Action full title:

Universal, mobile-centric and opportunistic communications architecture

Action acronym:

UMOBILE

Deliverable:

D5.4 “Proof of Concept (2)”

Project Information:

Project Full Title	Universal, mobile-centric and opportunistic communications architecture
Project Acronym	UMOBILE
Grant agreement number	645124
Call identifier	H2020-ICT-2014-1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

Topic	ICT-05-2014 Smart Networks and novel Internet Architectures
Programme	EU Framework Programme for Research and Innovation HORIZON 2020
Project Coordinator	Prof. Vassilis Tsaoussidis, Athena Research Center

Deliverable Information:

This deliverable provides the description of the integration of the UMOBILE system as well as the details of the two demos that integrate the proof-of-concept.

The proof-of-concept was initially described in the deliverable D5.3 "Proof-of-Concept (1)" in month 24; this deliverable describes the progress of the work and the enhancements of the different components of the UMOBILE architecture the Consortium gained since then.

Deliverable Number-Title	D5.4 Proof of Concept (2)
WP Number	WP5
WP Leader	FON
Task Leader (s)	AFA Systems
Authors	**COPELABS**: Paulo Mendes **ATHENA**: Sotiris Diamantopoulos, Christos-Alexandros Sarros **UCL**: Sergi Rene, Ioannis Psaras **UCAM:** Adisorn Lertsinsrubtavee, Carlos Molina Jimenez **SENCEPTION:** Rute Sofia, Igor dos Santos, José Soares **TECNALIA**: Iñigo Sedano Perez **AFA**: Francesco Amorosa, Gianmichele Russi **FON:** Alberto Pineda, Pablo Salvador **TEKEVER**: Ricardo Faria, Luís Deprez, André Oliveira
Contact	amorosa@afasystems.it
Due date	M34: 30/11/2017
Actual date of submission	M34: 30/11/2017

Dissemination Level:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

PU	Public	x
CO	Confidential, only for members of the consortium (including the Commission Services)	
CI	Classified, as referred to in Commission Decision 2001/844/EC	

Document History:

Version	**Date**	**Description**
Version 0.1	10/11/17	Initial template with Table of Contents
Version 0.2	28/11/17	Components list
Version 0.3	29/11/17	Fix ing Table of Contents
Version 0.4	30/11/17	Combine with Tekever contribution
Version 0.5	01/12/17	Combine with UCAM contribution
Version 0.6	05/12/17	Combine with Copelabs contribution
Version 0.7	07/12/17	Combine with Senception contribution
Version 0.9	11/12/17	Introduction of support tests to POC1 and update of UAV HW tests
Version 0.11	12/12/17	Combine with UCAM contribution
Version 0.13	18/12/17	Combine with final UCAM, Athena and Tekever contribution
Version 0.14	19/12/17	Combine with final UCL contribution
Version 1.0	21/12/17	Combine with final Senception, UCL and Copelabs contribution Final version

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

Table of contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

List of figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

List of tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

Executive Summary

Background

Work Package 5 "**Overall platform integration and validation**" of UMOBILE project aims at the evaluation of the solutions developed in the project. A proof-of-concept is expected as an outcome of WP5. Task 5.3 "Proof-of-Concept"; it was initially described in the D5.3; this Report D5.4 describes the updates about the "Proof of Concept", detailing implementation choices, as well as validation of concepts that were not selected to be implemented, and the reasons to do so.

Objectives

The goal of this document is to provide a description of the different UMOBILE components, as emerged from the project, in terms of UMOBILE software modules for the UMOBILE gateways and UMOBILE End-user Service as apps for Android devices.

The proof-of-concept remains based on two specific demos, as initially envised: two independent technological demonstrations that rely on two of the use-cases selected in WP2. This D5.4 will focus to envision the tests that can be done, possibly in the UMOBILE Lab, in order to adequately prepare the final demo.

This report is a follow-up of report D5.3 – Proof-of-concept, and intends to describe ongoing status, as well as designing changes due to implementation limitations, and validation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

1. Introduction

The main goal of the UMOBILE project is to develop a mobile-centric service oriented architecture that efficiently delivers content to end-users, by decoupling services from their origin locations and shifting the host-centric paradigm to a new paradigm that incorporates aspects from both information-centric and opportunistic networking. To achieve this, the UMOBILE architecture combines two emerging architecture and connectivity approaches, Information Centric Networking (ICN) and Delay Tolerant Networking (DTN), into one single abstraction.

The technology UMOBILE that has developed is capable of supporting various challenged scenarios, such as aftermath of disasters or networks with limited backhaul capacity, that pose several challenges such as increased latency, intermittent connectivity, etc. To address these challenges, UMOBILE architecture has developed several modules: resilient service migration platform, which takes advantage of recent advances in lightweight operating systems to transfer and instantiate service instances right to the network edge; a Delay Tolerant framework that is capable of tunnelling, a Keyword-Based Mobile Application Sharing (KEBAPP) and others that will be discussing in subsequent sections.

Having already described in detail the envisioned UMOBILE services in D3.3 and the architecture design in D3.1, in this deliverable we focus on the description of the UMOBILE system components from a functional point of view and, mostly, on the integration of the components. While D5.1 provides the evaluation of the components individually, the present document focuses on the implementation progress of the whole system through the definition of the proof-of-concept, as well as of its validation status.

The proof-of-concept has been created based on two independent demonstrations, which rely on two of the use-cases selected in WP2, while in 5.3, the proof-of-concept elements have been described, D5.4 is a follow-up and provide the full steps expected to be taken for the proof-of-concept.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

In addition to the aforementioned, the present deliverable includes also a short guideline to the usage of the UMOBILE Lab, which will be used as testbed for the proof-of-concept, as well as details on the implementation of the Lab (attached to D5.3 as Annex A).

This document is organized as follows:

- **Section 2** provides the description of the integration steps of the UMOBILE system, having in mind the use-cases developed in WP2. The UMOBILE devices are defined and the interaction between software modules is described.
- **Section 3** describes the UMOBILE Lab, the testbed that will be used for the proofs of concept described in Section 4.
- Two different proofs of concept, corresponding to two of the use-cases selected in WP2, are reported and analyzed in **Section 4**.
- **Section 5** concludes the report.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

2. UMOBILE System Integration

Figure 1 (extracted from D3.3) shows the high-level design of the UMOBILE architecture [6] divided into two distinct domains: the **UMOBILE domain** and the **Internet domain**.

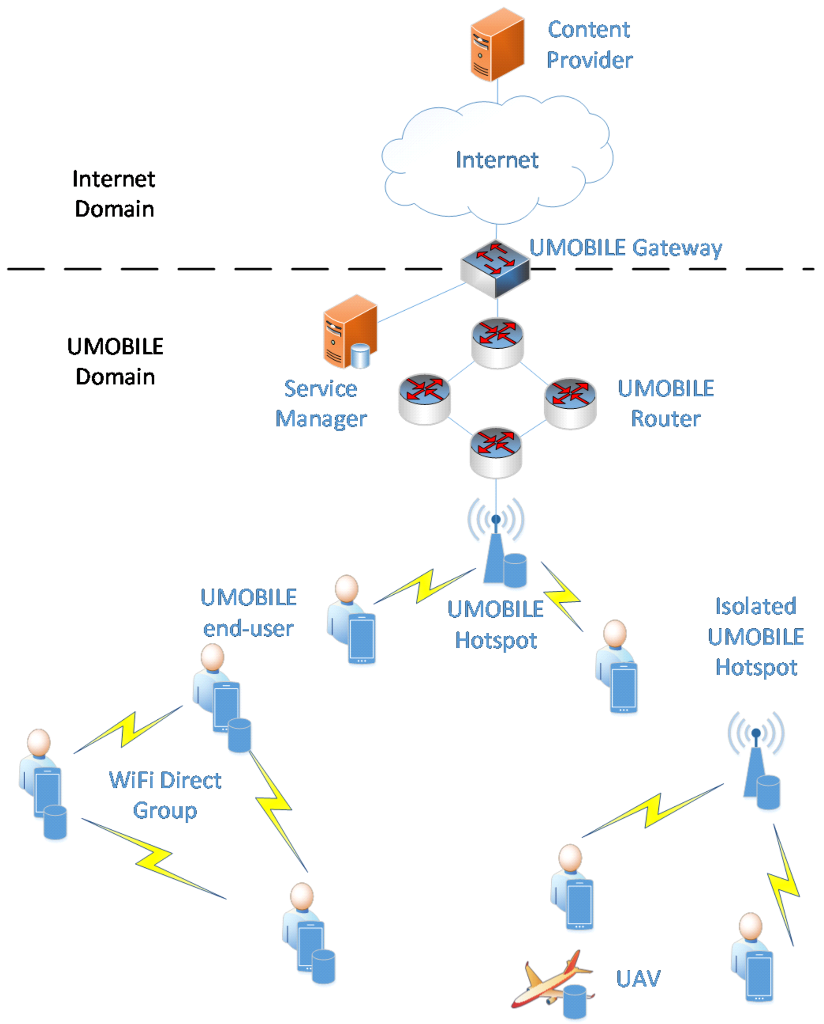


Figure 1: Overview of the UMOBILE platform

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

In deliverable D5.3, we have presented the UMOBILE architectural elements, four in total . These elements are software-based. Nonetheless, we contemplated in D5.3 potential hardware adaptations also, for instance, for the case of the UMOBILE-enabled UAVs and others, such as:

- **UMOBILE-enabled end-user devices** (i.e., smartphone, tablet), used to send and receive participatory data (e.g., photos, short messages) as well as opportunistic data (e.g., atmospheric pressure, temperature, noise, roaming patterns).
- **UMOBILE-enabled hotspots** are able to collect and relay relevant information (e.g., alert messages, instructions from emergency authorities), host some instantiated services or store collected data, check its validity and perform computational functions (e.g. data fusion) to increase the value of the information to the civil authorities.
- **UMOBILE-enabled UAV devices** able to collect and relay relevant information and connect two isolated areas.
- **UMOBILE-enabled gateways/proxies** provide interconnectivity between UMOBILE domain and the Internet domain.

While some hardware adaptation may be considered (e.g., for the case of UAVs), UMOBILE **is being developed as a modular software architecture, where some modules may or may not reside in a specific hardware element.** From a functional point of view, we have classified the UMOBILE architecture into functional blocks, which are shown in Figure 2. Table 1 shows their current progress.

UMOBILE Element	Description/Purpose	D5.3 status	Current status
UMOBILE Gateway (1)	It works as an interface between UMOBILE networks and the Internet. It basically consists in a functionality that uploads any service to be pushed to the UMOBILE network by the service manager	Implemented	Tested for file retrieval services
UMOBILE Service Manager (2)	It supports the deployment of services (eg. web services) that demand different levels	Partially implemented the following functionalities: -Integration with DTN.	1) Implemented and comprehensively tested the following functionalities:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

	QoS (e.g., less-than-best-effort, best-effort and premium) regardless of network availability. For instance, it is capable of making services available in areas suffering from intermittent connectivity and network partitions.	-Identification and evaluation (in laboratory settings)of the critical parameters that determine exhaustion of Raspberry Pi resources.	-Service controller. -Monitoring manager. -Service repository. -Push/Pull communication. 2) Evaluated the performance in a deployment on a real network (as opposed to laboratory deployment). 3) Implemented, tested and demonstrated the integration with DTN at: -Brussel Mar 2017 project review. -ICN'17 demo, Berlin. 4) Currently under additional (more demanding) testing and refinement to meet the requirements of the final demo.
UMOBILE End-User Service (3)	Access to native UMOBILE apps and to needed (background) services, such as contextual-based routing; support for NDN in opportunistic environments (NDN-Opp)	Demonstrated with NDN-Opp and PML - planned to include the following services: NDN-Opp Contextual Manager NREP KEBAPP	Integrates the following services: - NDN-Opp - Contextual Manager Connects to the following native apps: - Oi! - Now@ - PML - Emergency information service
UMOBILE HOTSPOT (4)	It has communication, storage and computation facilities. It provides users with network access to the UMOBILE domain and indirectly, to the conventional Internet. It is capable of accepting the deployment of services (e.g., web	Partially implemented the following functionalities: - Integration with DTN. -Identification and evaluation (in laboratory settings)of the critical parameters that determine exhaustion of Raspberry Pi resources.	1) Implemented and comprehensively tested the following functionalities: -Service Execution -Monitoring Agent -Push/Pull communication. 2) Evaluated the performance in a deployment on a real network (as opposed to

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

	services) and running them locally (with or without support from the main network) for the benefit of end-users.		laboratory deployment). 3) Implemented tested and demonstrated the integration with DTN at: -Brussels Mar 2017, project review. -ICN'17 demo, Berlin. 4) Currently under additional (more demanding) testing and refinement to meet the requirements of the final demo.
UMOBILE APPS (5)	Native UMOBILE Apps	Oi! - Instant messenger, demonstrated Now@ - push content planned Route Planner - demonstrated PML demonstrated	- Oi! - updated - Now@ - PML demonstrated - Emergency information service

Table 1: Functional blocks of UMOBILE architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

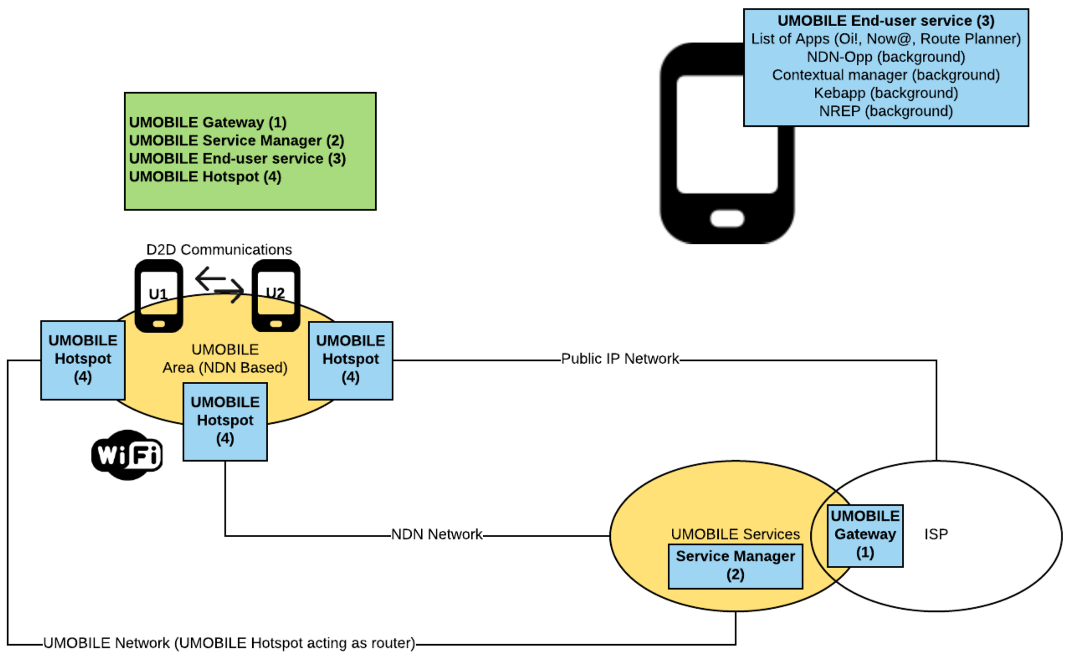


Figure 2: Functional blocks of the UMOBILE platform

The following sections describe the progress of the functional components provided in Table 1, in more detail focusing on the interaction among modules. Please refer to D.5.1 “Validation methodology and evaluation report” for a detailed description and validation of each of the components.

2.1 UMOBILE Gateway

The UMOBILE Gateway provides interconnectivity between the UMOBILE domain and the Internet domain. Such devices can be employed by service and content providers to act as repositories. They are able to store data received through the IP network and then to share it over the UMOBILE network (or vice-versa) upon request. The focus of the UMOBILE project is on service and content sharing over the UMOBILE network.

UMOBILE Gateways can be part of the infrastructure of service/content providers or civil authorities, being employed as repositories supporting both the IP and the UMOBILE part of the network. In particular, providers can utilize UMOBILE Gateways as “entry point” of the UMOBILE network, connecting their legacy IP-based infrastructure with other UMOBILE nodes, as depicted in Figure 2. This point of entry is normally expected to reside in the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

provider's premises. Depending on the deployment model, though, any UMOBILE hotspot can act as Gateway, if it is equipped with an IP interface and has sufficient storage and processing power.

The gateway assumes its role by providing universal access to content or services located in both the host-centric and information-centric domain. For example, the image of a service stored in the IP domain can be "fetched" by the UMOBILE gateway – with the help of the Service Manager – and stored in a service repository located in the UMOBILE part of the network. Gateway functionalities are central to the service migration platform that the UMOBILE project has implemented: it is the means of sharing services and information between the UMOBILE and IP domains.

The gateway can be implemented as an independent UMOBILE node, as such, it is deployed with and runs the UMOBILE platform shown in Figure 3. Consequently, if required, the gateway is capable of forwarding data over the DTN interface. Alternatively, gateway functionalities can be implemented in the UMOBILE Hotspots.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

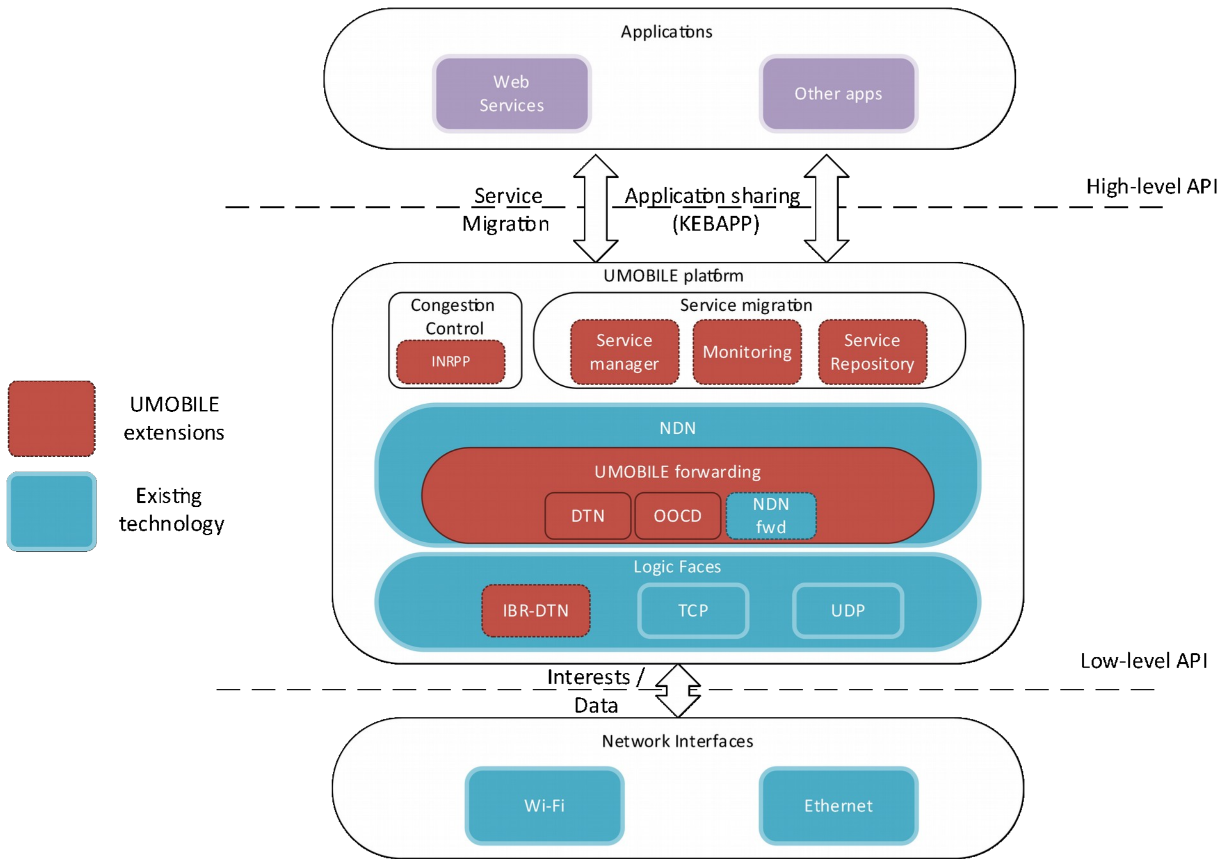


Figure 3: UMOBILE architecture as deployed in a UMOBILE Gateway

2.2 Service manager

A central aim of the UMOBILE project is to build a service-centric architecture that is capable of supporting the deployment of a diverse set of services with different QoS requirements ranging from best—effort to guaranteed QoS with different degrees of stringency. We address the challenge by means of integrating the abstractions natively provided by the ICN paradigm, Delay Tolerant Network (DTN) techniques and opportunistic service migration to the edge of the network. In pursuit of this aim, we have implemented three technologies that can operate either individually or integrated:

- A Service migration platform
- A DTN tunneling framework
- KEBAPP (Keyword-Based Mobile Application Sharing).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

The details of these three technologies are described in D3.4 “UMOBILE ICN layer abstraction final specification”; we now focus on the Service Manager, which is one the devices we can identify in the UMOBILE architecture. The role of the Service Manager within the UMOBILE architecture is depicted in Figure 4. It shows its relationship with the Service Migration Platform, the DTN tunnelling framework and KEBAPP.

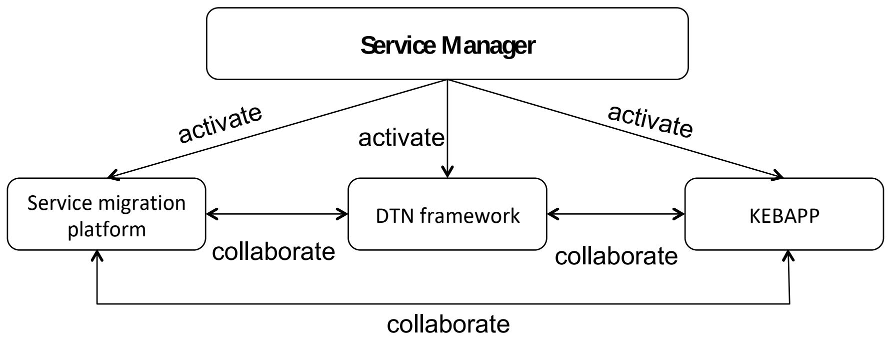


Figure 4: Relationship of the Service Manager with Service Migration Platform, DTN framework and KEBAPP

As shown in the Figure 4 and discussed at large in Section 4.1.5.1, the Service Manager is in charge and can activate each of the mechanisms to work individually or in collaboration to meet QoS requirements.

A detailed discussion of service migration, and the role of service manager in the UMOBILE architecture, is presented in D3.2 “UMOBILE architecture report (2)”. In this section, we will focus on its integration with DTN and KEBAPP.

2.2.1.Integration of the service migration platform with the DTN framework

The integration of the service migration platform with the DTN framework can help to deploy services in an area with no network connection either because it has been impacted by a network partition or because it has been neglected from network services. The service migration platform can be integrated with the DTN framework to mask network problems to honor QoS. In the following discussion we will focus on resilience which is one of the central requirements of POC1. As discussed in Section 4.2 of D5.3[D5.3], service migration is

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

expected to help in the deployment of an emergency service (map services) is an area with no communication services.

We have made significant progress in this direction. We have presented a demo at the ACM ICN 2017 conference[ICN2017Demo]. In this demo, we present a NDN-based approach to deploy a dockerised services closer to end-users located in a network section impacted by a network partition event. In this situation, we use a DTN-enabled node to tunnel traffic between two physically disconnected nodes. This is a pragmatic approach to increase resilience.

The scenario of the ACM ICN 2017 is depicted in Figure 5, where HS stands for Hotspot. We assume that HS1 is at the edge of the main network and that the disaster area network is miles away and disconnected. The aim is to retrieve a service (S) from the Main Network and deploy it in HS2 located in the Disaster area. We assume S to be a stateless service, e.g., a self-contained web server. The image of the service is available from[5].

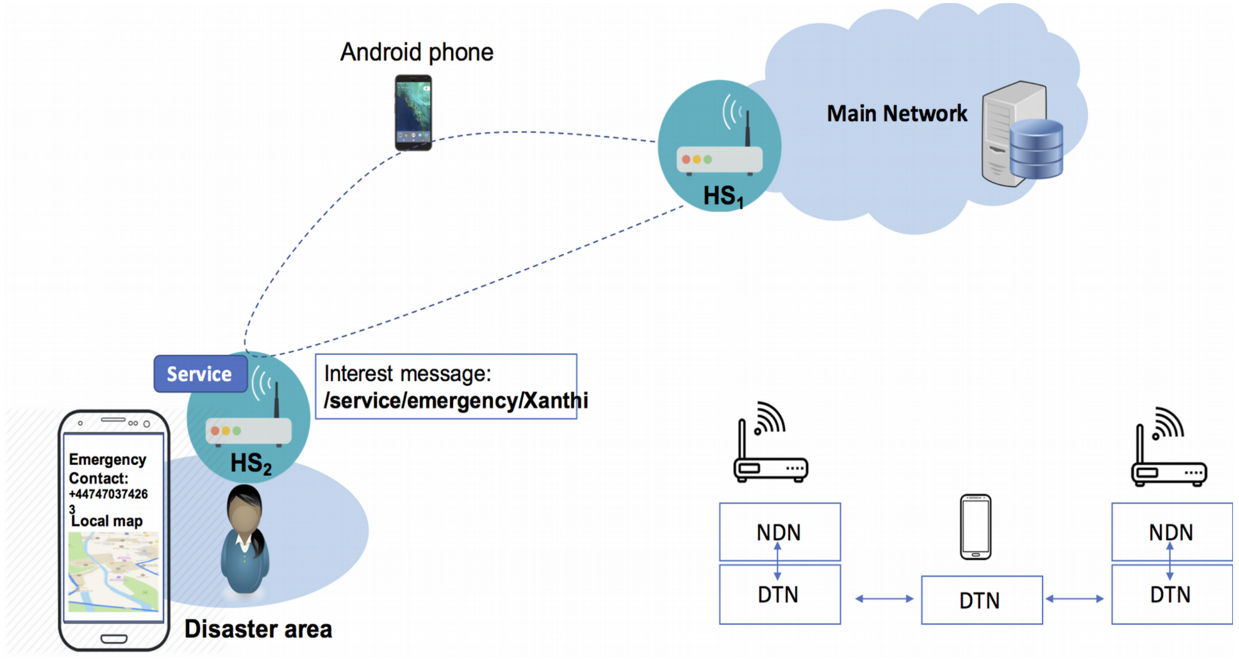


Figure 5: Demonstrating service migration scenario in challenging environments

Assumptions:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

The Android phone is a physically mobile DTN-enabled node that can travel backwards and forwards between HS2 and HS1 in a manner that when it can communicate with HS2 it cannot communicate with HS1 and vice versa.

IBR-DTN is running on all intermediate mobile devices.

Solution:

The DTN face uses the IBR-DTN implementation to forward bundles between the nodes.

Configuration:

1. On nodes running the NDN-DTN stack, the DTN daemon (dtnd) needs to be started first – separately from NFD. This is because the DTN face is created on NFD startup. The DTN daemon can be started by *dtnd -c [configuration file]* command.
2. When NDF is started one needs to manually register a FIB entry for a remote NDN-DTN node using the command:

   nfdc register [-I] [-C] [-c <cost>] <prefix> <faceId | faceUri>

   For example, to register a route for prefixes */umobile/dtntest* towards the remote NDN-DTN node *umobile2*, one can use following command:

   nfdc register /umobile/dtntest dtn://umobile2/nfd
3. Once the DTN and NFD daemons have been started on all nodes of interest, and it is made sure that the remote NFDs are reachable via their DTN interfaces (possibly by registering any remote prefixes), the experiment can be started.

Experiment procedure:

1) An Interest request is initially constructed by HS2, including the name of the desired service (S). The location of the selected area is embedded into the Interest name (/service/emergency/Xanthi).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

2) The Interest is forwarded to the DTN face when the Android phone becomes wirelessly reachable to HS2. The Interest is encapsulated in a DTN bundle and stored in the phone's persistent storage.

3) The phone loses contact with HS2 when it travels towards HS1. When it reaches HS1 the Interest is decapsulated and delivered to the NDN layer.

4) The Interest is transferred by HS1 through the main network, towards the service producer or the nearest cache.

5) The latter or another intermediate NDN node in possession of S retrieves it and prepares a service image with customized information (i.e., emergency contact of local civil protection authority or map in Xanthi).

6) The reply includes one or more Data chunks sent along a reverse path using the DTN face. This implies that the sequence of connections and disconnections explained above is executed one or more time, depending on the size (number of data chunks) of the image of the service.

7) When HS2 receives all the chunks of S, it calls a service execution function of the service migration platform to execute S to provide the emergency service.

The significant of the demo of Figure 5 is that it will play a central role in the demonstration of POC1. To asure that the integration of the service migration platform and the DTN framework will work as expected, we would like to replicate the experiment of Figure 5 remotely using the facilities offered by the UMOBILE lab (see Figure 19 of D5.3) before the POC1 demonstration. The main difficult that a potential remote replication involves is the physical manipulation of the Android phone, because of this, we might rule this intention out and take advantage of the UMOBILE lab in experiements that do not require physical manipulation of devices.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

2.2.2.Integration of the service migration platform with KEBAPP

KEBAPP is an application-centric framework for opportunistic computing at the edge of the network on mobile devices such as smartphones and tablets. It allows a mobile device to exchange information, in an opportunistic way, using smartphone apps, locally, with other devices that happen to be in that area. By locally we mean without involving communication with the global Internet. Examples of information that can be exchanged by KEBAPP-enabled devices are traffic problems, shopping opportunities in the area, lost-and-found articles, etc.

To be able to participate in a KEBAPP group, a mobile device needs the KEBAPP framework included in the UMOBILE end-user service (presented as an apk file) and a KEBAPP-enabled application.

A KEBAPP group can be a set of users sharing the same application that want to locally communicate to other users to share content and/or computation resources. For example, a KEBAPP-enabled application can be a Route-Planner application, able to calculate routes for other users that do not have the information necessary to calculate those routes or do not have connection to Internet. Another example could be a concert scenario, where a group of users can share pictures of the event using the same application. However, in all these examples, some problems may arise when a set of users are connected using Wi-Fi Direct without any participation of the infrastructure, such as the following.

- Battery: Wi-Fi Direct communications can waste smartphones battery, especially for the group owner (the leader that manages the Wi-Fi Direct group).
- Intermittent connectivity: Users' mobility can generate several disconnections, and therefore instability in the communications or broken messages, especially when the group owner leaves the group that implies a disconnection of the entire group.
- Limited resources: Caching and processing capabilities in smartphones are more than enough; however, users may rather avoid sharing smartphone resources with other users, such as local storage, data plans or other resources.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

For all these reasons, we think deploying KEBAPP-enabled services in UMOBILE hotspots can have benefits, in order to centralize communications between users without resource limitations and providing more stable communications.

2.2.2.1 Service migration facilities

Let us assume that the provider of the ICN infrastructure of Figure 6 has been delegated the responsibility of deploying a KEBAPP-enabled service (we consider a UMOBILE store as a KEBAPP-enabled service as well) and imagine the following situation.

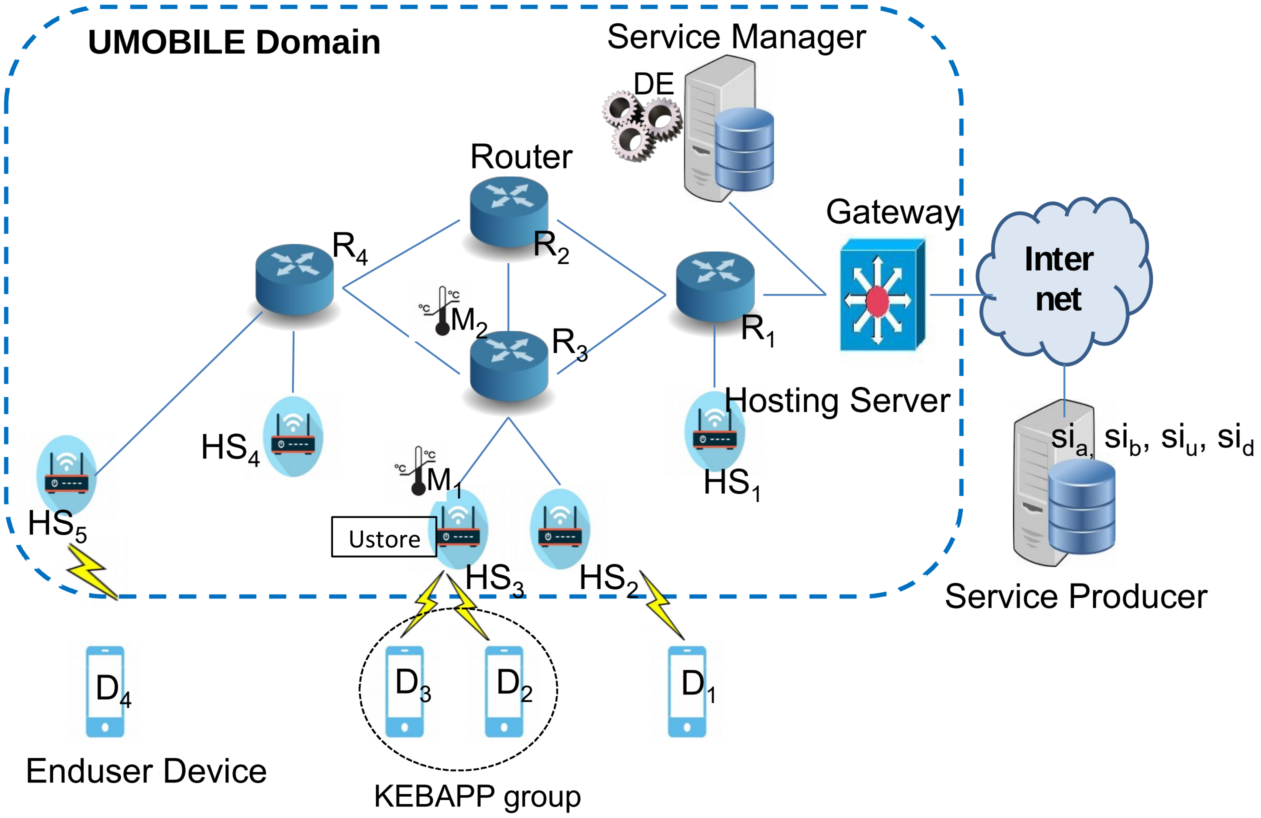


Figure 6: Integration of service migration and KEBAPP

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

1. The KEBAPP-enabled service has been dockerized and stored as a compressed image, say siK in the Service Producer from where the Service manager can retrieve it when needed.
2. D2 issues a request against the Service Manager to expressing interest in the deployment of KEBAPP. Let us assume that D2 has access to HS3, HS2 and HS1.
3. Upon receiving the request, the Service Manager instructs his Decision Engine to deploy siK as close as possible to D2 but under the consideration of the current network conditions, the features (disk, memory and CPU capacity) of the potential Hotspots (HS3, HS2 and HS1) and their current status such as currently available memory, CPU load and number of Docker containers hosted. The idea is to verify that the selected Hotspot has enough resources to run the KEBAPP-enabled service.
4. To make informative decisions, the decision engine relies on up to date information collected from several sources such as network monitors and actual Hotspots. Of central interest are parameters related to QoS. For instance, a Hotspot will be selected by the decision engine when certain conditions hold, for example, when Round Trip Time is above the acceptable level, memory usage is above 85% and cpu load less thant 70%.

2.2.2.2 Service deployment technology

The decision engine collects memory usage data by means of pull requests. Upon a successful migration, the selected UMOBILE hotspots are able to serve the KEBAPP-enabled service locally. This service migration process will run over NDN and use both push and pull communication models.

The aim is to demonstrate how the service migration platform can be used to deploy a KEBAPP-enabled service at the edge of the UMOBILE platform, for example in HS3, HS2 or HS1 on the basis of the reports sent to the decision engine by the resource consumption monitors deployed in HS3, HS2 or HS1. We can describe the operation flowchart in the following way:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

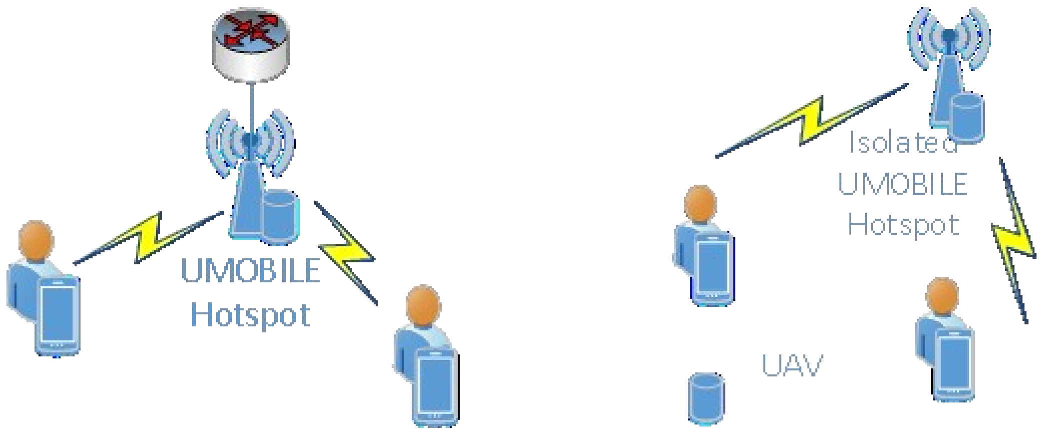
1. Deploy monitors (Python or shell scripts) in HS3, HS2 and HS1 to collect metrics about the status of their CPU memory and disk resources. Measured metrics are sent to the decision engine.
2. Use tools (Python or shell scripts) to enable D3 to place requests against the Service Manager to deploy KEBAPP-enabled service and to process the request file as soon as it becomes available. D3 awaits for a response.
3. The decision engine will deploy the service in HS3 as long as HS3 has enough resources to host it.
4. D3 request should be satisfied.
5. Use tools (Python or shell scripts) to artificially manipulate the CPU, memory and disk consumption of HS1, HS2 and HS3. For example, drive the resources of HS1 and HS2 to exhaustion and instruct D3 to place requests as in point 2.
6. Verify that the decision engine is capable of deploying the service in a Hotspot with enough resources. For example, the decision engine never selects a Hotspot with 75% of its memory consumed.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

2.3 UMOBILE Hotspot

Typically, wireless (or Wi-Fi) hotspots are essentially wireless access points providing network and/or Internet access to mobile end-user devices, e.g., in public locations. UMOBILE-enabled hotspots are specific UMOBILE network devices, like usual hotspots, but they support the UMOBILE architecture, can run services locally and are compatible with the UMOBILE services.

UMOBILE-enabled hotspots may be able to collect and relay relevant information (e.g., alert messages, instructions from emergency authorities), host some instantiated services or store collected data, check its validity and perform computational functions (e.g., data fusion) to increase the value of the information to the civil authorities.



a) UMOBILE connected hotspot b) UMOBILE isolated hotspot

Figure 7: UMOBILE hotspot

The specific characteristics of the UMOBILE-enabled hotspot (UMOBILE AP) are the following:

- UMOBILE hotspots can be isolated (not connected to the Internet) or connected to Internet.
- UMOBILE hotspots can host local services deployed using the service migration platform.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

- UMOBILE hotspots can provide KEBAPP-enabled services that UMOBILE users are not able to provide due to network restrictions, data-plan restrictions or battery restrictions.
- UMOBILE hotspots can support DTN, through IBR-DTN, and can integrate service migration.
- UMOBILE hotspots can be deployed in isolated UAVs, providing local services and DTN capabilities, or in connected UAVs (through a data uplink), providing connectivity services.
- UMOBILE hotspots can be compatible with NREP in order to prioritize emergency services and messages.
- UMOBILE hotspots can gather social and context information that will be later used by the NDN-Opp and/or PerSense.
- UMOBILE hotspots can be collocated with gateway functionalities in order to provide IP network services to the local opportunistic network. E.g. through KEBAPP Services (e.g. map service) to UMOBILE network (gateway function).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

2.4 UMOBILE End-User Service

The UMOBILE End-User Service (UES)[1] is introduced in this report as an application that assists the end-user in getting UMOBILE support in a user-friendly way. For that purpose, we have developed an application (for the proof-of-concept, in Android) which the user can rely upon to seamlessly benefit from UMOBILE, and which is illustrated in Figure 8. As illustrated, the UES gives access to UMOBILE native applications, as well as to UMOBILE (background services). The user does not access the services directly. These are activated via the selected applications. For instance, if a user selects the instant messenger app Oi! or the data sharing app Now@, then the services “Contextualization” and “Direct Communication” (implemented by NDN-OPP) become active and that will be visible for the user.

1 The UES is available via GitHub at: https://github.com/Senception/UMOBILE_UES

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

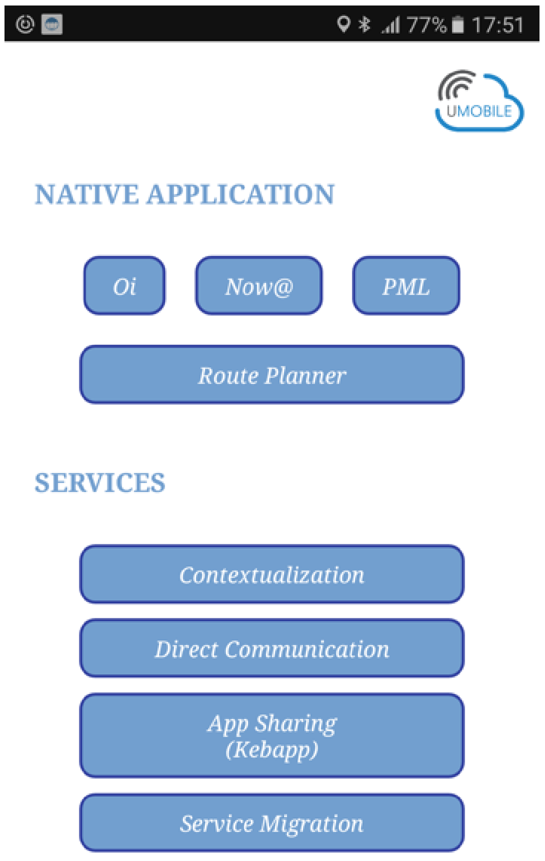


Figure 8: UES screenshot.

Currently being developed (proof-of-concept) for Android, the UES is a binary that is downloaded, e.g., from a UMOBILE hotspot. The purpose is to allow the end-user to have access to UMOBILE, even if Internet access is intermittent.

2.4.1.Supported Network Services

The following services are currently being called via the UES:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

- **NDN-Opp**. A new branch of the original NDN forwarding daemon, which assists one hop as well as multihop wireless communication. At the current stage, NDN-Opp [7] is able of offering NDN communications between intermittently connected wireless devices based on the following innovation:
  - OPPFaces: A novel face definition to allow mobile devices to exchange data directly over Wi-Fi direct. NDN-OPP creates an OPPFace for each Wi-Fi direct neighbour. Each OPPFace encompasses a data queue, which is served everytime the defined neighbout is in wireless range.
  - Connection and connectionless communication modes: OFFFaces can be served in a connection mode, via the TCP connection stablished with the Wi-Fi direct group owner, which will then relay data to the proper neighbour. This mode of communication is mainly used for large data objects. OPPFace queues can also be served in a connectionless mode, in which data is transferred directly between neighbour nodes during the Wi-Fi direct discovery phase. The connectionless mode is used for the fast dispatch of short (emergency) data objects.
  - Multi-homing management: in which an NDN-OPP mobile device is able of exploiting not only a set of Wi-Fi direct OPPFaces towards other mobile devices, but also Wi-Fi infrastructure face. The latter is used opportunistically to increase probability of delivery in a local communication scenario, and is also used to allow long range communication between NDN-OPP devices located in different wireless networks (which communicate via a core NDN network).
  - A push communication model, allowing data to be pushed to a specific destination. This communication model aims to support emergency services which require a device to send information towards a specific destination (e.g. authority) without waiting for the latter to generate a continuous flow of Interest packets. Currently the Oi! app uses the push communication model in order to implement a short message service.

  Currently data is forwarded based on a broadcast scheme, as described in the NDN framework. For the final demo, NDN-OPP will encompass a Name-prefix State protocol with Selective Information Diffusion (DABBER), in order to save resources by avoiding wireless broadcast. Such protocol is being implemented as an extension of the NLSR protocol to allow:

  - Multi-path routing combined with adaptive forwarding in wireless environments;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

- ○ Awareness of the context of the mobile device, via information collected from the Contextual Manger.
- ○ Local dissemination and computation of Name LSAs;
- ○ Selective dissemination of LSAs between (N-x) neighbours;

The complete description of the routing protocol will be made available via an Internet draft entitiled “Information-centric Routing for Opportunistic Networking Environments” (draft-mendes-icnrg-dagger-00.txt) to be submitted to the ICN Research Group of IRTF.

- **Contextual Manager**[2]. Specified in Deliverable D4.5, the Contextual Manager is a UMOBILE service that runs in the background of end-user devices, and that captures information concerning the device affinity network (roaming patterns and peers over time and space) as well as concerning usage habits and interests (internal device information). At the current stage, the Contextual Manager is under development, and available code is already provided to registered users, via GitHub or GitLab (LGPLv3.0).
- Kebapp: KEBAPP is an application-centric framework for opportunistic computing at the edge of the network on mobile devices that allows to exchange information, in an opportunistic way, using smartphone apps, locally, with other devices that happen to be in that area.

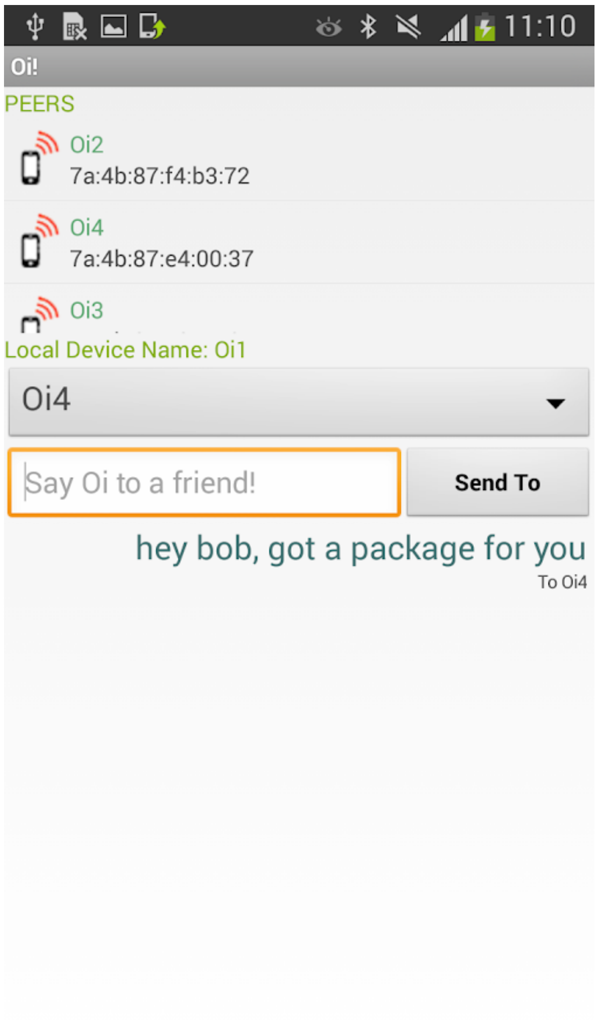
2.4.2.Native Applications

UMOBILE currently integrates the following applications:

- OI!application [4]: Oi! (which stands for "Hi!" in Portuguese) is an Android application for instant messaging based on a push communication model implemented by NDN-OPP. Due to this, Oi! can be used in places where internet access is intermittent. The Oi! application is currently being exploited to allow users to communicate in emergency situations, based on a predefined name prefix.

2 Code available via GitHub at https://github.com/UMOBILESenception/ContextualManager as well as via GitLab at https://gitlab.com/UMOBILESenception/ContextualManager.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124



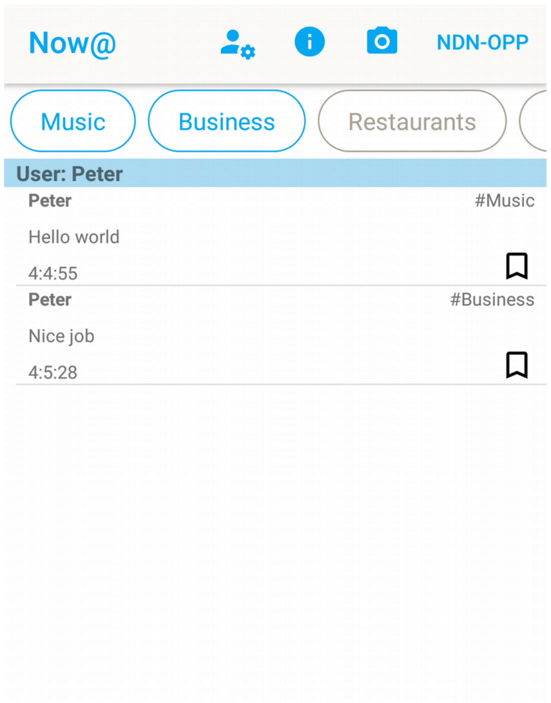
hey bob, got a package for you
To Oi4

Figure 9: Layout of the Oi! Application (V0.9)

- Now@ [8]: Now@ is an Android application for content sharing (text, documents, photos) over intermittent Internet access. Now@ current version relies on Chronosync. Now@ can run on top of NDN-OPP which means that data is then shared via Wi-Fi Direct or Wi-Fi connections, or on top of the original NDN Forwarding Daemon (NFD) for Android. Now@ allows users to exchange information by using predefined categories that help them to define the interests they want to communicate about. To do this, we use ChronoSync [9] to carry out the transfer and synchronization data between each of the users that uses the application even in condition without Internet connectivity. In contrast with applications like

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

ChronoShare and others which also work on top of ChronoSync, Now@ allows users to subscribe to more than one interest at the same time.



Peter #Music
Hello world
4:4:55

Peter #Business
Nice job
4:5:28

Figure 10: Layout of the Now@ Application (V0.9)

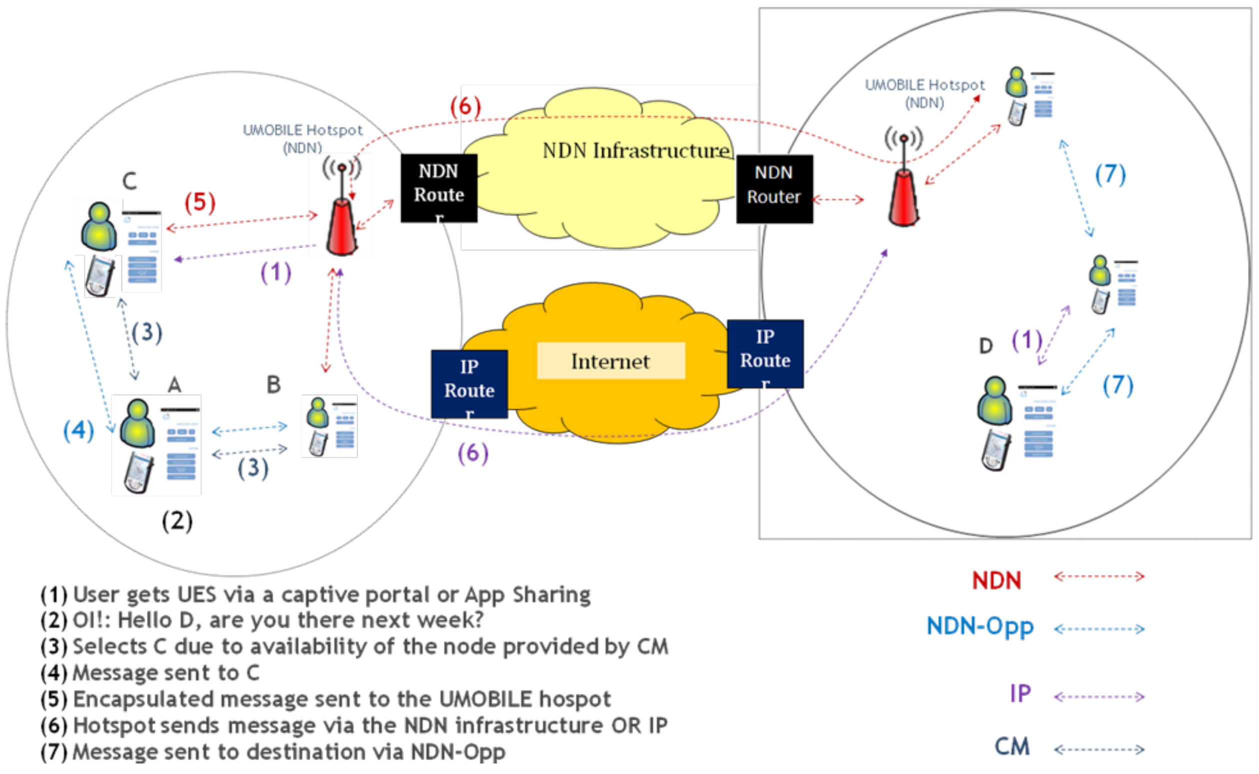
- PML, captures data concerning visited networks and peers around, generating daily reports and being able to send them to users.
- Routeplanner: Route calculator being able to calculate routes for other users using KEBAPP framework.
- Emergency information service: Emergency app that uses KEBAPP to discover and exchange emergency information (e.g. video with instructions or maps with safe paths) that can run either in smartphones but also in the UMOBILE hotspot.

2.4.3.Operation Scheme

Figure 11 provides the communication scheme for the UMOBILE UES, focusing on a micro-blogging scenario, where User A wants to send a message to User D. User A is in Lisbon, while User D is in Italy. User A is walking around in a city, and when passing via a UMOBILE hotspot, the user may get access to the UES proposed to be installed via a captive portal mechanism, in case it does not have the UES installed yet. (1). Hence, at this stage, the communication is performed via IP.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

User A then decides to send an instant message to his friend B, by selecting Oi!. A selection of this app implies that two networking services become active: NDN-Opp, and CM. The message forwarding is performed via contextual-based opportunistic routing, with NDN. This routing solution, currently being developed in UMOBILE, corresponds to an extension of the NDN Linked State Routing (NLSR) protocol suitable for opportunistic environments. NLSR is the routing protocol currently available in NDN fixed environments. The DAGGER routing protocol selects potential successors based on node popularity (eigenvalue centrality) as well as based on node availability. Such costs are provided by the CM module to the routing module, upon demand or periodically (refer to D5.4 for the specific costs computed by the CM), derived from prior or current scanning (3). In the provided example, node A selects as successor C (4), given that B availability is lower (due to higher use of internal resources such as CPU or battery).



(1) User gets UES via a captive portal or App Sharing
(2) Oi!: Hello D, are you there next week?
(3) Selects C due to availability of the node provided by CM
(4) Message sent to C
(5) Encapsulated message sent to the UMOBILE hospot
(6) Hotspot sends message via the NDN infrastructure OR IP
(7) Message sent to destination via NDN-Opp

Figure 11: UMOBILE UES example

Between node A and C, the message is forwarded by relying on the contextual-based routing approach provided by DAGGER, and integrated in NDN-Opp. To forward a instant message that was not requested (no Interest packet was created) NDN-OPP supports different push

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

communication models: in the current NDN-OPP version such model is implemented by means of a different Data Packet, pData. Such packet is used when the OPPFace selected is Wi-Fi Direct based. While when node C sends the message, if such message is sent via Wi-Fi (infrastructure mode), then the pData packet is converted into a regular NDN Interest packet (5). The UMOBILE hotspot can then opt to send the packet directly via NDN, or via IP (6). The same process is processed until the message arrives to D (7).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

3. UMOBILE Lab

3.1 Description

A laboratory has been prepared to test the software that the Consortium has developed; it is physically located within AFA Systems' premises (in Termoli – Italy) and is named the UMOBILE Lab or the Lab, in short.

The Lab is already a part of the NDN-testbed (https://named-data.net/ndn-testbed/); the Consortium is now evaluating the opportunity to participate to other federations and networks of research labs (e.g. the 'PlanetLab' and the 'OneLab').

The UMOBILE Lab has been in operation since May 2016 and follows the project evolution in its configuration. For example, UMOBILE Network Controller (UNC1) Server has been added to implement the Service Controller operated through the Service Execution Gateway (SEG) devices.

Currently, the Lab includes a number of devices as Wi-Fi access points, Linux systems (Raspberry PI) and Android systems (Banana PI). As it will be explained at large in a subsequent paragraph, remote access to the lab can be gained through VPN connections.

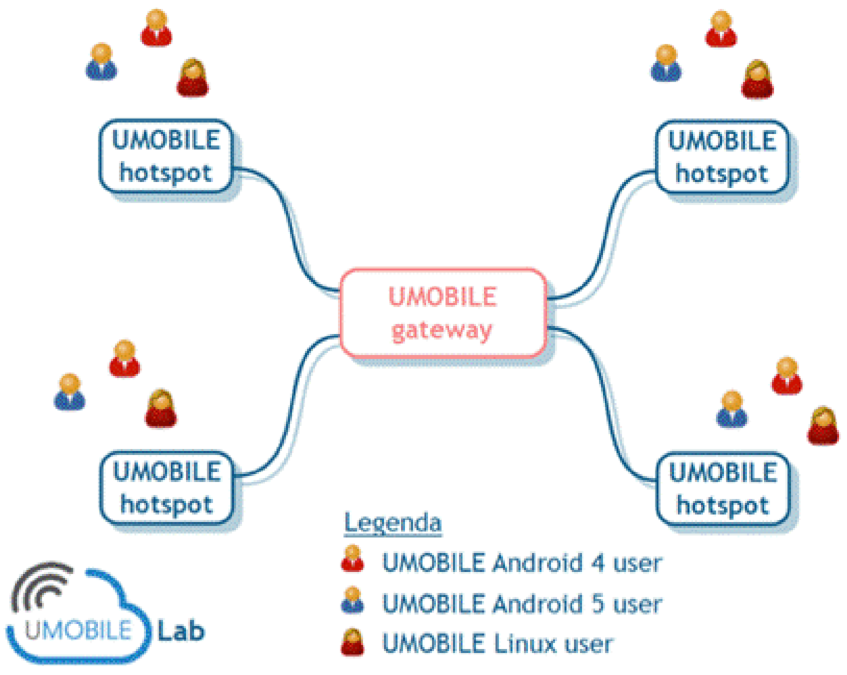
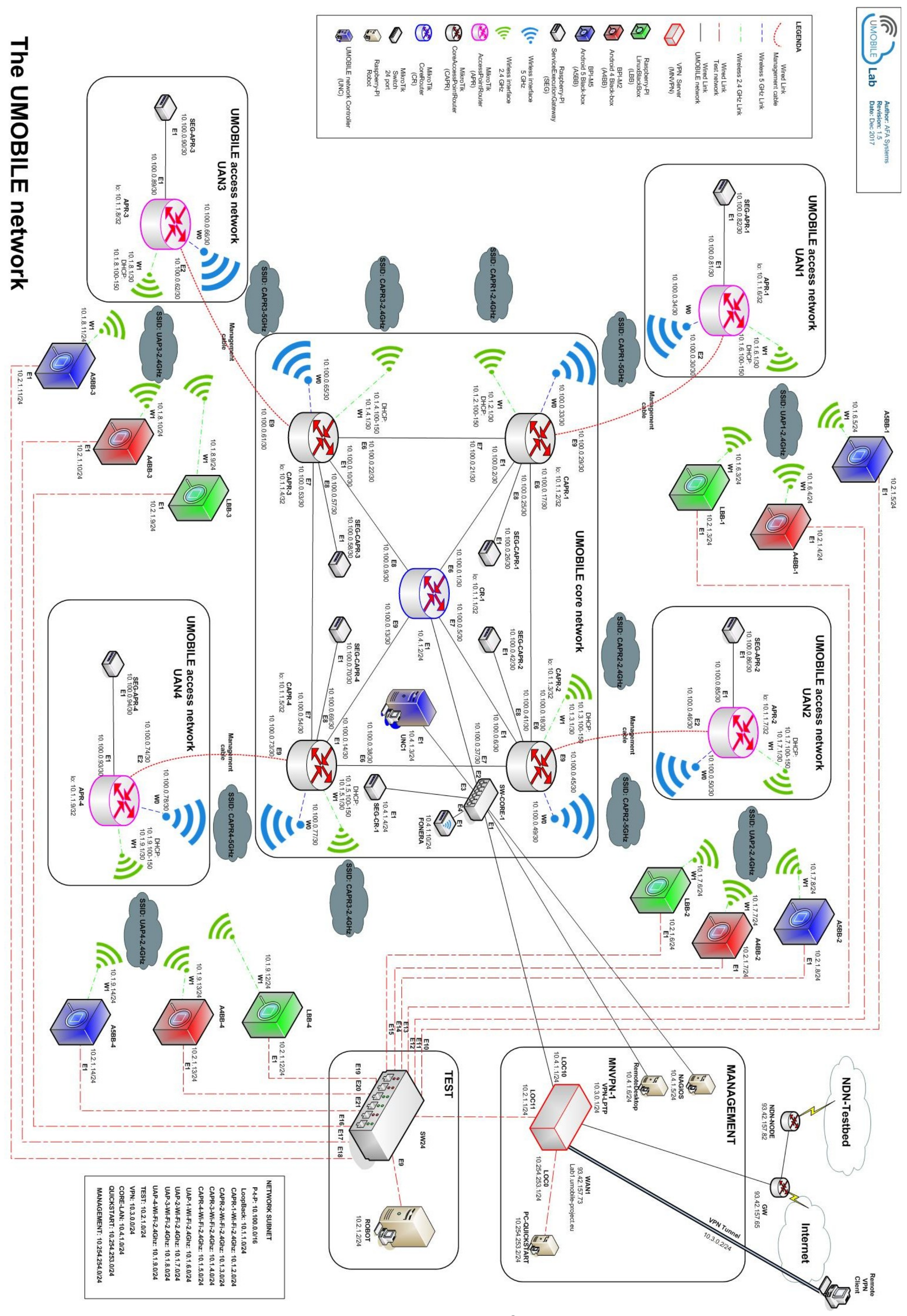


Figure 12: High level view of UMOBILE lab

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124



NETWORK SUBNET
P-t-P: 10.100.0.0/16
LoopBack: 10.1.1.0/24
CAPR-1-Wi-Fi-2.4Ghz: 10.1.2.0/24
CAPR-2-Wi-Fi-2.4Ghz: 10.1.3.0/24
CAPR-3-Wi-Fi-2.4Ghz: 10.1.4.0/24
CAPR-4-Wi-Fi-2.4Ghz: 10.1.5.0/24
UAP-1-Wi-Fi-2.4Ghz: 10.1.6.0/24
UAP-2-Wi-Fi-2.4Ghz: 10.1.7.0/24
UAP-3-Wi-Fi-2.4Ghz: 10.1.8.0/24
UAP-4-Wi-Fi-2.4Ghz: 10.1.9.0/24
TEST: 10.2.1.0/24
VPN: 10.3.0.0/24
CORE-LAN: 10.4.1.0/24
QUICKSTART: 10.254.253.0/24
MANAGEMENT: 10.254.254.0/24

Figure 13: Detailed architecture of the UMOBILE Lab

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

The Lab is meant to be used remotely by project partners and, upon request approved by the project PI (vtsaousi@ee.duth.gr), by other members of the general public such as researchers, sponsors, reviewers and industries. As such, we will keep it available beyond the completion of the project for as long as there is interest in the services that it provides or we run out of resources to maintain it. Figure 13 expands Figure 12 and shows the communication and computation components of the UMOBILE Lab.

To appreciate its physical realisation, it is worth examining Figure 14 which shows a photo of the UMOBILE Lab as it is in Dec 2017; a red circle hightlights the introduction of the Fonera access point in the Lab. The new link to the NDN-Testbed is shown in the right-upper corner.

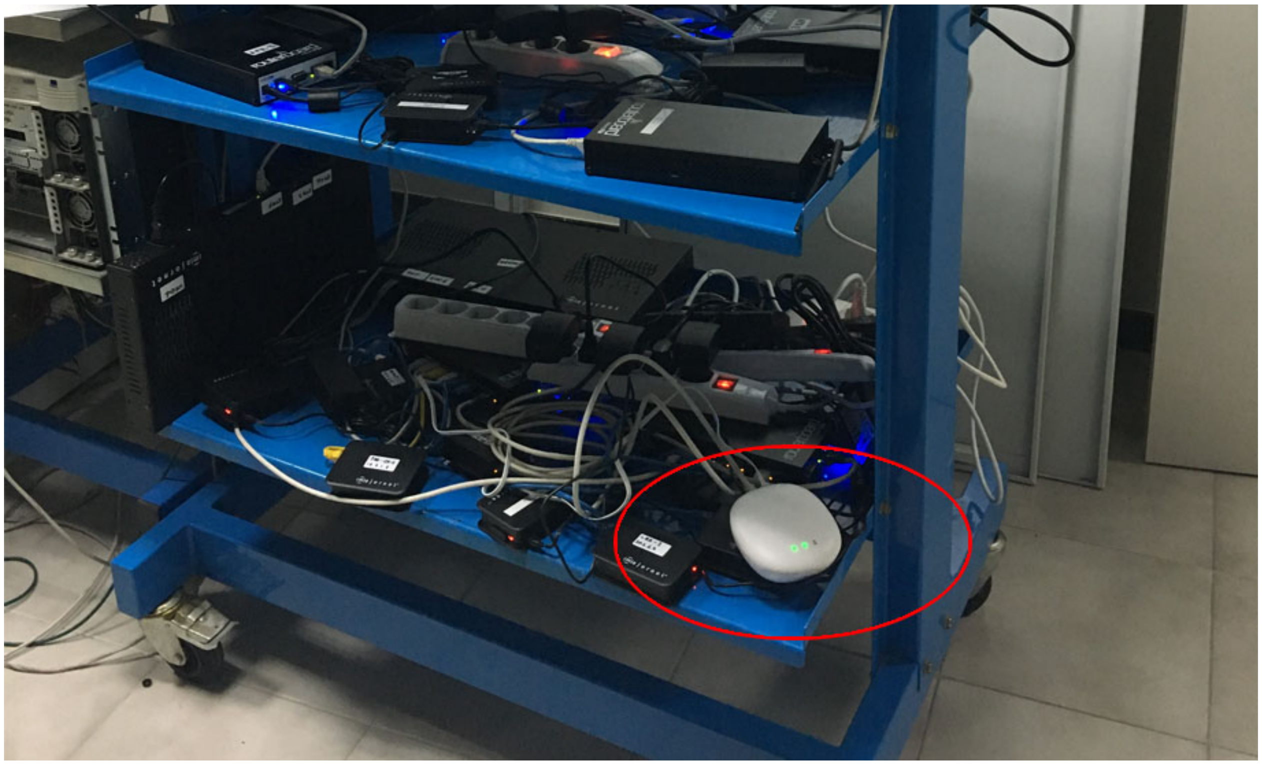


Figure 14: A Fonera device in the Lab

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

4. Proof of Concept

We have selected some specific use-cases identified in the WP2 for the purpose of feature demonstration. More specifically, we focus on two demonstrations: the first one covers both the emergency and the civil protection scenarios, and the second demonstration targets the service announcement and social routine scenarios.

The demonstration of the performance and efficiency of UMOBILE architecture can be partially conducted within the Lab.

In order to get a better understanding of the two POCs defined in UMOBILE, we use a fixed schema to describe the different aspects to take into account. Figure 15 depicts a mind map with all the concepts involved in the POC sections. A brief explanation follows.

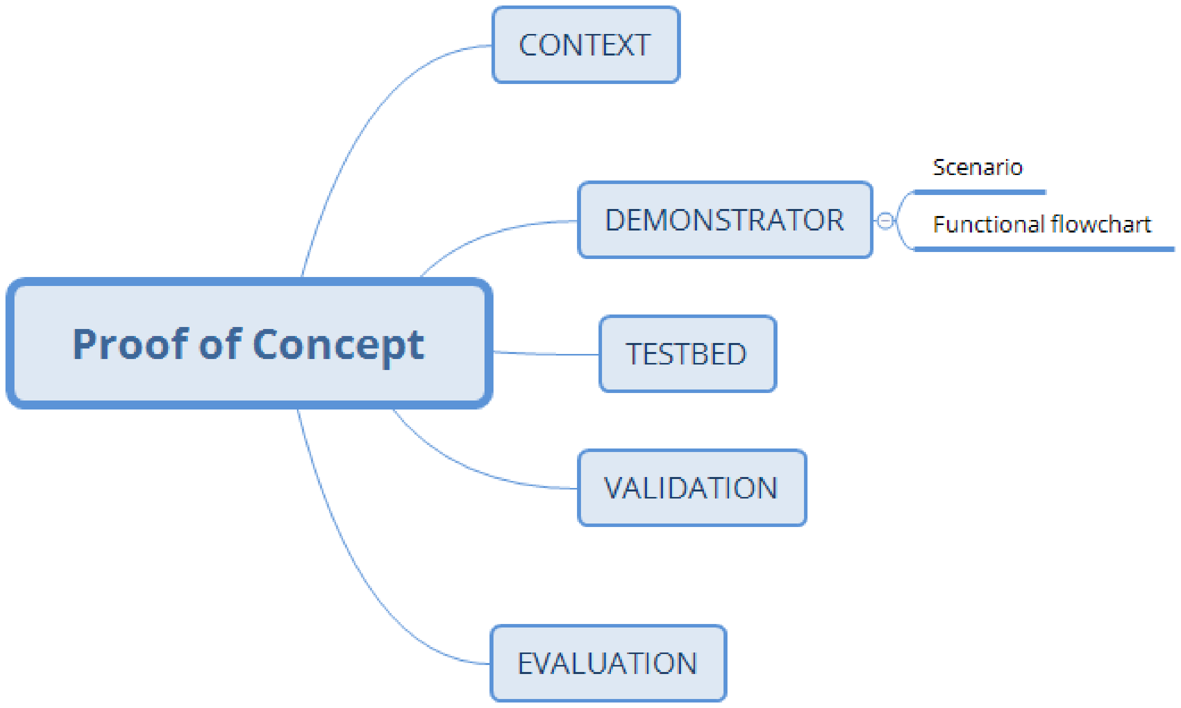


Figure 15: Proof of Concept schema

CONTEXT: The context section provides a general overview of the proof of concept.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

DEMONSTRATOR: The demonstrator is a description of the identified use case. The **scenario** describes the story line of the demo; the definition of the functional flowchart addressed in the POC is also provided.

TESTBED: This section describes the lab configuration necessary to demonstrate the POC.

VALIDATION PLAN: The validation plan is a list of actions and activities to perform on the testbed in order to validate the POC.

EVALUATION: The evaluation refers to the technical implementation and deployment of the POC and the results and conclusions drawn from it. The evaluation proceeds through the analysis of the different UMOBILE components of the POC.

4.1 POC 1: Emergency and Civil scenario

4.1.1.Context

In the first proof of concept (POC1), we demonstrate how facilities that the UMOBILE project has added to the original NDN platform can be used to deploy services in disconnected areas. We show how the UMOBILE platform can provides convenient mechanisms to assist responsible authorities in the occurrence of challenged events. We based our arguments on the fact that in emergencies, traditional communication services such as fixed or mobile networks and local Internet access become completely or partially inoperable. In these situations, UMOBILE can assist users in disseminating emergency information directly via end-user devices as well as via the UMOBILE hotspots and UAVs.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

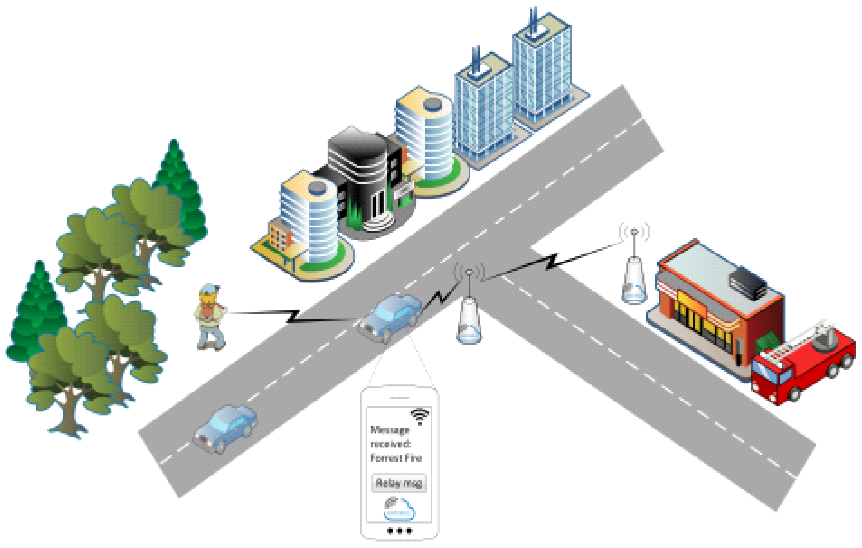


Figure 16: Emergency scenario & emergency message dissemination

4.1.2.Demonstrator

4.1.2.1 Scenario

We take the hypothetical emergency scenario documented in D2.1 “End user Requirements Report”. As illustrated in Figure 16, we imagine a **user** enjoying a day in a national forest. There is limited internet access in the area as this network topology is sparse showing participations in time and space. At some point, this person spots a fire and takes actions to alert about it. As he has no cellular coverage, the user resorts to the **Oi! app** made available in his/her mobile device when the UES was installed. The Oi! app is used to write a message, tagged as “emergency” to be sent to a authorized emergency entity. The message may includes geo-localization.

The user continues his walk in an alternative path close to main roads, where bikers and cars are passing by. Bikers, by means of the UES installed in their smartphones, will collect any emergency info by default (the message could be collected by the smatphones of a driver, driving slowly, as well). As soon as a biker has wireless connectivity, he will pass the message towards an **authorized emergency entity**, via other mobile devices, via Wi-Fi direct or through **UMOBILE HOTSPOT** via Wi-Fi.

The local authority, who also uses the Oi! app via UES, receives the message (someone in the departments is in charge of this) and sends a team of fire fighters to the location.

The rescue team equipment includes a “mobile office” which acts as a central station for the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

operators working in that area. The mobile office is equipped with a UMOBILE HOTSPOT able to create a local communication infrastructure in the area affected by the fire.

Members of the rescue team use the applications installed on their devices via UES (Oi!, Now@, Routeplanner) for communication purposes: to coordinate the operations among the operators, to share and update information with the central station.

Furthermore, they use their mobile devices to request the authority (which acts as a content provider) to deploy an emergency service in the affected area. The request reaches the authority through the central station, or even directly if the operators are equipped with satellite phones. An example of a **SERVICE** can be a web service, deployed by the Service Manager which is equipped with a Decision Engine. The Decision Engine, based on the issued requests, deploys the service in the UMOBILE Hotspot. The **image of the service can be transferred over DTN** by a biker with an Android phone, a car passing through the area, a satellite link or by other means equipped with DTN facilities.

Important messages or updates on the emergency situation (documents, photos) are provided to the citizens in that area via the Now@ application.

For external issues (e.g., flight license in a determined country/place) in this PoC1 we do not consider the use of UAVs as data mules in order to forward alert messages or to migrate images of services. In Section 4.3 we discuss an extension of PoC1 where we resort to UAVs to address lack of communication problems. We explain some experiments that we are conducting to validate the applicability of UAVs in terms of range, throughput and latency.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

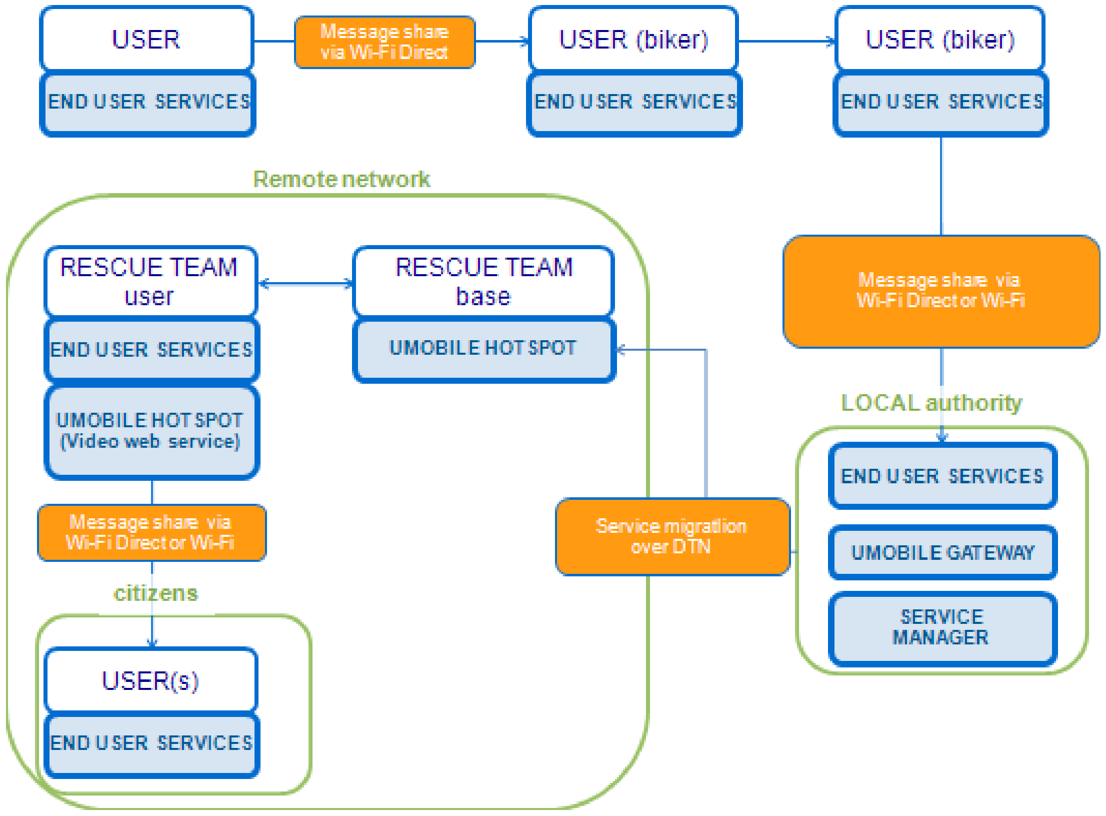


Figure 17: High-level flowchart of the first Proof of concept

4.1.2.2 Functional flowchart

From a functional point of view, the defined scenario can be mapped into the flowchart described in Figure 18.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

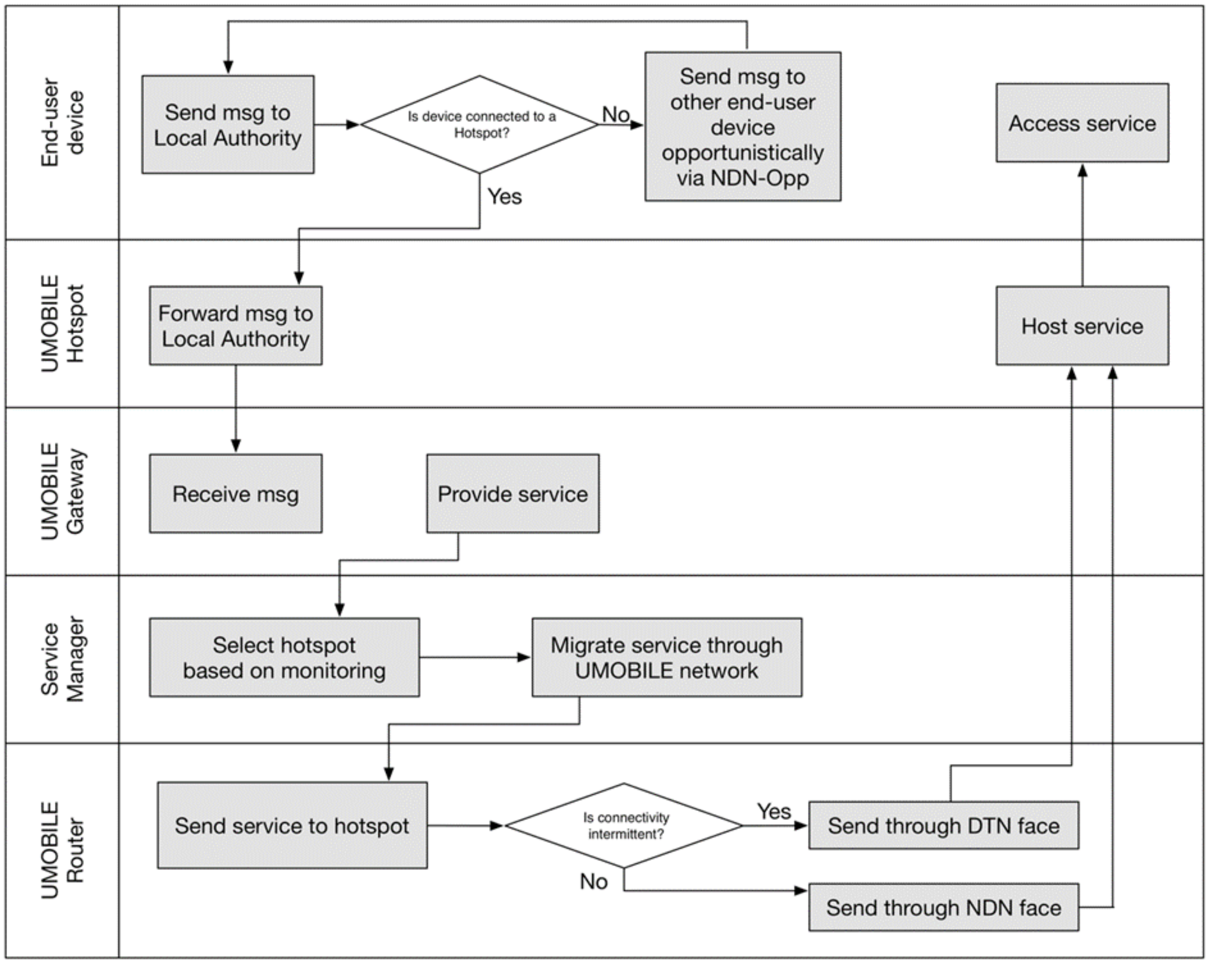

End-user device
Send msg to Local Authority
Is device connected to a Hotspot?
No
Yes
Send msg to other end-user device opportunistically via NDN-Opp
Access service
UMOBILE Hotspot
Forward msg to Local Authority
Host service
UMOBILE Gateway
Receive msg
Provide service
Service Manager
Select hotspot based on monitoring
Migrate service through UMOBILE network
UMOBILE Router
Send service to hotspot
Is connectivity intermittent?
Yes
No
Send through DTN face
Send through NDN face

Figure 18: Functional flowchart POC1

A list of requirements which need to be satisfied by the proof of concept, based on D.2.2, can be defined:

- UMOBILE APP SHOULD be compatible with a specific set of Device Feature to be defined
- UMOBILE APP SHOULD be compatible with a specific API level to be defined
- UMOBILE APP MUST be able to SEND and TAG (for example as "emergency") A MESSAGE to UMOBILE SYSTEM
- UMOBILE APP SHOULD be able to exploit every COMMUNICATION OPPORTUNITY to send the message

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

- UMOBILE APP MUST be able to SHARE the EMERGENCY MESSAGE among UMOBILE USERS using Wi-Fi Direct
- UMOBILE APP MUST be able to SHARE MESSAGES among UMOBILE USERS based on users' PREFERENCES and interaction in the system (i.e. subscription to "emergency services"), ensuring user privacy
- UMOBILE APP MUST be able to STORE the EMERGENCY MESSAGE until a UMOBILE USER is available to receive the message
- UMOBILE APP MUST be able to SHARE the EMERGENCY MESSAGE over NDN and IBR-DTN
- UMOBILE APP SHOULD be able to differentiate between messages shared by UMOBILE users and messages shared by authorities
- UMOBILE HOTSPOTS MUST be able to COLLECT, STORE and RELAY relevant
- UMOBILE SERVICE MANAGER MUST be able to migrate some services from the Internet and operate locally within the UMOBILE domain.
- UMOBILE HOTSPOTS SHOULD be able to PERFORM DATA FUSION, combining different pieces of data aiming to generate more reliable emergency information
- UMOBILE SERVICE MANAGER MUST be able to migrate some services from the Internet and operate locally within the UMOBILE domain.

4.1.3.Testbed

Figure 19 shows the UMOBILE Lab configuration set up that can be used to validate the operations (not necessarily all of them) involved in the first proof of concept.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

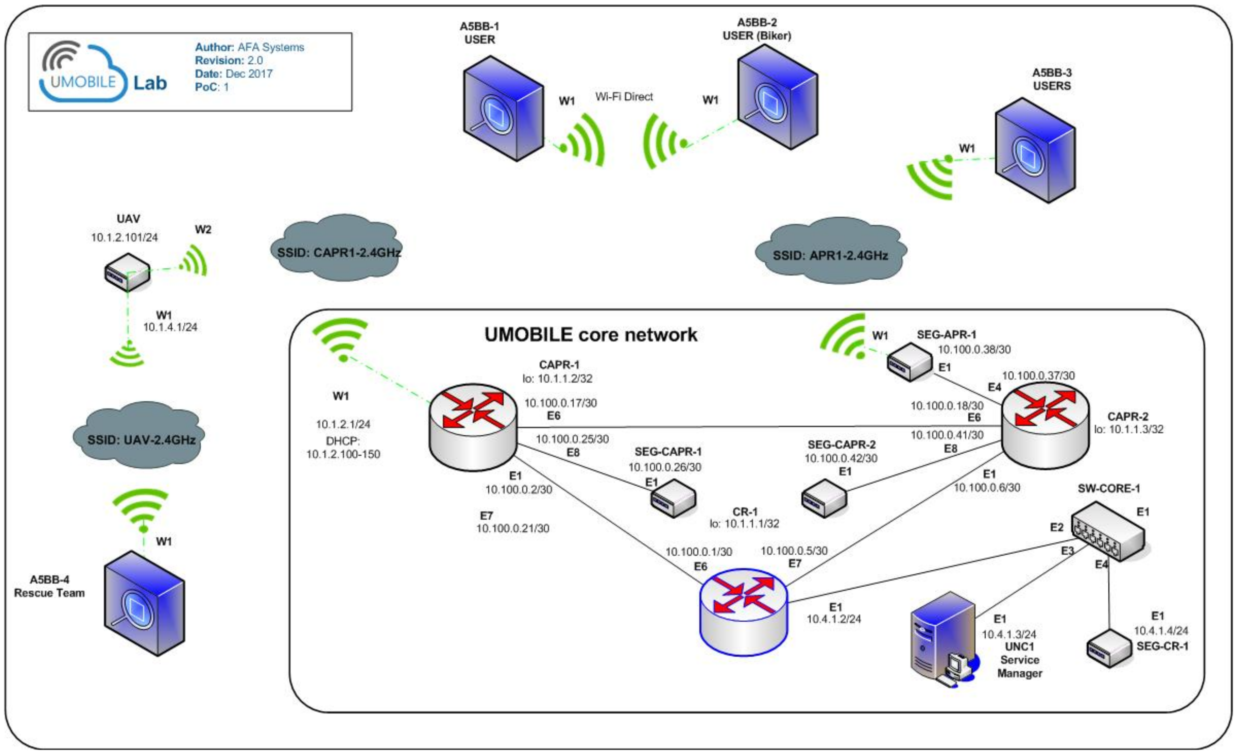


Figure 19: UMOBILE Lab configuration POC1

4.1.4. Validation

The following validation steps are defined:

1. Compose an emergency message (write text, add tag, automatically add geo-localization) with UMOBILE app from android black-box A5BB-1 (USER)
2. Keep down all the others devices (no Internet coverage)
3. Send the emergency message via Wi-Fi Direct (the message is stored until a receiver is available)
4. Enable the android black-box A5BB-2 (Biker), in order to receive the emergency message
5. Keep down android black-box A5BB-1
6. Enable the service manager SEG-CAPR-1
7. Enable the android black-box A5BB-3 (operator in the local authority)
8. The local authority receives the emergency message via NDN IBR-DTN

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

9. Enable Linux-box Satellite and setup local access point through connection to gateway
10. Compose a message with UMOBILE app from android black-box A5BB-4 and send it to the central station via Wi-Fi W1
11. Enable all the other devices
12. The service manager E1 checks the available hotspots
13. The service manager migrates a specific service to the selected hotspot CAPR-2 over a DTN tunnel.

4.1.5.Evaluation

The following paragraphs will help to understand the details of the relationships of the UMOBILE components in the POC1.

4.1.5.1 Integration of the service migration platform, DTN framework and KEBAPP

In this section we explain how the three QoS mechanisms that we have implemented in the UMOBILE project (service migration platform, DTN framework and KEBAPP) can be integrated to collaborate in the achievement of shared QoS objectives. To explain their potential collaboration, we will use the following hypothetical emergency scenario that corresponds to the POC1 documented in D2.1 "End user Requirements Report".

1. *Imagine an area that has been struck by an undesirable event such as a fire, floods, or earthquake, etc.*
2. *Consequently the network infrastructure in that area is temporarily disturbed by the event.*
3. *Upon being notified (over a secondary channel) about the situation, a rescue team arrives to the area and contacts (over a secondary channel) the Service Manager to request the deployment of emergency services in the affected area.*
4. *The expectation is that the services are available for the benefit of the rescue team and the victims of the event under the observance of specific QoS requirements. For instance, some services might tolerate arbitrarily long and unpredictable latency whereas others are latency-sensitive. Examples of such services are web servers that*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

offer news and maps of affected area.

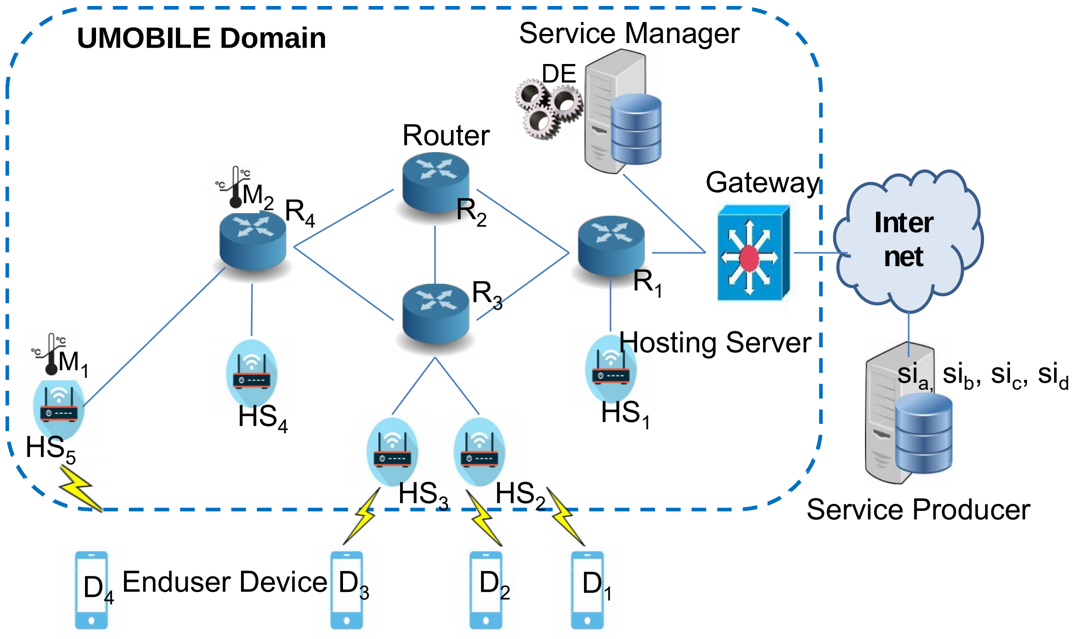


Figure 20: A view of the UMOBILE architecture with focus on Service Migration

- **UMOBILE Domain**: The UMOBILE Domain is a set of nodes deployed with UMOBILE software so that they are able to take advantage of the NDN facilities. It includes network routers (for example, R3) and applications hosts (for example, HS2). All the components shown in the UMOBILE domain require the UMOBILE platform software to support applications such as these demonstration scenarios. However, the deployment of UMOBILE platform software in end users' devices is optional since these devices can use conventional IP interfaces to connect to the UMOBILE domain. A UMOBILE Gateway links the UMOBILE Domain to the conventional Internet.
- **Gateway**: The UMOBILE Gateway is responsible for connecting the UMOBILE Domain to the Global Internet. Its functionality is to convert NDN Interest Requests to HTTP requests and HTTP responses to NDN Response. In the figure, it is deployed in one of the NDN routers (R0).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

- **Routers** (R1, R2, R3, R4): standard NDN router. We assume that UMOBILE Routers are in possession of storage that they use for in-network caching and for storing application level information such as dockerized service images.
- **Hotspots** (HS1, HS2, HS3, HS4): A Hotspot is a conventional computer with wireless communication facilities that can offer connectivity to End-user Devices (D1, ..., D4). It has disk storage facilities and virtualization software. In our experiments, we use Docker virtualization technology. Likewise, to implement the Hotspots we use Raspberry Pi computers that are capable of executing Linux containers.
- **End-users devices** (D1, D2, D3, D4): An End-user device is a mobile device with wireless facilities and interested in accessing services provided by the ISP provider. We assume that mobile devices communicate with the UMOBILE Hotspots over conventional HTTP.
- **Service Provider**: We assume the emerging business model where network providers are responsible for providing both network connectivity and access to services to end-users. In the figure, we assume that the service provider is the owner and in full control of the resources included in the UMOBILE Domain. Consequently, the Service Producer has delegated to the Service Provider the responsibility of deploying the services.
- **Service Producer**: It is an entity in possession of some arbitrary services of interest to the end-users. He stores them as compressed dockerized images sia, sib, sic and sid which are at the disposition of the Service Provider.
- **Services images** (si_a, si_b, si_c, si_d): A service image is a compressed dockerized images stored within the Service Producer.
- **Services** (s_a, s_b, s_c, s_d): A service is an application of interest to the end-user that can be instantiated from a corresponding compressed dockerized image. We assume that the services demand different levels of QoS, for instance different latencies. For example, service sa is latency-sensitive whereas sd is latency-tolerant.
- **Service Manager**: The Service Manager is a piece of software that implements all the functionality that the Service Provider needs to deploy his services, including disk space to store both services and compressed images. In the figure, the Service Manager is strategically deployed on a computer directly connected to the Gateway. This deployment simplifies the task of transferring compressed service images from

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

the global Internet to the UMOBILE Domain. At the heart of the Service Manager is a decision engine that is responsible for the actual deployment of services.

- **Decision Engine** (DE): The decision engine is a piece of software with all the necessary logics to make decisions about service deployment and migration. The decision engine has access to monitors deployed strategically within the UMOBILE Domain and instrumented to collect metrics about conditions of interest. On this basis, it decides about which services to deploy, when and where. For example, it creates a second replica of a given service in a neighbor Hotspot when the monitoring reports that the first replica is overloaded.
- **Monitors** (M1, M2): A monitor is a software tool for collecting real time information about the status of the resources included in the UMOBILE Domain, such as network conditions and current usage of their Hotspot resources (CPU, memory and disk). Only two monitors are shown in the figure, yet there is nothing to prevent from deploying as many as necessary. A good example of a monitor is a Python script deployed in the Raspberry Pi used to implement a Hotspot to measure and report its current free memory.

In subsequent sections, we explain how the core infrastructure can be used for addressing the QoS requirements demanded by the emergency scenario discussed above.

To recap, the Service Provider (a human being) is responsible for deploying services with specific QoS requirements. The QoS requirements associated to services result from negotiations and contractual agreements drawn between the Service Provider and the Service Producer. The Service Manager is the tool that the Service Provider has at his disposition to help him fulfill the QoS requirements associated with his services. He can use it to activate his QoS mechanisms. Figure 4 shows the relationship between the Service Manager and each mechanism.

As shown in Figure 4, the Service Manager can activate each of the mechanisms to work individually; for example, it can activate the Service migration platform and nothing else. Alternatively, it can activate two of them and make them collaborate; for example, it can activate the Service migration platform and the DTN framework and make them collaborate. The Service Provider can devise different combinations to meet different QoS parameters associated to different classes of services.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

It is worth clarifying that, in addition to the service migration platform, DTN framework and KEBAPP, the UMOBILE project has also studied the INRPP congestion control mechanism to help meet QoS requirements. Its usage and its role is explained at large in D4.4[D4.4]. We will leave it out of this discussion because the results that we have achieve so far are from simulation studies, consequently, INRPP congestion control cannot be used in the demonstration of the POC1.

4.1.5.2 Role of the service migration platform in POC1 and validation in the lab testbed

The hypothetical scenario of POC1 is detailed in D5.3 [D5.3]. A crucial stage of the scenario is the deployment of emergencies services (e.g., local map services) in an area struck by a catastrophic event (e.g., fire) and deprived of normal communication services (see point 13 of Section 4.1.4). The demonstration of the POC1 will show how the service migration platform can be used to deploy the emergency services opportunistically, by the local authorities after receiving a request from members of the rescue team.

The solution involves the transfer the image of the service from a service repository located in the main network to a Hotspot located in the affected area which is assumed to be disconnected from the main network. The solution is based on the integration and collaboration of the service migration platform with the DTN framework. The service migration platform is responsible for manipulating the image while DTN is responsible for providing a communication tunnel for transferring the image.

Physically, the DTN tunnel is built on a physically mobile DTN-enabled node that can travel backwards and forwards between the service repository and the Hotspot in a manner that when it can communicate with service repository it cannot communicate with Hot Spot and vice versa. As the DTN-enabled node travels, it data-mules data chunks of the image of the service [D4.4]. From this explanation, it follows that the functionality of the service migration platform in POC1 involves physical manipulation of the DTN-enabled node. Consequently, the UMOBILE lab cannot be used for full remote replication of the POC1. However, we take advantage of the UMOBILE lab in testing individual functions of the service migration procedure. We will describe one of them.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

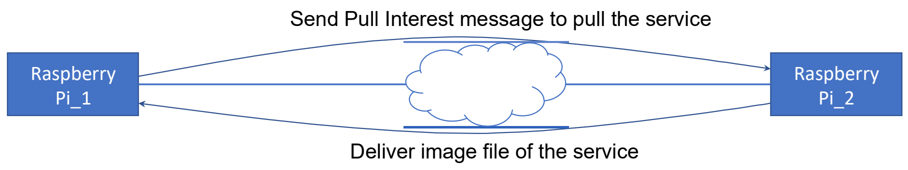

Send Pull Interest message to pull the service
Raspberry Pi_1
Raspberry Pi_2
Deliver image file of the service

Figure 21: Service migration experiment conducted in the UMOBILE lab

Figure 21 shows the architecture that can be used to demonstrate how the service migration platform can be used to migrate the image of a service. It involves two nodes that can communicate with each other through the LAN of the UMOBILE lab, namely Pi_1 and Pi_2 which can be realised by Raspberry Pi computers. In the experiment, Pi_1 sends, a Pull Interest message to Pi_2 to request the image of a service (a precisely, a Docker image). Pi_2 sends back the image of the requested service, to honour the request.

The experiment involves only logical manipulation of software components, consequently, the demo can be replicated remotely, say by a conventional user called *molina-jimenez.*

Assumptions:

1) We assume that a user called *molina-jimenez* has been granted to access remotely the UMOBILE lab facilities
2) Pi_1, Pi_2 and intermediate nodes are equipped with the UMOBILE platform
3) Pi_1 and Pi_2 are capable of running Python and Docker
4) The service manager script is running on Pi_1
5) The UMOBILE hotspot script is running on Pi_2

4.1.5.3 FONERA – KEBAPP – SERVICE MIGRATION INTEGRATION

In the last step of PoC 1 (see point 13 of Section 4.1.4), an emergency service is migrated and deployed in a UMOBILE hotspot placed in the rescue area. To overcome the absence of network communication, the service migration platform resorts to DTN tunnelling provided by an Android phone equipped with the DTN framework.

1. Service Execution Function: a service execution function that is capable of instantiating services out of Docker images migrated by the Service Manager needs to be deployed in the UMOBILE hotspot. The Fonera hardware (the FON hardware) is capable of providing access point capabilities and as such will be used to prototype a

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

UMOBILE hotspot. However, it is not yet able to run 64 bits applications necessary to run a Docker1 service required by the service migration platform. To overcome the problem, we will collocate with the Fonera a Raspberry Pi that will perform the Service Execution Functions. The raspberry Pi will have the WiFi interface disabled, and will connect to the Fonera using an Ethernet connection.

After the deployment of the service, the UMOBILE hotspot will be able of providing emergency information (e.g. instructions or map information) to the user (citizen) that needs to be rescued via a KEBAPP application. In order to do that, different integrations between UMOBILE devices need to be done.

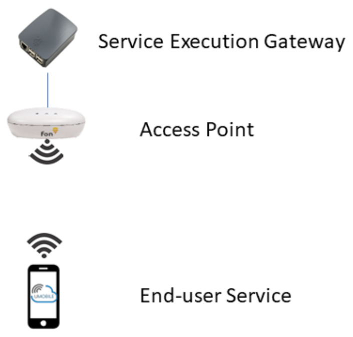


Figure 22: Devices involved in the UMOBILE hotspot – KEBAPP integration

2. The UMOBILE Hotspot (Fonera) will need to advertise the emergency service instantiated in order that any smartphone device recognize the presence of a UMOBILE hotspot running the emergency information service and then automatically decides whether to connect and retrieve the emergency information. This UMOBILE hotspot advertisement is developed using a DNS-based Service Discovery (DNS-SD) using 802.11u information delivered over Generic Advertisement Service (GAS). This allows UMOBILE hotspots great flexibility for network management. Wireless networks can be dynamically activated and advertised depending on the services instantiated and the users within the range of the hotspot, without having to activate permanently any specific network for any specific application and/or prior client connection in order to discover the services available. In the UMOBILE project we devise setting a WiFi access network in the hotspots for each application. However, there is flexibility to group applications in WiFi networks for better scalability and network management.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

3. End-user service (Android smartphone) needs to be able to automatically discover any service instantiated (or can be potentially instantiated) in the UMOBILE hotspot, connect to it when the service instantiated and retrieving the necessary information for the user. In order to do so, the end-user service implements the KEBAPP service, that is part of the UMOBILE architecture. A user application, that has been developed using the KEBAPP service, is used to automatically retrieve emergency service information from UMOBILE hotspots, when a user needs to be rescued or requires basic emergency information, but no connectivity is available other than the possibility to connect to a UMOBILE hotspot that is deployed in the area when an emergency message is sent to the local authorities. This user application can automatically detect and download any new emergency information in the UMOBILE hotspot, such as video messages with safety instructions or a map with a safe path to a meeting point.

ROADMAP for the demo

In the following table we can observe a detail of the multiple tasks necessary for the integration work necessary for the PoC:

UMOBILE device	Task	Status / Expected date
UMOBILE hotspot	Implement the Service Execution Function running in the Raspberry Pi. Notice that we can use the Raspberry Pi as a UMOBILE hotspot.	DONE
	Encapsulate any service into a Docker image to be instantiated in a UMOBILE hotspot.	DONE
	Implement and encapsulate the emergency information service into a Docker image.	01/18
	Integrate Service Execution Function with Fonera for the UMOBILE hotspot	DONE
	Activate 802.11u information	12/17
	Test service discovery with Android phones	12/17
	Test emergency service auto discovery and instantiation	01/18
	Implement user emergency app using KEBAPP	DONE
	Implement service discovery using 802.11u information	DONE
	Test network discovery and connectivity with UMOBILE hotspot	12/17

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

	Test the whole integration Service Execution Function - hotspot - KEBAPP	1/18
End-user service / KEBAPP	Implement service discovery using 802.11u information	DONE
	Test network discovery and connectivity with UMOBILE hotspot	12/17
	Test the whole integration Service Execution Function hotspot - KEBAPP	1/18

Table 2. Tasks and estimated completion date

UMOBILE Lab Actions

- Install a FONERA in the UMOBILE lab to enable remote testing of UMOBILE hotspots using the FON hardware: Model FON2601E
- Install KEBAPP service in the A5BB Android box: 12/17
- Install emergency service user app A5BB Android box: 12/17
- Test connectivity between A5BB and SEG: 12/17
- Test connectivity between service manager and SEG: 12/17
- Deploy discovery mechanisms FONERA: 1/18
- Test discovery mechanisms FONERA - Android: 1/18
- Deploy emergency information service in the service manager: 1/18
- Test automatic discover, service instantiation and information retrieval from Android (the whole process) : 1/18

4.1.6.Collaborative operation of the service migration platform, DTN framework and KEBAPP

In Section 2.2.2 we explained how the three technologies can collaborate bilaterally. The POC1 is more demanding and requires the integration of the three technologies together. Observe that:

1. The DTN framework operates as a transport mechanism in the affected area. It data-mules both requests for services issued by end-users and images of the services transferred by the service migration platform.
2. The service migration platform is responsible for receiving service requests and deploying the services where and when they are needed---all on the basis of the data-mulling transport services provided by the DTN framework.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

3. KEBAPP operates as an edge-network sharing mechanisms that allows end-users to access services locally (from other users) as opposed to accessing them directly from the core network. It relies on the support of the service migration platform which is responsible for deploying either the actual service or the KEBAPP application (Section 2.2.4) through the data-mulling transport services provided by the DTN framework.

Within the particular of Figure 63 and Figure 64, the three technologies participate in the following way:

1. DTN will be used to tunnel the service request message issued by the USER to the SERVICE MANAGER.
2. As shown in Figure 63, the service migration platform is under the control of SERVICE MANAGER which is a component software of the LOCAL authority.
3. Upon receiving a request (through either Wi-Fi Director or Wi-Fi) to deploy the emergency service in the Remote network, the service migration platform uses the DTN framework (see Service migration over DTN component) to honor the request.
4. The requested service is deployed on the UMOBILE HOT SPOT with the assistance of DTN since the Remote network is assumed to be unreachable to LOCAL authority through conventional communication.
5. Once the service is deployed on the UMOBILE HOT SPOT, it is executed locally, for the benefit of the members of the rescue team (See RESCUE TEAM base).
6. The UMOBILE HOTSPOT shown in Figure 63 offers communication, computation and storage facilities (see Figure 64) To implement it we use a combination of a FONERA device and Raspberry Pi computer. The Raspberry Pi computer provides storage and computation to run the service. Complementary, FONERA provides communication to make the service available to the members of the rescue team.
7. To take advantage of KEBAPP, we will deploy a KEBAPP aware service that can be shared by the end-users (citizens and members of the rescue team) located in the affected area.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

4.2 PoC 2: Service Announcement and Social-Routine scenario

4.2.1.Context

In this proof of concept, we present how the UMOBILE architecture can provide new types of services, such as micro-blogging and social-routine, showcasing the benefits of opportunistic communications and enhancements to smart routing and QoS aware services.

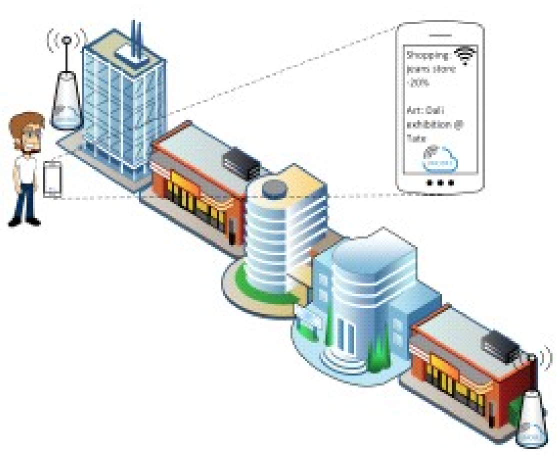


Figure 23: Service Announcement and Social-Routine scenario

4.2.2.Demonstrator

4.2.2.1 Scenario

In this demonstrator, a UMOBILE user, as illustrated in Figure 24, generates and shares an expression of interest in the form of tagged information (e.g., nearby supermarket offers or restaurant review), by means of the Now@ app. The message is shared among all UMOBILE users that can benefit from the local information. In addition, the UMOBILE system will keep track of the local event and update useful information to the UMOBILE subscribed users based on the new created information and its relevant hashtag. This information can be referred to the availability of some form of service (QoS aware service), as well as to user experience and user perception shared among users.

UMOBILE users will be able to exchange and share information, e.g., photos, videos, social

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

text comments among their contacts even if devices are not always connected to the Internet. Data is exchanged among people passing by, based on the NDN-OPP and the implemented DAGGER routing protocol. The UMOBILE system takes advantage of all available connectivity (e.g., wired or wireless) and intelligently chooses the most suitable transmission protocol depending on the network environment.

UMOBILE hotspots, deployed along this scenario, will store data based on its local meaningfulness, e.g. tips/photos about nearby shops, and disseminate among other peering hotspots or UMOBILE users.

Furthermore, the UMOBILE system will provide the user with additional information regarding their personal expressed interests and, e.g., estimation of the time to get to a certain suggested location based on history information.

Another crucial aspect supported by UMOBILE is the capability to capture personal data of UMOBILE users (e.g. visited networks, affinity network) with the ultimate goal of improving the user's routine.

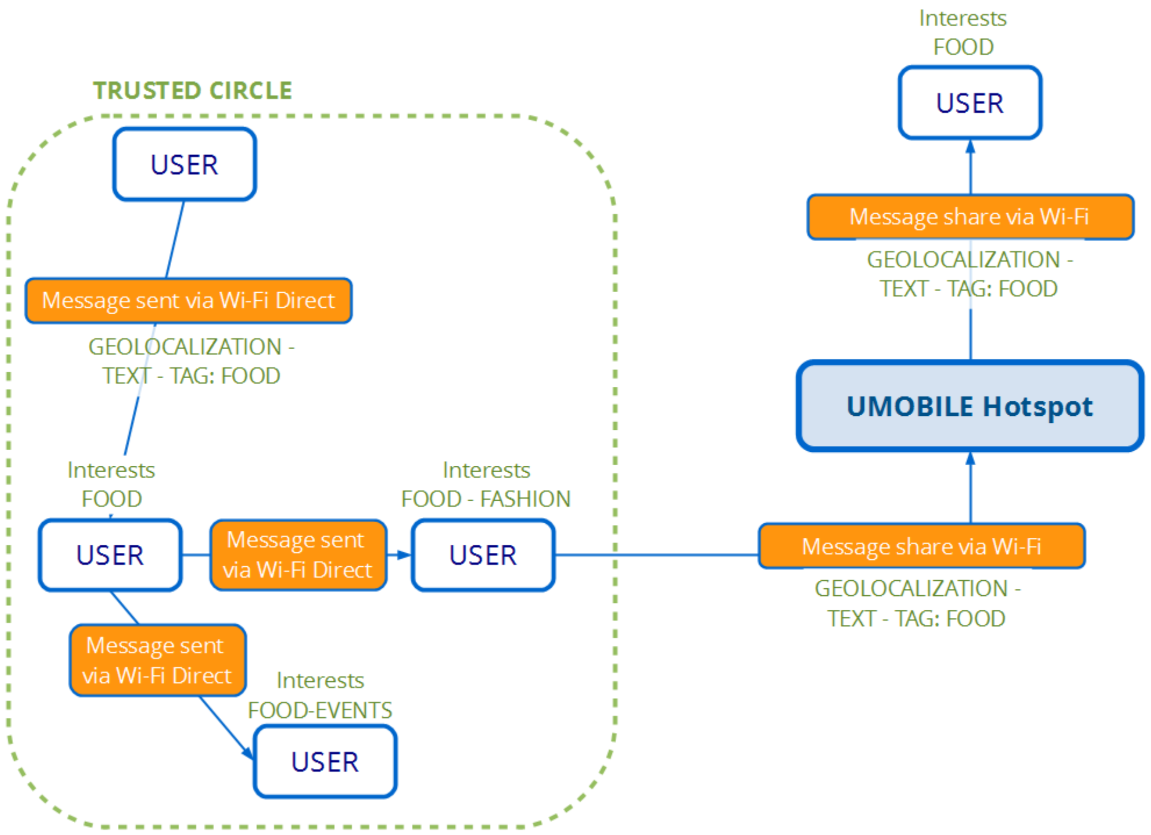

TRUSTED CIRCLE
USER
Message sent via Wi-Fi Direct
GEOLOCALIZATION - TEXT - TAG: FOOD
Interests FOOD
USER
Message sent via Wi-Fi Direct
Interests FOOD - FASHION
USER
Message sent via Wi-Fi Direct
Interests FOOD-EVENTS
USER
Interests FOOD
USER
Message share via Wi-Fi
GEOLOCALIZATION - TEXT - TAG: FOOD
UMOBILE Hotspot
Message share via Wi-Fi
GEOLOCALIZATION - TEXT - TAG: FOOD

Figure 24: High-level flowchart of the second Proof of concept

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

4.2.2.2 Functional flowchart

From a functional point of view, the defined scenario can be mapped into the flowchart described in Figure 25.

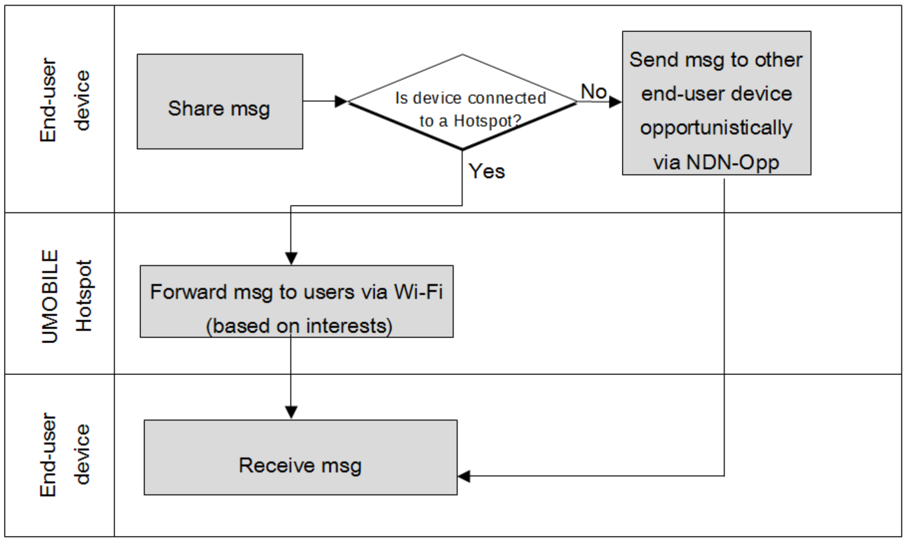

End-user device
UMOBILE Hotspot
End-user device
Share msg
Is device connected to a Hotspot?
No
Yes
Send msg to other end-user device opportunistically via NDN-Opp
Forward msg to users via Wi-Fi (based on interests)
Receive msg

Figure 25: Functional flowchart POC2

A list of requirements, which need to be satisfied by the proof of concept, based on D.2.2, can be defined:

- UMOBILE APP SHOULD be compatible with a specific set of Device Feature to be defined
- UMOBILE APP SHOULD be compatible with API level to be defined
- UMOBILE APP MUST be able to SEND and TAG (for example as “events”) A MESSAGE to UMOBILE SYSTEM
- UMOBILE APP MUST be able to INFER USER CONTEXT (geo-location) to complement the MESSAGGE.
- UMOBILE APP SHOULD be able to exploit every COMMUNICATION OPPORTUNITY to send the message
- UMOBILE APP MUST be able to SHARE the MESSAGE among UMOBILE USERS using Wi-Fi Direct

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

- UMOBILE APP MUST be able to SHARE the MESSAGE among UMOBILE USERS using Bluetooth
- UMOBILE APP MUST be able to SHARE MESSAGES among UMOBILE USERS based on users' PREFERENCES and interaction in the system (i.e. subscription to "food"), ensuring user privacy.
- UMOBILE APP MUST be able to STORE the MESSAGE until a UMOBILE USERS is available to receive the message
- UMOBILE HOTSPOTS MUST be able to COLLECT, STORE and RELAY relevant information, based on user circles and preferences
- UMOBILE HOTSPOTS SHOULD be able to PERFORM DATA FUSION, combining different pieces of data aiming to generate more reliable emergency information
- UMOBILE GATEWAY SHOULD be able to PERFORM DATA FUSION, combining different pieces of data aiming to generate more reliable emergency information.

4.2.3. Testbed

Figure 26 shows the UMOBILE Lab configuration set up in order to validate the second proof of concept.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

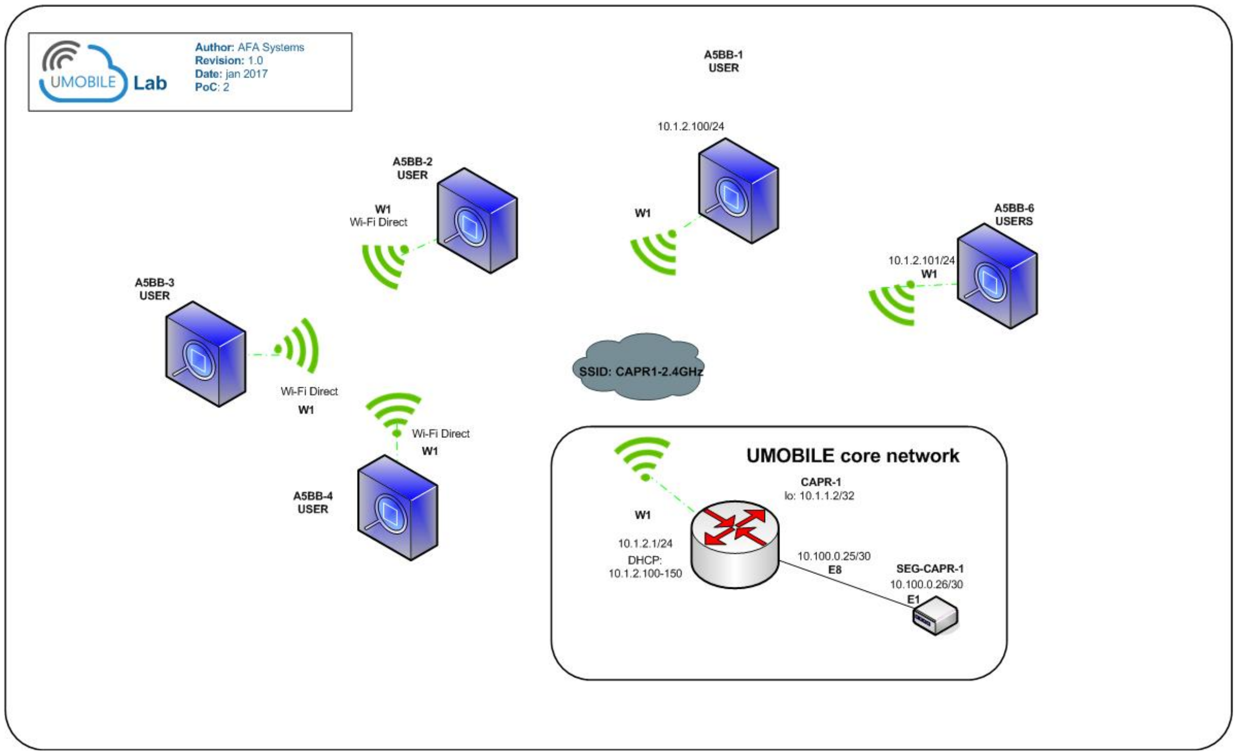


Figure 26: UMOBILE Lab configuration POC2

4.2.4. Validation

1. Compose a message with UMOBILE app from android black box A5BB-2: write text, add tag/keywords (i.e.: "food"), automatically add geo-localization.
2. Send the message via Wi-Fi Direct to users (A5BB-3 and A5BB-4) which satisfy the following requirements: their INTERESTS are relevant to the message (i.e.: based on the tag)
3. Send again the message using Bluetooth
4. Share the message with local UMOBILE enabled hotspot CAPR-1 using 3G connectivity
5. Share the message through Wi-Fi to user A5BB-6 which satisfy the following requirements: their INTERESTS are relevant to the message (i.e.: based on the tag).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

4.3 Tests supporting the UMOBILE PoC

4.3.1.Context

As mentioned in Section 4, in the demonstration of the emergency scenario of POC1 (see also point 13 of Section 4.1.4) an Android phone equipped with the DTN framework is used to overcome the absence of normal network communication. Precisely, it is used to tunnel (data-mule) the image of a service.

Another alternative that we are evaluating to mitigate the impact of the lack of communication facilities is the use of Unmanned Aerial Vehicles (UAVs).

To persuit this idea further, TEKEVER AU is evaluating the suitability of UVAs in the solution of some of the functions involved in POC1.

This endevour is being conducted independently from the POC1 activities listed in Section 4.1.4. Consequently, results from experimentations with UVAs will not be necessarily included in the demonstration of POC1 as envisioned in Section 4.1.4.

- A UAV can take on the role and physically implement the UMOBILE HOTSPOT located at the remote network (the rescue team). In this case, The UAV UMOBILE HOTSPOT may be employed to migrate services from the LOCAL Authority to the Remote Network as well as to provide a local communication infrastructure for first responders (rescuers).
- A UAV may also be used as a data mule providing connectivity between isolated networks such as between the USER and the biker in POC1 (taking on the role of the biker, collecting emergency info locally and transmitting the message towards an authorized emergency entity via UMOBILE system, in an opportunistic fashion).
- Finally, a UAV may be employed as a data mule providing connectivity between USERs in the remote network and local authorities.

The test setup described in this section has been designed to validate the use of an UAV in support of the functions mentioned above. It is intended to be another alternative to support the execution of the POC1 and subsequently the demonstration of the UMOBILE architecture to reach disconnected areas and assist authorities in challenged environments.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

4.3.2.Demonstrator

In emergency situations, it is of utmost importance to share data (e.g. imagery, text, etc.) between the field and decision makers. Information is power and in the case of emergency response, the quality and speed with which information is collected and distributed is fundamental to the success of rescue and response activities. Where normal connectivity does not exist, it becomes essential devise ad-hoc alternatives to transport digital data from one location to another.

UAVs can collect relevant data to help plan and monitor the evolution of emergency situations or to help locate victims. Generally, these vehicles will provide unobstructed lines of sight due to their altitude thereby making them ideal to relay data or transport it (functioning as a data mule) across long distances providing connectivity between isolated networks.

4.3.2.1 Scenario

In the scenario proposed herein, a situation where the line of sight advantage of UAVs cannot be used directly and the air vehicle is employed as an air mule to transport data collected from user terminals on the ground to a location where a decision maker can act on the data received in both an efficient and in a rapid manner. This scenario is consistent with the scenario of POC1 and will allow the consortium to assess how a UAV could offer another alternative to address the last two bullets described in the context section above (providing connectivity between isolated networks or users). This scenario can also be applied to test the ability of using a UAV as an alternative to the Android phone to migrate services between the decision makers (identified as LOCAL authority in POC1) and a rescue team or civilian user (identified as remote network in POC1).

The proposed scenario is represented in Figure 27. In this situation, a civilian (e.g. a park goer or hiker) detects an emergency situation such as a forest fire or is subject to an injury (e.g. a fall) and attempts to communicate the situation to the local first responder service (local authority). This information will be fundamental to the first responder service to coordinate first responder resources (e.g. fire-fighters) and decide upon which course of

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

action to apply to the situation. While trying to communicate, the civilian discovers she has no connectivity and no network access.

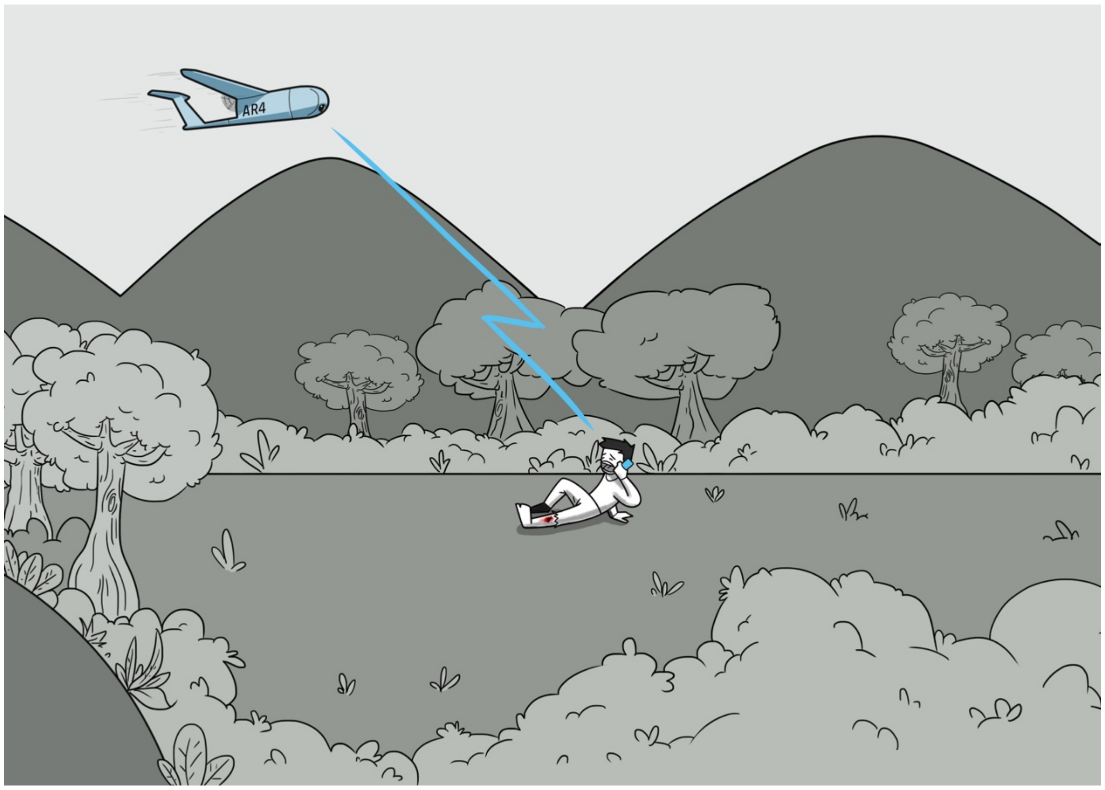
A first responder UAV flying a routine surveillance mission over the area overflies the civilian and, through its UMOBILE app collects the information from the civilian user device. As the UAV continues its mission and comes within range of its Ground Control Station (GCS) collocated with the local authority's command center, it will relay the civilian's message in an opportunistic way.

As mentioned earlier this situation is similar to the first part of POC1 (with the UAV taking on the role of the bikers) and the purpose of this test is to validate the potential use of the UAV as a data mule.

The test relies on a set of assumptions which are numbered below:

- There is no connectivity (cellular, WiFi or other) between the civilian detecting the emergency situation and the local emergency response authority;
- There is no direct radio link between the UAV and its GCS located at the local authority's centre, i.e. the UAV is flying beyond radio line of sight (BRLOS) and as such it is impossible for the aerial vehicle to relay directly the civilian's message to the local authorities;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

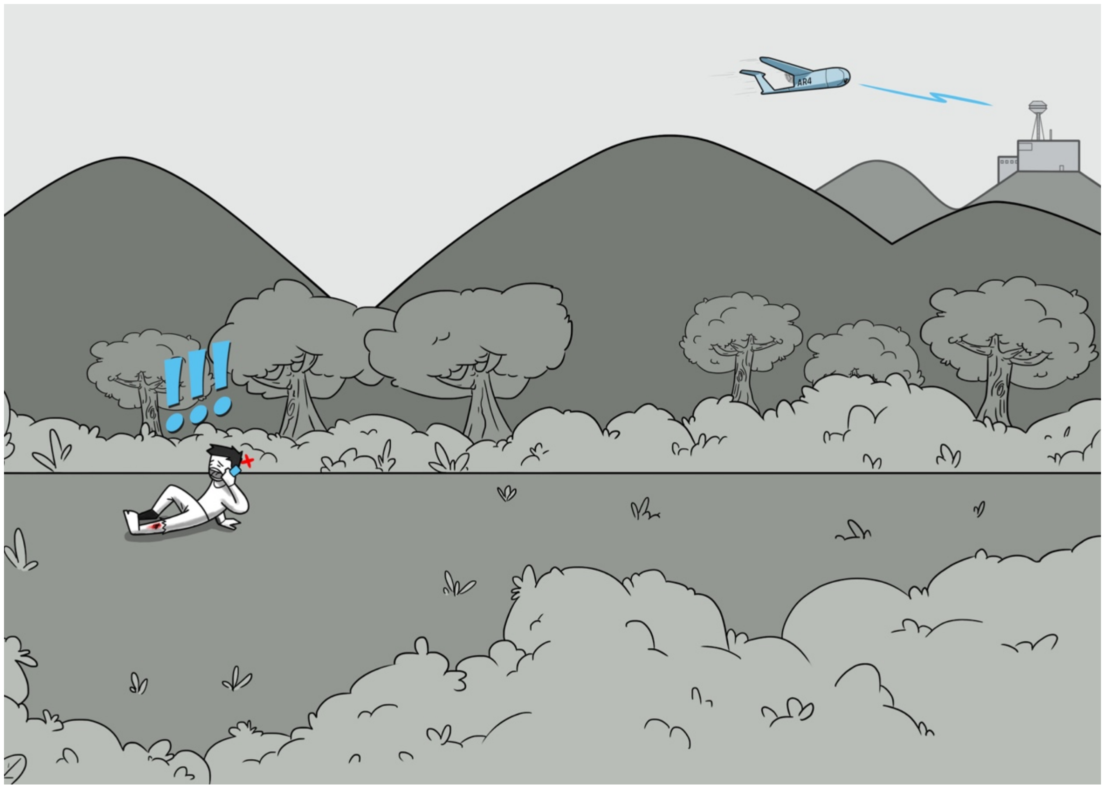


Figure 27: POC1 support test scenario (drawings not to scale)

In addition to the situation above, it is possible to test the ability of using the UAV to migrate a service from the local authority to the area where the emergency is taking place, i.e. to instantiate a service to support requests from the civilian or at a later stage a deployed team of first responders. This additional test may be used to verify the possibility of also applying a UAV as hotspot in the emergency area as described in POC1.

By mapping the situation above to physical equipment, one obtains the block diagram below:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

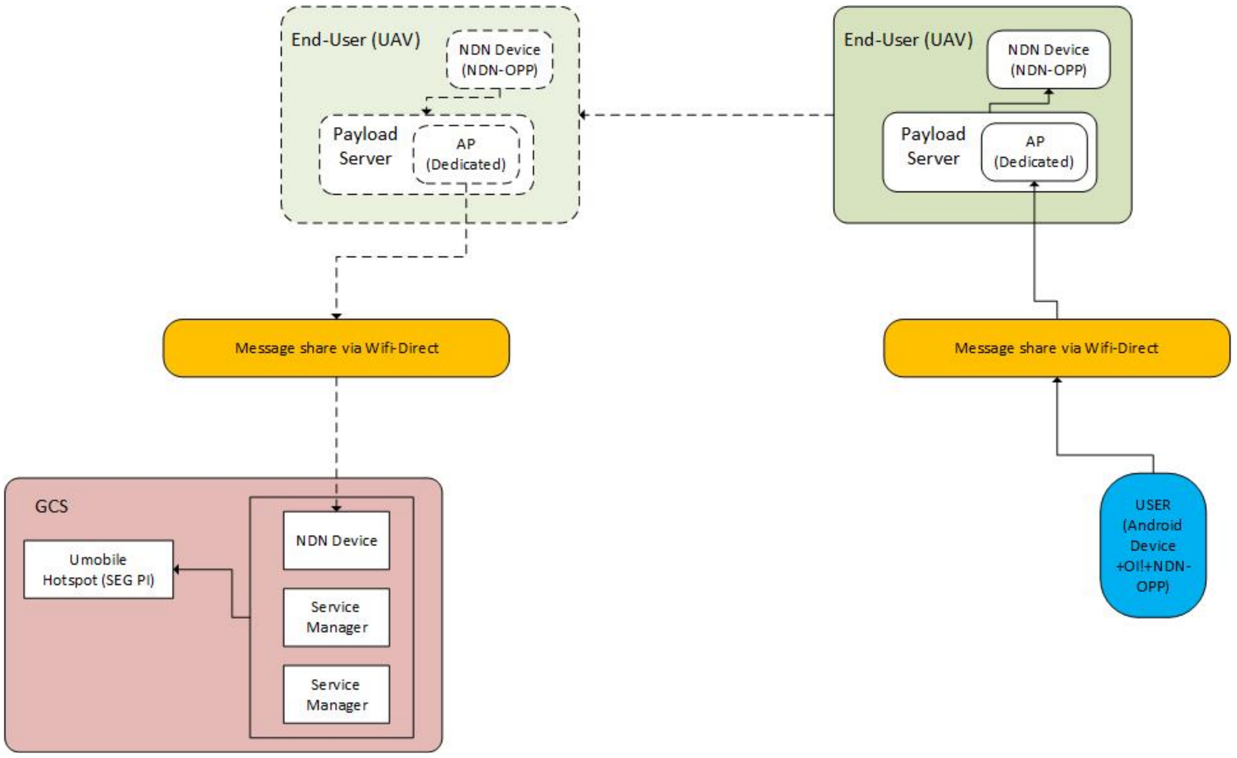


Figure 28: Block diagram for the support tests to POC1

The user device in blue above corresponds to an Android device running the Oi! Application. This device is used by the civilian reporting the emergency. The emergency message is passed on to the first responder UAV via NDN-Opp. To do this a dedicated radio supplied by TEKEVER and hosted in the UAV's payload server will be used instead of the UMOBILE Raspberry Pi. The reason behind this is that the Pi does not have sufficient power to allow coverage of the affected area by the UAV while maintaining safe flight (i.e. typical operational altitude). This decision is justified in section below following the results obtained to characterize the coverage obtained with the UMOBILE access point. Nevertheless, a UMOBILE Banana Pi functioning as a NDN device will be installed on-board the aircraft. In this instance, the UAV will function as another user device and will leave the affected area towards its Ground Control Station (GCS). When it gets within range of the GCS the Banana Pi NDN device will transmit the message from the civilian through the dedicated access point on the UAV to the GCS on the ground. The GCS will function as a UMOBILE hotspot and can host also a UMOBILE Gateway.

Additional tests may be carried out to validate the use of the UAV as a UMOBILE Hotspot capable of migrating UMOBILE services from the GCS (which could represent a LOCAL

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

authority in POC1) to a user in the field (e.g. .a civilian such as the one reporting the emergency or a first responder answering the emergency). In this case the block diagram representing the equipment used will be the one below.

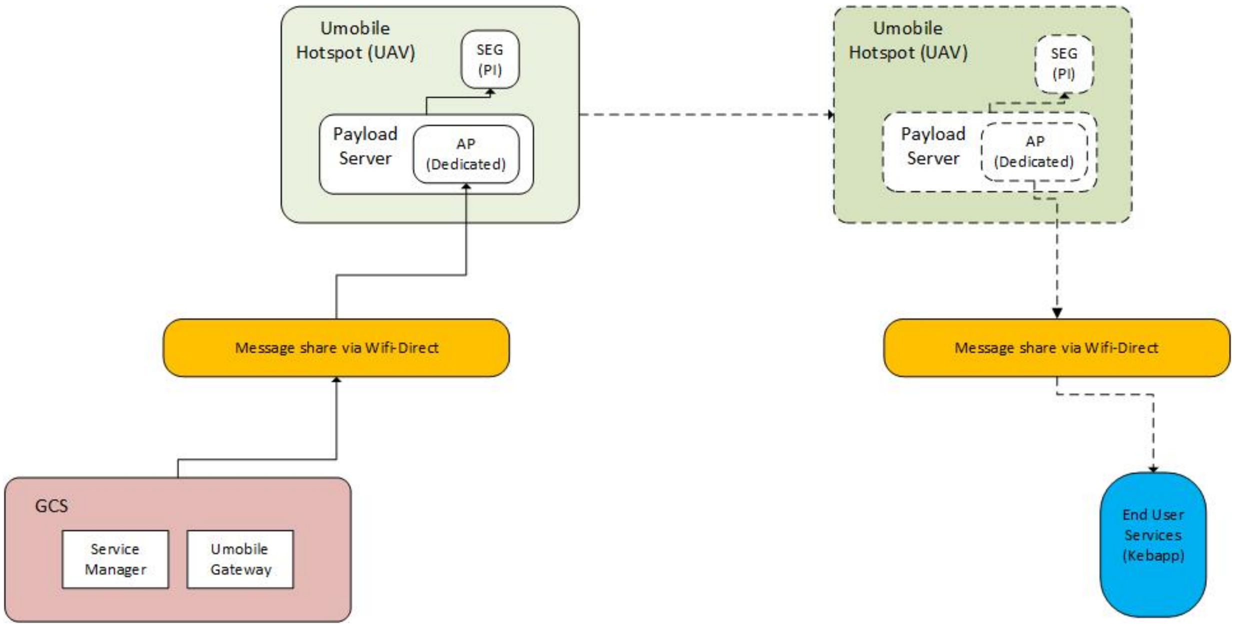


Figure 29: Block diagram for additional support tests to POC1 (service migration)

In this case, the UAV will carry UMOBILE hotspot in the form of a Raspberry Pi. After uploading the desired services over the GCS, the UAV flies out to the affected area and starts hosting the services to the user devices (either first responders or civilians) on the ground.

4.3.2.2 Functional flowchart

The following functional flowcharts represent the scenario above. The first flowchart (Figure 30) maps the planned test while the second flowchart (Figure 31) adds the potential validation of the use of the UAV to migrate a service between the local authority and either the civilian user device or a first responder user device.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

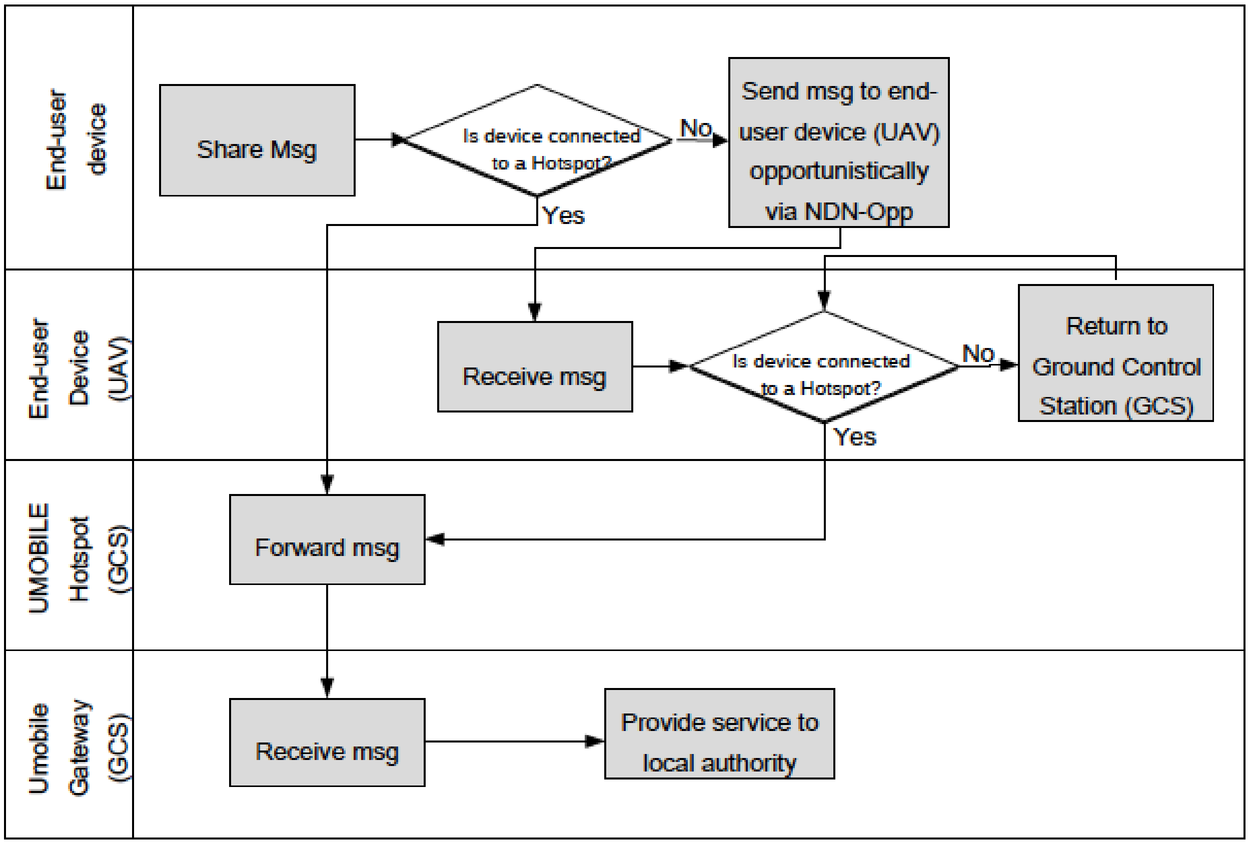

End-user device
Share Msg
Is device connected to a Hotspot?
No
Yes
Send msg to end-user device (UAV) opportunistically via NDN-Opp
End-user Device (UAV)
Receive msg
Is device connected to a Hotspot?
No
Yes
Return to Ground Control Station (GCS)
UMOBILE Hotspot (GCS)
Forward msg
Umobile Gateway (GCS)
Receive msg
Provide service to local authority

Figure 30: Functional flowchart for support test to POC1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

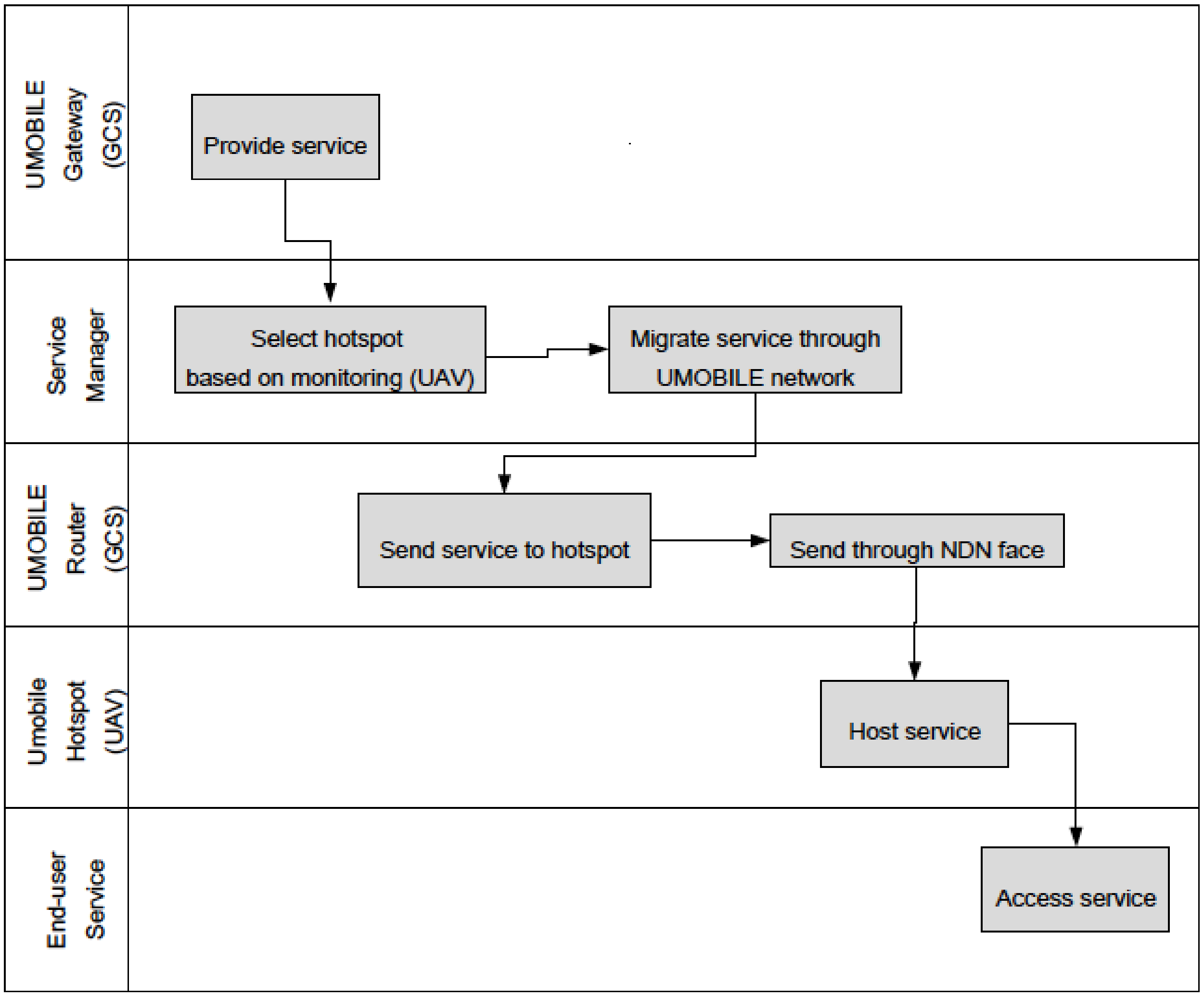


Figure 31: Functional flowchart for support test to POC1 with additional tests for service migration

A list of requirements which need to be satisfied by this test follows below:

- UMOBILE APP SHOULD be compatible with a specific set of Device Feature to be defined
- UMOBILE APP SHOULD be compatible with a specific API level to be defined
- UMOBILE APP MUST be able to SEND and TAG (for example as “emergency”) A MESSAGE to UMOBILE SYSTEM
- UMOBILE APP MUST be able to INFER USER CONTEXT (geo-location) to complement the EMERGENCY MESSAGGE.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

- UMOBILE APP SHOULD be able to exploit every COMMUNICATION OPPORTUNITY to send the message
- UMOBILE APP MUST be able to SHARE the EMERGENCY MESSAGE among UMOBILE USERS using Wi-Fi Direct
- UMOBILE APP MUST be able to SHARE MESSAGES among UMOBILE USERS based on users' PREFERENCES and interaction in the system (i.e. subscription to "emergency services"), ensuring user privacy
- UMOBILE APP MUST be able to STORE the EMERGENCY MESSAGE until a UMOBILE USER is available to receive the message
- UMOBILE APP MUST be able to SHARE the EMERGENCY MESSAGE over NDN and IBR-DTN
- UMOBILE SYSTEMS over UAV MUST be able to provide a local communication Wi-Fi infrastructure
- UMOBILE HOTSPOTS MUST be able to COLLECT, STORE and RELAY relevant information (e.g., alert messages, instructions from emergency authorities)

4.3.3.Testbed

The test foreseen in this section will not be performed in the UMOBILE Lab.

4.3.4.Feasibility of employing UMOBILE HW

A set of tests were carried out to ensure the well-functioning of the UMOBILE access point, in order to characterize the provided hardware and determine whether it would support the use of an UAV during the UMOBILE tests in support to POC1.

This began with static tests, having both Wi-Fi hotspot and collaborator standing still while performing network and coverage tests, and concluded with the maximum attainable coverage, signal quality and bandwidth. Moreover, on the dynamic tests, the hotspot was integrated within TEKEVER's UAV and the same tests were performed.

The purpose of the tests described in this section was twofold:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

- On the one hand characterize the range and coverage allowed by the UMOBILE access point in order to determine the feasibility of using this equipment in a UAV to perform tests supporting POC1;
- Provide insights on the operational conditions of the UAV to help determine flight envelopes that will enable communication between users on the ground and the aircraft.

As the purpose was to determine feasibility of use of the UMOBILE access point HW, none of the tests focused on the characterization of performance while using the UMOBILE NDN-opp implementation. A comparison between NDN-opp and regular WiFi will be presented in D5.5. The equipment provided and used for UAVs tests is described in the following table:

Equipment	Additional Info
Raspberry Pi 3	Model B, max total usb current draw:1.2A
Battery	Multistar High Capacity 20000mAh 4S 10C Multi-Rotor Lipo Pack
SD card	32GB
USB WLAN Adapter	Detailed info in Table
Power Converter	Ref: ptn78020; Converts from battery voltage to 5V; maximum current: 6A
RP-SMA Cable	3 meters

Table 3: Equipment used on UAV tests

The next table shows detailed information regarding the USB WLAN:

Features	USB WLAN Adapter Details
Model Name	CSL USB 2.0 WLAN Adapter 300 Mbit (204/5GHz) with high-power

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

	and high performance dual antenna
Use	Powerful CSL 300 Mbps WLAN Stick with two high-performance antennas ensures high ranges and data transfer rates
Chipset:	Ralink RT5572
Frequency Bands:	2.4 GHz 5 GHz (not usable in parallel)
Connections:	1x USB connector 2x RP-SMA antenna connector
WLAN speed:	Max. 300 Mbit/s
Network Standard	802.11 a/b/g/n
Encryption	64/128-bit WEP WPA WPA2 TKIP AES WAPI
Modulations	DSSS with CCK DQPSK DBPSK with BPSK QPSK 16QAM 64QAM
Data transfer rates	IEEE 802.11 up to 300Mbit/s

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

	a:	
	IEEE 802.11 n:	up to 300 Mbit/s
	IEEE 802.11g:	up to 54 Mbit/s
	IEEE 802.11b:	up to 11 Mbit/s
WPS PBC	Configuration at the push of a button	
Antenna dimensions	Length:	10.9 cm
	Diameter:	1.0 cm
Weight	32 g	
Gain	2 dBi	

Table 4: USB WLAN adapter details

For the bandwidth and signal quality/coverage testing, both Iperf3 and Acrylic Wi-Fi were tested, respectively. UDP speed tests were also conducted using Iperf3, providing additional information about the network, which demonstrated as being a very useful contribution on finding network bottlenecks and limitations.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

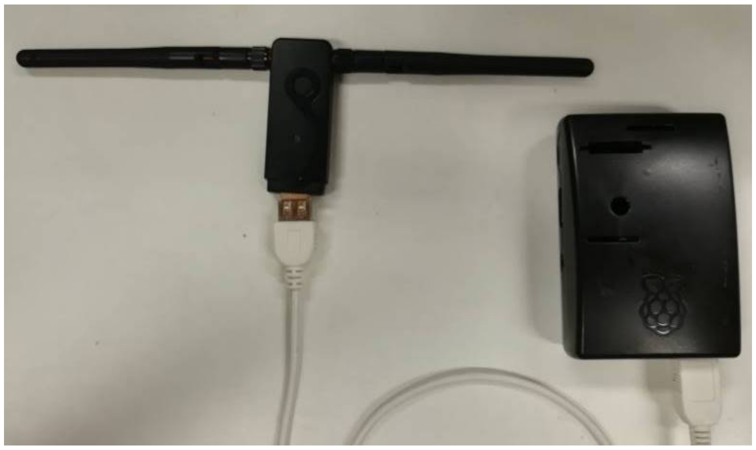


Figure 32: UMOBILE access point HW (Raspberry Pi 3 with Wi-Fi dongle extension)

The setup used is based on the UMOBILE access point hardware provided by the consortium partner FON, which is composed by a Raspberry Pi 3, equipped with a Wi-Fi dongle that carries two attachable external antennas, as shown in Figure 33.

4.3.4.1 Static tests

The tests were performed outside the facilities in Line of Sight (LoS). On the Raspberry Pi 3 was used the WLAN1 for the test bench. Measurements were taken from 10 meters to 80 meters, with 10 meter intervals. The schematization of the testing procedure is illustrated in the Figure 33.

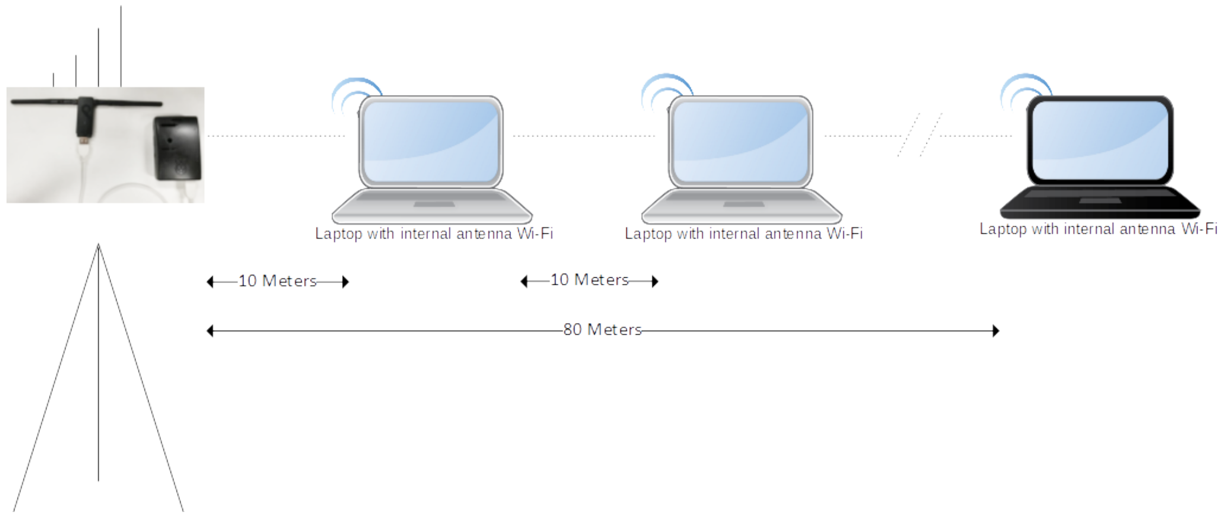

Laptop with internal antenna Wi-Fi
Laptop with internal antenna Wi-Fi
Laptop with internal antenna Wi-Fi
10 Meters
10 Meters
80 Meters

Figure 33: UMOBILE access point HW (Raspberry Pi 3 with Wi-Fi dongle extension)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

The receiving server endpoint used is a Laptop Panasonic CF-30 with internal Wi-Fi transceiver module (Intel Pro/wireless 3945ABG supporting the specification 802.11g), which has Iperf3 listening the specified port and logging received packets. The field test conditions are presented on the following figure, where the Raspberry Pi 3 and the Wi-Fi dongle antennas are attached to the tripod. The Raspberry Pi 3 is running the Iperf3 server, where the collaborator using a laptop is connecting through the wireless network provided by the hotspot. The collaborator is depicted in the figure on the right. The collaborator will move away from the server in steps of 10 meters, logging all the necessary results.

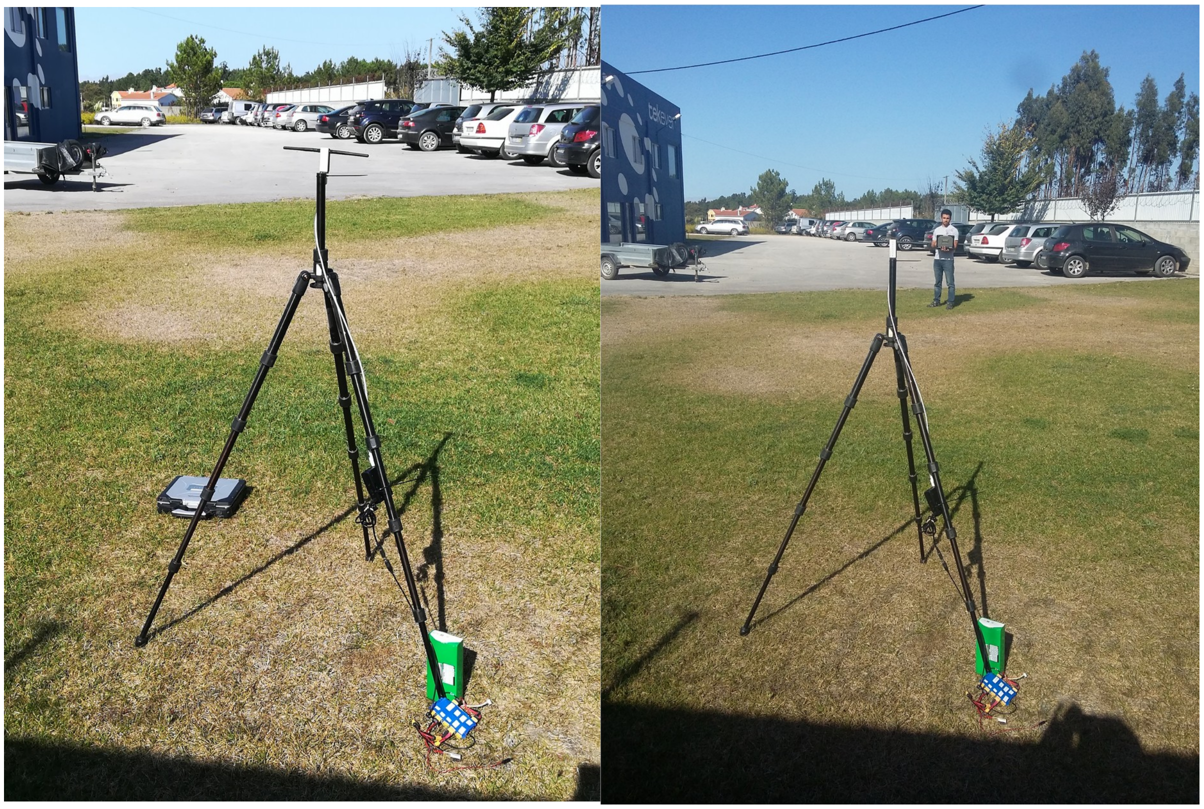


Figure 34: Static field tests setup

The following figures depict the results taken from the field tests in the previously presented test circumstances. Both bandwidth and jitter graphics on Figure 35 and Figure 36, respectively, represent the 4 tests executed at each one of the collaborator position – varying from 10 to 80 meters within 10 meters intervals. Graphics are also complemented with the average value at each position. Although certain tests present external interferences, the average line confirms the functioning of an operational Wi-Fi device, which results in a loss of bandwidth as the distance between collaborator and Wi-Fi hotspot

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

increases. Regarding the jitter, as expected, the time of delay tends to increase over the distance travelled by the signal.

The results were obtained by issuing ***#iperf3 -c <serverIpAddr> -u -i 5 -b 0 -t 60*** on the Raspberry Pi 3, through an established SSH connection with the device. The transport layer protocol is UDP with no bandwidth restrictions. The duration of each test is 60 seconds with 5 seconds report interval.

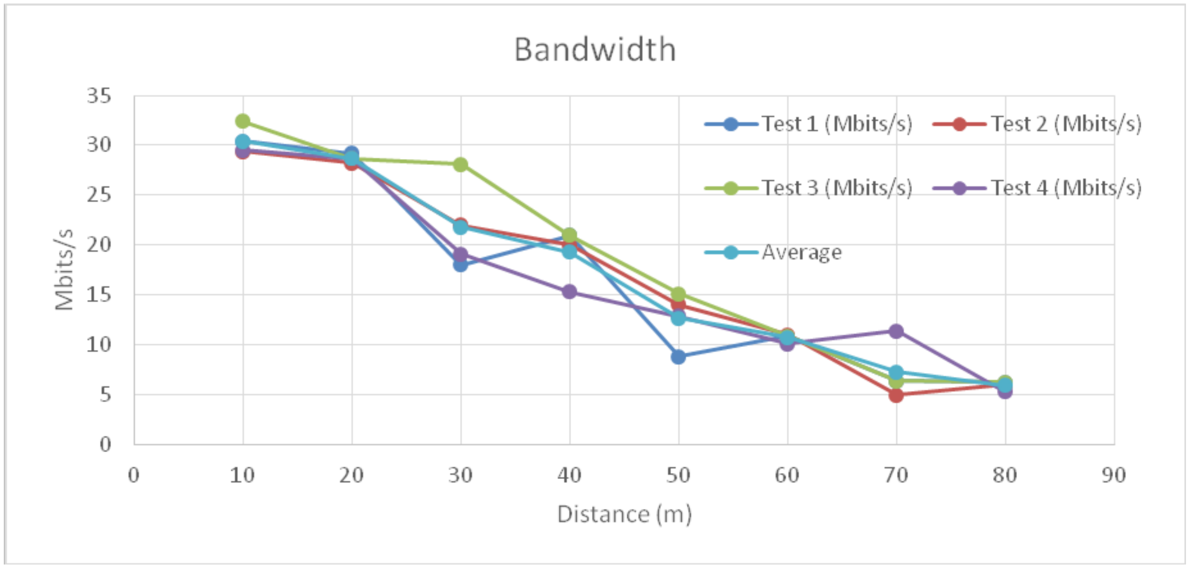


Figure 35 – Obtained bandwidth (in Mbit/s) over distance (in meters).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

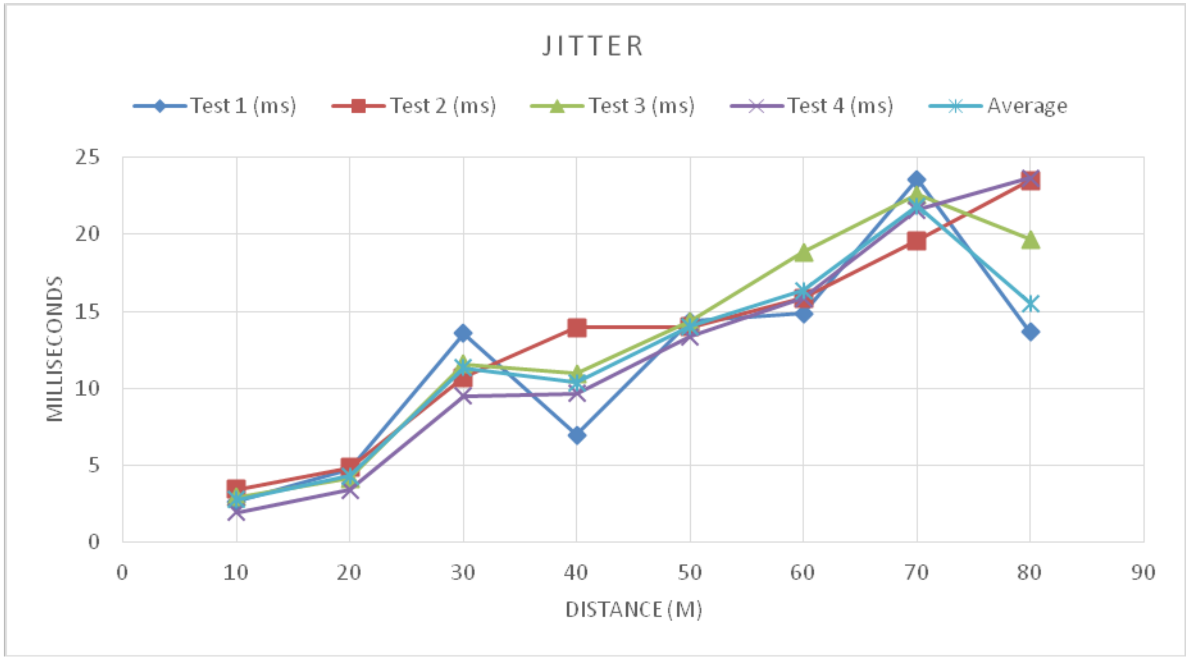


Figure 36 – Jitter in milliseconds over distance in meters.

As shown in Figure 35 and Figure 36 the bandwidth tends to decrease with the increase of Jitter. Consequently, more data packets are lost as the distance increases between collaborator and server, as depicted in Figure 37.

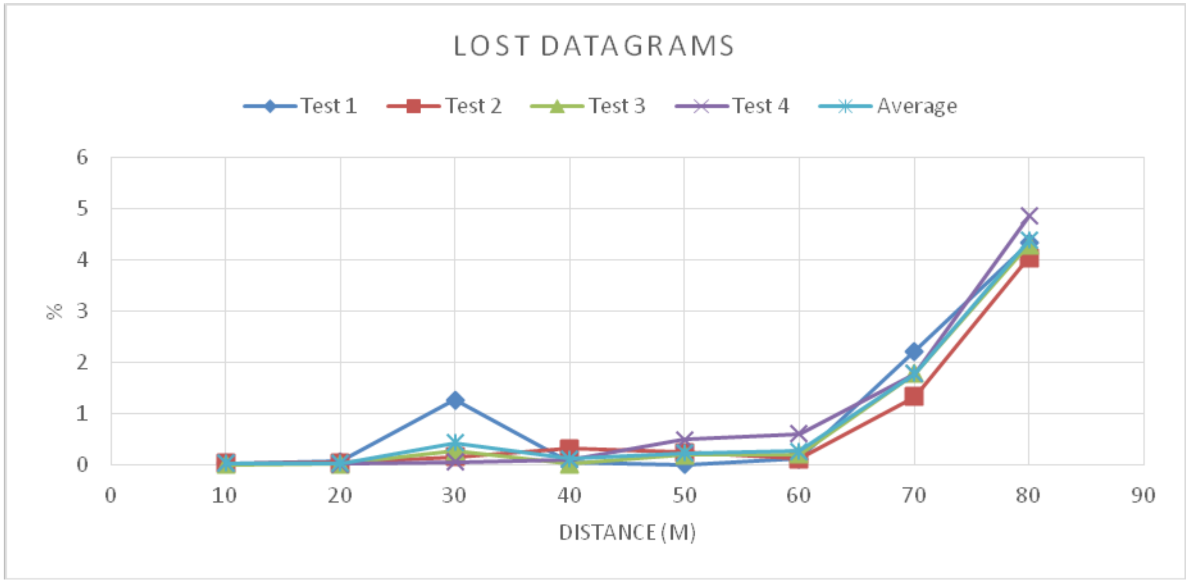
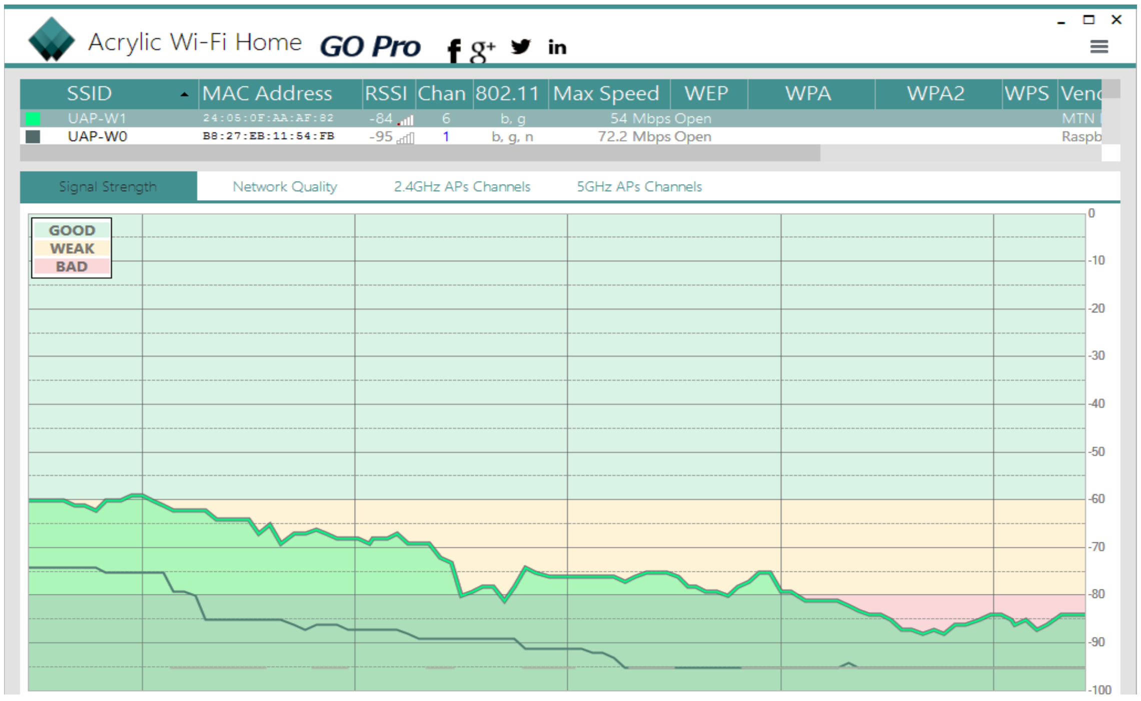


Figure 37 - Lost data packets over distance

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

Figure 38 also shows the signal strength tested using Acrylic Wi-Fi analyzer for a specific test. The Raspberry Pi remained still while the device with the Wi-Fi analyzer moves away from it. The signal strength decreases to a bad level when it passes the 60m mark. After this mark, as shown in 9, there is a significant increase of lost data packets. After the 80 meters mark, there was also an increased difficulty on establishing a reliable connection with the Iperf3 server, running in the Wi-Fi hotspot provider (Raspberry Pi 3). Consequently, recurrent time-outs occurred during the process of connection between server and collaborator. This was the main reason to stop the static tests at the mark of 80 meters.


Acrylic Wi-Fi Home GO Pro

	SSID	MAC Address	RSSI	Chan	802.11	Max Speed	WEP	WPA	WPA2	WPS	Venc
🟩	UAP-W1	24:05:0F:AA:AF:82	-84	6	b, g	54 Mbps	Open				MTN
■	UAP-W0	B8:27:EB:11:54:FB	-95	1	b, g, n	72.2 Mbps	Open				Raspb

Figure 38: Signal strength over distance, for both WLAN1 and WLAN0.

4.3.4.2 Dynamic test

The dynamic test main goal was to test the same hardware (Raspberry Pi + Wi-Fi dongle), used on the static tests presented before, but now properly integrated in an UAV that takes off with an already established communication link to the ground server. The same test bench was used as on static tests, recurring to the Iperf3 network tool for performance parameter recording. On the ground, an Iperf3 server waits for a collaborator's connection (issued from the UMOBILE access point - Raspberry Pi 3 on the UAV), in order to run the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

connection. Therefore, this test was elaborated fundamentally to validate the integration of the Raspberry Pi 3 HW with the UAV.

A schematic of the dynamic testing procedure is represented in the following figure. The UAV – TEKEVER's AR3 – performs a loiter (circles over a fixed location on the ground) at 50 meters altitude over the ground server, which is composed of a laptop with internal Wi-Fi transceiver module, as tested in the static case.

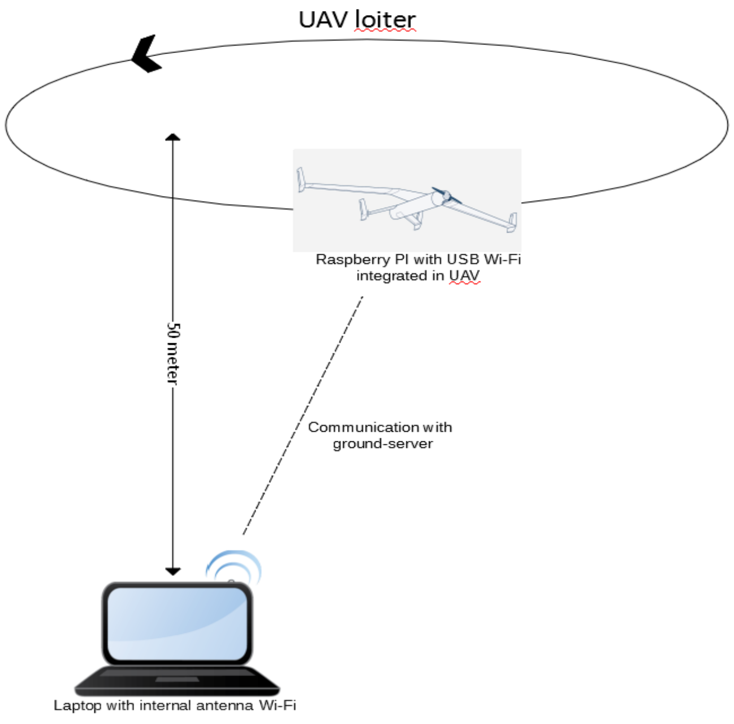
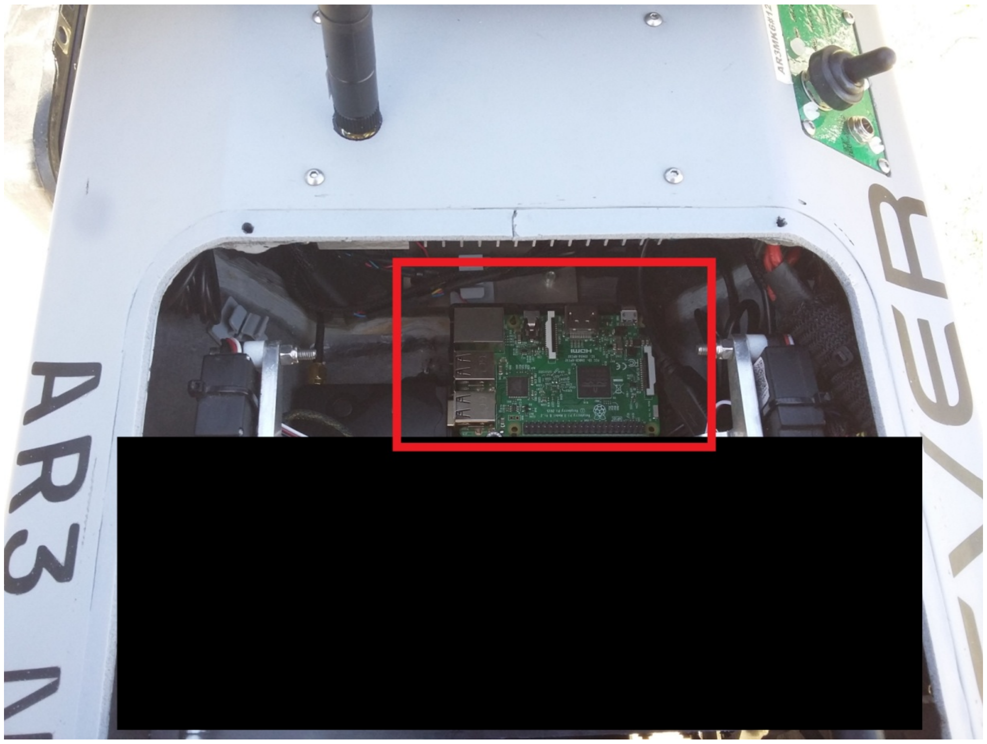

UAV loiter
Raspberry PI with USB Wi-Fi integrated in UAV
50 meter
Communication with ground-server
Laptop with internal antenna Wi-Fi

Figure 39 - Operational diagram for dynamic tests

The UAV integration work is shown on the following figures, in which it is possible to see the external Wi-Fi antennas attached to AR3's fuselage, as well as the UMOBILE access point (Raspberry Pi), identified by the red box. The final choice to carry the payload was the AR-3 due to the restricted space to carry extra payloads on the smaller AR-4 aircraft. Since the goal of this experiment was to find the maximum coverage achieved by the UMOBILE hardware, the use of AR-3 as a medium-range UAV had little influence on the final results.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124



[redacted]

Figure 40: Rasperry pi 3 on the AR3, identified by the red box

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

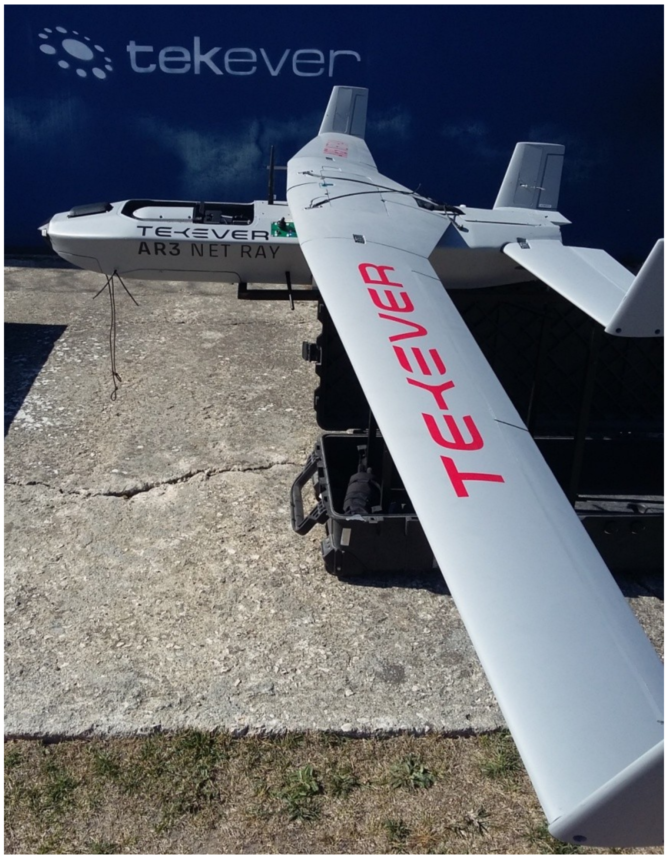


Figure 41: TEKEVER AR3

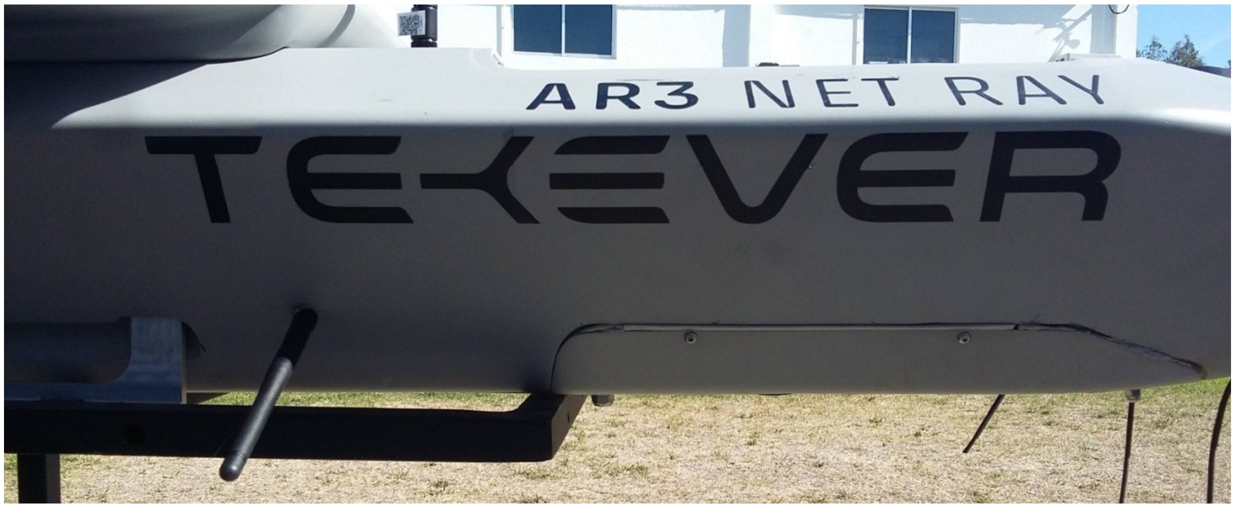


Figure 42: TEKEVER'S UAV AR3 with UMOBILE access point antenna

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

The obtained results are shown in the following figure. As stated, the collaborator loses communication with the server at approximately 130 meters - in accordance with the obtained static results, in which the maximum distance is approximately 80 meters. As is possible to notice, there is a decrease on lost datagrams when the bandwidth increases. This is an expected behavior. Having improved bandwidth the datagrams should have higher success rates of arrival to the server.

On an overall view, there is an excessive rate of data lost even when the UAV is near the server. This means that the hardware used in the test would have to be improved if a reliable link is required.

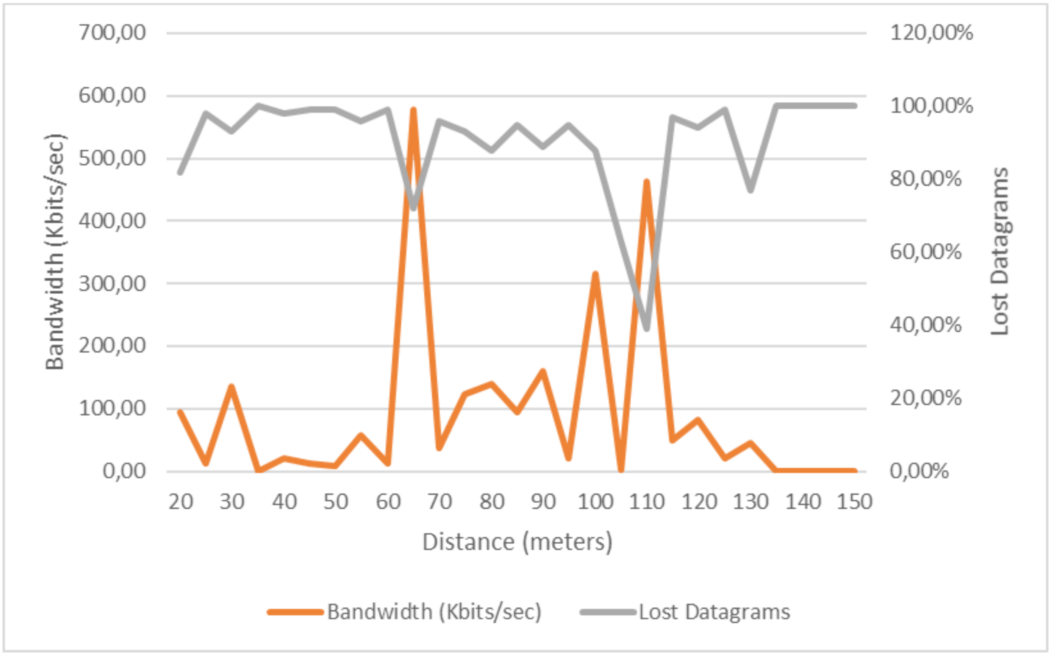


Figure 43 – Obtained results for lost datagrams in function of the bandwidth and the distance between user and server.

4.3.4.3 Conclusions

In conclusion, the results achieved with these tests on the ground and on the UAV allow us to determine the operational activity of the presented devices for both static and dynamic situations:

The involved devices demonstrated the same behavior as common or commercial WiFi devices currently available. This confirms, as expected, that the requirements for the planned tests of Section 4.3 are not totally achieved, as it is necessary to operate with

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

devices that allow a stronger transmission power. As such, the team will use a specific radio in the UAV's payload bay to provide connectivity between user devices on the ground and the UMOBILE AP on board the aircraft. This will ensure adequate range without compromising the safety of flight of the UAV.
Moreover, the tests made led the team to consider the use of different UAVs such as rotorcraft or other fixed wing aircraft capable of hovering or of reduced ground speeds and smaller loiter circuits. These characteristics appear to be desirable as we believe they will allow for longer times on target (e.g. over end-user devices) and are expected to improve the setup of the connection between ground and aircraft. These tests are reported in D5.5.
Finally, additional characterization tests will be carried out to verify performance gains obtained using NDN versus using regular IP over Wifi (namely lost datagrams and delays). These will be reported upon in D5.5.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

5. Conclusions

In this deliverable we have provided the progress of the integration of UMOBILE architecture and its components; the interaction between the components; the strategy for an overall evaluation of performance and efficiency through the proof-of-concept.

The proof-of-concept, based on two specific demos, has been updated respect to the D5.4 “Proof-of-Concept (1), published in M18.

The final Annex is the how-to guide to access and use the UMOBILE Lab from the Internet.

This project has received funding from the European Union's Horizon 2020 research and innovation programme
under grant agreement No 645124

6. References

[1] UMOBILE Project, “D.3.3 - UMOBILE ICN layer abstraction initial specification”, February 2016

[2] UMOBILE Project, “D.3.1 - UMOBILE architecture report (1)”, May 2016

[3] UMOBILE Project, “D.2.2 - System and Network Requirements Specification”, March 2016

[4] Luis. Amaral, Rute. C. Sofia, Paulo. Mendes, and Waldir. Moreira, “Oi! – opportunistic data transmission based on Wi-Fi direct,” in Proc. of IEEE INFOCOM (demo), San Francisco, USA, April 2016.

[5] [raspi-image] https://github.com/umobileproject/raspi-image

[ICN17Demo]Christos-Alexandros Sarros, Adisorn Lertsinsrubtavee, Carlos Molina-Jimenez, Konstantinos Prasopoulos, Sotiris Diamantopoulos, Dimitris Vardalis and Arjuna Sathiaseelan , “ICN-based Edge Service Deployment in Challenged Network”, Proc. 4th ACM Conf. on Information-Centric Networking (ICN 2017), Demo session, Berlin, Sep. 26-28, 2017

[6] Christos-Alexandros Sarros, Sotiris Diamantopoulos, Sergi Rene, Ioannis Psaras, Adisorn Lertsinsrubtavee, Carlos Molina-Jimenez, Paulo Mendes, Rute Sofia, Arjuna Sathiaseelan, George Pavlou, Jon Crowcroft, Vassilis Tsaoussidis, "Connecting the Edges: A Universal, Mobile centric and Opportunistic Communications Architecture", IEEE Communication Magazine, February 2018 - to appear

[7] Seweryn Dynerowicz, Paulo Mendes, "Named-Data Networking in Opportunistic Networks", in ACM ICN, Berlin, Germany, September 2017.

[8] Omar Aponte, Paulo Mendes, "Now@ - Content Sharing Application over NDN", in ACM ICN, Berlin, Germany, September 2017

[9] Zhenkai Zhu and Alexander Afanasyev. 2013. Let’s ChronoSync: Decentralized Dataset State Synchronization in Named Data Networking. In Proceedings of the IEEE ICNP, 2013.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

7. Annex A. Remote access to the UMOBILE lab

7.1 Remote access from Windows OS

The UMOBILE Lab is composed by two networks, to permit different kinds of tests. We have:

- UMOBILE network, IP routed by the OSPF protocol;
- TEST network, for devices handling (over ethernet), in order to guarantee accessibility during the change of the UMOBILE Lab wireless network.

To gain remote access to the UMOBILE Lab, go through the following procedure:

1. Open Control panel and select Network and Sharing center.

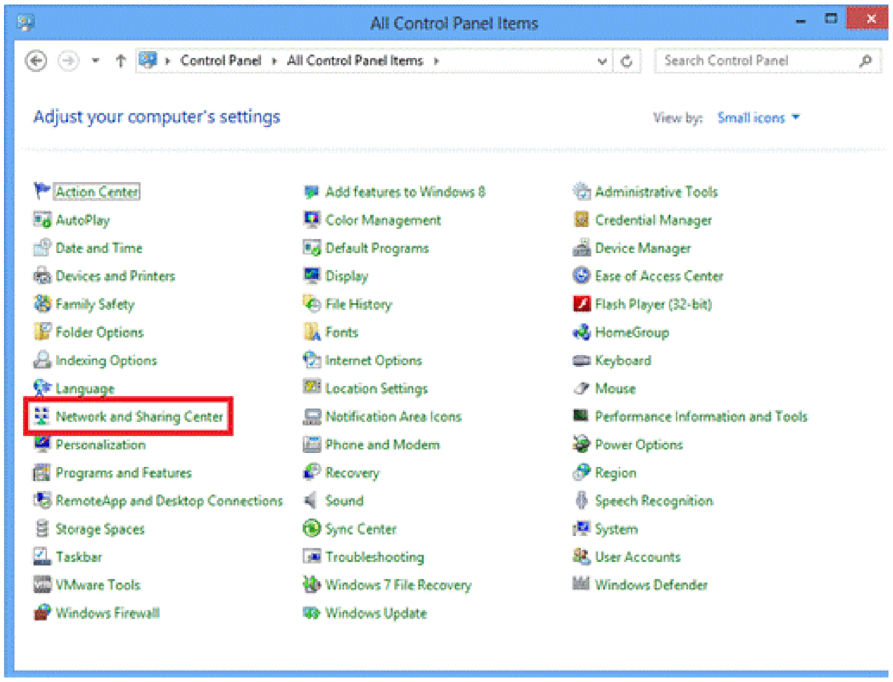
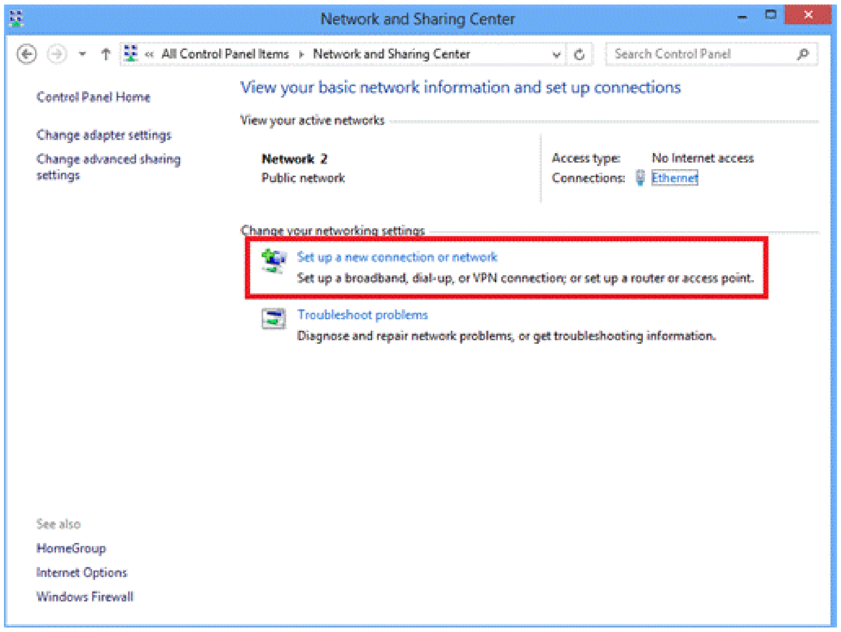


Figure 44: Network and Sharing center on Control panel

2. Choose **Set up a new connection or network** option.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124


Network and Sharing Center

All Control Panel Items ▸ Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

View your active networks

Network 2
Public network

Access type: No Internet access
Connections: Ethernet

Change your networking settings

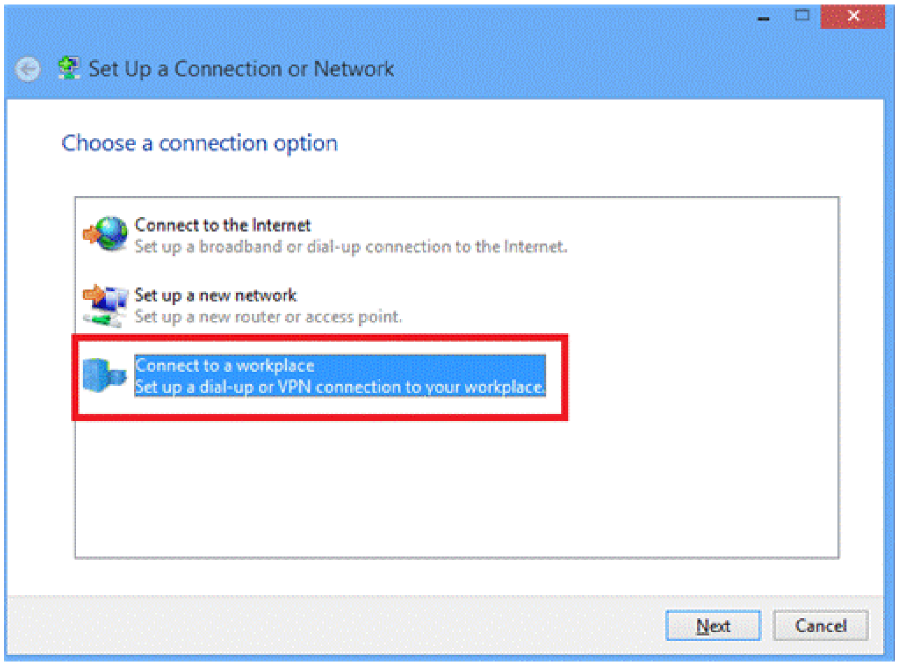
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

See also
HomeGroup
Internet Options
Windows Firewall

Figure 45: Set up a new connection or network option

3. Choose **Connect to a workplace** option and click **Next.**


Set Up a Connection or Network

Choose a connection option

Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

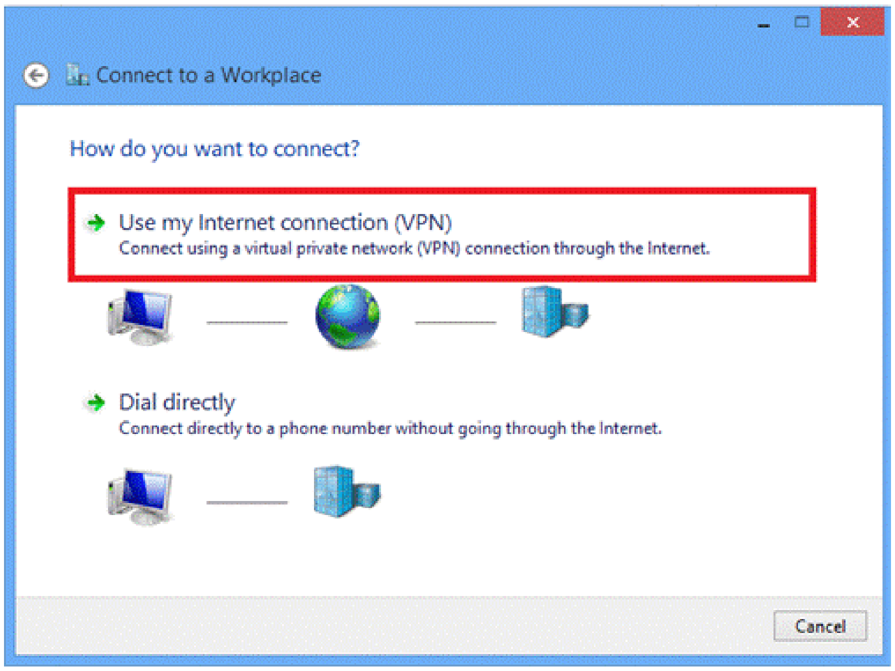
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Next Cancel

Figure 46: Connect to a workplace

4.Click **Use my Internet connection (VPN)** option.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124


Connect to a Workplace

How do you want to connect?

Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

Dial directly
Connect directly to a phone number without going through the Internet.

Figure 47: Use my Internet connection (VPN) option.

5. Enter IP address of ASA's WAN interface or FQDN and any name for VPN adapter which is locally significant and click **Create.**

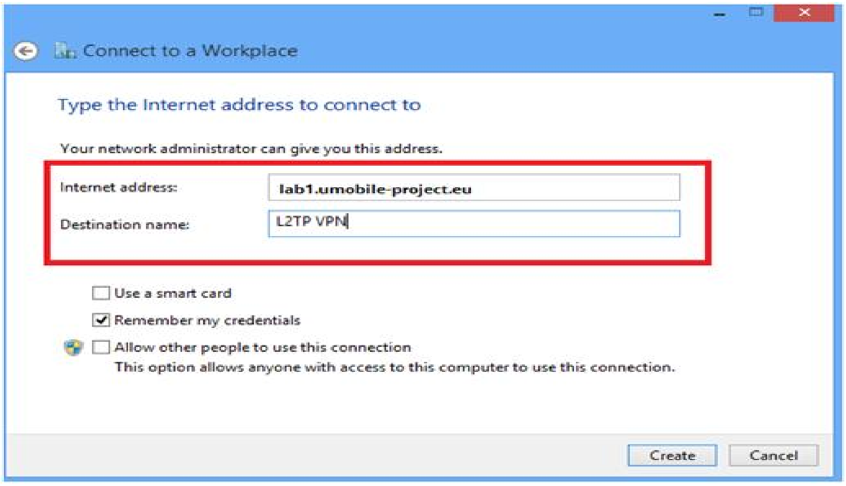
Server: **lab1.umobile-project.eu**

VPN Type: **L2TP/IPSec (Layer 2 Tunneling Protocol with IPsec)**

Advanced properties use preshared Key: **password**

Authentication Protocol allow only: **PAP**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124


Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: lab1.umobile-project.eu

Destination name: L2TP VPN

☐ Use a smart card

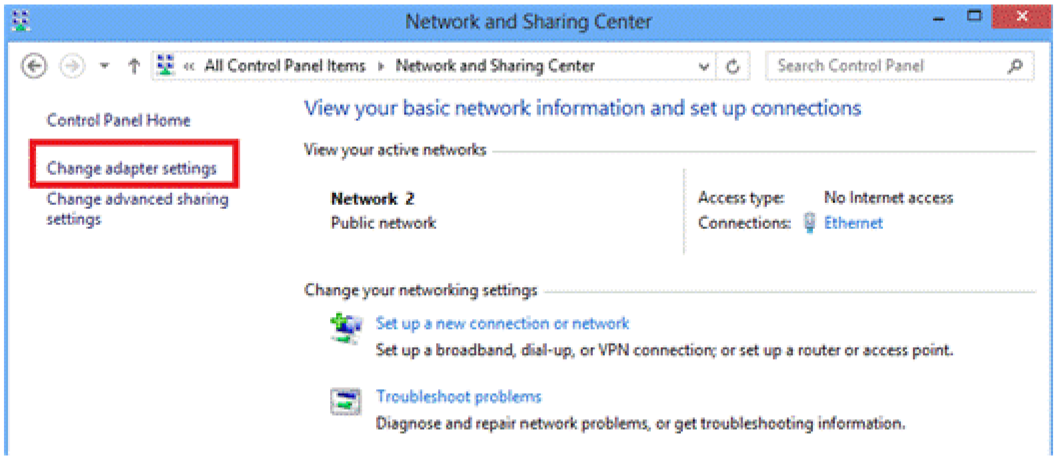
☑ Remember my credentials

☐ Allow other people to use this connection

This option allows anyone with access to this computer to use this connection.

Figure 48: Create Connection

6. On Network and Sharing Center, choose **Change adapter settings** option on the left pane of the window.


Network and Sharing Center

« All Control Panel Items ▸ Network and Sharing Center

View your basic network information and set up connections

View your active networks

Network 2
Public network

Access type: No Internet access
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Figure 49: Change adapter settings

7. Right click the recently created adapterfor L2TP VPN and choose **Properties.**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

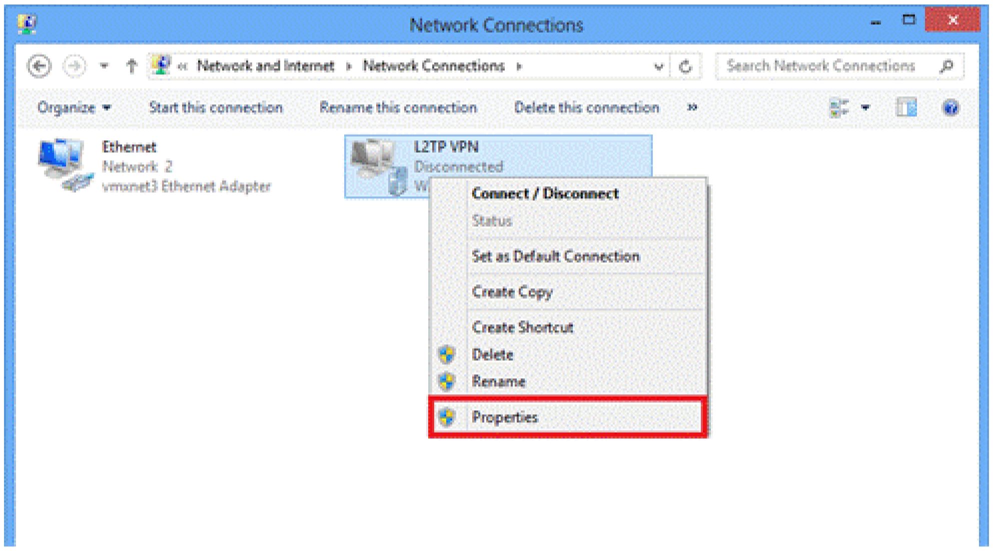
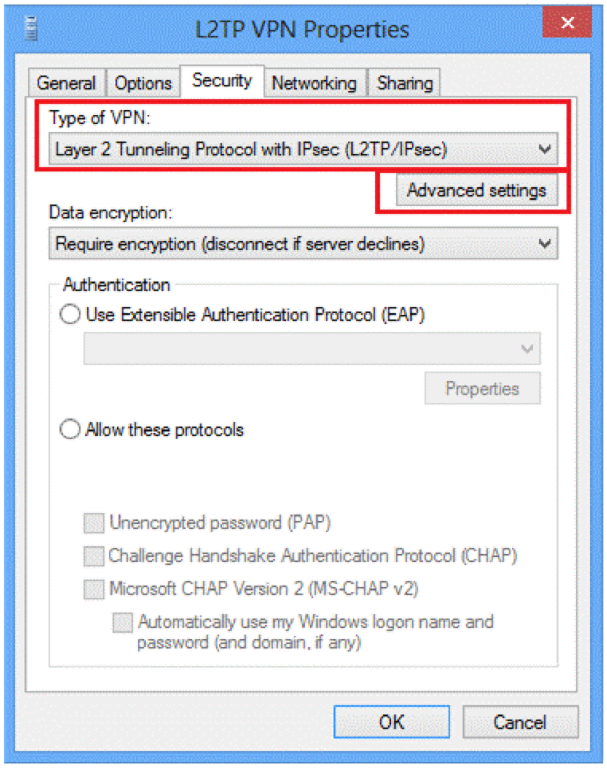


Figure 50: L2TP VPN choose Properties

8. Navigate to **Security** tab, choose the Type of VPN as **Layer 2 Tunneling Protocol with IPsec (L2TP/Ipsec)** and then click on **Advanced settings.**



Type of VPN: Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Data encryption: Require encryption (disconnect if server declines)

Use Extensible Authentication Protocol (EAP)

Allow these protocols

Unencrypted password (PAP)

Challenge Handshake Authentication Protocol (CHAP)

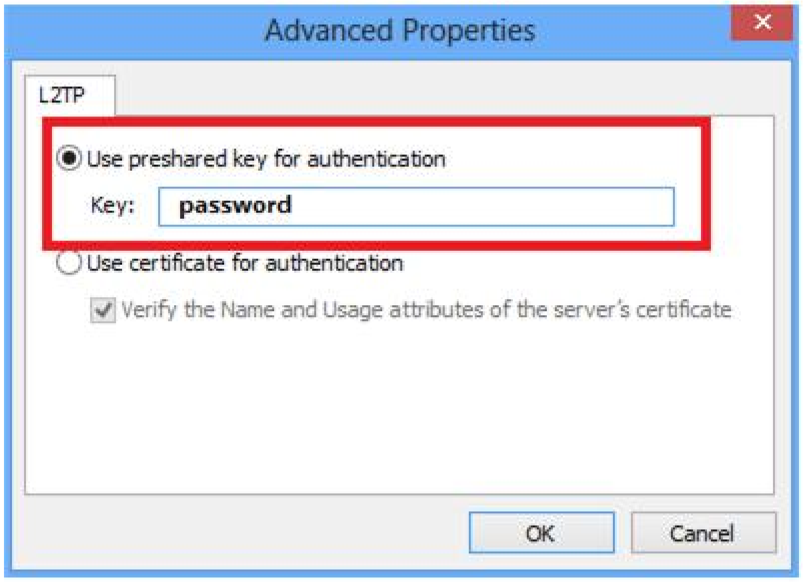
Microsoft CHAP Version 2 (MS-CHAP v2)

Automatically use my Windows logon name and password (and domain, if any)

Figure 51: L2TP VPN Properties

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

9. Enter the preshared key as the same mentioned in tunnel-group **DefaultRAGroup** and click **OK**. In this example, C!sc0@123 is used as the pre-shared key.



Advanced Properties

L2TP

(●) Use preshared key for authentication

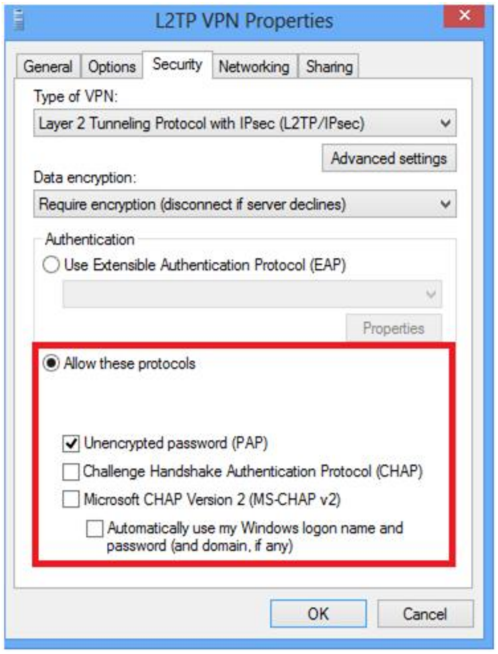
Key: password

( ) Use certificate for authentication

[✓] Verify the Name and Usage attributes of the server's certificate

Figure 52: Preshared key

10. Choose the authentication method as Allow these protocols and ensure that only "**Unencrypted password (PAP)** checkbox is checked and click **OK.**



L2TP VPN Properties

Type of VPN:

Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Data encryption:

Require encryption (disconnect if server declines)

Authentication

( ) Use Extensible Authentication Protocol (EAP)

(●) Allow these protocols

[✓] Unencrypted password (PAP)

[ ] Challenge Handshake Authentication Protocol (CHAP)

[ ] Microsoft CHAP Version 2 (MS-CHAP v2)

[ ] Automatically use my Windows logon name and password (and domain, if any)

Figure 53: Unencrypted password (PAP)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

11. Under network connections, right click on L2TP VPN adapter and choose **Connect/Disconnect.**

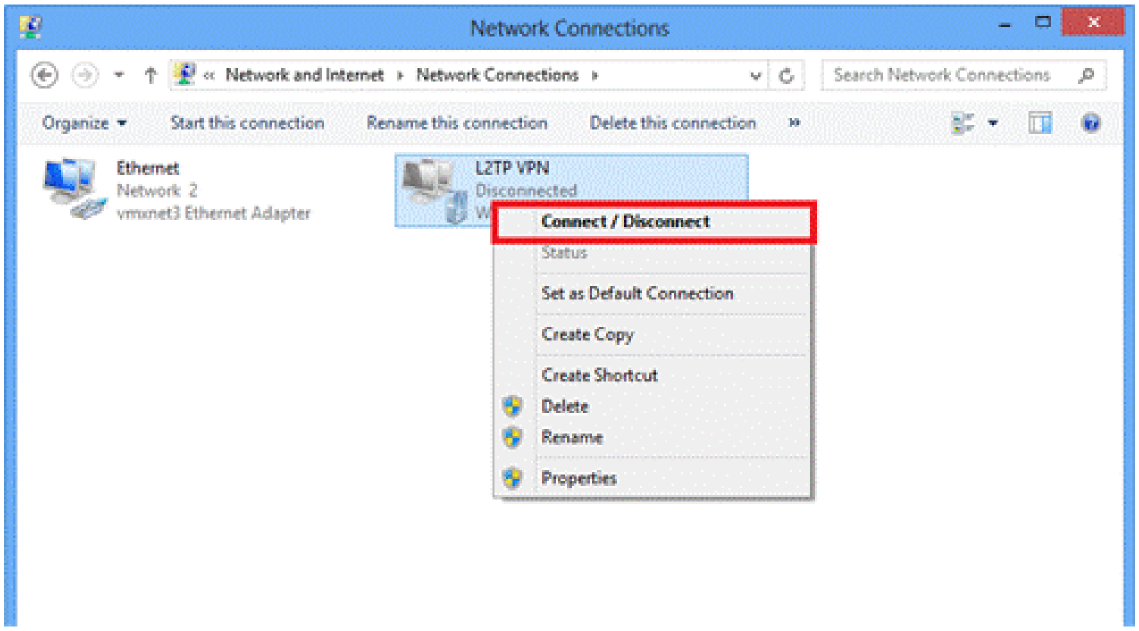


Figure 54: L2TP VPN Connect/Disconnect.

12. Networks icon will pop up and click **Connect** on L2TP VPN connection.

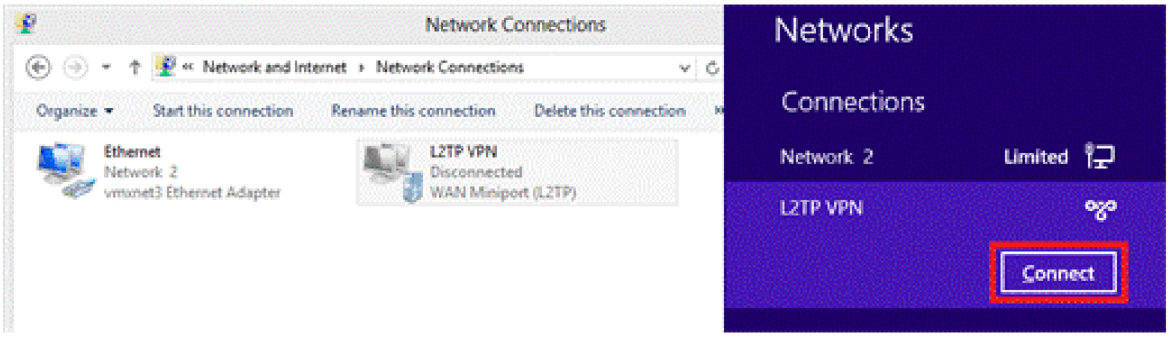
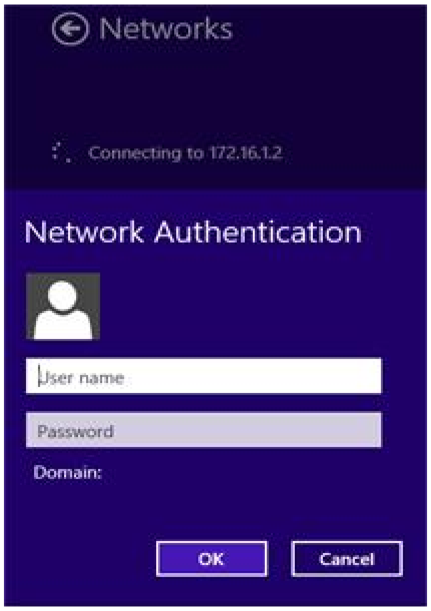


Figure 55: Connect on L2TP VPN connection

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

13. Enter the user credentials and click **OK**.


Networks

Connecting to 172.16.1.2

Network Authentication

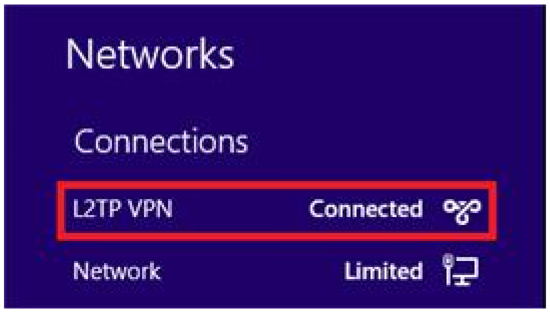
User name

Password

Domain:

Figure 56: User credentials

If the required parameters are matched on both the ends, L2TP/IPsec connection will be established.


Networks

Connections

L2TP VPN	Connected
Network	Limited

Figure 57: L2TP/IPsec connection established

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

2) Once logged into UMOBILE Lab, you have the devices shown in Table 5.2 at your disposition either through ssh or http.

In addition to devices, you have at your disposition:

- UMOBILE website and UMOBILE project-wiki;
- Internet access through a captive portal (see Figure 4.2.4), using the same username/password as L2TP;
- The Drive ---a common document repository.

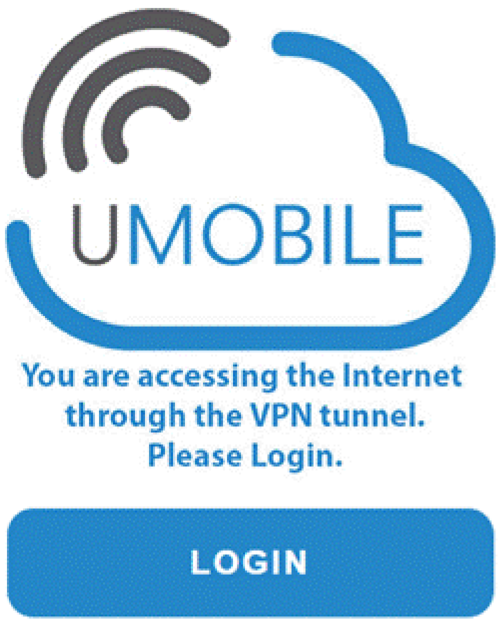

UMOBILE
You are accessing the Internet through the VPN tunnel. Please Login.
LOGIN

Figure 58: UMOBILE testbed: captive portal

3) Perform your test. For example, let us see how to install an App in an Android device. Observe that A5BB-x devices use Android 5.1 and, having their IP addresses, one can access them with the ADB (Android Debug Bridge) over TCP/IP.

1. Download the App of interest from the Internet, that is, its apk file, for example, **myapp.apk**
2. Use "**adb connect ipaddress:5555**"
3. Use "**adb install myapp.apk**".

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

4. Use "**adb shell**" to connect to the device and use the application that you have installed.

From practical experience we are certain that the UMOBILE Lab can be used for testing the following situations:

1. NDN communication between the nodes of the lab connected via cable and via Wi-Fi
2. Test automation through the robot
3. Service migration via docker on SEG node

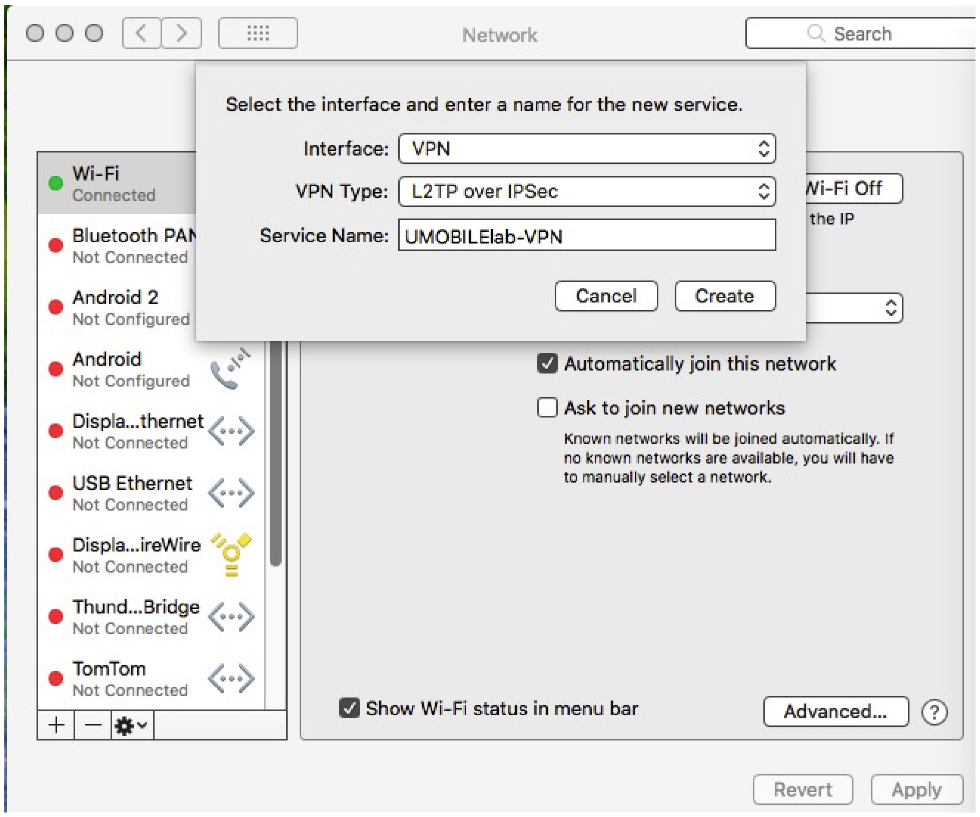
The usage of the Lab to simulate the PoC1 is described under the Section 'Proof of Concept'.

7.2 Remote access from Mac OS

The following example was executed from the Computer Laboratory of the University of Cambridge using a MacBook Air, running macOS High Sierra Version 10.13.1.

1. Set up a VPN network service: Open the network pop up window and type in the *interface* and *VPN type* parameters shown in Figure 59. (*Service Name* is any string you chose) and press *Create*.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124


Select the interface and enter a name for the new service.

Interface: VPN

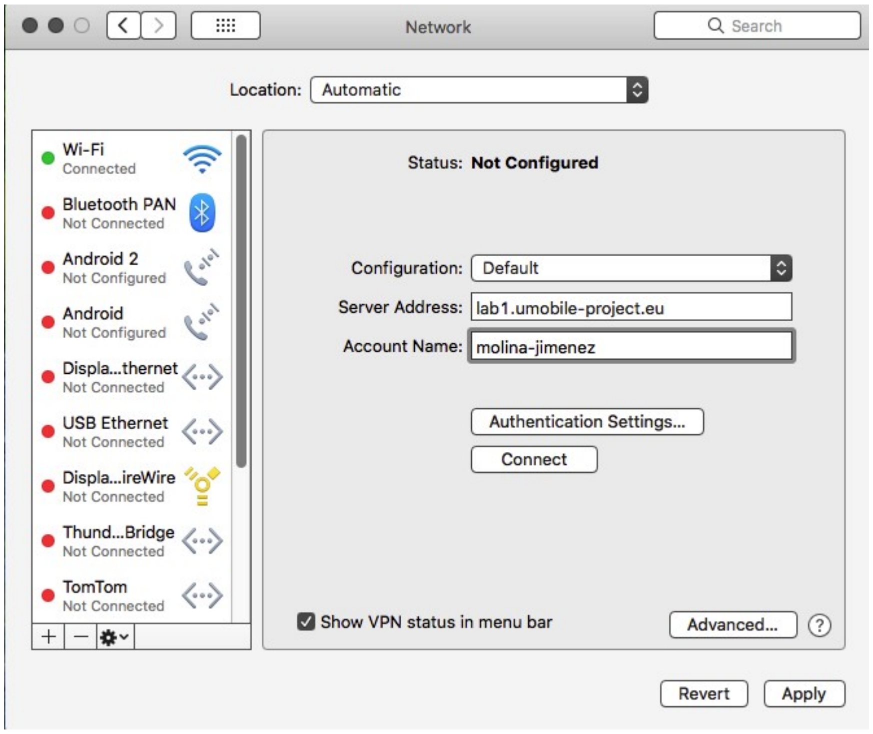
VPN Type: L2TP over IPSec

Service Name: UMOBILElab-VPN

Figure 59: A Creation of a VPN service: Interface and VPN Type

2. Fill in the *Server Address* and *Account Name* as shown in Figure 60. and press *Authentication Settings…. molina-jimenez* is the logging name that you have been previously granted by the administrator of the UMOBILE lab.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124


Network

Location: Automatic

Wi-Fi Connected
Bluetooth PAN Not Connected
Android 2 Not Configured
Android Not Configured
Displa...thernet Not Connected
USB Ethernet Not Connected
Displa...ireWire Not Connected
Thund...Bridge Not Connected
TomTom Not Connected

Status: Not Configured

Configuration: Default
Server Address: lab1.umobile-project.eu
Account Name: molina-jimenez

Figure 60: Creation of a VPN service: Server Address and Account Name

3. Fill in the *Password and Shared Secret boxes* shown in Figure 61 and press *OK*.

   - *Password:* is the password that you use to log into the UMOBILE lab under the Account Name of the previous Figure 60.
   - *Shared Secret:* the shared secret is the string *password*. Type it in the box.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

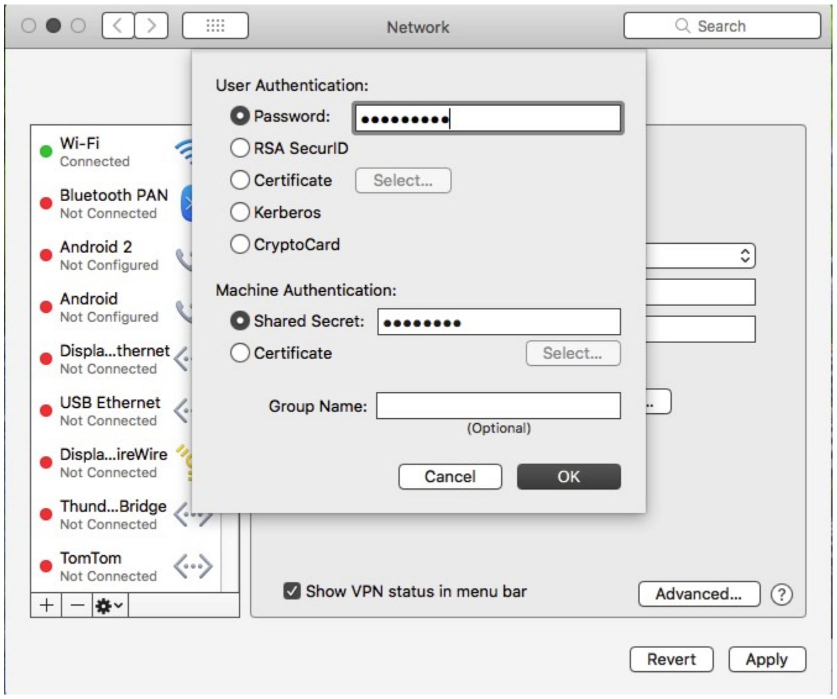
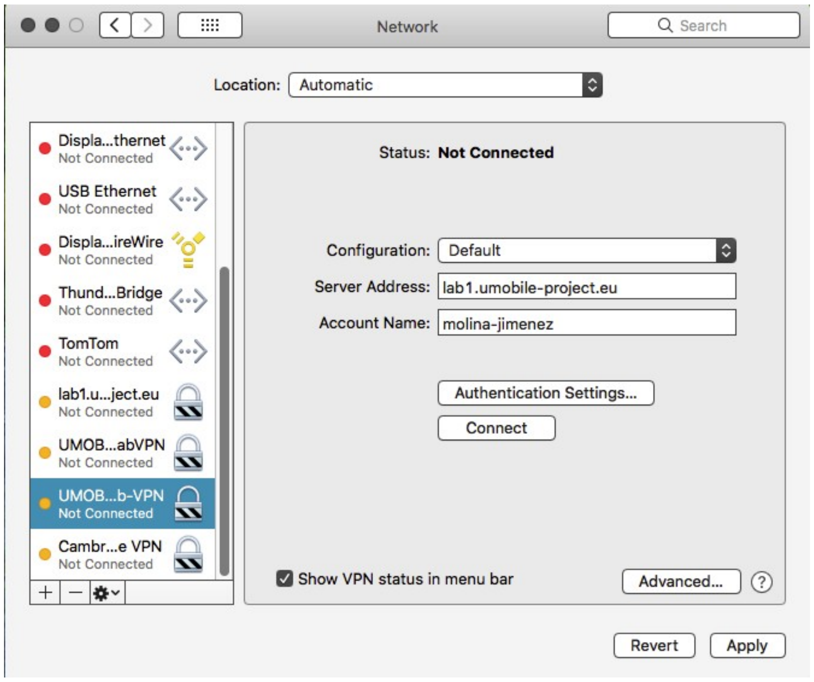


Figure 61: Creation of a VPN service: Password and Shared Secret

4. In Figure 62 press *Apply* to record all the configuration parameters.

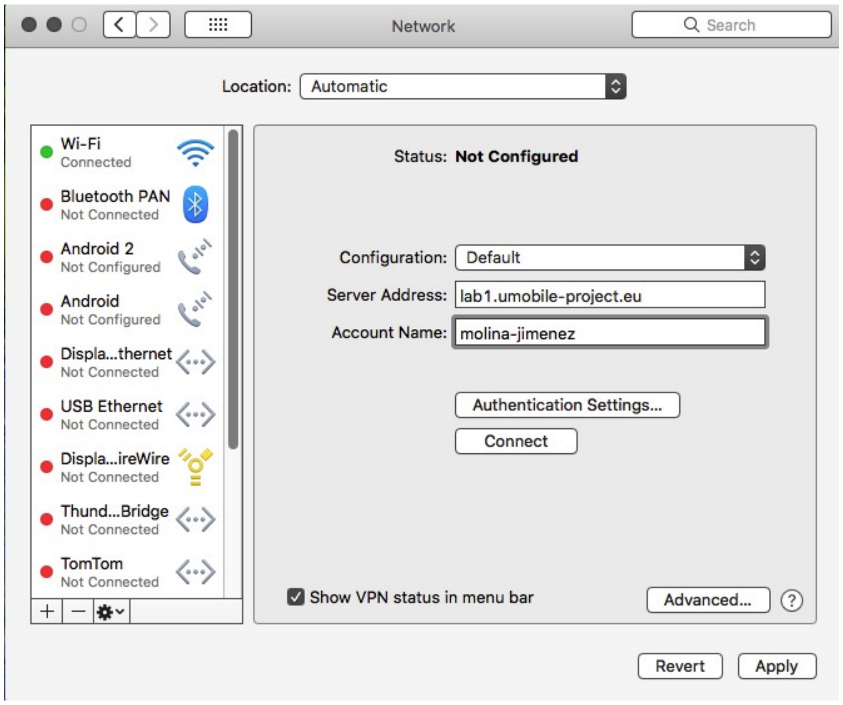


Status: Not Connected
Configuration: Default
Server Address: lab1.umobile-project.eu
Account Name: molina-jimenez

Figure 62: Creation of a VPN service: press Apply

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

5. The UMOBILElab-VPN network service is now ready for connection as shown in Figure 63.


Network

Location: Automatic

Wi-Fi
Connected
Bluetooth PAN
Not Connected
Android 2
Not Configured
Android
Not Configured
Displa...thernet
Not Connected
USB Ethernet
Not Connected
Displa...ireWire
Not Connected
Thund...Bridge
Not Connected
TomTom
Not Connected

Status: **Not Configured**

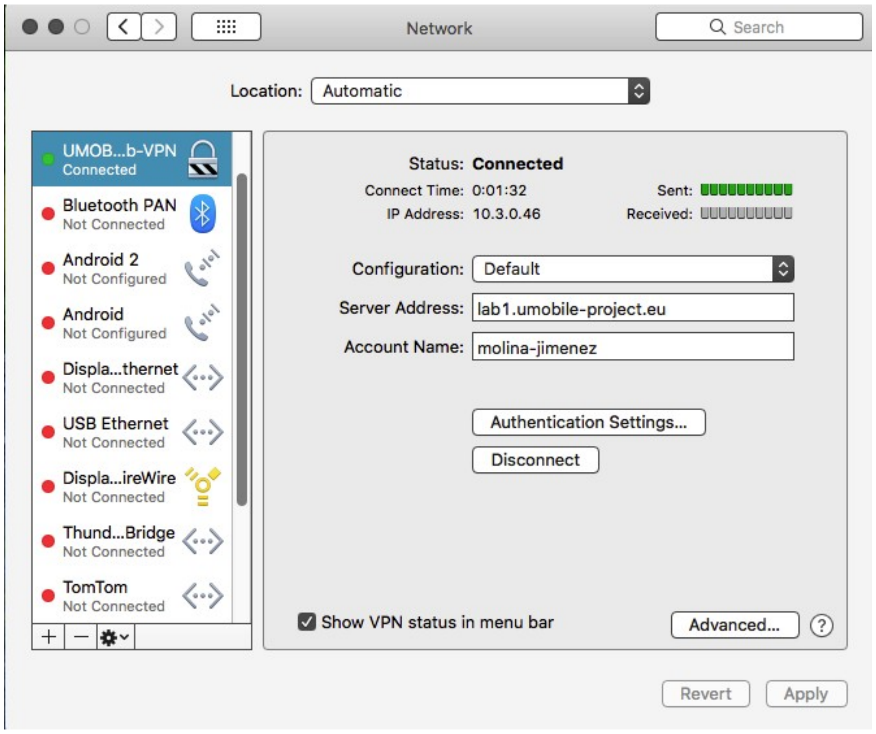
Configuration: Default
Server Address: lab1.umobile-project.eu
Account Name: molina-jimenez

☑ Show VPN status in menu bar

Figure 63: Creation of a VPN service: ready for connection

6. To connect to the UMOBILE lab, press Connect. You will see the screen shown in Figure 64. The VPN connection is established (see green bars near Sent, top, right) and ready for accessing the facilities of the UMOBILE lab.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124


Network
Search
Location: Automatic
UMOB...b-VPN Connected
Bluetooth PAN Not Connected
Android 2 Not Configured
Android Not Configured
Displa...thernet Not Connected
USB Ethernet Not Connected
Displa...ireWire Not Connected
Thund...Bridge Not Connected
TomTom Not Connected
Authentication Settings...
Disconnect
Advanced...
Revert
Apply

Status: **Connected**
Connect Time: 0:01:32
IP Address: 10.3.0.46
Sent:
Received:
Configuration: Default
Server Address: lab1.umobile-project.eu
Account Name: molina-jimenez
✓ Show VPN status in menu bar

Figure 64: Creation of a VPN service: connected

Press *Disconnect* to disconnect from the UMOBILE lab. To establish another connection, you press Connect again.

7.3 Remote access through SSH

Once the VPN connection is in place, *molina-jimenez* can access nodes of the UMOBILE lab to realise Pi_1 and Pi_2 of Fig SerMigr. We will use the devices suggested in Figure 19 (page 40) of the D5.3 deliverable [D5.3] for the realisation of POC1.

Namely, the role of Pi_1 and Pi_2 will be played by SEG-APR-1 and SEG-CAPR-1, respectively. Their IP addresses, Hostnames and other specifications are documented in Table 3 of D5.3 (pages 47-49). The same documentation is available from [UMOBILElab]. From Table 3 we can learn that both nodes run Raspbian 8 and are Docker enabled. We can learn as well that the IP address of SEG-CR-1 is 10.4.1.4 and that the IP address of and SEG-CAPR-1 is 10.100.0.26. You can log in to both devices under their *root* user using the *umxan628* password. In summary:

- SEG-APR-1 with IP= 10.4.1.4 corresponds to Pi_1
- SEG-CAPR-1 with IP=10.100.0.26 corresponds to Pi_2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

- user: *root*, password: *umxan628* for both nodes.

The devices are now ready to conduct the experiment of Figure 21. This task correspond and will be reported in deliverable D5.5. The central idea would be to test that the following functionalities of the service migration platform are operating correctly before integrating it the DTN framework using the service migration platform –DNT framework integration in the POC1.

- That Pi_1 can issue a Pull Request message against Pi_2.
- That Pi_2 can receive, the message, find and retrieve the requested image of the service and send back all the corresponding data chunks.
- When the Pi_1 receive all the data chunks, it will call the service execution function to instantiate the service (docker container). The message flow of communication between Pi_1 and Pi_2 is illustrated in Figure 65.

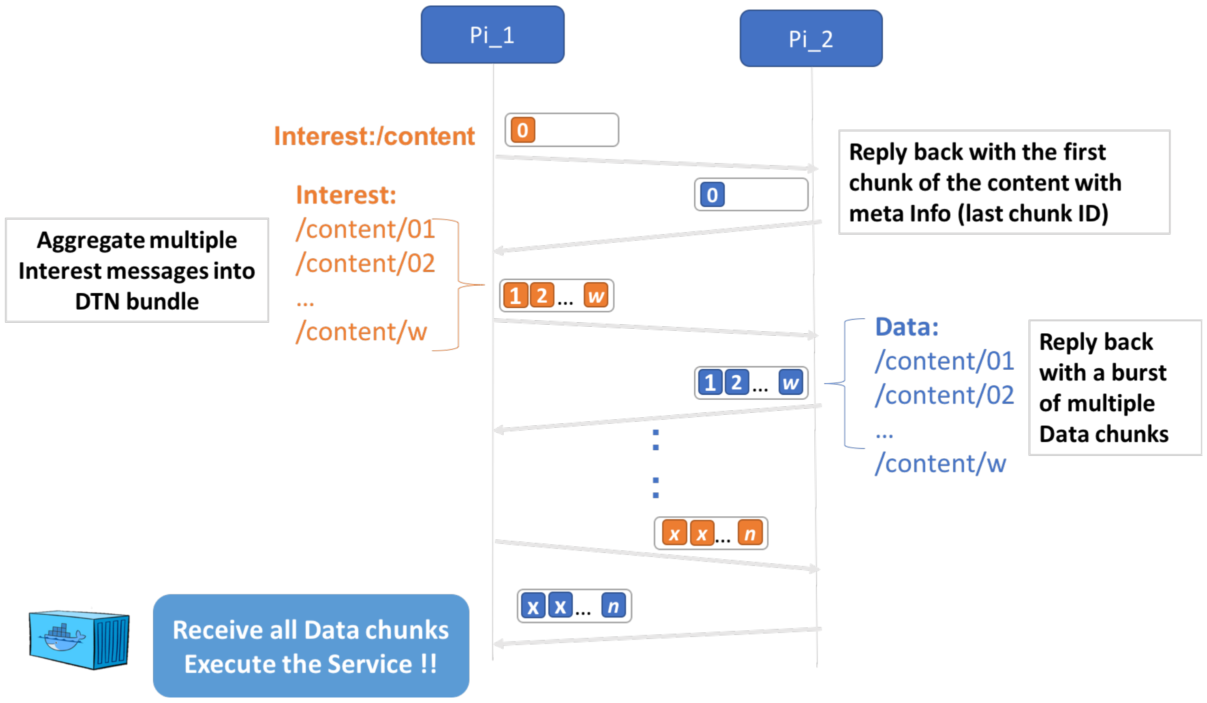

Pi_1
Pi_2
Interest:/content
0
Reply back with the first chunk of the content with meta Info (last chunk ID)
Interest:
/content/01
/content/02
...
/content/w
Aggregate multiple Interest messages into DTN bundle
1 2 ... w
Data:
/content/01
/content/02
...
/content/w
Reply back with a burst of multiple Data chunks
x x ... n
Receive all Data chunks Execute the Service !!

Figure 65: The communication flow of service migaration between Pi_1 (Consumer) and Pi_2 (Producer)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

The advantages of using the facilities of the UMOBILE lab, as opposed to using local hardware, is that the UMOBILE facilities shared by all members of the UMOBILE project and can if they are interested in, log in and experiment with the service migration platform before the actual demonstration of the POC1. In addition, members of the UMOBILE project count on the technical expertise of AFA in the configuration of the LAN and devices such as the Raspberry Pi computers. For instances, the OS of the Raspberry Pi computers have been upgraded several times.

7.4 Devices

Table 5 shows the lab components, specifying for each device the acronym used in the detailed architecture image (Figure 14). The technical specification of each device is reported in Annex A. of D5.3.

Device	**Usage**	**Ethernet**	**Additional ports**	**USB port**	**role in UM Lab**	**UM acronym**
RB493G	infrastructure	9 GE	Serial	y	CORE NETWORK	CRCAPR
RB435G	infrastructure	3 GE	Serial	y	ACCESS NETWORK	APR
R52n-M	infrastructure	-	-	-	radio add-on	-
Raspberry Pi3	infrastructure	1	HDMI	y	SERVICE EXECUTION	SEG
Raspberry Pi3	hand-held device emulation	1	HDMI	y	USER DEVICE	LBB
BPI-M2	hand-held device emulation	1	HDMI	y	USER DEVICE	A4BB
BPI-M3	hand-held device emulation	1	HDMI	y	USER DEVICE	A5BB
Tekever UAV	hand-held device	-	-	-	N	AR3
Tekever Ground Control Station	Infrastructure	1	HDMI	N	N	TEK-GCS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124

Umobile Control Station (Umobile Operation)	Infrastructure	1	HDMI	N	N	UM-CS

Table 5: Lab components overview

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 645124