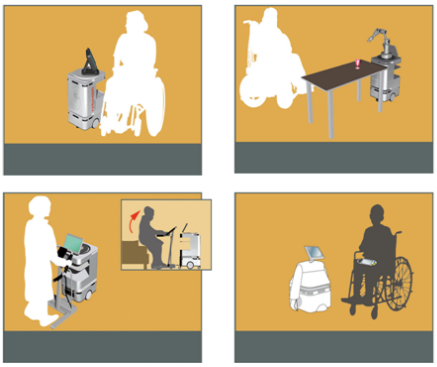

DOMEO Project
AAL-2008-1-159

D6.3 Data transmission validation and performance report

Document id: R-TAS-1_0-D6.3 Data transmission validation and performance report

Document Information	
Title	Data transmission validation and performance report
Workpackage/Deliverable	WP6 / D6.3
Responsible	TAS
Due Date	06/2012
Actual Date	04/2012
Type	Deliverable
Status	Version 1_0
Dissemination Level	Public
Authors	Pascal LOCHELONGUE – Xavier LADJOINTE
Project URL	N/A

Keyword List:
Telecommunication, Data transmission, Characterization, Performances

Table of Content

List of Figures

List of acronyms

1G	1st Generation Mobile System
2G, 2.5G	2nd Generation Mobile System
3G	3rd Generation Mobile System
4CIF	4 × CIF : 704 × 576
ADSL	Asymmetric Digital Subscriber Line
ADSLF	ADSL Forum
AMPS	Advanced Mobile Phone Service
AVI	Audio Video Interleave
CDMA	Code Division Multiple Access
CIF	CIF 352 × 288
CO	telephone Central Office
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DVB-RCS	Digital Video Broadcasting – Return Channel via Satellite
DVB-S	Digital Video Broadcasting via Satellite
ECG	Electrocardiogram
EDGE	Enhanced Data rates for GSM Evolution
ETSI	European Telecommunications Standards Institute
FDMA	Frequency Division Multiplexing Access
FLV	Flash Video codec
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
HMI	Human Machine Interface
HR	Heart Rate
HTTP	HyperText Transfer Protocol
IMT	International Mobile Communications
IP	Internet Protocol
IPTV	TV over IP
IR	Infra Red
ITU	International Telecommunications Union
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAP	Mean Artery Pressure
MDD	Medical Device Directive
MF-TDMA	Multi-Frequency Time Division Multiple Access
MP3	Moving Picture Experts Group Layer-3 Audio file format
MPEG	Moving Picture Experts Group
NAT	Network Address Translation
OGG	open standard container format used to provide more efficient streaming and higher quality presentation
OSAS	Obstructive Sleep Apnoea Syndrome
PCMCIA	Personal Computer Memory Card International Association
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
QCIF	CIF/2 : 176 × 144
QoL	Quality of Life

QoS	Quality of Service
RADSL	Rate-Adaptive Digital Subscriber Line
RCST	Return Channel Satellite Terminal
RTCP	Real-time Transport Control Protocol
RTP	Real Time Transport Protocol
SDSL	Symmetric Digital Subscriber Line
SIM	Subscriber Identity Module
SIT	Satellite Interactive Terminal
SLAM	Simultaneous Localization And Mapping
Speex	Lossy audio codec optimized for speech
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VDSL	Very-high-data-rate Digital Subscriber Line
VOD	Video On Demand
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network
WAV	Waveform Audio File Format
WIFI	IEEE 802.11b wireless networking
WMV	Windows Media Video
xLAW	Standard compression algorithms : (1) μ-law (2) A-law

1. Introduction

Purpose of Deliverable D6.3 “Data transmission validation and performances” is to present the results of the technical tests made in the frame of Workpackage 6 to characterize the possible implemented telecommunication networks of the DOMEO system. It is the thirdpard of Workpackage 6 technical activity whose aim was to describe, then to set-up and finally to validate the DOMEO network architecture.

The DOMEO system has been designed to make possible for the elderly and disabled to remain at home, safe and comfortable. Being safe and comfortable includes to be monitored and controled remotely by patient’s physician or healthcare staff in order to detect alerts and prevent any troubles with the shortest delay. Remote monitoring and control consists in exchanging data (either text/pictures or audio or video) with remote location and/or participant, thus transfering data over wide area networks.

In the frame of the DOMEO project, identified telecommunication networks are based on DSL, 3G or satellite technologies. While DSL and 3G technologies are the most likely as they are now largely available, it makes sens to consider also satellite technology for elderly living in isolated areas like mountains/campains/islands.

The technical tests have been performed at CHU Toulouse premises with engineering staffs of CHU TO and Thales Alenia Space.

Section 2 of the present document introduces the tests objectives and relevant parameters to be managed for network characterization.

Section 3 briefly reminds the general DOMEO architecture, then introduces the configuration set up at CHU Toulouse premises to perform the tests.

Section 4 introduces the methodology applied for network characterization as well as the tools used for traffic capture and analysis.

Finally, Section 5 presents the tests performed and results achieved.

2. Tests objectives

Performing telecommunication network characterisation allows to measure and determine the quality and potential transmission capability of the link. Traffic characterization is an important aspect that has to be considered for efficient network management and control in the DOMEO project, specially because of the variety of sources and the nature of the multimedia information that the DOMEO network carries.

The related technical telecommunication tests allow to:

- ⇨ Characterize the various dataflow produced by the system
- ⇨ Optimize application dataflows by validating the effects of some influent parameters like audio/video codes, resolution, frequency on the flowrate
- ⇨ Evaluate the effects of the limitaton of the technologies (DSL, 3G, satellite) on the DOMEO system functions and set priority/quality trade off to comply qith required needs.

As a reminder and as introduced in D6.1 “Telecommunication overall system description”, severall parameters can be measured to characterize the network. The main ones are reminded below :

Packet loss: Packet loss occurs when one or more packets of data traveling across a computer network fail to reach their destination. Packet loss can be caused by a number of factors, including signal degradation over the network medium, oversaturated network links, corrupted packets rejected in-transit, faulty networking hardware, faulty network drivers or normal routing routines. When caused by network problems, lost or dropped packets can result in highly noticeable performance issues or jitter with streaming technologies, voice over IP, online gaming and videoconferencing, and will affect all other network applications to a degree.

Latency: Bandwidth is just one element of what a person perceives as the speed of a network. Latency is another element that contributes to network speed. The term latency refers to any of several kinds of delays typically incurred in processing of network data. A so-called *low latency* network connection is one that generally experiences small delay times, while a *high latency* connection generally suffers from long delays. Excessive latency creates bottlenecks that prevent data from filling the network pipe, thus decreasing effective bandwidth.

Delay: The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. Delay may differ slightly, depending on the location of the specific pair of communicating nodes.

Jitter: Jitter is the variation in the time between packets arriving, caused by network congestion, timing drift, or route changes. A jitter buffer can be used to handle jitter.

As explained, applications behaviour analysis allows to determine whether the application will work properly over the network or if it maybe subject to disruption. Regarding the DOMEO project, we plan to apply the tests to the following applications :

1. Lokarria : Lokarria is set up to send command to as well as to monitor Robumate
2. Visiomeeting : Visiomeeting is set up to held a videoconference between the patient (Robumate) and a remote specialist
3. Biomedical data transmission which enables Robumate to send the patient vital parameters to a distant doctor

3. Set-up configuration

3.1. General architecture

As described in Deliverable D6.2 “Telecommunication connections integration report”, the DOMEO architecture is a distributed architecture :

It is composed of four main componants, namely:

- ⇨ **The patient’s Home**, hosting the robot and the modem for telecommunication purposes.
- ⇨ **The Healthcare Professionnal office,** which is the place from which the specialist will monitor the patient and provide its diagnosis.
- ⇨ **The telemedicine contact centre,** hosting the servers and routing the traffic as well as providing contact center operators (e.g. making and receiving calls, answering questions, filling in questionnaires, sending documentation).
- ⇨ **The telecommunication network,** which allows to link the end-points to the telemedicine contact center..

3.2. Tests set-up architecture

Availability and quality of DSL and 3G networks depends on locations and operators, then it is not possible to issue generic rules and characterization. Nevertheless, the telecommunication architecture set-up at CHU Toulouse for the tests is as representative as possible of the solutions proposed over Europe and which can be implemented in Hungary or Austria for the trials.

It is also convenient to consider that 3G, DSL or Satellite is implemented on the emitter side (patient’s home) while the receiver side (telemedicine center) is always connected via Internet link. When using DSL, 3G, satellite technology, respectively a DSL, 3G, satellite gateway interfaces the DSL, 3G, satellite network with the Internet network to deliver the transmitted data to the telemedicine contact centre.

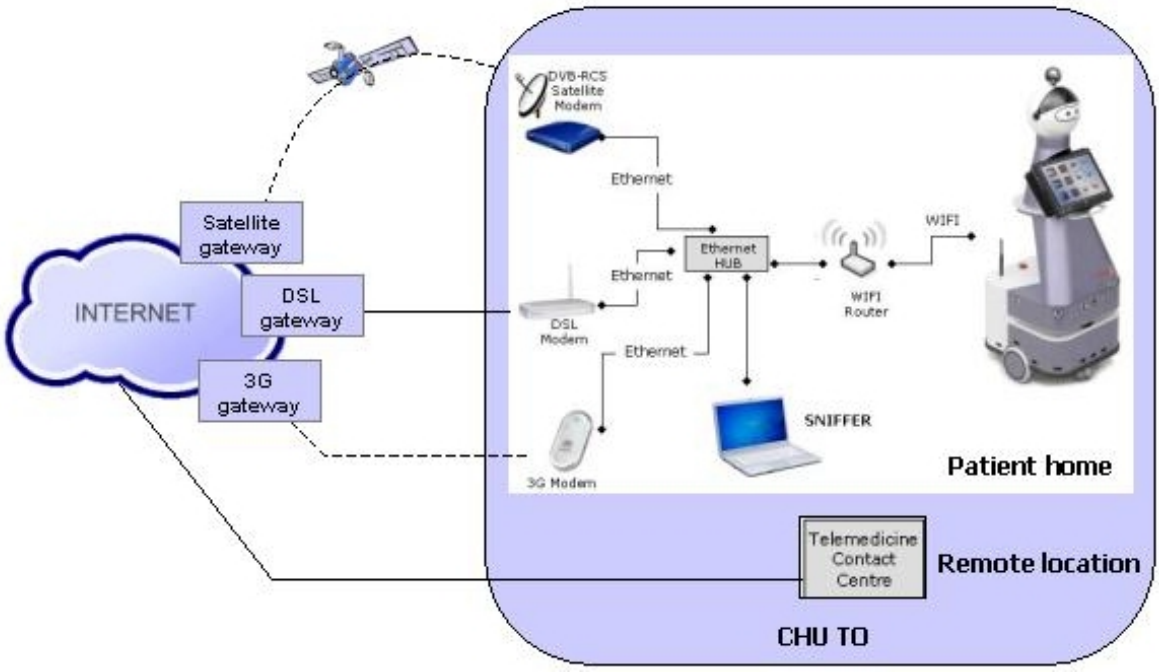

Figure 1: Test set-up architecture

In order to characterize and evaluate the relevant telecommunication parameters, a specific machine is connected to an Ethernet hub at patient's home side. This machine, also called "sniffer" will capture the traffic transmitted by the robot over the network without disturbing the dataflows.

Basically, the set-up requires the following equipment:

- A 10/100 Mbps Ethernet Hub
- A Wifi Router
- A PC equipped with software for traffic capture and analysis (see §4.2)

4. Methodology and Tools

4.1. Characterization methodology

Regarding telecommunication, the aim is to issue preliminary recommandations for each of the telecommunication architectures (DSL, 3G, Satellite) in order to optimize the overall behaviour of the DOMEO system applications.

Each dataflow must be characterized, then optimized first at network layer level and secondly at application layer level to reduce the traffic over the network while maintainaing the requested quality for patient's monitoring.

For each of the three telecommunication architectures, the proposed methodology is the following three steps methology:

Step 1: Validation of the telecommunication architecture

- ⇨ Install, connect and set-up network equipment
- ⇨ Test the end to end network link
- ⇨ Measure the characteritics of the considered architecture
    - o Available throughput (constant or burst / min, max, average value) versus theorical throughput
    - o Delay (min, max, average)
    - o Jitter (min, max, average)
    - o Packets loss (average)

Step 2: Flowrate characterization before optimisation

Once the telecommunication architecture is validated, it is necessary to characterize the applications before any improvement or optimization in order to know if the the applied changes/tuning is impacting the flowrate or more globally the overall performances of the system.

- ⇨ Play each function of the DOMEO application with default parameters
- ⇨ Modify the parameters and have the opinon of the user to analyze whether the modification improves or decreases the function
- ⇨ Capture the traffic at the network layer level and measure the related network characteristics for each funtion
    - o Throughput
    - o Delay (min, max, average)
    - o Jitter (min, max, average)
    - o Packets loss (average)

Step 3: Definition of the fine-tuned configuration

Step 3 consists in fine-tuning of the system wrt the telecommunication link. It allows with successive iterations to determine the fine parameters that guarantee the best result. Each parameter is modified and the impact is compared to the result obtained on Step 2. In case of improvement, the new value of the parameter is kept otherwise it is rejected.

- ⇨ Computer IP stack optimization
    - o IP packet size
    - o Buffer size
    - o Traffic congestion algorithm

- Selective acknoledgement algorithm
- MTU, PMTU

⇨ IP header compression
- QoS

⇨ QoS rules implementation
- PHB mechanism according to packet tagging. A PHB provides a particular service level (bandwidth, queuing and dropping decisions) in accordance with network policy.

4.2. **Measurement tools**

This section currently provides a short description of the 3 software measurement tools which have been installed on the test computer to proceed with DOMEO network characterisation.

⇨ **Iperf** is an easy-to-use free command line tool that allows to measure the network bandwidth by generating artificial traffic. Such a tool is useful to test whether the network speed is fast enough for Visiomeeting and Lokarria applications or not.

⇨ **Wireshark** is a network packet analyzer. This usefull network packet analyzer helps to capture network packets and to display that packet data as detailed as possible.

⇨ **Ntop** is a tool that shows network traffic usage. When installed in a place where it can capture network traffic (hub or a mirrored port of a switch), it logs and reports information concerning IP and traffic generated by each host in the network.

4.2.1. **Iperf**

Iperf is a tool to measure the bandwidth and the quality of a network link. The network link is delimited by two hosts running Iperf.

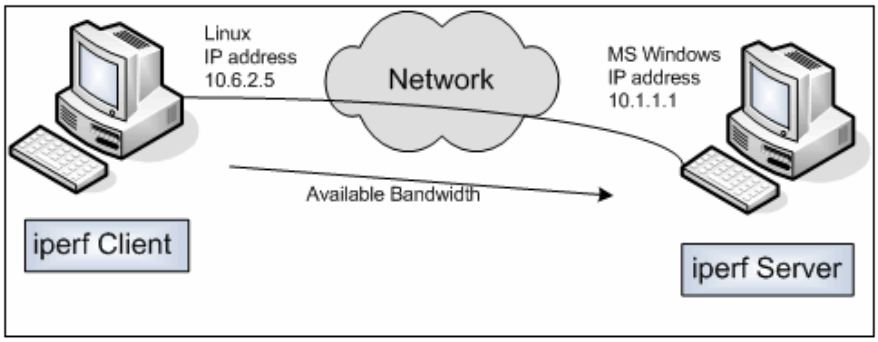

Figure 2: IPerf implementation

The quality of a link can be tested as follows:

- Latency (response time or RTT): can be measured with the Ping command.
- Jitter (latency variation): can be measured with an Iperf UDP test.
- Datagram loss: can be measured with an Iperf UDP test.

IPerf is based on a client/server model. As such IPerf binaries have been installed on all machines taking part in testing. IPerf is started on one node in 'server' mode (Visiomeeting, Lokarria servers). This node sits and listens for a connection on a specific port. IPerf is then started on the second node in 'client' mode (Robumate) and is provided with the host name or IP address of the

'server' node. The client node attempts to initiate a connection with the server node and once connected starts to push data over the connection.

The bandwidth is measured through TCP tests. IPerf attempts to push as much data as possible over the connection in a given amount of time and once complete uses the time taken and amount of data pushed to calculate a perceived bandwidth for the connection. To be clear, the difference between TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) is that TCP use processes to check that the packets are correctly sent to the receiver whereas with UDP the packets are sent without any checks but with the advantage of being quicker than TCP.
Iperf uses the different capacities of TCP and UDP to provide statistics about network links.

Before using IPerf to test the DOMEO network throughput between primary and secondary nodes we have ensured the following :

1) Any replication must be stopped. If running, replication is using a certain proportion of the available bandwidth between the nodes and as such causes IPerf to give an artificially small value for available bandwidth which can be misleading.
2) Any component using the port used to test throughput must be stopped. Failure to do this can cause IPerf to fail as it cannot bind to a given port or to give misleading results.

4.2.2. **Wireshark**

Wireshark is the world's most popular network analyzer. It is basically a tool for seeing the bits and bytes flowing through the network in human readable form. Without it, understanding a network communication exchange would be quite difficult.

Network protocol is broken down into 7-layers (see the OSI 7-layer model). The part that WireShark deals with is layer 2 up to 7. Most well know protocols can be decoded by WireShark.

The Wireshark strength comes from:

- its easiness to install.
- the simplicity of use of its GUI interface.
- the very high number of functionality available, among which are :
  - Deep inspection of hundreds of protocols, with more being added all the time
  - Live capture and offline analysis
  - Standard three-pane packet browser
  - Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
  - Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
  - Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
  - Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2

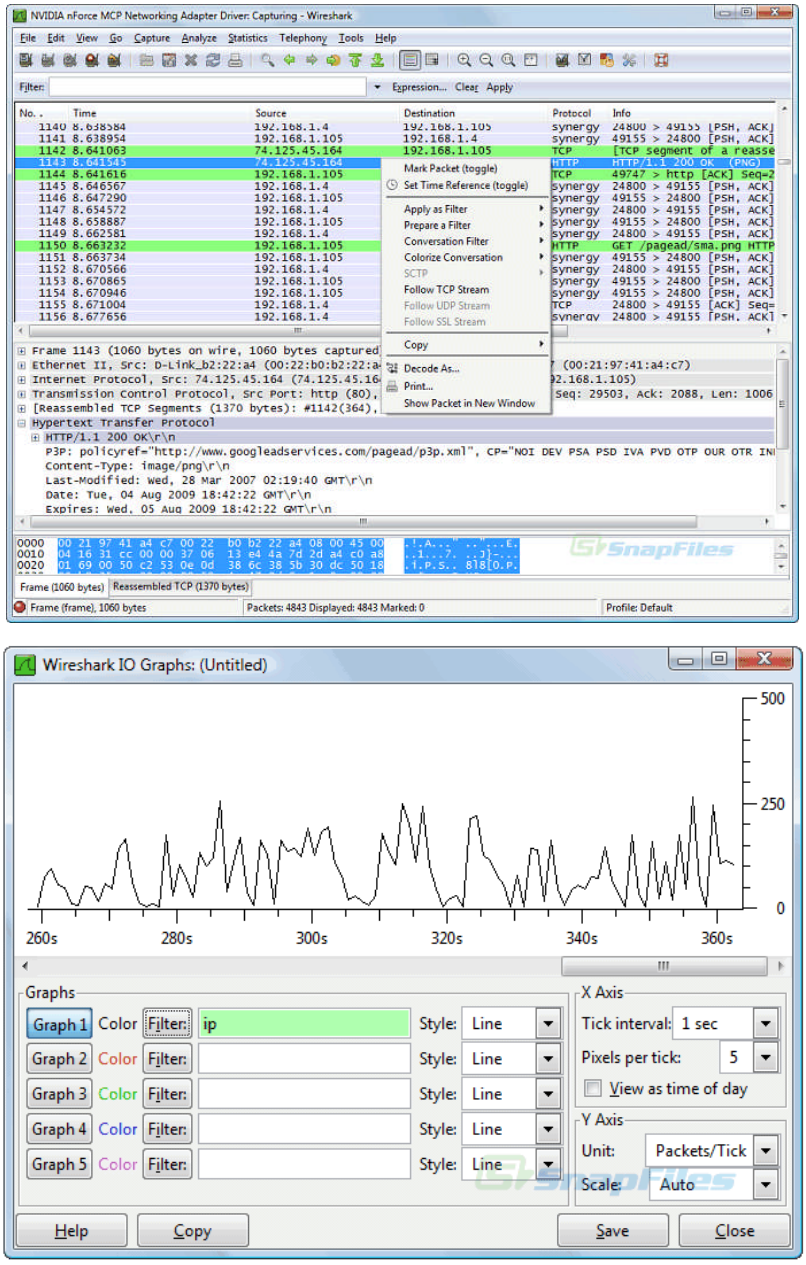

Figure 3: Wireshark screenshots

4.2.3. **Ntop**

Ntop is a network probe that shows network usage in a way similar to what top does for processes. In interactive mode, it displays the network status on the user's terminal. In Web mode, it acts as a web server, creating a HTML dump of the network status. It sports a NetFlow/sFlow emitter/collector, a HTTP-based client interface for creating ntop-centric monitoring applications, and RRD for persistently storing traffic statistics.

Basically Ntop allows to:

- Sort network traffic according to many protocols
- Show network traffic sorted according to various criteria
- Display traffic statistics
- Store on disk persistent traffic statistics in RRD format

- Identify the indentity (e.g. email address) of computer users
- Passively (i.e. withou sending probe packets) identify the host OS
- Show IP traffic distribution among the various protocols
- Analyse IP traffic and sort it according to the source/destination
- Display IP Traffic Subnet matrix (who's talking to who?)
- Report IP protocol usage sorted by protocol type
- Act as a NetFlow/sFlow collector for flows generated by routers (e.g. Cisco and Juniper) or switches (e.g. Foundry Networks)
- Produce RMON-like network traffic statistics

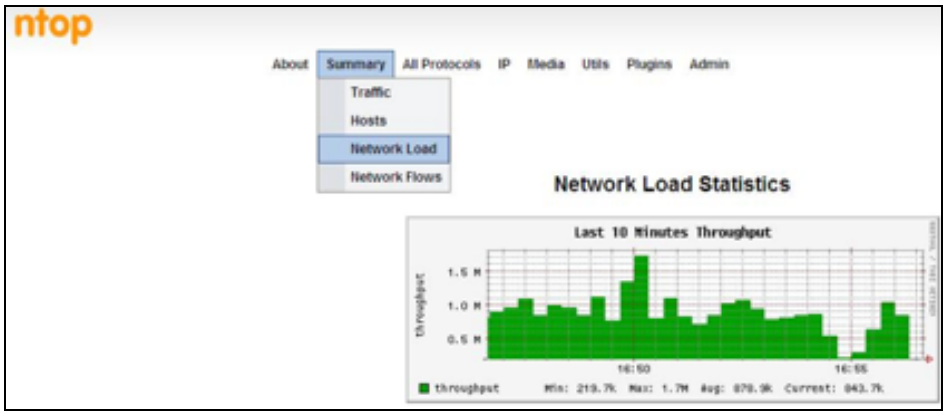

Figure 4: Ntop screenshot

5. Network characterization

The work consists mainly in characterizing the link between the robot (Robumate) and the server (Lokarria). Before doing anything, it is necessary to set up a fast, secure and reliable way to share information between both end points.
One popular technology to accomplish these goals is a VPN (virtual private network). A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. The VPN uses "virtual" connections routed through the Internet from the business's private network (Lokarria server location) to the remote site (Robumate location).

The testbed infrastructure, including 3G, Satellite and ADSL network access lines, has been set-up at CHU Toulouse premises (see §3.2).

The equipment dedicated to the tests are properly integrated into the overall infrastructure.
Appropriate softwares have been installed to allow traffic capture and analysis (see §4.2)

For each of the selected 3G, Satellite and ADSL technologies, a three steps procedure is applied including:

1) Blank link characterization
2) VPN setting-up analysis
3) Traffic capture during robot operation (moving)

From these different steps, traffic analysis plots and detailed traffic parameters are recorded. Traffic analysis plots are extracted from capture sequences, whose duration is one hour. Detailed traffic analysis results are a photo of the traffic at any given moment.

5.1. Satellite link characterization

5.1.1. Satellite blank link performances

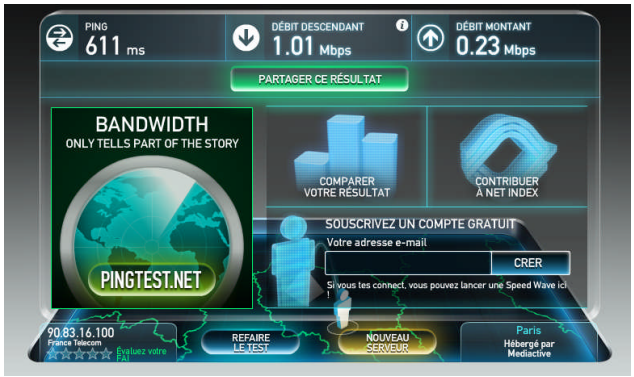

Figure 5: Satellite link performances

Before launching any application on the satellite network, it is necessary to define the performances of the blank satellite link. Then when running an application like videoconference, we can compare the new parameters with the blank ones and analyse the impact of the application on satellite network.

The blank link performances are obtained using the online www.pingtest.net tool, which runs a ping from the local machine to the a dedicated server on the WEB.
For the satellite link, results are:

- delay 611 ms
- downstream rate 1.01 Mbps
- upstream rate 230 kbps

5.1.2. **Setting up VPN in Satellite network**

Figure 6 illustrates the Satellite traffic changes while opening VPN connection between Robumate and Lokarria server. Set-up of the VPN connection has been achieved in about 3 secondes.

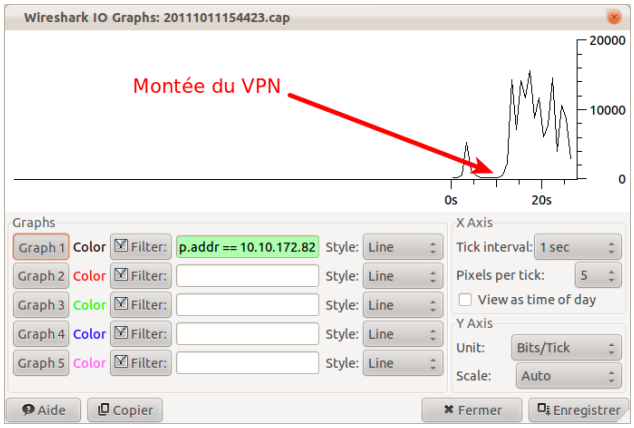

Figure 6: Opening VPN in satellite network

Figure 7 provides traffic details in terms of packets number, average packets size, average bytes and bitrate per seconde. It is noticable that the average occupied bandwidth is around 13 kbps (0,013 Mbit/sec), which is considered as negligible compared to the above measured satellite blank link values and that the average packet size of 164 bytes is small.

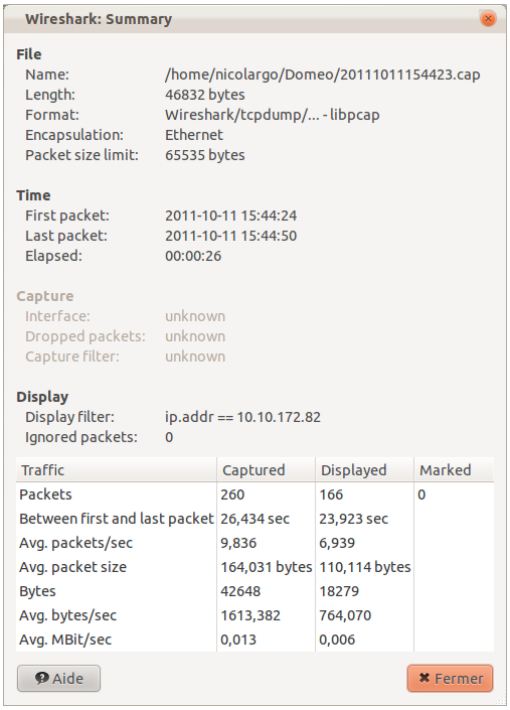

Figure 7: VPN/Satellite - Detailed traffic analysis

Closing of the VPN connection in satellite network has been achieved in a few secondes.

5.1.3. **Satellite Traffic analysis during operations**

The current section provides satellite traffic information during Robumate operations. While moving, Robumate receives acknowledgements, command and control information from the Lokarria server while it sends back localisation information or patient data to the server. This produces some traffic as illustrated on Figure 8, which is much higher from the robot to the server than from the server to the robot.

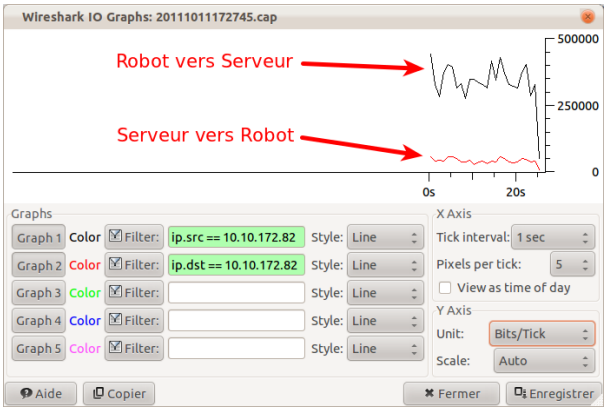

Figure 8 Satellite traffic analysis while robot moving

The detailled analysis of packets lenght sharing illustrated on Figure 9 provides relevant information. We can see that about 70% of the packets sent/received are in the range from 80 to 1279 bytes while 20% are higher than 1280 bytes.

In computer networking, the maximum transmission unit (MTU) of a communications protocol of a layer is the size in bytes of the largest protocol data unit that the layer can pass onwards. A large MTU brings great efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU also means processing of fewer packets for the same amount of data. In some systems, per-packet-processing can be a critical performance limitation.

For our tests, the MTU has been optimised and fixed to 1320 bytes.
Accordingly, we can consider that about 70% of the transmitted packets do not require fragmentation to match with this MTU size.

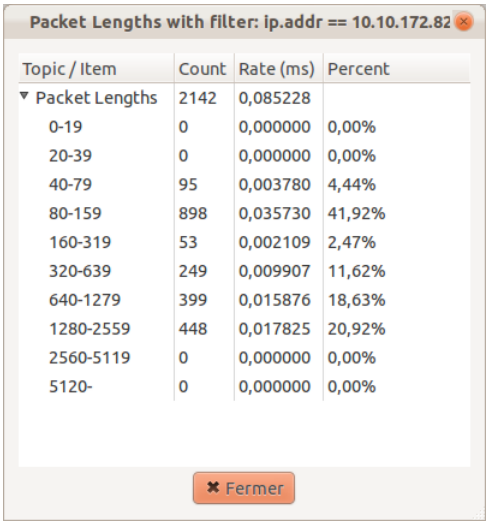

Figure 9 Packets length representation over satellite network

5.2. 3G link characterization

5.2.1. 3G blank link performances

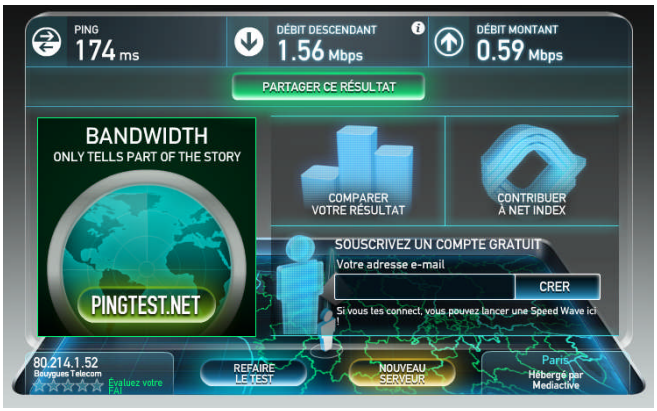

Figure 10: 3G link performances

Before launching any application on the 3G network, it is necessary to define the performances of the blank 3G link. Then when running an application like videoconference, we can compare the new parameters with the blank ones and analyse the impact of the application on 3G network.

The blank link performances are obtained using the online www.pingtest.net tool, which runs a ping from the local machine to the a dedicated server on the WEB.
For the 3G link, results are:

- delay 174 ms
- downstream rate 1.56 Mbps
- upstream rate 590 kbps

5.2.2. Setting up VPN in 3G network

Figure 11 illustrates the 3G traffic changes while opening VPN connection between Robumate and Lokarria server. Set-up of the VPN connection has been achieved in about 3 secondes like for satellite network.

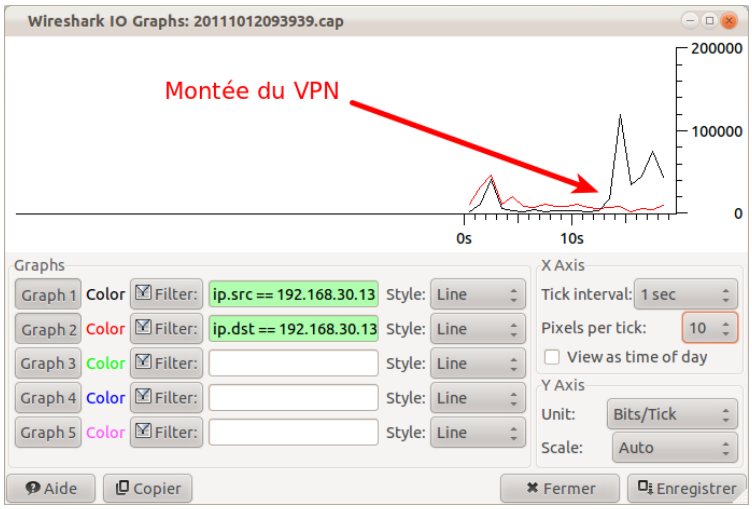

Figure 11 Opening VPN in 3G network

Figure 12 provides 3G traffic details in terms of packets number, average packets size, average bytes and bitrate per seconde. It is noticable that the average occupied bandwidth is around 42 kbps (0,042 Mbit/sec), which is considered as negligible compared to the above measured satellite blank link values and that the average packet size of 178 bytes is small.

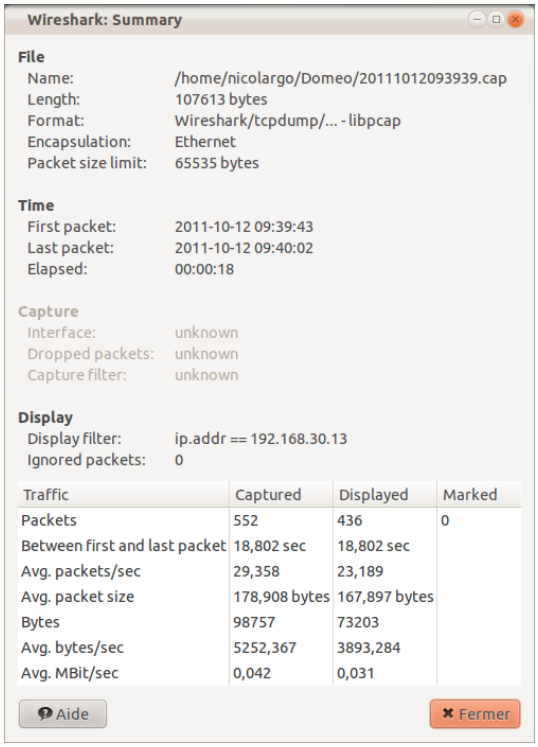

Figure 12 VPN/3G - Detailed traffic analysis

5.2.3. **3G Traffic analysis during operations**

The current section provides 3G traffic information during Robumate operations. While moving, Robumate receives acknowledgements, command and control information from the Lokarria

server while it sends back localisation information or patient data to the server. This produces some traffic as illustrated on Figure 13, which is much higher from the robot to the server than from the server to the robot.

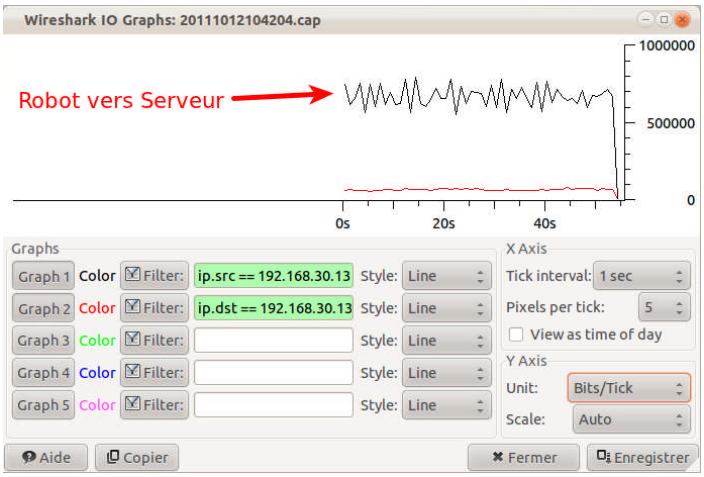

Figure 13 3G-traffic analysis while robot moving

The detailled analysis of packets lenght sharing illustrated on Figure 14 provides relevant information. We can see that about 66% of the packets sent/received are in the range from 80 to 1279 bytes while 33.5% are higher than 1280 bytes.

The size of the MTU in 3G network is the same (1320 bytes) as in satellite network.
Accordingly, we can consider that about 66% of the transmitted packets do not require fragmentation to match with this MTU size. Results are in the same order of magnitude regarding both satellite and 3G networks.

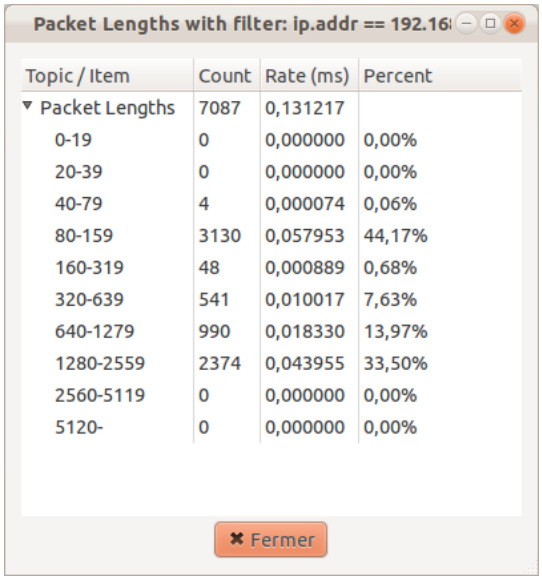

Figure 14 Packets length representation over 3G network

5.3. **ADSL link characterization**

Due to the lack of dedicated ADSL link at CHU Toulouse, it has been decided to conduct the tests at the healthcare giver office.

Figure 15: ADSL link performances

Before launching any application on the ADSL network, it is necessary to define the performances of the blank ADSL link. Then when running an application like videoconference, we can compare the new parameters with the blank ones and analyse the impact of the application on ADSL network.

The blank link performances are obtained using the online www.pingtest.net tool, which runs a ping from the local machine to the a dedicated server on the WEB.
For the ADSL link, results are:

- delay 59 ms
- downstream rate 6.46 Mbps
- upstream rate 640 kbps

5.3.1. **Setting up VPN in ADSL network**

It has been noted that the ADSL traffic changes while opening VPN connection between Robumate and Lokarria server are very similar to the traffic changes observed with 3G network. Set-up of the VPN connection has been achieved in about 3 secondes like for satellite network.
It has been as well observed that traffic details in terms of packets number, average packets size, average bytes and bitrate per seconde for ADSL network again is very similar to 3G network.

5.3.2. **ADSL Traffic analysis during operations**

The current section provides ADSL traffic information during Robumate operations. While moving, Robumate receives acknowledgements, command and control information from the Lokarria server while it sends back localisation information or patient data to the server. This produces some traffic as illustrated on Figure 16, which is much higher from the robot to the server than from the server to the robot.

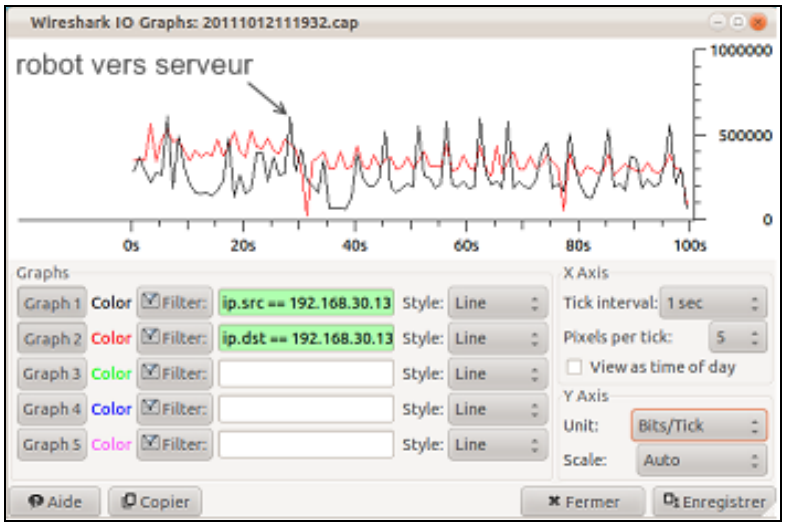

Figure 16 ADSL-traffic analysis while robot moving

The symmetrical aspect of the plot is due to some additional application, like videoconferencing, runing during operations.

The detailled analysis of packets lenght sharing illustrated on Figure 17 provides relevant information. We can see that about 100% of the packets sent/received are in the range from 80 to 1279 bytes.

The size of the MTU in ADSL network is the same (1320 bytes) than in satellite and 3G networks. Accordingly, we can consider that about 100% of the transmitted packets do not require fragmentation to match with this MTU size.

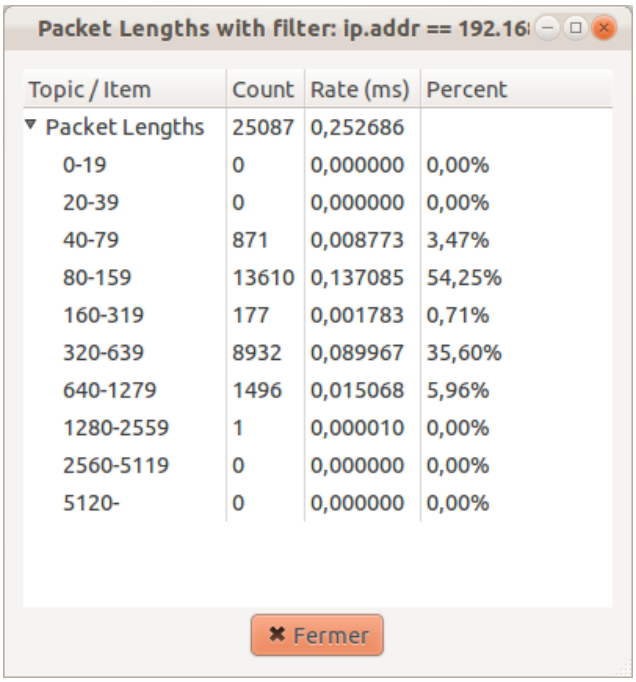

Figure 17 Packets length representation over ADSL network

6. CONCLUSION

The main conclusion of the technical tests phase is that the DOMEO system works on the three identified network technology. This offers a great potential for further deployment of the DOMEO system as it gives the opportunity to select one of the three technologies according to its availability and installation constraints.

The three network technologies have globally good performances. It could be assumed that ADSL network is the most appropriate, that 3G network is a good candidate as well while satellite network remains a possibility in case both previous networks are not available. However, it is important to note that performances may be subject to the time of use as a heavy traffic may occur at peak hours and then decrease performances.

Traffic analysis has demonstrated the importance of the MTU parameter. As far as packet size is higher than MTU, packets may need to be fragmented. Large packets can occupy a slow link for some time, causing greater delays to following packets and increasing lag and minimum latency. Large packets are also problematic in the presence of communications errors. Corruption of a single bit in a packet requires that the entire packet be retransmitted. At a given bit error rate larger packets are more likely to be corrupted. Retransmissions of larger packets take longer.
Accordingly, the main recommandation will be the packet size not to exceed the MTU in order to avoid fragmentation.

Additional considerations can also be addressed to increase the DOMEO system performances, like optimisation of the TCP/IP stack of Robumate and Lokarria server, selective acknoledgement algorithms, read/write buffering size. It is also necessary to manage the IP addresses translation mechanism to allow deployment of the DOMEO system with public Internet access ADSL box.

End of document