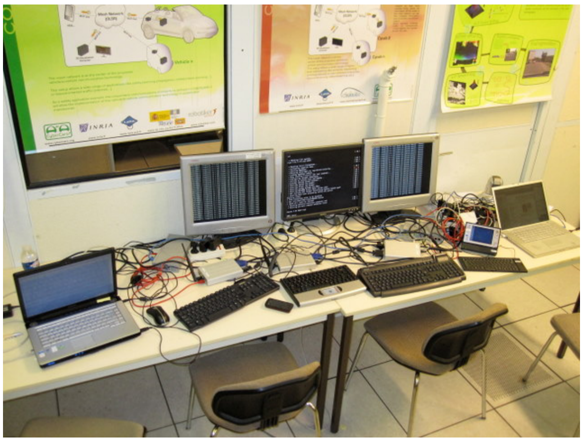


Figure 2.1: Indoor Testbed

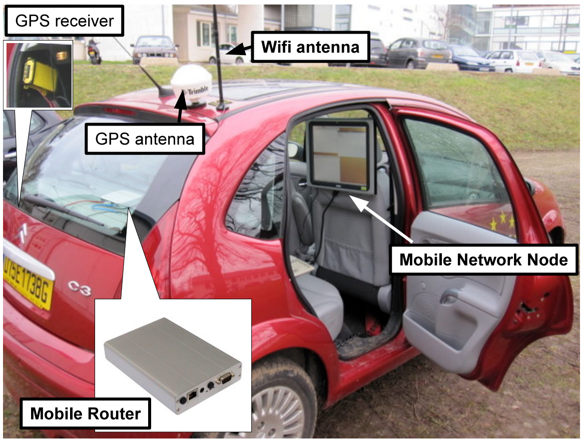


Figure 2.2: Outdoor Testbed

2.3 Overview of main communication flows

This section introduces the main communication flows that are used to evaluate the ITSSv6 communication stack. User Datagram Protocol (UDP), Transmission Control Protocol (TCP) and Internet Control Message Protocol version 6 (ICMPv6) are used to measure the network performance between two communication end-nodes (MNN to MNN):

UDP The User Datagram Protocol is a connectionless unidirectional protocol used in the OSI transport layer of computers. It is based on the exchange of datagrams and neither acknowledgement nor flow control are included. The header includes enough information to allow the routing of packets to the destination.

TCP The Transmission Control Protocol is one of the main protocols of Internet and it is also used in the OSI transport layer. It is connection oriented and provides flow and congestion management. In this way, it guarantees the delivery of packets without errors in the same order that they were transmitted.

ICMPv6 The Internet Control Message Protocol version 6 is a multi-purpose protocol designed for diagnosis, neighbor discovery and access to multicast addresses. There are two types of packets: error messages and informative messages. Within testing tasks, the informative messages Echo Request and Echo Reply are used to test the network operation and delay.

2.4 Overview of performance metrics

Many performance metrics used in the number of evaluations that will be finally carried out in the project will be the same, above all, the ones related to assessing the performance of the data traffic while the network operates under real or synthetic load. For this reason, it is found of interest to list those main metrics of interest that are used in current cases of study or future ones in the project. When specifying concrete cases of study, only new metrics that are not well-known will be defined.

2.4.1 Bandwidth

The bandwidth receives a different connotation depending on the communication layer considered. While it refers to the frequency spectrum used by communication technologies at physical level, for instance, evaluations in ITSSv6 are focused on the network and transport level and, hence, the bandwidth is understood in the rest of the document as the effective data rate that can be achieved during a period of time.

Specifically, the bandwidth should be understood as the amount of data than can be transferred through a communication link per time unit. In this document, and in further WP4 documents, the bandwidth is measured in Kilobits per second (Kbps) or Megabits per seconds (Mbps). Notice that bits are used instead of bytes, as it is usual when measuring network performance.

When the bandwidth is used in evaluations, it should be indicated if the data rate reported regards with the data load of IPv6 packets or the data load of other higher level protocols (such as TCP or UDP). When this is not specified it will be considered that the first case is applicable.

2.4.2 Packet delivery ratio

The packet delivery ratio refers to the number of packets correctly decoded by a receiver node as compared with the number of packets sent from a sender node. Since it stands for data packets received, it is commonly used in packet switched communication technologies at access layer or above.

The packet delivery ratio, also called PDR, is usually measured in % of packet correctly delivered to the receiver node during a period of time. It is common that protocols used for measuring the PDR are not connection-oriented, in order to be aware of all packets lost when they are sent. It is assumed, nevertheless, that lower layers (for instance the 802.11b MAC) could manage packet losses at a different level. These recoveries are not taken into account when measuring the performance from the networking and transport layer point of view.

2.4.3 Delay and latency

In networking performance evaluation, delay and latency are commonly used to measure the response time of the communication link. In general, the network delay is composed of four times:

Processing delay This is the time needed to process the different control headers of packets, to know what a network node has to do with them.

Queuing delay This is the time the packet waits to be sent through a communication channel, since other packets could be sent before it.

Transmission delay It is the time the communication equipment takes to send all bits of the packet.

Propagation delay This is the travel time of the packet through the physical medium.

As usual in IP-level evaluation studies, the delay or latency is treated end-to-end, between IP networking nodes. In this document and the rest of WP4 reports, this is also applicable, and, in general, processing, queuing, transmission and propagation times will not be analyzed.

The communication delay or latency is usually measured in milliseconds (ms), due to the relative short time needed to receive and process a packet sent from a remote node when the communication technologies considered in this project are used (see [ITSSv6-D2.2] for a complete list of the communication technologies used in the project).

2.4.4 Round-trip delay time

The round-trip delay time or RTT is used in computer networks to refer to the time a packet takes to reach the destination node, plus the time needed to receive a response to this packet at the sender node. The RTT is many times the most common way to measure the delay of the network, since it compensates the time drift between the sender and the receiver clocks. When the clock of both sender and receiver are not synchronized it is really difficult to compute the real delay (one-way) of the network.

In the same way than it is done for delay or latency, the RTT is usually measured in milliseconds (ms). Additionally, a well-known procedure to measure the RTT is by using the *ping6* utility, available in all operating systems. It uses the ICMPv6 protocol to generate Echo messages that are replied with Echo responses from the receiver node.

2.4.5 Jitter

The jitter is a measure of the variability over time of the packet latency across a network. A network with constant latency has no variation (or jitter). Packet jitter is expressed as an average of the deviation from the network mean latency. Our AnaVANET evaluation tool (Section **??**) computes it by using the RTT time.

2.4.6 Number of Hops

The performance of the network when direct V2V communication is used depends on the network configuration, particularly the number of hops that packets are transmitted through between their source and destination. Thus we can get the best network performance when the MRs is directly connected (single hop). In contrast, multi-hop configurations add transmission and processing delays. Evaluations in WP4 consider both single hop and multi-hop cases. In some evaluations where roadside ITS stations are used as an intermediate node between vehicles, considering the number of hops is also of interest.

CHAPTER 3

General scenario

3.1 Overall scenario

The general scenario considered as the basis for all cases of study can be seen in Figure 3.1. Scenarios considered on each case of study will be based on this, although each one is supposed to provide extended details about the final set-up, since the set of preliminary tests provided in this deliverable will be mostly carried out by individual partners. As can be observed in Figure 3.1, a Home Central ITS Station is used as the home domain for the vehicles (Mobile Routers - MRs) used in the tests. Here is hosted the Home Agent (HA) functionality, which offers mobility support to in-vehicle networks. An extra set of domains are obtained my means of Visited Central ITS Stations. For simplification reasons it is assumed in the model that each domain formed by each Central ITS-S offers connectivity with a different communication technology. This fact could slightly change and this would be indicated in each case of study but, at least, more that one domain is necessary and 802.11x and 3G communication technologies must be provided when mobility is evaluated.

When using 3G it is assumed that one of the domains, usually the Home Central ITS-S, is used to provide encapsulation of IPv6 over the IPv4 operator's network. As can be seen, it is assumed that testbed nodes are distributed among the partners most involved on implementation and testing issues (UMU, INRIA, TB and SZTAKI). Changes over this general scenario are indicated on individual cases of study.

Inside the in-vehicle network both ITS-S host and ITS-S router functionalities must be provided, in order to perform the necessary tests, an extra node at the infrastructure (Correspondent Node - CN) could be considered to test the communication with a computer located outside the ITS network.

3.2 List of considered technologies

The set of technologies which are tested in these preliminary testbeds and tests are listed in Section 2.1, but some of them are considered in the base scenario, since they could be used in all cases of study.

- UMTS/3G is used to support wireless communications as one of the technologies over which alternate in mobility scenarios.

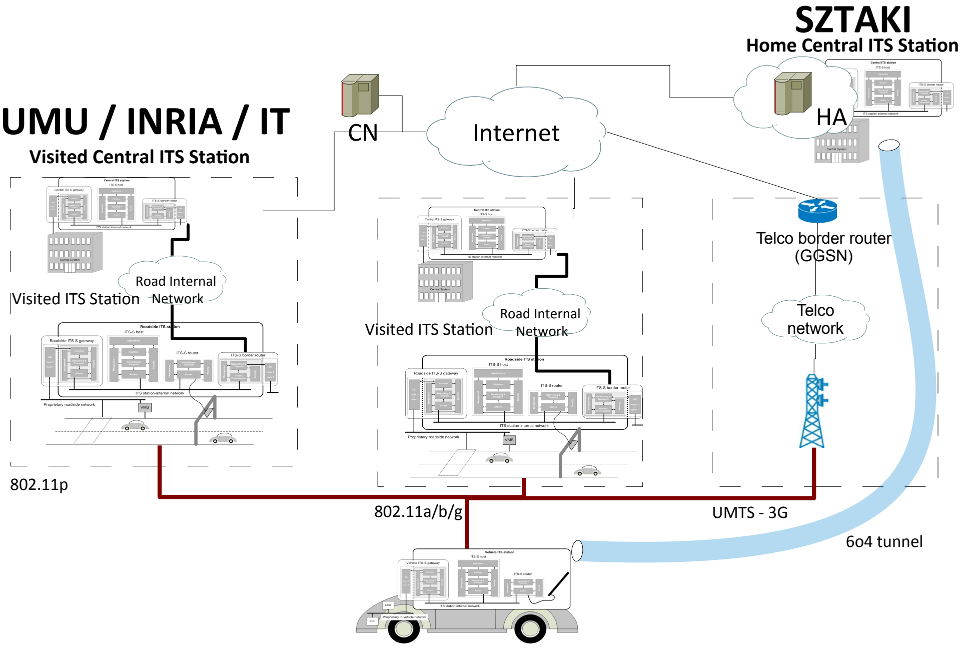


Figure 3.1: General scenario

- 802.11 a/b/g could be used on concrete areas with former hotspot capabilities and inside the vehicle, as a means to communicate hosts with the on-board ITS-S router (mobile router). Additionally, until 11p devices are available, 11a/b/g could also be used as the communication technology that connect vehicles to roadside units.

- NEMO is used in all cases of study included in this deliverable, since it is the basis to support network mobility for the in-vehicle terminals.

- Tunnelling technology to overcome the IPv4 to IPv6 transition issue. Depending on the case of study, OpenVPN, L2TP or 6o4 tunnelling could be used.

3.3 Involved nodes

The list of nodes/roles that, at least, are identified for the validations/evaluations described in this document are:

1. Vehicle ITS Station
   (a) ITS-S Host, as the edge for data traffic and acting as a mobile network node.
   (b) ITS-S Router, with the mobile router capabilities of the vehicle.
2. Roadside ITS Station

   (a) ITS-S router, providing both an 802.11 attachment point at the Access level, and access router functionality at the Networking and Transport level.

3. Central ITS Station

   (a) ITS-S border router, providing Internet connectivity.

   (b) Home Agent, when the Central ITS-S manages the home domain.

   (c) Tunnelling server, to support the IPv4-IPv6 transition when 3G is used.

3.4 Brief introduction to cases of study considered

As set of three initial cases of study have been found useful to test the essential operation required from the ITSSv6 communication stack:

Network mobility support Validation and evaluation of the basic operation and performance of NEMO over real wireless networks provided on different domains.

Geonetworking Validation and evaluation of the IPv6 support over Geonetworking to support both V2I and V2V message dissemination over interesting areas.

Multiple care of address evaluation with static flow distribution Validation and evaluation of the advantages of using multi-homed mobile routers to distribute traffic among multiple network paths.

These scenarios will be extended in next testing steps to be carried out during the project, as long as new others are included to finally test all Class-1 technologies and probably some Class-2 features. The next section details this first set of cases of study.

3.5 General evaluation scenarios

This section describes the most representative scenarios and use cases that will be taken into account in all WP4 tests. Most of the concrete tests described in this document and in future WP4 reports will follow equivalent tests.

3.5.1 Indoor evaluation

3.5.1.1 Basic indoor evaluation scenario for single and multiple-hops

The typical network set-up for indoor testing is showed in Figure 3.2, where tests are performed without moving terminals. In the indoor testbed, MRs are put close to one another. In this case, the three MRs are in the same wireless range and each MR can receive the beacons from the others. As can be seen, a Geonetworking layer is also showed to allow V2V communication. ITS station hosts act as mobile network nodes inside vehicles. GPS positioning is disabled for indoor evaluations and static positions previously recorded in a configuration file are used instead.

This scenario can be used to evaluate the latency when ICMPv6 traffic is used, for instance, the Packet Delivery Ratio (PDR), when UDP is used, or the throughput, when transmitting TCP packets. Hosts usually run a testing script to evaluate several performance metrics by changing various parameters. Additionally, since several mobile routers are used, both single-hop and multi-hop scenarios can be tested.

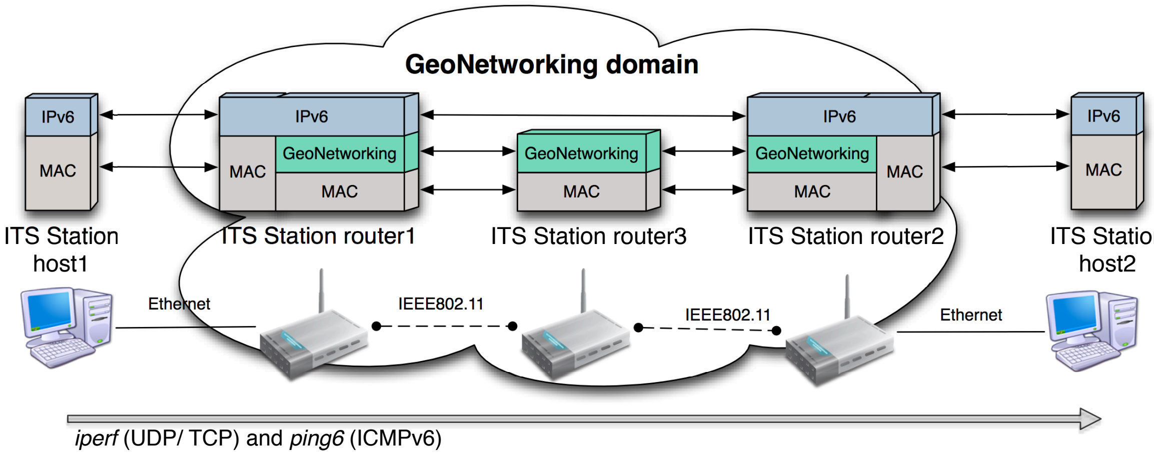


Figure 3.2: Indoor Network configuration

3.5.1.2 Network mobility evaluation scenario

A testing configuration where network mobility is enabled to access Internet can be seen in Figure 3.3. Here a host uses its home addressing to communicate with a correspondent node outside the ITS network. The first MR on the left is used in the host vehicle and it maintains its network addressing by using NEMO. Moreover, it could be the case that the host MR accesses the infrastructure network by mean of another vehicle, by using V2V Geonetworking communications. This is also illustrated in Figure 3.3.

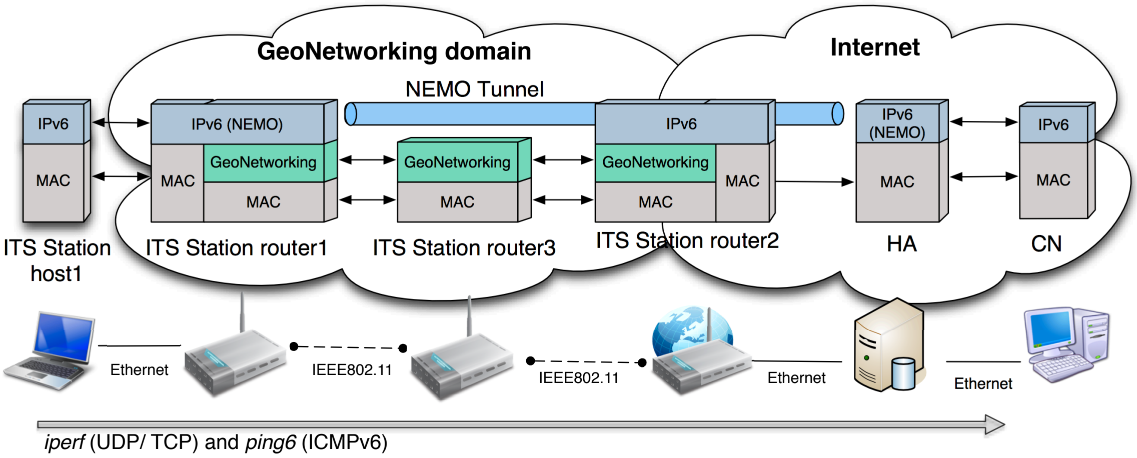


Figure 3.3: Network configuration of the indoor test

3.5.2 Outdoor evaluation

The most challenging scenario when testing prototype network is doing that in real environments. It is then when one detect problems not detected when simulations or controlled testbeds are used.

The network configuration considered could be the same as the ones described in indoors cases, except that a GPS device is usually accessed to dynamically obtain the vehicle position.

A set of general scenarios should be considered as the basis to test vehicular networks in real environments, taking into account several road parameters and constraints to remain tests as much realistic as possible and embrace significant information that could be applicable to many driving conditions. The main factors which determine these scenarios are:

Mobility Vehicle mobility is a key issue to cope with realistic Vehicular Ad-hoc Network (VANET) conditions. This way, not only static scenarios, to test the network operation in a controlled way, but also dynamic scenarios, under common traffic situations, should be considered. Of course, proper field operational tests should be conducted taking into account doppler shifting, fast fading, etc., which affect on the network performance.

Environment Urban and interurban environments affects communication performance in a different manner, because the signal propagation is hidden by buildings (among other elements), and the line of sight between vehicles is not always possible. Two environments should, at least, been considered in final tests: a semi-urban one, which will be probably located at INRIA-Rocquencourt and contains a set of small buildings surrounded by streets, and a highway stretch, which could be the A-12 motorway, near INRIA-Rocquencourt.

Number of vehicles The number of hops between the source and the destination vehicles affect the communication delay, as it can be expected. In addition to the extra forwarding delay, the packet loss at Medium Access Control (MAC) level also increases due to transmission interferences. Up to four vehicles will be considered in final WP4 trials, in order to check the communication delay as the number of hops increases.

The previous summary of recommendations when performing outdoors tests are considered in the four outdoor scenarios included in Figure 3.4. In this case testing scenarios are divided into urban and highway, and mobility has been set to static, urban-like speed, and high speed.

3.5.2.1 Distance test

The distance test should be performed with two vehicles to make easier the test, as shown in Figure 3.4. In the beginning of the test, both vehicles should be located at the same point. Then, one vehicle will remain static, while the other will leave its position along a straight road. The communication between them should be studied at low speed (up to 10 Km/h), in order to perfectly map communication problems with the distance. At some point the packet transmission between them will start drop packages because of the wireless radio range limitation. When the communication is lost the moving vehicle should return to the starting point. When the vehicle comes back, the communication should be reestablished as the distance becomes smaller. There should not be obstacles between vehicles, since the aim of this scenario is to check the maximum distance the wireless interface can reach.

3.5.2.2 Static test

As shown in Figure 3.4, static tests should be performed with a set of vehicles parked at significant points, where direct communication between not desired pairs of MRs is avoided. Building blocks can be used to do that. Under this configuration multi-hop scenarios where links are not changed could be reproduced.

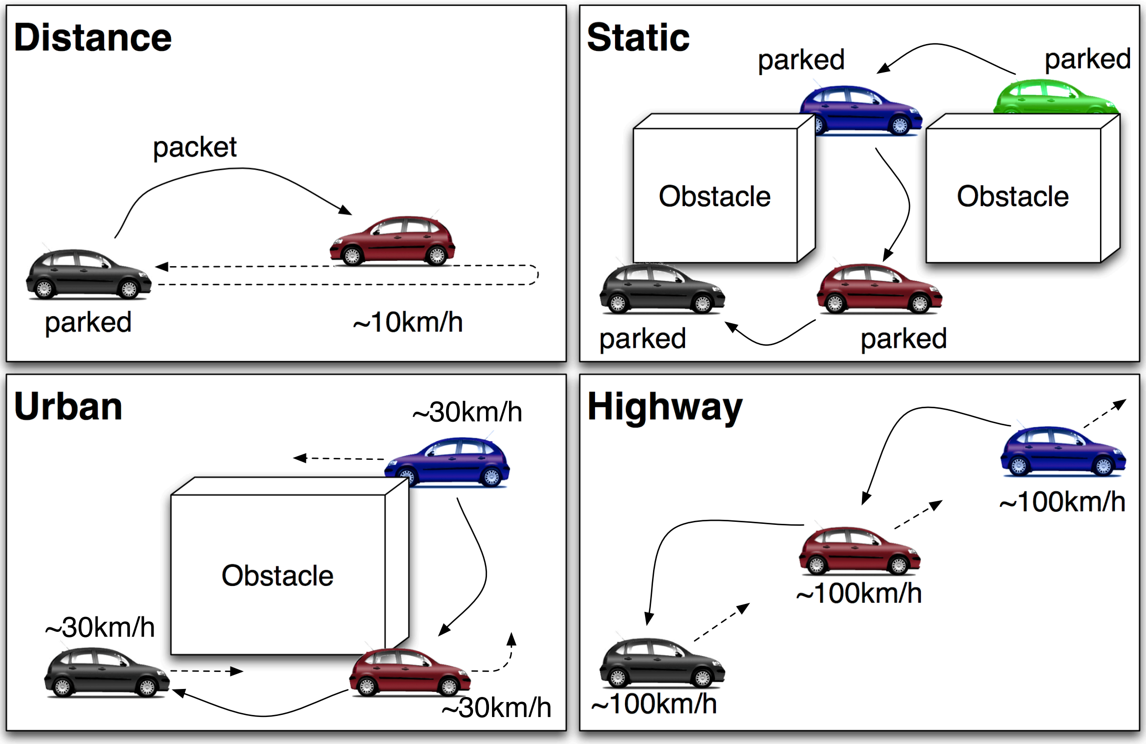


Figure 3.4: Real field Evaluation Scenarios

3.5.2.3 Urban test

As shown in Figure 3.4, Urban test could be performed with a set of vehicles that are moving slowly (up to 30 Km/h). Buildings or the other obstacles should block the wireless radio access among vehicles and between vehicles and roadside units. Because of the dynamic environment, multi-hop topologies should change and several roadside units could be used along the testing stretch. The aim of the test is measuring the network performance with dynamic topologies and handoffs, and evaluate the effect of obstacles that block the wireless radio communication.

3.5.2.4 Highway test

As shown in Figure 3.4, interurban tests should be tackled with a set of vehicles driving on a highway and connecting both among them or with the infrastructure by a set of roadside units. The speed of the vehicle should be maintained between 60 and 120 km/h to have meaningful results. The distance among vehicles should be changed to test V2V communications. As can be also noted in Figure 3.4, buildings should not block the wireless radio frequently.

CHAPTER 4

Data gathering and processing environment

The current chapter describes the AnaVANET (Analysis of Vehicular Ad-Hoc Networks) tool, which is used for gathering operation and performance evaluation data. These data is later used, in post process, to compute final performance metrics and plot graphical results about both signaling and data transfer processes of several protocols used in the project. At this stage of the project, not all scenarios and tests use this testing environment, and those trials that use it will be clearly specified when the study case is presented in Chapter 5.

AnaVANET is a tool developed by INRIA and University of Murcia to analyze vehicular networks. It was originally used to evaluate Optimized Link State Routing (OLSR)-based ad-hoc vehicular networks [Santa2009b, Santa2009a] . Then, AnaVANET was extended in order to analyze IPv6 packets transmitted with a Geonetworking header and Network Mobility (NEMO) header [GeoNet-D7.1, Tsukada2010b].

We first present the system overview of AnaVANET in Section 4.1. Then, basic packet processing methods are described in Section 4.2. The Geonetworking extension is described in Section 4.3. Section 4.4 gives the details of AnaVANET NEMO extension to treat packets with NEMO header and NEMO signaling (Binding Update (BU), Binding Acknowledgement (BA) and Binding Error (BE)). Initial AnaVANET was not designed for Internet-based communication, but only vehicle-based communication. This caused problems especially in handover scenarios. The packet processing when evaluating handover scenarios is described in Section 4.5.

4.1 AnaVANET system overview

Figure 4.1 provides an overview of the experimental evaluation process that is carried out in tests. The Sender (MNN) is in charge of generating data traffic, and both the sender and the receiver record a high level log, according to the application used to generate network traffic. All MRs record information about forwarded data packets by means of the *tcpdump* software, and log the vehicle position continuously. All this data is post-processed by the AnaVANET software and then analyzed. A Java application traces all the data packets transmitted from the sender node. This way, it is possible to detect packet losses and calculate statistics for each link and end-to-end, and merge all these per-hop information with transport level statistics of the traffic generator. As a result, AnaVANET outputs an Extensible Markup

Language (XML) file with statistics over one-second periods, and a packet trace file with the path followed by each data packet.

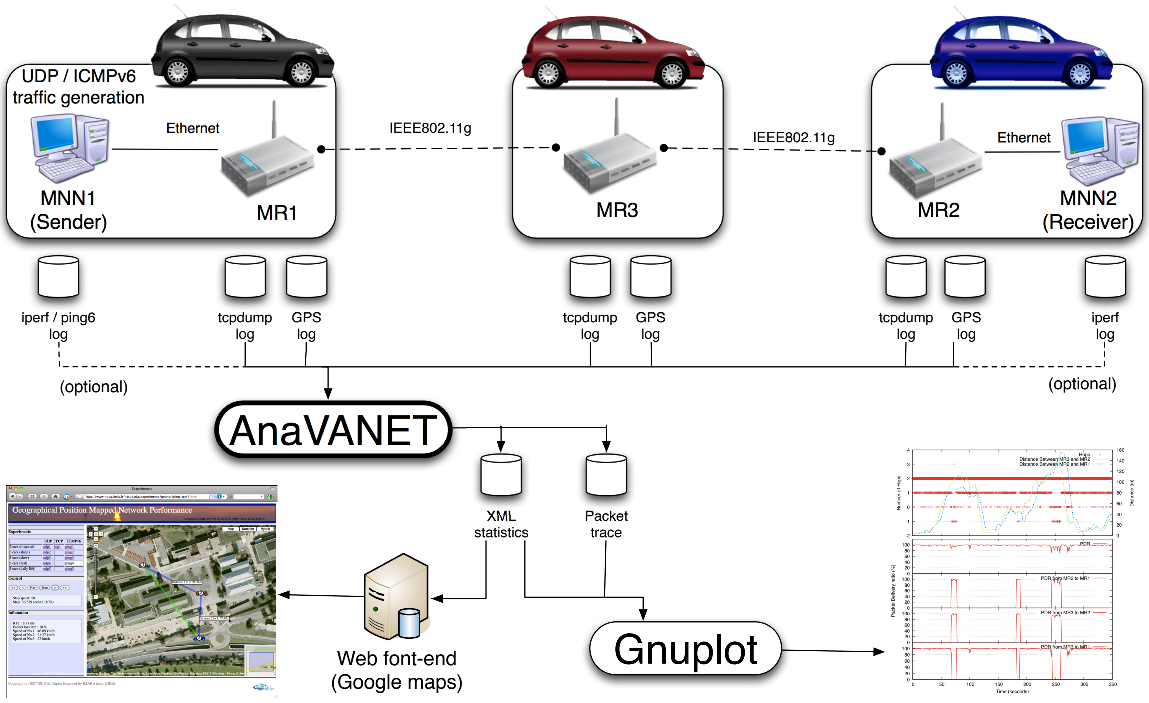


Figure 4.1: AnaVANET: Overview of packet processing and analysis

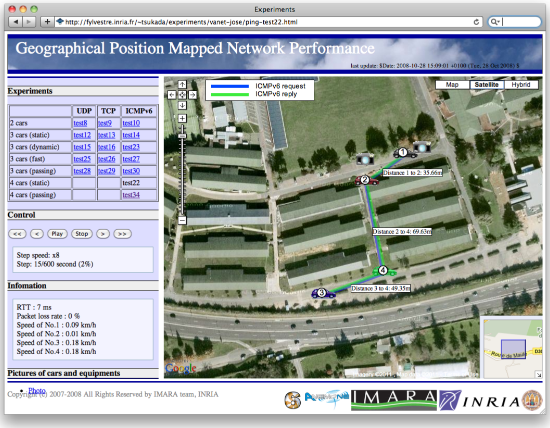
The experiments carried out are available on the websites and can be replayed on a map to see the momentary performance of the network during the tests. Figure 4.2–4.5 show screen shots of these websites. All the experiments can be selected and main performance metrics can be monitored at any time. Users can play and stop at any arbitrary point of the test with the control buttons on the left side of the page. The player speed, one step forward and one step backward are also implemented. On the map, the position and movement of the vehicle are depicted with the speed of each vehicle and the distance between them. The transferred data size, bandwidth, packet loss rate, Round-Trip Time (RTT) and jitter, for each link and end to end are displayed. The network performance is visualized by watching the width of links and the colors used to draw them.

As said, AnaVANET was used in network performance measurement when OLSR is used to create a VANET (Figure 4.2)[1] [Santa2009b, Santa2009a], but also it was the utility used to test GeoNet project implementations (Figure 4.3)[2] [GeoNet-D7.1, Tsukada2010b]. It is currently being used in CarGeo6 evaluation in INRIA (Figure 4.4)[3] [Toukabri2011] and Nara Institute of Science and Technology (NAIST) in Japan (Figure 4.5)[4].

4.2 Basic packet processing

After experiments, the *tcpdump* files and GPS files are collected from all MRss to input the AnaVANET java software. The command in Figure 4.6 shows the case of ICMPv6 evaluation,

[1] http://www-rocq.inria.fr/~tsukada/experiments/vanet-jose/
[2] http://www-rocq.inria.fr/~tsukada/experiments/geonet/
[3] http://www-rocq.inria.fr/~tsukada/experiments/itsnet/
[4] http://dev.inet-lab.me/inet-doc/public/anavanet/



Experiments

http://fylvestre.inria.fr/~tsukada/experiments/vanet-jose/ping-test22.html

Geographical Position Mapped Network Performance

last update: $Date: 2008-10-28 15:09:01 +0100 (Tue, 28 Oct 2008) $

Experiments

	UDP	TCP	ICMPv6
2 cars	test8	test9	test10
3 cars (static)	test12	test13	test14
3 cars (dynamic)	test15	test16	test23
3 cars (fast)	test25	test26	test27
3 cars (passing)	test28	test29	test30
4 cars (static)			test22
4 cars (passing)			test34

Control

Step speed: x8
Step: 15/600 second (2%)

Infomation

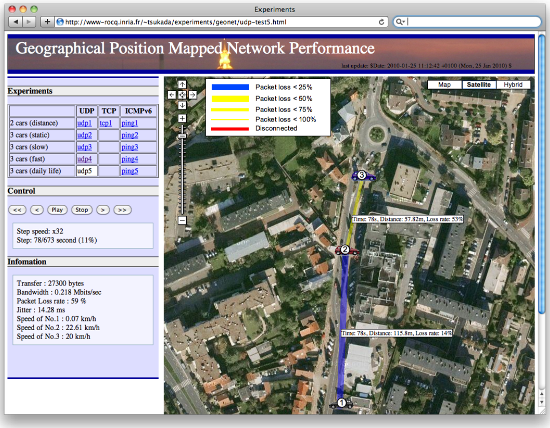
RTT : 7 ms
Packet loss rate : 0 %
Speed of No.1 : 0.09 km/h
Speed of No.2 : 0.01 km/h
Speed of No.3 : 0.18 km/h
Speed of No.4 : 0.18 km/h

Pictures of cars and equipments

- Photo

Copyright (c) 2007-2008 All Rights Reserved by IMARA team, INRIA

Figure 4.2: OLSR measurement



Experiments

http://www-rocq.inria.fr/~tsukada/experiments/geonet/udp-test5.html

Geographical Position Mapped Network Performance

last update: $Date: 2010-01-25 11:12:42 +0100 (Mon, 25 Jan 2010) $

Experiments

	UDP	TCP	ICMPv6
2 cars (distance)	udp1	tcp1	ping1
3 cars (static)	udp2		ping2
3 cars (slow)	udp3		ping3
3 cars (fast)	udp4		ping4
3 cars (daily life)	udp5		ping5

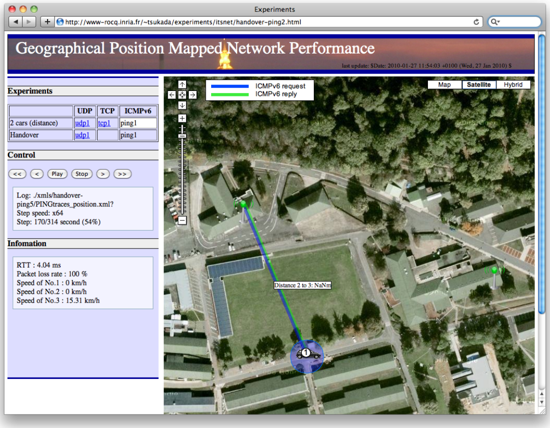
Control

Step speed: x32
Step: 78/673 second (11%)

Infomation

Transfer : 27300 bytes
Bandwidth : 0.218 Mbits/sec
Packet Loss rate : 59 %
Jitter : 14.28 ms
Speed of No.1 : 0.07 km/h
Speed of No.2 : 22.61 km/h
Speed of No.3 : 20 km/h

Figure 4.3: GeoNet measurement



Experiments

http://www-rocq.inria.fr/~tsukada/experiments/itsnet/handover-ping2.html

Geographical Position Mapped Network Performance

last update: $Date: 2010-01-27 11:54:03 +0100 (Wed, 27 Jan 2010) $

Experiments

	UDP	TCP	ICMPv6
2 cars (distance)	udp1	tcp1	ping1
Handover	udp1		ping1

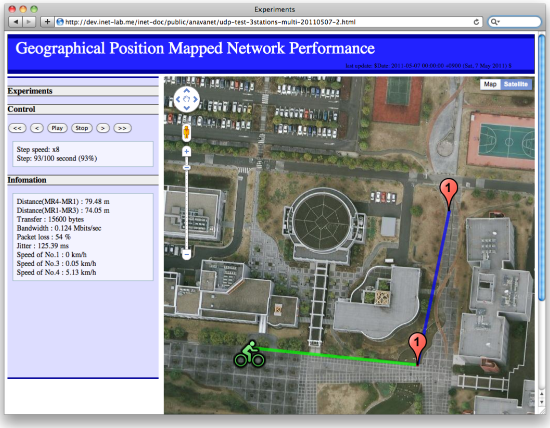
Control

Log: ./xmls/handover-ping5/PINGtraces_position.xml?
Step speed: x64
Step: 170/314 second (54%)

Infomation

RTT : 4.04 ms
Packet loss rate : 100 %
Speed of No.1 : 0 km/h
Speed of No.2 : 0 km/h
Speed of No.3 : 15.31 km/h

Figure 4.4: CarGeo6 measurement (INRIA)



Experiments

http://dev.inet-lab.me/inet-doc/public/anavanet/udp-test-3stations-multi-20110507-2.html

Geographical Position Mapped Network Performance

last update: $Date: 2011-05-07 00:00:00 +0900 (Sat, 7 May 2011) $

Experiments

Control

Step speed: x8
Step: 93/100 second (93%)

Infomation

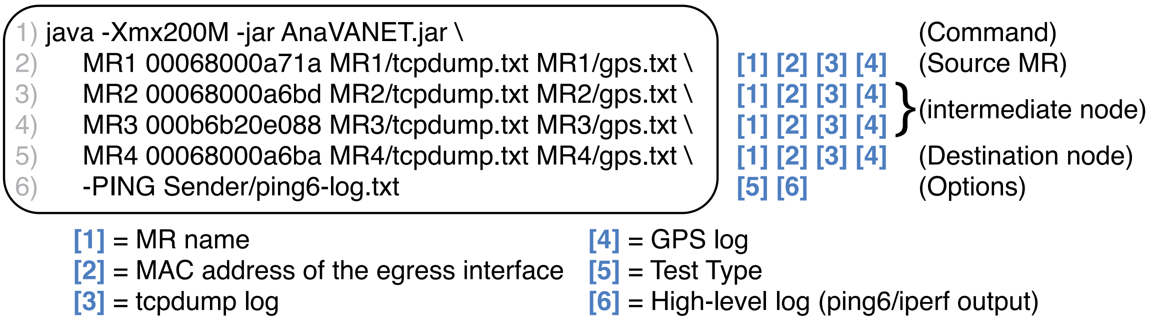
Distance(MR4-MR1) : 79.48 m
Distance(MR1-MR3) : 74.05 m
Transfer : 15600 bytes
Bandwidth : 0.124 Mbits/sec
Packet loss : 54 %
Jitter : 125.39 ms
Speed of No.1 : 0 km/h
Speed of No.3 : 0.05 km/h
Speed of No.4 : 5.13 km/h

Figure 4.5: CarGeo6 measurement (NAIST)

however TCP and UDP evaluation shares the command except for the last line.

The first line of the command launches AnaVANET whereas the other lines provide configuration parameters. The second line gives the information of the source MR where attached MNN generates the ICMPv6 echo request. The name of the MR, the MAC address of the egress interface, *tcpdump* log and GPS log (see Figure 4.8) are given as parameters. Lines 3 and 4 are information of intermediate nodes, which actually can be repeated for each intermediate node. The parameters of intermediate nodes are the same as the one used in the second line. Line 5 configures the destination MR where the attached MNN receives the ICMPv6 Echo Requests and replies ICMPv6 with Echo Reply messages to the attached MNN to source MR. The parameters are described as well. The last line defines the test type (PING, UDP and TCP) and specifies the file of high-level log (the output of *ping6* or the evaluation tool *Iperf*, depending on the test type).

Figure 4.7 shows the functional modules of AnaVANET. Non-colored rectangles are the basic modules that the initial AnaVANET implementation had, and colored modules are extensions of Geonetworking, NEMO and handover scenarios described in the following sections. The packet processing starts from top, and the results of the processing is recorded to the per-packet trace file (text file) and per-second statistics file (XML file compatible with Google Maps). There are six steps in the AnaVANET processing, as it is depicted in Figure



```
java -Xmx200M -jar AnaVANET.jar \
    MR1 00068000a71a MR1/tcpdump.txt MR1/gps.txt \
    MR2 00068000a6bd MR2/tcpdump.txt MR2/gps.txt \
    MR3 000b6b20e088 MR3/tcpdump.txt MR3/gps.txt \
    MR4 00068000a6ba MR4/tcpdump.txt MR4/gps.txt \
    -PING Sender/ping6-log.txt
```

(Command)
[1] [2] [3] [4] (Source MR)
[1] [2] [3] [4]
[1] [2] [3] [4] (intermediate node)
[1] [2] [3] [4] (Destination node)
[5] [6] (Options)
[1] = MR name
[2] = MAC address of the egress interface
[3] = tcpdump log
[4] = GPS log
[5] = Test Type
[6] = High-level log (ping6/iperf output)

Figure 4.6: Command used to launch AnaVANET

4.7: GPS log processing, *tcpdump* log processing, packet tracing and statistics, high-level log matching and output file generation. AnaVANET traces the packets for UDP and ICMPv6, because TCP packets are resent from the MNN with the same sequence number when the packet is lost. This makes mis-processing (double counting) for packet trace. TCP test only considers vehicles' position and end-to-end performance taken from *Iperf* log (first, fifth and sixth step are considered in Figure 4.7.)

As a first step, AnaVANET processes GPS log. With the file, first, AnaVANET synchronizes the time between *tcpdump* log recorded with hardware time and GPS log that recorded with GPS time. The GPS log is described in National Marine Electronics Association (NMEA) format as shown in Figure 4.8. The hardware time recorded in *tcpdump* logs present drifts among MRs, because it is very difficult to synchronize the time of many devices for a long time in second order. On the other hand, the GPS time given by satellite is always synchronized when devices are located in almost the same place. Thus the GPS time is used for the rest of the calculation for the packet processing. The hardware time recorded in *tcpdump* file is calibrated with GPS time by calculating the gap between GPS and the hardware time in the beginning of the processing.

As shown in Figure 4.8, the line that starts with $\$GPRMC$ in the GPS file gives the position of the vehicle and speed. AnaVANET uses this information for distance calculation between each pair of vehicles.

When the ITS Station's latitude and longitude are defined as $lat1$ and $long1$ and a neighbor ITS Station's latitude and longitude are defined as $lat2$ and $long2$, the distance d to the neighbor ITS Station is given by the *Haversine* formula shown in equation 4.1, where $R = 6378.7km\,(earth's\,radius)$.

$$d = R \cdot acos\left[sin\left(lat1\right) \cdot sin\left(lat2\right) + cos\left(lat1\right) \cdot cos\left(lat2\right) \cdot cos\left(long2 - long1\right)\right] \qquad (4.1)$$

In the next step, *tcpdump* log is processed. All the packets in the log are stored in the packet hash table with the time, source MAC address, destination MAC address, source IPv6 address, destination IPv6 address, packet type and sequence number. Only packets which match to the test type (ICMPv6, TCP, UDP) given in the command line option are considered, while the other packets are ignored (*i.e.* beacons). The *tcpdump* log is a text file as shown in Figure 4.9 (it shows the case of ICMPv6 test). The first line shows important packet attributes including time, source IPv6 address, destination IPv6 address, packet type and sequence number. The time is recorded by the hardware time, thus it is converted to the GPS time and stored to the hash table. Then AnaVANET takes the source and destination addresses from the first 48 bits and the next 48 bits.

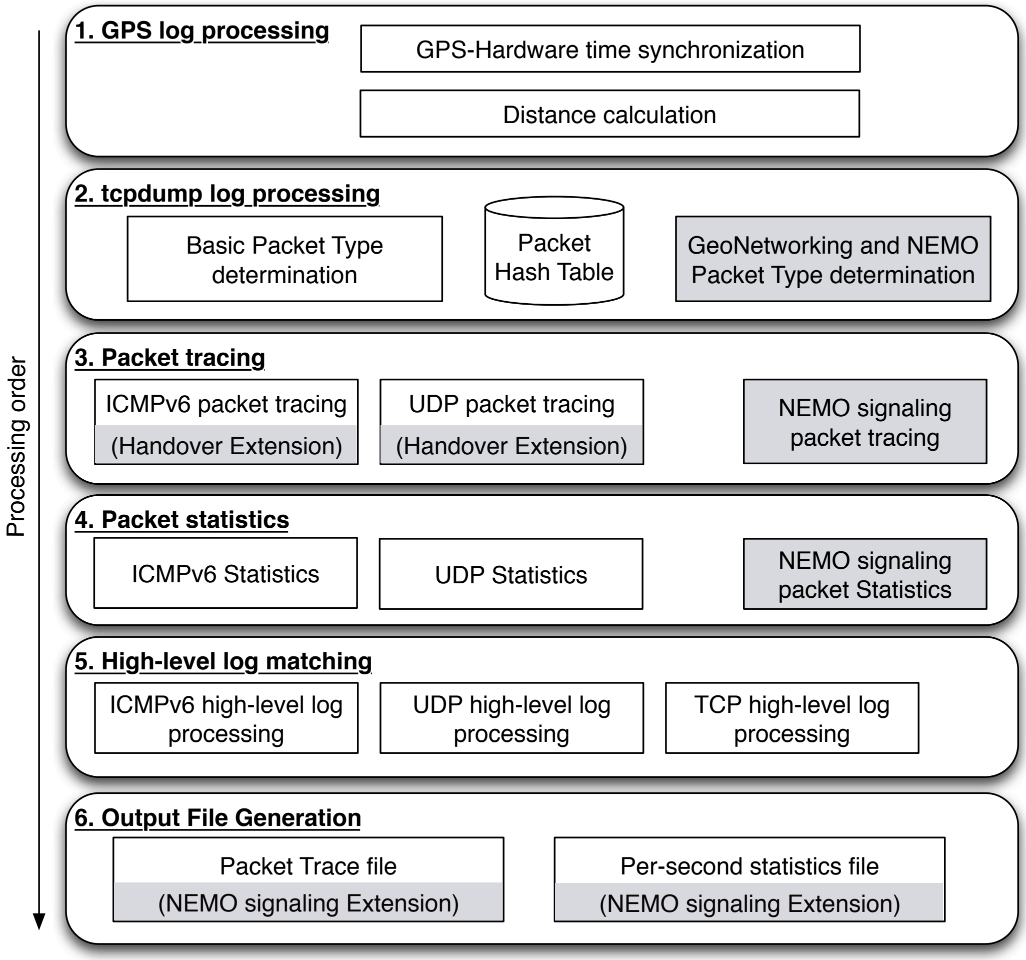
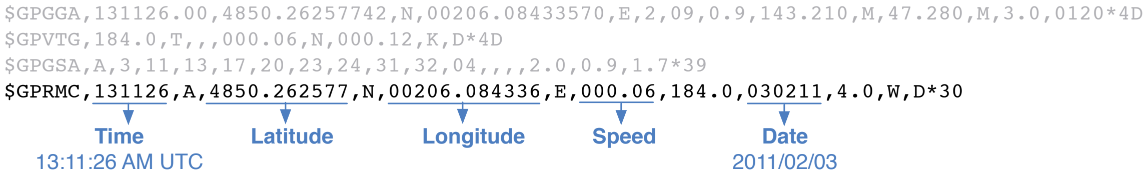

Processing order
1. GPS log processing
GPS-Hardware time synchronization
Distance calculation
2. tcpdump log processing
Basic Packet Type determination
Packet Hash Table
GeoNetworking and NEMO Packet Type determination
3. Packet tracing
ICMPv6 packet tracing
(Handover Extension)
UDP packet tracing
(Handover Extension)
NEMO signaling packet tracing
4. Packet statistics
ICMPv6 Statistics
UDP Statistics
NEMO signaling packet Statistics
5. High-level log matching
ICMPv6 high-level log processing
UDP high-level log processing
TCP high-level log processing
6. Output File Generation
Packet Trace file
(NEMO signaling Extension)
Per-second statistics file
(NEMO signaling Extension)

Figure 4.7: AnaVANET software modules

After interesting packets have been identified and stored, in the next step (packet tracing) packets are traced based on the MAC address stored in the packet hash table. The trace starts from the sender MR and then the software checks if the packet has been received by the next MR, according to the destination MAC address of the traced packet. This check continues successively until the packet arrives the destination given by the command or it is lost (if it is not received by one of the MR marked as the next hop. In the ICMPv6 case, the Echo Reply packet is matched with Echo Request by the sequence number. The check continues successively from destination MR to the source MR again, which finally receives the reply packet. The result is used for the per-packet packet log in step 6 (Output file generation) in Figure 4.7.

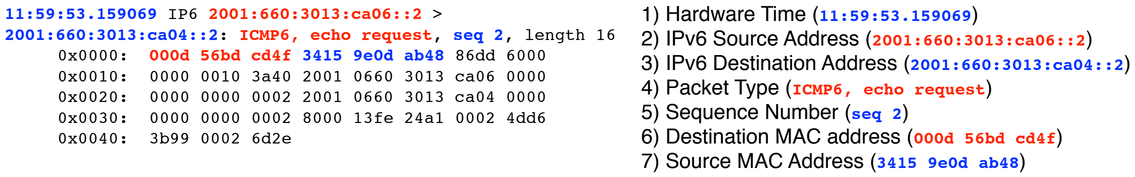
The Packet Delivery Ratio (PDR) for each link are calculated a rate of 1 Hz. For example, in the scenario with three MR, all the links are MR1 → MR2, MR1 → MR3, MR2 → MR1, MR2 → MR3, MR3 → MR1 and MR3 → MR2. The PDR is calculated by the number of arrived packet divided by number of sent packets on the link.

In high-level log matching, AnaVANET processes the test file outputed by *ping6* or *Iperf*. The result of the processing is matched to the previous result in packet statistics (step 4). In ICMPv6 tests, the *ping6* output in the sender is processed, which includes the RTT between the sender and receiver in each second. When UDP is used, the *Iperf* output in the receiver



```
$GPGGA,131126.00,4850.26257742,N,00206.08433570,E,2,09,0.9,143.210,M,47.280,M,3.0,0120*4D
$GPVTG,184.0,T,,,000.06,N,000.12,K,D*4D
$GPGSA,A,3,11,13,17,20,23,24,31,32,04,,,,2.0,0.9,1.7*39
$GPRMC,131126,A,4850.262577,N,00206.084336,E,000.06,184.0,030211,4.0,W,D*30
```

Figure 4.8: GPRMC sentence in GPS log



```
11:59:53.159069 IP6 2001:660:3013:ca06::2 >
2001:660:3013:ca04::2: ICMP6, echo request, seq 2, length 16
        0x0000:  000d 56bd cd4f 3415 9e0d ab48 86dd 6000
        0x0010:  0000 0010 3a40 2001 0660 3013 ca06 0000
        0x0020:  0000 0000 0002 2001 0660 3013 ca04 0000
        0x0030:  0000 0000 0002 8000 13fe 24a1 0002 4dd6
        0x0040:  3b99 0002 6d2e
```

1) Hardware Time (11:59:53.159069)
2) IPv6 Source Address (2001:660:3013:ca06::2)
3) IPv6 Destination Address (2001:660:3013:ca04::2)
4) Packet Type (ICMP6, echo request)
5) Sequence Number (seq 2)
6) Destination MAC address (000d 56bd cd4f)
7) Source MAC Address (3415 9e0d ab48)

Figure 4.9: IPv6 native packet processing

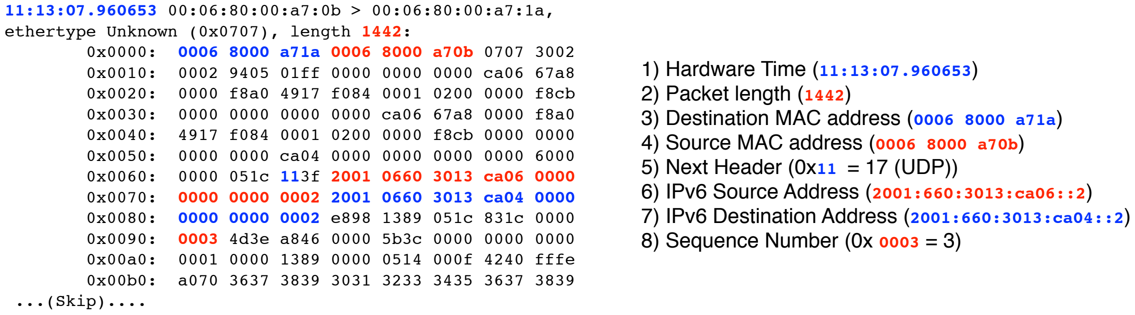
side is processed, which includes the transferred bytes, the bandwidth and the jitter. In TCP tests, the output of *Iperf* is recorded at the sender point, including the transferred bytes and the bandwidth.

The final step is the generation of two output files. One file includes all information about the per-packet trace study as a result of step 3. It records the packet itinerary from the source MR to the destination MR (it may be dropped somewhere) with the transmitted time and number of hops. This file is generated only for UDP and ICMPv6 tests. The other file includes per-second statistics as a result of step 4 and 5. The file is an XML structure that can be used for displaying results on Google maps.

4.3 Geonetworking Packet Processing

AnaVANET has been extended to process packet with the Geonetworking header. The extended module is the packet type determination in *tcpdump* log processing (step 2) in Figure 4.7. In command line, $-GeoNet$ option switches using from Basic packet type determination to Geonetworking packet type determination. The extended packet type determination considers 80 octets of the Geonetworking header.

Figure 4.10 shows an example of Geonetworking packet type determination. First of all, the first line of *tcpdump* log does not give the attribute of the packet unlike IPv6 native packets. The line gives only the recorded time and packet size. AnaVANET takes the source and destination MAC address from second line (line of $0x0000$). In order to determine the packet type, it should see the next header field in the IPv6 header, which is marked $0x11 = 17$ in Figure 4.10. In the example, as the protocol number 17 means UDP, AnaVANET can determine the packet type (When the protocol number is $0x3a = 58$, it is ICMPv6 packet. This is the case of the example provided in Figure 4.11 in the next section). Then from the IPv6 header, the IPv6 source and destination address are taken. The first four digits of line $0x0090$ is a sequence number of the UDP packet. The number is used as an identification number of the packet in AnaVANET. The packet information taken above is stored in the packet hash table as well as IPv6 native packet. The rest of the processing is the same described in Section 4.2.



```
11:13:07.960653 00:06:80:00:a7:0b > 00:06:80:00:a7:1a,
ethertype Unknown (0x0707), length 1442:
        0x0000:  0006 8000 a71a 0006 8000 a70b 0707 3002
        0x0010:  0002 9405 01ff 0000 0000 0000 ca06 67a8
        0x0020:  0000 f8a0 4917 f084 0001 0200 0000 f8cb
        0x0030:  0000 0000 0000 0000 ca06 67a8 0000 f8a0
        0x0040:  4917 f084 0001 0200 0000 f8cb 0000 0000
        0x0050:  0000 0000 ca04 0000 0000 0000 0000 6000
        0x0060:  0000 051c 113f 2001 0660 3013 ca06 0000
        0x0070:  0000 0000 0002 2001 0660 3013 ca04 0000
        0x0080:  0000 0000 0002 e898 1389 051c 831c 0000
        0x0090:  0003 4d3e a846 0000 5b3c 0000 0000 0000
        0x00a0:  0001 0000 1389 0000 0514 000f 4240 fffe
        0x00b0:  a070 3637 3839 3031 3233 3435 3637 3839
 ...(Skip)....
```

1) Hardware Time (11:13:07.960653)
2) Packet length (1442)
3) Destination MAC address (0006 8000 a71a)
4) Source MAC address (0006 8000 a70b)
5) Next Header (0x11 = 17 (UDP))
6) IPv6 Source Address (2001:660:3013:ca06::2)
7) IPv6 Destination Address (2001:660:3013:ca04::2)
8) Sequence Number (0x 0003 = 3)

Figure 4.10: Packet with Geonetworking Header

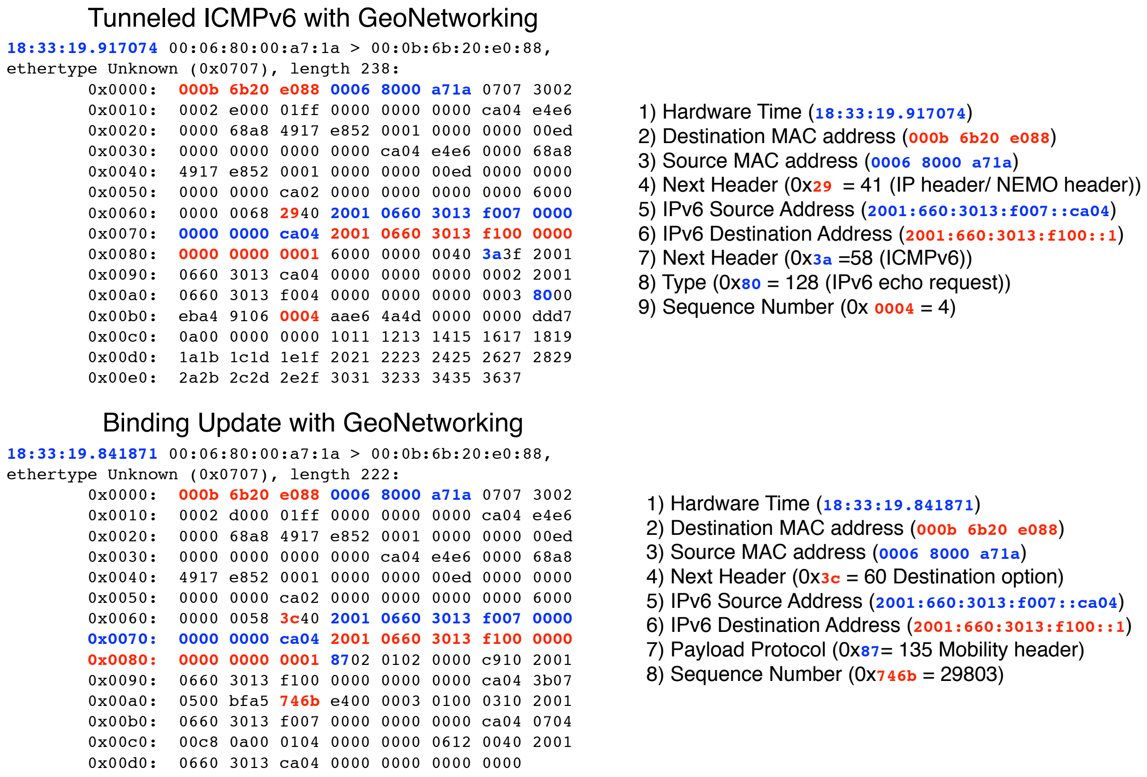
4.4 NEMO packet processing

NEMO extension to AnaVANET consists of two parts: packet type determination with NEMO header (actually IPv6 header, 40 octets) and NEMO signaling packet processing. The packet type determination with NEMO header is added to the *tcpdump* log processing (step 2 in Figure 4.7). Regarding NEMO signaling processing, three parts are extended, that are NEMO signaling processing added to packet tracing (step 3), NEMO signaling statistics added to the packet statistics (step4) and NEMO signaling extension added to the output file generation (step 6). All the NEMO extension functions are activated with $-NEMO$ option in command line.

In *tcpdump* log processing (step 2), the NEMO header should be considered for the packet type determination. Figure 4.11 shows an example with a packet with the NEMO header and Geonetworking header. The first line of the *tcpdump* log does not give the packet attributes except for the recorded time as well as in the previous section, because it is also encapsulated with the Geonetworking header. The source and destination MAC addresses are given in the first line as well. After the Geonetworking header, the IPv6 header appears (line $0x0060$). The next header field ($0x29 = 41$) in the line shows that the packet is encapsulated by IPv6 header (NEMO header). When AnaVANET discovers the NEMO header, it looks for an inner packet in order to determine the packet type. After the 40 octets of the NEMO header, it shows the inner IPv6 header. In the example of Figure 4.11, the next header field of the inner IPv6 packet has $0x3a = 58$, which means that the next header is ICMPv6. The first two digits of the next header shows that the packet is whether an ICMPv6 Echo Request ($0x80 = 128$) or an ICMPv6 Echo Reply ($0x81 = 129$) message. At that point, the packet type is determined completely, and then the sequence number is taken from the line $0x00b0$ and it is used as the identifier of the packet in the rest of the process.

The NEMO signaling packets (BU and BA) are also processed when the $-NEMO$ option is enabled. An example of a BU message is illustrated in Figure 4.11. As well as the other packet with Geonetworking, the recorded time, source MAC address and destination MAC address are detected. Then it checks the next header field in the IPv6 header. For the case of BU, the destination option ($0x3c = 60$) is specified in the field. (In case of a BA, the IPv6 routing header ($0x2b = 43$) would be specified). In both cases, BU and BA, the payload protocol is specified as mobility header ($0x78 = 135$). The sequence number of the BU and BA is used as identification number to match the correspondent NEMO signaling message. The packet information is stored in the packet hash table as well as the other packets.

The other function of NEMO extension is tracing NEMO signaling and statistics. The NEMO signaling is traced in order to analyze if the binding registration is terminated successfully or not, and where the signaling packet is dropped at packet tracing (step 3). First,



Tunneled ICMPv6 with GeoNetworking

```
18:33:19.917074 00:06:80:00:a7:1a > 00:0b:6b:20:e0:88,
ethertype Unknown (0x0707), length 238:
        0x0000:  000b 6b20 e088 0006 8000 a71a 0707 3002
        0x0010:  0002 e000 01ff 0000 0000 0000 ca04 e4e6
        0x0020:  0000 68a8 4917 e852 0001 0000 0000 00ed
        0x0030:  0000 0000 0000 0000 ca04 e4e6 0000 68a8
        0x0040:  4917 e852 0001 0000 0000 00ed 0000 0000
        0x0050:  0000 0000 ca02 0000 0000 0000 0000 6000
        0x0060:  0000 0068 2940 2001 0660 3013 f007 0000
        0x0070:  0000 0000 ca04 2001 0660 3013 f100 0000
        0x0080:  0000 0000 0001 6000 0000 0040 3a3f 2001
        0x0090:  0660 3013 ca04 0000 0000 0000 0002 2001
        0x00a0:  0660 3013 f004 0000 0000 0000 0003 8000
        0x00b0:  eba4 9106 0004 aae6 4a4d 0000 0000 ddd7
        0x00c0:  0a00 0000 0000 1011 1213 1415 1617 1819
        0x00d0:  1a1b 1c1d 1e1f 2021 2223 2425 2627 2829
        0x00e0:  2a2b 2c2d 2e2f 3031 3233 3435 3637
```

1) Hardware Time (18:33:19.917074)
2) Destination MAC address (000b 6b20 e088)
3) Source MAC address (0006 8000 a71a)
4) Next Header (0x29 = 41 (IP header/ NEMO header))
5) IPv6 Source Address (2001:660:3013:f007::ca04)
6) IPv6 Destination Address (2001:660:3013:f100::1)
7) Next Header (0x3a =58 (ICMPv6))
8) Type (0x80 = 128 (IPv6 echo request))
9) Sequence Number (0x 0004 = 4)

Binding Update with GeoNetworking

```
18:33:19.841871 00:06:80:00:a7:1a > 00:0b:6b:20:e0:88,
ethertype Unknown (0x0707), length 222:
        0x0000:  000b 6b20 e088 0006 8000 a71a 0707 3002
        0x0010:  0002 d000 01ff 0000 0000 0000 ca04 e4e6
        0x0020:  0000 68a8 4917 e852 0001 0000 0000 00ed
        0x0030:  0000 0000 0000 0000 ca04 e4e6 0000 68a8
        0x0040:  4917 e852 0001 0000 0000 00ed 0000 0000
        0x0050:  0000 0000 ca02 0000 0000 0000 0000 6000
        0x0060:  0000 0058 3c40 2001 0660 3013 f007 0000
        0x0070:  0000 0000 ca04 2001 0660 3013 f100 0000
        0x0080:  0000 0000 0001 8702 0102 0000 c910 2001
        0x0090:  0660 3013 f100 0000 0000 0000 ca04 3b07
        0x00a0:  0500 bfa5 746b e400 0003 0100 0310 2001
        0x00b0:  0660 3013 f007 0000 0000 0000 ca04 0704
        0x00c0:  00c8 0a00 0104 0000 0000 0612 0040 2001
        0x00d0:  0660 3013 ca04 0000 0000 0000 0000
```

1) Hardware Time (18:33:19.841871)
2) Destination MAC address (000b 6b20 e088)
3) Source MAC address (0006 8000 a71a)
4) Next Header (0x3c = 60 Destination option)
5) IPv6 Source Address (2001:660:3013:f007::ca04)
6) IPv6 Destination Address (2001:660:3013:f100::1)
7) Payload Protocol (0x87= 135 Mobility header)
8) Sequence Number (0x746b = 29803)

Figure 4.11: Packet with NEMO and Geonetworking

the BU sent from source MR is traced successively by source and destination MAC address until arriving at the destination node (Access Point (AP)). When the BU arrives at an access router (AR), the correspondent BA is also traced until it reaches to the source MR. The two-way packets trace file (BU and BA) is generated in the step 6 in Figure 4.7.

When logging the NEMO signaling status, three statuses are recorded in the per-second statistics file: NEMO signaling not sent (0), NEMO signaling successful (1) and NEMO signaling unsuccessful (2).

4.5 Processing for handover scenarios

AnaVANET was initially designed for analyzing unicast vehicle-based communication. Thus the source MR and destination MR are given in the command line. This does not cause problems in the case of roadside-based communication, however, new problems arise when Internet-based communication is used, because there are multiple exits (destinations) from the VANET point of view upon the case of handover between APs. The packet from the source MR goes out of the VANET in an AP, but the AP may change depending on the movement of the vehicle. Thus the AnaVANET trace system should have multiple destinations. The multiple destination option is specified with the argument $-destMR\,number$ option in the command line. With this option, AnaVANET traces the packet until reaching the specified destination in packet trace (step 3). ICMPv6 packets (Echo Request and Echo Reply) and NEMO signaling (BU and BA) are traced from the selected destination to the source MR.

CHAPTER 5

Cases of study

5.1 Case of study 1: network mobility support

The aim of this case of study is testing the operation of NEMO under real conditions and considering different domains and communication technologies.

The project technologies tested in this case of study are:

- UMTS/3G
- 802.11b
- NEMO
- 6o4 tunneling

5.1.1 Scenario description

5.1.1.1 Overall architecture

The scenario considered for this case of study is a simplification of the general scenario described above, where nodes have been distributed at UMU installations. The overall picture of the scenario is showed in Figure 5.1.

As can be seen, the Home Central ITS Station is placed indoors, in one of the laboratories of UMU. Two physical domains are considered, the one provided by the Home Central ITS-S (home domain), trough a 6o4 tunnel over 3G, and a visited domain provided by a Visited Roadside ITS-S. However, two different domains could be set-up within the WiFi area. The 802.11b support has been physically provided by two antennas and an access point installed on the top of a faculty located on the centre of the UMU campus, as can be seen in Figure 5.2. Since the Visited Central ITS-S does not provide any service to vehicles, it has been omitted, and ITS-S Border Router capabilities of the Roadside ITS Station are used to connect with the outer network. 802.11b is used to provide a medium/short-range wireless communication capabilities from the roadside equipment, since 802.11p media are not available in the frame of the project yet. A physical embedded computer installed together with the access point integrates the required router capabilities. Vehicles drive around the campus, which has a

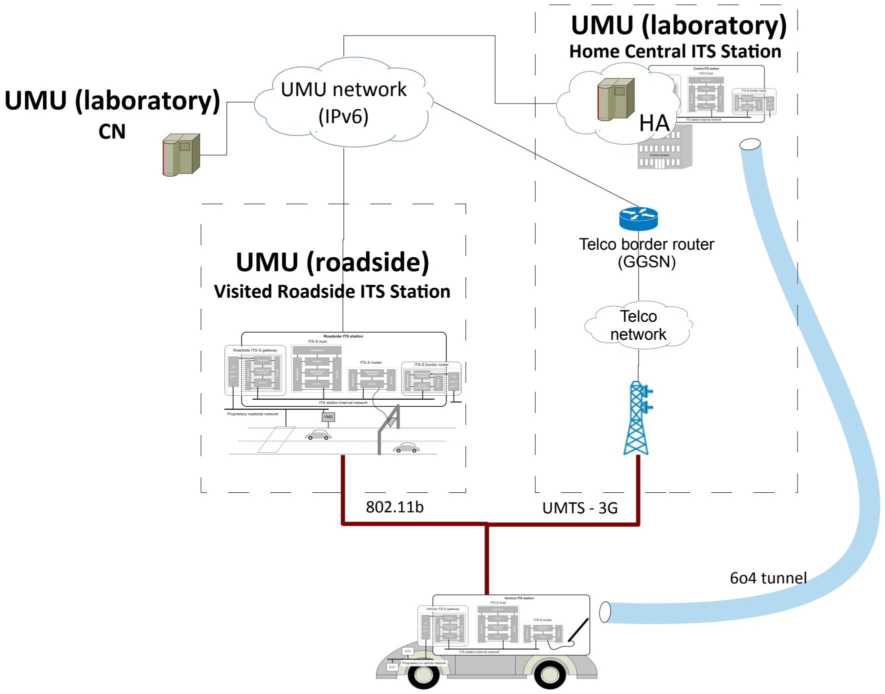


Figure 5.1: Scenario for case of study 1

good 3G coverage everywhere, but only a stretch of about 780m of the path is provided with 802.11 coverage by means of the two high-gain antennas, as can be seen in Figure 5.3.

Finally, a correspondent node (CN), i.e. a common networked host, has been placed in one of our laboratories to provide an edge for evaluating data connections under mobility. A common vehicle is used to carry an embedded computer which provides ITS-S router capabilities (mobile router) to the Vehicle ITS-S.

5.1.1.2 Network design

The network architecture of the scenario is depicted in Figure 5.4. A direct equivalence can be found between the overall architecture presented above and the network view. In the diagram, it is showed the path followed by Router Advertisement (RA) messages, which are sent through the two available communication routes, the one supported by means of a WiFi access, and the one provided by using the 3G operator's infrastructure.

The addressing scheme is also showed in Figure 5.4. As can be noted, all IPv6 addresses are fake and they have been used only for testing purposes. Moreover, two access routers are used, the one located in the visited Roadside ITS-S and the one remotely provided through the 3G link. This last access router is also used as the edge of the 6o4 tunnel.

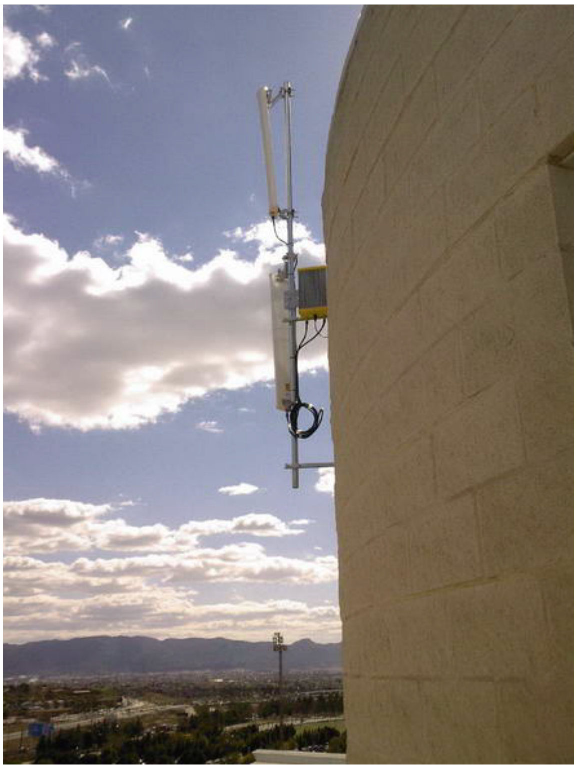


Figure 5.2: Access point used to provide 802.11b connectivity

5.1.1.3 Testbed set-up

A summary of the hardware components used in the tests is provided in Table 5.1. As relevant software modules, the NEMO implementation UMIP 0.4 and the IKEv2 software OpenIKEv2 0.96 have been used. Although the current ITSSv6 software packet has not been used, due to a network selection module is still pending to work on wireless interfaces, all relevant software modules, including the previous ones, are the same included in the project software distribution.

Additionally a list of the most important configuration parameters used in several components of the testbed is provided in Table 5.2.

5.1.2 Technological validation of protocols (control and management)

Since the main feature to be tested is mobility, the NEMO operation is studied in detail, in order to analyse the operation of the protocol when a handoff between different technologies and/or network domains occurs.

5.1.2.1 Traffic

The NEMO messages that are analysed are:

- Binding Update (BU).
- Binding Acknowledgement (BA).

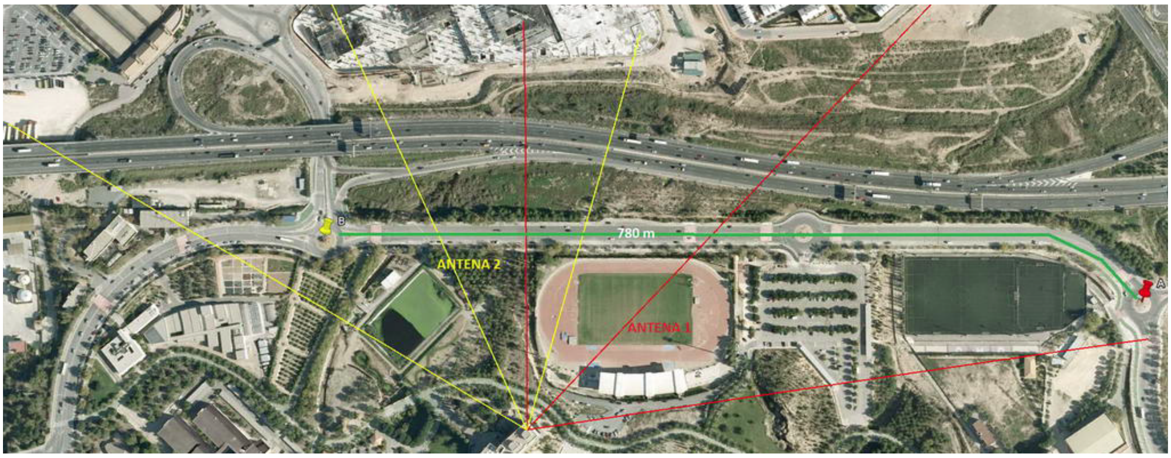


Figure 5.3: Stretch provided with 802.11b connectivity

Table 5.1: Hardware components used in case of study 1

Node	Hardware	Software
Mobile Router	PC Asus EB1501P, Atom 1.8 Ghz, 2 GB	Ubuntu 10.4
Host	Laptop Asus K52JK, Intel i5, 4GB	Ubuntu 10.4
Home Agent (HA)	Mini-ITX PC, Via 532Mhz/476MB	Ubuntu 10.4
Home Internal Router	PC Intel P-4, 2 GB	Ubuntu 10.4
Access Router 2	PC Intel i5, 3.1 Ghz, 3 GB	Ubuntu 10.4
UMU border router	<High-end router>	<Proprietary software>
Correspondent Node (CN)	PC Intel Core 2 Duo, 2 GB	Ubuntu 10.4
Access Router 1	Mini-ITX PC, Via 532Mhz/476MB	Ubuntu 10.4
Wide-Range WiFi AP	Lobometrics Lobo 924TS	<Proprietary software>
Wide-Range WiFi client	Alfa AWUS036H	<Proprietary software>
3G USB	Novatel Ovation MC950D	<Proprietary software>

5.1.2.2 Evaluation tool

The software tools used to analyse the previous traffic are:

- *tcpdump*, which is used to collect signaling traffic from the mobile router.
- UNIX command-line tools to filter the results.

5.1.2.3 Metrics

The metrics considered for analysing signalling traffic in mobility are:

- BU/BA round-trip delay time, while the mobile router performs a handoff.
- Overall attachment time consumed in the handoffs. This metric comprises both network and link-layer processes, that are analysed as a unique block to be studied for the two technologies considered: 3G and WiFi 802.11b.

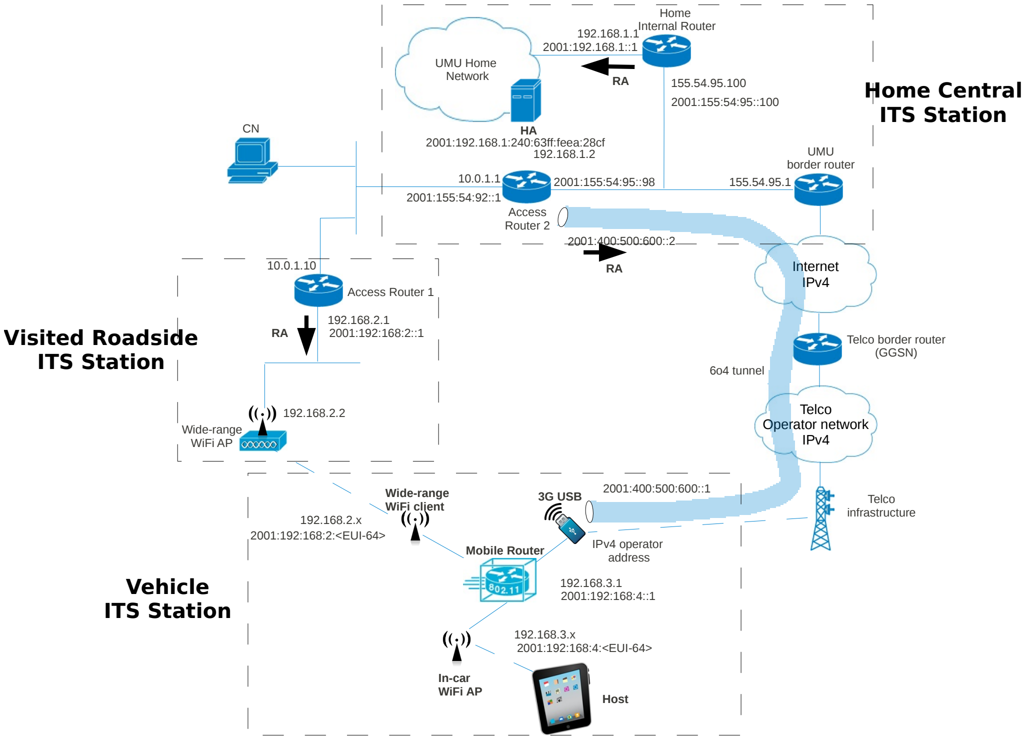


Figure 5.4: Network design for case of study 1

5.1.3 Performance analysis (data traffic)

A common Internet-equivalent data flow is used to test the performance of the network under mobility conditions, maintaining a data link between the mobile router and a correspondent node located at the infrastructure side.

5.1.3.1 Traffic

The types of traffic considered for the tests are:

- Transmission Control Protocol (TCP). A data flow at the maximum allowable speed is generated from the in-vehicle host to the CN.

Table 5.2: Configuration parameters used in case of study 1

Node	Parameter	Value
Access Router 1	Router Advertisement (RA) rate	1 - 3 secs
Access Router 2	Router Advertisement (RA) rate	2 - 4 secs
Home Internal Router	Router Advertisement (RA) rate	1 - 3 secs
Mobile Router	Max. Binding Lifetime	30 secs

- User Datagram Protocol (UDP). A data flow is generated from the CN to the in-vehicle host at a rate of 500 Kbps, and in the opposite direction.

- Internet Control Message Protocol (ICMP). A ping-like flow is generated from the in-vehicle host to the CN at a rate of one ICMP request message per second, and in the opposite direction.

5.1.3.2 Evaluation tool

The software tools considered in the test are *Iperf* (UDP and TCP) and *ping6* (ICMP). These tools are called through a set of scripts that can be found in Appendix A.

5.1.3.3 Metrics

The metrics considered for the tests are:

- Delay
- Bandwidth
- Jitter
- Packet Delivery Ratio

5.1.4 Detailed description of the test

The purpose of the test is checking the operation of the mobility procedures and observe the performance of a data channel maintained during the handoffs. In the test, the vehicle moves within the Espinardo Campus at the University of Murcia (see Figure 5.3), taking advantage of both the 3G connectivity and the limited 802.11b coverage.

The list of steps that detail the test carried out can be found next:

1. The vehicle (MR) starts communicating through its home domain, through 3G.

2. The vehicle (MR) is moving and leaves its home domain. It enters in a visited domain with a different communication technology (WiFi): inter-domain and inter-technology.

3. While the data connection is still maintained by the old data path through 3G, the vehicle (MR) connect to the WiFi AP, but it needs to gain network access obtaining a new CoA with the new RSU. This is performed once the a RA message is received.

4. Mobility procedure is activated, and the new CoA is registered in HA to change the data path used in both up and down directions.

5. The vehicle keeps moving, and leaves its current point of attachment (RSU) and connects through 3G to its home domain: intra-domain and intra-technology.

6. Steps 3 and 4 are executed.

5.1.5 Preliminary results

The previous test plan has been carried out three times, considering TCP and UDP data traffic generated by *Iperf*, and ICMP data traffic using the *ping6* utility. Most important results are presented in this part. The scripts used to execute the test are included in Appendix A.

The bandwidth results obtained in the TCP test are showed in Figure 5.5. As can be seen, the slow-start algorithm of TCP tries to adapt to the wireless medium for both the 3G and WiFi cases. Moreover, the bandwidth of the network is also affected by the movement of the vehicle. The test starts by using the 3G network, and then two handoffs occur: the first one from 3G to WiFi, just after time 300 sec., and the second one, from WiFi to 3G at time 440 sec. At these moments the communication is blocked for a while, but there are not packet losses thanks to TCP retransmissions. It is evident the quite better performance obtained while the WiFi infrastructure is used, with a maximum of 2.4 Mbps. The performance when using 3G is maintained around 0.4 Mbps. After the second handoff, the network evidences some problems to stabilize, what is due to the distance to the UMTS base station now and the location of the vehicle at a small valley, which make communication with the base station more difficult. Until the vehicle reaches a higher position and the HSPA adaptation module stabilizes according to the signal quality.

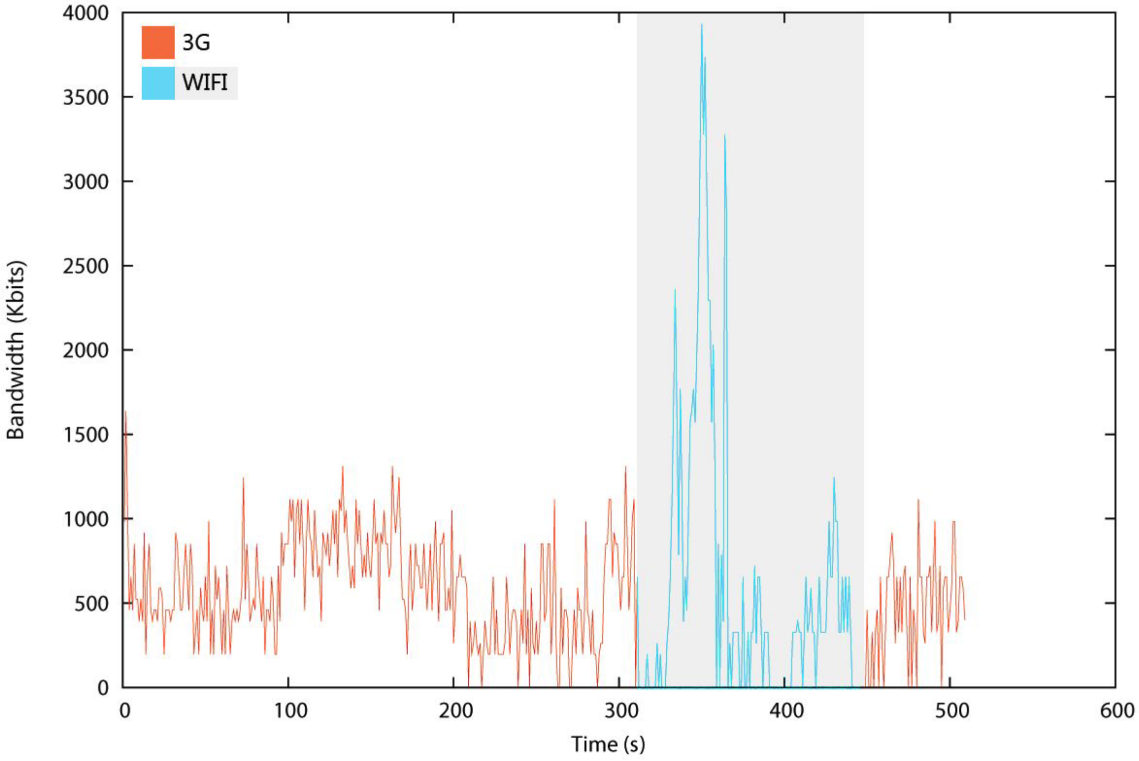


Figure 5.5: Bandwidth evaluation for case of study 1

The PDR results of the mobility system are plotted in Figure 5.6. The data transmission have been performed from the CN located at the infrastructure to the vehicle host, hence evaluating the downlink channel. The handoff from 3G to WiFi is again evident between times 320 sec. and 430 sec. Although the achievable bandwidth is potentially higher in this stretch of the testing path, as it has been showed above, the amount of packet losses is higher than when the 3G link is used. This is due to the distance to the WiFi access point and the fact that the 802.11b technology is not suitable for providing a reliable connectivity to moving terminals. Anyway good results are obtained taking into account that the access point is about 300 m far away of the vehicle.

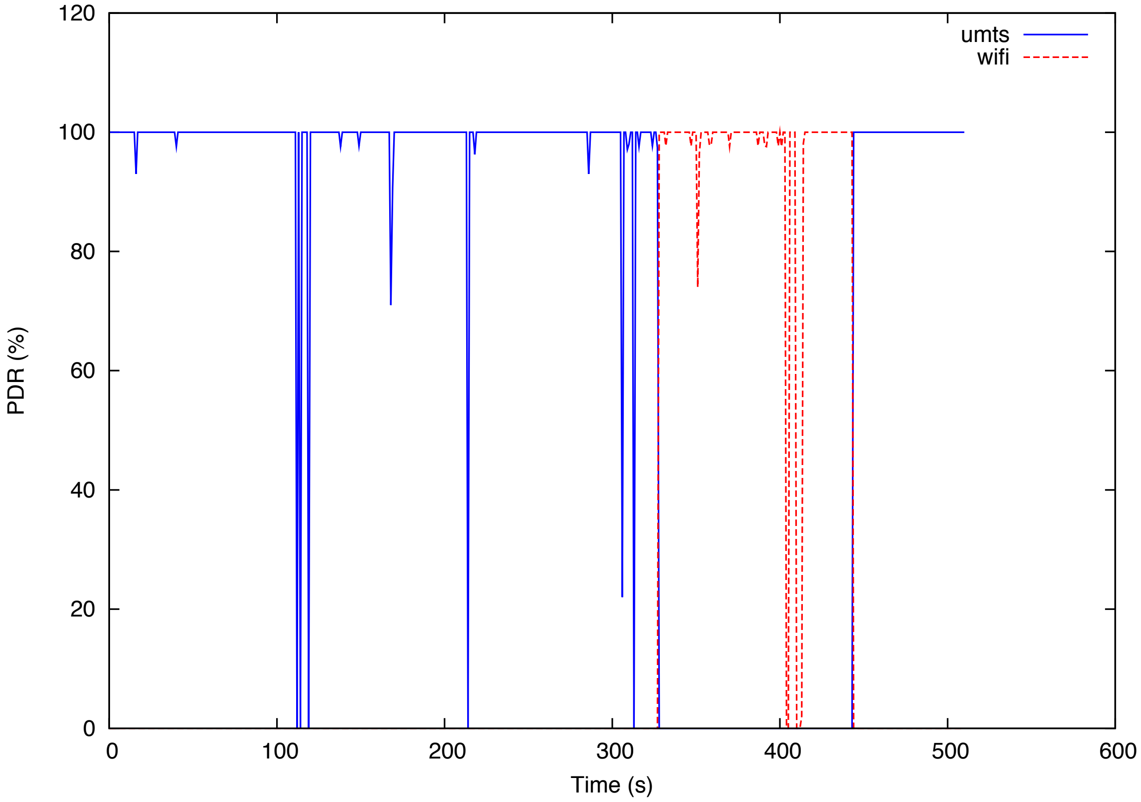


Figure 5.6: PDR evaluation for case of study 1

An interesting value for ITS applications, even more than the maximum bandwidth and packet losses, is the network latency. The round-trip delay time has been evaluated attending to the time that takes the reception of the ICMPv6 Reply messages from the CN, in response to a ICMP Request messages from the vehicle host. Figure 5.7 shows the RTT results obtained. No losses have been detected during the test, which demonstrates that the network operates better when the traffic is small and hence the MAC layer is able to solve data losses. As can be seen in the graph, the RTT is around 200 ms for the 3G case and around 10 ms when the WiFi link is used.

5.2 Case of study 2: IPv6 Geonetworking

In this section, we describe the evaluation results of performance measurement of the CarGeo6 implementation, by means of experimental evaluation in indoor testbed and outdoor testbed. The basic configuration of the evaluation is common with the test performed in [GeoNet-D7.1] using the GeoNet implementation. Thus we compare the performance difference between them. With outdoor testbed, we evaluate the performance in Internet-based communication by combining CarGeo6 and NEMO implementation (MIP6D). The performance measurements are processed and analyzed with AnaVANET.

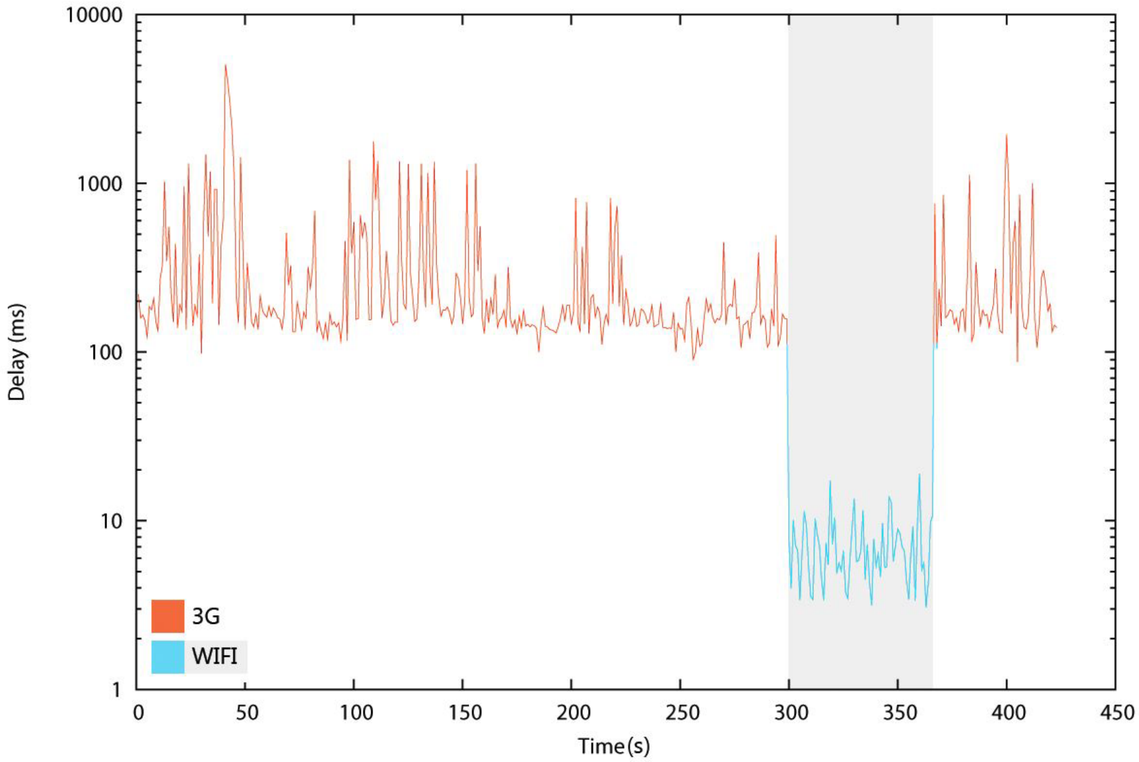


Figure 5.7: RTT evaluation for case of study 1

More details of indoor tests are published in [Toukabri2011].

5.2.1 Direct Path Evaluation in Indoor Testbed

The latency evaluated by the RTT value is indicated in the *ping6* output. The *ping6* output indicates the minimum, maximum and average RTT for a given size of packet. The test consists on sending 100 ICMPv6 requests every 0.1ms with different packet size values increased each time by 20 bytes and varying from 20 bytes to 1500 bytes. The *ping6* output indicates also the packet loss average for each size of ICMPv6 packet. We report in Figure 5.8 and Figure 5.9 the results we had for a *ping6* from MNN1 to MNN2 in both single hop and multi-hop configurations.

5.2.1.1 ICMPv6 Evaluation in Single hop scenario

Figure 5.8 indicates that there are packet losses for the packet packet size exceeds 1300 bytes. This is explained by the fact that we fixed the MTU of the TUN/TAP virtual interface to 1350 bytes in our test, which means that packets from 1320 bytes and more are automatically dropped as no fragmentation mechanism is either enabled or implemented at the TUN/TAP interface. The lack of a fragmentation mechanism at the Geonetworking layer could also have an impact on the packet loss: The maximum MTU is fixed to 1500 bytes. The figure shows also that the average RTT for all packet size values varies mostly between 2ms and 10ms except for a packet size of 370 bytes where we noticed a 25ms maximum average RTT value with 8% packet loss.

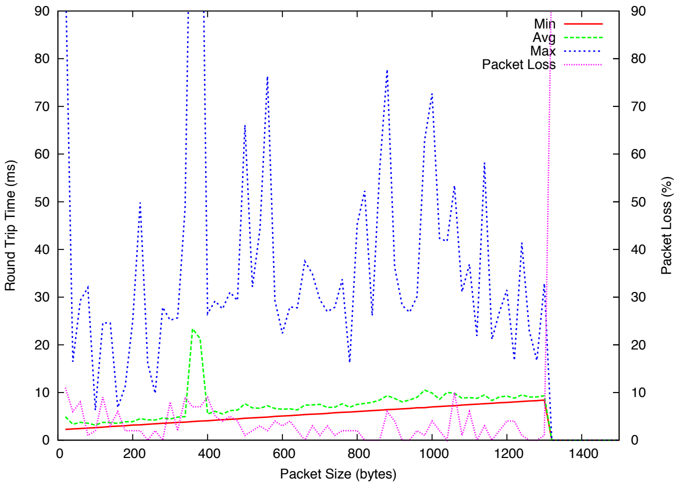


Figure 5.8: ICMPv6 performance in single hop case

If we compare these results to GeoNet results described in [GeoNet-D7.1] for the same test, we can say that CarGeo6 average RTT values are globally better than GeoNet average RTT. Same as for the packet loss, values are almost similar in both implementations. However, these results could be improved by the implementation of an IP Next Hop cache. Currently, the IP Next Hop is resolved for each IPv6 packet at the IPv6 over Geonetworking sub-module (adaptation module) which implies a processing delay on the RTT. The IP Next Hop cache avoids the software resolving the IP Next Hop address for packets having the same destination address. In other words, the cache will keep a periodically refreshed table with the destination Geonetworking ID of an IP Next Hop and will not repeat this operation for packets having the same destination.

Besides, the packet loss values (maximum of 11%) could also be improved. Even if the indoor testbed is intended to minimize interferences impact on the experiment, we cannot suppress definitely this constrain that could be caused by wireless engines located in the proximity of the testbed. Thus, interference impact could be avoided by the choice of a less noisy wireless channel and the isolation of the testbed as well as possible. The activation of QoS at the wireless interface could also improve the packet loss but may imply unfortunately an overhead.

5.2.1.2 ICMPv6 Evaluation in Multi hop scenario

As depicted in Figure 5.9, we can see that global values of RTT and packet loss are significantly higher with one Geonetworking Forwarder node than in the single hop configuration. The minimum packet loss value is 40% for a 1340 bytes packet size. Moreover, as in single hop case, packets are lost for packet size values over 1350 bytes due to the lack of fragmentation mechanisms at the Geonetworking layer. The maximum average RTT is also obtained when the packet size is 370 bytes. Globally, RTT values in multi-hop are about 10 times higher than RTT values in single hop case and more than 40% packets are lost.

As written before, RTT values could generally be improved by the implementation of an IP Next Hop cache but we assume that this is not sufficient in the multi-hop case. RTT and packet loss high values are caused also by the Location Service mechanism implemented at the Geonetworking level. This mechanism is responsible for finding the Geonetworking ID of a node not in the neighborhood of the source. A process of Request/Reply packets is then

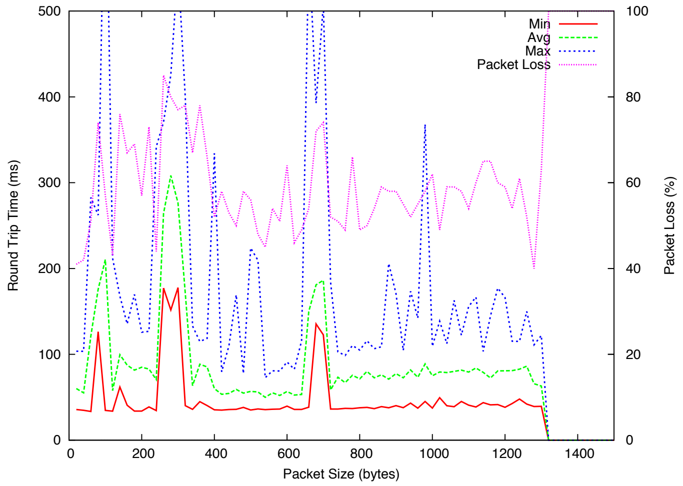


Figure 5.9: ICMPv6 performance in multi-hop case

triggered in order to find that ID. This mechanism implies a long waiting, until the source gets the reply with the Geonetworking ID of the destination: the more we have intermediary nodes the bigger is the RTT and chances of packet loss. To improve this, a multi-hop beaconing mechanism where the source beacon is relayed until the destination through intermediary Geonetworking forwarders could be added.

5.2.1.3 Overhead of IPv6 Geonetworking in ICMPv6 Evaluation

In order to evaluate the overhead between IPv6 and Geonetworking, we compare in Figure 5.10 the RTT values for different packet sizes for IPv6 without Geonetworking and for IPv6 with Geonetworking. The figure shows that the overhead between IPv6 and Geonetworking in the single hop case is about 3ms, while it reaches 30ms in the multi-hop case. We think that this overhead (multi-hop case) could be reduced if we implement the multi-hop beaconing mechanism instead of the Location Service mechanism.

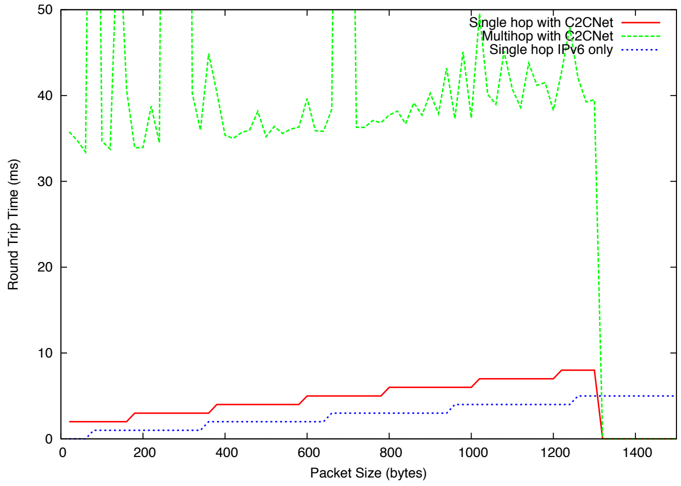


Figure 5.10: Overhead between Geonetworking and IPv6

5.2.1.4 UDP Evaluation

In this part, we report UDP performance results for the single hop case. The performance is evaluated according to packet delivery ratio values and the throughput at the receiver side. The test consists on varying the datagram size from 100 bytes to 1900 bytes for different values of the UDP sending rate varying from 250 Kbits/sec to 2 Mbits/sec.

Figure 5.11 shows the packet delivery ratio in the single hop case. The packet delivery ratio is low when the datagram size is too small: 60% packets are delivered for a 700 bytes datagram size and 250 Kbits/sec sending rate. The maximum packet delivery values (97% to 100%) are registered for a datagram size between 1150 bytes and 1380 bytes and with 250 Kbits/sec sending rate. Though, only 50% packet delivery is registered for the same datagram sizes with 1 Mbits/sec sending rate.

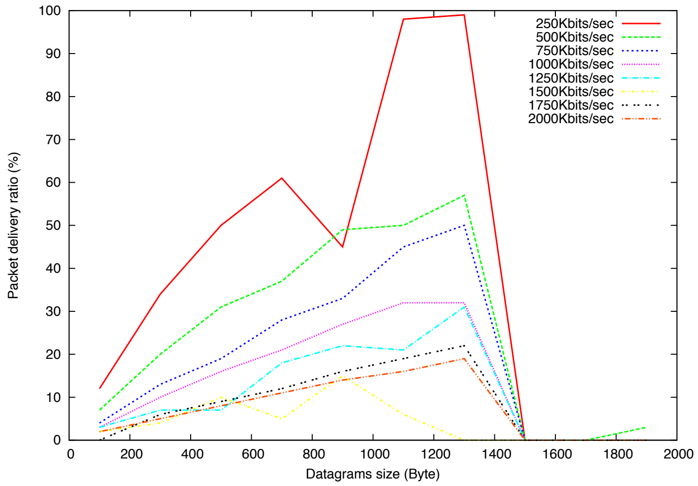


Figure 5.11: UDP performance in single hop case

Figure 5.12 shows the throughput obtained in the same test. Throughput is maximized for all rates with 1360 bytes datagram size. Besides, the maximum throughput value is registered for 420 bytes datagram size with 1250 Kbits/sec, 1750 Kbits/sec and 2 Mbits/sec sending rates. We decided to limit our measurement interval to 2 Mbits/sec sending rate because packets are dropped for rates more than this value.

In comparison with GeoNet results for UDP performance described in [GeoNet-D7.1], CarGeo6's performance for UDP is currently poor but could be improved. A feasible reason for these results could be the interferences present in the wireless media, as mentioned before.

Besides, the quality of the Geonetworking link could also be the issue. As we suspect processing delays at the Geonetworking layer, this could have an impact on the UDP traffic transmission from the source to the destination.

Currently, our assumption is the following: With the *Iperf* tool, the server sends statistic information about the link state to the client (sender node) periodically after receiving a certain number of datagrams. If packets take too much time to arrive, and as UDP is an unreliable protocol, the server could send state information of the link before receiving the packets. This means that late arrived packets could be considered as lost. Moreover, we noticed according to the Figure that, the bigger the sending rate is, the lesser packets arrive to the destination. This could confirm the assumption that the processing time implies too much delay in the end-to-end communication: the bigger the packet the bigger the processing delay and the chance to lost the packet.

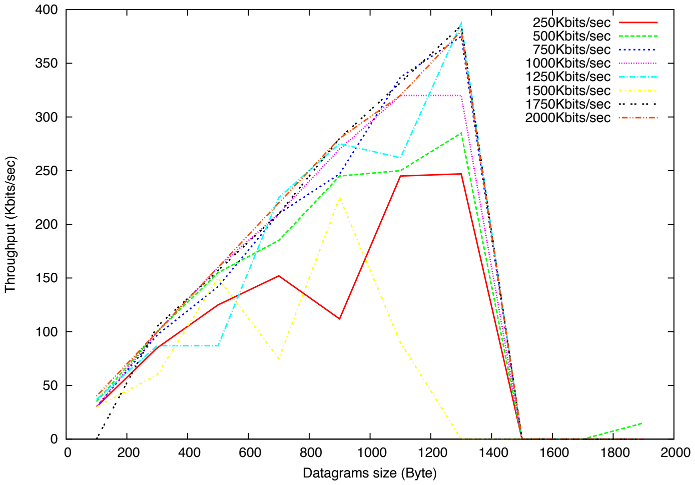


Figure 5.12: UDP throughput in single hop case

5.2.2 Anchored Path Evaluation in Real Field Testbed

5.2.2.1 Handover Scenario

ICMPv6 and UDP evaluations in handover scenarios were performed in INRIA Paris-Rocquencourt campus with two ARs. The two ARs are installed on different buildings as shown in the maps in Figure 5.13 and Figure 5.15. The software and hardware configuration of the two ARs are identical to the MRs used in the previous section. Otherwise, the ARs send RAs in the Geonetworking link with 3 seconds interval. The ARs do not have GPS device, and instead of that, the position is pre-configured statically. Without GPS, the method to synchronize the hardware time to GPS (See Section 4.2 for details) for AnaVANET is not available in the ARs. Instead of using GPS, Network Time Protocol (NTP) is used. For administrative reasons to allocate a new prefix to AR2, IPv6-to-IPv6 tunnels are established towards the Ethernet of AR2 to the router next hop to the HA used in the tests. This configuration gives 40 bytes of additional header to the packets, but it does not incur any additional hop in the route of packets.

As shown in the itinerary in Figure 5.13 and Figure 5.15, AR2 is present most of the times in the tests and AR1 is available in the last one. Thus we could expect that the handover occurs at the end of the test. This is because the building behind AR1 blocks the line of sight to the square that the vehicle goes around. And also, the building stands on the corner in north west of the square blocks the wireless radio to AR2. Approximately ten trees in the south of the square can be obstacles to the access to AR2.

The speed of the vehicle was limited to less than 15 km/h like in the urban scenario. The MR equipped in the vehicle has the same hardware configuration that appears in the previous sections. The modified MIP6D described before is installed in the MR. An HA supports MRs moving around the INRIA campus and the lifetime of the binding updates are configured with a period of 12 seconds. The CN, also located at the INRIA campus, is connected to the vehicle MNN. The ICMPv6 and UDP traffic are generated by *ping6* and *Iperf* software.

All the result of the real field evaluations are also published in the website[1].

[1] http://www-rocq.inria.fr/~tsukada/experiments/itsnet/

5.2.2.2 ICMP Evaluation in Handover Scenario

In the scenario shown in Section 5.2.2.1, ICMPv6 echo request (64 bytes) is sent from the MNN to the CN twice in a second. The CN replies the echo reply. The results collected in the ICMPv6 tests are plotted in Figure 5.13. The lower part shows the itinerary of the vehicle and the locations of AR1 and AR2 on the map, whereas the upper part shows the RTT, the packet loss and the result of the mobility signaling. The X-axis and the Y-axis of the upper part are the latitude and the longitude of the vehicle and correspond to the position of the map in lower part. When either the request or the reply is lost, the RTT is marked as 0, and at the same time, the mark of "packet loss" is drawn. Binding registration success is plotted when the BU and the BA is successfully processed. In contrary, either of them is lost, Binding registration fail is plotted at the position.

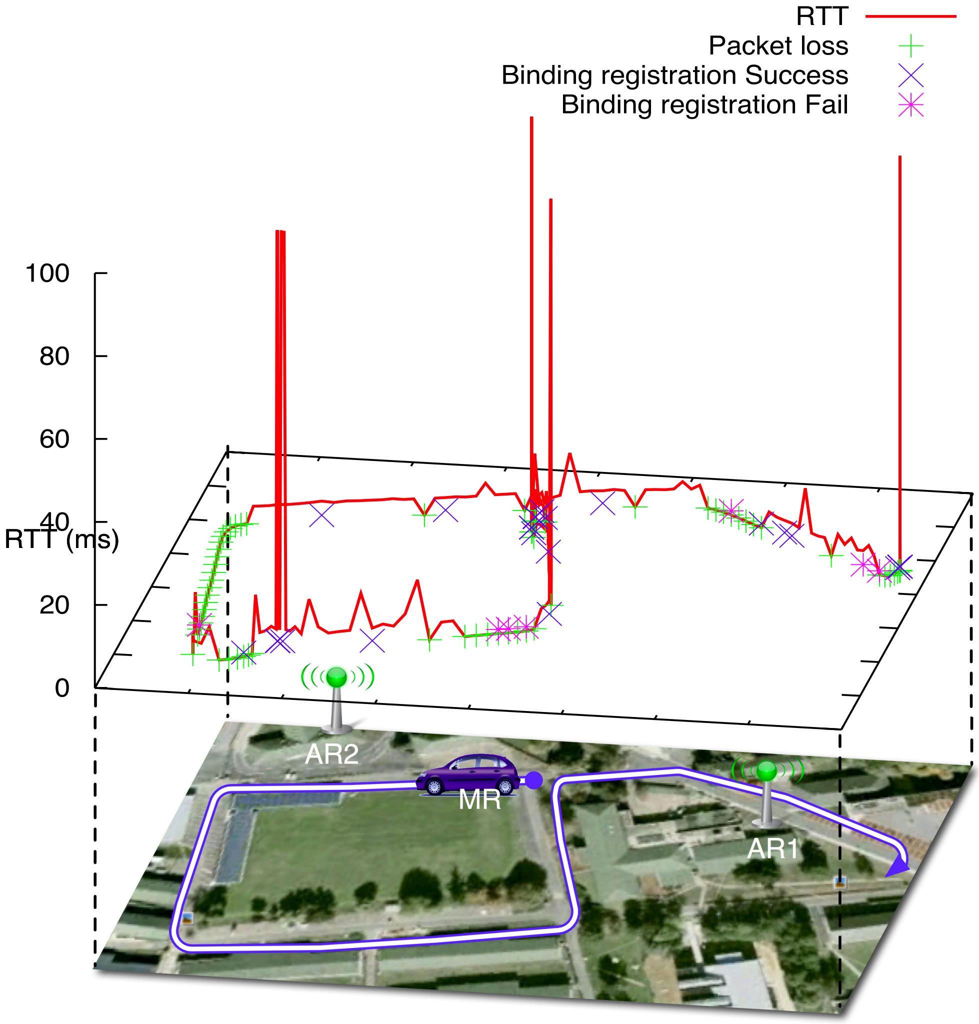


Figure 5.13: RTT, Packet Loss and Mobility Signaling of ICMP evaluation in handover scenario

As can be seen, the RTT is stable with about 5 milliseconds in the beginning of the evaluation. In this moment the MR connects to AR2 that is installed at about 100 meters away. It sends constant BUs and the binding registration is successfully performed. Soon, after the vehicle turns the first corner (north west of the square), the packets start to be dropped, until the second corner. This is because the building shuts out the wireless radio.

The binding signaling is dropped as well in the segment.

The straight road in south of the square is less stable than the one in the north, because of two reasons. First, the location of south straight road is 250 meters farther to AR2 than the one in the north. Thus the signal strength is weaker in the south. Seconds, the trees in meddle of AR2 and the MR interferes the wireless radio. Especially, the trees at the end of the south straight block three consecutive binding messages.

The last straight road in the east has stable wireless radio and no binding message was dropped, while the RTT of two sets of ICMPv6 request and reply exceeds 100 milliseconds. The vehicle approaches to the AR2 along the straight road in the east and turns right to leave from AR2.

The MR starts receiving the RA from AR1 when the distance to AR1 is 50 meters. However the RA from AR2 also reaches to the zone. As the result, the vehicle triggers the movement detection, and sends the mobility signaling via the AR where it receives the RA. When the MR sends the packets to AR2 from the zone, the some ICMP packet and mobility signaling were lost because of the distance and the obstacle (building). When the MR switches to AR1, the packets are stably transmitted.

Figure 5.14 shows the same result of the test with mapping to the time. The upper graph shows the RTT and the distance to the two ARs, the middle shows the PDR to the two ARs, and the lower plots the status of the NEMO signaling. “Success”of NEMO status means the binding registration is successfully performed and “Fail” means either the BU or the BA is lost.

As can be seen, the RTT and the PDR to AR2 is stable in the north straight road. The binding registrations are done successfully in each 12 seconds interval without packet loss. After the first corner, the packets start dropping as well as the mobility signaling. Then it recovers when the vehicle comes to the straight road in the south. The mobility signaling is sent again with regular interval.

In the end of the straight road, the ICMPv6 packet is suddenly lost because of the tree in the corner of southeast. At the time, three consecutive binding registrations are lost as well. When the MR fails to receive a valid matching response within the selected initial retransmission interval, the MR should retransmit the message until a response is received. The retransmission by the MR must use an exponential back-off in which the timeout period is doubled upon each retransmission, until either the MR receives a response or the timeout period reaches the value of maximum timeout period as specified in [rfc6275].

In the case, the MIP6D tried to send the BU one second after the first failure of the binding. Then when it fails, it increases the retransmission time to two, four, eight seconds, and etc. In the case, the BA is returned as a response of forth BU. The disconnection time after the binding registration failure was seven seconds ($= 1 + 2 + 4$).

The east straight road has stable condition for RTT, PDR to AR2 and the NEMO signaling. After turn right to go toward AR1, at the $t = 253$, a mobility signaling is dropped. Then $t = 257$, a binding registration is successfully performed. Actually the registration is transmitted to AR2 because the PDR to AR2 recovers soon after the registration. However $t = 260$ and $t = 261$, the MR receives a RA from AR1 and the trigger the movement. The two BU are successfully registered to the HA and the MR send packets via AR1 (See PDR to AR1 increase at $t = 260$). This time, the handover were possible without any packet loss.

5.2.2.3 UDP Evaluation in Handover Scenario

In the scenario previously shown UDP packets are sent from the MNN to the CN at 1 Mbits/sec sending rate with 1250 bytes packets. The results collected in the ICMPv6 tests are

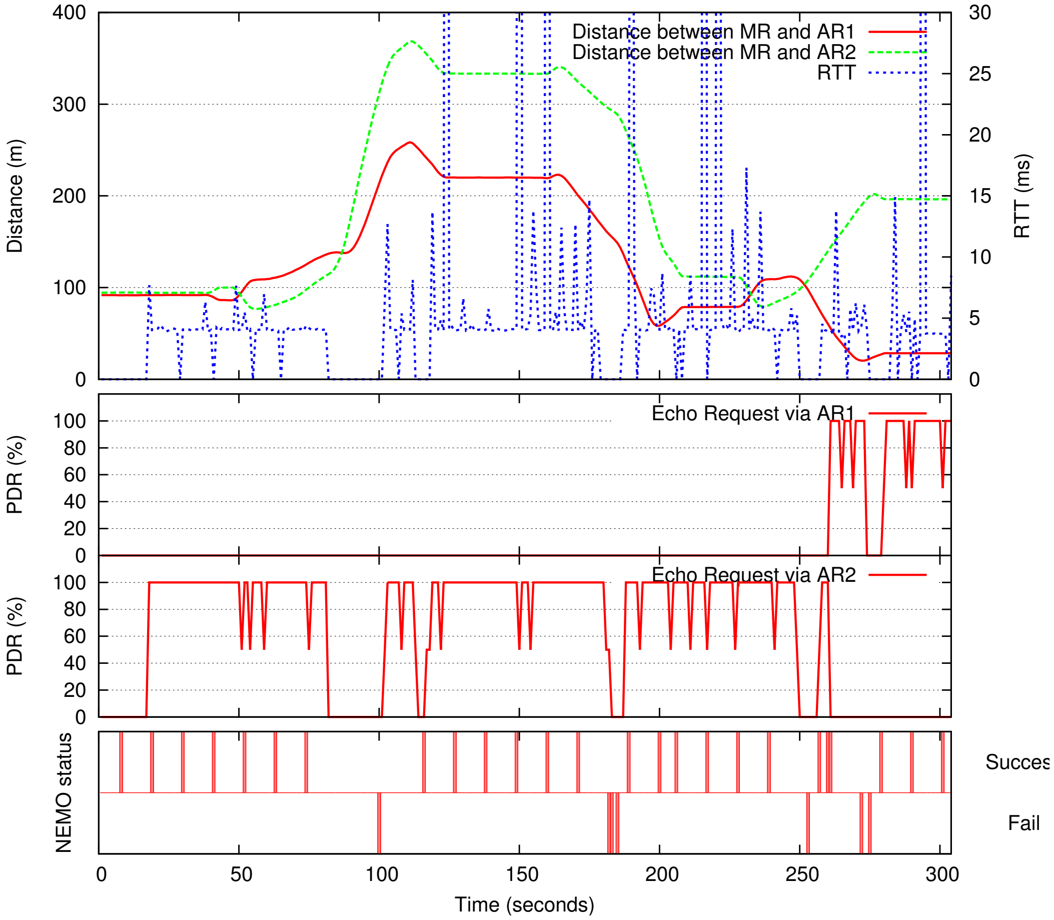


Figure 5.14: RTT, Packet Loss and Mobility Signaling of ICMP evaluation in handover scenario

plotted in Figure 5.15. The lower part shows the itinerary of the vehicle and that corresponds to the PDR to the ARs and the binding registration result shown in the upper part, as well as the previous section. As can be seen in the figure, the place is same as the scenario described in the previous section, however the itinerary of the vehicle are reverse direction around the square in this test.

According to the indoor testbed result in Section 5.2.1.4, the PDR of the UDP configuration is 30%−35%. Actually, the PDR was around 30%−35% in the most stable period in the outdoor testbed in the output of *Iperf* as well as the indoor test result. However, the PDR to the two ARs sometimes reaches to 100% as in Figure 5.15. This is because the AnaVANET calculates the PDR based on the MAC address in the air, on the other hand, the bottleneck of the path exist in the CarGeo6 software at that time. In other word, 70% of the UDP packets are dropped in CarGeo6 and the other 30% transmitted from wireless interface were not lost so much. This reason also explains the phenomenon where the binding registration messages are lost while none of the UDP packets are lost (This can be seen in the straight road in the south of the square). In this case, the BUs are lost in the CarGeo6 software and are not transmitted from the wireless interface.

As can be seen, AR2 is only available most of the test period (especially, around the square) except for the end of the test. When the vehicle runs in the first straight road in the east, the PDR to AR2 is almost 100%. During this period, no binding message was dropped.

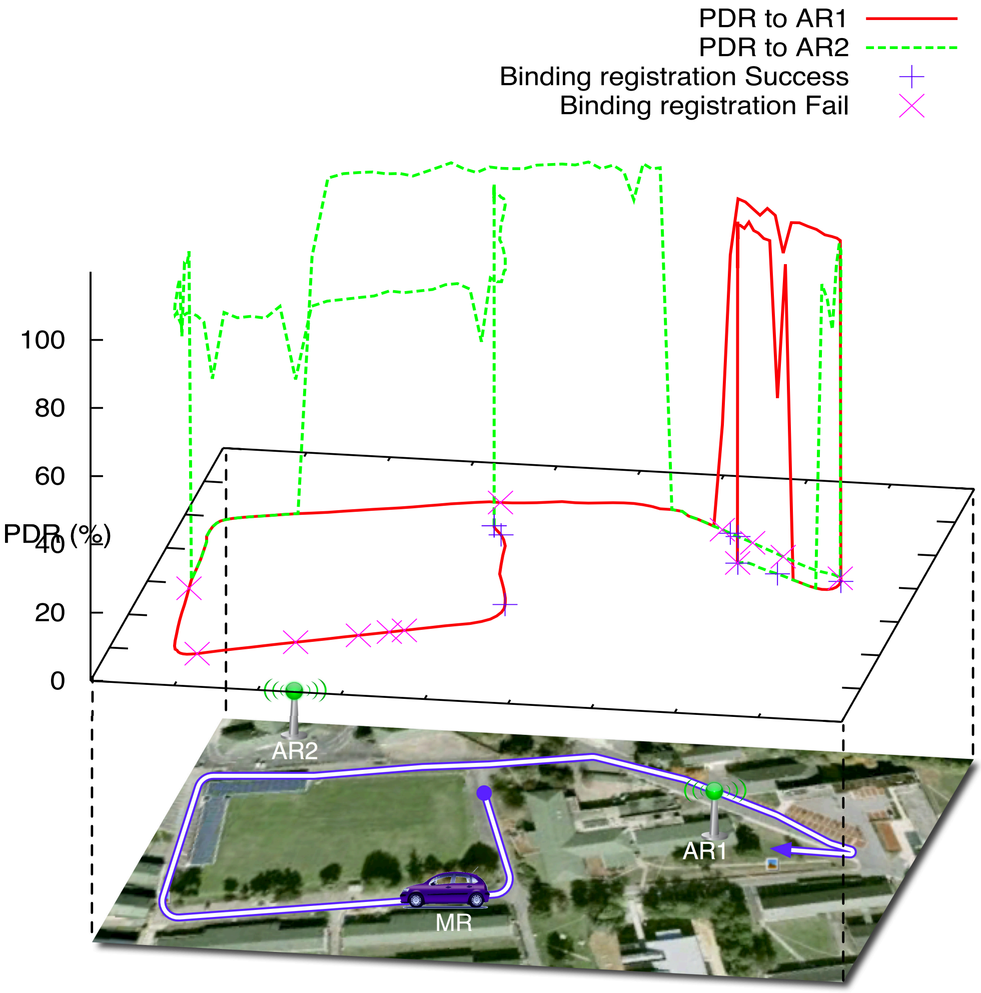


Figure 5.15: PDR to the two ARs and Mobility Signaling of UDP evaluation in handover scenario

The BUs are sent regularly with 12 seconds interval.

In contrary, all the binding registrations are lost in the south straight road. After the first packet loss of mobility signaling, the binding registration continuously fails until the vehicle goes around and arrives at the area of AR1. Thus the UDP packet does not arrive at CN during the period, because the HA has not the binding and discards the tunneled packet from the MR. The MR sends tunneled UDP packets to the HA during the period where the mobility signaling fails. The PDR to AR2 shows that over 80% of the packets from the MR are delivered to the AR2 constantly, when the vehicle runs in the south straight road.

The packets start dropping on the west of the square because the building on the north west corner of the square blocks the wireless radio. When the beacons exchanged between Geonetworking nodes twice in a second are dropped, the correspondent entry of the location table expires in 5 seconds, because the lifetime of the location table entries are configured as 5 seconds.

When the vehicle approaches at 20 meters from AR1, a binding registration with the CoA obtained in AR's access network is successfully performed. The path to the Internet is switched via AR1 at the moment. The PDR to the AR1 shows almost 100% packets are delivered from the MR to the AR1. The RA from AR2 sometimes reaches to the area, and the MR makes a binding registration with the CoA obtained from AR2. The path to the Internet is switched via AR2 again. Since the MR receives the RAs from both AR1 and AR2 at the area, the MR detects the movement when it receives the new different RA from the previous one.

Figure 5.16 shows the same test with mapping to the time. The upper graph shows the Throughput of UDP from the MNN to the CN, the middle part shows the PDR to the two ARs, and the lower plots the status of the NEMO signaling. Success"of NEMO status means the binding registration is successfully performed and "Fail" means either the BU or the BA is lost.

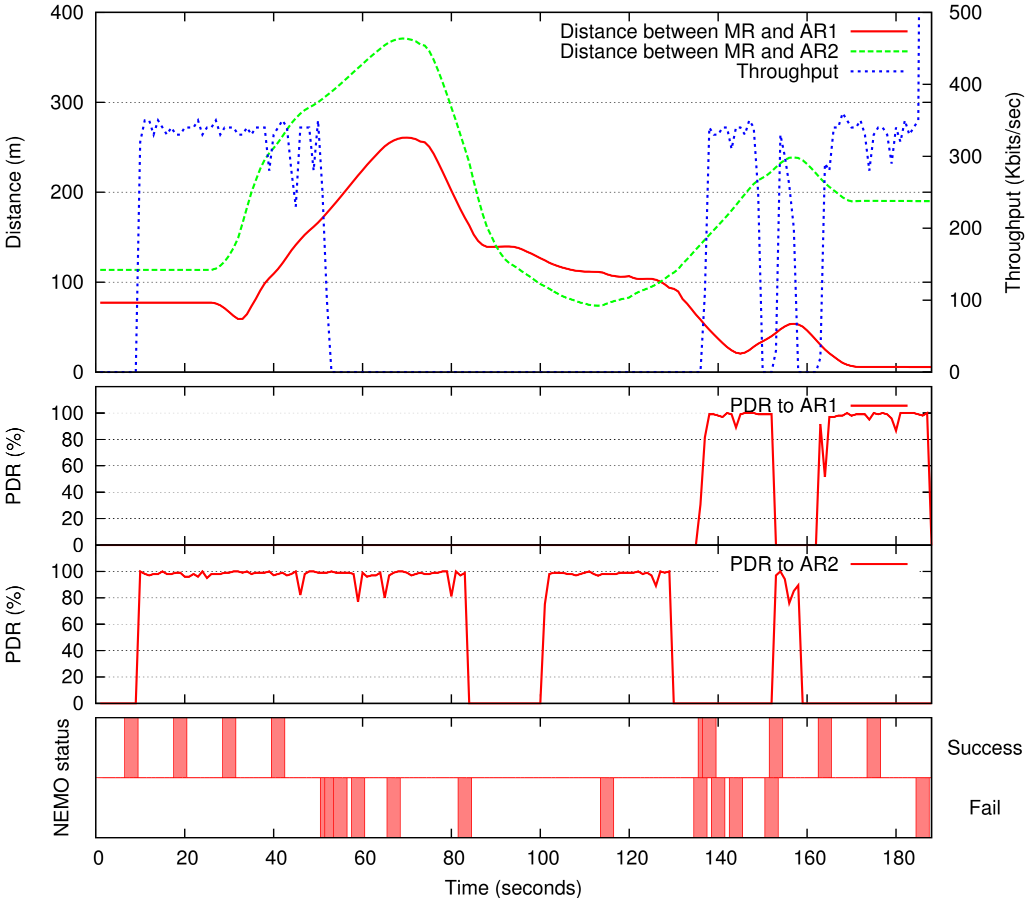


Figure 5.16: PDR to the two AR and Mobility Signaling of UDP evaluation in handover scenario

As can be seen, the throughput from the MNN to the CN, and the PDR to AR2 is stable in the beginning of the test (the vehicle is 80 meters away from AR2 in the north east of the square). The binding registrations are done successfully in each 12 seconds interval without packet loss. After the first corner, the throughput drops to zero as well as the binding registration fails, while the PDR to AR2 is still almost 100%. This shows the mobility signaling packets are lost in CarGeo6 as mention in the beginning of this section. Since the binding fails, the HA dos not have the binding for the MR and discard the packet from the MR. The interval of the BUs are increased exponentially from 1 seconds to 32 seconds (1, 2, 4, 8, 16 and 32 seconds).

Then at $t = 139$, when the vehicle is 20 meters away from AR1, the first binding registration of the CoA from AR1 success. The UDP packets are switched to AR1 from the moment.

Then at $t = 155$, the binding registration is successfully performed via AR2 again. During the handover from AR1 to AR2 from $t = 155$ to $t = 158$, three seconds of disconnection are counted in the *Iperf* log. At $t = 166$, the path to the Internet is switched to AR1 again. At this handover, the UDP packets are lost during 4 seconds from $t = 166$.

5.2.3 Conclusion

Indoor tests show the network performance using CarGeo6 in terms of delay and throughput. In single hop test, the delay was about 5 ms, that is as small as the one using GeoNet implementations. However, the delay on multi-hop has about 35 ms, which is twice bigger than the one using the GeoNet one. The maximum UDP throughput using CarGeo6 in single hops is around 400 Kbits/sec, that is ten times smaller than the one using GeoNet one. The bigger delay and smaller throughput using CarGeo6 are explained by two reasons. The two non-standard optimization works implemented in the GeoNet implementations (the next hop IPv6 address cache and multi-hop beaconing) is not implemented in CarGeo6. Thus the CarGeo6 resolves the next hop IPv6 address from the routing table for each forwarding packet regardless of either single hop or multi-hop. This increase the processing delay in the source MR. In addition, in multi-hop case, the source MR launches the location service in request-reply manner for all the forwarding packet. This causes the additional processing delay and signaling delay.

The outdoor test using NEMO left as a future work in the GeoNet project is performed using CarGeo6. ICMPv6 and UDP evaluations in handover scenarios were performed in INRIA Paris-Rocquencourt campus with two ARs. In all the tests, the line of sight between the vehicle and the roadside ITS Station has been a key factor to maintain communication links. The communication between them are disturbed by the trees not only the buildings. When the signaling packet (*i.e.* Binding Update (BU) and Binding Acknowledgement (BA)) is dropped, the disconnection takes some time. From the test, we confirm the packets are dropped in the CarGeo6 Geonetworking modules and they are not dropped in the air.

5.3 Case of study 3: Multiple Care of Address evaluation with static flow distribution

The aim of this case of study is testing the operation of the communication stack when more than one interface is active under network mobility circumstances, by using the multiple care of address capability of the vehicle ITS-S router.

5.3.1 Scenario description

5.3.1.1 Overall architecture

The case we are studying concentrates on the behavior of MCoA with static flow distribution in a simple two-interfaces virtualized mobile router setup. This indoor test aims at checking the consistency of the policies and measuring the network performances when using them. The intent of this study case is to evaluate *only* the policies and not the standard behavior of MCoA relative to the preferred interface for general traffic.

The setup consists of a Home Agent, and ITS-S Router on which we evaluate the policies, some Hosts connected to it, and a Correspondent Node. The ITS-S Router is attached intermittently with two access networks, thus permitting to evaluate an inter-domain and intra-technology handover.

5.3.1.2 Network design

The network architecture used is depicted in Figure 5.17. This is a simple architecture with two access networks to be attached to. It is entirely contained inside the virtualized environment.

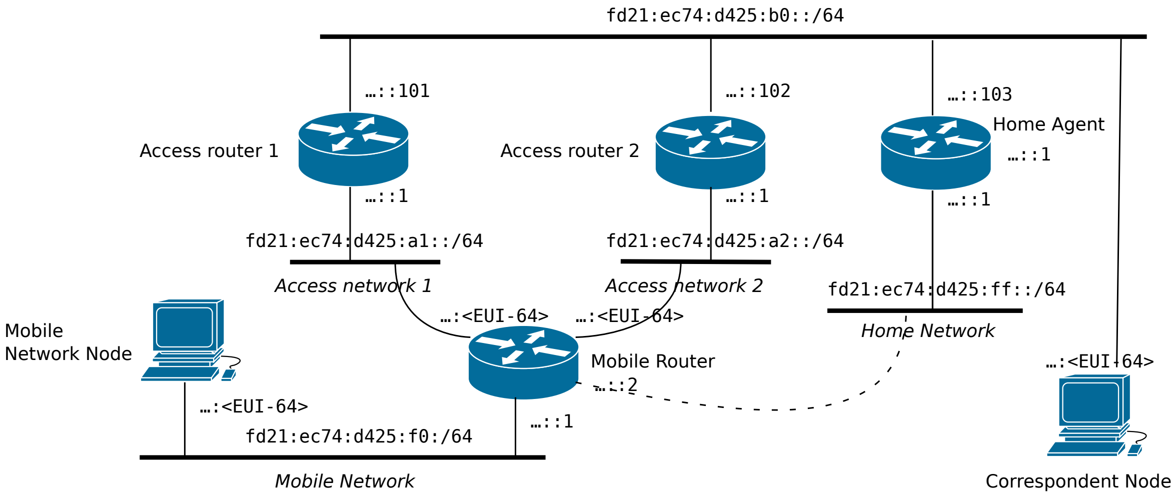


Figure 5.17: Network design for case study 3

The addressing is done with ULA addresses, and the chosen random-generated prefix for these test is `fd21:ec74:d425::/48`. One subnet is used as a backbone, and two other subnets are the two access networks, one is used for the Home Network, and the other one for the Mobile Network.

5.3.1.3 Testbed set-up

The virtual machines are created through libvirt, using the KVM virtualization infrastructure. Virtual networks are also created through libvirt, using tun/tap devices and bridging them together as needed. The images used for testing are the ITSSv6 Linux platform, revision 674. Each component of our architecture is configured for its role. On the Mobile Router, the first interface is set as the preferred one in the MCoA setup.

5.3.2 Technological validation of protocols (control and management)

5.3.2.1 Traffic

In these tests, we generate traffic of different types: we set some specific port of some specific protocol, and optionally add policies for them. We use the following policies among the two interfaces of the MR, and we organize them in "classes":

Class A: TCP traffic from the MR on port 80 is preferably routed through the first interface.

Class B: UDP traffic from the MR on port 53 is preferably routed through the second interface.

Class C: TCP traffic from the MR on port 21 has no preference and is thus routed through the globally preferred interface.

Class D: TCP traffic from a MNN on port 443 is preferably routed through the first interface.

Class E: UDP traffic from a MNN on port 161 is preferably routed through the second interface.

Class F: TCP traffic from a MNN on port 22 has no preference and is thus routed through the globally preferred interface.

The traffic is generated by *Iperf*.

5.3.2.2 Evaluation tool

The trafic flowing through both access networks is recorded in `pcap` files. Traffic is then analyzed offline.

5.3.3 Detailed description of the tests

5.3.3.1 Single interface test — from MR

Setup: Connect the MR's first interface to one access network.

Expected result: The mobility procedure is set up correctly. Traffic of all types generated from a MNN is routed through this single interface. Traffic flowing back is also routed through this interface.

Interface	Traffic class
1st	A, B and C
2nd	None

5.3.3.2 Two interfaces test — from MR

Setup: Connect the MR as previously done, and connect its second interface to a second access network.

Expected result: The mobility procedure is set up correctly. Traffic generated from a MNN flows on the right interface. Traffic flowing back comes from the rigth interface too.

Interface	Traffic class
1st	A and C
2nd	B

5.3.3.3 Loss of an interface test — from MR

Setup: Connect the MR as previously done, and then disconnect the first interface.

Expected result: The mobility procedure is set up correctly. Traffic of all types generated from a MNN is routed through the remaining interface. Traffic flowing back is also routed through this interface.

Interface	Traffic class
1st	None
2nd	A, B and C

5.3.3.4 Single interface second test — from MNN

Setup: The same used in test 5.3.3.1.

Expected result: Traffic of all types generated from the MNN is routed through the only MR interface interface. Traffic flowing back is also routed through this interface.

Interface	Traffic class
1st	D, E and F
2nd	None

5.3.3.5 Two interfaces second test — from MNN

Setup: The same used in test 5.3.3.2.

Expected result: Traffic generated from the MNN flows on the right interface in the MR. Traffic flowing back comes from the right interface too.

Interface	Traffic class
1st	D and F
2nd	E

5.3.3.6 Loss of an interface second test — from MNN

Setup: The same used in test 5.3.3.3.

Expected result: Traffic of both types generated from the MNN is routed through the remaining MR interface. Traffic flowing back is also routed through this interface.

Interface	Traffic class
1st	None
2nd	D, E and F

CHAPTER 6

Conclusions and next steps

This first deliverable of Work Package 4 has presented the scope of the project regarding tests and evaluations, which are based on the developments done in Work Package 3. The general testing methodology has been described, together with the most important parameters, performance metrics and communication flows that have been and will be used in project experimental evaluations. As it has been remarked, an initial set of indoor evaluations will be followed by an experimental assessment of the ITSSv6 communication stack. The most important communication patterns to be considered under different outdoors conditions have also been listed, as a framework for WP4 tests. Moreover, one of the deliverable chapters has been focused on describing the software environment used for collecting performance indices and carry out post-process tasks. This tool has been developed by members of ITSSv6 an it has been improved in several research projects during the last years. It will be also adapted in this project too, in order to analyze new data flows and present new figures of merit about the communication stack performance.

Three initial and basic cases of study have been presented in this deliverable. These are essential experimental set-up and evaluations about core technologies to be included in the ITSSv6 communication stack: IPv6 network mobility, Geonetworking support, and flow distribution through multiple care of address. As the reader can note from the three cases of study, the communication stack performs correctly in the three experiences. It is able to provide the in-vehicle network with a continuous IPv6 connectivity and addressing, while the vehicle is moving and changing its point of attachment to the network. This capability has been validated through a set of outdoor trials carried out in real traffic conditions. Moreover, geographical routing features through the IPv6 over Geonetworking has also been validated through a vast set of tests. This demonstrates how the communication stack provides an IPv6 support over a native V2V communication protocol to disseminate messages over interesting areas. Finally, the last case of study shows the communication stack potential for distributing data flows on different communication interfaces when the multiple care of address support is used. By a set of (sub)scenarios, different flows have been checked to be correctly transmitted through different data paths, which is a network optimization with regards to basic network mobility.

In next steps in frames of Work Package 4, the ITSSv6 partners efforts will be directed to integrate all cases of study in a single testing emplacement. The stack features evaluated in this deliverable will be tested again in this new environment, and new features will be added to the list of technologies to validate in new cases of study. For instance, it is envisaged to include 802.11p communications and testing basic security features of the communication stack. Efforts are directed to create in the last phase of the project a final testing environment where a set of real vehicles (up to four) will be used to validate and assess the performance of the whole communication stack implemented in the end of the project. The results of this deliverable and next evaluations in frames of Work Package 4 will be essential to validate ITSSv6 implementations and make easier the porting tasks to be done inside Work Package 5.

Appendix

APPENDIX A

Testing scripts used in Case of Study 1

This appendix contains a set of scripts used to gather validation and performance data in the tests carried out in the case of study 1.

A.1 ICMP test

```
#!/bin/bash

if [[ $# -ne 2 ]]; then

echo "usage: $0 <ipv6_address> <output_file>"
exit -1
fi

ping6 $1 >> $2
```

A.2 TCP test

A.2.1 Server part

```
#!/bin/bash

iperf -s -i 1 -V
```

A.2.2 Client part

```
#!/bin/bash

if [[ $# -ne 2 ]]; then

echo "usage: $0 <ipv6_address> <output_file>"
exit -1
fi
```

```
iperf -c $1  -i 1 -V -t 10000 >> $2
```

A.3 UDP test

A.3.1 Server part

```
#!/bin/bash

if [[ $# -ne 1 ]]; then

echo "usage: $0 <output_file>"
exit -1
fi

iperf -s -u -i 1 -V >> $1
```

A.3.2 Client part

```
#!/bin/bash

if [[ $# -ne 2 ]]; then

echo "usage: $0 <MR_ipv6_address> <bandwidth_in_bytes>"
exit -1

else

iperf -c $1 -u -i 1 -b $2 -V --time 1000000

fi
```

APPENDIX B

List of acronyms

2G 2nd Generation mobile telecommunications
3G 3rd Generation mobile telecommunications
A-GPS Assisted GPS
AnaVANET ANAlyzer for Vehicular Adhoc NETworks
AP Access Point
AR access router
ASN.1 Abstract Syntax Notation One
AU Application Unit
BA Binding Acknowledgement
BC Binding Cache
BE Binding Error
BID Binding Identification number
BOP Basic Open Platform
BU Binding Update
BUL Binding Update List
BR border router
BT Bluetechnix Mechatronische Systeme GmbH
C2C-CC Car-to-Car Communication Consortium
C2CNet Car-to-Car Network
CALM Communications Access for Land Mobiles
CAM Co-operative Awareness Messages
CCU Communication and Control Unit
CDMA Code Division Multiple Access
CE Correspondent Entity
CEN European Committee for Standardization
CI Communication Interface
C-ITS Cooperative Intelligent Transportation Systems
C-ITSS central ITS station
CIMAE Communication Interface Management Adaptation Entity
CN Correspondent Node
CoA Care-of Address
CoDrive Co-Pilote pour une Route Intelligente et des Véhicules Communicants
Coopers Co-operative Systems for Intelligent Road Safety
CoT Care-of Test
CoTI Care-of Test Init
CR central router
CVIS Cooperative Vehicle-Infrastructure Systems
DAD Duplicated Address Detection
DENM Decentralized Environmental Notification Messages
DHAAD Dynamic Home Agent Address Discovery
DHCP Dynamic Host Configuration Protocol
DMIPS Dhrystone MIPS, Million instructions per second
DNS Domain Name System
DoT U.S. Department of Transportation
DriveC2X Connecting vehicles for safe, comfortable and green driving on European roads
DSRC Dedicated Short Range Communications

EC European Commission

ETSI European Telecommunications Standards Institute

FlowID Flow Identifier

FM Frequency Modulation

FMIPv6 Fast Handovers for Mobile IPv6

FOT Field Operational Test

FOTsis Field Operational Test on Safe, Intelligent and Sustainable Road Operation

FP6 Sixth Framework Programme

FP7 Seventh Framework Programme

GLONASS Global Navigation Satellite System

GeoNet IPv6 GeoNetworking

GPRS General Packet Radio Service

GPS Global Positioning System

GPSR Greedy Perimeter Stateless Routing

GSM Global System for Mobile communications

HA home agent

HIP Host Identity Protocol

HMIPv6 Hierarchical Mobile IPv6

HNA Host and Network Association

HoA Home Address

HoT Home Test

HoTI Home Test Init

HSPA High Speed Packet Access

I2V Infrastructure-to-Vehicle

ICMPv6 Internet Control Message Protocol version 6

ICT Information Communication Technologies

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IME Interface Management Entity

INP Internal Network Prefix

INPA Internal Network Prefix Advertisement

Inria Institut National de Recherche en Informatique et en Automatique

INPD IPv6 Internal Network Prefix Discovery

IINP ITS Station Internal Network Prefix

IP Internet Protocol

IPFR IP Filter Rule

IPsec Internet Protocol security

IPTE Schalk & Shalk OG

IPv6 Internet Protocol version 6

ISO International Organization for Standardization

ITS Intelligent Transportation Systems

ITSSP ITS Station Protocol

ITSSPD ITS Station Protocol Daemon

ITS-S ITS station

ITSSv6 web page http://www.itssv6.eu

IT Institut Mines Telecom

ITU International Telecommunication Union

L2 Layer 2

L2TP Layer-2 Tunneling Protocol

L3 Layer 3

LAN Local Area Network

LDM Local Dynamic Map

LLC Logical Link Control

LTE Long Term Evolution

LS Location Service

LT Location Table

LW lesswire

MAC Medium Access Control

MADM Multiple Attribute Decision Making

MAN Metropolitan Area Network

MANET Mobile Ad-hoc Network

MAP Mobility Anchor Point

MCoA Multiple Care-of Addresses Registration

MIB Management Information Base

MIPS Million instructions per second

MLME MAC Layer Management Entity

MN Mobile Node

MNN mobile network node

MNP Mobile Network Prefix

MNPP Mobile Network Prefix Provisioning

MobiSeND	Mobile Secure Neighbor Discovery
MR	mobile router
MTU	Maximum Transmission Unit
NA	Neighbor Advertisement
NAT	Network Address Translation
NDP	Neighbor Discovery Protocol
NEMO	Network Mobility
NemoBS	Network Mobility Basic Support
NEPL	NEMO Platform for Linux
NMEA	National Marine Electronics Association
NS	Neighbor Solicitation
NTP	Network Time Protocol
OASIS	Operation of Safe, Intelligent and Sustainable Highways
OBU	On-Board Unit
OLSR	Optimized Link State Routing
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAN	Personal Area Network
PathID	Path Identifier
PDR	Packet Delivery Ratio
PFBU	Peer Flow Binding Update
PHY	Physical
P-ITSS	personal ITS station
PM	Person-Month
PLME	PHY Layer Management Entity
PMIPv6	Proxy Mobile IPv6
PPP	Point-to-Point Protocol
PR	personal router
PRESERVE	Preparing Secure Vehicle-to-X Communication Systems
QoS	Quality of Service
R2C	Roadside ITS station to Central ITS station
RA	Router Advertisement
RADVD	Router Advertisement Daemon
RDS	Radio Data System
RFC	Request for Comments
RIPng	Routing Information Protocol
R-ITSS	roadside ITS station
RO	Route Optimization
RPDB	Routing Policy Database
RS	Router Solicitation
RSSI	Received Signal Strength Indication
RSU	Road Side Unit
RR	roadside router
RTT	Round-Trip Time
SafeSpot	Cooperative vehicles and road infrastructure for road safety
SAP	Service Access Point
SAT	ITS station access technologies layer
SAW	Simple Additive Weighing
SCORE@F	Système COopératif Routier Expérimental Français
SCTP	Stream Control Transmission Protocol
SeVeCom	Secure Vehicular Communication
SF	ITS station facilities layer
SHIM6	Level 3 Multihoming Shim Protocol for IPv6
SHIM6	Site Multihoming by IPv6 Intermediation
SLAAC	Stateless Address Auto-Configuration
SME	ITS station management entity
SMIv2	Structure of Management Information Version 2
SNMP	Simple Network Management Protocol
SNT	ITS station networking & transport layer
SPI	Security Parameter Index
SSE	ITS station security entity
STP	Specific Target Platform
SZTAKI	Magyar tudomanyos akademia szamitastechnikai es automatizalasi kutato intezet
SZT	SZTAKI
TC204 WG16	Technical Committee 204 Working Group 16
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMU	Universidad de Murcia
UMTS	Universal Mobile Telecommunications System

UTC Coordinated Universal Time
V2C Vehicle ITS station to Central ITS station
V2I Vehicle-to-Infrastructure
V2L Vehicle ITS station to legacy system
V2P Vehicle ITS station to Personal ITS station
V2R Vehicle ITS station to Roadside ITS station
V2V Vehicle ITS station to Vehicle ITS station
VANET Vehicular Ad-hoc Network
V-ITSS vehicle ITS station
VR vehicle router
VCI Virtual Communication Interface
WAVE Wireless Access in Vehicular Environments
WG Working Group
WGS-84 World Geodetic System 84
WIMAX Worldwide Interoperability for Microwave Access
WLAN Wireless Local Area Network
WSMP Wireless Access in Vehicular Environments (WAVE) Short Message Protocol
XML Extensible Markup Language

Bibliography

[GeoNet-D7.1] GeoNet. D7.1 GeoNet Experimentation Results. Public deliverable, June 2010. pages 24, 25, 39, 41, 43

[ITSSv6-D2.2] ITSSv6 Members. ITSSv6 STREP No.210519 D4.1 Preliminary System Specification. *ITSSv6 Deliverable*, 2012. ITSSv6-D2.2-v1.0. pages 12, 14, 17

[Santa2009a] José Santa, Manabu Tsukada, Thierry Ernst, Olivier Mehani, and Antonio Gómez-Skarmeta. Assessment of vanet multi-hop routing over an experimental platform. In *Int. J. Internet Protocol Technology*, volume Vol. 4. Inderscience Publishers, 2009. pages 24, 25

[Santa2009b] J. Santa, M. Tsukada, T. Ernst, and A. F. Gomez-Skarmeta. Experimental analysis of multi-hop routing in vehicular ad-hoc networks. In *Proc. 5th International Conference on Testbeds and Research Infrastructures for the Development of Networks. Communities and Workshops TridentCom 2009*, pages 1–8, April 6–8, 2009. pages 24, 25

[Toukabri2011] Thouraya Toukabri, Manabu Tsukada, Thierry Ernst, and Lamjed Bettaieb. Experimental evaluation of an open source implementation of IPv6 GeoNetworking in VANETs. In *ITST 2011 : 11th International Conference on Intelligent Transport System Telecommunications*, Saint-Petersburg, Russie, Fédération De, August 2011. Conference is technically co-sponsored by IEEE Communications Society and co-organized by the Technical Sub-Committee on Vehicular Networks and Telematics (VNAT). pages 25, 40

[Tsukada2010b] Manabu Tsukada, Ines Ben Jemaa, Hamid Menouar, Wenhui Zhang, Maria Goleva, and Thierry Ernst. Experimental evaluation for IPv6 over VANET geographic routing. In *IWCMC '10: Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*, pages 736–741, New York, NY, USA, 2010. ACM. pages 24, 25

[rfc6275] C. Perkins, D. Johnson, and J. Arkko. Mobility Support in IPv6. RFC 6275 (Proposed Standard), July 2011. pages 46