Seventh Framework Programme
Information and Communication
Technologies Theme

MONET REQUIREMENTS

MONET
Grant No. 247176

Deliverable Information
Deliverable Number: D2.3 **Work Package:** WP2
Date of Issue: 13-01-2011
Document Reference: MONET-ICT-247176-D2.3
Version Number: 1.0
Nature of Deliverable[1]: R **Dissemination Level of Deliverable[2]:** PU
Author(s): ASTRIUM, TEKEVER, UNIS, ISDEFE, URSZR
Keywords: End-users assessment, operational requirements, technical requirements

Abstract:
The objective of the present Task 2.2 is to define the requirements of the future integrated MONET system.
Two steps are considered: the first one is based on the results of Task 2.3 and on the outcomes of the end-users assessment realised through out the Workshop, the questionnaires and interviews. The purpose is to define in details the mission and operational requirements. The second one is the technical translation of the operational requirements in terms of general, performances, and functional requirements... The technical requirements are defined at system level from an end-to-end perspective and are derived on both the satellite segment and the ad-hoc network.
This detailed specification will then be used to precisely define and size the integrated satellite-MANET system. The compliance of the proposed solution with the requirements will be verified during in-lab testing. Moreover, this specification will be also a guidance document to check that the end-users needs during real fields conditions are fulfilled.

[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
19/02/2010	0.1	Draft content
09/03/2010	0.2	Comments – URSZR
10/03/2010	0.3	Definition of contributions
09/06/2010	0.4	Contributions based on Madrid Workshop
30/08/2010	0.5	Contributions from ISDEFE and UNIS
20/09/2010	0.6	Contributions from all partners
06/10/2010	0.7	Contributions from all partners
07/10/2010	0.8	Contributions from all partners
30/11/2010	0.9	Revision of document
13/01/2011	1.0	First issue

Document Authors

Entity	Contributors
ASTR	Melanie MONIER Philippe BOUTRY Fabrice PLANCHOU Valentin KRETZSCHMAR Eric ALBERTY
TEKEVER	André Oliveira Pedro Sinogas
ISDEFE	Sergio de la Fuente Álvarez Raquel Lozano Bernal Judith Pertejo López
UNIS	Dan HE Lei Liang Haitham Cruckshank
URSZR	Katja Banovec Juros

Executive Summary

Mobile wireless Ad-hoc Networks (MANET) yield good results in a wide variety of applications which require local connectivity. However, these applications often happen in infrastructure-less or remote regions where remote connectivity to the outside world has to be provided by some other means. MONET solves this issue using satellite links not only as a component of an alternative routing path but also as part of a unique integrated hybrid system.

In order to define the requirements of the MONET system, end-users opinion and feedback are taken into account. These needs not only cover the features provided by communication systems currently used by public safety actors, but also contain several requests that can fulfilled by MONET and that would definitely improve the communication efficiency in the selected scenarios. These requirements are classified according to their importance toward Public Protection and Disaster Relief operations.

The mission requirements are then derived into technical requirements that define the objectives of MONET in term of performances and functionalities. These requirements are to be fulfilled and validated by the end of the project. The derivation is made taking into account both the needs of the end-users and the scope of MONET. Feasibility has also been considered as a decisive parameter in the selection of requirements.

Table of Contents

List of Tables

List of Figures

List of Acronyms

Acronym	Meaning
ATH	At The Halt
BO	Back office
CP	Command Post
DMR	Digital Mobile Radio
DoS	Denial Of Service
FR	First Responder
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
MANET	Mobile Ad-hoc NETwork
MONET	Mechanisms for Optimization of hybrid ad-hoc networks and satellite NETworks
NCC	Network Control Centre
NGO	Non governmental Organization
OTM	On The Move
PPDR	Public Protection and Disaster Relief
P2P	Point-To-Point
PTT	Push-To-Talk
QoS	Quality of Service
RCST	Return Channel Satellite Terminal
RSGW	RCST Satellite Gateway
RTP	Real-time transport Protocol
RTT	Round Trip Time
SMS	Short Message Service
TDM	Time Division multiplexing
TWTA	Travelling Wave Tube Amplifiers
UDP	User datagram Protocol
UHF	Ultra High frequency
URSZR	Uprava RS za zascito in resevanje, Administation of the Republic of Slovenia for Civil protection and Disaster Relief
VHF	Very high frequency
VoIP	Voice on IP

Table 1 – List of acronyms.

1 Introduction

1.1 Objectives

This document aims at providing the technical requirements for the MONET system. Based on the requirements collected from the end-users, it specifies the technical aspects of the system in order to ensure it answers correctly to communication needs on natural disasters/public safety operations. Specific requirements to investigate include sizing of the system in order to provide a scalable solution that can handle small incidents as well as major disasters, compliance with services both currently used and requested by the end-users, and aspects contributing to a highly responsive, reliable and effective communication system.

The first part of the document will summarize the data collected from the end-users, which is afterward derived into general requirements of the public safety field. Functional requirements will describe the services and the functionalities the MONET system shall offer, while performance requirements will present the sizing of the system. Specific requirements linked to the inclusion of a satellite segment into the system is presented at the end of the document, underlining critical points to be taken into account as well as technologies the system would greatly benefit from.

1.2 Background & inputs

This document is based on the outcome of the campaign of data collection from the end-users. This campaign has been organized in order to get the feedback of end-users on current procedures and requirements specific to the public safety operations. These have been collected through a workshop which outcomes are presented in D2.2: Workshop proceedings document. The end-users that contributed to the campaign belong to civil protection services, medical services, fire brigades and airport security services.

Based on this document and on the study scenarios presented in the D2.1 document, user requirements have been compiled in the D2.4 document which also constitutes an input for the present document.

2 Mission requirements

2.1 End-users assessment synthesis

2.1.1 End-user information collection

In order to assure the successful implementation of any system, it is very important to meet, as much as possible, the expectations of the end users about that system. In particular, for first responders, changing an element of the techniques used during their intervention not only means an investment coming from the acquisition of new devices or system but also an investment in changing actuation protocols and users trainings coming from these new protocols.

For this reason, the first step to determine system requirements has been to collect end users needs. To achieve this goal, interaction with users has been considered essential. To formalize such an interaction, questionnaires have been developed to gather requirements from end users (previously identified) and personal interviews have been held to present the objectives of the project and get help the completion of the questionnaires on one hand, and, on the other hand, to get additional information that could be useful for the project. The results were presented in a workshop held in Madrid to open a discussion among the end users and the MONET technical partners. End users requirements have been therefore translated into technical ones (see MONET D2.2 Workshop proceedings). After this workshop, all info collected from questionnaires and during this event was summarized and organized. Personal interviews with the end users were held in order to refine the identified needs. All information collected during this process, as the information extracted from relevant documents (Ref AD1, AD2, RD1, RD2, RD3) is presented in the next chapter.

2.1.2 End-user requirement synthesis

The following table synthesizes the user needs gathered previously in documents D2.4 Study Scenarios Report (Ref RD2) and D2.2 Workshop Proceedings (Ref RD1). It presents the requirements concerning the MONET equipment and is split into seven categories: environmental, mechanic and electric, performance, radio interface, service, security and economical requirements. Moreover, the requirements are split according to the demand level. Each category includes three levels of requirements following their importance according to the end-users. These levels are:

- *Mandatory* refers to a service of information for which failure to deliver, disruption or delay is not tolerate in view of its impact on public safety operations.
- *Required* refers to data that allows some tolerance relating to the specified value.
- *Desirable* refers to future desires that would be an asset for current operational practises.

Types of requirement	Requirement		Requirement level		
			Mandatory	Required	Desirable
Environmental requirements	Shock		No degradation when subjected to a 1metre fall	Fully operational when subjected to a 1metre fall	No degradation when subjected to a 2m fall
	Temperature range		From -30ºC to 60ºC		
	Humidity ratio		Support 100%		
Mechanical and electrical nodes requirements	Portable node	Weight	< 1kg	< 0,8kg	0,5kg
		Dimensions		150 x 60 x 40 mm	
		Autonomy	5h		8h
		Power Supply	Through battery		
	Vehicular node	Weight	< 30kg		
		Power Supply	Through vehicular battery (12V or 24V)		
	Relay node	Weight	< 10kg		
		Dimensions		300 x 300 x 200 mm	
		Autonomy	8h		12h
		Power Supply	Through battery		
	Fixed node	Power Supply	Through power grid		
Performance requirements	MONET network deployment in the scenario		< 5min		
	Interoperability with other technologies used for emergency and mobile communications: TETRA, DMR, etc.				100%
Radio interface requirements	Node coverage		50 meters	100 metres	300 metres
	Interferences with wireless systems		Avoid (especially in case of urban area)		
	Frequency band exclusivity				Regulated

Service requirements	Data	Data refresh rate (e.g. meteorological and biometric sensors information)		Every 5 sec		
		Bit rate		64 kbps		128 kbps
	Positioning	Data positioning refresh rate		Every 5 min stopped, every 1,5 min or 200 metres in movement, and every 10 sec for fire-fighters in hot area. Every 20 sec or 20 metres in an airport		
		Bit rate		9,6 kbps		
	Voice	Voice communication set-up	PTT[3] voice calls	< 1 sec		< 500 milisec
			P2P[4] voice calls	< 3 sec		
		Average call duration	PTT voice calls	10 - 35 sec		
			P2P voice calls	60 sec		
		Number of PTT calls per player	during rush hour	8 PTT/15mins		
			during medium busy period	4 PTT/15mins		
		Number of P2P calls	from CP to BO	12 P2P/h		
			from CP to external users (e.g. hospital) per each injured	2 P2P/h		
		Bit rate		15 kbps		
	Video	Availability		Non-stop for mountain rescuers and police	Non-stop for fire-fighters	
		Bit rate		256 kbps		512 kbps
Security requirements	Access security			Authentication and authorization		
	Channel security			Confidentiality and integrity		
Economical requirements	Cost			< 1000euros		< 800euros

Table 2 - End-user requirement synthesis

[3] Push-to-talk calls are used by talkgroups.
[4] Point-to-point calls are used by emergency managers.

2.2 Mission requirements definition

2.2.1 Actors and entities

The actors involved in the MONET system are organizations dedicated to public safety and disaster relief: NGO, Civil Protection units, Police forces, fire-fighters, medical services…
As presented in the study scenarios (ref AD1), the users can separated in several categories.

- First Responders (FR) are units sent to the field of operation and operating at the very core of the crisis theatre. They can be Fire-fighter preventing a fire to expand, or medical services brining help to casualties.
- Command Posts (CP) corresponds to operation centres. While they are also located close to the theatre, their role is to manage the field operation by assessing the situation thanks to data collected by FRs, dispatching the FRs and eventually ask for backup units.
- The Back Office (BO) is located far from the theatre and corresponds to Control centres such as the SitCen of European Union. Its role is to connect the deployed units with existing infrastructures. It has a overview of the situation and can supply with backup units and critical for the efficient management of on-field situation

Moreover, the system shall account for communication outside the directly involved actors toward external entities. Such entities are not included in the system but communication with them is essential as they can provide services that the specialized units cannot perform or critical data, such as hospitals for remote medical support.

2.2.2 Theatre of Operations Classification

The average size of the area of accident is very difficult to determine. For example: a heavy traffic accident is limited to a relatively small area with existing communication infrastructure. In this case rescuers can even use a public mobile network if needed.

The following table categorises the theatre of operations into a five-level scale classification. Some public safety incident examples are given to yield further clarification of theatre size and dimension of each level.

Theatre of Op. classification	Affected area	Disasters examples	Players involved	Time to solve the crisis (hours)
Level 1	Very frequent and localized incidents.	Minor structure fire, car accident.	1< p < 10	0< h < 8
Level 2	Less frequent incidents with no possibilities of expansion or collateral damage generation. Reduce affection to the population.	Medium structure fire, mountain rescue.	10< p< 100	0< h < 8
Level 3	Adjacent communities/districts affected. Less than hundred victims or injures.	Medium floods or terrorist attacks, medium forest fire, large public event (national or international)	100< p < 1000	8< h < 48
Level 4	Several sectors in a city or extends over a large rural area. Hundreds of victims.	Medium magnitude earthquakes, urban aerial accidents,	1000< p < 2000	48< h < 1 week

		terrorist attacks, uncontrolled wildfires		
Level 5	Great impact on one or several cities or countries affecting drastically their regular functionality and economy. Thousands of victims and seriously injured casualties.	Large natural disasters (earthquake, major tropical storm, a major ice storm, floods), large-scale criminal incidences.	p > 2000	h > 1 week

Table 3 - Theatre of Operations Classification

According to interviews, three Public Safety agencies are on duty on the disaster spot area: Fire Brigade, Medical Services and Police, represented approximately by the 70%, 20% and 10% of global players involved, respectively. End-users report that in the public safety scenario – Forest Fire [1] - fire fighters group into 8 members per vehicle, whereas medical staff and Police group into 3 and 2 members per vehicle, respectively.

2.2.3 MONET Network: Concept of Use

Establishment of the MONET Ad-hoc Network

- Anticipating Actions
  - To guarantee satellite availability depending on the geographical situation in order to deploy MONET network.
  - To book enough satellite capacity (in term of bandwidth).
  - To pre-configure initially MONET network (e.g. configuration of different node profiles or creation of different sub networks for each emergency body).
- Actions during operations
  - To deploy MONET network (including configuration and network monitoring) in a maximum setup time of 5 minutes.
  - To replace nodes if a failure takes place in a node or if batteries capacity is low.

MONET nodes assignment

The following intervention area classification has been defined for security reasons taking into account the public safety operational practises, but it can be extended to the rest of operations theatres.

- Cold area
  - Portable and vehicular nodes shall be assigned to ambulances or additional support vehicles.
  - Fixed nodes shall be assigned to BO.
- Warm area
  - Portable nodes shall be assigned to medical and police units.
  - Vehicular nodes shall be assigned to CPs and emergency bodies vehicles.
- Hot area
  - Portable nodes shall be assigned to fire fighters.
  - Vehicular nodes shall be assigned to fire trucks.
  - Relay nodes shall be used to avoid coverage gaps that may appear in the wireless MANET network. Relay nodes are temporarily carried by pedestrian or vehicular FRs and left at strategic places of hot area.

MONET nodes integration

- MONET nodes shall be integrated with FRs equipment, especially with biometric sensors used by fire fighters to monitor their state of health in hot area.
- MONET nodes should comply with European Open Interoperability Standards to provide interoperability with Private Voice networks (e.g. TETRA, TETRAPOL, DMR, etc.).
- MONET network shall be integrated with UAV and helicopters vehicles.

2.2.4 Coverage area

MONET system should be functional everywhere in the world. Natural disasters can happen in a large variety of locations and in the case of large scale disasters, units from different countries are sent to provide relief. Therefore these units should be able to use the MONET system even if they are not in their own country.

A fortiori, it is mandatory that the MONET system functions everywhere in Europe, especially for cross-border operations involving units of different countries.

2.2.5 Connectivity

A CP will be deployed for each critical location (e.g. fire centre) and will be in charge of its own FRs. It shall form a MANET network with the FRs and shall be mainly responsible for communication with the BO and other CP/MANET.

The FRs that are in the same location shall be able to communicate between themselves and with their CP. Point-to-point and point-to-multipoint (group call) shall allow the FRs to exchange data such as positioning and voice message between themselves and the CP, through point-to-multipoint communication. They also need to establish point-to-point communication with the CP in order to provide him with video or sensor data that the other FRs don't need to know.

Each mobile CP should have the equipment to receive, integrate and display all data coming from FR equipment in order to facilitate FRs risk management. FRs will receive alerts, positioning information, commands to proceed, etc, through voice communication or data displayed in FR equipment.

Communication between all the CPs is important in order to ensure a better coordination of the resources. They can exchange information on the situation such as indicate that a fire is heading toward another CP.

A bidirectional communication between a CP and the Back Office (BO) is needed for exchanging data. The CP may ask the BO for backup or mapping data and communicates the information on the situation it gathered from the FRs. The BO communicates the requested data and can give dispatching instructions.

A CP also needs to be able to contact external entities to request data or backups, and to retrieve information from external database, such as meteorological information.

2.2.6 Capacity requirements in terms of data rate and types of traffic

The system global capacity should be enough to handle all the traffic carried within it. New public safety applications are driven by an increasing demand in term of bitrate. Due to the

criticality of the data, congestion and packet losses must be avoided at any cost. Mechanisms for effective management of the traffic shall be implemented, which must also take into account the hybrid nature of the MONET network (satellite and MANET).

In particular, bottleneck on terminals bridging the satellite link and the MANET must be avoided.

The end-users made it clear that current services used by the intervention units must maintained at all cost, while new services must be set up with the slightest impact on current procedures. Amongst already used services, we can mention:

- **Voice call**: are essential for basic communication between units. Group calls (also called point-to-multipoint) enable a quick propagation of the information amongst the units, whereas point-to-point calls establish a communication between 2 units.
- **Transmission of Short Message (SMS)**
- Transmission of **alarm** signals

New services to be enabled are meant to offer a higher level of understanding of the situation in order to ensure a quick resolution of the crisis and the maximum safety for the FR. They include:

- **Video:** Visual information enables a real-time monitoring of the evolution of the situation. This kind of application especially demanding in term of bitrates
- **Positioning information** keeps the command post informed of the position of every FR, which helps it ensure an effective dispatching of the units
- **Data transfer** can either consist on external data such as medical files or digitals maps that helps the FRs in their operations, or sensor data collected by the FRs and transmitted to the CP which can use it to assess the wellness of the FRs and its environment.

2.2.7 Mobility requirements

MONET nodes shall be carried by pedestrian units or vehicles. While vehicles move at a high speed when they are heading to the crisis theatre, they are more static or move slowly when they are deployed. Pedestrian FR units ate walking and will be considered to move at a speed of about 3-5km/h.

Vehicles such as cars or helicopters can move at high speed and may disconnect themselves to the MANET network being outside the coverage of the other nodes. Therefore such a vehicle can either leave the MANET, or enter another MANET or even get isolated. In the first case, the MONET system must ensure that the vehicle connects with the second MANET thanks to a communication handover. Mechanisms such as updating routing tables and registering the vehicle as a new node of the MANET will be implemented. The maximum targeted speed for the handover is 50 km/h.

In the second case, the vehicle can remain connected with the network if it owns a satellite terminal, but establishing a link while moving is hard to achieve, especially at high speeds. Therefore satellite connections will only be supported for static entities.

2.2.8 Interconnection with remote location

A communication with a back office or a command centre is mandatory. The back office gathers the reports and information sent by the field unit (CP and FR) and leads the deployment of these units. It is in charge of assessing the situation and taking the decisions

that will solve the crisis. This back office must be located far from the theatre in order to be safe and to have a global vision of the situation. Thus a long distance communication capability between field units and this back office is of major importance.

The CP also needs to be able communicate with distant entities, such as hospital in order to exchange information on injured people. It also may need to access remote databases (dynamic or static) to retrieve information (meteorological, digital mapping…)

In Slovenia the intervention leader needs to have a constant and reliable voice connection with a competent 112 centre in order to be able to activate additional search and rescue forces in the case of need. According to the development of the intervention the leader decides whether he/she needs additional help. Therefore a possibility of a constant contact with 112 centres has to be assured.

2.2.9 Interoperability

Another critical point is the **interoperability** with existing systems. It is not possible to assume that MONET is available to every intervention force on the emergency scene. This is especially true when a crisis involves actors from several countries. The difference between the used communication systems can make the coordination of intervention forces difficult and expand the duration of the emergency phase. A very unfortunate but good example was the recent earthquake in Haiti where according to the information from MIC (Monitoring and Information Centre with the European Commission) even more than one week after the earthquake strike only satellite and radio communications worked.

However, equipments such as TETRA which widely spread amongst public safety intervention forces are proprietary systems. Interoperating with it will be hard to achieve and thus it will be left out of the scope of MONET.

Combined operations of today between different public safety users from different countries for example require an ‘ad-hoc’ way of interconnecting with the systems of unexpected external parties (like NGOs). Ad hoc interoperability is an attempt to define in the first place the lowest common denominators needed for a basic level of interoperability between very different organisations. At the lower communications layers possible solutions can assume adoption of standard established communications protocols, notably ISDN, IP, for mobility UMTS and related mobile telecommunications standards, and for local connectivity the emergent standards of IEEE-802.11 and Bluetooth. At the middleware level solutions can assume adoption of well established and easily obtained systems and software and at the information level solutions may seek simple interchange methods:

- Formatted messages
- Standard file exchange capabilities [e.g. via FTP]
- Standard sub-set of file formats:
- Word, RTF
- JPG, TIFF
- MPG, Mov
- ASCII Files
- Screen scraping

Ad-hoc interoperability requires the underlying information standards (data models) to be more flexible than is currently the case, so that new types of information can be added to the existing structure without extant data.

For MONET, and given the scope of different systems and data models in use by different public users and emergency response bodies, it can only be envisaged to achieve a simpler level of interoperability, namely of ad-hoc interoperability and co-existence. The fact that most systems now in use by police, civil protection, medical emergency and firemen are closed and proprietary adds to the complexity of creating truly interoperable and integrated solutions. Thus, it does not make sense to derive as a requirement the necessity to interoperate MONET with other networks and systems at higher levels than interchange. Of course, the MONET architecture should and will be designed to take into consideration as much as possible the capability to interoperate with other systems, namely European open standards on DMR. The consortium will also strive to provide insights and views on how higher levels of interoperability could be achieve in the future.

2.2.10 Availability

The system shall achieve the highest availability rate possible. It is mandatory to have access to the system at least **99,90**% of the time. A rate of **99,99**% would be desirable. In order to achieve this rate, the system must take into account potential congestions during the emergency phase of the crisis as well as the environmental constraints linked to the different theatres (smoke on fire centre, rain/fog in coastal area…). Interferences with other frequency bands must also be considered, especially if the exclusivity of the band used for the MONET system cannot be guaranteed. If not, the deployment of the MONET system in non-usual locations (in case of an intervention in another country, for instance) could interfere with already present systems.

2.2.11 Security

The system must offer sufficient security mechanisms to cope with the criticality of the data carried on the system. Some of the communication cannot suffer from being lost and sent again, as time is a most important factor in the early phases of the crisis. In particular, voice communications need to be clear and understandable by every party, because asking to repeat critical information or take the risk that an instruction may be misunderstood, cannot be tolerate.

The system must also ensure the immediacy of the transmission of data, and avoid congestions. For instance, the management, of the positions of FRs must be precise. In that regard, the positions of every FRs are updated every 5s. The delay of the refreshment should be minimal in order to preserve the accuracy of the dispatching.

As the potential scenarios encompass criminal activities, it is mandatory that the communication is encrypted with a sufficient level to ensure confidentiality. For the search and rescue missions authentication as well as ciphering is required. With them eavesdropping from uninvited third parties is prevented.

The security mechanisms shall apply on every communication happening between any of the units and shall be compliant with the different segments that compose the MONET system (MANET and satellite).

2.2.12 Resilience

The system must be resilient in order to offer the greatest availability. Due to the extreme conditions of the theatres the MONET system will be deployed in, incidents are likely to happen and may disable a node. The overall system shall provide backups mechanisms, in case such an incident were to happen.

Also, the importance of the data carried on the system means that redundancy mechanisms shall be used to ensure a minimum loss rate.

2.2.13 Quality of Service

The system must offer sufficient security mechanisms to cope with the criticality of the data carried on the system. Some of the communication cannot suffer from being lost and sent again, as time is a most important factor in the early phases of the crisis. In particular, voice communications need to be clear and understandable by every party, because asking to repeat critical information or take the risk that an instruction may be misunderstood, cannot be tolerate.

The system must also ensure the immediacy of the transmission of data, and avoid congestions. For instance, the management, of the positions of FRs must be precise. In that regard, the positions of every FRs are updated every 5s. The delay of the refreshment should be minimal in order to preserve the accuracy of the dispatching.

3 Technical requirements

3.1 System requirements

3.1.1 High level architecture prerequisites and requirements

3.1.1.1 Classification and type of Nodes

- **Portable** nodes will be carried by pedestrian FRs. They must easy to carry, have a sufficient autonomy and possess interface with the other equipments carried by the pedestrian FR, such as sensors. This kind will likely not have any satellite capability. This node will convey sensor data, voice, video, and alarms

- **Relay** nodes will be dropped by an FR or any other mean on the emergency theatre. Its goal is to be a radio relay amongst the FR, in order to ensure the continuity of the MANET and avoid too many splits within the network. As such, the weight requirements are not as restrictive as for the portable node, but it needs greater autonomy and resilience. It could also embed sensors, store data for post-emergency analysis, and provide satellite capability.

- **Vehicular** nodes will be embedded within emergency vehicles. As such they can be heavier than field nodes, and includes more components. They will be in charge of treating a greater amount of data and must be able to display and process this information. They also need satellite capability in order to ensure backhauling and connectivity with the rest of the field nodes. They will be powered by the vehicle battery.

- **Fixed** nodes will be used in fix basements, such as the BO, or any emergency unit headquarter. The restriction on weight and autonomy are very low, but they need to be able to process a lot of data and have satellite capability to connect to the rest of the network.

3.1.1.2 Classes of Public Safety traffic and services

The importance of a given traffic can be defined in two ways:

- Urgency – in that case, the age of the information is critical. Retransmission is not an option in so far as the value of the information transmitted decrease with the time taken to deliver it,
- Delivery – in that case, the value of the data transmitted is the content of the data, which needs to be delivered even with a few delay. The packets are time sensitive but they do not become less important if they are delivered slightly later.

Mission critical services can be both important in terms of urgency and delivery. For the MONET project, it is proposed to adopt a classification of typical traffics used in Public Safety and Security operations that has been defined in the MESA project, in order to ensure the coherence between MONET outcomes and the other related projects (ref AD2). This classification takes into account 2 parameters: delivery and urgency.

Class 0	Urgency: Very High Delivery: Very High
Mission critical voice, video and data communications. Immediate delivery. Retransmission is not an option. Group communications. Bidirectional transmissions.	
Class 1	Urgency: High Delivery: Medium
Non mission critical voice and video conferencing. Retransmission might be an option. Group communications and group management. Voice and video standard requirements in terms of latency, jitter and packet loss, in order to ensure a good Quality from the user point of view.	
Class 2	Urgency: High Delivery: High
Signalling and control messages. Low latency and packet loss. This class of messages should only represent a small amount of the total traffic. TCP or similar session protocol is recommended to ensure the delivery of those control messages.	
Class 3	Urgency: Medium Delivery: High
Instant messaging and database queries. Interactive low band communications. Packet loss should be prevented. Retransmission of lost packets. (TCP or similar protocol is recommended). Reasonable latency.	
Class 4	Urgency: Low Delivery: High
Data transfer (images, files, video streaming). High bandwidth communications. Time independent. Packet loss should be prevented. Possible retransmission of loss packets. Delay of transmission in case of other classes pre-emption.	
Class 5	Urgency: Low Delivery: Low
General network applications (web browsing, e-mails, others…).	

Table 4 - Class of traffic - MESA project

3.1.1.3 System mechanisms

The overall system must be easy to deploy. Intervention units arriving on a crisis scene must be able to act immediately relying on an accurate data collection and an appropriate communication framework in order to safely begin the operations. Because of this requirement, the MONET system must self-install quickly and be easily used by the emergency teams.

As the units are often in critical conditions where the environment can change very fast, the system must adapt itself in an efficient way according to the operation flow. For instance, it must react quickly to events such as an FR leaving the scene, a change in environmental condition (expansion of the fire centre...), or a failure in a component of the system.

Self-installation and self-reorganization of the entire network shall maximize the effectiveness of the system while letting the end-users focus on the operations instead of being distracted by network management.
These mechanisms include:

- Automatic discovery and integration of new nodes
- Switching from radio interface to satellite interface (if available) in case of a split of the MANET
- Activating a second satellite terminal besides the CP to avoid a congestion within the MANET
- Handover of a node transiting from one MANET to another
- Switching to another satellite interface with the BO if the CP fails.

3.1.2 General requirements

3.1.2.1 Type of traffic

Video is essential as it provides a visual report of the situation on field. Classical video streaming can be done with several protocols, most of which are relying on the IP protocol. One of the common solutions is the use of the RTP/UDP protocol. Video does not require strong timelessness, although the delay of the streaming should be low, as it is supposed to provide a real-time evaluation of the situation. Potential troublesome points specific to video include the bitrate which is quite high even for a low quality video. Video streaming is likely to be the major factor increasing the overall bitrate in the network. Also, it is to consider that video streaming may require encoding/decoding, which can ask for a lot of processing power. It is mandatory that a MONET node can stream a video without suffering any loss of quality due to processing power

Data transfer can be a download from an entity within the system from an external source, or an exchange of data between entities. In the first case, the data is transferred for support purposes and complete the data collected by FRs. The requirements for this type of data are low, since it can be big but there is no need for them to be real time.

On the other hand, data exchanged between 2 FRs, for instance, are usually generated by the sensors carried by the FRs. This data can be considered as critical as it represents real-time information. Therefore it is used to establish a continuous monitoring of the situation, thus requesting periodic refreshment. As an example, positioning data need to be updated every 5s, or when it moves over a specific distance, in order to track its movements.

Voice needs a low bitrate but is the most important service within the system. In particular, its requirements in term of timelessness are very high in order to preserve the quality of the communication. In this regard, jitter for voice communication must be kept really low. Also,

even if delay is less important, it should be low as well because of the importance of time in a emergency.

3.1.2.2 Terminals characteristics

- **Portable** nodes shall have a maximum weight of 1kg and should have dimensions around 150 x 60 x 40 mm. Power supply of portable node shall be by means of a battery with a minimum autonomy of 5 hours.

- **Vehicular** nodes shall have a maximum weight of 30kg. Power supply of vehicular node shall be through vehicular battery (12V or 24V).

- **Relay** nodes shall have a maximum weight of 10kg and should have dimensions around 300 x 300 x 200 mm. Power supply of relay node shall be by means of a battery with a minimum autonomy of 8 hours.

- **Fixed** nodes do not have weight and dimensions restrictions. Power supply of portable node shall be through power grid.

3.1.2.3 Connectivity requirements

The MONET system is composed of several kinds of entities that interact in many ways. It is important to define which will communicate, what kind of traffic will be exchanged, if the communication is bidirectional and if it involves more than 2 entities, in order to predict the repartition of the traffic load on the network. The following diagrams present the communication flows between each entities, and the traffic involved. Several units composed of a CP and several FRs are represented as communication can happen between such groups. Strayed arrows represent communication flows that are less important, because it represents a requirement that would be nice to have but is not mandatory considering current procedures, or because their implementation is difficult in the frame of MONET.

Voice communication between MONET entities involves:

- Point-to-point (P2P) voice communication between :
  - CP and BO
  - CPs
  - CPs and external entities
  - FR to BO
  - FR to external entities

- Point-to-multipoint voice communication between
  - all of the FRs within the same unit and the CP responsible for this unit
  - the CP to the FRs of its unit
  - Several talk groups (e.g. Medical services and Civil guard)
  - The CP and FRs from the same unit and the BO

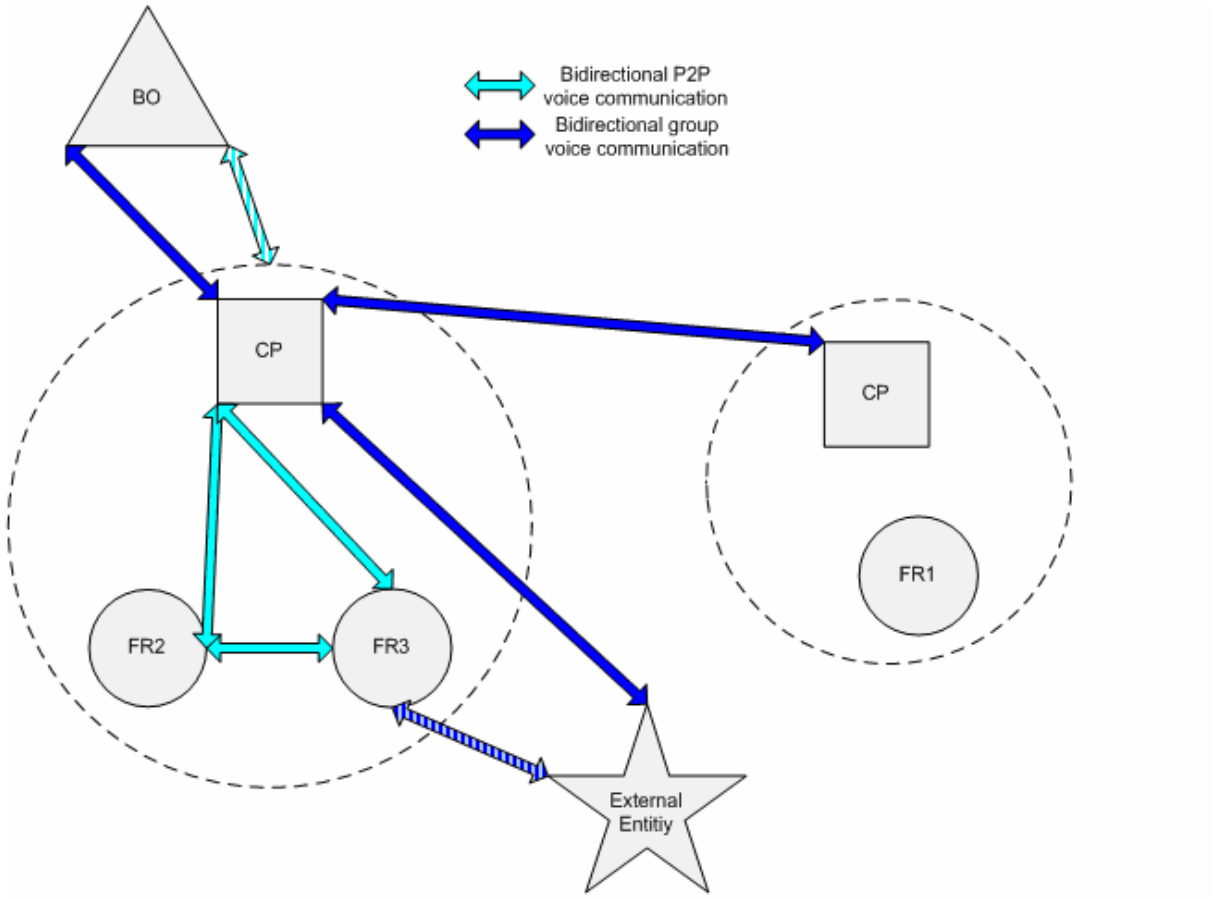

Figure 1 - Communication flows (voice) between MONET entities

Other kinds of communication between MONET entities involve:

- Real time video transfer from :
  - CP to BO
  - FRs to CP
- Bidirectional data communication (biometric data, sensor data) between :
  - FR and CP
  - CP and BO
- Location services from FR to CP
- Data retrieval (maps, meteorological data..) from external sources from:
  - CP
  - BO
- Communication between CP and external entities (voice, data, file transfer

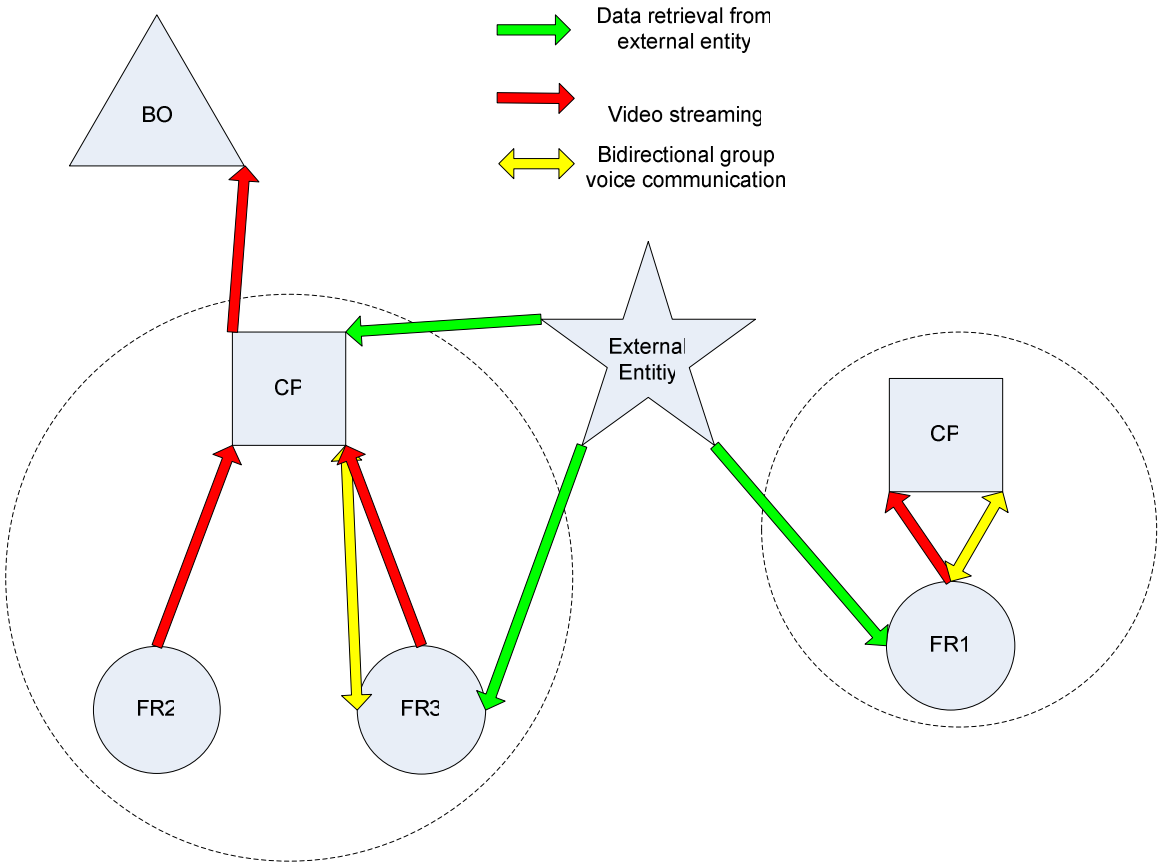

Figure 2 - Communication flows (other) between MONET entities

3.1.2.4 Data rate and global capacity requirements

The system shall support a traffic load greatly changing from one type of emergency to another. 4 sizes of theatres have been defined based on the usual classification (see Table 3) and the study scenario of the MONET project.

- Emergency **level 1** theatres involve **around 10** concurrent users. This class of theatre is used to qualify small everyday operations
- Emergency **level 2** theatres involve **between 10 and 100** concurrent users. This class of theatre is used to qualify small to medium operations
- Emergency **level 3** theatres involve **between 100 and 250** concurrent users. This class of theatre is used to qualify medium to large operations
- Emergency **level 4** theatres involve **around 500** concurrent users. This class of theatre is used to qualify large operations

In order to calculate the overall capacity of the system, average bitrates have been defined for each kind of terminal according to their service requirements:

- **Portable Nodes** shall be carried by pedestrian FRs. They don't have any satellite capacity and exchange data, voice calls, video, positioning information, and alarm signals. Therefore they need at least 300 Kbps. Activity rate is set to 70 % due to the

frequency of voice calls in emergency phases and the permanence of data and video exchange at all times.

- **Relay Nodes** shall be carried and dropped on the field by pedestrian FRs. They don't have any satellite capacity and send sensor data, video, images and positioning information. Therefore they need at least 300 Kbps. Activity rate is set to 50 % due to data and video exchange at all times.

- **Vehicular nodes** are embedded on vehicle and do possess satellite capability. Therefore they can be isolated from the MANET and still communicate with it through the satellite link. The occurrence of this situation has been set at 20 % of the time. The vehicular node exchanges data, voice calls, video, positioning information, and alarm signals with the rest of the MANET and concentrates all the data sent by the FRs. Therefore it needs at least 400 Kbps. The activity rate has been set to 80%. On the other hand, a vehicular node can be considered as a CP which is connected with the back office for backhauling purposes. This type of communication is exclusively done by satellite and consists in exchanging data, video, and voice calls between the CP and the BO. Therefore the required data rate should be at least 330 Kbps. The activity rate is around 80%.

- **Fixed nodes** are located in the back office and are exchanging data, video, and voice calls with the CP through satellite. Therefore the required data rate should be at least 330 Kbps. The activity rate is around 80%.

Platform	nb	Data rate (Mbps per unit)		Repartition		Activity rate %	Capacity (Mbps)			
				Satellite	Terrestrial		Satellite		Terrestrial	
ER level 1		Min	Max				Min	Max	Min	Max
Portable Node	8	0,35	0,6	0%	100%	70%	0	0	1,96	3,36
Relay Node	1	0,3	0,6	0%	100%	60%	0	0	0,18	0,36
Vehicular Node (field)	5	0,4	0,8	20%	80%	80%	0,32	0,64	1,28	2,56
Vehicular Node (Backhauling)	1	0,33	0,6	100%	0%	100%	0,33	0,6	0	0
Fixed Node (BO)	1	0,33	0,6	100%	20%	100%	0,33	0,6	0,066	0,12
TOTAL	**16**	**1,71**	**3,2**				**0,98**	**1,84**	**3,486**	**6,4**
ER level 2		Min	Max				Min	Max	Min	Max
Portable Node	15	0,35	0,6	0%	100%	70%	0	0	3,675	6,3
Relay Node	2	0,3	0,6	0%	100%	60%	0	0	0,36	0,72
Vehicular Node (field)	15	0,4	0,8	20%	80%	80%	0,96	1,92	3,84	7,68
Vehicular Node (Backhauling)	2	0,33	0,6	100%	0%	100%	0,66	1,2	0	0
Fixed Node (BO)	1	0,33	0,6	100%	20%	100%	0,33	0,6	0,066	0,12
TOTAL	**35**	**1,71**	**3,2**				**1,95**	**3,72**	**7,941**	**14,82**
ER level 3		Min	Max				Min	Max	Min	Max
Portable Node	135	0,35	0,6	0%	100%	70%	0	0	33,075	56,7
Relay Node	10	0,3	0,6	0%	100%	60%	0	0	1,8	3,6
Vehicular Node (field)	60	0,4	0,8	20%	80%	80%	3,84	7,68	15,36	30,72
Vehicular Node (Backhauling)	4	0,33	0,6	100%	0%	100%	1,32	2,4	0	0
Fixed Node (BO)	1	0,33	0,6	100%	20%	100%	0,33	0,6	0,066	0,12
TOTAL	**210**	**1,71**	**3,2**				**5,49**	**10,68**	**50,301**	**91,14**
ER level 4		Min	Max				Min	Max	Min	Max
Portable Node	350	0,35	0,6	0%	100%	70%	0	0	85,75	147
Relay Node	20	0,3	0,6	0%	100%	60%	0	0	3,6	7,2
Vehicular Node (field)	100	0,4	0,8	20%	80%	80%	6,4	12,8	25,6	51,2
Vehicular Node (Backhauling)	10	0,33	0,6	100%	0%	100%	3,3	6	0	0
Fixed Node (BO)	2	0,33	0,6	100%	20%	100%	0,66	1,2	0,132	0,24
TOTAL	**482**	**1,71**	**3,2**				**10,36**	**20**	**115,082**	**205,64**

Figure 3: Matrix of traffic for MONET network

As shown above, requirements in term of bitrates for large theatre involving around 500 concurrent users are very heavy and are likely to be hard and/or costly to achieve. Due to the difficulty of validating large scale scenarios, the testing phase will concentrate on validating the level 1 scenario (10 users), which is achievable in term of simulation.

As for the other levels, the impact of scaling MONET to larger theatres will be studied in the optimization phase. Scalability to 50, 100 and 500 users shall be theoretically assessed in order to have an insight of the capability of MONET to be used on large scale events. The studied elements will include the cost of the satellite link for a high bandwidth, the ability of a MANET network to support large systems and loads of traffic, and the impact of scalability in term of operational needs.

3.1.3 Synthesis of General requirements

Previously defined requirements are compiled hereafter. They are classified following categories of requirements, for better organization. They also have been given a priority number which meaning follows:

- **1** is mandatory: this requirement is part of the concept of MONET and cannot be overlooked
- **2** is important: the requirement is claimed by the end-users and would definitely enhance the system. However, would it be impossible to meet or its implementation would involve dramatic changes to the overall architecture, it should not be implemented.
- **3** is desired: Those requirements concern MONET orientations which are close to the border of the scope of MONET. They could become interesting ideas for a further development, but achieving them is not a priority of the project.

It must be noticed that these levels do not correspond exactly to those stated in section 2.1.1, which describe the importance granted to user needs by the users themselves. The present ones take into account the feasibility of the requirements, therefore mitigating the formers. For instance, a user need labelled as required could get translated into functional requirements and get a priority of 1, considering it is important to the user and it has been preliminary assessed as feasible. On the other hand, a user need which is considered mandatory by the user but is out of the scope of MONET will get a lower priority.

3.1.3.1 Connectivity requirements

Connectivity Requirements		
Requirement	**Priority**	**Description**
R_Gen 1	1	The system shall ensure point-to-point (P2P) voice communication between : • CP and BO • CPs • CPs and external entities
R_Gen 2	3	The system shall ensure point-to-point (P2P) voice communication between : • FR to BO • FR to external entities

R_Gen 3	1	The system shall ensure point-to-multipoint (PTT) voice communication between • all of the FRs within the same unit and the CP responsible for this unit • the CP to its unit FRs
R_Gen 4	3	The system shall ensure point-to-multipoint (PTT) voice communication between • Several talk groups (e.g. Medical services and Civil guard)
R_Gen 5	1	The system shall ensure real time video transfer from FRs to CP
R_Gen 6	3	The system shall ensure real time video transfer from CP to BO
R_Gen 7	1	Bidirectional data communication (biometric data, sensor data, images…) between : • FR and CP • CP and BO
R_Gen 8	3	The system shall ensure the transmission of location data from FRs to their CP

Table 5 – connectivity requirements.

3.1.3.2 Mobility requirements

Mobility Requirements		
Requirement	**Priority**	**Description**
R_Gen 9	1	**Portable nodes** shall support ATH (At The Halt) communication capabilities on their terrestrial interface.
R_Gen 10	1	**Vehicular nodes** shall support ATH (At The Halt) communication capabilities on their terrestrial interface.
R_Gen 11	1	**Relay nodes** shall support ATH (At The Halt) communication capabilities on both terrestrial and satellite interfaces.
R_Gen 12	1	**Fixed nodes** shall support ATH (At The Halt) communication capabilities on both terrestrial and satellite interfaces.
R_Gen 13	1	**Portables nodes** shall support OTM (On The Move) communication capabilities up to 5 km/h on the terrestrial interface.
R_Gen 14	1	**Vehicular nodes** shall support OTM (On The Move) communication capabilities up to 50 km/h on the terrestrial interface.

Table 6 – mobility requirements.

3.1.3.3 Compatibility

Interfaces Requirements

Requirement	Priority	Description
R_Gen 16	1	The system shall provide compatibility with video recording equipments carried by the intervention units
R_Gen 17	1	The system shall provide compatibility with positioning equipments carried by the intervention units
R_Gen 18	1	The system shall provide compatibility with sensor equipments (medical, bio-sensors…) carried by the intervention units
R_Gen 19	1	The system shall provide compatibility with alarm equipments carried by the intervention units
R_Gen 20	1	The system shall provide compatibility with voice equipments carried by the intervention units
R_Gen 21	2	MONET nodes user interface channels should support the following interface types: • Speech-To-Text • Text-To-Speech

Table 7 – interface requirements.

3.1.3.4 Interoperability,

Interoperability Requirements		
Requirement	**Priority**	**Description**
R_Gen 22	1	The system shall be compliant to European Open interoperability standards
R_Gen 23	1	The system shall allow communication with other intervention forces, institutions and companies involved in the incident
R_Gen 24	1	The system shall allow communication between intervention units from European countries, for cross-border operations and major disasters involving a large panel of players

Table 8 – interoperability requirements.

3.1.3.5 Operational requirements

Operational Requirements		
Requirement	**Priority**	**Description**
R_Gen 25	1	The system shall provide mechanisms for auto configuration and self reorganization, including: • Automatic setup of the MANET. • Automatic discovery and integration of new nodes • Handover of a node transiting from one MANET to another • …
R_Gen 26	1	The system installation and setup on the emergency field will need less than 5mn before being fully operational.
R_Gen 27	1	The system shall provide means to ensure the **resilience** of

		the network. Backup, redundancy and self re-organization mechanisms will guarantee that a failure of a single node cannot bring the entire system down. These means include: • Switching to another satellite interface with the BO if the CP fails. • Activating a second satellite terminal besides the CP to avoid a congestion within the MANET • ..

Table 9 – operational requirements.

3.2 Functional requirements

Traffic Requirements		
Requirement	**Priority**	**Description**
R_Func 1	1	The communication system shall allow all types traffic based on IP protocols: VoIP, video streaming, FTP transfer, image transfer, e-mail exchange, etc. It will also support the transmission of alarm and SMS services.
R_Func 2	1	The communication system shall provide **unicast** communication capability.
R_Func 3	1	The communication system shall provide **multicast** communication capability.

Table 10 – traffic requirements.

QoS Requirements		
Requirement	**Priority**	**Description**
R_Func 4	1	The system shall allow **prioritization** of traffic, in order to ensure critical flows to be transmitted
R_Func 5	1	The system shall ensure the **compliance** of Satellite and MANET segments QoS mechanisms

Table 11 – QoS requirements (functional).

Security Requirements		
Requirement	**Priority**	**Description**
R_Func 6	1	The system shall ensure **confidentiality** of mission critical communications.
R_Func 7	1	The system shall ensure **authentication** of end-users entering the MONET system
R_Func 8	1	The system shall control the **authorization** all entities belonging to it and allow the definition of conditions of access to information. • By default, all users will be authorized to view all information, transmit information and receive information. • By default, users will not be able to change information transmitted by other users.

R_Func 9	1	The system shall provide **data resilience mechanisms** to ensure **delivery** of the information
R_Func 10	1	The system shall ensure **authentication** of end-users for mission critical communications.
R_Func 11	1	The system shall provide means to ensure the **resilience** of the network. Backup, redundancy and self re-organization mechanisms will guarantee that a failure of a single node cannot bring the entire system down.

Table 12 - security requirements.

Positioning Requirements		
Requirement	**Priority**	**Description**
R_Func 12	1	**Portable nodes** shall be able to send positioning information to the command post
R_Func 13	1	**Relay nodes** shall be able to send positioning information to the command post
R_Func 14	1	**Vehicular nodes** shall be able to send, receive and display positioning information
R_Func 15	1	**Fixed node** shall be able to receive and display positioning information

Table 13 – positioning requirements.

3.3 Performance requirements

Data rate requirements		
Requirement	**Priority**	**Description**
R_Perf 1	1	**Portable nodes** shall ensure communication at a minimum data rate of 600 kbps/600 kbps (uplink/downlink) for Portable Nodes The least acceptable bitrates will be 350 kbps/350 kbps
R_Perf 2	1:	**Relay nodes** shall ensure communication at a minimum data rate of 550 kbps / 550 kbps (uplink/downlink) The least acceptable bitrates will be 300 kbps / 300 kbps
R_Perf 3	1	**Vehicular nodes** shall ensure communication with the MANET at a minimum data rate of 800 kbps / 800 kbps (uplink/downlink) The least acceptable bitrates will be 400 kbps / 400 kbps
R_Perf 4	1	**Vehicular nodes** acting as CP shall ensure backhauling communication at a minimum data rate of 600 kbps/600 kbps (uplink/downlink) The least acceptable bitrates will be 330 kbps / 330 kbps
R_Perf 5	1	**Fixed nodes** shall ensure communication at a minimum data rate of 600 kbps / 600 kbps (uplink/downlink)

		The least acceptable bitrates will be 330 kbps / 330 kbps

Table 14 – data rate requirements.

Global capacity requirements		
Requirement	**Priority**	**Description**
R_Perf 6	1	The system shall be able to support up to 10 concurrent users The impact of scaling the system to 50, 100 and 500 users shall be assessed in WP4 in term of: • Cost of bandwidth for the satellite link • Capacity of the MANET to handle high number of users • Capacity of the MANET to handle a very high traffic load. • ...
R_Perf 7	1	The MONET node shall provide radio coverage of **100m.** The least acceptable range shall be 50m
R_Perf 8	2	Extending the coverage of the MONET node to **300m** shall be studied in term of impact, cost and feasibility, and if satisfactory, implemented.
R_Perf 9	1	The system shall ensure a global satellite capacity of **2 Mbps** in order to be used on large scale theatres. The least acceptable bitrate shall be 1 Mbps
R_Perf 10	1	The system shall ensure a global MANET capacity of **6,5 Mbps** in order to be used on large scale theatres. The least acceptable bitrate shall be 3,5 Mbps

Table 15 – global capacity requirements.

QoS requirements		
Requirement	**Priority**	**Description**
R_Perf 11	1	Latency of mission critical flow (Class 0) such as voice shall be less than **600 ms.** Latency of Class 1 flow shall be less than **1s.**
R_Perf 12	1	Jitter of mission critical flow (Class 0) such as voice shall be less than **50 ms.**
R_Perf 13	1	For voice and video conference applications, packet loss shall be less than: • 2% for Class 0 • 4% for Class 1
R_Perf 14	1	For PTT voice calls, maximum set-up duration of **200ms** shall be ensured. The least acceptable setup time shall be 1s.

R_Perf 15	1	For P2P voice calls, a maximum set-up duration of **3s** shall be ensured

Table 16 – QoS requirements (performance).

Availability requirements		
Requirement	**Priority**	**Description**
R_Perf 16	1	For mission critical (Class 0), the communication capability shall be available **99.95%** of the time.
R_Perf 17	1	For other class, the communication capability shall be available **99.90%**

Table 17 – Availability requirements.

Energy requirements		
Requirement	**Priority**	**Description**
R_Perf 18	1	Relay nodes shall be powered by battery and have autonomy of **12 hrs.** The lowest acceptable autonomy shall be 8 hrs
R_Perf 19	2	Portable nodes shall be powered by battery and have an autonomy of **8 hrs** The lowest acceptable autonomy shall be 5 hrs
R_Perf 20	1	Vehicular nodes shall be powered by the vehicle battery

Table 18 – energy requirements.

3.4 Hardware requirements

The following requirements are not relevant to a MONET prototype. They won't be validated in the scope of MONET but represent low level requirements that should definitely be met in order for MONET to be usable in real conditions.

Dimension requirements		
Requirement	**Priority**	**Description**
R_Hard 1	1	Portable Node shall not exceed a size of 150 x 60 x 40 mm
R_Hard 2	2	Relay nodes shall not exceed a size of 300 x 300 x 200 mm

Table 19 – HW dimension requirements.

Weight requirements		
Requirement	**Priority**	**Description**
R_ Hard 3	1	Portable Node weight shall not exceed 1 kg
R_ Hard 4	1	Relay Node weight shall not exceed 10 kg

R_ Hard 5	2	Vehicular Node weight shall not exceed 30 kg

Table 20 – HW weight requirements.

Resilience requirements		
Requirement	**Priority**	**Description**
R_ Hard 6	1	**Portable nodes** shall support **temperatures** from -30°C to 60°C
R_ Hard 7	1	**Relay nodes** shall support **temperatures** from -30°C to 60°C
R_ Hard 8	1	**Portable nodes** shall support a **humidity** ratio of 100%
R_ Hard 9	1	**Relay nodes** shall be support a **humidity** ratio of 100%
R_ Hard 10	1	**Portable nodes** shall be highly resilient to shocks and vibrations
R_ Hard 11	1	Relay nodes shall be highly **resilient** to shocks and vibrations
R_ Hard 12	1	**Vehicular nodes** shall be highly **resilient** to shocks and vibrations
R_ Hard 13	1	**Portable nodes** shall be compliant with the **ATEX regulation** for devices working in explosives atmospheres
R_ Hard 14	1	**Relay nodes** shall be compliant with the **ATEX regulation** for devices working in explosives atmospheres
R_ Hard 15	1	**Vehicular nodes** shall be compliant with the **ATEX regulation** for devices working in explosives atmospheres

Table 21 – HW resilience requirements.

Cost requirements		
Requirement	**Priority**	**Description**
R_Cost 1	1	Portable nodes price shall not exceed 800 Euros. The lowest acceptable price shall be 1000 Euros.

Table 22 – HW cost requirements.

3.5 Impact & requirements – Satellite segment

The following section contains some requirements specific to the satellite segment. A part of them answers to specific considerations caused by some aspects of the satellite segment, while others are a derivation of the formerly defined requirements in the scope of satellite.

3.5.1 Impact on the satellite segment

The advanced satellite technologies will have impacts on several aspects to the MONET system when integrating both satellite networks and ad-hoc networks together due to the internetworking needed. It includes impacts on system architecture, functional blocks, resource management, security and QoS.

- **System architecture**: The satellite network can act as a hub for all terrestrial ad-hoc networks for its wide coverage and no need of terrestrial infrastructure support. That implies a star topology of the whole MONET system. Clearly, all traffics between each pair of two ad-hoc network will go through the satellite network. It gives the opportunity for hierarchical architecture with distributed logical centres with the root in the satellite network and sub-root(s) in each ad-hoc network plot. This architecture takes advantage of the star network topology and benefit the network management at each root and sub-root. It also lowers the risk of scalability issues with a logical centre for each ad-hoc network plot. Traffic engineering algorithms to optimize the network traffics can be easily deployed and maintained on these centre nodes. By applying multiple centre nodes using some optimized means in each centre can provide robustness and resilience to the whole system.

- **Functional blocks**: To interwork between satellite networks and ad-hoc networks, new functional block is essential to allow traffic flow through the system while being transparent to end users. The satellite networks need understand whatever protocols chosen to be used in the ad-hoc network that will include signalling, routing, QoS, address mapping, security, etc. There are management functions as well within the satellite network in order to negotiate with counter parts in ad-hoc networks. Furthermore, the satellite network might need to host some functions that are not suitable to locate within ad-hoc networks such as multicast routers.

- **Resource management**: resource management can be handled within each ad-hoc network and satellite network separately. However, to achieve optimized results, global resource management might be needed to maximize the utility of limited bandwidth resources in the satellite network and minimize the power consumption within ad-hoc networks.

- **Security**: Due to the broadcast nature of satellites eavesdropping and traffic monitoring by intruder is easier in satellite networks. Thus data encryption is required over the satellite link. In addition, other threats are possible such masquerading (an intruder pretending to be legitimate user), Denial of Service (DoS), message modifications and replay of old (authentic) message attacks. Therefore for certain type of MONET services, there will be a need for satellite data encryption and integrity checking (for example using digital signature). The MONET security architecture may support hop-by-hop and end-to-end encryption and authentication. This will require security interworking between adhoc and satellite network. However, there is one negative impact of end-to-end security (for example using IPSec in transparent mode), which might prevent middle entities (such as QoS or resource management stations) from working properly, if they require access to the IP packet data such as TCP, UDP, RTP or HTTP headers.

- **QoS:** MANET ad-hoc networks have their own QoS algorithms be taking the power consumption and mobility into account which satellite networks do not care. What the satellite networks QoS algorithms are trying to achieve is to maximize the bandwidth utilities by using bandwidth reservation, dynamic bandwidth allocation and advanced scheduling algorithm. These differences will cause conflictions when to provide end-to-end QoS solutions within such a hybrid system. For instance, the ad-hoc nodes

acting as satellite terminals might run out power very quickly when execute all those procedures for bandwidth reservation, bandwidth allocation and advanced scheduling.

- **End-to-end performance:** The normal data Round Trip Time (RTT) could be up to 600ms within a GEO satellite network and signalling for call setup could be several seconds. This impact is unavoidable and has to be taking into account when evaluate the network performance for MONET system.

3.5.2 Satellite segment requirements

Satellite service requirements		
Requirement	**Priority**	**Description**
R_Sat_Serv 1	1	Full Cross-Connectivity between Uplink and Downlink shall be supported by regenerative payload
R_Sat_Serv 3	1	The system shall support both Unidirectional connections and Bi-directional connections
R_Sat_Serv 4	1	The MONET satellite network shall provide connectivity with IP public or private networks.
R_Sat_Serv 5	1	The MONET satellite network shall provide the Internet/Intranet Access Service for terminals working in router or bridge modes
R_Sat_Serv 6	1	Users may have a private or a public IP address to access to the Internet
R_Sat_Serv 7	1	Stateless auto configuration or DHCP self-configuring protocol server shall be included in the terminal, in order to allow the deployment of a self-configuring Network behind the terminal.
R_Sat_Serv 8	1	The satellite network should support the following services with corresponding QoS criteria: o Internet / Intranet access o VoIP and Video conferencing o Video Broadcast Service o Audio and Video on-demand (streaming) o Internet Services (e-medicine, e-commerce, e-government) o Media content download (Store & Forward) o Remote control of applications o Shared applications o Video surveillance

Table 23 – satellite service requirements.

Satellite Security requirements		
Requirement	**Priority**	**Description**
R_Sat_Serv 9	1	Data confidentiality shall be provided over the satellite link in order to prevent the eavesdropping attacks.
R_Sat_Serv 10	1	Protection of the satellite MAC address will be ensured in order to prevent an intruder from tracking the identity of MONET users and the volume of their traffic.

R_Sat_Serv 11	1	Integrity protection and source authentication to stop active attacks.
R_Sat_Serv 12	1	Protection against replay attacks.
R_Sat_Serv 13	2	Satellite key management functions should be decoupled from the MONET security services such as encryption and source authentication. This allows the independent development of both systems.
R_Sat_Serv 14	1	Support should be provided for automated as well as manual insertion of keys and policy into the relevant databases.
R_Sat_Serv 15	2	For interworking between satellite and adhoc networks, a centralised key management might be required to co-ordinate the key generation and distribution for various subsystems.

Table 24 – satellite security requirements.

4 Conclusion

This document describes and compiles the technical requirements for MONET. They have been derived from current procedures and expectation from end-users. Each requirement has been assigned with a priority which represents its criticality and the degree of effort it should get to be implemented.

The set of requirements will be used to design the MONET system, and will form the basis of the set of verifications to be applied to verify the compliance of the system with user needs.

As the requirement phase has been carried without considering the MONET system design feasibility, it may possible that some requirements appear too stringent, and non compliance will be analysed on case per case basis, also involving feedback from end users to quantify and mitigate their impact.

References

Reference documents

[RD1] MONET consortium, MONET-ICT-247176-D2.1 - Concept and use cases, 2010.

[RD2] MONET consortium, MONET-ICT-247176- D2.2 – Workshop Proceedings, 2010.

[RD3] MONET consortium, MONET-ICT-247176- D2.4 – Study scenarios, 2010.

Applicable documents

[AD1] MASON analysis: Public Safety mobile broadband spectrum needs

[AD2] MESA system overview