A resilient, multi-access communication solution for USaR operations: the INACHUS approach

Anastasios Rigos
Institute of Communication & Computer Systems (ICCS)
National Technical University of Athens
Athens, Greece
anastasios.rigos@icccs.gr

Dimitrios Sofianos
Intrasoft International S.A
Athens, Greece
dimitris.sofianos@intrasoft-intl.com

Vasilis Sourlas
Institute of Communication & Computer Systems (ICCS)
National Technical University of Athens
Athens, Greece
v.sourlas@iccs.gr

Evangelos Sdongos
Institute of Communication & Computer Systems (ICCS)
National Technical University of Athens
Athens, Greece
esdongos@iccs.gr

Miltiadis Koutsokeras
Institute of Communication & Computer Systems (ICCS)
National Technical University of Athens
Athens, Greece
miltos.koutsokeras@iccs.gr

Angelos Amditis
Institute of Communication & Computer Systems (ICCS)
National Technical University of Athens
Athens, Greece
a.amditis@iccs.gr

Abstract— **When a disastrous event occurs and an urban area suffers from collapsed buildings, Urban Search and Rescue (USaR) teams require a fast and thorough building damage assessment, to focus their rescue efforts accordingly. After the evaluation process, their observations/results have to be transferred to their base (center of operation - COP) for further assessment and orchestration of the survival extraction actions. In this work, a communication scheme that can be used in emergency situations is introduced. The proposed solution doesn't depend on existing functional cellular networks such as GSM, 3G, 4G, etc., neither assumes Wi-Fi connectivity to the Internet, since in disaster scenarios they could be unavailable or they could have large interruptions and delays. On the contrary, we propose a low-cost solution that is easy to build and deploy and is modular to expand from a small area to a large part of an urban setup, based on the needs of the USaR activities. Particularly, a wireless mesh-network is designed to cover the needs of the first responders in the actual disaster area, whereas a long-range wireless network is designed to transfer the data securely back and forth to the center of operation.**

Keywords— Mesh Network, Wi-Fi Network, Long-Range Network, DTN, USaR.

I. INTRODUCTION

The society is increasingly expecting seamless information access at any moment and place. This expectation rides upon a plethora of recent technological advancements, culminating to the impending arrival of 5G networks, which promise even higher data rates and shorter latencies. In the heart of these is the key requirement to guarantee rapid and reliable response to information requests regardless of device capabilities, bandwidth required and network conditions. While modern networks focus on low-latency communication, this is only one part of the total information response time. To ensure guaranteed response time, the design space should not be constrained by technological advancements in terms of speed only, but should also encompass actual network resilience especially under network perturbations such as failures due to natural disasters, malicious attacks, etc.

Disaster-based failures can seriously disrupt a communication network, making its services unavailable. Such disruptions may follow from natural disasters, technology-related failures, or malicious attacks. These disruptions are observably increasing in number, intensity and scale. The problem needs to be urgently addressed, due to the lack of suitable mechanisms deployed in current networks. When network services that are part of a critical infrastructure become unavailable, commercial and/or societal problems are the inevitable result.

Even more important, when an emergency occurs, the ability to communicate is vital. This capability is needed for the general public but also for authorized professionals who are involved in any of the different emergency phases, such as prevention, mitigation or recovery. Unfortunately, real-time communication becomes a difficult task under crisis situations. Existing communication solutions exhibit restrictions to provide response in real-time conditions and additionally they cannot automatically enable mechanisms to overcome congestion problems or network unavailability issues. In this work, it is assumed that in an emergency case (mainly focused on collapsed buildings after earthquake/ terrorism events) there are data in the area of disaster gathered by the Urban Search and Rescue (USaR) teams (firemen, volunteers etc.) and these have to (i) be available among partners in the disaster field and (ii) to be transferred in a long distance where a center of operation (COP) of the USaR team is located. The communication solution should satisfy the following:

- It has to be a secure network (the transferred data should be encrypted).

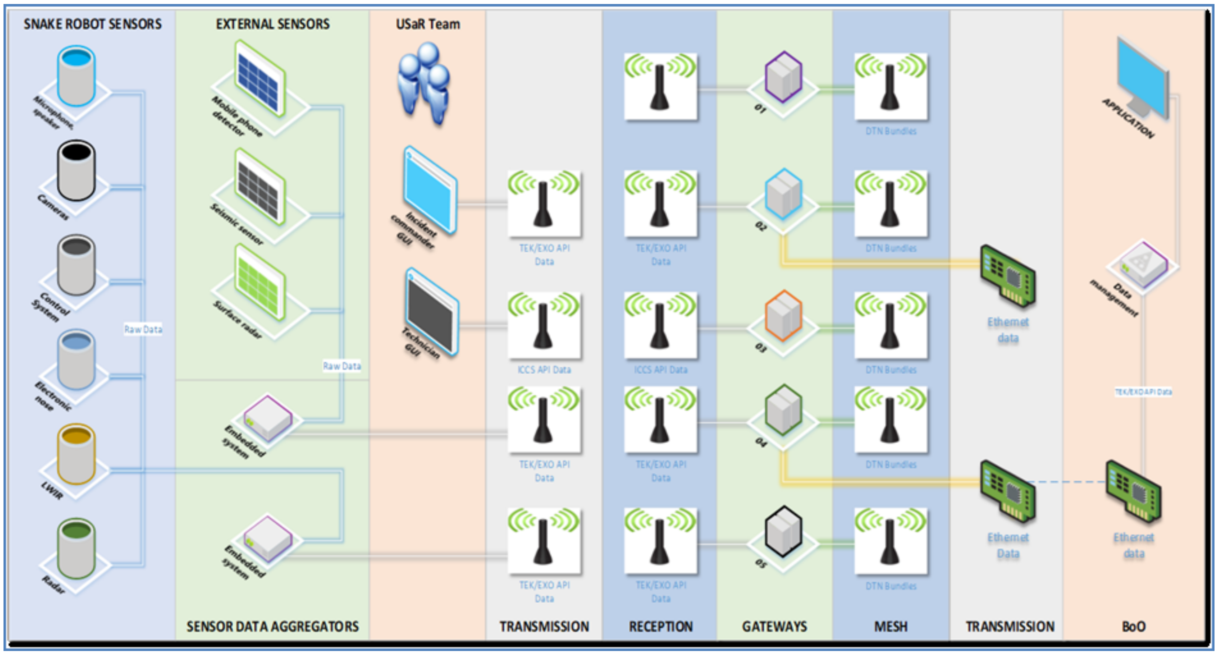

Fig. 1 The INACHUS communication solution.

- It has to store the transferred data in the case of no network connectivity (Delay-tolerant networking capabilities).
- It has to be easily accessed by the first responders; as such it should be composed by access points operating at the widely-used IEEE 802.11 Wi-Fi protocols that every handheld device (i.e., phone/tablet/PC) can support it.
- It has to be composed by resilient all weather low-powered devices, that can operate for many hours and under any possible weather condition.
- It has to be easily deployable and operational by non-communication experts (e.g., USaR first responders) and also lightweight to be transferable in the disaster area.

A. *The INACHUS approach*

In this work we describe the communication solution developed in the course of the INACHUS FP7 EU project (Fig. 1). Within INACHUS, a set of technologies and tools are developed in order to assist USaR teams in their operations during disasters. Particularly, INACHUS has developed a range of tools and sensors that can assist USaR members in their rescuing activities. The INACHUS robot acts as a mobile sensor deployment platform able to penetrate the rubble pile while carrying a) the e-nose sensor array detecting gases that indicate human presence; b) the robot radar detecting movement; c) the LWIR camera for the infrared detection of human presence; and d) microphone and speakers for the two-way communication between the trapped victims and the rescuers. Moreover, INACHUS offers sensors that are deployable in the surface of the rubbles: a) a mobile phone detector used to locate any active mobile phones in the vicinity of the worksite (potential indication of human presence); b) surface radar able to penetrate the rubble pile and detect movement indicating the presence of trapped victims; and c) ground based seismic sensors detecting noises coming from inside the rubble pile. The information generated by the sensors is combined (data fusion) in order to provide a more accurate picture enabling the responders to take better informed decisions regarding the strategies to follow so as to reach and rescue the trapped victims. To facilitate this, the project delivers the INACHUS portal and common operational picture back in the center of operation that provides access to the emergency support system and the data fusion capabilities of the framework.

B. *The INACHUS communication solution in a nutshell*

In order to allow a seamless communication of the various INACHUS components a communication solution/platform is designed to allow the interconnection between other networks (cellular, etc.), as well as to provide redundancy and recovery functionalities. A multi-layer architecture was followed for the communication and the routing as well as the mobile gateway functionality, as shown in Fig.1. The mobile gateway can be accessed by the operator, from the control center, as well as locally by the first responders, when/if needed; and also remotely controlled and maintained by specialized maintenance staff.

For extending the capabilities and range of the crisis network in case of failures and/or congestion and to provide a distributed architecture, portable gateways and a long-range communication solution are envisaged. These gateways can be positioned according to relevant and appropriate network dimensioning, even deployed by personnel where needed (i.e. mobile gateways) and they can be automatically or manually switched on. The gateways support the functionality of any other mobile USaR center as an alternative and cost effective solution in an integrated ad-hoc manner but with redundancy, extendibility and security capabilities to assure robustness, flexibility and reliability.

The rest of the paper is organized as follows: In Section II, the technical details of the proposed communication platform are presented. In Section III, an initial on-site real world evaluation of the communication platform is presented, whereas in Section IV, we conclude the paper and give pointers for future investigation.

II. Proposed Communication Solution

The proposed solution consists of two main parts. The first part is the short range wireless solution, which consists of many embedded Linux boards, each of them acting as an access point and a mesh-network node at the same time. The second part consists of the long-range communication solution. The following sections describe the hardware and software components of the embedded boards, the long-range wireless solution and finally the network topology of the network.

A. Embedded boards with mesh network (Hardware)

An embedded board was chosen in order to create a mesh network in the disaster area. This embedded board is equipped with two Wi-Fi modules (one to create a mesh-network with the other boards in the area and one to act as an access point). The embedded board selected is the Sparkgate-7 by Shiratech (Fig.2) (CPU: ARM Cortex -A5 processor at 536MHz, 512MB RAM). For the Wi-Fi, the Sparklan WUBR-508N module was selected in order to create the mesh-network between the boards and the Sparklan WUBA-171GN in order to create an access-point on each board; both modules support the wide used security protocols WEP/WPA/WPA2 and use the standard wireless protocols 802.11 b/g/n, both operating at the 2.4GHz frequency. Those Wi-Fi modules are attached using a USB-Hub on each board and a PCI antenna was attached to each of the modules (Fig.2 and Fig.3).

In order to make them self powered, a 34.5Wh battery (a 10,000mAh lithium battery) was attached to each node except the one that was connected to the long-range wireless network; the last one was connected to a 108Wh battery (a sealed lead-acid battery rated 9Ah at 12V) (Fig. 3). Each node consumes about 0.5A@5V (when not transmitting data) to 1.5A@5V (when transferring data through the Wi-Fi modules), so each node except of the last one, would be autonomous for about 4.5-13 hours depending on the Wi-Fi usage and the last one should be autonomous for about 14 hours (assuming continuous Wi-Fi usage). The last node (the one connected to the long range communication module) has been also equipped with:

- a solar panel (Solarland SLP003-12U) and with a solar charger/controller (Sunsaver SS-6L-12V) in order to charge its battery while that power is consumed,
- a battery charger (Noco Genius G750) in order to charge the battery from a 220V power outlet when available and,
- a power step-down converted to convert 12V to 5V to power the board (a charger rated at 2A was used)

All the nodes are finally enclosed in water-proof (IP66) enclosures. An image of the final construction using the 34.5 Wh battery is shown in Fig. 2 and Fig.3 shows the one with the 108 Wh battery.

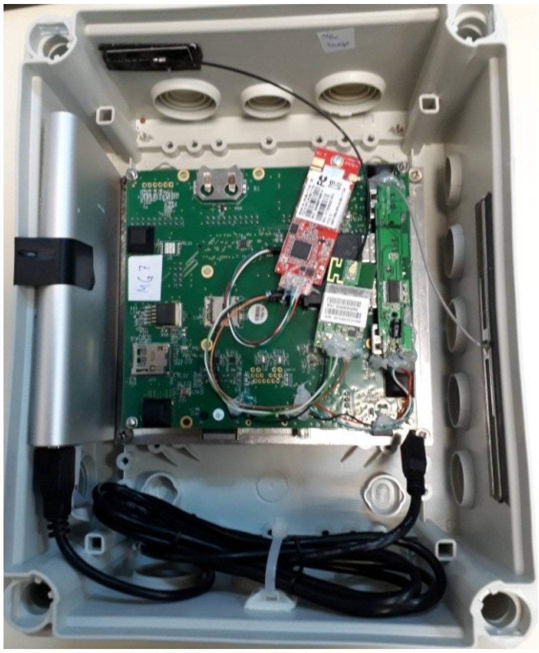

Fig. 2. The embedded board, with the two Wi-Fi modules, two PCB antennas and a lithium battery.

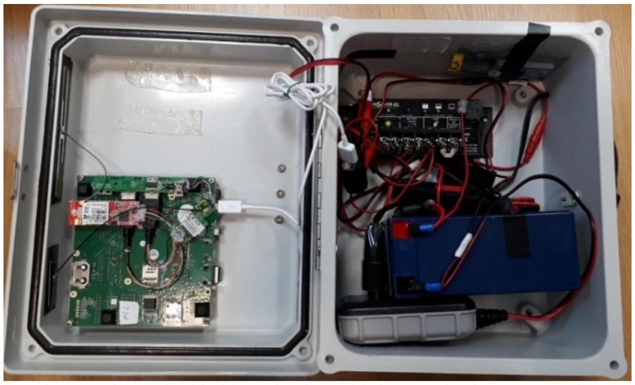

Fig. 3. The embedded board using a high-capacity battery, a solar charger/controller and a 12v battery charger.

B. *Software of the embedded board*

The software stack installed on the embedded boards is generated using the Buildroot [1]. Buildroot tool is used to create software for embedded boards; it actually creates a Linux image using only the drivers and the packages that we need to install by cross-compiling them (i.e., the process of making executable files for a target processor with different architecture of the one that Buildroot is running) in order to run them on ARM processors. Except for the drivers, the main packages installed using the Buildroot tool for the described purposes are:

- The "Better Approach To Mobile Ad-hoc Networking" (B.A.T.M.A.N. also known as "open-mesh") routing protocol for mesh networks [2]. B.A.T.M.A.N. is a proactive routing protocol for Wireless Ad-hoc Mesh Networks, including Mobile Ad-hoc Networks. The protocol proactively maintains information about the existence of all nodes in the mesh that are accessible via single-hop or multi-hop communication links. The strategy of B.A.T.M.A.N. is to determine for each destination in the mesh one single-hop neighbor, which can be utilized as best gateway to communicate with the destination node.

- The Delay-tolerant networking library by IBR (IBR-DTN) [3] which stores network data in the cases of network no-connectivity and delivers them when the network is available. DTN networking was originally created for interplanetary networking [4], i.e., for cases that satellites are not in line of sight (LOS) with earth. The IBR-DTN is an implementation of the bundle protocol RFC5050 [5], it is designed for embedded systems and can be used as framework for DTN applications. The module-based architecture with miscellaneous interfaces, makes it possible to change functionalities like routing or storage of bundle just by inheriting a specific class. The IBR-DTN belongs to the state of the art solutions which are currently available and its source code is open and accessible. IBR-DTN supports the TCP and UDP convergence layers, the Bundle Security Protocol and IPND neighbor discovery specifications. IBR-DTN aims to fit on portable systems, it is originally designed to run on embedded systems using the OpenWrt Linux operating system [6] in router devices, such as the WRT54G of Linksys. It can be used on a variety of operational systems (x86/x64 Linux distributions, OS X and Android Phones) with different processor architectures (x86, MIPS, ARM).

- The Dnsmasq [7] package. Dnsmasq provides network infrastructure for small networks: DNS, DHCP and network boot. It is open-source and is designed to be a lightweight subsystem that provides a local DNS server for the network, with forwarding of all query types to upstream recursive DNS servers and caching of common record types.

- The Hostapd [8] package. It is a Linux daemon process for access point and authentication servers. It implements IEEE 802.11 access point management, IEEE 802.1X/WPA/WPA2/EAP authenticators are supported. The hostapd process together with the dnsmasq are used to create an access point secured with the WPA2 protocol.

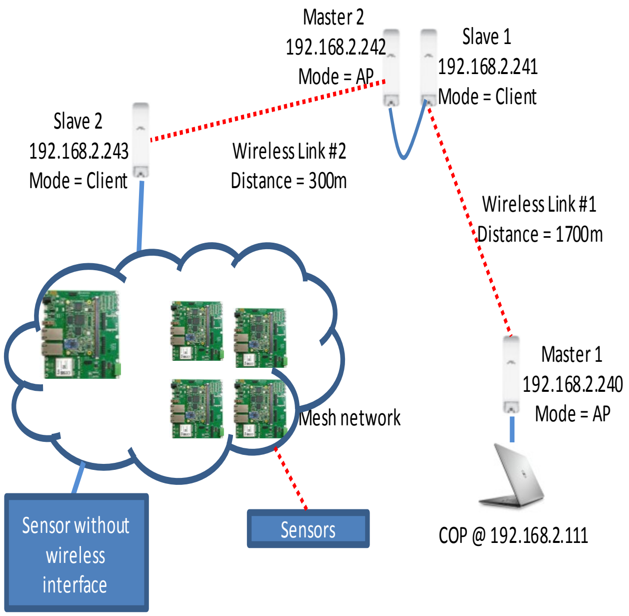

Fig.4. The network connections of the experiment in France. Blue lines denote a connection with ethernet (RJ45) cable and dotted red lines denote a wireless connection

C. *Long-Range wireless connectivity*

In order for the USaR team to be able to send data to the COP, a long-range wireless connection has to be used. This solution has to be easily deployable by someone without any special knowledge, so highly directional antennas with beamwidths smaller than 20° (like the parabolic-type and the dish-type ones [9]) should be avoided; they are directional, big-sized and their installation is time consuming. If possible, an operational frequency different than the 2.4GHz should be preferred, in order to avoid any interferences with other devices in the vicinity. The 2.4GHz band is usually referenced as "overcrowded" because it is used by Wi-Fi and Bluetooth devices, DECT phones, etc.

As a first solution, a pair of the "Multihop Ethernet DataRadio" by "Banner Engineering" was chosen, they consist a "black-box" solution for network connectivity, where you simply connect two devices with an Ethernet cable on the adapters and they are on the same network (the devices emulate an Ethernet cable too). They consist a low-power solution (65mW consumption), they support a maximum data transfer speed of up to 300kbps and they can reach a distance of 3.2km in open space, according to their specifications. Unfortunately, on-site tests show that this is not a viable solution for the INACHUS target USaR scenarios.

Due to the limited capabilities of the solution described above and after a thorough research between many available commercial products, finally the "NanoStation 5 MiMo (NSM5)" by Ubiquiti was chosen (Fig. 4 and Fig. 5). They are transmitting on the 5GHz band, are powered using power-over-ethernet (PoE) at 24V and they are plug-and-play. Their power consumption is 8W maximum at extreme conditions (we actually measured it to 6W), they are waterproof and they emit a beamwidth angle of 41◦ - 43◦ (Vertical/Horizontal) so they are not highly directional. Also, they can transmit data up to 15km according to the device's specifications (only a maximum of 3Km distance has been tested by the authors so far). The transmitting power of these devices gain can be adjusted by setting the desired distance that the antennas will be placed (using the provided software). It has to be mentioned that this solution works only on Line of sight (LOS) and also the user has to take care of the Fresnel zone [10] during the device installation. A solution for the case without LOS is described in the next section.

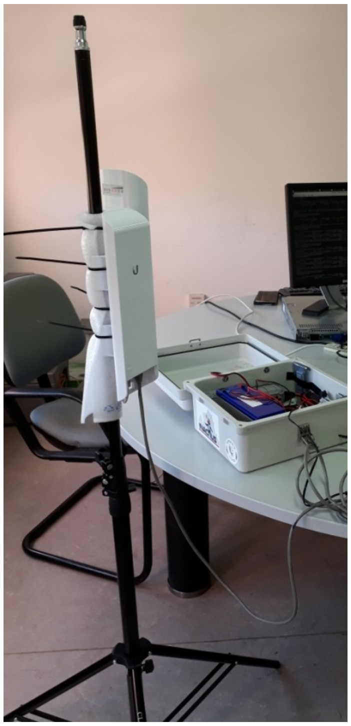

Fig.5. Two long-range antennas mounted on a mast to facilitate a network hop.

D. Network Topology

All the devices in the disaster area are connected into the same mesh network; and one of them is also connected to the long-range wireless device using its ethernet interface. The long-range wireless devices connect the mesh network on the disaster field with a computer located at the COP. At the previous case we supposed that the two places (the disaster area and the center of operation) are in line of sight (LOS) with each-other. If they are not, one more pair of long-range wireless devices could be used at a nearby place (e.g., a hill or the top of a high building) that has visual contact to both places that have to be connected, so two Point-to-Point links will be established (Fig.4 and Fig.5). All the network devices of the INACHUS communication solution are in the same network subnet. It should be mentioned that there is no Internet connectivity in our scenarios, since in cases of emergency it could be unavailable.

The local network used is the 192.168.2.X/24; each of the boards is named as GatewayX where X = 1,2,..9 (currently nine boards were built), the mesh Wi-Fi module on each board uses the IP 192.168.2.X, the access point has the IP 192.168.2.(10 · X), the addresses that the access point associates to a client connected on it are in the range 192.168.2.(10 · X +1) to 192.168.2.(10 · X+9) and the ethernet adapter of each board has the IP 192.168.2.(100+X). Table I shows a map with those IP addresses. So finally, the IPs in the range 192.168.2.110-192.168.2.255 are not used by the 9 boards and will be used by the long-range devices and the computers at the COP (Fig. 4).

TABLE I. THE IPS USED BY THE GATEWAYS

	Gateway1		**Gateway9**
Ethernet	192.168.2.101	...	192.168.2.109
Mesh Wi-Fi adapter	192.168.2.1		192.168.2.9
Access Point (AP)	192.168.2.10		192.168.2.90
Devices connected on the AP	192.168.2.11-19		192.168.2.91-99

III. ON-SITE PERFORMANCE EVALUATION

In this section, we describe the performance evaluation of the INACHUS communication solution, tested in real world conditions and in various USaR test sites in Europe (i.e., France and Germany).

The Hardware and Software of the embedded Linux Gateways have been thoroughly tested and they work as expected. They create a mesh network and by connecting devices (mobile phones/laptops) on them using their ethernet interface or their access point, available data can be transferred between them and back to the center of operation. Firewalls that could block traffic through specific ports are not installed on the gateways, so any data transferring protocol between two devices could be used. Also the DTN has been tested; unplugging the mesh network interface (by plugging its USB cable) while sending data and plugging it back after a while has resulted no data loss.

The first Long-Range wireless devices that were tested ("Multihop Ethernet DataRadio") did not provided acceptable performance, since their actual transfer rate was measured to be

60kbps on small distances (2m and 200m distances were tested resulting similar results) using the iPerf2 Linux tool [11] on two laptops. On a distance of 500m the two laptops could not even ping each other; or they could, but with major delays (>3sec) that are not acceptable for the INACHUS solution. As such, this device is considered as inappropriate for the purposes described here, despite their very low energy consumption. This device might be a valid solution to transfer data from a single sensor that transfers a small amount of data at a great distance and at very small rate.

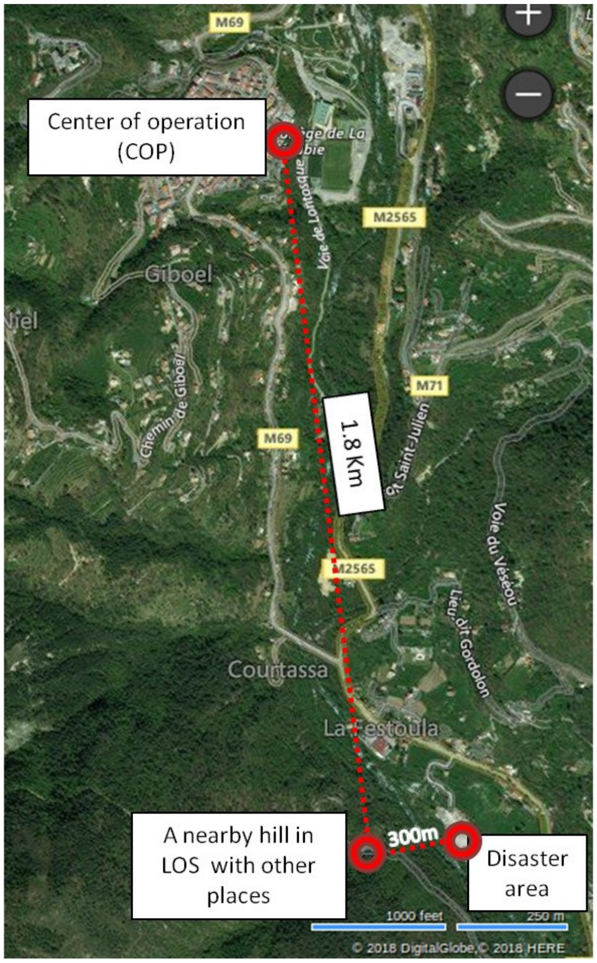

Fig.6: The location of the COP and the disaster area where the INACHUS communication solutions was tested.

The second Long-Range wireless solution (Ubiquiti's NanoStation 5 MiMo) was tested in an inter-urban setup, in order to assess the transfer rates on distances that will be faced in a real disaster event, and with non-directional Point-to-Point deployment. On a distance of about 1.8km, transfers speeds of 7-8MBps (about 56-64Mbps) were measured when transferring compressed files using the SCP [12] protocol. Also, by using the iPerf2 tool [11] transfer rates in the range 40-90 Mbps were measured, as well. The measurements are not in the same range since the SCP protocol encrypts the transferred data while iPerf2 tool measures the maximum bandwidth using the TCP/UDP protocols. During this installation, each of the wireless devices were not perfectly aligned with each other using any special tool (e.g., RSSI catchers or the included software of the NanoStations) so the results prove that this second examined solution is a robust and easily deployed scheme for the purposes covered by the INACHUS project. In order to create the Point-to-Point multihop link for a pair of devices, one of them has to be set up as an "Access Point" and the other has to be set as a "Client/Bridge" through the devices' software. Also, for security reasons, the client was "locked" only to a specific Access Point (by associating with its MAC address) and the protocol named "AirMAX" was chosen to be used so that devices from other manufacturers that don't support the same protocol won't be able to connect to corresponding link.

In Fig.6 we depict the setup of the above mentioned example that forms the final pilot test of the INACHUS project (test site in south France), where all the USaR component will be tested and their measurements will be transferred with the INACHUS communication solution back to the center of operation.

IV. Conclusions and Future Work

In this paper a novel communication solution for USaR missions, developed for the purposes of the EU project INACHUS, was presented. The corresponding solution has incorporated all the requirements that apply in USaR critical missions. Namely, the developed communication solution provides secure interconnection among the involved stake-holders, and does not require special equipment to be used by them since the access points that composes it, operate at the widely-used IEEE 802.11 Wi-Fi protocols that every handheld device (i.e., phone/tablet/PC) can support. The proposed solution is resilient to harsh weather conditions (i.e., temperature and rain), whereas all parts are designed to be of low-energy consumption, so that they can operate for many hours and under any possible weather condition. Finally, the INACHUS communication solution is easily deployable and operational by non-communication experts (e.g., USaR first responders) and also lightweight to be transferable in the disaster area.

The proposed solution can be extended in many different ways. A possible, extension could be the use of the IEEE 802.15.4 protocol, such as Zigbee, Xbee or LoRa commercial products. These solutions are low-power solutions and are designed for low data-rates (200-300 kbps) that can be used to transfer small text messages or alerts. Communication solutions using Satellite routers is another option. They also allow only low transfer rates, but they are expensive and can be considered as an alternative to rural areas where the distances between the COP and the first responders cannot be joint with other traditional means. Finally, another solution could be the installation of intermediate non-directional (i.e., omni-directional) wireless devices deployed by unmanned aerial vehicles (UAVs) to connect the COP with the disaster area.

This is actual an idea that has been examined in INACHUS too, where the UAVs used to assess the disaster area, can also be used as communication "mules".

Acknowledgment

This work was funded by INACHUS (Technological and Methodological Solutions for Integrated Wide Area Situation Awareness and Survivor Localization to Support Search and Rescue Teams), a FP7 project with grant number: 607522. For more information check https:/www.inachus.eu/ also.

References

[1] P. Korsgaard, "BuildRoot", *https://buildroot.org , Accessed Jul 13th 2018*.

[2] A. Neumann, C. Aichele, M. Lindner, and S. Wunderlich, "Better approach to mobile ad-hoc networking (BATMAN)," *IETF Draft*, pp. 1–24, 2008.

[3] M. Doering, S. Lahde, J. Morgenroth, and L. Wolf, "IBR-DTN: an efficient implementation for embedded systems," in *Proceedings of the third ACM workshop on Challenged networks*, 2008, pp. 117–120.

[4] S. Burleigh *et al.*, "Delay-tolerant networking: an approach to interplanetary internet," *IEEE Commun. Mag.*, vol. 41, no. 6, pp. 128–136, 2003.

[5] K. Scott and S. Burleigh, "Bundle protocol specification," 2007.

[6] Team, *OpenWRT: A Linux distribution for WRT54G*. .

[7] S. Kelley, "Dnsmasq," *Simon Kelley*, 2008.

[8] J. Malinen, "hostapd: Ieee 802.11 ap, ieee 802.1 x," WPA/WPA2/EAP/RADIUS Authenticator. online: http://hostap.epitest.fi/hostapd, 2014.

[9] R. Flickenger, S. Okay, E. Pietrosemoli, M. Zennaro, and C. Fonda, "Very long distance wi-fi networks," in *Proceedings of the second ACM SIGCOMM workshop on Networked systems for developing regions*, 2008, pp. 1–6.

[10] W. Tomasi, *Electronic Communications Systems: Fundamentals Through Advanced*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 1987.

[11] J. Dugan, J. Estabrook, J. Ferbuson, A. Gallatin, M. Gates, and K. Gibbs, "Iperf2," 2006.

[12] D. J. Barrett, D. J. Barrett, R. E. Silverman, and R. Silverman, *SSH, the Secure Shell: the definitive guide*. O'Reilly Media, Inc., 2001.