Porte et al. EURASIP Journal on Wireless Communications and Networking (2020) 2020:184
https://doi.org/10.1186/s13638-020-01793-3

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Heterogeneous wireless IoT architecture for natural disaster monitorization

Joaquim Porte*, Alan Briones, Josep Maria Maso, Carlota Pares, Agustin Zaballos and Joan Lluis Pijoan

* Correspondence: joaquim.porte@salle.url.edu
GRITS Department (Internet Technologies and Storage Research Group), LaSalle–Ramon Llull University, Barcelona, Spain

Abstract

A heterogeneous sensor network offers an extremely effective means of communicating with the international community, first responders, and humanitarian assistance agencies as long as affected populations have access to the Internet during disasters. When communication networks fail in an emergency situation, a challenge emerges when emergency services try to communicate with each other. In such situations, field data can be collected from nearby sensors deploying a wireless sensor network and a delay-tolerant network over the region to monitor. When data has to be sent to the operations center without any telecommunication infrastructure available, HF, satellite, and high-altitude platforms are the unique options, being HF with Near Vertical Incidence Skywave the most cost-effective and easy-to-install solution. Sensed data in disaster situations could serve a wide range of interests and needs (scientific, technical, and operational information for decision-makers). The proposed monitorization architecture addresses the communication with the public during emergencies using movable and deployable resource unit technologies for sensing, exchanging, and distributing information for humanitarian organizations. The challenge is to show how sensed data and information management contribute to a more effective and timely response to improve the quality of life of the affected populations. Our proposal was tested under real emergency conditions in Europe and Antarctica.

Keywords: Drones, DTN, Emergency network Natural Disaster, NVIS, WSN

1 Introduction

During an emergency, the detection of the environment is more effective when the management and communication of the information is part of the planned design and the execution. The integration of a communication plan into the overall action plan and the management of valuable information from the environment will provide a faster and more effective assistance to people affected by a disaster.

In the case of natural disasters such as earthquakes, hurricanes or tsunamis, the first 24–48 h is crucial to save lives and assess the situation. In such situations, the communication of technology is paramount to a coordinated and informed response.

The estimation of damage must be done locally and transmitted to the central authorities, while instruction for responders and the population must be disseminated from the central authorities [1].

At the present time, we are highly dependent on cellular or mobile communications. Unfortunately, mobile infrastructure is the first one to collapse in times of disaster, and it becomes unviable immediately. In addition, most of the mobile phones become inoperative for a few hours as people do not have power to charge their batteries due to the constant power outages [2].

When the telecommunication infrastructure is significantly or completely destroyed in a disaster, radio communications (especially radio-amateur and satellite services) become important for disaster-relief operation [3]. The recovery of the communication and the monitorization of the area in this disaster conditions becomes a challenge for emergency management. Isolated areas can only be communicated using HF communications with ionospheric reflection, satellite communications, and mini-HAPs (High Altitude Platforms), such as balloons acting as repeaters. Satellite transceivers are expensive, and it is unlikely that high-altitude platforms will be available over disaster zones to provide high-bandwidth communications. Therefore, communications in the HF band (3–30 MHz) are the most cost-effective and easy-to-install solutions.

1.1 Disaster situations

As an example, in the case of the earthquake in Nepal in 2015 [4], local Civil Society Organizations had access to radio coverage, although on a rather limited basis: the Nepal Red Cross Society broadcasted twice a week on its frequencies, although these channels were often shared among different organizations and the public over 25 community radio stations. During the hurricane Maria in Puerto Rico in 2017, the American Radio Relay League was requested by the American Red Cross to deploy 50 ham radio operators in the field [5].

In the case of an emergency, most of the available frequencies in the HF band become overcrowded due to the individual attempts to communicate. Hurricane Katrina demonstrated that emergency responders cannot fully rely on interoperable radio or satellite telephone in the face of a catastrophe. During the response of Katrina, emergency personnel found that nearly all forms of communication, such as cell phones, landlines, and satellite phones, were down; furthermore, the Louisiana State Police radio was inoperable because the frequency on which it was operated was clogged with users [6]. For that reason, a cognitive radio system which is able to select the available frequency of the spectrum at any time is a must.

In such emergency situations, users described real-time voice capabilities as vital for the operations of rapid assessment and decision making. In addition, data communication capabilities are required to support the operational analyses of disaster response. The possibility to send medical information, Geographic Information System (GIS) information, weather information, or any image and video of the affected area is becoming increasingly important [7].

1.2 Current research on disaster recovery

Some previous works contribute to solve the congestion of the traffic [8], or highlight the need of organizing a disaster recovery plan for each area [9]. While there are

solutions based on the virtualization of cloud services [10], other solutions desegregate the network to minimize equipment failure risks and propose protection approaches for fast recovery of network nodes after disaster happens [11]. As all these contributions are focused on adaptations of the current network to a disaster scenario, they will not be a realistic solution if the communication infrastructures crash. This is the reason why nearly every application and service added to the emergency area involves the deployment of a new Information and Communication Technology (ICT) infrastructure.

Therefore, there is a possible dangerous fragmented map of applications and communication technologies, which makes it difficult to achieve some designed functionalities and assure data management in general. This fact usually results in disorganized infrastructures and functions; hence, a desegregated ICT to the actual network communication is required. A heterogeneous mesh network is helpful to solve communication problems under emergency situations as it is usually a choice in other deployed critical communication infrastructures [12]. Some architectural solutions manage to decrease the damage in such kind of situation. In the work [13], the authors describe a new system through a new routing schema by sharing their locations to remote servers. The authors show a kick deployment network, but the coverage area of this solution will be limited through the actuation in a big disaster. In [14], the authors show new algorithms with more efficiency and the improvements of the computational analysis of the data allow to improve the wireless systems architectures with real-time analysis in such situations for Unmanned Ariel Vehicles (UAVs). In the works [15, 16], a new system is shown using the actual communications architectures. This system improves the actuation during a disaster, but it is attached to the existing networks. Moreover, the newest IoT networks appear as a new architecture to coordinate natural disasters. In the works [17, 18], the authors propose a new system based on an IoT-dedicated network architecture. All these works will help first responder performances in front of disaster management, but the network required is vulnerable versus a natural disaster as it can be destroyed.

1.3 Heterogeneous network solution

Our goal is to design and deploy a unique integrated heterogeneous system where all the applications and services can coexist, as any single technology can meet all the needs by itself. We propose the use of HF communications for a new communication network approach for emergencies. If the waves are transmitted nearly vertically at frequencies below the critical frequency of the F2 layer, a coverage can be achieved throughout a surface of approximately 200–250-km radius. This is called Near Vertical Incidence Skywave (NVIS) and is a good alternative to VHF and UHF links for longer distances and without the need of line of sight. Besides, due to the nature of a situation of emergency, wireless sensors networks (WSN) are apparently the most suitable technology for the access communication network, especially by using mobile nodes when several places are not readily accessible. However, as a technological option, it presents some technical drawbacks.

Our proposal employs a combination of WSN, delay-tolerant network (DTN), and NVIS technologies for the designed access network and backbone network. This combination will provide voice and low-rate data services with a very affordable

infrastructure which can be deployed in less than an hour after the disaster occurs. Also, it will improve the effectiveness of first response agents for disaster recovery enabling the communication between the different emergency teams and monitoring the key indicators to focus the resources in the areas most affected.

This chapter is organized as follows. In Section 2, the different technologies that define the base of this paper are presented. Section 3 defines the network requirements for the network access and the backhaul. Once the requirements of the network have been introduced, in Section 5, the distribution and the functionalities of the heterogeneous network, formed by the network access and the backhaul, are explained. In Section 6, a functional prototype is specified and the different scenarios where the network has been tested are described. Finally, Section 7 contains the conclusions of the backhaul and the access network deployed.

2 Technical methods of the disaster monitoring ICT

The system consists in two main parts: the NVIS node, backhaul, and the sensor data collector, access network, as seen in Fig. 1. This kind of hierarchical topology allows the interconnection between the different sensor networks. The backhaul facilitates the acquisition of the data and structures the different interconnections between the multiple nodes. In this section, we will include the design of the study. The type of the technology that we will use to solve the problem and the analysis of the network defined.

2.1 NVIS

NVIS technology is based on the communication in the HF band. This frequency band (3–30 MHz) is characterized by the reflection in the layers of the ionosphere, enabling a coverage ratio of 250 km without line of sight. The reflection is directly related to the

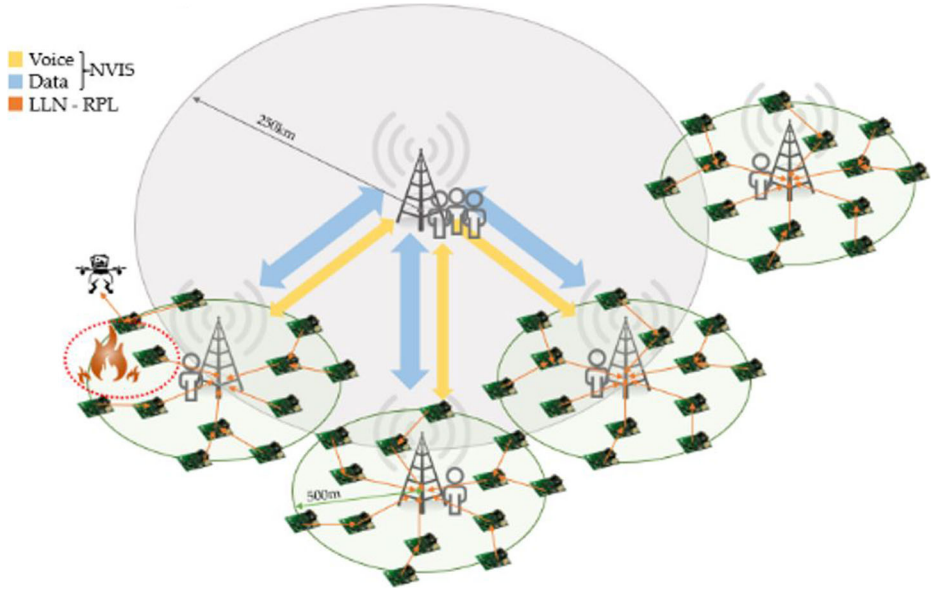

Fig. 1 Block diagram of the NVIS network for emergencies. We have presented a block diagram of the overall network with the NVIS and DTN network

solar activity since it is caused by the ionization of the ionosphere by the ultraviolet radiation. The reflection is also dependent on the terrestrial magnetic field and the angle of incidence of the wave [19], which must be between 90 and 70° for NVIS. In case of an angle of incidence below 70°, the communication will be oblique, and a link of 3000 km per hop can be achieved.

In the present day, many stations based on NVIS are installed around the world for sounding the total electron content of the different layers of the ionosphere. The main goal of these studies is the space weather forecast to reduce the effects of the geospace to several communication systems such as GPS or Galileo. These effects can lead to severe inaccuracies in the positioning, and all the services that rely on it may be affected [20].

On the other hand, NVIS communications have an increasing interest to communicate remote areas without any type of telecommunications coverage, due to either the orography of the terrain or because they are located very far from the nearest base station, for example, in the sea or in deserts. NVIS links are a more affordable alternative to satellite operators for remote zones, since there is no need to deploy a network of repeaters [21]. Moreover, a NVIS network is much easier to install, so it can be a real option for emergency situations when other emergency networks fail, and the deployment of a new network becomes critical.

In NVIS communications, there is a window of usable frequencies [21] for each pair of communicating nodes, depending on the ionosphere status. The ionosphere does not reflect at the same frequencies during day or night. This is due to the strong dependence of the solar activity; during the day, the reflecting frequencies will be higher than during the night. Furthermore, every 5 years, the solar activity varies and the reflecting frequency too. In Fig. 2, we can see the solar cycle of the Sun since 1945.

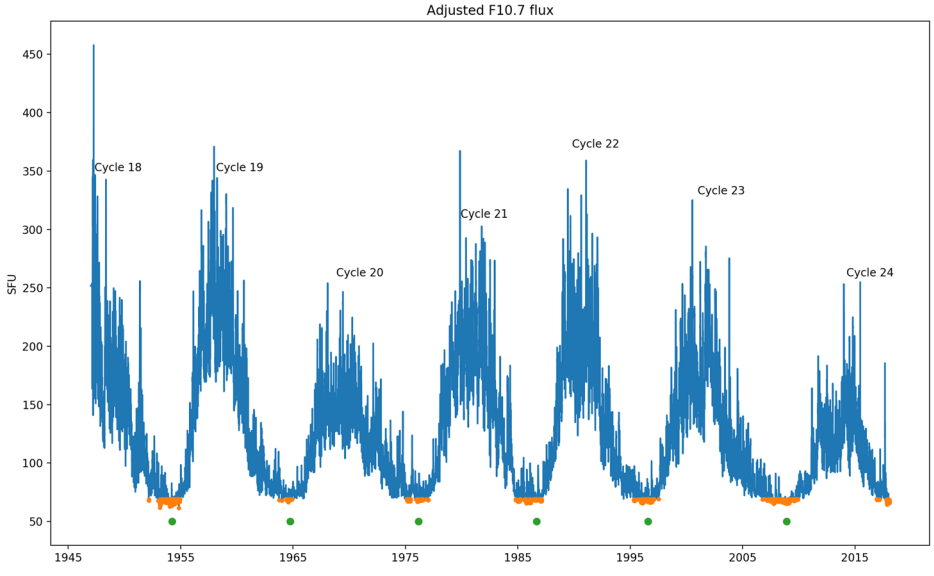

Fig. 2 Density Solar Cycle 1945–2018 [22]. In this figure, we can see the variation of density solar Cycle. This figure allows us to preview the state of the ionosphere. The ionospheric channel varies constantly, and we must be able to constantly work with this variation. In this scenario where technology will have to live a long time, we have to foresee these long-term variations

Automatic Link Establishment (ALE) strategies aim to find the best transmission frequency automatically. The transmitter tries all the frequencies from the assigned set while all the other nodes measure the signal quality received. When there is no network activity, ALE radios scan the available spectrum and update the lists of quality links [23].

2.2 IoT applied to disaster monitoring

According to [24], the IoT technology available today is quite mature and has the potential to be very useful in disaster situations. Relief teams require from disaster monitoring to successfully assist people in the affected areas and to speed-up first response activities and communications between the teams. The monitoring allows to focus the attention in the areas where more resources are required. As stated in [19], the WSN technology has applied in disaster recovery for more than a decade. A WSN is also referred as Low Power and Lossy Network (LLN). In agreement with the RFC 7102, a WSN or a Low Power and Lossy Network (LLN) is a network composed of many interconnected embedded devices with limited power, memory, and processing resources [25]. In the following section, we introduce the full IETF (Internet Engineering Task Force) LLN protocol stack [26].

2.3 Overview of the IETF LLN Protocol stack

To meet the requirements of constrained networks, the working groups IPv6 over Low Power WPAN (6LoWPAN) and Routing Over Low Power and Lossy Networks (ROLL) were created by the IETF [26]. The first group, 6LoWPAN, has detailed encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks [27] while the latter group, ROLL, has specified a proactive routing protocol based on distance-vector: RPL (Routing Protocol for Low-Power and Lossy Network) [28]. The full protocol stack is shown in Table 1.

Among the protocols suited for LLNs, the most promising protocol is RPL, because it allows us to logically divide the network into multiple instances (traffic classes), thus assuring traffic differentiation. A protocol overview is provided in the subsequent section.

2.4 RPL protocol overview

The goal of RPL is to build a network topology on top of an LLN that includes multiple partially overlapping link-layer broadcast domains [29]. To optimize routes for traffic to or from one or more roots, which act as sinks, it creates a topology in the form of

Table 1 LLN protocol stack

Layer	Protocol
Application	CoAP
Transport	UDP
Network	IPv6/RPL
Adaptation	6LoWPAN
MAC	IEEE 802.15.4
Physical	IEEE 802.15.4

multiple Destination-Oriented Directed Acyclic Graphs (DODAGs), finite directed graphs rooted at different sinks, with no directed cycles and with each node reaching a single destination (see Fig. 3).

RPL introduces the concept of an RPL instance to enable traffic prioritization. A DODAG can be part of at most one RPL instance. Each RPL instance may have multiple DODAGs, all of them using the same routing metrics and constraints defined by the objective function. The objective function is used to compute the rank of a node, its distance to the DODAG root with respect to a given metric, assuring the most suitable parents are selected. Each RPL node may participate in multiple DODAGs on the condition that each of them belongs to a different RPL instance.

This topology is created and maintained via multiple control packets advertised by each node. The construction of a DODAG starts from the root when it sends DODAG Information Object (DIO) messages to its neighbors. DIO messages carry information that allows nodes to discover an RPL instance, learn its configuration parameters, select a DODAG parent set, and maintain the DODAG. Once a node has joined a DODAG, it computes its rank and, if configured to act as root, it starts advertising the graph information with the new information to its own neighboring nodes [30]. This process enables the establishment of upward routes (towards the root node). RPL nodes use Destination Advertisement Object (DAO) messages to propagate prefix information of the nodes in its sub-DODAG to the root that aggregates the prefixes and builds downward routes, making them available to the parents. Additionally, RPL nodes can send DODAG Information Solicitation (DIS) messages to solicit DIO messages from their neighbors. The rate at which DIO messages are sent is tuned using the Trickle algorithm. A node transmits data unless it hears a few other transmissions whose data suggest its own transmission is redundant [31].

3 Network requirements design

In Fig. 1, we have presented a block diagram of the overall network. In this section, we are going to focus on the deployment of the LLN.

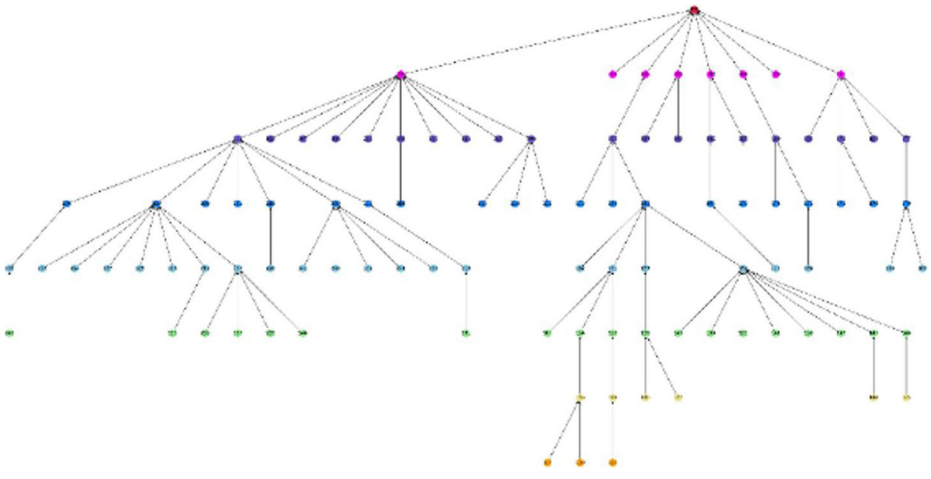

Fig. 3 DODAG with 100 nodes. Example of a Destination-Oriented Directed Acyclic Graph (DODAGs) with 100 nodes

For each site, we are going to have a WSN rooted at a gateway placed next to the NVIS station. This WSN will cover a circular area of 0.785 km^2 (see Fig. 1) thanks to the tree-like topology built using RPL. RPL nodes, such as the M3 node presented in Section 3.3, are going to be spread over the monitor area, and they will be static. Sensor data as well as text and voice messages are going to be collected by these nodes and routed to the gateway. Following the QoS requirements presented in Section 3.2, we expect nodes to be located at different distances, i.e., nodes collecting voice and text messages using Bluetooth will be situated closer to the gateway than nodes only transmitting sensor data, which can be positioned farther, leaving approximately 100 m between each other, covering the total area with 10 hops.

Sensors of interest include temperature, luminosity, gases, humidity, and presence. Moreover, people are going to use their smartphones to send voice and text messages via Bluetooth to the RPL nodes. Bluetooth is a wireless connection standard intended to connect different devices and transfer data over short distances [32], and its extension Bluetooth Low Energy (BLE) has been carefully designed with a great deal of attention to achieve low power consumption and high performance [33]. Therefore, with the BLE protocol in a star network topology, RPL nodes will act as central nodes (masters), while smartphones will act as peripherals (slaves). Bluetooth 5 supports packets up to 255 bytes and offers multiple data rates: 125 Kbps, 500 Kbps, 1 Mbps, and 2 Mbps, depending on the PHY mode (coded or uncoded) [34]. All these data rates are higher than the maximum throughput offered by the NVIS link, 20 kbps. Therefore, the characteristics of the Bluetooth 5 standard make it the most adequate wireless data transfer protocol for voice and text messages.

Furthermore, GPS (Global Positioning System) information will be added to sensor measurements to know the exact place where samples were taken. Finally, two different traffic classes are going to be established depending on the source, human and non-human. Overlapped RPL instances will allow the required traffic differentiation: human data—Instance 1, and sensor data—Instance 2.

The information provided by the mentioned sensors may not be enough for relief teams to design an actuation plan. For this reason, we propose the creation of a DTN using a mobile node placed on top of a drone.

3.1 The need for a DTN

As stated in [35], DTN architecture comprises the concepts of occasionally connected networks that may suffer partitions repeatedly. Data networks to which DTN architecture applies include sensor-based networks and terrestrial wireless networks with intermittent connectivity and satellite networks with moderate delays and periodic connectivity. The existing TCP/IP protocols do not work well in some environments due to some fundamental assumptions built into the Internet architecture such as the existence of an end-to-end path between the source and the destination during the entire communication session.

Mobile infrastructures can be managed as extra mobile nodes used to deliver messages in mobile-infrastructure-based framework. In order to relay messages to disconnected parts of the network, enforced routing solutions such as message ferries and data mules can be used, having mobile devices moving over predefined paths in order

to provide connectivity [36]. In our proposed architecture, drones with non-random movements act as mobile access point that provide communication service for nodes inside the emergency area. Drones act as data mules [37], delivering messages among isolated networks deploying an opportunistic network. Using a third RPL instance, they create a DODAG to pick up environmental data from the sensors around them, store it, and finally drop it off to the NVIS backhaul. When in the emergency area, drones will be responsible for taking pictures as well. Human messages cannot be delivered by the data mule.

Supporting mobility is a must in the proposed scenario. Both ends of the communication in the proposed MDRU (Movable and Deployable Resource Unit) may be mobile, with location-based services being a typical wide-spread example [7]. Current IoT solutions do not provide efficient means to support mobility since they usually rely on overlay architectures, e.g., "anchoring" to central servers, which obviously cannot scale while additional levels of complexity are introduced. Moving towards a unified architecture, mobility must be inherently supported by making the location of mobile smart objects and their data, which may reside in "migrate-able" servers, transparent to the communicating parties.

A block diagram of the proposed architecture with the three already mentioned RPL instances can be found in Fig. 4.

3.2 Quality of Service (QoS)

As it has been mentioned before, RPL introduces the concept of an RPL instance to enable traffic prioritization. Therefore, QoS inside the WSN is achieved by splitting up the network into multiple partially overlapping link-layer broadcast domains. At the

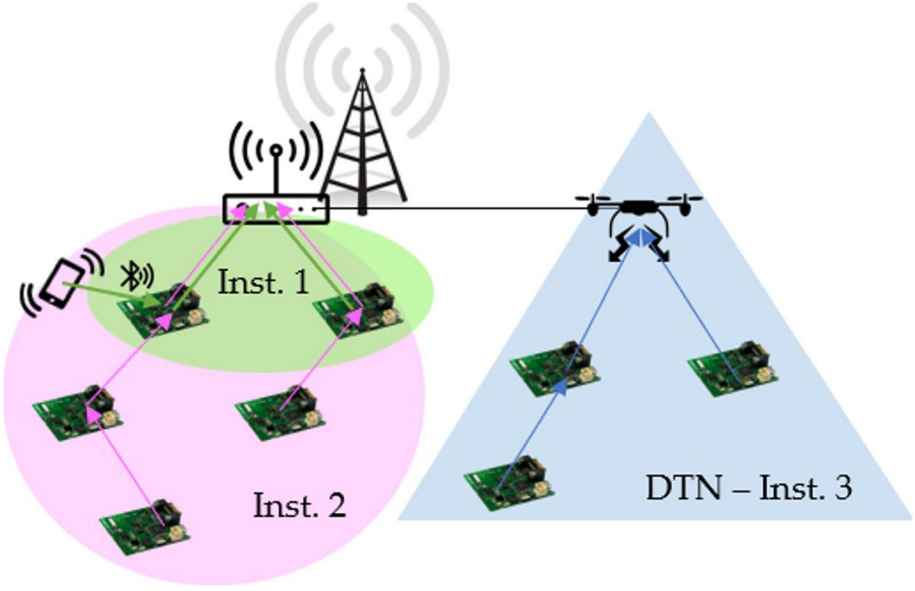

Fig. 4 WSN block diagram (Instances 1, 2, 3). The diagram shows the distribution of RPL instances 1, 2, and 3 of the wireless sensor network (WSN) defined in this work. This block diagram shows the proposed architecture with the three already mentioned RPL instances. Where Inst.1 represents the human data, Inst.2 sensor data and finally, Inst.3 it is a DTN using a mobile node placed on top of a drone

Table 2 Mapping between RPL instances and their corresponding PCP value

RPL instance	PCP value
1	7
2	0
3	4

edge between the WSN and the NVIS link, traffic must be tagged in order to achieve QoS end-to-end. We propose the use of the standard IEEE 802.1p [38] to differentiate the different traffic classes. The mapping between RPL instances and their corresponding PCP (Priority Code Point) value is shown in Table 2.

As we can see, human-generated data will have a higher priority over sensor data. Furthermore, sensor data collected on the emergency area by our drone will have a higher priority over regular sensor data. The scheduling mechanism used at the NVIS gateway will be Weighted Fair Queuing (WFQ) with Weighted random early detection (WRED) for congestion avoidance. The following scheme describes the mentioned process as shown in Fig. 5.

Among all the network specificities concerning availability that we have considered, one of the fundamental requirements is to continue operating securely even in a communication with intermittent connectivity [39, 40] and security due to NVIS network. Furthermore, some delay-tolerant networks may suffer from severe resource scarcity, making some form of authentication and access control to the network itself indispensable from many circumstances. Besides, IoT environments have heterogeneous technologies and services in several application domains, and thus, they become exposed to specific security requirements such as confidentiality, integrity, authentication, availability, and non-repudiation. Moreover, in many cases, common security policies and countermeasures cannot be directly applied to IoT technologies because of the different standards, resource constraints, and communication stacks involved [41, 42]. Given the broadness of cyber security issues, the scope of this paper is limited to communication network issues.

3.3 Experiment setup for requirements of the access network

To test our network requirements, several experiments have been carried out on the sensor testbed FIT IoT-LAB [43]. Small wireless sensor devices and heterogeneous

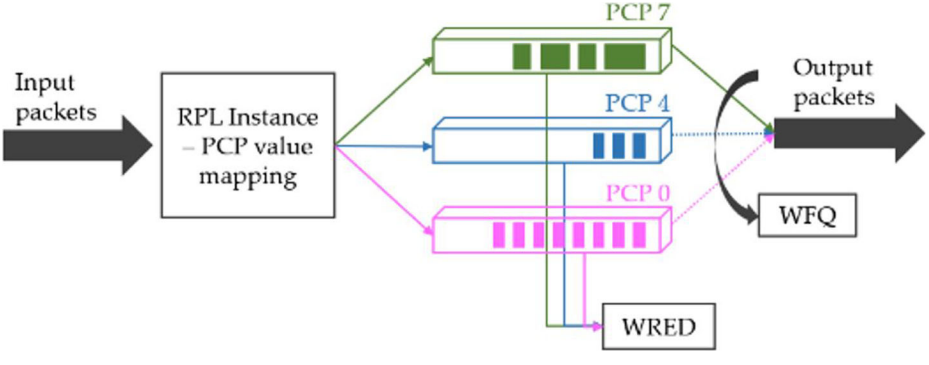

Fig. 5 NVIS gateway QoS mechanism. Definition of the mechanism used to apply QoS to the different services of the network

communicating objects can be tested in the FIT IoT-LAB infrastructure facility [44]. Over 1500 wireless sensor nodes are spread across six different sites in France, and for our experimentation, we have chosen the site of Grenoble [44].

A variety of wireless sensors are available, with different processor architectures and wireless chips. The sensors chosen are the M3, which feature a 32-bit ARM CortexM3 micro-controller (STM32FI03REY), an AT86RF231 IEEE 802.15.4 radio chip and sensors. The M3 is representative of today's state-of-the-art IoT devices [43] (Fig. 6).

The chosen hardware supports multiple Operating Systems: Contiki, Riot, OpenWSN, Zephyr and Contiki-NG [43]. For this study, we have chosen Contiki [45] because it is open source, it comes with multiple meaningful examples that you can try on the provided simulator Cooja [46], and it has a huge community support platform.

The physical topology of the network is presented in Fig. 7. Selected nodes are marked in orange and blue color. The node marked with a blue square has been set up as the sink of the network. This node has been chosen as the sink because it is the one that allows more flexibility when the logical topology of the network is being formed.

Three parameters of interest have been analyzed: convergence time, packet loss ratio, and one-way packet delay. To do so, the sink has been set up as a UDP server while the rest of nodes have been set up as UDP clients. Several Python [47] scripts have been used to process the data logs and to plot the presented graphs. Below we can find the abovementioned network parametrization.

4 Network design results and discussion

4.1 Convergence time

The first parameter of interest is convergence time. Our mobile node, the drone, will have to build and quickly destroy a DODAG on the emergency area to collect data from the nodes around. The convergence time is the minimum amount of time that

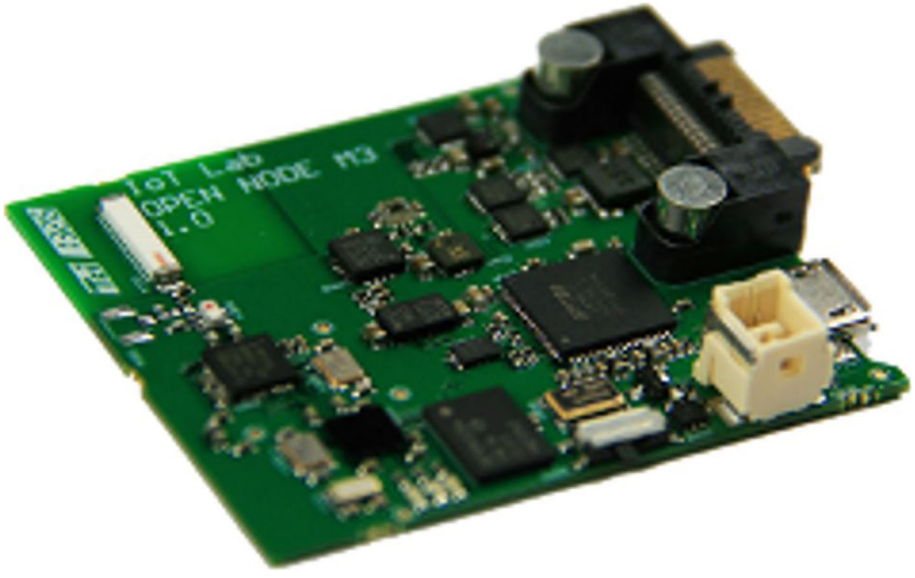

Fig. 6 M3 node. M3 is the sensor chosen to get all the data (Features: 32-bit ARM Cortex M3 microcontroller (STM32FI03REY), an AT86RF231, IEEE802.15.4)

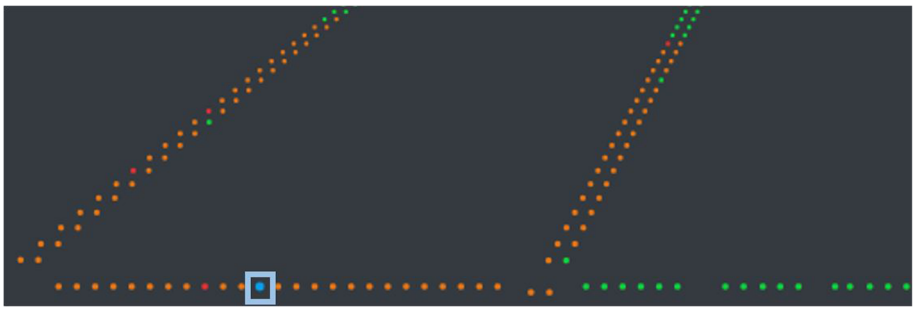

Fig. 7 Selected nodes from the Grenoble site (orange and blue). Physical topology of the network designed

the drone must stay on the site, so the DODAG is created and it can start receiving messages from the nodes.

Four different scenarios, each with a different number of nodes (20, 40, 60, and 100), have been tested. For each scenario, the nodes selected are those closest to the root node, i.e., for the first scenario, the 20 nodes closest to the root are selected. Convergence time has been calculated as the time since root node sends the first control message until it receives a hello-message from the last node. The obtained results are shown in Fig. 8.

As it has been shown above, the bigger the DODAG, the more time the drone has to stay in the emergency area to collect data. Since the drone is meant to provide more information about the affected area in case of emergency detection, the faster it can go, the better. Hence, the size of the DODAG in Instance 3 has to be limited to a maximum of 20 nodes.

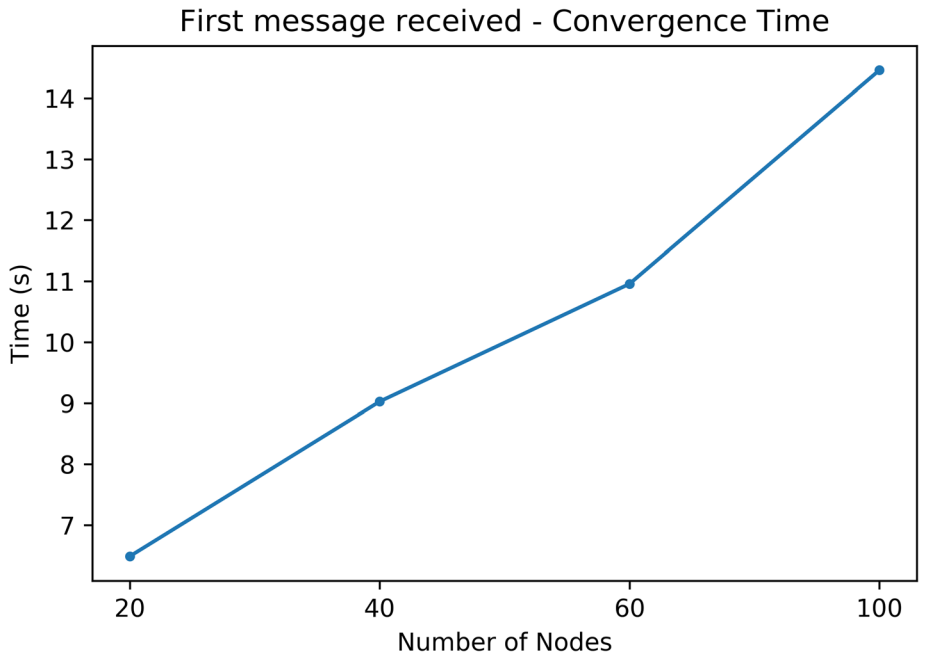

Fig. 8 RPL convergence time. This figure shows the evolution of the convergence time of the RPL protocol for different scenarios and with a different number of nodes (up to 100 nodes)

4.2 Packet loss ratio

The second parameter of interest is packet loss ratio. It is important to know the stress value of our WSN and to compare it with the bandwidth of 20 kbps of the NVIS link. A scenario of 100 nodes has been set up to measure the desired parameter. A total of 60 packets each with 10 bytes of data have been sent per node at different sending intervals. The number of nodes per hop has been plotted at the background (in blue) to give weight to the plotted medians (Fig. 9).

We can see that by sending one packet every 10 s, PLR gets much worse as we get further from the root, reaching values of 80% packets lost when nodes are at 10 or more hops from root node. Consequently, with this sending interval, some nodes receive less packets than if we were sending packets at a higher interval. For this reason, a minimum sending interval of one packet per node every 20 s has to be established for applications to work correctly. Therefore, we can conclude that the LLN limits much more the data rate than the NVIS link does.

Besides, not every application can work in this architecture. Depending on the distance to the root node, we have observed how the LLN has different characteristics. The closer to the root node, the lower the PLR. This is the reason why nodes that are located at one hop from root will be the only ones allowed to join Instance 1 from Fig. 4, which is going to be used for voice and text messages. Instance 2 will have no limit, and it will be used for sensors' data, as it has been mentioned before.

4.3 One-way packet delay

Finally, the third parameter of interest is one-way packet delay. For our use case, disaster monitoring, the freshness of the information must be taken into account. It is very important that information reaches relief teams as quickly as possible, so they can start defining the action plan.

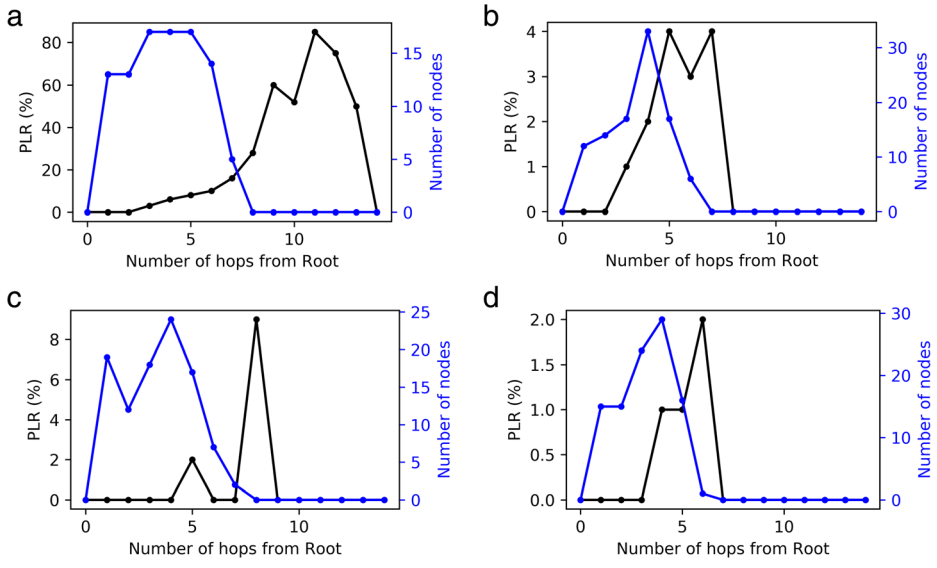

Fig. 9 PLR at different sending intervals. **a** One packet per node every 10 s. **b** One packet per node every 20 s. **c** One packet per node every 60 s. **d** One packet per node every 120 s. This result allows us to analyze the loss of packets depending on the number of nodes and hops of the WSN and defines the maximum stress that the network can allow

Using a similar procedure to that of the previous experiment, four different sending intervals have been tested and the obtained delays are shown in Fig. 10.

Having limited the minimum sending interval at 20 s in the previous section, we can conclude that as we get farther from the root node, the one-way packet delay increases (Fig. 11). Therefore, critical applications that require real-time data must limit the maximum rank (the distance from the root node) that nodes can have when joining the DODAG. This conclusion goes in accordance with the abovementioned limitation that Instance 1 can only have nodes located at one hop if we want human data to arrive as quickly as possible.

4.4 NVIS backhaul requirements

The capacity of the NVIS network is directly related to the ionosphere. As mentioned before, this communication channel with vertical rebound allows us to have a radius coverage of 250 km (Fig. 1). To communicate a large extension, the system must be able to intercommunicate all the nodes to bring the information to the central node. Limited in distance, the system must be able to allow all the nodes to act as a repeater of the data transmitted by other nodes.

Each channel has 20 kbps to communicate with the central node. To ensure this bandwidth to each NVIS node, each one needs a specific channel as shown in Fig. 12. This configuration guarantees 20 kbps to all the nodes situated at a distance less than one hop. As we have mentioned before, using the correct frequency between 3 and 10 MHz, the signal is reflected in the ionosphere. Using the critical frequency *foF2* of the layer *F2* as a reference point, we have to distribute the available bandwidth with the

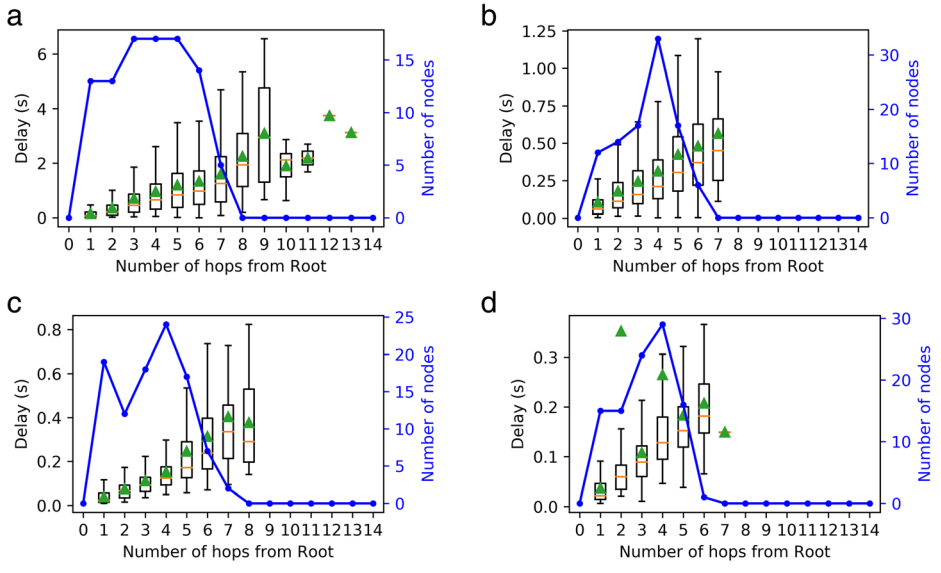

Fig. 10 One-way packet delay at different sending intervals. **a** One packet per node every 10 s. **b** One packet per node every 20 s. **c** One packet per node every 60 s. **d** One packet per node every 120 s. Those figures show the analysis of the packet delay at different data sending intervals. Those results were depending on the number of hops between the sensors. This analysis is important in a disaster monitoring to know the time delay to get the information and act as quickly as possible depending on the sensors data information

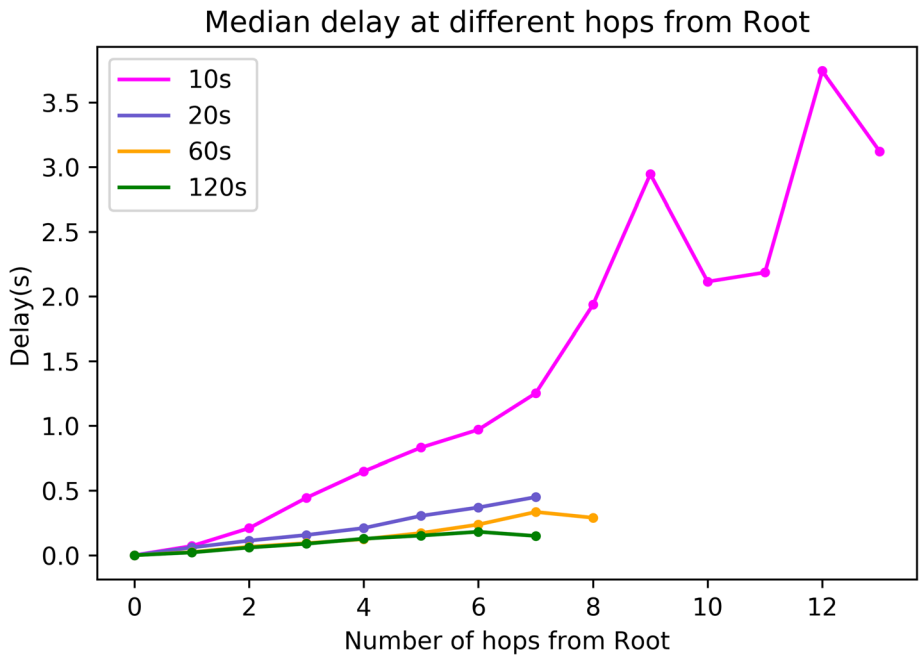

Fig. 11 One-way packet delay comparison at different sending intervals. One-way packet delay comparison at different sending interval shows that the network can only support sending intervals of at least 20 s

different nodes in channels of 3 kHz. The chosen channel spacing is *6 kHz* to avoid interference between nodes. This configuration allows us to allocate up to 100 NVIS nodes in *600 kHz* of the available frequency spectrum of the ionosphere which is much lower than the available (up to *3 MHz*). This frequency distribution allows us to test all the possible configurations that we have described in the Section 3.3, with a maximum number of 100 NVIS nodes.

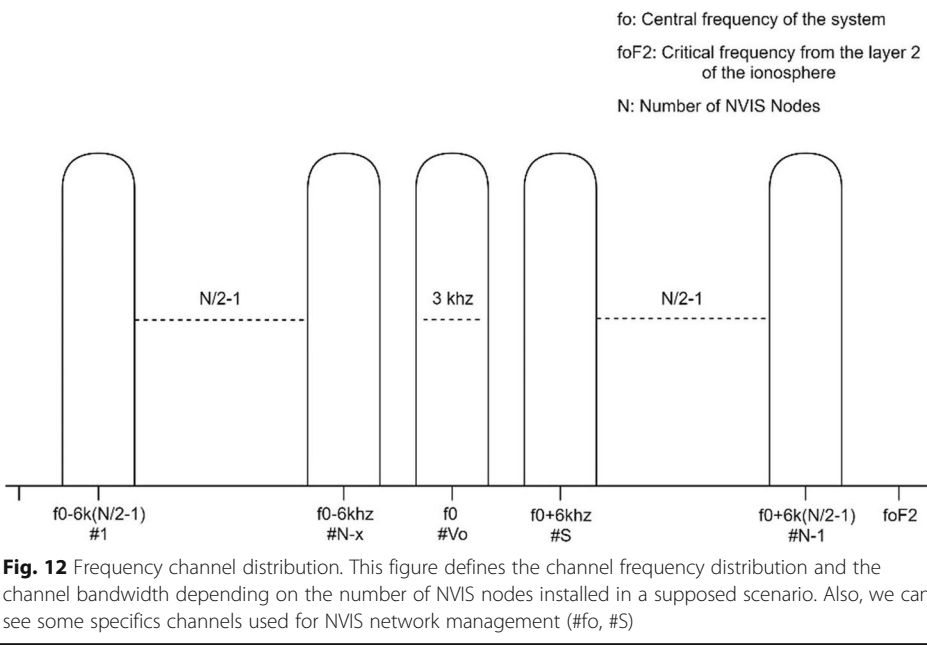

Fig. 12 Frequency channel distribution. This figure defines the channel frequency distribution and the channel bandwidth depending on the number of NVIS nodes installed in a supposed scenario. Also, we can see some specifics channels used for NVIS network management (#fo, #S)

Figure 12 describes how the different channels are allocated in the frequency domain. We can see that each channel has a specific function. One channel is reserved for the digital voice, another for the synchronization between the different nodes and the last one for the transmission of the data of each sensor. This function will be explained in detail in the next section.

5 High level design (HLD) of a sensor network with NVIS technology: design and results

The distribution of the nodes and their configuration in the NVIS network influences directly the performance of the entire system. To achieve the requirements of the sensors data network in terms of delay and total bit rate available for each connection, a specific configuration for these network purposes is required. To achieve these needs, one of the most important aspects to consider is the ionosphere. This communication channel allows us to mount the entire network, but with some restrictions.

In this section, we will see the distribution of the NVIS network and their requirements of use, nodes, and channel distribution. We will describe the high-level design of the network that has been proposed to implement the study of the data sensors explained in the previous section.

To define this network of NVIS nodes, the HLD diagram that we propose is the following (Fig. 13):

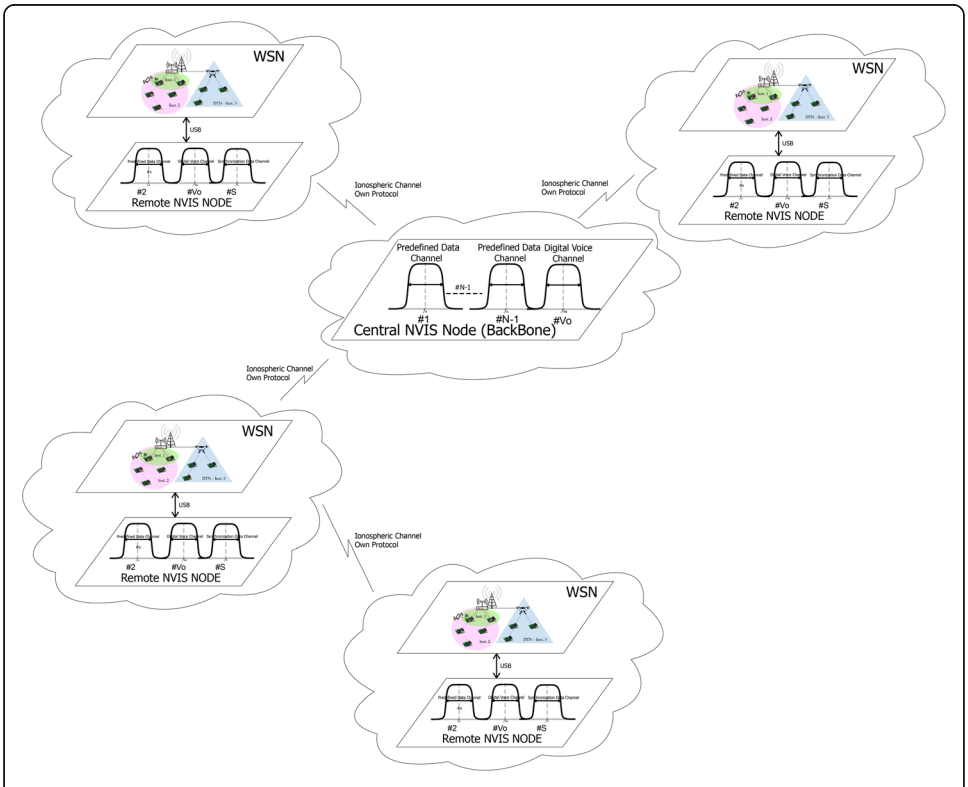

Fig. 13 HLD NVIS network distribution. Schematic of how the network is distributed to communicate the sensors data from the WSN collected by a NVIS remote node to the backbone

5.1 NVIS backhaul

As we can see in Fig. 13, the backhaul defines two types of nodes: the remote node and the central node.

The central node (Fig. 14) of the hub&spoke network is configurated to allow communication at the same time with all the remote nodes. To make this configuration possible, the hardware of this node is more expensive and has a superior intelligence than the remote node. Moreover, this configuration requires that the system is replicated in several transceivers where each one controls a different channel to communicate with a node situated at only one hop.

All the nodes must be able to transmit the data to the central node, even if they are outside of its coverage area (> 250 km) (Fig. 15).

5.2 NVIS remote

One specific channel *#S* is defined to communicate the nodes located further than one hop from the central node. In an initial stage, all the remote nodes listen from this channel. When any sensor needs to transmit data, the system switches to the specific channel of the node #(N-1) (Fig. 16). The node located two hops away from the central node will have to synchronize with other nodes to send their data with the *#S* channel.

Another specific channel is reserved for the digital voice transmission. The remote node switches from the predefined data channel to the #Vo channel. In Section 3.2, the different services priorities have been specified. Depending on the type of service, the node will shift to the corresponding channel.

Differentiation for priority control is useful when end-systems can generate different priority traffic flows. Then, the network may selectively discard packets with low priority, if necessary, in order to protect network performance for high priority cells or may implement control access policies. The implemented traffic shaping by RPL instances ensures conformance with bandwidth resources and delay constraints. Besides, stream differentiation enables scalable service discrimination in the deployed scenario without the need for a per-flow state in the access network and signaling at every hop in the NVIS backhaul.

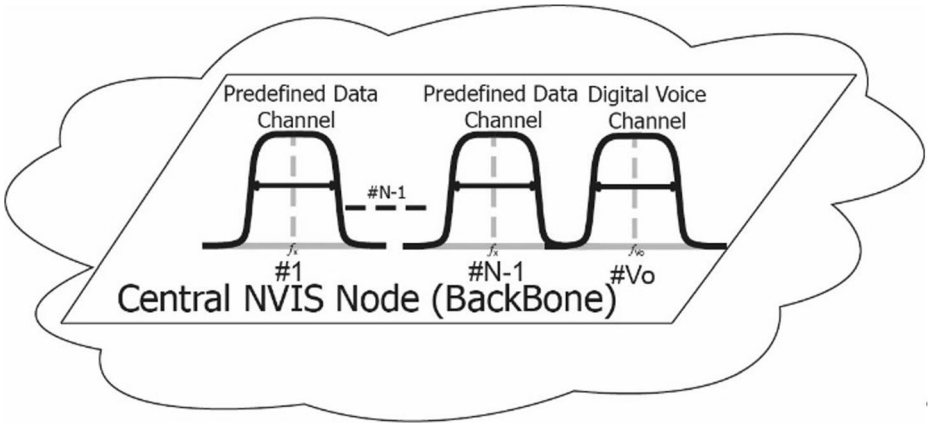

Fig. 14 Central NVIS node. Frequency and bandwidth distribution of each NVJS channel of the backbone

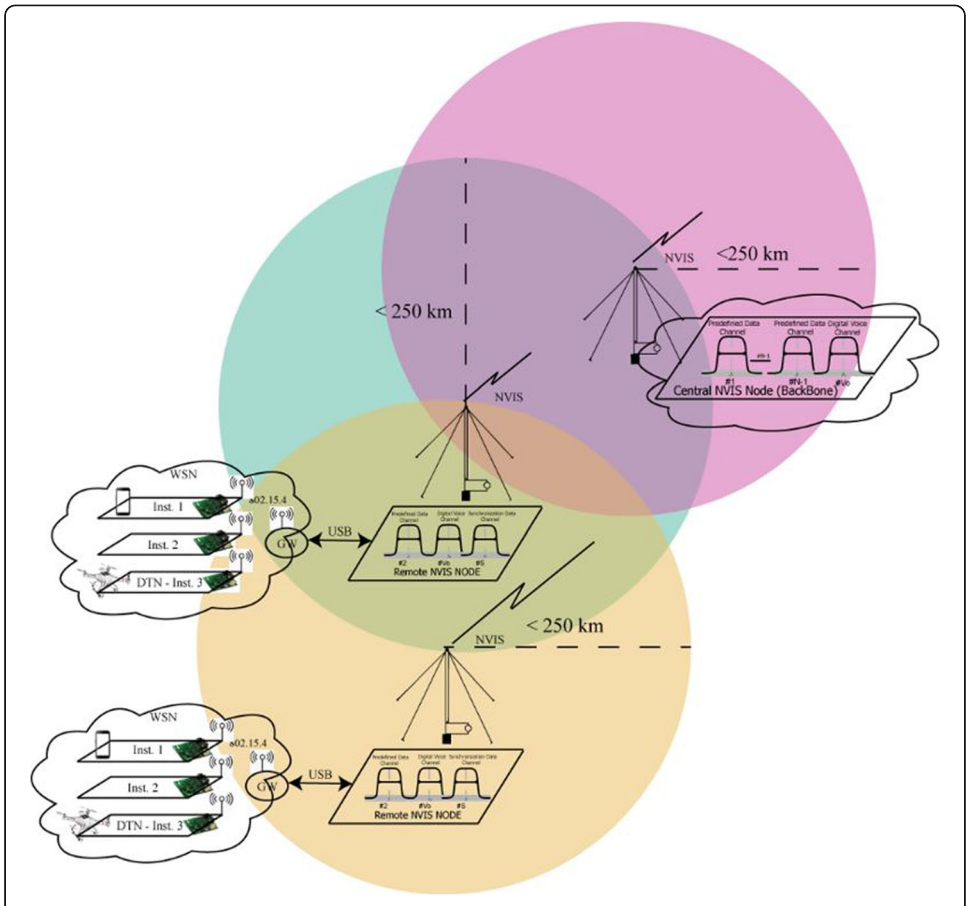

Fig. 15 Backhaul network. The coverage area of a possible backhaul network distribution. We can see how a remote node situated more than one hop to the central node can send the WSN data

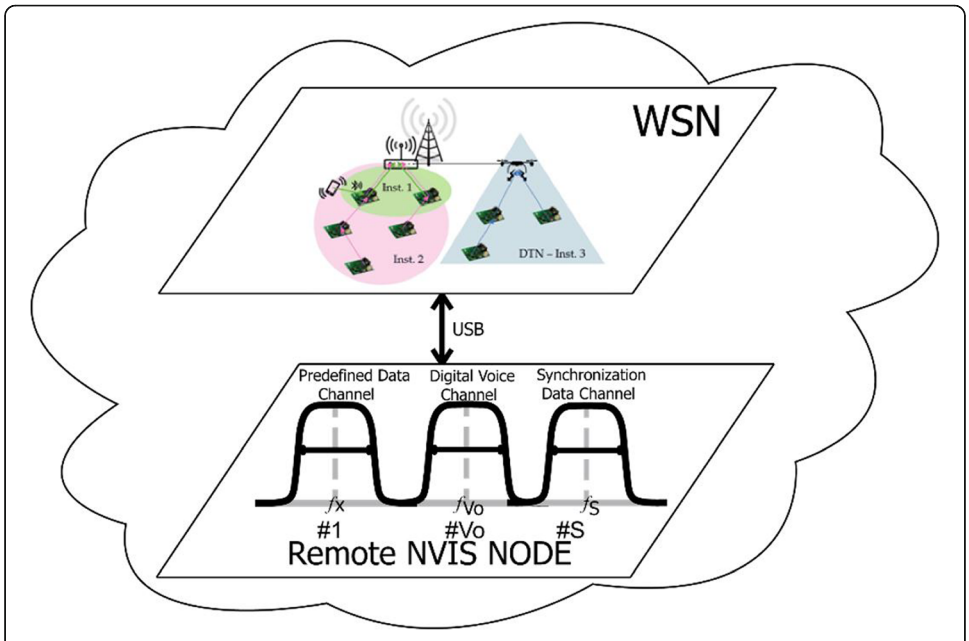

Fig. 16 Remote NVIS node. Connections between the NVIS node and the WSN network. Sensor data acquisition and transmission to the NVIS remote node

The proposed applications for the already deployed sensors are detailed in Table 3 [48–50].

Furthermore, the voice and text messages will be collected and transmitted with a mobile phone using Bluetooth as explained in Section 3 "Network requirements design". All the data sent via NVIS to the central node can contain errors and even the packets can get lost. The probability of recovering the errors within the packets will depend on the ECC (Error Correcting Code) used. In Fig. 17, we can see a CDF (cumulative distribution function) of the BER measured in the transmissions made from the remote nodes to the central node without any ECC. As we can observe, the probability of receiving the data without any bit error is 83.7%. If we consider three retransmissions in case of a bit error, that probability increases up to 99.93%. On the other hand, if we make use of a BCH code, we can improve the probability of packet success to a 98.00%.

The average packet delay is another key issue to consider. For every transmission, every packet takes 2.477 ms to travel the mean distance of the ionosphere F2 layer where the signal is usually reflected. Once the signal is received, the processing time is about 300 ms. We can see that the most significant part of the transmission delay is due to the signal processing algorithm, which could also be improved.

5.3 NVIS to WSN interface

The protocol IEEE 802.15.4 is used to get the data from the sensors, and an own NVIS protocol to transmit the data between the different nodes.

The data from the sensor network collected by the gateway is sent via Universal Serial Bus (USB) to the NVIS transmitting node (Fig. 18). The system capable of detecting the state of the ionosphere stores all the data to be transmitted. Then, it analyzes the data to define its priority and origin to decide for which channel data has to be sent. Therefore, the data transmitted from the sensors through 802.15.4 must be adapted to the NVIS transmission system. This data is packaged in NVIS's own frame. The operation of the prototype is explained in Section 6.

6 Prototype of a functional platform

For testing the proposed theory, a functional prototype of the system has been developed. The prototype is mainly composed by a Red Pitaya and a Raspberry Pi 3 among others less important peripherals. Red Pitaya is a low-cost Software Defined Radio (SDR) platform with a FPGA+ARM through which all the HF signal processing has been implemented. Primarily, it is on charge of upsampling and downsampling the frames which are going to be transmitted or have been received by the antenna. All the

Table 3 IoT application proposed

Sensor	Application
Temperature	Detects fires.
Ultrasound	Detects air temperature as well as river water level. Helps in floods.
Luminosity	Helps assessing the emergency area for trapped victims.
Gases	Detects gas leaks.
Presence	Detects that somebody is close to the sensor. His/her state should be verified.

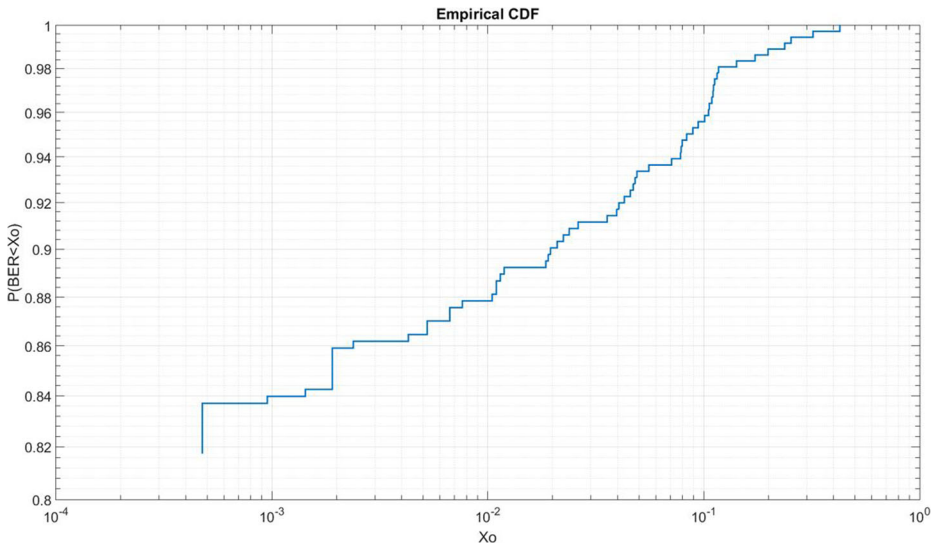

Fig. 17 CDF of remote test. Results of the implementation of a remote NVIS node data transmission test. This figure shows the probabilities of getting a BER (bit error rate) in a transmission (test made with more than 1 Mb)

software implemented on Red Pitaya is VHDL code. On the other side, Raspberry Pi 3 is a processor board which is on charge of demodulating the received signal on data and modulating the data that we want to transmit. It also mounts all the transmitting frames and is the one that takes the decisions depending on the data received. In this case, all the software implemented has been developed on C code. Other peripherals used for the prototype are a power amplifier, a receiver amplifier, an antenna relay, and an amplifier controller. The development and the results of the functionalities are more detailed on our previous work [51–53]. In Fig. 19, we can see a brief schematic of the developed prototype.

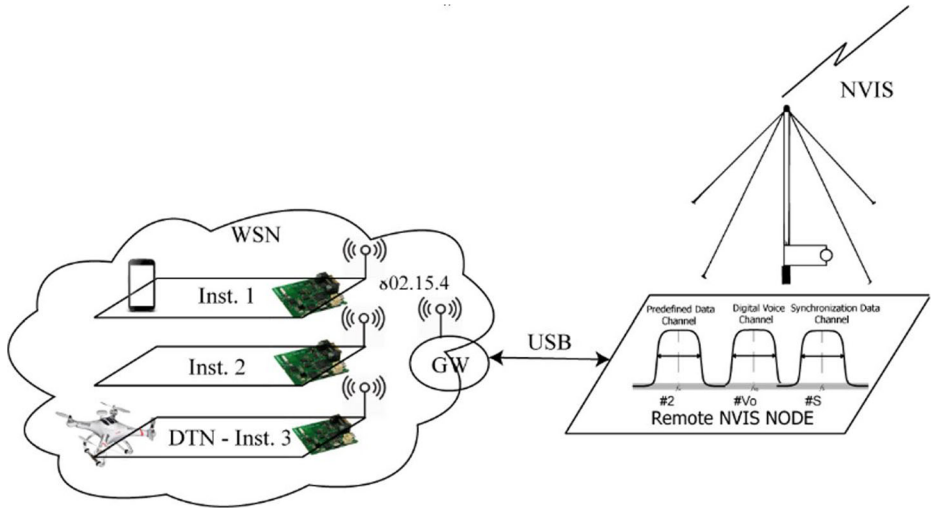

Fig. 18 WSN interface with NVIS node. Protocol and connectivity chosen to transmit sensors' data to the NVIS remote node, and then to the central node

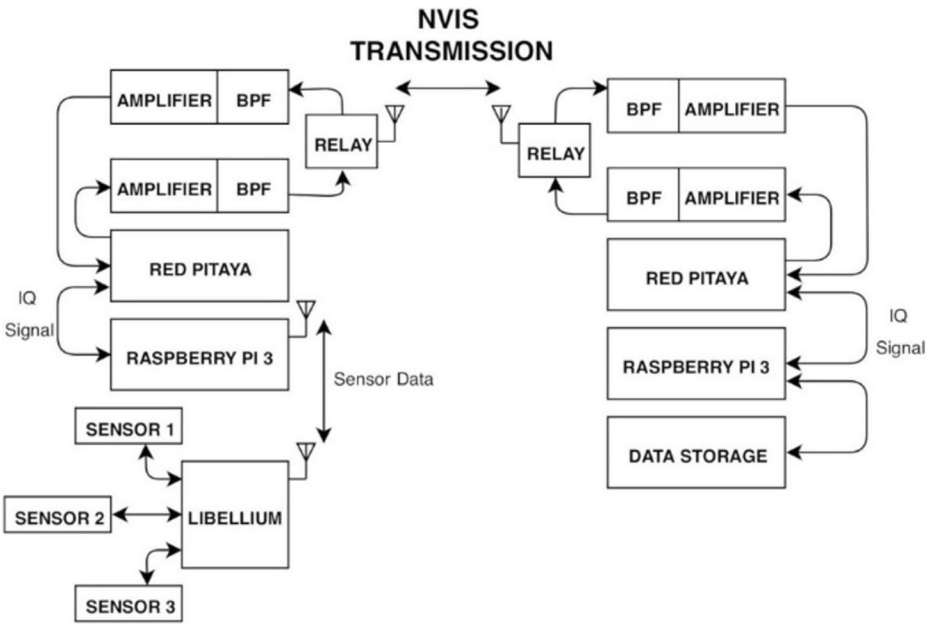

Fig. 19 Block diagram of the NVIS node. Block diagram of the NVIS node hardware and software. This figure shows how data is modulated and transmitted from the data acquisition, to the reception and data demodulation

The platform designed can be divided into two blocks: the analog and the digital block. As we can see, both the transmission and the reception schemes are quite similar. In reception mode, the signal must be properly amplified and filtered before it is processed in the SDR. The first stage is an analog bandpass filter (2 to 7 MHz) that attenuates other signals outside the bandwidth of the signal. The second stage is the amplification of either the transmission or the reception signal, which are switched by a relay. In the transmission stage, we use a power amplifier of 100 W, while in the reception stage we use a low noise amplifier (LNA) of 30 dB. The expected received signal is around − 90 dBm, so the signal must be amplified by the LNA to allow the ADCs converters work correctly. Finally, the Red Pitaya (FPGA) and the Raspberry (ARM) analyze the received signal, or they generate the baseband signal that must be transmitted (Fig. 20).

The platform is designed to minimize the cost and the power consumption. The antenna used matches both specifications. We use an inverted-V wired antenna with a maximum gain of 2.5 dB or 5.5 dB depending on the type of soil. The radiation diagram of the antenna fixes the maximum gain between 90 and 70° that fits in well with the angles needed for NVIS technology. The inverted-V is easy to install, and a single mast is required (see Fig. 21). In [51, 53], the study of the antenna design is described in more detail.

In terms of time recovery, the NVIS nodes are the most restrictive. We should consider that NVIS networks will always be deployed. So, when a disaster occurs and no other network works, the developed network will start working since it has been deployed previously. In our previous works [51–53], we have tested that the installation of a remote node takes 20 min. In that case, if some zone is not connected, the deployment and installation of a single urban node takes a maximum of 20 min. If a new node

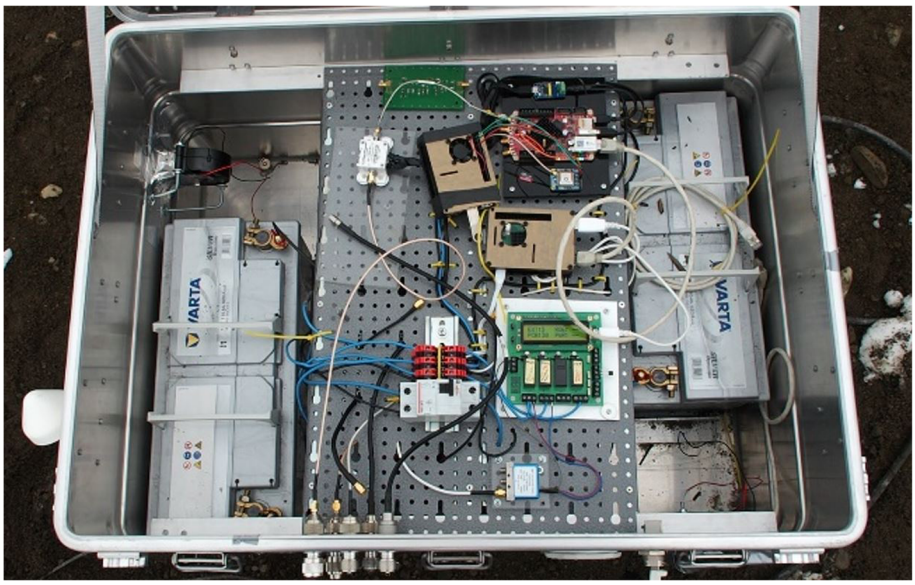

Fig. 20 NVIS remote node installed in Argentina Cove. Installation of a remote node in the Antarctica scenario. This node was situated 2 km away from the central node

must be installed in a new area, the time needed to transport all the required materials must be added to the previously mentioned 20 min. Finally, each NVIS remote node needs approximately 1 min to be operational and establish the link with the central node. Regarding the WSN, the time needed to deploy it is very low, compared to that of the NVIS nodes, just a few seconds (see Fig. 8).

The power consumption of all the NVIS nodes, without any energy saving measures, is about 31.2 W. The nodes will be electrical mains operated if possible or powered by a diesel generator in the case of emergency. In the case of power outage or remote locations without power supply, the NVIS nodes will be powered directly by lead-acid batteries supported by renewable sources such as solar panels to maintain the charge.

In the case of emergency, a fuel generator will power the NVIS nodes, so the RF power is not as limited as in the battery case. A power of 100 W will allow higher order modulations to perform with an acceptable Bit Error Rate ($< 10^{-3}$); therefore, bit rates of around 20 kbps can be guaranteed. In the system used for the realization of the tests, the remote nodes have been powered by lead-acid batteries while the central node was powered by the electrical network. In any case, the system consumption was about 31.2 W, which is not a high consumption even though no energy saving measures have been applied.

The protocol used for assuring the integrity of the data transmitted is half duplex. When a frame is transmitted from a remote node to the backbone, the central node sends an ACK frame to the remote node. To ensure that a frame received does not have data errors, every frame transmitted contains a FCS (Frame Check Sequence) which is reviewed on reception. If the FCS does not agree with the one generated from the received data, the central node will send a frame requesting a streaming. Moreover, if the remote node does not receive an answer from the central node, it will resend the frame until it receives an answer from the central node.

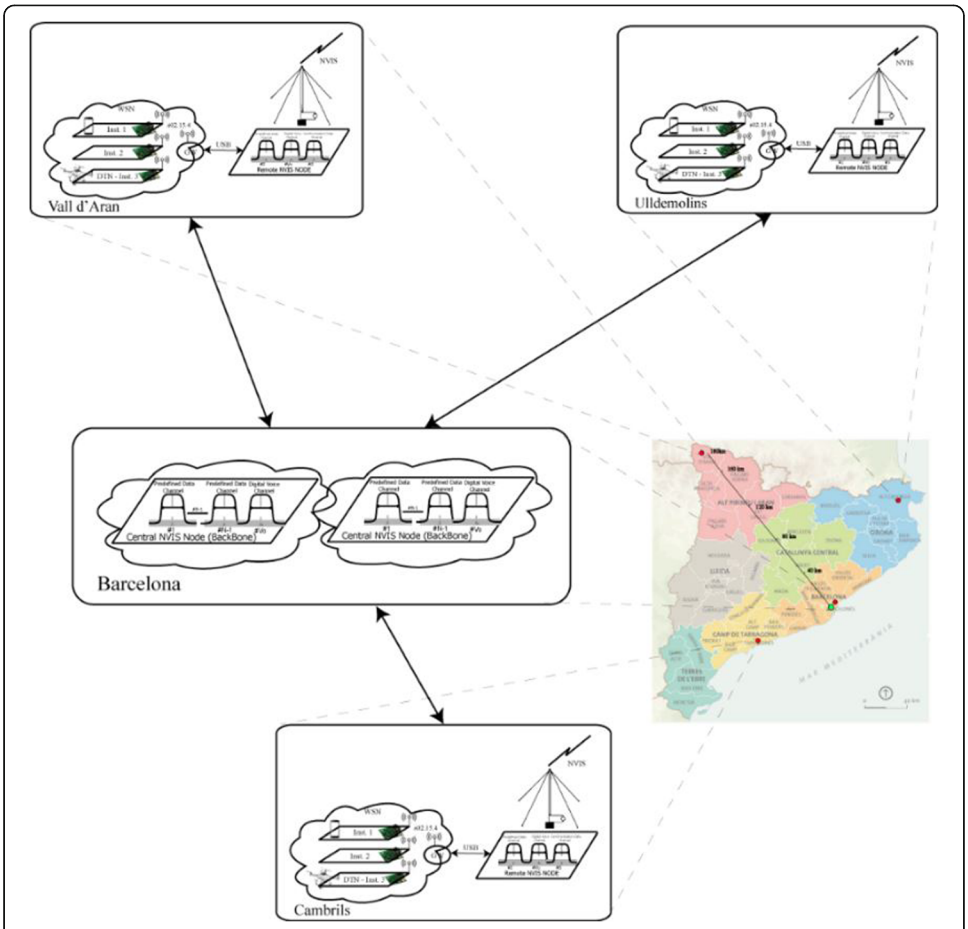

Fig. 21 Catalonia Nodes distribution. Distribution of the real test implemented in Catalonia. Three remote nodes were installed to test and get the results of the network analysis. A central node with redundancy was also installed. The remote nodes were situated between 100 and 200 km away from the central node (backbone)

For testing the system and estimating the probability of a retransmission, the system has been implemented in two different scenarios: one in an urban localization and the other one in a rural localization. In both cases, the frequency carrier for transmitting and receiving has been set at 5 MHz.

In the urban case, a central node has been installed in the city of *Barcelona* (Spain) and three remote points have been strategically placed to supply most of the coast (*Cambrils* and *Ulldemolins*) and in the upper mountains (the *Vall d'Aran*) (Fig. 21). In this scenario, the most important characteristic is the high spectral noise in our channel. To have redundancy in the central node, two nodes have been installed with the characteristics of a central node in Barcelona. This phenomenon makes more difficult the process of demodulating the received signal, and consequently, more data errors are generated.

On the other side, for testing the prototype [54, 55] with the lowest spectrum noise, a base node has been installed in the Spanish Antarctica base Juan Carlos I in Livingston Island. Other two remote nodes have been installed in Livingston Island, one in Argentina Cove (1.28 km from the central node) and the other one in Rocky Glacier (Fig. 22) (5.59 km from the central node).

Fig. 22 Rocky Glacier remote node installation. Installation of second remote node in the Antarctica scenario. This node was situated 5 km away from the central node

7 Conclusions

A new network easy to deploy in emergency situations has been presented. Combining a NVIS physical layer backhaul together with a WSN acting as an access network, a promising infrastructure is obtained with the potential of helping in disaster relief operations due to the communication distances that it can achieve.

First of all, we present the NVIS network as the physical layer where a maximum of 100 nodes located up to 250 km away are allowed due to bandwidth restrictions. By dividing the frequency spectrum of the ionosphere into several channels, a better network performance is obtained. A maximum bitrate of 20 kbps and a bit error rate lower than 10^{-3} are reached. One specific channel is defined to communicate the nodes situated at more than one hop to the central node, while another one is reserved for the transmission of digital voice. To ensure the emergency communication, an ALE will select the best frequency to establish the ionospheric communication. Also, if the message received has some errors, a retransmission will be requested to guarantee the integrity of the message.

On the other hand, the WSN network uses RPL as a routing protocol, overlapping link-layer broadcast domains can be created to allow for traffic differentiation. A DTN with a drone acting as a mobile node helps on providing further information from affected areas by collecting data from isolated nodes and gathering more information by taking pictures. The experiment set-up on the IoT LAB establishes the upper bound, in terms of the number of nodes, for DODAGs that belong to the third RPL instance. A DODAG of a maximum of 20 nodes can be constructed with the drone acting as a sink. Additionally, the interval between packets sent by every node has also been defined. A minimum sending interval of one packet per node every 20 s is needed to allow the WSN to deliver valuable data. Furthermore, the compromise between the node rank and its packet delay has been presented. Since one-way packet delay is increased at every hop, some applications may need

to limit the maximum distance from the root allowed to reach their objectives of maximum delay permitted.

Finally, two use cases of the presented infrastructure have been defined: an urban scenario around Catalonia (Spain) and a remote scenario around Livingston Island (Antarctica). An operational prototype was deployed in both scenarios that confirms the viability of the proposal.

Abbreviations

NVIS: Near Vertical Incident Skywave; DTN: Delay-tolerant network; ICT: Information and Communication Technology; IoT: Internet of Things; DODAG: Destination Oriented Directed Acyclic Graph; FCS: Frame Check Sequence; FPGA: Field-programmable gate array; ARM: Advanced RISC Machine; LNA: Low noise amplifier; SDR: Software Defined Radio; CDF: Cumulative distribution function; ECC: Error coding code; LLN: Low Power and Lossy Networks; RPL: Routing Protocol for Low-Power and Lossy Networks; ALE: Automatic Link Establishment; RSNA: Robust secure network architecture; PLR: Packet loss ratio; BER: Bit error rate

Acknowledgements

The authors thank the anonymous reviewers and editors for their efforts in providing valuable comments and suggestions.

Authors' contributions

AZ And JL.P conceptualizes the idea and defines the constraints of the research and supervised the research. CP and AB design, simulate, and implement the IoT and DTN network defined in the manuscript. JP and JM.M design, simulate, and implemented the NVIS network. All authors read and contributed in the writing of and approved the final manuscript.

Funding

This work was funded by the Ministry of Economy and Competitiveness and the European Regional Development Fund under the contract CTM2015-68902-R (MINECO/FEDE) and RTI2018-097066-B (MINECO/FEDER).

Availability of data and materials

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Competing interests

The authors declare that they have no competing interests.

Received: 16 October 2019 Accepted: 6 September 2020
Published online: 23 September 2020

References

1. R. Austin, P. Bull, S. Buffery, *A Raspberry Pi Based Scalable Software Defined Network Infrastructure for Disaster Relief Communication*, In Proceedings of the 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud); IEEE (2017), pp. 265–271
2. A. Kwasinski, F. Andrade, M.J. Castro-Sitiriche, E. O'Neill-Carrillo, Hurricane Maria Effects on Puerto Rico Electric Power Infrastructure. IEEE Power Energy Technol. Syst. J. ***6***, 85–94 (2019)
3. P. Wilkinson, D. Cole, The role of Radio science in disaster management. URSI Radio Sci. Bull. **335**, 45–51 (2010). https://www.ursi.org/files/RSBissues/RSB_335_2010_12.pdf
4. M. Wendelbo, L. Federica China, H. Dekeyser, L. Taccetti, S. Mori, V. Aggarwal, O. Alam, A. Savoldi, R. Zielonka, *The Crisis Response to the Nepal Earthquake: Lessons Learned* (2016)
5. C. Maitland, J.M. Peha, Wireless Network Recovery Following Natural Disaster: Puerto Rico after Hurricane Maria (March 16, 2018). TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy 2018. Available at SSRN: https://ssrn.com/abstract=3142393
6. P.C. Smith, D.M. Simpson, Technology and Communications in an Urban Crisis: The Role of Mobile Communications Systems in Disasters. J. Urban Technol. **16**, 133–149 (2009)
7. Y. Jahir, M. Atiquzzaman, H. Refai, A. Paranjothi, P.G. Lopresti, Routing Protocols and Architecture for Disaster Area Network: A Survey. Ad Hoc Networks **82**, 1–4 (2019)
8. N.A. Mahiddin, N. Sarkar, *An Efficient Gateway Routing Scheme for Disaster Recovery Scenario*, In Proceedings of the 2019 International Conference on Information Networking (ICOIN); IEEE (2019), pp. 204–209
9. G. Parise, L. Martirano, L. Parise, *Electric Infrastructures Equalized to Strategic for Disaster Recovery in Emergencies*, In Proceedings of the 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe); IEEE (2018), pp. 1–5
10. L. Globa, I. Volvach, *Mobile networks disaster recovery*, In Proceedings of the The Experience of Designing and Application of CAD Systems in Microelectronics; IEEE (2015), pp. 84–86
11. Volvach, I.; Globa, L. Mobile networks disaster recovery using SDN-NFV. In Proceedings of the 2016 International Conference Radio Electronics & Info Communications (UkrMiCo); IEEE, 2016; pp. 1–3.
12. Z. Agustin, V. Alex, M. Selga Josep, Heterogeneous Communication Architecture for the Smart Grid. IEEE Netw **25**, 30–37 (2011)
13. A. Khan, A. Munir, Z. Kaleem, F. Ullah, M. Bilal, L. Nkenyereye, S. Shah, L.D. Nguyen, S.M.R. Islam, K.-S. Kwak, RDSP: Rapidly Deployable Wireless Ad Hoc System for Post-Disaster Management. Sensors **20**, 548 (2020)

14. L. Nguyen, A. Kortun, T. Duong, An Introduction of Real-time Embedded Optimisation Programming for UAV Systems under Disaster Communication. EAI Endorsed Trans. Ind. Networks Intell. Syst. **5**, 156080 (2018)
15. O. Cheikhrouhou, A. Koubaa, A. Zarrad, A Cloud Based Disaster Management System. J. Sens. Actuator Networks **9**, 6 (2020)
16. X. Lv, Y. Liao, L. Deng, *Natural Disaster Emergency Rescue System Based on the Mobile Phone's High-Precision Positioning*, In Proceedings of the 2018 3rd IEEE International Conference on Image, Vision and Computing, ICIVC 2018; Institute of Electrical and Electronics Engineers Inc. (2018), pp. 797–801
17. R.P. Centelles, F. Freitag, R. Meseguer, L. Navarro, S.F. Ochoa, R.M. Santos, A LoRa-Based Communication System for Coordinated Response in an Earthquake Aftermath. Proceedings **31**, 73 (2019)
18. Dar, B.K.; Shah, M.A.; Shahid, H.; Fizzah, F.; Amjad, Z. An architecture for fog computing enabled Emergency Response and Disaster Management System (ERDMS). In Proceedings of the ICAC 2018 - 2018 24th IEEE International Conference on Automation and Computing: Improving Productivity through Automation and Computing; Institute of Electrical and Electronics Engineers Inc., 2018.
19. Davies, K. *Ionospheric Radio*; IET: The Institution of Engineering and Technology, Michael Faraday House, Six Hills Way, Stevenage SG1 2AY, UK, 1990; ISBN 9780863411861.
20. D.C. Ferguson, S.P. Worden, D.E. Hastings, The Space Weather Threat to Situational Awareness, Communications, and Positioning Systems. IEEE Trans. Plasma Sci. **43**, 3086–3098 (2015)
21. B.A. Witvliet, R.M. Alsina-Pagès, Radio communication via Near Vertical Incidence Skywave propagation: an overview. Telecommun. Syst. **66**, 295–309 (2017)
22. El ciclo solar se precipita hacia el mínimo. - Grupo Amateur de Meteorología Espacial GAME Available online: http://blog.meteorologiaespacial.es/2018/02/09/ciclo-solar-se-precipita-hacia-minimo/ (Accessed 28 Apr 2019).
23. Johnson, E.E.; Koski, E.; Furman, W.N.; Jorgenson, M.; Nieto, J. Third-generation and wideband HF radio communications; Artech House, 2013; ISBN 1608075036.
24. A. Sinha, P. Kumar, N.P. Rana, R. Islam, Y.K. Dwivedi, Impact of internet of things (IoT) in disaster management: a task-technology fit perspective. Ann. Oper. Res. **283**, 759–794 (2019). https://doi.org/10.1007/s10479-017-2658-1
25. Vasseur, J.P. Terms Used in Routing for Low-Power and Lossy Networks; RFC Editor, 2014;
26. I. Ishaq, D. Carels, G. Teklemariam, J. Hoebeke, F. Abeele, E. Poorter, I. Moerman, P. Demeester, *IETF Standardization in the Field of the Internet of Things (IoT): A Survey*, vol 2 (2013) ISBN 3293314899
27. Montenegro, G.; Kushalnagar, N.; Hui, J.; Culler, D. Transmission of IPv6 Packets over IEEE 802.15.4 Networks; RFC Editor, 2007;
28. Winter, T.; Thubert, P.; Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.P.; Alexander, R. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks; RFC Editor, 2012;
29. E. Ancillotti, R. Bruno, M. Conti, The role of the RPL routing protocol for smart grid communications. IEEE Commun. Mag. **51**, 75–83 (2013)
30. J. Nassar, M. Berthomé, J. Dubrulle, N. Gouvy, N. Mitton, B. Quoitin, Multiple instances QoS routing in RPL: Application to smart grids. Sensors (Switzerland) **18**(8), 2472 (2018)
31. Levis, P.; Clausen, T.; Hui, J.; Gnawali, O.; Ko, J. The Trickle Algorithm; RFC Editor, 2011;
32. P.P. Ray, S. Agarwal, *Bluetooth 5 and Internet of Things: Potential and architecture. In Proceedings of the International Conference on Signal Processing, Communication, Power and Embedded System, SCOPES 2016 - Proceedings; Institute of Electrical and Electronics Engineers Inc.* (2017), pp. 1461–1465
33. S. Bluetooth, *Specification of the Bluetooth System-Covered Core Package version: 4.0* (2010)
34. M. Collotta, G. Pau, T. Talty, O.K. Tonguz, Bluetooth 5: A Concrete Step Forward toward the IoT. IEEE Commun. Mag. **56**, 125–131 (2018)
35. Cerf, V.; Burleigh, S.; Hooke, A.; Torgerson, L.; Durst, R.; Scott, K.; Fall, K.; Weiss, H. Delay-Tolerant Networking Architecture; RFC Editor, 2007;
36. T. Spyropoulos, R.N.B. Rais, T. Turletti, K. Obraczka, A. Vasilakos, Routing for disruption tolerant networks: Taxonomy and design. Wirel. Networks **16**, 2349–2370 (2010)
37. R.C. Shah, S. Roy, S. Jain, W. Brunette, Data Mules: Modeling and Analysis of a Three-Tier Architecture for Sparse Sensor Networks. Elsevier Ad Hoc Netw. **1**, 215–233 (2003)
38. IEEE 802.1 Available online: available: https://1.ieee802.org/ (Accessed 18 Apr 2019).
39. J. Sánchez, G. Corral, R. Martín de Pozuelo, A. Zaballos, Security issues and threats that may affect the hybrid cloud of FINESCE. Netw. Protoc. Algorithms **8**, 26 (2016)
40. A. Zaballos, J. Navarro, R.M. De Pozuelo, A custom approach for a flexible, real-time and reliable software defined utility. Sensors (Switzerland) **18**, 718 (2018)
41. S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in Internet of things: The road ahead. Comput. Networks **76**, 146–164 (2015)
42. J. Granjal, E. Monteiro, J.S. Silva, Security for the internet of things: a survey of existing protocols and open research issues. IEEE Commun. Surv. Tutorials **17**, 1294–1312 (2015)
43. C. Adjih, E. Baccelli, E. Fleury, G. Harter, N. Mitton, T. Noel, R. Pissard-Gibollet, F. Saint-Marcel, G. Schreiner, J. Vandaele, et al., *FIT IoT-LAB: A large scale open experimental IoT testbed*, IEEE World Forum Internet Things, WF-IoT 2015 - Proc (2015), pp. 459–464
44. FIT/IoT-LAB Very large scale open wireless sensor network testbed Available online: https://www.iot-lab.info/ (Accessed 14 Apr 2019).
45. Thingsquare Contiki: The Open Source Operating System for the Internet of Things. Available online: http://www.contiki-os.org (Accessed 18 Apr 2019).
46. Get Started With Contiki, Instant Contiki and Cooja | V Mware | Digital & Social Media. Available: https://es.scribd.com/document/392384210/Get-Started-With-Contiki-Instant-Contiki-and-Cooja. Accessed 15 Sept 2020
47. Python Software Foundation Welcome to Python.org Available online: https://www.python.org/ (Accessed 18 Apr 2019).
48. Y.G. Sahin, T. Ince, Early Forest Fire Detection Using Radio-Acoustic Sounding System. Sensors **9**, 1485–1498 (2009)
49. Y.G. Sahin, Animals as mobile biological sensors for forest fire detection. Sensors **7**, 3084–3099 (2007)
50. C. Price, Lightning sensors for observing, tracking and nowcasting severe weather. Sensors **8**, 157–170 (2008)

51. J. Porte, J. Maso, J.L. Pijoan, M. Miret, D. Badia, J. Jayasinghe, *Education and e-health for developing countries using NVIS communications* (2019), pp. 1–5
52. J. Porte, J. Maso, J.L. Pijoan, D. Badia, Design, implementation and test of a SDR for NVIS communications. J. Circuit Theory Appl. **47**(9), 1502–1512 (2019)
53. J. Porté, J. Lluis Pijoan, J. Masó, D. Badia, A. Zaballos, and R. Maria Alsina-Pagès, Advanced HF Communications for Remote Sensors in Antarctica. In Antarctica - A Key To Global Change, IntechOpen, London, 2019. https://doi.org/10.5772/intechopen.81108
54. J. Maso, J. Porte, J.L. Pijoan, D. Badia, in *Proceedings of the HF Nordic*. Internet of things communications for remote sensors in Antarctica using NVIS (Fårö, 2019)
55. J. Porte, J.M. Maso, J.L. Pijoan, D. Badia, Sensing system for remote areas in Antarctica. Radio Sci **55**, e2019RS006920 (2020)

Publisher's Note