applied sciences

Article

Combining LoRaWAN and NB-IoT for Edge-to-Cloud Low Power Connectivity Leveraging on Fog Computing

Giacomo Peruzzi [1] and Alessandro Pozzebon [2,*]

[1] Department of Information Engineering and Mathematics, University of Siena, 53100 Siena, Italy; peruzzi@diism.unisi.it
[2] Department of Information Engineering, University of Padova, 35131 Padova, Italy
* Correspondence: alessandro.pozzebon@unipd.it

Abstract: Low Power Wide Area Networks (LPWANs) play crucial roles in the implementation of low-power and low-cost wide area distributed systems. Currently, two enabling technologies are the main competitors within the connectivity field for the Internet of Things (IoT), primarily because of their scalability, wide range and low power features: Long Range Wide Area Network (LoRaWAN) and Narrowband IoT (NB-IoT). In this paper, a brand new network architecture is presented, which combines both aforementioned technologies. Such a network accounts for sensor nodes, multi-protocol gateways, an a cloud infrastructure. Sensor nodes may be alternatively provided with LoRaWAN or NB-IoT. Multi-protocol gateways can receive and demodulate LoRaWAN packets and upload them to the cloud via the Message Queue Telemetry Transport (MQTT) protocol over NB-IoT. The cloud is transparent with respect to the transmission technology, meaning that data are acquired and stored regardless of the exploited technique (i.e., LoRaWAN or NB-IoT). Indeed, sensor nodes using NB-IoT can send data to the cloud and can directly communicate with other NB-IoT nodes setting up a fog computing paradigm on peer-to-peer subnetworks. This approach may be crucial for the development of complex IoT infrastructures while providing high flexibility.

Keywords: LoRaWAN; NB-IoT; edge computing; fog computing; cloud; peer-to-peer; MQTT; low power

check for updates

Citation: Peruzzi, G.; Pozzebon, A. Combining LoRaWAN and NB-IoT for Edge-to-Cloud Low Power Connectivity Leveraging on Fog Computing. *Appl. Sci.* **2022**, *12*, 1497. https://doi.org/10.3390/app12031497

Academic Editors: Fabrizio Granelli, Dan García Carrillo, Laurent Toutain and Rafael Marín López

Received: 16 October 2021
Accepted: 28 January 2022
Published: 30 January 2022

1. Introduction

The rapid diffusion of Internet of Things (IoT)-based facilities is leading to the definition of day-by-day more complex technological architectures, encompassing a large number of devices ranging from simple sensor nodes to complex edge computing equipment within single heterogeneous infrastructures. The different requirements of these elements have paved the way to the adoption of a plethora of different data transmission technologies, of which the technical features are designed to satisfy specific system requisites. In particular, they have driven the technological development of IoT data transmission techniques that implement crucial characteristics for a myriad of application scenarios: reduced power consumption, long transmission range and low cost. In the last five years, a number of technologies satisfying these requirements emerged, leading to the definition of the Low Power Wide Area Network (LPWAN) concept. Under the LPWAN umbrella, well-known technologies such as SigFox, Long Term Evolution for Machines (LTE-M), Long Range Wide Area Network (LoRaWAN) and Narrow Band IoT (NB-IoT) lie at the moment, for which the specific features can lead to the choice of any of them according to the needs of the application scenario.

Nevertheless, the different features of these technologies may also be simultaneously exploited to create more complex network architectures, with the aim of covering specific operational gaps that may emerge when shaping network infrastructures to specific application contexts. One example concerns the usability of LoRaWAN networks in remote places, where some kind of network connection is required for packet forwarding from LoRaWAN Gateways to the Network Server. This is in general provided by means of standard cellular connectivity, relying on power-consuming radio modules, thus requiring some kind of continuous power source (e.g., energy harvesting systems or mains). Other examples include coexistence within the same network of standalone nodes and sub-clusters: in this case, different technologies may be combined according to the specific needs. For example, standalone SigFox nodes may be enabled to exchange data with LoRaWAN Nodes that are integrated into LoRaWAN sub-networks.

With the aim of demonstrating the feasibility of this typology of architectures, this paper focuses on two specific technologies, belonging to the two macro-areas in which LPWANs are usually distinguished (i.e., the cellular and the non-cellular ones). Among cellular LPWANs, NB-IoT [1,2] is the one that has seen the largest diffusion and has been widely employed in several application scenarios [3–5]. The non-cellular chosen one is LoRaWAN, which can be actually considered as de facto standard among non-licensed LPWANs operating in the sub-GHz band (i.e., at frequencies below 1 GHz). Since LoRaWAN demonstrated excellent features in terms of transmission distance and low power consumption [6–8], it was applied in a plethora of different use-cases [9–11]. Despite their diffusion, these two technologies were integrated within the same infrastructure, though only in very limited cases.

This paper attempts to fill this gap by demonstrating the feasibility of a hybrid LoRaWAN-NB-IoT network, pointing out the achievable improvements and the different implementable services. In particular, the usage of NB-IoT as a link between LoRaWAN Gateways and the Cloud is experienced: this solution is relevant in all applications concerning a limited number of LoRaWAN End Devices, each of them transmitting a reduced amount of data. In this case, the throughput of the NB-IoT link can be considered adequate to ensure packet forwarding, with a notable reduction in power consumption with respect to other standard cellular connections. At the same time, the bidirectional integration of the two technologies within an interoperable network is tested: this may allow for direct packet exchange among nodes regardless of the transmission technology, with an increase in the flexibility of the overall infrastructure with respect to the usage of the single communication technologies on their own.

The rest of the paper is arranged as follows. Section 2 proposes a literature review composed of some related work, while Section 3 describes the network architecture as well as each of the network components. Section 4 reports some tests aimed at assessing network functioning, feasibility and reliability, while the relative results are reported and discussed in Section 5. Finally, Section 6 highlights the conclusions and final remarks.

2. Related Works

The concept of hybrid networking within the IoT domain has been discussed in a number of papers. Before the emergence of LPWAN facilities, the cooperation of different radio technologies was already evaluated within Wireless Sensor Network (WSN) architectures, for example combining ZigBee and Ultra Wide Band to differentiate data transmission according to the specific application requirements [12]. The rise in LPWANs has paved the way to the implementation of massive and dense network architectures, with an exponential growth in the number and complexity of interconnected devices that act as drivers for the definition of future communication techniques [13]. In this context, the combination of multiple radio technologies was considered a viable solution to create modular networks to satisfy different intricacy levels.

Focusing on the two technologies exploited in this paper, some examples of hybrid networks emerge for both, with a prominence of LoRaWAN-based solutions. A theoretical approach focusing on the integration of different LPWANs forming hybrid networks is proposed in [14]: while the actual implementation of the network is not described in detail, the proposed architecture is prone to the integration of the most LPWAN standards in cooperation with other cellular (i.e., LTE) and non-cellular (i.e., Wi-Fi) data transmission technologies.

Hybrid LoRaWAN solutions were proposed with a number of communication techniques: however, most examples in the literature mainly leverage the Long Range (LoRa) physical layer, without implementing a full LoRaWAN infrastructure. An obvious integration is the one with Bluetooth Low Energy (BLE), thus combining low power local area and wide area connectivity: in [15], BLE was employed to set up local data transmission among nodes that were integrated in LoRa clusters, while BLE connectivity was seen as a local area extension of a LoRa network in [16]. Finally, an integration at the physical layer between the two technologies was proposed in [17]. In parallel with LoRa, NB-IoT was also integrated with BLE: in [18,19], both channels were simultaneously exploited for data transmission according to a multi-modal paradigm that was based on the optimisation of power consumption. The extension of a LoRaWAN network with short range connectivity was also discussed in [20], where LoRaWAN Class A devices were integrated with Wake up Radio (WuR) low-power radio modules that were ad hoc designed to consistently reduce the power consumption of the edge segment of the network.

LoRa networks were also integrated with other wide area technologies: while the standard configuration of a LoRaWAN network foresees the presence of an Internet connection between Gateways and Server, that is in general set up with Ethernet, WiFi or 4G connections, some work focused on architectures where this link was set up via satellite [21] or Fifth Generation (5G) cellular connection [22]. In the context of 5G connectivity, Chandrashekar et al. [23] applied the concept of multiple Radio Access Technologies (Multi-RAT), whihc was successively extended to LoRa and 4G in [24].

The concept of Multi-RAT has been recently expanded to the convergence of LoRaWAN and NB-IoT into hybrid networking: in particular, in [25], a theoretical analysis was carried out to assess the achievable benefits with the implementation of this kind of infrastructure, while in [26], a prototype of a hybrid LoRaWAN-NB-IoT node was described and tested, mainly in terms of power consumption. However, with respect to the one proposed in this work, the systems described in [25,26] were basically end devices provided with both data transmission technologies: the two channels could be used alternatively or in parallel but were not integrated to set up a hybrid channel. Together with these two works, only another contribution addresses the combination of these two technologies by proposing the design of a very simple LoRa-NB-IoT Gateway for packet forwarding scopes [27]. However, notable differences can be found between that work and this paper. First, only the LoRa physical layer is exploited in this hybrid gateway, thus notably limiting the field of use of this solution. Indeed, the LoRaWAN protocol is crucial for the management of a large quantity of end devices. Second, only a very simple, Arduino-based multi-protocol gateway is presented: conversely, this paper proposes a multi-purpose network architecture where different combinations of the two technologies are set up, allowing for transparent usage of the network independent from the specific transmission technology.

Then, despite these last contributions, to the best of the authors knowledge, the definition of a fully interoperable LoRaWAN-NB-IoT infrastructure such as the one presented in this paper, allowing for transparent, bidirectional data transmission between nodes regardless of the specific technology, together with the packet forwarding to the Cloud without the usage of any traditional Internet connectivity, has been never presented before.

3. Network Architecture Description

The network architecture is schematically outlined in Figure 1. For the sake of clarity, such a network is fully modular and scalable to be employed in the most diverse application scenarios. These features foster the network usability even in harsh and critic contexts. The network is made of three stacked layers: Sensor Nodes, Forwarding and the Cloud. As its name suggests, the Sensor Nodes Layer includes the network sensor nodes. In particular, they are of a twofold species depending on the communication technology upon which they rely: LoRaWAN Nodes and NB-IoT Nodes. The Forwarding Layer is in charge of forwarding data from the Sensor Nodes Layer to the Cloud Layer and viceversa. To this end, such Layer is composed of LoRaWAN-NB-IoT Gateways, which are de facto multi-protocol Gateways, and Long-Term Evolution (LTE) base stations, named evolved Node B (eNodeB), which are in charge of running the NB-IoT network. Finally, the Cloud Layer is responsible for collecting and storing data as well as for arranging downlinks towards the sensor nodes and for allowing users to interact with the whole system. Each of the layers components are described in detail later on.

This network allows for bidirectional transmissions. Indeed, the devices within the Sensor Nodes Layer can be equipped with sensors and/or actuators. Therefore, users may issue commands to be executed by the nodes on the basis of what they sense within the deployment environment. Moreover, such commands may be also automatically emitted by the Cloud itself (e.g., whenever a physical phenomenon exceeds a certain threshold). In addition, NB-IoT Nodes are capable of setting up a peer-to-peer subnetwork to directly exchange data between them without involving either the users or the Cloud. Given the network functioning scheme, an edge-to-cloud connectivity framework is set up along with a fog computing paradigm due to the fact that data are sparsely processed throughout all of the network layers.

Finally, three different communication protocols are involved. The first one is the well-known LoRa modulation, which provides LoRaWAN Nodes with wireless connectivity as the LoRaWAN standard prescribes. Second, the Message Queue Telemetry Transport (MQTT) protocol over NB-IoT is involved. It is exploited by the NB-IoT Nodes to communicate towards eNodeBs. Finally, the MQTT protocol over LTE is concerned, by which eNodeBs forward and receive data to and from the Cloud Layer.

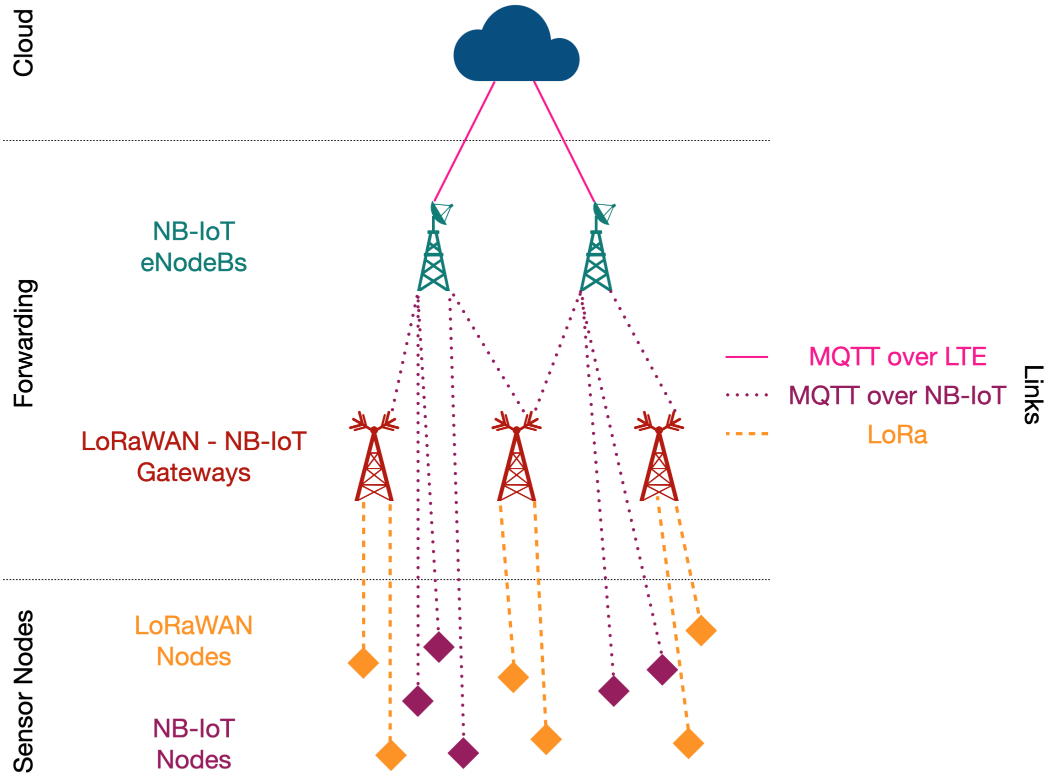


Figure 1. Network architecture overview.

3.1. Sensor Nodes Layer

The sensor node architecture is the standard one of any node-forming WSN (see Figure 2), and this section highlights the modularity and flexibility of the network. In general, the node in its minimal form is composed of a microcontroller, an energy source, sensors and/or actuators, and a transceiver. Each of these components could be an off-the-shelf solution as well as an ad hoc customised one. The microcontroller is the core of the device since it is in charge of managing all of the peripheral, along with carrying out all of the routines that are hardcoded in its firmware. The energy source could be either a non-renewable one (e.g., batteries) or a renewable one (e.g., solar energy). Of course, this choice is strongly dependent on the application scenario and on the overall system requirements. In addition, miscellaneous electronics are usually required to correctly power the sensor node (e.g., voltage regulators) or to properly exploit the selected renewable energy source (e.g., battery management systems). Similarly, the choice of sensors and actuators is fully subject to the extent and the type of physical phenomenon to be monitored (e.g., temperature or humidity) or to the kind of action to be executed (e.g., controlling the state of an opening, or switching on and off external appliances). Finally, the transceiver is fundamental for providing the node with connectivity to remotely control it and to allow the node to send data. Sensor nodes within the network of this paper can alternatively embed LoRaWAN or NB-IoT transceivers.

LoRaWAN Nodes bidirectionally communicate towards the LoRaWAN-NB-IoT multi-protocol Gateways by exploiting LoRa modulation as it usually happens within standard LoRaWAN networks. Similarly, NB-IoT Nodes establish a bidirectional communication with the eNodeBs. However, NB-IoT Nodes exploit the MQTT protocol over NB-IoT to send and receive information. Thus, the network allows for both uplinks and downlinks. At the same time, NB-IoT Nodes are capable of setting up subnetworks with the aim of establishing a peer-to-peer paradigm that still relies on MQTT. Such a feature provides for an autonomous connectivity scheme to which the nodes can resort whenever neither actions from users nor controls at the Cloud Layer are required. For instance, this technique is effective in all contexts in which the state of an actuator must be changed upon the occurrence of a given event that is properly sensed at the edge of the network.

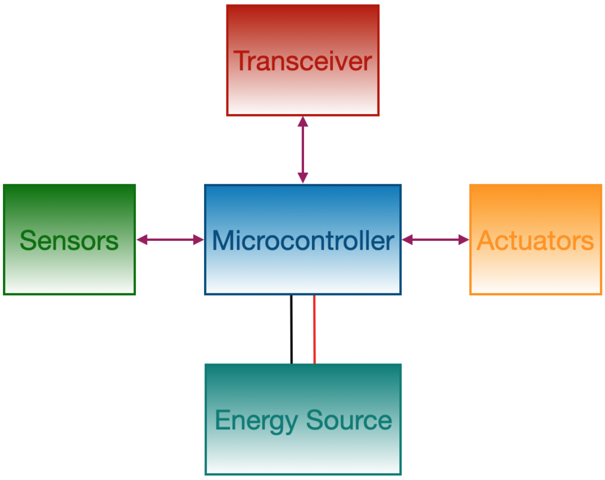
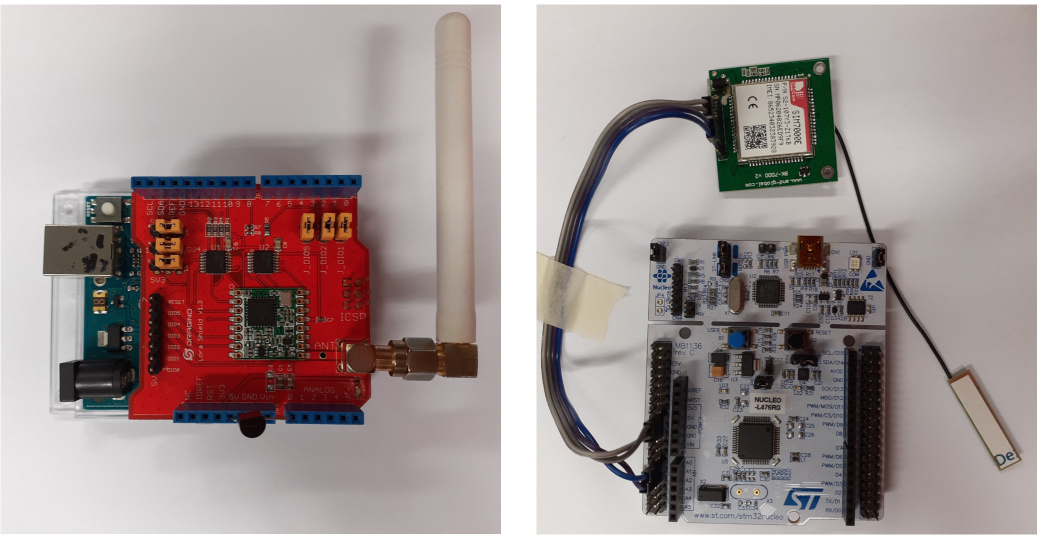


Figure 2. Sensor node general architecture block scheme.

MQTT protocol was originally invented by IBM two decades ago. As it is stated in its reference website [28], MQTT is a publish/subscribe, extremely simple and lightweight messaging protocol designed for constrained devices with low bandwidth and high latency within unreliable networks. The design principles are to minimise network bandwidth and device resource requirements whilst also attempting to ensure reliability and some degree of assurance of delivery. These principles also turn out to make the protocol ideal for emerging Machine to Machine (M2M) or the IoT world of connected devices and for mobile applications where bandwidth and battery power are at a premium. In MQTT systems, there are a multitude of clients communicating with a server, which is also known as a broker, once they establish a prior connection to it. Clients may be either publishers and subscribers. In particular, a client could behave as a publisher and a subscriber at the same time. Publishers exchange messages enveloping information with subscribers by posting them on topics that have a hierarchical structure (e.g., `this/is/a/topic`), to which clients have subscribed. Between publishers and subscribers, there is the broker, whose task is to take charge of all of the messages posted by the publishers and to forward them to any clients that have subscribed to the topic on which those messages were posted.

Therefore, to test the network functionalities, minimal sensor nodes were developed by resorting to off-the-shelf components only (see Figure 3). Moreover, hardware components (e.g., microcontrollers) of LoRaWAN Nodes were different with respect to the ones of NB-IoT Nodes to pinpoint the modularity and the flexibility of the network. However, it has to be underlined that whichever node that is compliant, at least in a weak sense, with the block scheme of Figure 2 can be exploited within the network.



(**a**) (**b**)

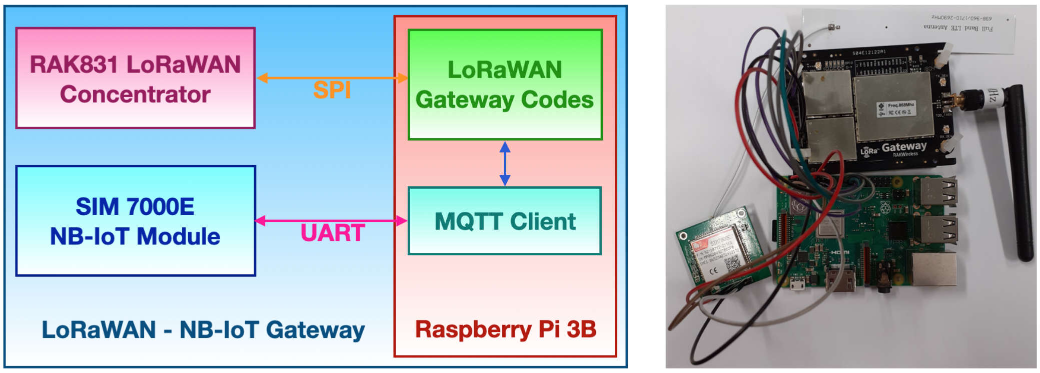
Figure 3. Sensor node hardware implementation: (**a**) LoRaWAN Node; (**b**) NB-IoT Node.

LoRaWAN Nodes were composed of an Arduino UNO board and a LoRa shield manufactured by Dragino. The latter embeds a LoRa transceiver (i.e., the HRF95 made by HopeRF), which relies on a Semtech SX1276 LoRa module. The shield also features an antenna connector to which a $\lambda/8$ whip antenna was attached. The microcontroller implements a LoRaWAN Class A device. In particular, it encrypts the packets payload twice by exploiting both the Network Session Key (NwkSKey) and the Application Session Key (AppSKey) by means of an Advanced Encryption Standard (AES) (i.e., AES-128). In addition, packets are wirelessly sent to any LoRaWAN-NB-IoT Gateway in the nodes closeness via LoRa links. They are set up by establishing a frequency diversity scheme via a frequency hopping technique amid eight different channels belonging to the 863–870 MHz Industrial, Scientific and Medical (ISM) band. Nonetheless, regional regulation concerning the time occupancy of ISM bands (i.e., in Europe and for the aforementioned ISM band, the spectrum can be occupied for no longer than the 1% of the time by each of the transmitters) are abode by. Finally, a simple temperature sensor (i.e., the LM35 made by Texas Instruments) was included since it is useful for the testing phases of the network. Conversely, NB-IoT Nodes were composed of a Nucleo-L476RG board produced by STMicroelectronics, which drives an NB-IoT transceiver (i.e., the SIM7000E manufactured by SIMCom). Such a transceiver allows for both LTE Machine Type Communication (LTE-MTC) and NB-IoT communication. Connectivity is ensured via a a micro Subscriber Identity Module (SIM) card, belonging to the Italian telco provider TIM, which is especially devoted to M2M cellular communication purposes. As it will be explained later on, all of the network nodes were powered via a USB port of a PC since it is exploited as a sort of data-logger throughout the network testing procedures. Nevertheless, the energy source chosen had to be feasible provided that it fits the application scenario at hand.

3.2. Forwarding Layer

The Forwarding Layer is composed of two different entities: LoRaWAN-NB-IoT Gateways and NB-IoT eNodeBs. Herein, only LoRaWAN-NB-IoT Gateways can be described because eNodeBs are directly designed, set up and maintained by the telco providers, while LoRaWAN-NB-IoT Gateways can be designed and implemented in the same vein of the components of the network Sensor Nodes Layer.

Figure 4 shows both the LoRaWAN-NB-IoT Gateway block scheme and its hardware implementation. It is in charge of demodulating incoming LoRaWAN packets and of forwarding the associated data and metadata to the Cloud Layer by resorting to the MQTT protocol over NB-IoT. Indeed, such devices are equipped with both a LoRaWAN concentrator and an NB-IoT module: the former deals with the LoRaWAN signals, while the latter copes with NB-IoT communication.



(**a**) (**b**)

Figure 4. LoRaWAN-NB-IoT Gateway: (**a**) block scheme; (**b**) hardware implementation.

The concentrator (i.e., the RAK831 produced by RAKWireless) is a device that features a LoRa modem and two LoRa transceivers: the former is a Semtech SX1301, while the latter ones are two Semtech SX1257. Thus, the concentrator is capable of simultaneously receiving up to eight LoRaWAN packets on as many different channels as possible. This hardware setup allows for a very high sensitivity spanning from −126 dBm down to −137 dBm in function of the transmission parameters (i.e., the bandwidth and the Spreading Factor). The concentrator is driven by a Raspberry Pi 3 model B+ by exploiting the Serial Peripheral Interface (SPI) bus. The Raspberry Pi is also in charge of coping with data forwarding towards the Cloud Layer by relying on an Internet connection. Normally, it is ensured by making use of either Wi-Fi or Ethernet ports that the Raspberry Pi is provided with, but LoRaWAN-NB-IoT Gateways accomplish such tasks by exploiting an NB-IoT module instead. In particular, the same NB-IoT module of the NB-IoT Nodes (i.e., the SIM7000E) is chosen, and it is driven by the Raspberry Pi via the Universal Asynchronous Receiver-Transmitter (UART) peripheral. The choice of providing the gateways with Internet connectivity via NB-IoT, rather than Wi-Fi or Ethernet, fosters the gateways installation within harsh or critic environments. Indeed, therein, the chance of a standard Internet connection availability is often low. By contrast, by relying on a cellular technology, a pervasive coverage can be ensured. However, standard cellular facilities (e.g., 4G) have non-negligible drawbacks: high running costs and high power consumption. Fortunately, NB-IoT solution counteracts such shortcomings, thus entailing from the one hand the limitation of running costs (which is strongly dependent on the subscribed data plan) and from the other hand a notable power consumption reduction that potentially allows for the adoption of batteries or renewable sources of energy for powering the gateway. Finally, for what concerns the gateway software components, two units are run. All of the gateway routines dealing with the radiofrequency interfaces are implemented within a multi-thread C program. It exchanges data through a local socket with a Python script that connects to the eNodeBs, resorting the the MQTT protocol via NB-IoT. Thus, data coming from LoRaWAN Nodes are forwarded to the Cloud Layer.

3.3. Cloud Layer

The network Cloud Layer is shown in Figure 5. It is principally formed by an MQTT broker; MQTT clients; two server routines; and a MySQL database, which is devoted to the storage of all of the incoming information broadcast by the nodes. In other words, the network Cloud Layer directly derives from the one of a previous work [29]. The servers are the Network Server and the Application Server. Both of them are implemented by resorting to Node-RED (i.e., a flow programming language grounded on JavaScript). It is a development environment originally issued by IBM that relies on Node.js (i.e., a run-time environment carrying out JavaScript snippets outside a browser in order to allow their usage on the server side). Conversely, the exploited MQTT broker is Mosquitto, which was released by Eclipse open source. It is in charge of forwarding MQTT messages from MQTT clients, prior to their successful connection to the broker itself. Indeed, the core of MQTT is the broker, since all of the clients stand on its shoulders because it routes all of the messages. Clients may be publishers and/or subscribers, and in particular, a client could behave as publisher and subscriber at the same time. The network of this paper includes MQTT clients in the LoRaWAN-NB-IoT Gateway, in the NB-IoT Nodes and in the Network Server. Specifically, all of them simultaneously behave as publishers and subscribers. Publishers exchange messages enveloping information with subscribers by posting them on topics to which the latter clients are subscribed. Between publishers and subscribers, there is the broker that all those clients were previously connected to, whose task is to take charge of all of the messages posted by the publishers and to forward them to any client who is subscribed to the topic on which those messages were posted.

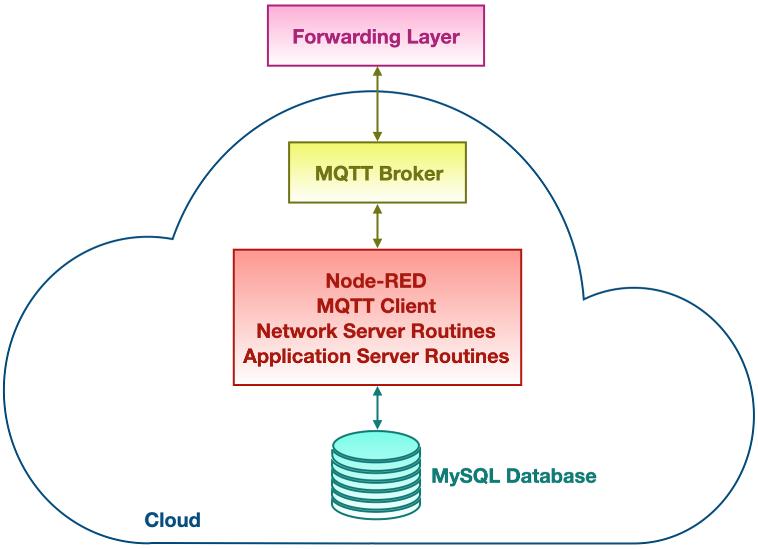


Figure 5. Cloud Layer block scheme architecture. The Forwarding Layer is included for the sake of completeness. Marsh grass arrows represent MQTT links, while the turquoise arrow stands for database connections.

The Network Server is carried out via a Node-RED flow, and it works as follows (see Figure 6). Two different types of MQTT clients are concerned in such a server: the former is related to LoRaWAN-NB-IoT Gateways, while the latter is related to NB-IoT Nodes. To make the explanation clearer, let us consider that a message from the Gateways is received by the Server. No sooner had such a message arrived than the Server sent back an acknowledgment to the Gateway at hand by exploiting the MQTT protocol to perform a network diagnostic. Then, the Server checks the type of data within the incoming message. Indeed, it could contain either Gateway functioning statistics or data from the LoRaWAN Nodes. In the former case, the statistics are processed and then stored within the database. In the latter case, the Server accomplishes further routines. In the case of multiple Gateway deployments, it is highly likely that a packet coming from a LoRaWAN Node could be received and therefore forwarded to the Cloud Layer by multiple Gateways. Therefore, the Network Server filters out such duplicates. Successively, the Server decrypts the LoRaWAN packets by resorting to the NwkSKey and to the AppSKey. Such a procedure gives both the decrypted payload and the Message Integrity Code (MIC) as the outcome. Thus, the MIC is controlled because it could be either valid or invalid. If it is valid, then, the payload at hand was decrypted with the same AES keys with respect to the exploited ones used to encrypt it. This translates into the fact that the transmitting node at hand belongs to this network. On the other hand, if an invalid MIC is generated, then the AES keys used in turn for encryption and decryption are different, thus meaning that the transmitting node at hand does not belong to this network, and the relative packet is discarded. Consecutively, if a valid MIC is observed, then the packet is processed and further controlled. Indeed, it could additionally contain commands to issue to NB-IoT Nodes (as it will be shown later on (see Section 4.2) within a particular a test scenario). In such a case, the command is prepared to be given to the relative NB-IoT Node by exploiting the MQTT protocol. Finally, regardless of the presence of commands for NB-IoT Nodes, the data within the LoRaWAN packets are stored within the database. Conversely, let us suppose that packets from NB-IoT Nodes are received by the Server. In this case, no controls are performed since only NB-IoT Nodes belonging to the network are allowed to send data to the Network Server. Therefore, the data are processed and then stored within the database.

For the sake of completeness, it has to be underlined that the Network Server does not take charge of the data or information flowing whenever a peer-to-peer network is setup. This is due to the fact that, in this condition, only NB-IoT Nodes are included. They directly communicate with each other, relying on the MQTT protocol, thus forming a decentralised network; therefore, only the MQTT broker is involved.

The Application Server is carried out by means of Node-RED too. Its routine is far easier than the ones of the other server. Indeed, it just extracts data from the database to makes it available to users by exploiting graphic interfaces that can be requested by Internet browsers running on PCs, tablets, smartphones, etc. Therefore, such a server acts as the network interface.

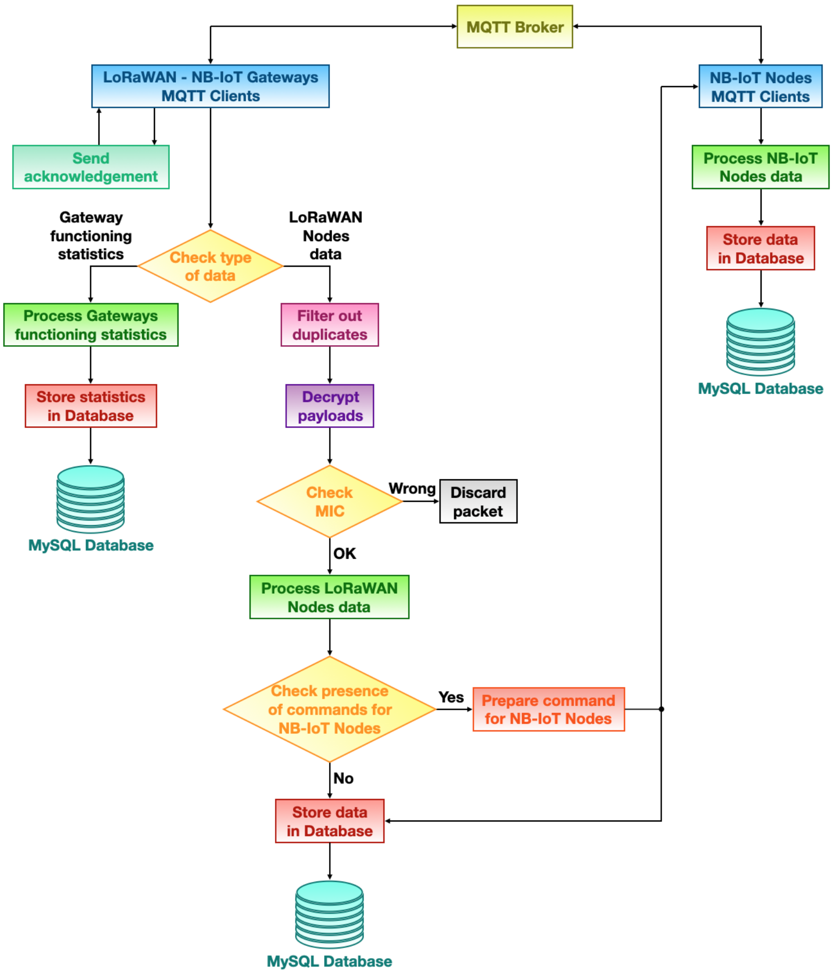

MQTT Broker
LoRaWAN - NB-IoT Gateways MQTT Clients
NB-IoT Nodes MQTT Clients
Send acknowledgement
Gateway functioning statistics
Check type of data
LoRaWAN Nodes data
Process Gateways functioning statistics
Filter out duplicates
Store statistics in Database
Decrypt payloads
MySQL Database
Check MIC
Wrong
Discard packet
OK
Process LoRaWAN Nodes data
Check presence of commands for NB-IoT Nodes
Yes
Prepare command for NB-IoT Nodes
No
Store data in Database
MySQL Database
Process NB-IoT Nodes data
Store data in Database
MySQL Database

Figure 6. Network Server block scheme. The MQTT broker is included for the sake of completeness.

4. Tests

The network was tested by setting up three different functioning schemes that are often found in a myriad of application scenarios. Such frameworks were devised so to reproduce typical use cases of WSN. Packet loss, Round Trip Time (RTT), latency and power consumption of the LoRaWAN-NB-IoT Gateway were considered as metrics for network performance assessment. On the other hand, another interesting characteristic to be assessed for network performances is bandwidth. However, such a feature is established a priori by both the LoRaWAN and NB-IoT standards, making such a parameter un-tunable when performing a sort of sensitivity analysis to be translated into an additional metric for network performances.

4.1. Test #1

Test #1 represents the most basic example of data gathering by means of WSN: measuring a physical phenomenon and transmitting such sample on a temporal basis. Throughout this testbed, only LoRaWAN Nodes were employed since they suit situations when data need to be periodically sent. In particular, a LoRaWAN Node embedding the LM35 temperature sensor was exploited, and the room temperature of a laboratory was sampled and broadcast for a 50 h timespan. LoRaWAN packets were transmitted by exploiting a bandwidth of 125 kHz, a Spreading Factor of 7 and a coding rate of 4/5 and by sending a packet every 48.6 s. The aim of this test was to assess neither the quality of the measurements nor the performances of the LoRaWAN node (indeed, both of them are quite trivial to evaluate and, at the same time, they are not so meaningful). Actually, this test rates the performance of the LoRaWAN-NB-IoT Gateway in terms of packet loss. Since the gateway and the node were placed 2 m apart, it is reasonable to deem that no packet loss occurred in the LoRa links in between the node and the gateway. Therefore, data loss can be ascribed to anomalous behaviours of the gateway or to the lack of cellular coverage.

4.2. Test #2

Test #2 examines the system capability of setting up a peer-to-peer subnetwork. Throughout these trials, only two NB-IoT Nodes were employed since NB-IoT technology is far more suitable than LoRaWAN whenever the necessity of data interchanging between nodes arises. Indeed, while LoRaWAN uplinks can occur at any time they are needed provided that regulations on ISM bands temporal occupancy are concerned, downlinks can only take place at specific moments just after the uplinks. Indeed, LoRaWAN protocol imposes that nodes can receive downlinks in two temporal windows, which are opened only after each of the uplinks. Once such windows expire, the node is virtually unreachable unless it performs an additional uplink. On the other hand, NB-IoT is not subject to such a functioning scheme, thus resulting in being more appropriate in this context. In particular, the experiment was carried out by resorting to the following methodology. One of the nodes acted as the master, while the remaining one was the slave. The master sent an NB-IoT packet, which contained a progressive counter as the payload, to the slave via MQTT over NB-IoT. Then, the master waited for 30 s. No sooner had the slave received the packet, than it sent back such data to the master by making use of the same technique (i.e., MQTT over NB-IoT). If the master received the response from the slave within the timeout, then the test turned out to be successful; otherwise, it did not. In the former case, the RTT was measured since it was considered a significant test metric along with the success rate of packets received by the master from the slave. RTTs were measured by exploiting a PC. In particular, the master was connected to a PC USB port that was monitored by the PC itself. Indeed, the master logged through the events resulting from the process of sending data to the slave and from the process of receiving the slave response, if it occurred, to the serial port. Each of the logs had the incremental counter within the payload since it was logged too. Then, the PC recorded the respective timestamps associated with such events to calculate RTTs by performing a subtraction, along with the logs coming from the master. The USB port monitoring as well as the recording of the timestamps were accomplished via a Python script, while RTT identification, calculation and analysis were carried out by resorting to MATLAB. Specifically, RTTs had to be identified by making use of the progressive counter in the packet payload, since if the timeout expired, then no RTT was measured and the relative packet was considered lost. This testing scenario reproduces all of those contexts in which two nodes assiduously require interactions with each other on the basis, for instance, of the sensed environment to act on a remote part of the latter. In addition, such a framework recreates those settings in which both the nodes alternatively behave as sensors and actuators.

4.3. Test #3

Test #3 sorts out a hybrid configuration since it accounts for a LoRaWAN Node and an NB-IoT Node as well. Every minute, the LoRaWAN Node sent a packet containing an incremental counter, and such data was forwarded to the NB-IoT Node by the network Cloud Layer. The LoRaWAN Node exploited the same transmission parameters that were employed during Test #1. This setup traces all of those contexts in which an actuator has to perform some actions on the basis of what another sensor sampled: for instance, regulating the flow within a pipeline on the basis of the extent of the transported fluid at the pipeline outlet. In this scenario, the latency between the moment in which the LoRaWAN Node broadcast the packet and the moment in which the NB-IoT Node received the command from the Cloud Layer was measured, along with the packet loss. In order to limit the number of involved variables within the experiment, the exploited LoRaWAN Gateway was a standard one (i.e., Internet connectivity was provided via Ethernet rather than NB-IoT). Moreover, the LoRaWAN Node and the Gateway were positioned 2 m apart so that packet losses could be only ascribed to abnormal functioning of the NB-IoT Node or due to a lack of cellular coverage. This can be considered reliable since data loss within LoRa links is especially unlikely when just a 2 m length has to be covered. Latency was measured in a similar way with respect to the RTTs of Test #2. Indeed, a PC was still exploited. Moreover, both the nodes were connected to as many PC USB ports that were monitored by the PC itself. Similar to Test#2, the nodes logged through their serial ports events related to their functioning. In particular, the LoRaWAN node logged the fact that it sent a packet, along with the incremental counter forming the packet payload, while the NB-IoT node logged the occurrence related to the reception of a packet, still combined with the incremental counter within the payload. Then, the PC recorded the timestamps associated with such events as well as the logs coming from each node. The USB ports monitoring and the recording of the timestamps were accomplished via a Python script, while latency was identified, calculated and analysed by exploiting MATLAB. Latency had to be identified by making use of the incremental counter in the packet payload, and then, it was calculated by performing a subtraction.

4.4. Test on Power Consumption of the LoRaWAN-NB-IoT Gateway

Besides the aforementioned tests on assessing network performances with respect to several benchmark metrics, the power consumption of the LoRaWAN-NB-IoT Gateway was also assessed by measuring its current draw. In particular, such a test was carried out by comparing this consumption with the one of a LoRaWAN-4G Gateway, still by considering its current draw. The two Gateways shared the same architecture and hardware components, apart from the method they were provided with the Internet. Indeed, the former exploited the SIM7000E NB-IoT module as it was previously shown (see Section 3.2), while the latter was connected through a USB port of the Raspberry Pi to the E3372 4G dongle manufactured by Huawei. Thus, the difference amid the two technologies (i.e., NB-IoT and the standard 4G) from the point of view of power consumption can be pinpointed. Both Gateways, in particular the two Raspberry Pi, were powered via a dual channel bench power supply, and the current draws were measured with two digital multimeters Agilent 34410A. The two instruments were controlled via LabVIEW, and their readings were acquired at a sampling frequency of 5 Hz. Then, the sampled measurements were analysed by means of MATLAB. The test methodology was as follows. No sooner had the current draws acquisition started, than the Gateways were turned on. Moreover, both the devices were placed one next to the other to ensure they shared the same cellular coverage. Then, some time was waited to let the devices complete their initialisation routines. Afterwards, five LoRaWAN packets were broadcast by exploiting the same LoRaWAN Node of Test #3 (i.e., the node hardware, the payload and the transmission parameters stayed the same). The only difference with respect to the functioning scheme of the LoRaWAN Node of Test #3 was that only 15 s of inter-transmission time was considered instead of 60 s to speed up the test procedures. In addition, the LoRaWAN Node was placed 2 m apart from the Gateways to limit the number of variables within the test. Subsequently, the Gateways were turned off and the current draw acquisition was stopped.

5. Results and Discussion

All of the tests turned out to be satisfactory, first, because the overall network functioning was concerned and, then, because tests metrics were good enough to claim such that a network architecture may potentially find a wide application in a vast set of operation scenarios.

Test #1 results are shown in Figure 7. As was previously stated, this test aimed to assess the performances of the LoRaWAN-NB-IoT Gateway in terms of successfully forwarded packets from the Sensor Nodes Layer to the Cloud Layer. Throughout the test, 3724 LoRaWAN packets were broadcast by the LoRaWAN Node and 3006 packets were correctly forwarded by the gateway to the Cloud Layer (i.e., a packet loss 19.28% of was experienced). In light of this, the results of this test can be considered satisfactory, thus validating the effectiveness of the LoRaWAN-NB-IoT Gateway, mainly because of two reasons. On the one hand, LoRaWAN technology implicitly implies a minimum amount of data loss. Therefore, the adoption of the LoRaWAN-NB-IoT Gateway caused a packet loss that can be comparable with the one of the LoRaWAN protocol. On the other hand, apart from few data points, packet loss was predominantly experienced in two different circumstances (i.e., from packet number 593 to packet number 1049 and from packet number 2583 to packet number 2826). Such a phenomenon suggests that losses may be ascribed to a lack of cellular coverage rather than a gateway fault. On the contrary, all of data points related to losses lying outside the aforementioned intervals may be due to Gateway faults. However, there are only 20 instances. Therefore, it can be deemed that the LoRaWAN-NB-IoT Gateway can be a valuable alternative to standard LoRaWAN Gateways whenever the application scenario is devoid of Internet connection.

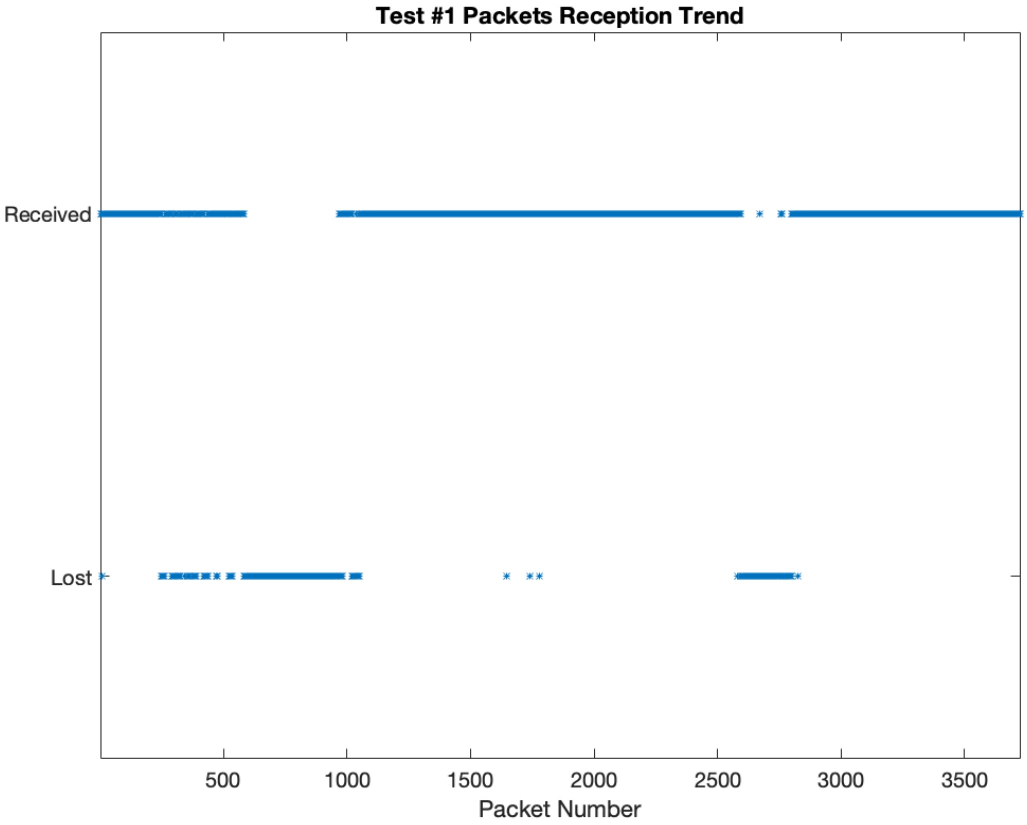
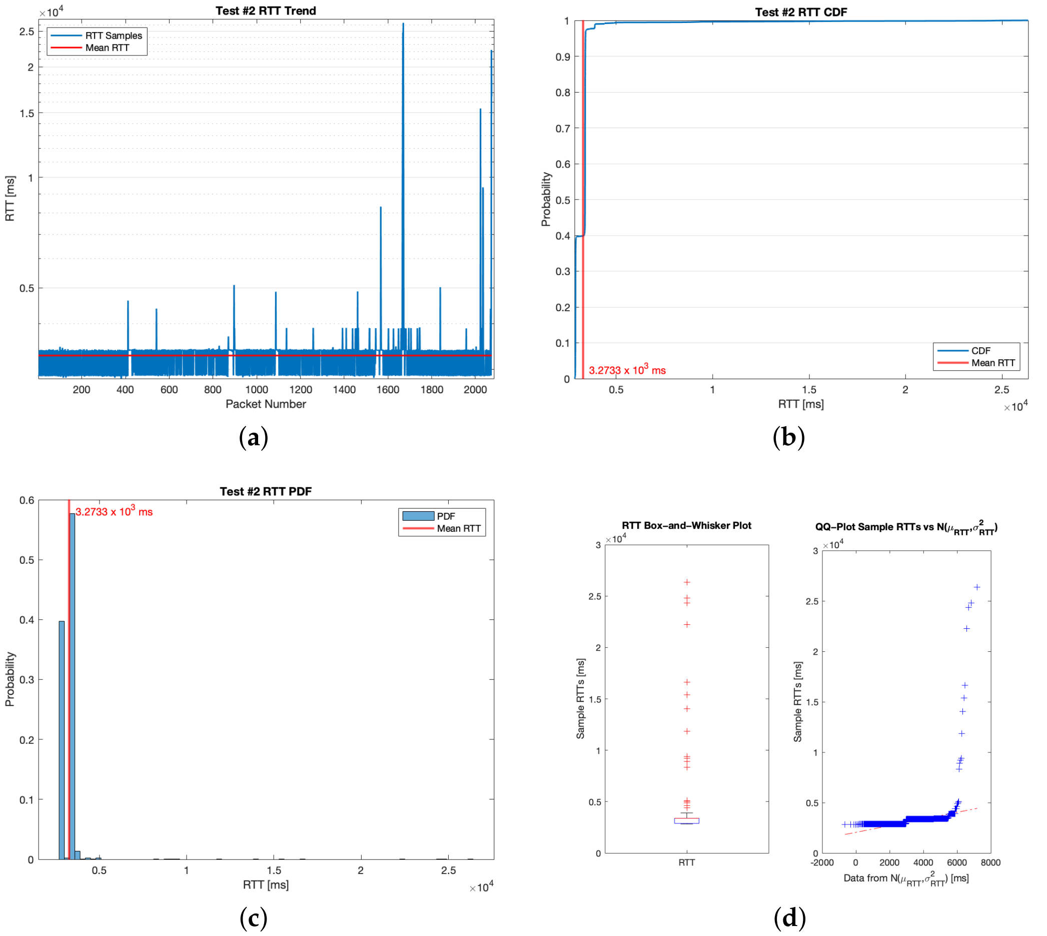


Figure 7. Test #1 results.

The Test #2 results are outlined in Figure 8. Throughout the test, the master node sent 2216 NB-IoT packets, and it received 2074 responses from the slave within the timeout (i.e., the peer-to-peer subnetwork was effective 93.59% of the times). The mean RTT was $\mu_{RTT} = 3.2733 \times 10^3$ ms, while the RTT standard deviation was $\sigma_{RTT} = 1.1224 \times 10^3$ ms. From RTT Cumulative Distribution Function (CDF), it can be noticed that RTT is above μ_{RTT}, with a probability of 0.6. Though this could be undesirable, the CDF also shows that RTT is less than 3.4338×10^3 ms, with a probability of 0.9725, or that it is less than 5.0258×10^3 ms, with probability of 0.9937. Therefore, the majority of RTTs are close to μ_{RTT}, thus underlying the good repeatability of such a metric. This is also stressed by the RTT Probability Density Function (PDF), which is highly concentrated near μ_{RTT} apart from a few outliers, thus being sensibly leptokurtic. Such outliers are also noticeable within the box-and-whisker plot. Finally, the QQ plot confirms the fact that, besides the outliers, the experimental data adequately follow the distribution $N(\mu_{RTT}, \sigma^2_{RTT})$. Of course, the experimental data can never be negative since RTTs are involved; therefore, a perfect overlapping with the aforementioned distribution cannot be obtained. Apart from a few

RTT samples that were notably longer than the mean, such a test showed the feasibility and the effectiveness of the peer-to-peer subnetwork, especially because of the experienced RTT values, which can be considered adequate for IoT contexts related to, for instance, monitoring issues within widespread and severe environments.

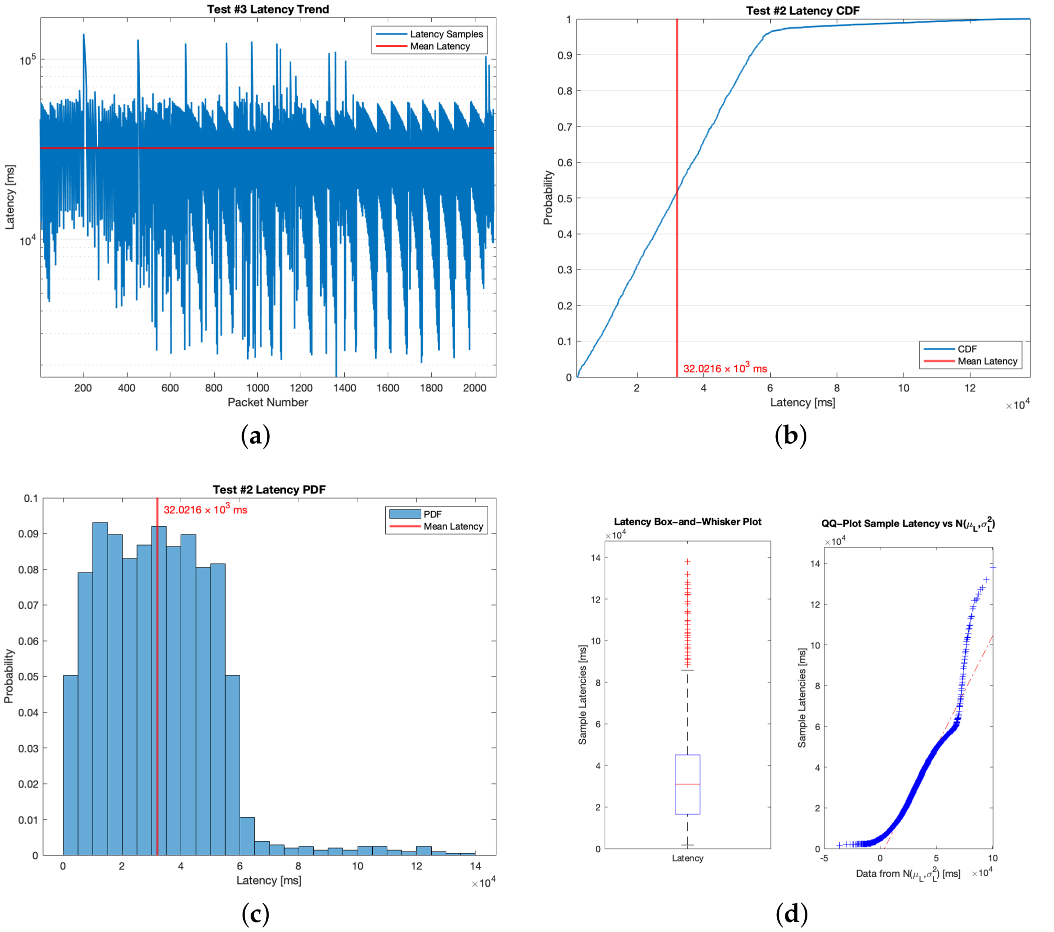


(**a**) (**b**)

(**c**) (**d**)

Figure 8. Test #2 results on RTT: (**a**) temporal trend; (**b**) CDF; (**c**) PDF; (**d**) box-and-whisker plot along with QQ plot.

The Test #3 results are highlighted in Figure 9. At first glance, a massive variability with respect to the results of Test #2 can be noticed. However, this is reasonable since this test entailed the sequential usage of both the enabling technologies (i.e., LoRaWAN and NB-IoT) and of the three network layers. During these trials, the LoRaWAN Node sent 2117 packets and the NB-IoT Nodes received 2086 packets (i.e., a successful complete communication paradigm was experienced in 98.54% of the times). Although this test provided better results with respect to Test #2 from the point of view of packet loss, it has to be remarked that, in Test #3, no timeouts occurred. That is also the reason why mean latency and latency standard deviation values (i.e., in turn $\mu_L = 32.0216 \times 10^3$ ms and $\sigma_L = 19.4938 \times 10^3$ ms) were particularly bigger than μ_{RTT} and σ_{RTT} of Test #2. However, this should not be considered as a hindrance because such latency values can be commonly found whenever LoRaWAN protocol is employed for monitoring purposes due to the regional regulation concerning ISM bands temporal occupancy. On the other hand, the paradigm in which a sensor is LoRaWAN enabled and an actuator is NB-IoT enabled was proven to be a reliable and effective solution owing to the fact that NB-IoT is not devised to be capable of receiving downlinks within predefined temporal slots (as opposed to LoRaWAN). A finer analysis can be accomplished by considering the latency CDF. It can be noticed that latency is above μ_L, with a probability of 0.4789. Even though it could obtain a better result with respect to Test #2, the CDF hints at the fact that the data are more spread out than RTTs. Indeed, the latency is longer than 42.1931 × 10^3 ms, 54.1691 × 10^3 ms and 79.9798 × 10^3 ms with probabilities of 0.3015, 0.1016 and 0.0187. Accordingly, the spread of latency is remarked within the relative PDF, which shows a considerable platykurtosis apart from the outliers, which are also visible within the box-and-whisker plot. Lastly, the QQ plot confirms that, besides such outliers, the experimental data decently follow the distribution $N(\mu_L, \sigma_L^2)$. Similar to what was said for the discussion of Test #2, the experimental data can never be negative since latency is considered; thus, a perfect overlapping with the aforementioned distribution cannot be met.

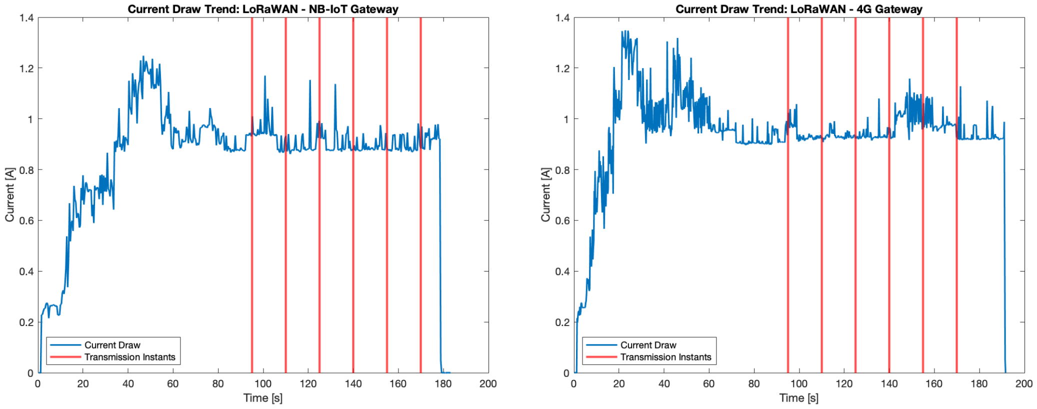


(**a**) (**b**) (**c**) (**d**)

Figure 9. Test #3 results on latency: (**a**) temporal trend; (**b**) CDF; (**c**) PDF; (**d**) box-and-whisker plot along with QQ plot.

Figure 10 displays the results of the Gateways power consumption test. At first glance, two main findings can be noticed: on the one hand, both current draws exhibit the same trend; on the other hand, the LoRaWAN-NB-IoT Gateway turned out to need less power than the standard LoRaWAN-4G. However, this result is far from unexpected. Indeed, NB-IoT facility was devised to be more efficient from the point of view of energy requirements than standard cellular technologies such as 4G. At the same time, it has to be said that the difference in terms of current draw is scant because the LoRaWAN-NB-IoT Gateway of this paper is only a prototype. Conversely, the exploited 4G dongle is a commercial product, and therefore, it underwent an optimisation process resulting also in power optimisation. The initialisation phase is the energy-hungrier one, requiring up to 1.25 A and 1.35 A, respectively, for NB-IoT and 4G. In addition, such procedures last 92 s and 73 s in turn for NB-IoT and 4G, hence noting the prototypical stage of the LoRaWAN-NB-IoT Gateway of this paper. After these time periods, the Gateways indefinitely listened for incoming

LoRaWAN packets averagely, drawing 877 mA and 900 mA individually for NB-IoT and 4G. During these listening periods, some peaks can be noticed, but they cannot be ascribed to reception of the LoRaWAN packets since they are not synchronised with the transmission instants (i.e., 95 s, 110 s, 125 s, 140 s, 155 s and 170 s). If it would not be so, then the current draws should be periodic from the first transmission time instant (i.e., 95 s) on. This hints at the fact that data reception and forwarding are accomplished by averagely requiring no additional energy. Notwithstanding this, it is reasonable to claim that generally opting for an NB-IoT Internet connection, rather than the standard 4G one, is preferable due to the reduced running costs: they are directly caused by the subscribed data plan, and NB-IoT telco providers are striving for issuing affordable data plans, thus encouraging users to choose such a solution.



(**a**) (**b**)

Figure 10. Gateways current consumption test results: (**a**) LoRaWAN-NB-IoT Gateway; (**b**) LoRaWAN-4G Gateway.

6. Conclusions

The aim of this paper was to demonstrate the feasibility of a fully interoperable LoRaWAN-NB-IoT network, allowing for transparent interconnection among edge nodes regardless of the specific communication channel. A network infrastructure integrating LoRaWAN End Devices, NB-IoT Nodes and NB-IoT-powered LoRaWAN Gateways was set up and validated. In particular, three different scenarios were tested, according to the different channel configurations. These included a scenario where NB-IoT was employed for packet forwarding from LoRaWAN Gateways to the Servers, while the other two scenarios were designed to test peer-to-peer connection among nodes or subnetworks. In the first case, a direct NB-IoT connection among nodes was tested, while the last scenario focused on a hybrid bidirectional channel encompassing LoRaWAN and NB-IoT nodes. Moreover, the power consumption of the LoRaWAN-NB-IoT Gateway, in terms of current draw, was compared with the one of a LoRaWAN-4G Gateway. Such a test showed that little difference between the two solution can be noticed. However, this does not directly mean that the multi-protocol Gateway of this paper fails from the point of view of a low power feature. Indeed, it is still a prototype, contrary to the LoRaWAN-4G one, thus hinting at the fact that there is still room for improvement and optimisation from the point of view of power consumption. Such a claim is reasonable due to the power-saving policies that an NB-IoT facility implements with respect to standard cellular technologies such as 4G. Therefore, it is rational to assert that an NB-IoT Internet connection can be culled in favor of 4G since it entails smaller running costs compared with other cellular technologies.

In all the aforementioned cases, the network demonstrated its operation, depending on the actual performances of the two technologies. Indeed, packet loss and latency were chosen as metrics for the evaluation of the system performances. Nonetheless, based the obvious dependence of performances on NB-IoT coverage and on quality of the equipment (e.g., characteristics of the gateway components, hardware and software bugs, etc.), it is reasonable to deem that such results are useful to provide readers with a flavour of network capability and reliability. The positively achieved outputs throughout the tests suggest the feasibility of large-scale network deployments of this kind of infrastructure. These may be applied in a huge number of application scenarios where edge devices feature different requirements. Similarly, such a combination of technologies may lead to the definition of novel network topologies as well as of new protocols for the implementation of energy-management strategies.

Author Contributions: G.P. and A.P. conceived and designed the overall architecture; G.P. developed the network components; G.P. sorted out the tests; G.P. carried out data analysis; G.P. and A.P. wrote the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available from the corresponding author upon request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ratasuk, R.; Vejlgaard, B.; Mangalvedhe, N.; Ghosh, A. NB-IoT system for M2M communication. In Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, Doha, Qatar, 3–6 April 2016; pp. 1–5.
2. Feltrin, L.; Tsoukaneri, G.; Condoluci, M.; Buratti, C.; Mahmoodi, T.; Dohler, M.; Verdone, R. Narrowband IoT: A survey on downlink and uplink perspectives. *IEEE Wirel. Commun.* **2019**, *26*, 78–86. [CrossRef]
3. Li, Y.; Cheng, X.; Cao, Y.; Wang, D.; Yang, L. Smart choice for the smart grid: Narrowband Internet of Things (NB-IoT). *IEEE Internet Things J.* **2017**, *5*, 1505–1515. [CrossRef]
4. Malik, H.; Alam, M.M.; Le Moullec, Y.; Kuusik, A. NarrowBand-IoT performance analysis for healthcare applications. *Procedia Comput. Sci.* **2018**, *130*, 1077–1083. [CrossRef]
5. Parrino, S.; Peruzzi, G.; Pozzebon, A. LoPATraN: Low Power Asset Tracking by Means of Narrow Band IoT (NB-IoT) Technology. *Sensors* **2021**, *11*, 3772. [CrossRef] [PubMed]
6. San Cheong, P.; Bergs, J.; Hawinkel, C.; Famaey, J. Comparison of LoRaWAN classes and their power consumption. In Proceedings of the 2017 IEEE symposium on communications and vehicular technology (SCVT), Leuven, Belgium, 14 November 2017; pp. 1–6.
7. Adelantado, F.; Vilajosana, X.; Tuset-Peiro, P.; Martinez, B.; Melia-Segui, J.; Watteyne, T. Understanding the limits of LoRaWAN. *IEEE Commun. Mag.* **2017**, *55*, 34–40. [CrossRef]
8. Lombardo, A.; Parrino, S.; Peruzzi, G.; Pozzebon, A. LoRaWAN vs NB-IoT: Transmission Performance Analysis within Critical Environments. *IEEE Internet Things J.* **2022**, *9*, 1068–1081. [CrossRef]
9. Luvisotto, M.; Tramarin, F.; Vangelista, L.; Vitturi, S. On the use of LoRaWAN for indoor industrial IoT applications. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 3982646. [CrossRef]
10. Davcev, D.; Mitreski, K.; Trajkovic, S.; Nikolovski, V.; Koteli, N. IoT agriculture system based on LoRaWAN. In Proceedings of the 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), Imperia, Italy, 13–15 June 2018; pp. 1–4.
11. Parri, L.; Parrino, S.; Peruzzi, G.; Pozzebon, A. Offshore LoRaWAN Networking: Transmission Performances Analysis Under Different Environmental Conditions. *IEEE Trans. Inst. Meas.* **2020**, *70*, 1–10. [CrossRef]
12. Zatout, Y.; Campo, E.; Llibre, J.F. Toward hybrid WSN architectures for monitoring people at home. In Proceedings of the International Conference on Management of Emergent Digital EcoSystems, Lyon, France, 27–30 October 2009; pp. 308–314.
13. Guo, F.; Yu, F.R.; Zhang, H.; Li, X.; Ji, H.; Leung, V.C. Enabling massive IoT toward 6G: A comprehensive survey. *IEEE Internet Things J.* **2021**, *8*, 11891–11915. [CrossRef]
14. Chen, M.; Miao, Y.; Jian, X.; Wang, X.; Humar, I. Cognitive-LPWAN: Towards intelligent wireless services in hybrid low power wide area networks. *IEEE Trans. Green Commun. Netw.* **2018**, *3*, 409–417. [CrossRef]
15. Ayele, E.D.; Das, K.; Meratnia, N.; Havinga, P.J. Leveraging BLE and LoRa in IoT network for wildlife monitoring system (WMS). In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 342–348.
16. Ferreira, C.M.S.; Oliveira, R.A.R.; Silva, J.S. Low-energy smart cities network with LoRa and bluetooth. In Proceedings of the 2019 7th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Newark, CA, USA, 4–9 April 2019; pp. 24–29.
17. Li, Z.; Chen, Y. BLE2LoRa: Cross-technology communication from bluetooth to LoRa via chirp emulation. In Proceedings of the 2020 17th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Como, Italy, 22–25 June 2020; pp. 1–9.

18. Basu, S.S.; Haxhibeqiri, J.; Baert, M.; Moons, B.; Karaagac, A.; Crombez, P.; Camerlynck, P.; Hoebeke, J. An end-to-end LwM2M-based communication architecture for multimodal NB-IoT/BLE devices. *Sensors* **2020**, *20*, 2239. [CrossRef] [PubMed]
19. Basu, S.S.; Haxhibeqiri, J.; Baert, M.; Moons, B.; Hoebeke, J. An Energy-Efficient Multi-Modal IoT System Leveraging NB-IoT and BLE. In Proceedings of the 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS), Bali, Indonesia, 27–28 January 2021; pp. 30–36.
20. Djidi, N.E.H.; Courtay, A.; Gautier, M.; Berder, O.; Magno, M. Opportunistic Cluster Heads for Heterogeneous Networks Combining LoRa and Wake-up Radio. In Proceedings of the 2020 International Conference on Embedded Wireless Systems and Network (EWSN), Lyon, France, 17–19 February 2020; pp. 200–205.
21. Lysogor, I.; Voskov, L.; Rolich, A.; Efremov, S. Study of data transfer in a heterogeneous LoRa-satellite network for the internet of remote things. *Sensors* **2019**, *19*, 3384. [CrossRef] [PubMed]
22. Yasmin, R.; Petajajarvi, J.; Mikhaylov, K.; Pouttu, A. On the integration of LoRaWAN with the 5G test network. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–6.
23. Chandrashekar, S.; Maeder, A.; Sartori, C.; Hohne, T.; Vejlgaard, B.; Chandramouli, D. 5G multi-RAT multi-connectivity architecture. In Proceedings of the 2016 IEEE International Conference on Communications Workshops (ICC), Kuala Lumpur, Malaysia, 23–27 May 2016; pp. 180–186.
24. Sanchez-Iborra, R.; Santa, J.; Gallego-Madrid, J.; Covaci, S.; Skarmeta, A. Empowering the internet of vehicles with Multi-RAT 5G network slicing. *Sensors* **2019**, *19*, 3107. [CrossRef] [PubMed]
25. Leenders, G.; Callebaut, G.; Ottoy, G.; Van der Perre, L.; De Strycker, L. Multi-RAT for IoT: The Potential in Combining LoRaWAN and NB-IoT. *arXiv* **2021**, arXiv:2104.10536.
26. Mikhaylov, K.; Stusek, M.; Masek, P.; Petrov, V.; Petajajarvi, J.; Andreev, S.; Pokorny, J.; Hosek, J.; Pouttu, A.; Koucheryavy, Y. Multi-rat lpwan in smart cities: Trial of lorawan and nb-iot integration. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
27. Boonchieng, E.; Saokaew, A.; Chieochan, O. The Prototype of the Integration between Low Cost Single Private LoRa Gateway and Public AIS NB-IOT. *J. Internet Technol.* **2019**, *20*, 1313–1322.
28. MQTT Protocol. Available online: http://mqtt.org (accessed on 13 December 2021).
29. Parri, L.; Parrino, S.; Peruzzi, G.; Pozzebon, A. A LoRaWAN network infrastructure for the remote monitoring of offshore sea farms. In Proceedings of the 2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Dubrovnik, Croatia, 25–28 May 2020; pp. 1–6.