Seventh Framework Programme
Information and Communication Technologies
Theme

EVALUATION METRICS AND TEST PLAN

MONET
Grant No. 247176

Deliverable Information
Deliverable Number: D3.2 **Work Package:** WP3
Date of Issue: 13/01/2011
Document Reference: MONET-ICT-247176-D3.2
Version Number: 1.0
Nature of Deliverable[1]: R **Dissemination Level of Deliverable[2]:** PU
Author(s): ASTRIUM (Responsible), UNIS, TEKEVER, UoR-CRAT, URSZR
Keywords: Performance measurement, evaluation, parameter, metric, test plan
Abstract:
This deliverable D3.2 of the work package 3 aims to define the metrics or combinations thereof for performances assessment based on the requirements defined in WP2 and on the general architecture definition realised in WP3. This definition will be used as what to measure in the test plan later. It is also to determine baselines for performance comparison in order to evaluate the designed system.

A test plan is to be defined in this deliverable which aims to assess all the functions, techniques and performances. This plan will be carried out in WP6 for the integration and testing work. It will cover several issues in addition to what to measure as defined in the early part of this deliverable including why to measure, how to measure, when to measure as well as expected test outputs.

[1] Nature of deliverable: **R** = Report; **P** = Prototype; **D** = Demonstrator; **O** = Other
[2] Dissemination level: **PU** = Public; **PP** = Restricted to other programme participants (including the Commission Services); **RE** = Restricted to a group specified by the consortium (including the Commission Services); **CO** = Confidential, only for members of the consortium (including the Commission Services).

Document History

Date	Version	Remarks
27/05/2010	0.1	Draft content
05/07/2010	0.2	First comments and contributions
30/08/2010	0.3	Contributions coordinated with D3.1
07/09/2010	0.4	Draft revision
06/10/2010	0.5	Contributions resulting from progress meeting in Slovenia
08/11/2010	0.6	Final contributions by partners
10/01/2011	0.7	Final Draft
13/01/2011	1.0	First issue

Document Authors

Entity	Contributors
UNIS	Lei Liang, Dan He, Zhili Sun
ASTRIUM	Michael Crosnier, Melanie Monier, Valentin Kretzschmar, Fabrice Planchou, Cedric Le Guern
TEKEVER	André Oliveira, Mário Lima, Igor Ferreira
CRAT	Andrea Fiaschetti, Marco Castrucci, Roberto Cusani, Guido Oddi, Antonio Pietrabissa, Alberto Isidori
URSZR	Katja Juroš, Boštjan Tavčar

Executive Summary

This document describes the testing procedures that will be used for MONET validation. The MONET project describes an entire network system whose requirements have been defined based on end-users interview and requests, and corresponding scenarios. The architecture of the system has been built so that it answers the best to those requirements, in order to guarantee that MONET meets end-users demands and reach maximum usability.

With this objective in mind, it is important that the architecture goes through a testing phase that will ensure that the system that implemented effectively addresses the project primary goals. In MONET, the validation procedure has been split in two subsequent steps:

i) At first, a validation phase with the purpose to show the end-users what has been achieved in the project and the functional features of the prototype is planned
ii) Secondly, a test phase that will have the prototype undergo an extensive test campaign in order to verify its compliance with technical requirements will follow.

This document focuses on this second phase. However, it is not the goal of this document to describe all of the test scenarios, as this will be done later in the project so that they are more compliant with MONET prototype which is yet to be developed in WP4. So this document is both a preparatory work for the following steps of the project, and a framework that will help define the test campaign afterwards.

The first step is to define the metrics that will help to verify that MONET reaches the targeted performances and features. These metrics have to accurately cover the particularities of the MONET system and provide a mean to assess every aspects of the system. Some basic metrics that are generally used to measure any network performances will be completed by more advanced metrics specific to MONET. These advanced metrics can be a combination of simple network metrics adapted to the particular context of MONET, or entirely different metrics which are only relevant to this project.

In a second part of this document, the test-bed that will be used for the test campaign is described. This work is mandatory as it will provide directions for implementation regarding what is to be tested. Each equipment of the test-bed is described, from the simulation equipments that reproduce the transmission environment (wireless communication and satellite link), to the MONET nodes that are actually tested. At this stage, the monitoring tool that will measure the previously mentioned metrics will also be described.

Finally, an example of what a test scenario will look like is provided in order to give the reader useful indications on how each test will be built. This example will serve as guidelines for the upcoming definition of all the test scenarios.

Table of Contents

List of Tables

List of Figures

List of Acronyms

Acronym	Meaning
ACM	Adaptive Coding and Modulation
AMP	Active Measurement Program
ATM	Asynchronous Transfer Mode
BLUELab	Broadband Links Under Experiment LABoratory
BOD	Bandwidth On Demand
BMWG	Benchmarking Methodology
CAIDA	Cooperative Association for Internet Data Analysis
CCM	Constant Coding and Modulation
DVB-S2	Digital Video Broadcasting - Satellite - Second Generation
DVB-RCS	Digital Video Broadcasting Return Channel by Satellite
EAX	Expected Any-path Transmissions
ExACT	Expected Any-path Communication Time
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IPPM	IP Performance Metrics
GPS	Global Positioning System
LiPo	Li-ion Polymer
M&C	Monitoring and Control
MIB	Mobile Information Base
MONET	Mechanisms for Optimization of hybrid ad-hoc networks and satellite NETworks
MPR	Multipoint Relay
OLSR	Optimized Link State Routing Protocol
PDR	Packet Delivery Ratio
PTT	Push-To-Talk
QEF	Quasi-Error Free
QoE	Quality of Experience
QoS	Quality of Service
RF	Radio Frequency
RFC	Request for Comments
RIO	Real-time IP Observer
RIPE	Réseaux IP Européens
RMON	Remote MONitoring
RP	Rendezvous Points
RTT	Round Trip Time
SATEM	SATellite EMulator
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
TCP	Traffic Control Protocol
UDP	Uniform Datagram Protocol
VCM	Variable Coding and Modulation
WP	Work Package

Table 1 – List of acronyms.

1 Introduction

1.1 Purpose and Scope of the Document

This document describes the testing procedures that will be used for MONET validation. The MONET project describes an entire network system whose requirements have been defined based on end-users interview and requests, and corresponding scenarios. The architecture of the system has been built so that it answers the best to those requirements, in order to guarantee that MONET meets end-users demands and reach maximum usability.

With this objective in mind, it is important that the architecture goes through a testing phase that will ensure that the system that implemented effectively addresses the project primary goals. In MONET, the validation procedure has been split in two subsequent steps:

iii) At first, a validation phase with the purpose to show the end-users what has been achieved in the project and the functional features of the prototype is planned

iv) Secondly, a test phase that will have the prototype undergo an extensive test campaign in order to verify its compliance with technical requirements will follow.

This document focuses on this second phase. However, it is not the goal of this document to describe all of the test scenarios, as this will be done later in the project so that they are more compliant with MONET prototype which is yet to be developed in WP4. So this document is both a preparatory work for the following steps of the project, and a framework that will help define the test campaign afterwards.

1.2 Organization of the Document

The document is structured as follows: in the first part performance measurements and metrics will be introduced, specific both for a generic network and in the MONET context. In the second part the test bed used in MONET will be described as well as a sample test scenario. At the end of the document some major conclusions will be drawn.

2 Performance Measurement and Metrics

2.1 Introduction to Performance Measurement

IP network performance measurement is crucial to the traffic engineering function. It provides the means to have insights on the network operation state and can be used for problem anticipation. It is useful for optimising the network because it can provide the feedback data for the engineer to adaptively optimise network performance in response to events and stimuli originating within and/or outside the network. It is essential to determine the quality of network services and to evaluate the effectiveness of traffic engineering policies. Indeed experience indicates that measurement is most effective when acquired and applied systematically [Awduche2002].

To deploy the measurement on a network, one has to address the following questions:

- Why is measurement needed in this particular context?
- What parameters are to be measured?
- How should the measurement be accomplished?
- Where the measurement should be performed? When should the measurement be performed?
- How frequently should the monitored variables be measured?

- What level of measurement accuracy and reliability is desirable?
- What level of measurement accuracy and reliability is realistically attainable?
- To what extent can the measurement system permissibly interfere with the monitored network components and variables?
- What is the acceptable cost of measurement?

The answers to these questions will determine what measurement tools and methodologies are suitable for the particular engineering context.

Measurement in support of the TE function can occur at different levels of abstraction. For example, measurement can be used to derive packet level characteristics, flow level characteristics, user or customer level characteristics, traffic aggregate characteristics, component level characteristics, and network wide characteristics [Awduche2002].

2.2 Network Performance Metrics and Measurement

The identification of what parameters are needed to measure is the most important factor before launching the measurement procedure. It is the key to decide measurement tools, methodologies and accuracy. The Internet Engineering Task Force (IETF) IP Performance Metrics (IPPM) working group has developed a set of standard metrics that can be applied to the quality, performance, and reliability of Internet data delivery services. Another working group named Benchmarking Methodology (BMWG) made a series of recommendations concerning the measurement of the performance characteristics of various internetworking technologies, which includes terminology, identifying a set of metrics that describes the traffic characteristics, and methodologies required to collect those metrics. Additionally, the ITU-T Working Group T1A1.3 made a similar network performance parameter definition [ITU-T2002].

The IPPM developed a set of parameters as well as the correspondent measurement methodologies with the cooperation of other related working group such as BMWG, TEWG, ITU-T SG 12 and SG 13. Those parameters include:

- **Connectivity**: If a packet transmitted at time T from a source A can reach its destination B, it is said that A has the connectivity to B at time T.
- **One-way delay**: The difference between the time when the source sends out the first bit of the packet and the time when the destination receives the last bit of the packet.
- **One-way loss**: If a packet transmitted from source A cannot reach its destination B in a limited time, it is said that this packet is lost;
- **Round-trip delay**: The total time needed for a test packet to travel from source A to destination B and back to A.
- **One-way delay variation**: The difference between the one-way delays of a selected pair of packets in the stream going from source A to destination B.
- **Loss patterns**: The packet loss statistical distribution.
- **Bulk transport capacity**: The expected long term average data rate (bits per second) of a single ideal TCP implementation over the path in question.

The IPPM defined a general framework [Paxson1998] for particular parameter metrics that can be deployed to gain common understanding by Internet users and Internet providers of the performance and reliability. These metrics apply both to end-to-end paths through the Internet and to specific 'IP clouds' that comprise portions of those paths. The term “metric” is defined as a carefully specified quantity that is relative to the Internet performance and reliability. It recommends defining particular metrics under some criteria and disciplines in

order to allow people to speak clearly about Internet traffic performance. In several IETF meetings criteria for these metrics have been specified as follow [Paxson1998]:

- These metrics must be concrete and well defined.
- A methodology for a metric should have the property that it is repeatable: if the methodology is used multiple times under identical conditions, it should result in consistent measurements.
- The metrics must exhibit no bias for IP clouds implemented with identical technology.
- The metrics must exhibit understood and fair bias for IP clouds implemented with non-identical technology.
- The metrics must be useful to users and providers in understanding the performance they experience or provide.
- The metrics must avoid inducing artificial performance goals.

Each parameter metric will be defined in terms of standard units of measurement. The international metric system will be used, with the following points specifically noted:

- When a unit is expressed in simple meters (for distance/length) or seconds (for duration), appropriate related units based on thousands or thousandths of acceptable units are acceptable. Thus, distances expressed in kilometres (km), durations expressed in milliseconds (ms), or microseconds (us) are allowed, but not centimetres (because the prefix is not in terms of thousands or thousandths);
- When a unit is expressed in a combination of units, appropriate related units based on thousands/thousandths of acceptable units are acceptable, but all such thousands/thousandths must be grouped at the beginning. Thus, kilometres per second (km/s) are allowed, but meters per millisecond are not;
- The unit of information is the bit.
- When metric prefixes are used with bits or with combinations including bits, those prefixes will have their metric meaning (related to decimal 1000), and not the meaning conventional with computer storage (related to decimal 1024). In any RFC that defines a metric whose units include bits, this convention will be followed and will be repeated to ensure clarity for the reader.

2.2.1 General Network Performance Measurement

Lots of research has been done to develop measurement methodologies, e.g. using LOG files and capturing packets form the Internet using software and hardware tools. The measurement methodologies can be divided into two main categories: *passive* and *active*. Both have their advantages and should be considered as complementary. They can also be used together.

2.2.1.1 Passive Measurement

The passive measurement approach implies to use devices to monitor the traffic when it passes by. These devices could be some specific tools such as sniffer hardware, or they can be pure software built into some network equipments such as routers, switches and end node hosts. Examples of such built in techniques include Remote Monitoring (RMON) [Waldbusser2000], which enables various network monitors and consoles to exchange the monitored network data using a kind of database named Management Information Base (MIB), and Simple Network Management Protocol (SNMP) [Presuhn2002] [Presuhn2002A],

which is one network management protocol by using specific messages and MIB, capable devices.
The passive measurement will not create or modify the traffic on the network. This is the main difference with active measurement, in which specific test packets are introduced into the network. The basic principle of the passive measurement can be shown on Figure 1.

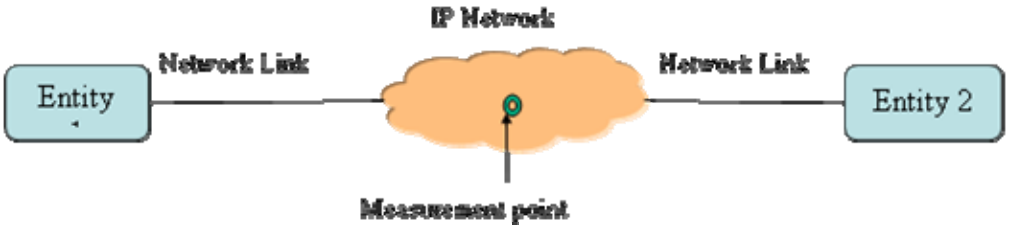

Figure 1 - Basic principle of passive measurement

Figure 1 shows that two Entities are connected via an IP network through network links. The traffic between these two entities is measured at a specific point. The "Entity" on Figure 1 can represent various network situations. For example, the two Entities could be two end users or one organization internal network and the external Internet, or two routers, and so on. They could also be two part of the Internet, e.g. the backbone and one edge network.

Passive measurement can provide a set of detailed information of the interested traffic at one point in the network that is being measured. Examples of the information passive measurements can provide are:

- Traffic / protocol mixes
- Accurate bit or packet rates
- Packet timing / inter-arrival timing

It can also be deployed as a network application debugging method by capturing the entire packet contents. All of these advantages make the passive measurement valuable in network trouble-shooting, single node behaviour study, source modelling and capacity management.

There are two major categories that passive measurement systems can fall into. The first is on-line processing that process data in real time. For instance, observing packet type, throughput in a period of time, and so on. It is useful to monitor the instant network status and bandwidth utilization situation.

The second category is off-line processing that enables the monitoring device to save the captured packets as well as additional information such as arrival time. The captured data is then processed and analysed after the measurement.

The on-line processing requires very powerful devices to capture the packet while doing extra calculation when monitoring a high-speed network. This is the case, for example, of a user that wants to know the instant throughput with a graph based on the captured traffic. In nominal conditions, the monitoring device would save the captured packets in a buffer and update the throughput graph periodically. But when the link is heavily loaded (hundreds of megabytes per second for instance), it is highly possible that the monitoring device might drop packets passing by while calculating the throughput and updating the graph. It could be worse when users want to know many instantaneous parameters. Therefore, analyzing the traces off-line will be much suitable though it costs more storage space to save packets and relevant additional information. One can spend more time to derive more details, such as inter-arrival time, packet lost rate, flow distributions and so on, from these saved traces.

People have tried to save partial packets instead of its entire contents in order to save both processing time and storage space. One very common subset of the data that is saved is the IP header and transport layer headers. One other common subsection of data captured is the data link layer headers. This is used primarily in ATM networks, but this type of capture has limited use for IP level analysis. The IP header provides information on the source of the datagram, the destination of the datagram, the length of the datagram and which transport protocol is carried in the payload. The transport layer can give an indication of what type of traffic was contained within the packet.

Header traces are commonly used for both of the on-line and off-line passive measurement configurations discussed, and wherever the network speed allows traces to be taken. Full capture of all packet data on a link is normally restricted to the on-line process situation. The data rates created by a single computer are low when compared to backbones and gateways. Full capture allows complete analysis of the actual data passing on the network, which could be used for debugging purposes and also allow later `playback' of the entire data stream.

2.2.1.2 Active Measurement

The active approach relies on the capability to inject test packets into the network or send packets to servers and applications. It increases the network traffic. The volume and other parameters of the introduced traffic are fully adjustable and small traffic volumes are enough to obtain meaningful measurements.

Active measurement provides very little information about a single point of a network. It instead provides a representation of the characteristics of the entire network path between two hosts. Active systems can provide such indications of a networks performance as:

- Packet round trip time (RTT);
- Average packet loss;
- Connection bandwidth.

Some active systems can also give indications of the following:

- Asymmetric delay times;
- Alterations in routing paths between hosts.

The active approach provides explicit control on the generation of packets for measurement scenarios. This includes control on the nature of traffic generation, the sampling techniques, the timing, frequency, scheduling, packet sizes and types (to emulate various applications), statistical quality, the path and function chosen to be monitored. Being active implies testing what you want, when you need it. Emulation of scenarios is easy and checking whether QoS or Service Level Agreements (SLA) are met or not is relatively straightforward.

There are several public projects deploying active measurement. They can be divided in two categories, taking into account whether they make one-way measurements or round trip (two-way) measurements. Surveyor project (http://www.advanced.org/surveyor/) and Réseaux IP Européens (RIPE) (http://www.ripe.net/ripe/) make one-way delay measurements and require a Global Positioning System (GPS) to provide clock synchronization between sites. NLANR Active Measurement Program (AMP) (http://amp.nlanr.net/AMP/) & Ping End-to-end Reporting (PingER) (http://www-iepm.slac.stanford.edu/pinger/) make two-way measurements using the Internet Control Message Protocol (ICMP) ping facility today, and do not require a GPS. The Cooperative Association for Internet Data Analysis (CAIDA) using a measurement tool named skitter (http://www.caida.org/tools/measurement/skitter/) aims more at global Internet

measurements and so tends to be more generic than the others and in some ways the most unique among the five.

Passive measurement and active measurement are very different in terms of increase of network traffic and measurement objective. However, they are complementary rather than competing approaches. For example, the active measurement probe can schedule passive measurements of appropriate metrics at appropriate points along the path, while the active measurements are being made. When the active measurement is completed then the appropriate passive measurements can be paused thus reducing the gathering of unnecessary data. By comparing and contrasting the active and passive measurements, the co-validity of the different measurements can be verified, and much more detailed information on carefully specified/scheduled phenomena is made available. It is very common that one may need both measurement results to gain the final conclusion.

2.2.2 General Network Performance metrics

IPPM gives 6 sets of standardized metrics for the following parameters under the above criteria:

- Metrics for measuring connectivity [Mahdavi1999];
- One-way delay metric [Almes1999];
- One-way packet loss metric [Almes1999A];
- Round-trip delay [Almes1999B];
- One-way loss pattern [Koodli2002];
- Packet delay variation [Demichelis2002].

Each of these metrics is normally defined with three sections including metric name, metric parameters and metric units:

- The metric name contains basic information of the measurement such as packet type, unidirectional or bi-directional, and parameter name.
- The metric parameter section defines what traffic parameters should be recorded in the metric that can be used for further analysis.
- The metric unit part describes the unit type of the metric.

For instance, the one-way delay metric is named “Type-P-One-way-Delay” that means packets measured in this metric are all type P packet where P could be protocols such as TCP, UDP and ICMP. Its metric parameters are *Src*, the IP address of the packet source, *Dst*, the IP address of the packet destination, and *T*, the time the source sent out the first bit of the type P packet.

Corresponding to each metric, at least one measurement methodology is defined to acquire data from the network. These methodologies should have the property that it is repeatable: if the methodology is used multiple times under identical conditions, it should result in consistent measurements or continuity results with small variations.

These traffic parameters and their measurement methodologies were defined by IETF for the purpose of network performance and reliability analysis. They are vital for the network evaluation, especially QoS evaluation. Some of these metrics that are relevant to MONET are presented below.

2.2.2.1 Latency

Latency includes both one-way and round-trip delay. The definition of one-way delay of a packet is the difference between the time when the source sends out the first bit of the

packet and the time when the destination receives the last bit of the packet (whenever a time, i.e., a moment in history, is mentioned in this document, it is understood to be measured in seconds (and fractions)) [Almes1999].

In the case of round-trip latency, the round-trip delay is defined as the sum of the times needed for a test packet travel from the source to the destination and from the destination back to the source [Almes1999B]. Note that round-trip latency does not take the packet processing time by the nodes into account.

Latency is an important evaluation parameter because it mostly affects the performance of video and voice calls since these services require low latency. In satellite communications, latency is a common problem caused by the distance.

2.2.2.2 Bit rate

The definition of bit rate is the number of bits that are transmitted in one channel per unit of time. So, the bit rate is the capacity that a link has to transmit data. Links between nodes that have higher bit rate than others are more efficient in terms of capacity to transmit data. For example, a connection with low bit rate can not be able to perform a video call or transmit a high data rate.

In summary, this metric is essential to evaluate the capacity of a link to transmit data between two nodes and can be a parameter used to choose the best path to do that.

2.2.2.3 Packet delay variation (Jitter)

The one-way delay variation of a pair of packets within a stream of packets is defined as the difference of the one-way delays of a selected pair of packets in the stream going from measurement point MP1 to measurement point MP2 [Demichelis2002].

Jitter is used as a variability of the packet latency across a network, i.e., an average of the deviation from the network mean latency. The common effect of the jitter is the delay experienced by the packets which varies very often from the mean latency.

Jitter affects the network performance in the same way that latency affects which is mostly in video and voice calls.

2.2.2.4 Loss rate

If a test packet does not arrive at its destination in a time threshold, it is defined lost [Almes1999A]. In communication protocols that features transmission acknowledgement, when a packet is not received, the source must retransmit that packet. This event means that a packet drop has occurred. The loss rate is a measurement of the number of dropped packets in function of time.

The network reliability depends on loss rate because when a communication has a high loss rate, the message content is affected. The impact of the losses changes along the type of traffic the losses occur on: a video call is not much affected by the loss of some frames, but when some credentials are transmitted, one single packet is important.

In summary, a low loss rate means a reliable connection whereas a high rate will require several mechanisms such as redundancy, packet protection and retransmission options to improve the network reliability.

2.3 MONET specific metrics

This section presents metrics that are specific to the scope of MONET. The peculiarity of the MONET architecture is the coexistence of a Satellite and a Mobile Ad-Hoc Networks segment, se the key performance indicators must be tailored first of all on these two technologies, and secondly on the scenarios features (in terms of traffic profiles and requirements). Since the scenarios will be lately defined, in this section the network peculiar metrics will be examined deep in detail.

First of all, it is useful to sum up the peculiarities of the MONET environment.

- MANET segment - key issues:
  - The mobile devices usually have low power supply, so the energy consumption becomes critical;
  - The mobile devices, if not equipped with Satellite antenna, can transmit traffic with not extremely high bandwidth, thus producing sometimes bottlenecks;
  - The mobile devices changes their position, meaning that the topology dynamically change;
  - The routing information must be updated often to guarantee the correct delivery of traffic from source to destination: this can introduced overhead;
  - QoS cannot be guaranteed a-priori in a MANET because of possible faults (e.g. the path from source to destination may be cut off).

Given these obstacles, the MANET segment is considered to work properly if:

- It is possible to establish a path from source to destination;
- It is possible to re-route traffic in case of faults in some links;
- The traffic is balanced among all the terminals to avoid excessive power consumption in some node or possible bottlenecks;
- Packets are correctly delivered (no losses).

2.3.1 Advanced Network metrics

All metrics described below are important to the mobile ad-hoc network segment. As the nodes are mobile, there is an extreme necessity to perform some techniques in order to make the network more efficient and provide a good quality of service on a MANET system. Metrics described below are used to define some network or device characteristics to achieve high efficiency levels. These metrics can have a different weight values in the network management depending on the operation scenarios.

2.3.1.1 Network capacity

The network capacity is the quantity of traffic the network is able to support, i.e. the maximum quantity of information it can transmit at a given instant without failing. If the network load is below this value, it means that the network is not used to its full extent and that some capacity is wasted. If it's above, it means the network is running close to or at maximum capacity and the network is likely to crash.

This metric is important as it gives information on the ability of the network to support maximum loads of traffic. It is also relevant toward the network load as it will help configure the services so that the generated traffic doesn't exceed this capacity.

2.3.1.2 Link utilization/network load

This metric is about the quantity of traffic on the network at a specific moment compared to the total capacity of the network. Considering the network as a pool of bandwidth, the network load is the share of this pool that is currently used. Thus this value is given as a percentage.

This metric is important as it provides good information on how the bandwidth is used. The Satellite resource is expensive, so it must be used adequately. By knowing the network load, it is possible to know if there is some resource left free and reallocate it for other services. In the case in which each service has a dedicated amount of bandwidth, this dynamic sharing can improve the efficient use of the bandwidth, which is given by the difference between the network capacity and the network load.

2.3.1.3 Bandwidth per user

The available bandwidth per user depends on various aspects so its distribution must be done carefully [Prasad2003]. One important aspect has to do with the number of users on the MANET which can lead to a different number of connections in each node and therefore some of them being subjected to more traffic. In these cases, path for destination should avoid these nodes to increase the system performance. If the network detects that one node usually has a lot of traffic (e.g. video and voice applications), MANET tries to allocate more bandwidth for that node while reducing it for other nodes that have less traffic [Brahim2006].

The equipments in each node may have different specifications leading to a different transmission capacity/throughput. Another very important aspect is the wireless connection used for data transmission, ex., on a UMTS/BGAN satellite system, the bandwidth allowed will be greater than a GSM connection but smaller than a Wi-Fi or WiMAX connection.

Application scenarios also have a great impact on the system performance. In a rural scenario without GSM/UMTS connection, satellite connection will be used leading to less transmission capacity and high latency. In urban scenarios a lot of choices will be available but we have to assess other parameters such as limited bandwidth of GSM connections, power consumption, costs of satellite communications and multipath propagation of Wi-Fi and WiMAX connections that causes deep fades in this kind of scenarios.

From an operational point of view, MONET supports multiple services including voice, video and data. Each transmission type requires different throughputs and latency to provide an acceptable quality of service. Metrics should be taken into account so that the allocated bandwidth for each user meets their needs. This allocation should conform to the QoS policy that defines the priorities and needs (in terms of bandwidth, latency and jitter) of each service supported by MONET. It is evident that the most critical services must receive more bandwidth (i.e. the first responders needs to coordinate their effort , so they deserve high priority and guaranteed bandwidth, while best service traffic generate by citizen can wait before being served).

From an economic point of view, the MONET resource management mechanism must be able to distribute the bandwidth with respect to the contract paid by the end-user. Apart from that presented above, there is still another point that should be taken into account which is the transmission emergency level which implies that we must set a percentage of bandwidth for emergency situations. This can be achieved through setting classes of service with different levels of priority.

Bandwidth per user thus plays an important role on the MONET system so it must be measured to guarantee the correct distribution among all users based on their needs.

2.3.2 Routing metrics

2.3.2.1 Convergence time for routing protocols

The convergence time of a routing protocol is the time a network using a given routing protocol needs to reach a convergence state. In this state, the routing is operational and all the routers possess the information to direct the packets through the network. To reach it, the routers have to exchange information about the topology until they all possess the same information, which has to be correct. Thus, in the convergence state, all the routers have a uniform and exact picture of the network topology.

Any change in this topology knocks it out of the state of convergence and the same process of information exchange has to be repeated again to update the routing tables. This value is very important, as it defines the delay needed for the routing protocol before it is operational. A long convergence time means a long delay before the nodes are able to communicate with each other. Of course it is better to have the smallest convergence time possible.

Several factors can affect this duration. The type of protocol directly defines what happens during the convergence phase (ie what information needs to be exchanged, between who…) so it has an impact on the convergence time. It is admitted that link state protocols have lower convergence time than classical distant vector protocols. Indeed, these protocols propose to spread a change happening in topology to all routers instead of updating periodically all the routing tables. By reducing the amount of information to spread and potentially the number of updates occurring, the convergence time can be reduced. For instance, OSPF is a link state protocol and has a very quick convergence compared to RIP.

Convergence time is also highly impacted by the size of the network, since more complex topology means more information to spread and more time to agree between the routers. The network design and configuration also plays an important role into the speed of convergence.

This metric is important to know for MONET as ensuring a fast convergence is the first to a quick setup and helps making MONET viable for emergency scenarios.

2.3.2.2 Routing overhead

Transferring information from source to a destination node in a computer network is achieved by routing, i.e., selecting paths along which to send the data. The eternal goal and the most fundamental problem for any kind of network, is to efficiently transmit the data between the endpoints [Zhou2009, Viennot2004].

One of the considerations that we must have is the influence of the routing protocol in the network and devices. The way to evaluate that called routing overhead and is based on the number (or the total size) of the sent and received packets in the transmission dedicated to the routing process. These packets can be the Topology Control messages, Hello messages, etc, sent or forward with the goal of performing the routing protocol. To implement a robust ad-hoc network, an efficient routing protocol is desired. However, a good relation between efficiency of routing protocol and routing protocol computation effort is necessary. It is not recommended to implement a good routing protocol if the computation effort to implement that uses all the computation resources. The size of each routing packet must be taken into

consideration due to the different type of routing packets necessary to perform the routing protocol. So, the routing overhead must be obtained in function of the total size of the sent routing packets and the total size of the data packets used to transmit data.

On the other side, the routing protocol cannot compromise the available bandwidth in the network system. For example, a routing protocol can have low computation effort but turns impractical for some communications if a high bandwidth is necessary to perform that. Using a high bandwidth with routing packets limits obviously the remainder available bandwidth to make the other communications. This subject is crucial, for example, in a situation that has systems with low bandwidth and has necessity to transmit HD video.

Summarizing, a routing protocol that uses a low computation resources and low bandwidth to transmit and receive routing information is needed. The relation between these two parameters can be different for several cases, giving weight to one parameter in detriment of the other. Everything will depend on the desired network performance.

For instance, OLSR is a proactive routing protocol that controls the traffic by using only selected nodes, called multipoint relays (MPRs), to retransmit control messages. This technique significantly reduces the number of retransmissions required to flood a message to all nodes in network. This protocol allows reducing the necessary time to initiate the transmission. It is achieved through the proactive method that builds a table with the nodes information thus allows having the paths to all nodes before receive a transmission request. When there is a request to give path to some node, it is already made and it is immediately available. OLSR use Hello and Topology Control messages to discover and disseminate link state information throughout the ad-hoc nodes.

2.3.2.3 General routing metrics

IETF draft [KVP2009] gave a nice category on routing metrics for MANET environment. And RFC 2501 [SM1999] also addresses the performance issues on MANET routing protocols, both in quantitative metrics and qualitative properties. Some qualitative properties can be converted into quantitative metrics. In this section, we will list most common metrics for MANET routing measurement.

MANET routing qualitative properties have the following considerations:

- Distributed operation is essential;
- Loop-freedom is required in worst-case scenarios to avoid overall performance downgrade;
- Demand-based operation is required at the different traffic pattern in order to utilize network energy and bandwidth more efficiently;
- Proactive operations is required in the context of demand-based operation incurs unacceptable delay;
- Security and unidirectional link support.

MANET routing quantitative metrics can be assess the performance of any routing protocol:

- End-to-end data throughput and delay. These statistical measures of routing performance are important;
- Routing setup time. It is the time required to establish routes delivery;
- Packet delivery ratio, PDR, is defined as the ratio between the number of successfully received packets and the number of packets a node is participated in averaged over all nodes;
- Packet delivery delay is the average time between the first transmissions of a packet and its reception and successful decoding at the destination nodes;

- Packet overhead is the ratio between the number of transmitted packets at the MAC layer and the number of successfully decoded packets. Also we can have other internal routing efficiency measure;
- Average number of data bits transmitted/data bit delivered. This can be viewed as the bit efficiency of delivering data within a network;
- Average number of control bits transmitted/data delivered. This measure stands for control overhead to delivery data. This metrics also can be normalized control overhead.

On the other hand, MANET routing metrics can be specific to particular mechanisms. Such as single-path routing and multipath-routing, they can be different metrics. Single-path routing metrics:

- The ETX of a link is the expected number of data transmissions needed to deliver a unicast packet over a link, including retransmissions. For example, the ETX of a three-hop route with perfect links is three; the ETX of a one-hop route with a 50% delivery ratio is two;
- Hop count stands for the number of hops. It implies the length of a routing path.

Multipath routing metrics:

- Expected Any-path Transmissions (EAX) stands for a pair of nodes with a given set of candidates that captures the expected number of transmissions between them under opportunistic forwarding. EAX uses priorities to the candidates to be selected for forwarding packets;
- Expected Any-path Communication Time (ExACT) stands for the total transmission time needed to deliver a packet from a given node to its destination sending at the specified rate at each hop under opportunistic routing.

2.3.3 Service related metrics

2.3.3.1 Session setup time

A subset of the services supported by MONET requires establishing a session between 2 or more users before the service can function. This is the case of phone calls, where the caller has to retrieve the address of the called user before establishing a phone conversation with him. It is very important that this value is as low as possible, since critical applications such as these phone calls rely on them. In an emergency situation, phone calls are short so it is unreasonable to think than a call could be shorter than its setup time.

2.3.3.2 Quality of experience

The traffic served by the network can be split in different classes of services, each one characterized by specific requirements. The requirements are expressed in term of priority of a class toward another, a bandwidth guaranteed to the traffic belonging to this class, or a maximum delay before this traffic is delivered to its destination.

Therefore it is important to know for each class of traffic if the requirements are met. For bandwidth and delay, these metrics have already been defined as network performance metrics that only have to be applied to a specific class of traffic. So instead of measuring this data for the whole traffic going through a node, it is necessary to measure for a fraction of this traffic that corresponds to a specific class of service.

As for the priority of a service toward another, this can only be witnessed in case of congestion, when the overall bandwidth of a node is not sufficient to sustain 2 services. In this case, if priorities are correctly applied, one service should be function correctly while the second one is starved and is unable to transmit all of its packets. This can be done also by measuring the bandwidth for each class of service and witnessing the starvation of one of the 2.

2.3.4 Other functional metrics

2.3.4.1 Energy consumption

Currently, one of the principal constraints in radio systems is the energy consumption by the electrical devices. This parameter directly influences the battery life of the mobile nodes. The weight that the mobile radio must obey, limits the components weight and therefore, the power that batteries can deliver is affected too. Without power, the radio cannot work, so it is useless to the network. Due to the importance of this parameter, it must be made an effort to reduce the power consumption. The inclusion of the battery level of the radio in the routing protocol can help to preserve the node power.

With that information, one node with low battery cannot be used for some transmissions if there are alternative nodes available to make them, increasing this way, the battery life.

The energy consumption can be even more important in some operating scenarios than others. For example, in a rescue operation on mountains away from civilization, where the accessibility is null and the transport of material require a huge effort, the importance of battery life of the nodes can be superior, for example, that the necessity of bandwidth. In the extreme case of low battery it is better to have a few communications with the other nodes, than have no communications at all.

Some theoretical studies of the energy consumption in a mobile ad hoc network have been made, like [Gao2002] and [Moustafa]. In practice, the maximum value of the energy consumption depends on the power of the radio present in the node. Using the characteristics of one radio of wireless ad-hoc networks, the maximum power consumption is around 10 watt. That quantity seems low but the node must be functional by some hours. Knowing power consumption and taking into account the maximum weight of the node, it has to be guaranteed energy during the stipulated functional time for the node.

Other requirement is the node ability to turn off the system to avoid the battery damage. In some batteries, like LiPo technology, the voltage level cannot fall below some percentage values. This protection avoids damages on the cells that constitute the batteries. This battery protection permits in life or death situations use the rest of battery energy to make, for example, one last communication with the last knowing GPS position, send the health state of the operator or even send a periodic signal to facilitate the localization by the rescuers. This extreme scenario can damage the batteries, but is possible to save lives.

In this metric can be evaluate two different measurements, the battery charge level and the energy consumption rate. With this information it can be obtained the power consumption. However, if there is a frequently battery charger level analysis, the charger level values provide a good metric. Even the node has a high energy consumption rate, that consumption is reflected in the battery charge level and that information used to perform the routing.

Other information that must be obtained is the battery lifetime on the different types of utilization. The tests must be performed using the nodes with the follow 4 different types of utilization: intensive, nominal, low and connected with a satellite terminal.

2.3.4.2 System setup time

An important metric of every communication system is the time that the system needs to initiate until be operational. That time is called setup time of the system and is obtained by measuring the time between the start of the system (the activation of the nodes) and the moment when the system is able to initiate communications between the nodes.

Setup time is an important parameter to take into consideration because a good system performance is needed when used in emergency scenarios. For example, if the system needs 20 minutes to be operational from its start-up, it becomes less useful for emergency scenarios but can still be used in other scenarios without emergency situations.

2.3.4.3 Connectivity

Connectivity is the ability to communicate between 2 specific nodes. It is a binary metric that states if nodes are able to communicate, whether directly or not. This metric is useful in use cases featuring configuration mechanisms or routing protocols. These mechanisms are supposed to organize the network and make sure every node can communicate taking into account the network topology. Connectivity is way to verify that these mechanisms work adequately.

2.3.4.4 Handover duration

Handover is a process of changing from/to something else. For example, in cellular networks, handover is a process of transferring an ongoing call or data session from one cell to another cell that provides more power or availability. In MONET system, the handover process can take several forms.

The first case is about handling the movements of a node whenever it leaves a MANET for another. The goal of the handover process is then to manage this change, by registering the node in his new MANET and deleting it from the tables of the old one.

Another handover process occurs when switching communication from a terrestrial wireless technology to a satellite link. In this case, the change happens between 2 communication technologies and the goal is to ensure a seamless switch between the 2.

Finally, handover can be about changing the Gateway node. This node is a gateway to the satellite link for an entire MANET, but this role can be transferred to another node should the first fail. In this case, handover is about transferring the responsibilities to the new node and ensure that all the MANET is aware of this change.

The problem of handover is the duration that it takes to process the transfer. As the handover always affect the communication capabilities of one or several nodes, it is important to keep it as short as possible so the communications are not too much disturbed. So, if the duration is high, it will affect the performance of the network because it can stop a communication between two nodes.

2.3.4.5 Metrics for Download and Upload time duration

Several metrics will be used in the final test to evaluate the MONET network performance in terms of data downloading and uploading applications, including measurement at both packet level and file level.

At packet level, the following metrics will be used:

- One-way delay: the time needed for packets travelling from a source host to a destination host;
- End-to-end delay: the mean of one-way delay;
- Round-trip delay: the time needed for packets travelling from a source host to a destination host and then immediately being sent back to the source host;
- One-way packet loss: the number of packets lost from a source host to a destination host during a measurement interval time;
- End-to-end packet loss rate: the ratio of one-way lost packets to the totally transmitted packets.

These metrics are applicable to both file download and upload. The measurement is disaggregated in to sub-measurement in terms of different network segments. These segments are:

- From end users to their local satellite access points;
- Among satellite access points;
- From satellite access points to their end users;
- From end users to end users.

This disaggregating measurement is helpful to understand the performance of different networks segment involved in the whole MONET service system over satellites. It can provide sufficient information to locate potential network problems if any happened during the evaluation. For instance, one-way parameters measured from an end user to its local satellite access point can reflect the performance of the local ad-hoc network and how it impacts on the end user to end user performance.

One-way Delay

The definition of one-way delay of a packet is the difference between the time when the source sends out the first bit of the packet and the time when the destination receives the last bit of the packet (whenever a time, i.e., a moment in history, is mentioned in this document, it is understood to be measured in seconds and fractions).

The format of the one-way delay metric of a sampled packet stream is:
Metric name: <MONET one-way delay metric – type – beginning time/date/duration>
Metric parameters are:

- The source IP address;
- Destination IP address;
- Delay time;
- Packet length;
- Packet type (data);
- File size.

The motivations to measure one-way delay are:

- It is needed to rate a network system that supporting file download and upload. It's potentially useful to evaluate any proposed optimization algorithm in MONET;
- It has to be used to calculate the end-to-end delay;
- The minimum value of this metric provides an indication of the delay due to only propagation and transmission delay;
- Values of this metric above the minimum provide an indication of the congestion present in the path.

For MONET trial, the one-way delay will be measured in segmented networks as presented above. Different one-way delays are needed to be studied to clarify the effect of each of the segments of the network on the performance of the MONET system over satellite networks. For instance, if all of the four delays are known, the delay effects caused by processing packets on the two access points in the end-to-end path can be calculated.

Here, the time required for a packet to travel through the network is measured by comparing the time reported by a clock at one end of the packet's path, corresponding to when the packet first entered the network, with the time reported by a clock at the other end of the path, corresponding to when the packet finished traversing the network [Paxson1998]. Synchronization of the source and the destination are needed.

Network measurement tools, such as Wireshark, run on selected hosts and satellite access points to monitor packets. All of these nodes should be synchronized, which means the offset of the clocks of one measured host pair should be zero or very close to zero. The relative skews and drifts [Paxson1998] of the two host clocks should be minimal. The output clocks can get their time notion from an external source, e.g. a GPS device.

An alternative can be achieved based on the round-trip delay measurements. The idea is to divide the round-trip delay by 2 to approximate the one-way delay. The advantage is that this method does not need two hosts have accurately the same time. However, effects of the skew and drift of the two clocks cannot be avoided. The disadvantage is that the links of the round trip may be asymmetrical, i.e. the link from host 1 to host 2 may not be the same as the link from host 2 back to host 1. Thus, simply using half of the round-trip delay as one-way delay will introduce inaccuracy.

In the measurement, a host should keep on sending fixed length data packets to another host in a sampling period. To have an accurate metric of the one-way delay, some issues have to be noted:

1. To collect samples, periodic sampling [Paxson1998] method can be implemented considering its simplification. However, to minimize the effects of the network periodic behaviour, the sampling should be made separately at different intervals of time;
2. The packets transmitted during measurement should be the same type. This means all of the packets must have the same source and destination, the same UDP/TCP port number and the same length. To minimize the effect of packet fragmentation [Paxson1998], the packet lengths in the measurement should all be the maximum.

If the packet does not arrive at the destination before the sampling period and a threshold time is finished, it will be treated as a lost packet. The destination needs to keep monitoring the network until the threshold time after the measurement to ensure the last packet can be measured if it arrives before the threshold time. In the threshold time after the measurement, only packets with source timestamps falling into the measurement period can be recorded and assigned destination timestamps.

The detailed measurement procedure and algorithm will be described within the relevant test scenario based on [Shalunov2006].

End-to-end Delay

The mean one-way delay was chosen to be end-to-end delay. The types of end-to-end delay correspond to the types of the one-way delay.

Round-trip Delay

The round-trip delay is defined as the sum of the times needed for a test packet travel from the source to the destination and from the destination back to the source.

The format of the round-trip delay metric of a sampled packet stream is:
Metric name <MONET round-trip delay metric – type – beginning time/date/duration>
Measurement parameters:

- The source IP address;
- Destination IP address;
- Delay time;
- Packet length;
- Packet type (data);
- File size.

Round-trip delay provides an alternative to measure one-way delay because it is easy to implement. Unlike the one-way delay measurement, it often does not need install any measurement software at the destination. Moreover, the high requirement of the synchronization of the two clocks at the source and destination are not necessary. The round-trip delay can be measured using algorithm introduced in [Hedayat2008].

One-way packet loss

If a test packet does not arrive at its destination in a threshold, it is defined lost. The format of the one-way packet loss metric of a sampled packet stream is:
Metric name: <MONET one-way packet loss metric – type – beginning time/date/duration >
Measurement parameters:

- The source IP address;
- Destination IP address;
- Lost or not (Boolean). “0” means packet is transmitted successfully. “1” means packet lost;
- Packet length;
- Packet type (data);
- File size.

The motivations to measure one-way loss are:

1. Excessive packet loss may make it difficult to support file download and upload applications;
2. The larger the value of packet loss, the more difficult it is for transport-layer protocols to sustain high bandwidths.

For MONET, the one-way loss is measured on the same kind of link for the one-way delay measurement. One-way packet loss conditions on different links are needed to study the effect of different parts in the MONET system over satellite networks on the network performance. They provide more information to improve the system.

The procedures to measure the one-way packet loss will be described in the relevant test scenarios later.

End-to-end packet loss rate

The ratio of the lost one-way packet to the very transmitted packet is a very important statistical parameter to judge the performance of a hybrid network as MONET. Both the lost packet number and the very transmitted packet number can be found from the one-way packet loss metrics. At file level, the metrics are:

- File upload delay: the time needed for upload a complete file from an ad-hoc end user to a server located in the internet.

    - Metric name: <MONET file upload delay metric – file size – beginning time/date/duration>
    - Metric parameters are:
    - The source IP address;
    - Destination IP address;
    - Delay time;
    - File size.
- File download delay: the time needed for download a complete file from a server located in the internet to an ad-hoc end user.

Metric name: <MONET file download delay metric – file size – beginning time/date/duration>
Metric parameters are:

- The source IP address;
- Destination IP address;
- Delay time;
- File size.

2.3.4.6 Reliability

Network reliability [Cook2008, Kharbash2007] is critical in disaster and rescue scenarios because a network failure could bring negative results on the mission effectiveness. In this kind of scenarios, reliability plays an important role so it must be assigned with a higher metric. In other scenarios, reliability could be assigned with a lower metric since bandwidth or energy consumption takes more important roles.

Reliability is one of the most problematic parameter for classification in terms of metrics because a network failure can occur with a simple increase in the metric of the mentioned parameters (bandwidth, power consumption, routing overhead …) if a particular node is subjected to a lot of traffic.

The system is reliable if it properly delivers the traffic from the source to the destination. Reliability mechanisms operate before a packet loss, by trying to prevent this loss (coding, congestion control mechanism …) or after the loss, by providing means to retrieve that loss (retransmission…).

Network reliability can be assessed based on the number of retransmissions, number of transmission errors and number of acknowledges received. These three points are related since a retransmission only happens when a packet acknowledgement is not received. Measuring only the number of retransmissions is not sufficient to assess the reliability because a transmission can be successfully done but the acknowledgement may fail.

The procedure to evaluate network reliability consists in measuring loss rate and jitter using Rio software. The loss rate is the percentage of lost packets and it is a measuring parameter which covers the three points mentioned above. Apart from loss rate, jitter can also be measured to find out if packets are arriving delayed from each others because jitter is a measure of variability over time of the packet latency across a network.

3 Test Plan

The objective of this section is to define a test plan which can be followed in WP6 for final system test and measurement on the test-bed. There are presented some tests that can be done to check the metrics. It explained the objectives of the test, the inputs and outputs, the test duration, the test steps and the number of tests.

3.1 Testbed description

The tests will be performing in the BLUE Lab (Broadband Links Under Experiment LABoratory). It is the ASTRIUM laboratory located in Toulouse, France, where the telecom system related validation and testing activities are performed. The facilities include satellite antennas, modems, networks equipment, and several emulation and validation tools for both fixed and mobile systems.

The architecture which will be used to perform the tests in Astrium laboratory is pictured on the figure below. Four or five MONET nodes will be connected to a module that simulates the behavior of the signal in real scenario. This module emulates the propagation characteristics, the mobility of the nodes, variable attenuators and introduces noise in the communications. The satellite connections are emulated too, allowing this way to test the inclusion of the satellite links on the MANET. With this equipment, the MONET system can be simulated and the system functionality validated.

The figure below depicts a diagram describing the MONET system that will be simulated.

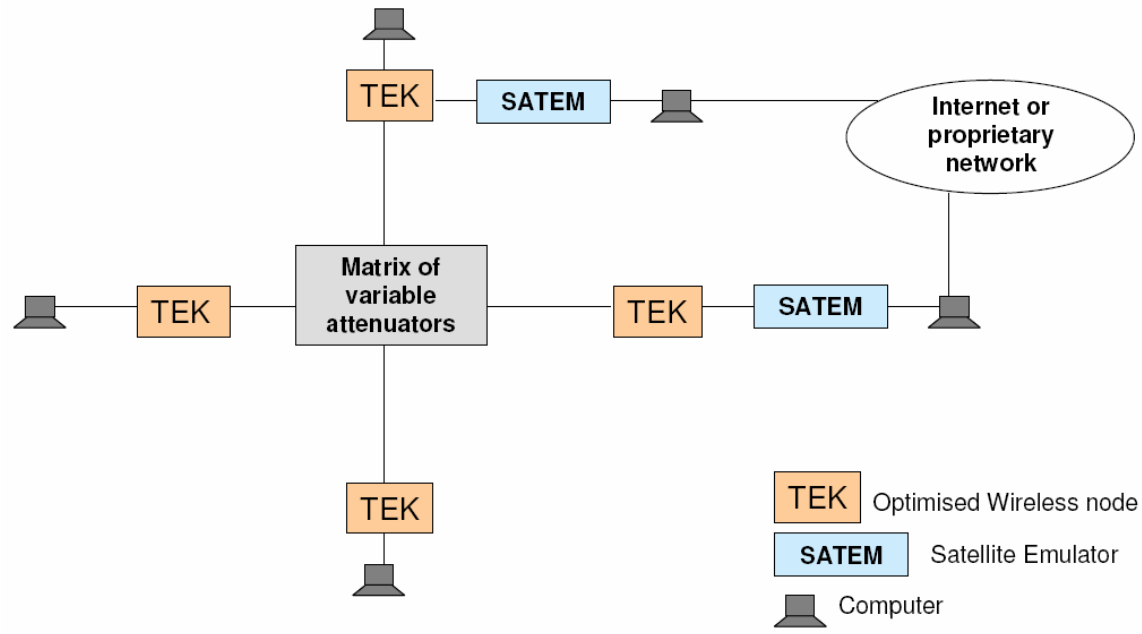

Figure 2 - Test Architecture to be performed on ASTRIUM laboratory

The computers represent users that will carry a MONET node. These computers will generate the traffic within the network by running softwares providing the services considered in MONET.

The ad-hoc nodes can communicate through RF communications or through a satellite links. RF communications are simulated with the matrix of attenuators that reproduces wireless between the nodes. Communication through satellite is reproduced with the SATEM tool that

emulates satellite link and space transmission attenuations. Only selected nodes can communicate through the satellite link, which means that these nodes are responsible to forward all traffic relative to satellite and cell based systems.

In the test-bed, there are 4 or 5 nodes according to the scenario. This number is a compromise between of the requirement of a test-bed being not too big, and the necessity to have a minimum complexity of the network. With this number, it is possible to have 2 MANETs of 2 nodes each and a wandering node, or 2 MANETs with a different number of nodes, or even a single MANET with all the nodes.

The bandwidth tests must be done by software to measure the transfer time of a file. The latency (ping) must be measure to, due to the interferences caused in the performance of videoconferences and calls. Based on the results we can assess if metrics are correctly applied.

3.1.1 End Equipments

3.1.1.1 Traffic generating PCs

In the test bed, the users will be simulated by PCs that will generate traffics as normal users would do, according to the services defined in the scope of MONET. These PCs will be connected to the MONET network through MONET nodes.

Computer	Dell Precision T5500
CPU	Intel Xeon E5630 @ 2.53Ghz, 4 cores
Video Adapter	Quadro Nvidia FX580
RAM	4 GB
OS	Windows XP professional

Table 2 - User PC specification

3.1.1.2 MONET Nodes

MONET nodes are the core of the MONET network. The actual equipment will be developed by Tekever as a outcome of the WP5. Prototypes will be used in the test bed of the WP6.

Each node is a Radio WAC developed by TEKEVER. This radio presented below, support several services like GPS and also allow several devices to connect to it. It communicates to the other node through WiFi, which is the physical layer that was chosen for implementation tests. In the test bed, those nodes will be connected to PCs serving as users, and will transmit the traffic generated by them to the rest of the network by wireless means.

Figure 3 - MONET node (prototype) by TEKEVER

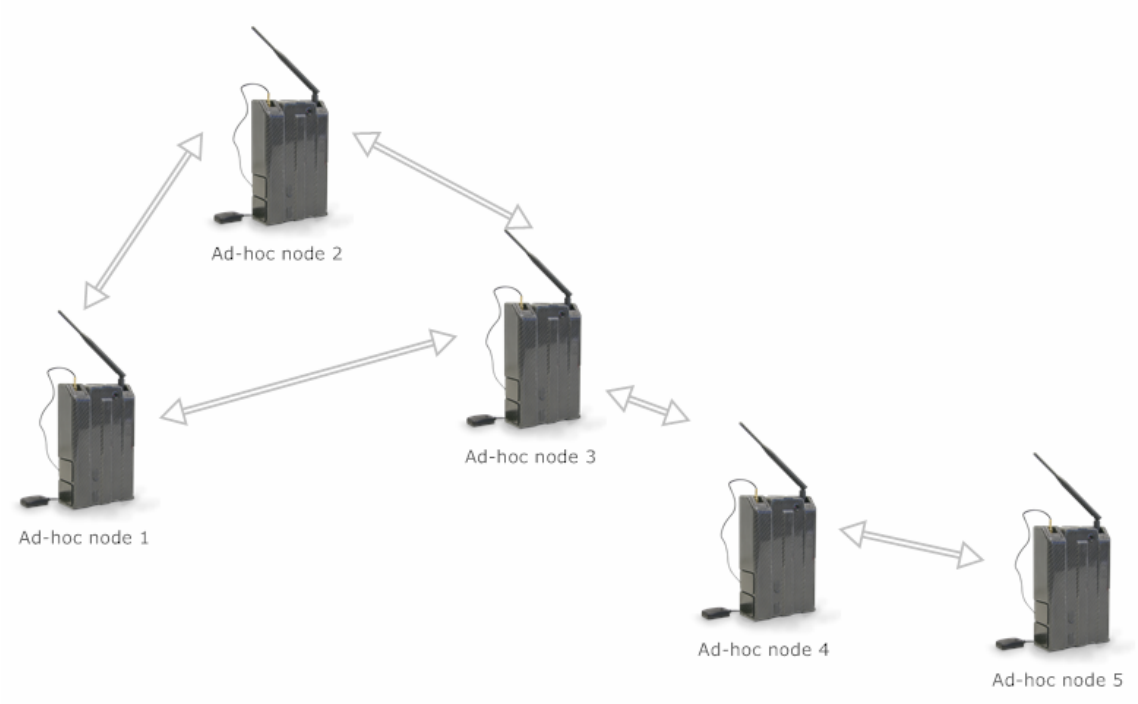

Figure 4 - Mobile ad-hoc Network (MANET)

3.1.2 Transmission Equipment

3.1.2.1 Matrix of variable attenuators (pentatope)

The pentatope is a tool designed to perform the simulation of a MONET network for test purposes. It reproduces wireless communications between the MONET nodes plugged onto it.

The tool contains variable attenuators for each communication channel between the nodes and therefore can reproduce fading events caused by movements or environment conditions (meteo, smoke…).

The tool has been subcontracted to ASSYSTEM which will be in charge of the design, development and integration of the tool according to the following specifications.

The following figure presents the proposed architecture of the attenuators matrix. On this figure, the Wifi routers are the mobile nodes

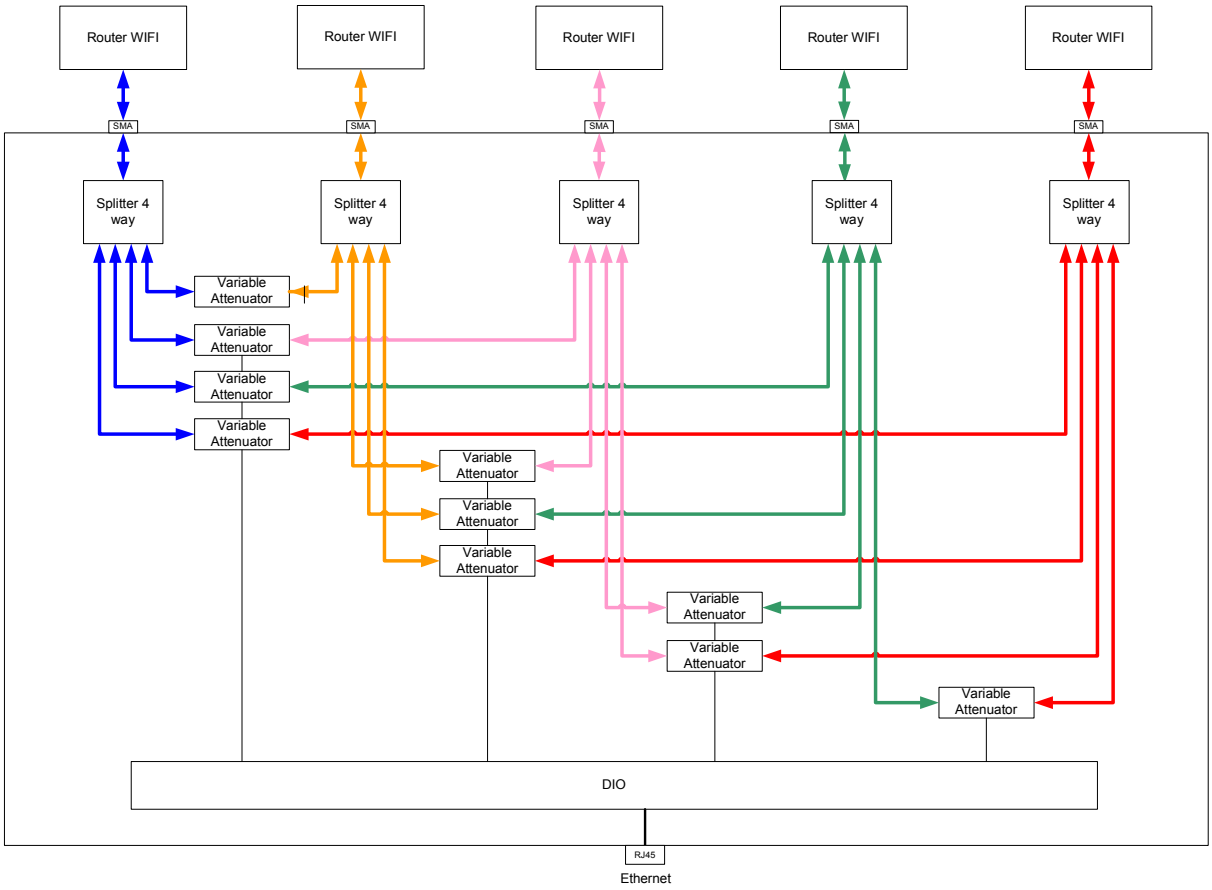

Figure 5 - Matrix of attenuators internal diagram

The present paragraph details the technical specifications of the system. Requirements are classified in three categories: “Mandatory”, “Important” and “Optional”

Functionality

Mandatory Each node can communicate with all the others. Therefore 10 bidirectional links shall be considered.

Mandatory The matrix shall allow to parameter the attenuation on each bidirectional link. The same attenuation value is required on both directions on a given link (send = receive).

Frequency band

Mandatory [2.4 to 2.6 GHz] & [5 to 6 GHz]

Interface

Mandatory 5 SMA female interfaces (to be interconnected to the mobile nodes).

Mandatory 1 RJ45 Ethernet interface for monitoring

Dynamic attenuation

Mandatory	32 dB
Important	60 dB

Attenuation step

Mandatory	0.1 dB

Monitoring & supervision & remote control

Mandatory	The matrix shall be supervised and remotely controlled using LabView.
Mandatory	The monitoring/control interface shall be an RJ45 Ethernet interface.
Mandatory	The monitoring and control function shall allow to modify the attenuation value on each emulated radio communication link.

Alimentation

Mandatory	The matrix shall be compatible with French power supply.
Mandatory	A light shall indicate the status of alimentation, on the front panel of the rack.

As stated in the above specifications, the tool will be monitored by an interface developed with LabView (to be developed). This interface will enable the monitoring of each variable attenuators and the creation of fading patterns that will match the test scenarios.

3.1.2.2 SATEM

For emulating the satellite segment, the SATEM tool from Astrium is selected. SATEM (SATellite Emulator) is a tool that simulates satellite systems at IP level. It simulates the behaviour of a satellite link in terms of performances, such as the link capacity availability, the packet losses, the delay, the jitter and the Quality of Service (QoS) differentiation. The use of a simulator reduces costs related to the achievement of real tests while providing enough accuracy and realism.

The SATEM tool comes in the form of a hardware device and is designed to be connected to the hosts communicating with each other. SATEM emulates the satellite communication system including a gateway, a geostationary satellite and a terminal earth station as illustrated in the figure below. The emulated scenarios enable both broadcasting and interactive services based on the DVB-S2 and DVB-RCS standards. This tool intercepts IP packets that pass between the hosts and modify the network traffic to simulate the transmission over satellite links.

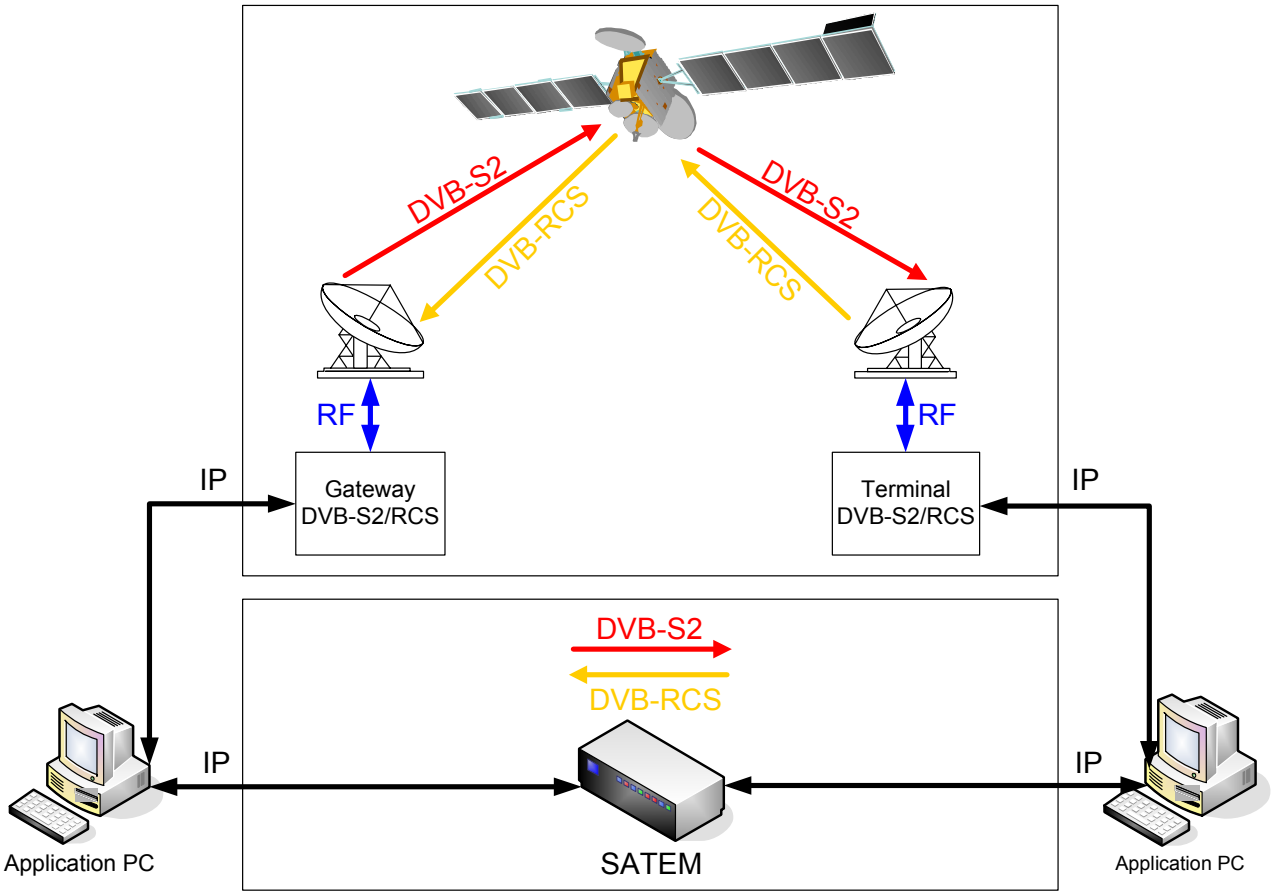

Figure 6 - SATEM satellite system simulation

The SATEM tool offers the following features:

- Ethernet input and output interfaces
- Video Broadcast over Satellite Emulation
- Emulation of delay and jitter through the satellite network, representative of geostationary satellite links
- Emulation of data rate capacity of the link in real time, according to different representative fading time series (eg. clear sky, typical fading, deep fading), as a result of the CCM/VCM/ACM mechanisms, that can be reproduced deterministically for repetitive tests
- Emulation of the modulator transmission buffer, generating packet drop in the case of congestion (data rate demanded larger than the link capacity)
- Emulation of congestion when link C/N+I is close to QEF threshold

The system consists in a small PC offering plug-and-play facility and presented in the figure below.

Figure 7 - SATEM tool

The router is composed of a Monitoring and Control (M&C) interface, and 4 LAN ports meant to connect the simulation end equipments (e.g. Server and Clients).

3.1.2.2.1 SATEM Architecture

SATEM emulates the satellite link traffic condition by operating traffic shaping on the traffic transiting through it.

Linux is chosen as the operating system for the emulator as it offers traffic control tools and advanced customisation capabilities. Traffic control is accurately done by applying queuing disciplines to the outgoing traffic which allows adding variable delay, implementing packet loss algorithms, reordering and duplicating packets.

SATEM thus controlled the four following parameters:

- Bit rate
- Delay
- Jitter
- Packet loss

To perform losses, the buffer is given a percentage and it will randomly drop packets according to it. Delay is achieved by retaining packets for the defined duration while jitter follows a statistical distribution correlated with the delay. Finally sizing the buffer enables bit rate control.

QoS differentiation allows applying a different policy for each of traffic. A policy includes a MODCOD, a priority over the access to the bandwidth and bandwidth limitation. QoS differentiation is performed with a filtering system that is applied to the incoming traffic, separating the IP streams into different queues. This filtering may involve several criteria such as source and destination ports, or used protocols.

The system management is done remotely through an external computer running an executable file that provides a user interface for monitoring and control (M&C) depicted below.

Through the GUI (Graphical User Interface), the user configures the parameters of the satellite network and has the possibility to observe the traffic going through the router ensuring effective control of the system. The M&C system performs real time calculations of the satellite link settings and sends commands at IP level to the router. The traffic statistics are collected every second and displayed as graphs.

The bandwidth is shared between the QoS queues according to quotas set by the user combined with the spectral efficiency of each MODCOD. In case of congestion, when the incoming traffic volume exceeds the allocated capacity, the queues are full, and packets may be lost.

The delay is setup manually, while the jitter follows a statistical distribution correlated with the delay. A delay is applied to each QoS class, corresponding to the propagation time via satellite. Some random variable delay can model the jitter at the IP level. Different statistical distribution of variable delay are implemented: uniform, normal, Pareto, normal Pareto, BOD with high priority, BOD with low priority.

Finally, the loss ratio can be setup manually or is deduced from the C/N. A packet loss at the channel can also be applied randomly, when the link conditions are insufficient for the signal to be properly received by the demodulator and decoder. For the simulation, delay and losses have been configured to be representative a real situation.

The C/N is defined from files representing a fading event such as rain or heavy clouds. The software performs an analysis on the file and emulates the influence of the C/N according to the other satellite settings. For instance, in the case of CCM, if the C/N goes below the QEF threshold, the link is lost; therefore the SATEM won't transmit packets anymore.

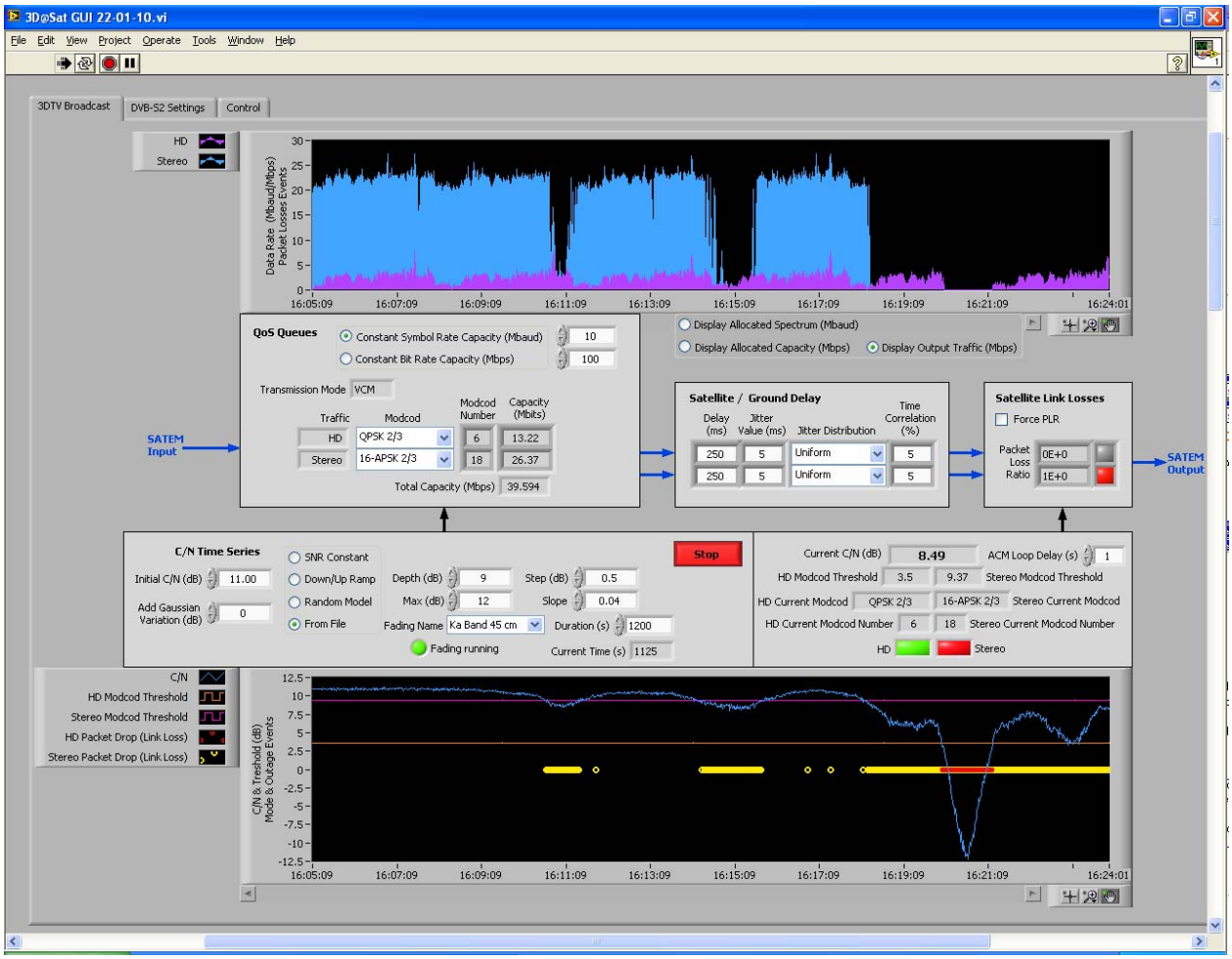

Figure 8 - Sample of SATEM monitoring interface

3.1.3 Monitoring Equipments

3.1.3.1 RIO

The test bed integrates RIO (Real-time IP Observer), which is a software designed by Astrium that analyses the IP traffic and provides statistics.

This tool captures the packets on 2 points: between the server and the modulator, and between the demodulator and the client. The software compares these packets and provides real-time information on the bit rate, losses, the jitter and the delay.

RIO features a functionality which can filter traffic according to the IP address or ports. Thanks to it we can run several instances of RIO, each of them monitoring a specific traffic: between 2 users, belonging to a specific class of traffic, etc.

In order to capture the packets without disturbing the traffic, a TAP is located on every capture point. This device copies and reproduces each packet transmitted, and send the copy to RIO, while the original one continues. RIO can thus analyse the traffic between the streamer and the client without adding any interference to the test.

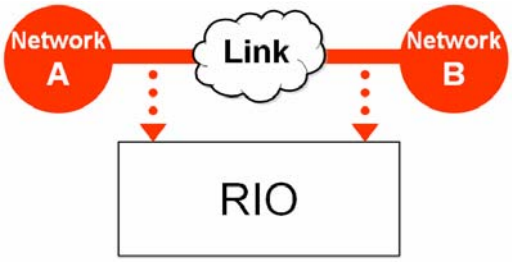

Figure 9 - RIO principle

RIO will run on specific PCs purchased for the project, whose specifications follow.

Computer	Dell Precision T5500
CPU	Intel Xeon E5630 @ 2.53Ghz, 4 cores
Video Adapter	Quadro Nvidia FX580
RAM	4 GB
Network	Intel Gigabit Quad Port PCIe
OS	Windows XP professional

Table 3 - RIO PC specification

3.1.3.2 SATEM IP traffic monitoring

SATEM also provides a function for IP traffic monitoring. It can record and export data of the traffic going through it (ie the traffic that goes through the satellite link), including the bandwidth (used and free, for a particular class of traffic…), satellite latency and jitter, and errors (losses). It also can export the parameters of the satellite links such as the MODCOD, the C/N and the link total capacity in order to correlate the behaviour of the traffic with the link conditions.

The outputs are recorded as numeric values into a CSV file that can be processed afterward.

3.1.4 Services

MONET supports several services like voice (PTT and voice calls), video and data. These services require different link conditions like low latency for video a voice calls or high throughput for data services. The routing algorithm should be able to choose the best path to forward data according to its service. The testing procedure is quite simple; nodes should initiate each service and verify if it works correctly for a defined period of time.

3.1.4.1 Video

Video sessions shall be initiated between several nodes and the impact on traffic load of the network will be analysed. In order to produce this type of traffic, classical streaming software such as VLC can be used. Video content that matches MONET requirements (in term of bit rate and resolution) will be selected and used during the test. The quality of the video in reception should also be assessed if possible, as a QoE validation parameter.

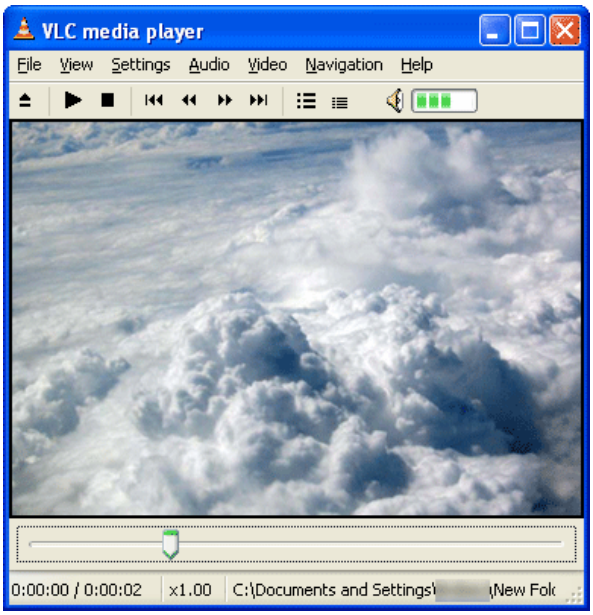

Figure 10 - VLC media player

3.1.4.2 Voice Call

Voice calls are setup using the architecture described in the D3.1 document. A node will be used as a server for the other nodes to establish a voice call.

The server will be established using classical open solutions such as Asterisk servers, and open clients such as Blink will be used as well.

Figure 11 - Asterisk solution.

3.1.4.3 SMS

Short message will be sent from one client to another using SMS APIs such as gsmlib or Open SMPP API.

3.1.4.4 File transfer

File transfer will be reproduced with the FTP protocol, using some open clients such as Filezilla. File of different sizes will be used. Using large files is a way to monitor long time download, which can be a source of useful information for certain metrics such as test duration. It is also a way to load the network in order to observe its ability to large traffic loads.

3.1.5 Testbed monitoring

The test bed will be controlled by a single interface as much as possible. By using LabView, each equipment can be accessed and controlled remotely by an interface which role is to manage the bed and run the tests. Because of the potentially large number of tests to be performed, automation of the test bed is an objective that can be achieved thanks to this centralization.

Depending on the test scenario, the interface will select the appropriate parameters for each equipment (pentatope, SATEM..), and run the test; once it is finished, it will also gather the results from the monitoring equipments (SATEM, RIO…) and store them together, ready for post-processing and analysis.

3.2 Test scenario sample

In this section, we intend to define a typical scenario as they will be defined in WP6. The proposed structure will help narrowing the test objectives to a set of scenarios and preparing the tests campaigns. The topic chosen to illustrate the scenario structure is a handover from terrestrial to satellite communication. In this scenario, a node belonging to a MANET leaves the range of this MANET is not connected to the other nodes anymore. To avoid getting isolated, it activates its satellite interface which connects it again to the MONET network.

3.2.1 Test Objective

The goal of this test is to validate the functionality of MONET which ensures the self configuration of the network. It is supposed to be able to react quickly to any change of topology and maintain communication within the whole network. This use case is also an opportunity to assess the performance of the network in such a situation.

The performance of the self-reconfiguration itself will be assessed. This mechanism should be very fast and leave the network in the same state as it was before, in operational terms (connectivity between the nodes…).

It is also an opportunity to assess the impact of such an event on the network. A change of communication technology will have an influence on the performance of communication (bandwidth and delay), which have to be taken into account depending on the service. For instance, video services require a lot of bandwidth which may not be satisfied anymore if the communication uses the satellite link.

3.2.2 Test Input

The configuration of the test bed will include:

- **Pentatope**: a fading pattern has to be provided to reproduce the movements of a node leaving the MANET. The LabView interface allows to defining attenuation for each path between 2 nodes. It is thus possible to simulate the distance between 2 nodes with it, and, by modifying this attenuation, simulate the motion of a node.
- **SATEM**: a link budget will be used to configure the link used in the MONET network such as the following:

Forward Link	Ku
Aircraft in receive Terminal Downlink Frequency	11,70 GHz
Symbol Rate	28,0 MSymb/s
Satellite Transmit Section	
Satellite EIRP	55,0 dBW
Output Back-off wrt unmodulated carrier	0,5 dBi
Number of Carrier per tube	1
Satellite EIRP per TDM carrier	54,5 dBW
Distance	40000 Km
Free Space Loss	205,8 dB

Atmospheric attenuation (in cruise)	0,5 dB
FAST Aircraft Terminal Reception	
Clear Sky G/T (antenna & radome)	12,0 dB/K
Pointing Loss	0,5 dB
G/T degradation (clear sky)	0,0 dB
Total G/T	11,5 dB/K
Downlink C/No	88,3 dBHz
Downlink Interferences	
ACI (adjacent satellite) degradation	20,0 dB
C/Io due to adjacent satellite systems	94,5 dBHz
NPR C/I	30,0 dB
NPR C/Io	104,5 dBHz
Cross Polar C/I	20,0 dB
Cross Polar C/Io	94,5 dBHz
Downlink C/(No+Io)	86,5 dBHz
Uplink C(No+Io) degradation	1,0 dB
System Margin	1,0 dB
Total C/(No+Io)	84,5 dBHz
Total C/(N+I)	10,02 dB
ModCod	8-PSK 3/4
Data Rate	62,8 Mbps

Table 4 - Example of a satellite link budget

- **Service**: some traffic has to be generated within the network. High bandwidth demanding services such as file transfer or video services, and delay-sensitive services such as voice calls, will be used.

3.2.3 Test output

The expected results include:

- Total handover duration (from the moment the communication with the node is lost to the moment it is retrieved).
- Battery consumption: the change on the node battery lifetime between the 2 modes (wireless and satellite) shall be monitored.
- Bandwidth of the wandering node (potentially for different services)
- Latency on the wandering node (potentially for different services)

3.2.4 Test steps

The test consists in 3 phases:

- In the first phase, the system is in the nominal state. In this state we will measure the defined metrics as reference values.
- In the second step, the scenario begins. In this case, it is the node that begins to move. This phase ends until the system is stabilized again. In this phase we can

measure the time needed for reconfiguration but other network metrics such as bit rate or latency are of lesser use since the network is in an unstable state.

- In the third phase, the system is back in a stable state (the node is connected to the network through its satellite interface). This phase is the opportunity to measure the difference between the metrics in term of network performances (bit rate and delay).

3.2.5 Test duration

The first and the third should last long enough in order to provide meaningful results to compare. They should at least last for 5 minutes.

The second phase's duration is unclear as it mainly depends on the duration of the handover, which is the metric to measure in this test. This phase should thus last longer than the time needed for all the handover steps, including the reconfiguration. It begins when the node starts to move and ends as soon as the systems are stable again.

3.2.6 Number of tests

The test should be repeated several times in order to assess the impact of the handover on several kinds of service. Because testing all the services as the same time makes the results difficult to differentiate, it has to be run for each of the services that have to be tested, such as voice calls or video. This way we can also confirm the handover duration which doesn't change along with the service.

4 Conclusion

In this document we have defined general metrics and specific metrics to measure the network performance aspects of MONET. An overview of the testbed environment that will be used for the technical validation of MONET is also provided. The defined metrics will provide all the requirements to validate the technical components of the system. Those metrics will be measured with the monitoring equipment included in the test bed. The testing procedure will make sure that meaningful results are extracted in order to assess the performance of MONET.

The test-bed architecture has been designed. It accurately reproduces a small MONET network, including real MONET prototype nodes. The use of powerful simulation tool such as the matrix of attenuators and SATEM will help guaranteeing the quality of the results. In this document we also proposed a model for the scenarios that will be defined later in the project. The whole document will help as a framework for the realisation of the test-bed, the definition of the test scenarios and the process of the test campaign.

References

[Awduche2002] - D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, X. Xiao, “Overview and Principles of Internet Traffic Engineering,” IETF RFC 3272, May 2002.

[ITU-T2002] - ITU-T Rec. Y.1540, “Internet Protocol Data Communication Service - IP Packet Transfer and Availability Performance Parameters,” ITU-T Study Group 13, Dec 2002.

[Paxson1998] - V. Paxson, G. Almes, J. Mahdavi, M. Mathis, "Framework for IP Performance Metrics,” IETF RFC 2330, May 1998.

[Mahdavi1999] - J. Mahdavi, V. Paxson, “IPPM Metrics for Measuring Connectivity,” IETF RFC 2678, September 1999.

[Almes1999] - G. Almes, S. Kalidindi, M. Zekauskas, “A One-way Delay Metric for IPPM,” IETF RFC 2679, September 1999.

[Almes1999A] - G. Almes, S. Kalidindi, M. Zekauskas, “A One-way Packet Loss Metric for IPPM,” IETF RFC 2680, September 1999.

[Almes1999B] - G. Almes, S. Kalidindi, M. Zekauskas, “A Round-trip Delay Metric for IPPM,” IETF RFC 2681, September 1999.

[Koodli2002] - [R. Koodli, R. Ravikanth, Axiowave, “One-way Loss Pattern Sample Metrics,” IETF RFC 3357, August 2002.

[Demichelis2002] - C. Demichelis, and P. Chimento, “IP Packet Delay Variation Metric for IP Performance Metrics,” IETF RFC 3393, November 2002.

[Waldbusser2000] - S. Waldbusser, ‘Remote Network Monitoring Management Information Base,’ IETF RFC 2819, May 2000.

[Presuhn2002] - R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, ‘Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)’, IETF RFC 3418, December 2002.

[Presuhn2002A] - R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP),’ IETF RFC 3416, December 2002.

[Shalunov2006] - S. Shalunov, B. Teitelbaum, A. Karp, J. Boote, M. Zekauskas, “A One-way Active Measurement Protocol (OWAMP)”, IETF RFC 4656, September 2006.

[Hedayat2008] - K. Hedayat, R. Krzanowski, A. Morton, K. Yum, J. Babiarz, “A Two-Way Active Measurement Protocol (TWAMP)”,RFC IETF 5357, October 2008.

[SM1999] - S. Corson, J. Macker, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, IETF RFC 2501, January 1999.

[KVP2009] - M. Kim, JP. Vasseur, K. Pister, H. Chong, Routing Metrics used for Path Calculation in Low Power and Lossy Networks, IETF draft-mjkim-roll-routing-metrics-03, 2009

[Prasad2003] – Prasad, R. S.; Dovrolis, C.; Murray, M.; Claffy, K. C.; ”Bandwidth estimation: metrics, techniques, and tools”; IEEE Network, vol. 17, no. 6, pp. 27-35; November-December 2003

[Brahim2006] – Brahim, S.; Farouk, K.; Hajer, T.; “Performance Evaluation Study of an Available Bandwidth Measurement Technique in Multi-Hop Wireless Ad Hoc Networks”, IFIP – International Federation for Information Processing, vol. 197/2006, pp. 99-108; 2006

[Gao2002] – Gao, J. L.; ”Analysis of energy consumption for ad hoc wireless sensor networks using a bit-meter-per-joule metric”; IPN Progress Report 42-150; August 15 – 2002

[Moustafa] – Moustafa, H.; Labiod, H.; “Energy Consumption for Mobile Ad Hoc Networks”; GET/ENST/INFRES Paris, France

[Zhou2009] – Zhou, N.; Abouzeid, A.; “Information Theoretic of Proactive Routing Overhead in Mobile Ad Hoc Networks”, IEEE Transactions on Information Theory, vol. 55, no. 10, pp. 4608-4625; October 2009

[Viennot2004] – Viennot, L.; Jacquet, P.; Clausen, T.; “Analyzing Control Traffic Overhead versus Mobility and Data Traffic Activity in Mobile Ad-hoc Network Protocols”; Wireless Networks, vol. 10, no. 4, pp. 447-455; July 2004

[Clausen2003] – Clausen, T.; Jacquet, P.; “Optimized Link State Routing Protocol”; IETF - RFC3626; October 2003

[Cook2008] – Cook, J.; “Reliability of Mobile Ad-hoc Wireless Networks”; Stevens Institute of Technology, Ph.D. Dissertation; December 2008

[Kharbash2007] – Kharbash, S.; Wang, W.; “Computing Two-Terminal Reliability in Mobile Ad hoc Networks”; IEEE Wireless Communications and Networking Conference, pp. 2831-2836; 11-15 March 2007

[López2004] – López, J.; Barceló, J. M.; García-Vidal, J.; “Analysing the overhead in mobile ad-hoc network with a hierarchical routing structure”, Technical University of Catalonia; 2004

[Sucec2002] – Sucec, J.; Marsic, I.; “Clustering Overhead for Hierarchical Routing in Mobile Ad hoc Networks”, IEEE; 2002

[Li2007] – Li, Y.; Ephremides, A.; “A joint scheduling, power control, and routing algorithm for ad hoc wireless networks”; ScienceDirect - Ad Hoc Networks 5 (2007) 959–973; 2007.