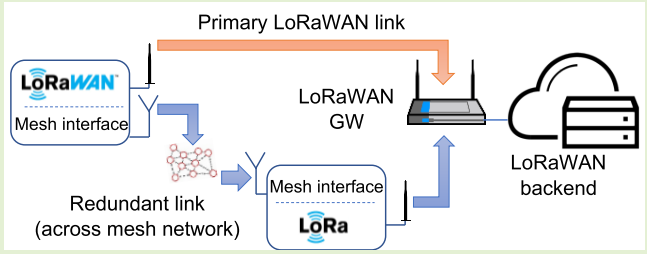
Evaluating the Joint Use of LoRaWAN and Bluetooth Mesh to Improve Survivability for Critical Sensor Applications

Emiliano Sisinni, *Member, IEEE*, Alessandro Depari, *Member, IEEE*, Alessandra Flammini, *Fellow, IEEE*, Stefano Rinaldi, *Senior Member, IEEE*, and Paolo Ferrari, *Member, IEEE*

***Abstract*—Wide area, wireless, Internet of Things (IoT)-based, distributed sensor systems can be employed in mixed criticality solutions for measurement/detection/signaling of emergencies, dangers, accidents, and disasters. All these scenarios require reliability, security, and safety. This work introduces and characterizes a new proposal to enhance existing LoRaWAN applications by adding a transparent redundant channel just for critical traffic. Network survivability and delivery success of critical messages, even with low LoRaWAN signal quality (as in indoors), is increased. The proposal preserves the LoRaWAN backend structure (including end-to-end (E2E) security) using short-range radios to implement an underlying redundant mesh channel for transparently transporting LoRaWAN traffic of critical applications. Hybrid scenarios with legacy standard nodes coexisting are also permitted. The proof-of-concept combines LoRaWAN and, without losing generality, a redundant channel with Bluetooth mesh (BM). This work includes: metrics definition, evaluation of complex scenario by means of simulations, and real experiments demonstrating feasibility and integration with LoRaWAN-compliant backend using commercial hardware/firmware/software. In particular, results confirm that packet loss in the order of 1% on the BM side can be obtained and therefore the critical traffic delivery success is improved by almost two orders of magnitude.**



***Index Terms*—Distributed sensor system, low power area network (LPWAN), mesh network, mixed criticality, multi-interface, protocol encapsulation.**

I. Introduction

ACCORDING to the Internet of Things (IoT) paradigm, smart devices (i.e., the "things") enabled by some computational capabilities can communicate their own data toward the cloud relying on the Internet. Similarly, end users can access the cloud to retrieve information of interest to take decisions, possibly after further processing. Therefore, very diverse sources of information can coexist in the same application, each one having different characteristics and requirements [1], [2].

Some application-centric communication features, including the delivery constraints, such as the update periodicity, the latency, the sustainable throughput, etc., are well-known and well-studied [3], [4], being inherited from traditional distributed sensor systems, industrial control, and smart sensing solutions.

However, unlike legacy approaches, that typically had only one criticality level, IoT-based systems can be mixed-critical [5]. Criticality must be intended as the criticality of the data for the correct operation of the critical parts of the system in terms of reliability, security, and safety. For example, critical measurement applications that can exploit the IoT paradigm include the industrial supervision systems, emergency response systems, the detection and signaling of possible dangers and accidents, the disaster management, and many other scenarios. Consequently, the application criticality dictates the selection of the appropriate quality of service (QoS) mechanisms of the networking infrastructure, which can result in a heterogeneous architecture consisting of nodes (and devices) leveraging on different technologies [6]. This is espe-

Manuscript received 23 April 2024; accepted 15 May 2024. Date of publication 30 May 2024; date of current version 16 July 2024. This study was carried out within the MOST - Sustainable Mobility National Research Center and received funding from the European Union Next-GenerationEU (PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) - MISSIONE 4 COMPONENTE 2, INVESTIMENTO 1.4 - D.D. 1033 17/06/2022, CN00000023), Spoke 5 "Light Vehicle and Active Mobility". This manuscript reflects only the authors' views and opinions, neither the European Union nor the European Commission can be considered responsible for them. The associate editor coordinating the review of this article and approving it for publication was Prof. Lan Lan. *(Corresponding author: Emiliano Sisinni.)*

The authors are with the Department of Information Engineering, University of Brescia, 25123 Brescia, Italy (e-mail: emiliano.sisinni@unibs.it; alessandro.depari@unibs.it; alessandra.flammini@unibs.it; stefano.rinaldi@unibs.it; paolo.ferrari@unibs.it).

Digital Object Identifier 10.1109/JSEN.2024.3403308

cially true when wireless connectivity has to be implemented (e.g., for ensuring flexibility and scalability). As a matter of fact, comprehensive investigation of actual traffic characteristics is mandatory to properly select the network infrastructure.

In this work, LoRaWAN, based on single-hop LoRa sub-GHz radios and star-of-stars topology, is considered because of the open nature of the backend, which defines several logical entities that can be deployed both on the cloud and on-premises and can be managed privately or by a provider [7]. Messages are enciphered at the application level, but integrity is checked at the network level. Interesting to notice, recently device-to-device (D2D) capability has been purposely added to address network survivability for control and alarm detection and response applications [8]. However, security is poor due to the exploitation of multicasting, in which there is no join procedure at all (session keys are preconfigured [9]).

Mesh networks have multiple paths that improve the connectivity of end nodes, so they are suitable for managing mixed criticality applications. A higher delivery success for critical messages is obtained, minimizing retransmissions. Indeed, proposals for changing LoRaWAN into a mesh network have been described in literature [10], potentially jeopardizing compatibility with the standard.

Our proposal, on the other hand, enhances LoRaWAN adding a redundant and transparent communication channel for critical traffic, while noncritical traffic relies on standard LoRaWAN communication channel. Starting from advantages of multi-hop [10], we consider a whole mesh network of short-range radios as the redundant link (with space and channel diversity). The proposed methodology is innovative and offers many advantages. The backend structure is preserved, and private deployments are permitted. In particular, the applications are not aware of the underlying redundant channel and the LoRaWAN infrastructure is not modified, thus hybrid scenarios with legacy standard nodes coexisting with enhanced dual interface devices are permitted. Differently from the aforementioned D2D, regular LoRaWAN provisioning is preserved.

The article is aimed to the proposal characterization, and the main contributions are listed in the following.

1) The suggestion of a new, additional transport mechanism of LoRaWAN traffic over a mesh of short-range devices for critical applications, without jeopardizing security
2) The introduction of a reference implementation based, without losing generality, on Bluetooth low energy (BLE) and Bluetooth mesh (BM) as an example of short-range solution capable of mesh topology.
3) The definition of metrics for evaluating the obtainable performance.
4) The execution of simulations for evaluating the performance of the proposed method in a complex scenario.
5) The execution of tests in a real-world deployment based on proof-of-concept prototypes, for demonstrating the feasibility using commercially available hardware.

Simulations allow to verify the performance in a worst case scenario where the BM network is heavily loaded and the LoRaWAN devices possibly exceed traffic limits imposed by duty-cycle restrictions. As regards the real-world tests, commercial firmware/software without any modifications is used. Therefore, no LoRaWAN rule is violated and integration with LoRaWAN compliant backend solutions is actually permitted.

The proposed approach is not limited to BM, since other wireless protocols may be adequate as well. Also, the choice of a wireless mesh technology is not mandatory, but useful for easing the placements of multi-interface devices providing the redundant path.

The article is organized as follows: in the next section, an overview of wireless technologies for IoT is provided. In Sections III and IV, the proposed approach is detailed, including security. In Section V, the simulation testbed and results are discussed, while Section VI details experimental testbeds and results. Finally, conclusions are drawn.

II. WAN for the Wireless IoT

The IoT protocol stack resembles an hourglass, with the Internet protocol acting as a collector for a plethora of protocols of the lower and upper layers [11]. Especially for lower layers, there is no one-size-fits-all solution, and medium access strategies and radios must be carefully chosen [12].

For these reasons, multi-interface approach to wireless sensor networks for critical measurement situations has been investigated since long time. The main research focus was on optimization of QoS [13]. Following the evolution of wireless network technology, the multi-interface nodes started including IEEE802.11 (WiFi), IEEE802.15.1 (Bluetooth), IEEE802.15.4, on the one hand, and mobile (4G/NB-IoT) communications on the other. The former group includes short-range technologies, possibly supporting multi-hop and mesh topologies to extend the coverage, operating in unlicensed bands. On the contrary, mobile communications implement wide area networks based on a sort of star-of-stars topology, where many wireless base stations are wired connected with the backend; they operate in licensed bands and require a third-party provider. More recently, the use of last 5G technologies promises to further extend the capabilities of critical wireless sensor networks on large areas, thanks to the virtualization of network functions. Interesting to note, with the introduction of the 5G ultra reliable and low latency communications (URLLC), the idea of duplicated packets across different data planes is introduced [14].

A. Advent of LPWAN

However, the most interesting innovations come from the introduction of low power area networks (LPWANs) operating in unlicensed bands, which combine low-power and long-range with a backend infrastructure that could be (also) private, mimicking the star-of-stars topology of mobile, but exploiting cheap gateways (GWs) at the edge. Without bindings to third party infrastructure (i.e., without subscriptions), the application of LPWAN technologies like LoRaWAN is ramping. These LPWANs trade off the sensitivity (i.e., the coverage) with the throughput, addressing the needs of applications tolerating sporadic communications, especially in the uplink direction (i.e., from the field to the backend) [15]. Many previous research works have confirmed their suitability in very different smart environments (industry, farming and agriculture, etc.) including (low speed) mobility [16], [17]. Thus,

outdoor, and indoor coverage is often required, resulting in an increased number of GWs and/or degradation of the time performance [18], since boosting the communication robustness requires to lower the data rate. However, (adaptively) lowering the data rate results in longer frame airtimes, which affect consumption and increase the collision probability. Operating in sub-GHz unlicensed bands contributes to the wide area coverage, but also limits the number of available channels, which in turn obliges to reduce the number of messages in the downlink direction to favor the opposite one.

B. Technologies for Mixed Criticality Applications

As stated in the introduction, distributed measurement, IoT-like mixed-criticality applications pose different requirements to the communication infrastructure in terms of QoS. In particular, the heterogeneous data delivery model, enabling both low- and high-criticality tasks management, may require trading off low latency with low data rate [19]. Additionally, there is need for:

1) low-power consumption;
2) secure data transfers;
3) mobility and possible topology changes, including localization (for navigation and for proximity as well);
4) scalable operations, minimizing reconfiguration efforts.

Unfortunately, there is no "one-size-fits-all" solution that may encompass all of them.

LoRaWAN emerged as a de facto standard for IoT-like applications (including industrial ones [20], [21]), thanks to the possibility to operate in unlicensed bands and the openness of the specification, drafted by the LoRa Alliance.

Bluetooth technology has been jointly considered with LoRaWAN in this work to address the previously listed requirements. Indeed, Bluetooth is a widely accepted solution for local (wireless) connectivity and it recently gained support for mesh topology, to ensure flexible operations on larger areas [22].

III. Proposed Approach

The typical IoT communication infrastructure, used to exchange the information flows (sensing data for the upstream, control data for the downstream) with the computing and storage devices in the cloud, includes access and core networks. When wireless communications are considered: the radio access network (RAN) consists of end nodes, relays and access points and/or GWs toward the cloud; and the core network represents the backbone interconnecting the (logical) entities in the backend managing and controlling the infrastructure [23]. LoRaWAN specifications natively define the RAN and provide a description of the functionalities implemented in the backend, despite the implementation details depend on the actually deployed solution. It is well-known that LoRa, as any digital communication technology, suffers from an abrupt increase of the packet error rate if the signal quality at the receiver drops below a threshold, as reported in literature [24], [25], [26]. As a consequence, especially for mixed-criticality scenarios, ensuring good connectivity and a reasonable QoS may require the deployment of a large number of GWs, which is expensive and not always possible.

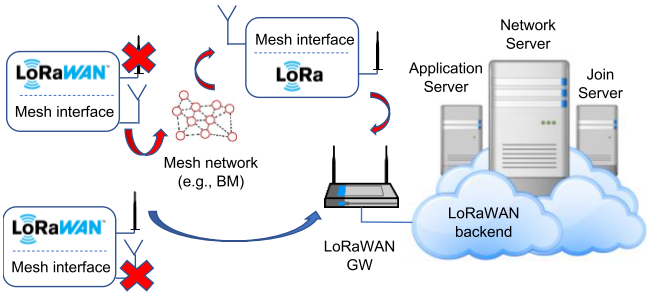


Fig. 1. Architecture of the proposed LoRaWAN redundant communication via mesh overlay network.

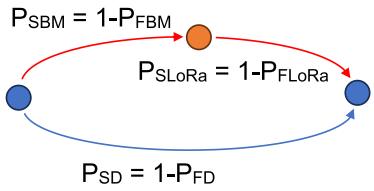


Fig. 2. Simplified success/failure probability model describing the proposed redundant path for critical traffic.

The new proposal of this article is to add a redundant communication interface implementing an overlay LoRaWAN Class A network over a mesh network (e.g., like BM). The overview of the proposed architecture is depicted in Fig. 1, where the backend Network, Application, and Join servers, {NS, AS, and JS}, are also shown (additional details in Appendix). If connectivity on the LoRaWAN interface becomes unsatisfactory for the critical data flow (e.g., moving from outdoor to indoor), the mesh connectivity enables a parallel redundant communication path, able to reach the GW by means of dual interface device hosting a LoRa radio. It should be stressed that some form of overlay of LoRaWAN communications was suggested, but only for adding GW-to-GW connectivity [27], thus it does not match requirements of this work.

The proposed architecture can be described by the simplified model depicted in Fig. 2, useful for evaluating the success/failure probability along the uplink direction when direct LoRaWAN link suffers from non-optimal coverage. Note that a similar model can be devised for downlink messages (if exist). The two models are independent, since LoRa radio uplink and downlink are orthogonal due to the I/Q baseband phase inversion, which permits to nodes to only listen at GWs and vice versa.

The failure probability P_{F} of a single critical uplink data transaction is described by (1), where $P_{\mathrm{SD}}/P_{\mathrm{FD}}$ is the probability for the GW to succeed/fail the reception of an uplink message using the regular direct LoRaWAN path, and $P_{\mathrm{SR}}/P_{\mathrm{FR}}$ is the probability for the GW to succeed/fail the reception of an uplink message along the redundant path

$$P_{\mathrm{F}} = (1 - P_{\mathrm{SD}})(1 - P_{\mathrm{SR}}) = P_{\mathrm{FD}} \cdot P_{\mathrm{FR}} \leq P_{\mathrm{FD}}. \qquad (1)$$

The P_{F} expression can be further elaborated observing that $P_{\mathrm{FR}} = (1 - P_{\mathrm{SBM}} P_{\mathrm{SLoRa}}) \approx (1 - P_{\mathrm{SBM}})$, where $P_{\mathrm{SBM}}/P_{\mathrm{FBM}}$ is the success/failure probability along the BM network and $P_{\mathrm{SLoRa}}/P_{\mathrm{FLoRa}}$ is the success/failure probability for the dual

interface device hosting the LoRa radio. In absence of interferences, it can be assumed that $P_{\mathrm{SLoRa}} \approx 1$ or $P_{\mathrm{FLoRa}} \approx 0$, so that (1) can be rewritten as (2)

$$P_{\mathrm{F}} = P_{\mathrm{FD}} \cdot (1 - P_{\mathrm{SBM}}) = P_{\mathrm{FD}} \cdot P_{\mathrm{FBM}}. \tag{2}$$

Therefore, providing good connectivity of the redundant BM network (i.e., properly tuning P_{SBM} which, for instance, depends on the advertize time ad better detailed in Section IV), it is possible to ensure the P_{F} desired by the considered critical application. As regards the dual interface devices, the only requirement is the mesh support for multicast/group addressing, in order to easily identify the subset of those devices capable to retransmit LoRaWAN messages. On the other hand, not all the mesh devices must have dual interface. Last, power consumption of dual interface devices may be not so relevant in the mixed criticality scenario since the goal is to improve the robustness of sporadic critical data.

Among the possible wireless mesh technology, this work will use BM for the feasibility demonstration. Since its advent, Bluetooth has been suggested as a suitable candidate for implementing high performance wireless sensor networks, including wireless fieldbus [28], [29], thanks to the good throughput and latency. Laying above BLE, BM offers extended range, as nodes can relay messages to reach are far away devices; moreover, multiple paths across the mesh allow for self-healing capabilities. Integration of both technologies is possible, e.g., by means of heterogeneous, purposely designed hybrid GWs, as suggested in [30]. Additionally, nowadays integrated solutions supporting both kind of radios are also available. These are the reasons why BM has been considered as the reference mesh solution in this article.

IV. Enhancing LoRaWAN Using BM

In this section, the peculiarities of the encapsulation of LoRaWAN messages into BM traffic, preserving end-to-end (E2E) security in a transparent way.

A. Transporting LoRaWAN Traffic Over BM

The proposed approach starts considering that LoRaWAN is L1 (physical) layer protocol agnostic, meaning that information of upper protocol layers is completely decoupled from the radio actually transferring it, thus avoiding protocol conversion at intermediate nodes (as in [31]). Focusing on the uplink direction, it implies the frame generated by the LoRaWAN stack of a dual interface node (DIN) can be tunneled across the mesh network to be retransmitted by the LoRa radio of another DIN (named DINR and belonging to the same multicast group). Deduplication is natively carried out by the NS, which considers only the first arrived message. As previously stated, intermediate BM relay nodes do not necessarily need to be equipped with a LoRa radio, since the LoRaWAN frame is the application payload of the BM message, as shown in Fig. 3.

We focus on Class A behavior, so that it is not needed to explicitly map the LoRaWAN device address on the BM address, since each information exchange is an "uninterruptable" sequence of uplink and (optional) downlink frames initiated by the end-node. The subset of DINs able to

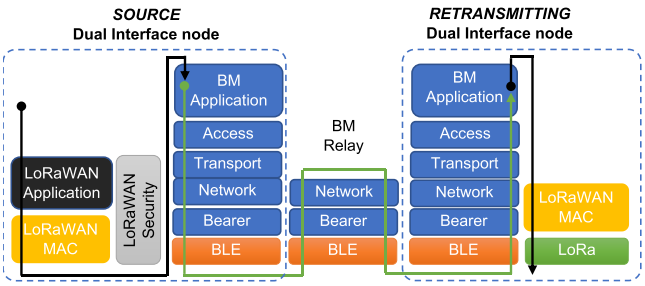


Fig. 3. Basic stack and data flow showing transportation of a LoRaWAN uplink message over a BM network (opposite direction for downlink).

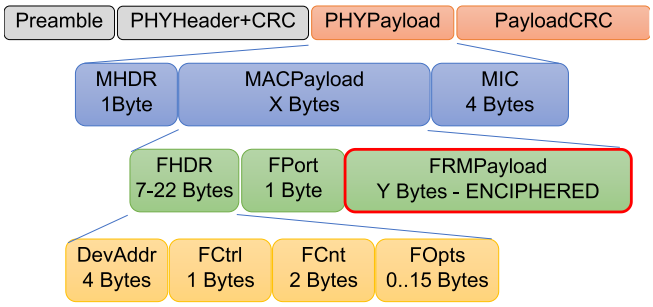


Fig. 4. LoRaWAN message fields; only gray fields depend on the LoRa radio.

retransmit the received LoRaWAN frames (transported by the underlying BM network) are identified by a common BM multicast address. In this way, multiple copies of the same LoRaWAN message can arrive at the NS, which natively performs deduplication according to the arrival order. As regards the downlink messages, each dual interface device opens the required receive windows (according to the LoRaWAN Data Link layer-L2 configuration). In this way, any dual interface devices that transmitted an uplink frame will eventually get the downlink (and will propagate back to the intended destination, i.e., to the uplink source).

LoRaWAN general format is depicted in Fig. 4; since the LoRaWAN L1 payload is typically longer than BM maximum Transport protocol data unit (PDU), fragmentation is exploited (thus affecting the overall delay). The payload and the cyclic redundancy check (CRC), are given by the initiator of the exchange; in order to be correctly processed, the message integrity code (MIC) must be computed and the so-called FRMPayload must be enciphered using session keys obtained during the join procedure. Vice versa, MIC of downlink messages must be validated, and the payload must be deciphered.

In order to become a member of a LoRaWAN or BM network, provisioning is required. The identity and the initial security keys are furnished by a provisioner. In the proposed approach the LoRaWAN provisioning occurs as usual; then, once provisioned, the dual interface LoRaWAN node becomes an out-of-band provisioner for the co-resident BM counterpart. For the sake of clarity, details about security of both LoRaWAN and BM are reported in the following.

B. LoRaWAN and BM Security Aspects

LoRaWAN security and integrity is seamlessly maintained in the proposed approach. LoRaWAN application and network

data traverse the BM stack unchanged, with their own security in place. Mechanisms for ensuring confidentiality, integrity, and availability (CIA) are natively provided by LoRaWAN and BM; in this work, they are used without modification.

LoRaWAN exploits AES-CMAC for integrity protection and AES-CTR for encryption. Two session keys exist: *NwkSKey* is used by the NS for integrity checking (and enciphering the so-called MAC commands), while *AppSKey* is used by the end node and the AS for E2E encryption. Provisioning can occur by means of activation by personalization (ABP) or using the over-the-air activation (OTAA). The ABP procedure is of limited interest, since it requires the session keys to be preconfigured in the end node; in the OTAA, session keys are obtained from the backend servers leveraging on preconfigured root keys, used only in the initial affiliation. An end node trying to join first sends a *join_request* message; after positive validation, the NS replies with a *join_accept*. The latter contains information encrypted with the root keys by means of which the actual session keys are derived.

As regards BM, provisioning usually starts with an *invitation* over the BLE link from the provisioner, followed by the exchange of keys and authentication. In our case, the node identity is already confirmed and simplified authentication procedure is carried out. Subsequently, provisioning data are forwarded to the unprovisioned node; provisioning data are exchanged securely, since they are enciphered using AES-CCM by means of a shared *SessionKey*, and a session nonce. Indeed, to become a BM node, the device requires a network key (known as the *NetKey*), a device key (known as *DevKey*), a security parameter index (known as the *Initialization Vector IV*), and a unicast address. Resuming, the *NetKey* permits to access the specific network of interest and it is used to encrypt and authenticate the payload of lower BM stack layers. The unique *DevKey* is used to secure direct communication with a specific BM device, e.g., during the configuration. The application key (known as *AppKey*and bound to a specific *NetKey*) provides confidentiality to data exchanged by nodes belonging to the same application; in other words, it is used to encrypt and authenticate upper layers payload.

Practically, each LoRaWAN node with BM capability only needs its own BM keys, and there is no need for sharing them with other devices.

V. Simulations

In order to evaluate the performance of the redundant communication path and the impact of the LoRaWAN critical traffic on possible coexisting regular BM activity, a purposely simulator has been implemented, exploiting the MATLAB Bluetooth Toolbox. Bluetooth specs 4.X are considered, that require advertize messages to be transmitted only in the primary channels. In particular, the impact of selecting different configurations for the BM and the overlaid LoRaWAN networks has been evaluated, showing how packet loss probability (Ploss) and E2E latency are affected.

A. Simulated Scenarios and Test Bench

In detail, the analysis carried out is focused on evaluating.

1) The effect of segmentation of LoRaWAN messages. For the sake of generality, a user payload of 40 B, permitted by all the SF values, has been considered. Such a user payload originates five segments at BM (due to: additional 13 B of the LoRaWAN header and trailer, additional 7 B due to the BM MIC, and the vendor and opcode IDs imposed at the BM Transport layer). Since the usage of consecutive advertising events greatly affects performance, different advertize times have been considered for nodes belonging to such a distributed LoRaWAN source. In particular, $T_{\mathrm{ADV,LW}} = \{50, 100, 200\}$ ms, while for regular BM traffic $T_{\mathrm{ADV}} = 20$ ms.
2) The effect of different LoRaWAN message update rates. Taking into account sporadic behavior of critical communications, the update range is chosen in the set $T_{\mathrm{LW(1)}} = \{1, 2, 4, 12, 60\}$ msg/h with the simulation duration set to $T_{\mathrm{SIM(1)}} = 24$ h. Moreover, in order to better highlight the impact of BM traffic, an additional set $T_{\mathrm{LW(2)}} = \{60, 120, 240, 720\}$ msg/h has been also considered with the simulation time set to $T_{\mathrm{SIM(2)}} = 1$ h (both situations consider a comparable number of LoRaWAN messages).

It must be noted that if a single DINR is present in the BM network, duty-cycle limits in the order of 1% (as those imposed by EU regulation in the sub-GHz bands) result in an actual message rate ranging from 15 to 360 msg/h, when the considered 40 B payload is transmitted varying from SF12 down to SF7.

The simulated scenarios have been carefully selected to be as general as possible and application agnostic. Since flooding is used as a forwarding/routing method by BM, increasing the number of devices behaving as a relay generally worsen network congestion and results in a higher packet loss [32]. The BM network consists of a relatively large number of relay nodes (25), that provide adequate regular spatial coverage. Such an arrangement is often found in real scenarios; they can represent a set of already in place BM devices (not necessarily related to any LoRaWAN-based application) like, for instance, being part of a co-located smart parking solution (usually, fixed devices are also main powered). With the aim of maximizing the simulation scope, relays are arranged on a grid topology, as shown in Fig. 5 (following the approach in [33]). Each radio has range $R = 12$ m, while grid spacing is 10 m. Five DINs have been considered; four DINs generate LoRaWAN critical uplink traffic in a round-robin arrangement, while another one is the DINR. This configuration represents a possible scenario where the DINRs are in well-known positions ensuring good LoRaWAN coverage, while the DINs suffer from low signal quality and rely on the redundant path for transmitting critical traffic.

As regards LoRaWAN, the sparse critical traffic sources are DINs $= \{26, 27, 28, 29\}$, to interest the whole considered area. The DINR is hosted by node $\{13\}$, located at the center of the grid and acting as a sink for the LoRaWAN source nodes. The shortest path in this case is four-hop long. These nodes are scheduled for transmission in a round-robin fashion, providing one new LoRaWAN frame in agreement with the aforementioned update rate.

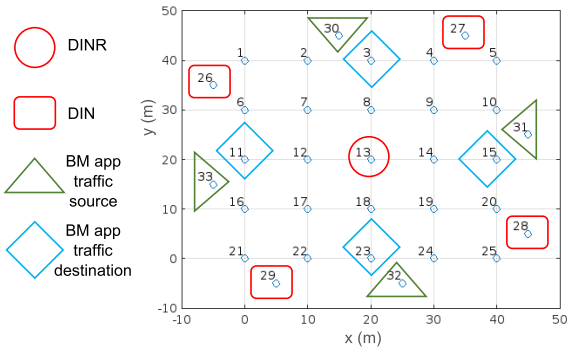


Fig. 5. Simulated BM network: relay nodes are deployed on a 5 × 5 grid; nodes generating BM application traffic are located out of the grid in symmetrical positions, while sinks are part of the grid.

TABLE I
RESUME OF RELEVANT SIMULATION PARAMETERS

T_{ADV} [ms]	$T_{ADV,i}$ [ms]	T_{SCAN} [ms]	T_{RN} [ms]	T_{RR} [ms]	NTC	RTC
20	20	30	20	20	2	2
Flow 1	Flow 2	Flow 3	Flow 4	DIN		DINR
30→23	32→3	31→11	33→15	{26,27,28,29}		{13}

As regards the BM traffic, four different flows are considered, involving the following source/destination pairs, along north-south and east-west directions: {30, 23}, {32, 3}, {31, 11}, and {33, 15}. Node locations are symmetrical, in order to similarly interest all the relay devices; the shortest path required five hops to reach the final destination, passing through the DINR. As regards the update rate, a worst case scenario is addressed, considering a heavily loaded BM network. In particular, a new BM frame (having the maximum permitted PDU—length of 39 B) is transmitted every T_{BM} = 2 s (with a random initial offset), a suitable value for a demanding application scenario as the industrial one [22]. Relevant simulation parameters for the BM network are resumed in Table I.

B. Simulation Results

Performance has been evaluated in each simulated scenario (i.e., T_{SIM} = 24 h, T_{SIM} = 1 h, and different overlaid LoRaWAN traffic) using the following metrics.

1) The probability of failing the delivery of a critical LoRaWAN message Ploss, LW (i.e., at least one of the 5 BM segments is not correctly received) and of a BM application message Ploss, BM (i.e., a BM packet is not correctly received).
2) The trip time for a LoRaWAN message $T_{E2E,LW}$ and the trip time for a BM application message $T_{E2E,BM}$.

A comparison of failure probability and trip time variations for the LoRaWAN traffic is reported in Figs. 6 and 7, respectively.

Considering the simplified expression in (2) and assuming Ploss, LW = P_{FBM}, these experiments confirm that: 1) a trade-off exists between the desired failure probability (worsening with shorter $T_{ADV,LW}$) and the desired latency (worsening with longer $T_{ADV,LW}$) and 2) since the $P_{FBM} \approx 1\%$, the overall

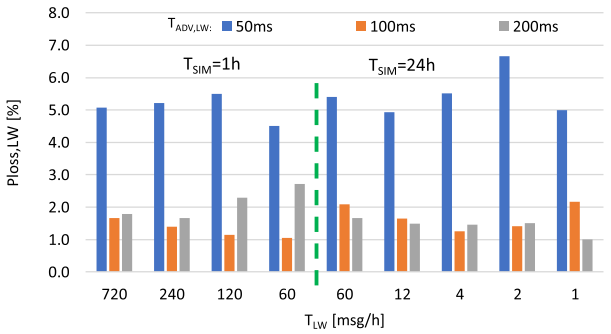


Fig. 6. Failure probability for the critical LoRaWAN traffic (across the BM network) under different critical LoRaWAN traffic condition.

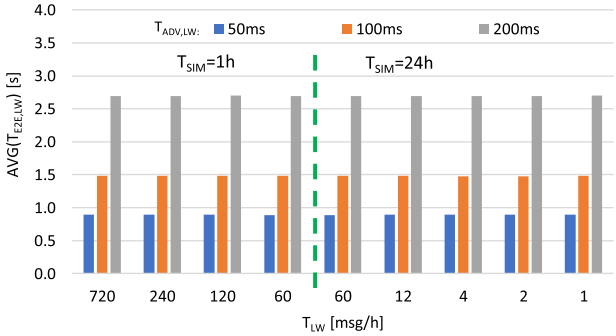


Fig. 7. Average trip time for the critical LoRaWAN traffic (across the BM network) under different critical LoRaWAN traffic condition.

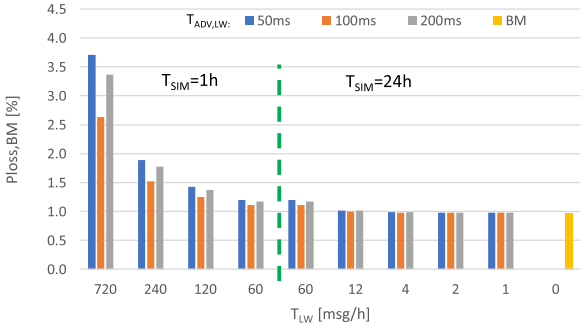


Fig. 8. Failure probability for the BM traffic under different critical LoRaWAN traffic condition (including no LoRaWAN traffic at all).

failure probability P_F is reduced by almost two orders of magnitude.

Additionally, comparison of failure probability and trip time variations for the coexisting BM traffic under different LoRaWAN traffic (including its absence) is reported in Figs. 8 and 9, respectively.

As expected, the distribution of trip times across the BM network is not symmetrical, as highlighted by (5) and (7) in Appendix, and dictates the following bounds (T_{MIN} T_{MAX}) for one-segment long messages moving across the shortest path: [100, 400] ms. An example of such a distribution is shown in Fig. 10, in which the tail is due to paths different from the shortest one.

As regards the critical LoRaWAN traffic, which consists of five-segment long messages, when the shortest path is considered, different bounds are obtained, depending on:

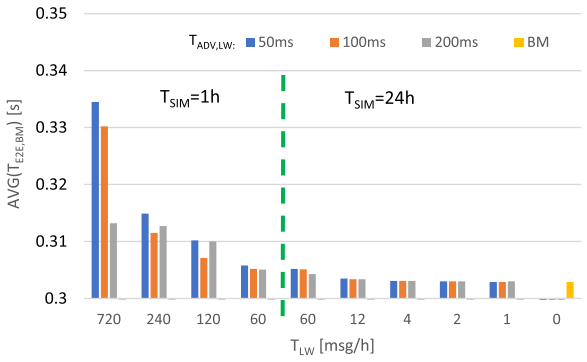


Fig. 9. Average trip time for the BM traffic under different critical LoRaWAN traffic condition (including no LoRaWAN traffic at all).

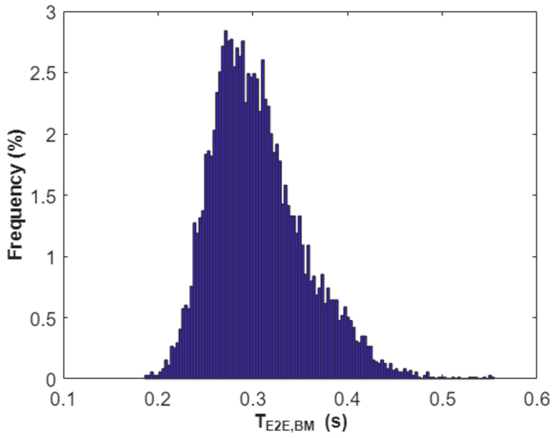


Fig. 10. Distribution of end to end trip time $T_{E2E,BM}$ for a sample simulation run when $T_{SIM} = 1$ h (LoRaWAN traffic is absent; bin width is 3 ms).

TABLE II
STD AND SKEW OF THE E2E TRIP TIME FOR THE LORAWAN TRAFFIC

	T_{LW} [msg/h]	STD $T_{E2E,LW}$ [s]	SKEW $T_{E2E,LW}$	STD $T_{E2E,LW}$ [s]	SKEW $T_{E2E,LW}$	STD $T_{E2E,LW}$ [s]	SKEW $T_{E2E,LW}$
		Tadv = 50 ms		Tadv = 100 ms		Tadv = 200 ms	
T_{SIM}: 1h	720	0.06	0.8	0.07	1.3	0.06	1.0
	240	0.06	0.8	0.06	1.5	0.06	1.0
	120	0.05	0.7	0.05	1.2	0.06	1.0
	60	0.06	0.5	0.05	1.1	0.06	1.0
T_{SIM}: 24h	60	0.06	0.8	0.06	1.2	0.09	1.8
	12	0.06	0.7	0.06	1.2	0.09	1.7
	4	0.06	0.7	0.06	0.6	0.09	1.7
	2	0.06	0.8	0.06	1.0	0.10	1.4
	1	0.05	0.4	0.06	1.2	0.09	1.7

1) $T_{ADV,LW} = 50$ ms: [110, 1230] ms; or
2) $T_{ADV,LW} = 100$ ms: [160, 1980] ms; or
3) $T_{ADV,LW} = 200$ ms: [260, 3480] ms.

For this reason, other than the average value, standard deviation and skewness have also been collected and reported in Tables II and III.

In particular, $N_{SIM} = 10$ simulation runs have been executed per each scenario and metrics average values are reported; a sensitivity analysis has been performed evaluating the standard deviation of the metrics of interest for the considered runs; for the sake of clarity, upper bounds are in Table IV.

TABLE III
STD AND SKEW OF THE E2E TRIP TIME FOR THE APPLICATION BM TRAFFIC

	T_{LW} [msg/h]	STD $T_{E2E,BM}$ [s]	SKEW $T_{E2E,BM}$ [s]	STD $T_{E2E,BM}$ [s]	SKEW $T_{E2E,BM}$ [s]	STD $T_{E2E,BM}$ [s]	SKEW $T_{E2E,BM}$ [s]
		Tadv = 50 ms		Tadv = 100 ms		Tadv = 200 ms	
T_{SIM}: 1h	720	0.086	1.8	0.071	1.3	0.057	1.0
	240	0.065	1.8	0.057	1.5	0.064	1.0
	120	0.058	1.6	0.051	1.2	0.058	1.0
	60	0.054	1.3	0.048	1.1	0.056	1.0
T_{SIM}: 24h	60	0.054	1.4	0.047	1.1	0.055	1.0
	12	0.050	0.9	0.045	0.8	0.054	1.0
	4	0.050	0.8	0.044	0.8	0.054	1.0
	2	0.050	0.8	0.044	0.8	0.054	1.0
	1	0.049	0.8	0.044	0.7	0.054	1.0

	STD $T_{E2E,BM}$ [s]	SKEW $T_{E2E,BM}$ [s]
none	0.049	0.8

TABLE IV
SIMULATION SENSITIVITY ANALYSIS: STANDARD DEVIATION OF PLOSS, AVG, STD, AND SKEW

Ploss,BM [%]	AVG($T_{E2E,BM}$) [s]	STD($T_{E2E,BM}$) [s]	SKEW($T_{E2E,BM}$)
< 0.5	< 0.001	< 0.001	< 0.1
Ploss,LW [%]	AVG($T_{E2E,LW}$) [s]	STD($T_{E2E,LW}$) [s]	SKEW($T_{E2E,LW}$)
< 3.0	< 0.01	< 0.01	< 0.5

It is interesting to highlight that the choice of the $T_{ADV,LW}$ is important, especially considering the segmentation of LoRaWAN (large) messages. Indeed, when the $T_{ADV,LW}$ increases, the five segments spread across longer interval, justifying the $T_{E2E,LW}$ performance worsening. However, the higher BM raw data rate with respect to the LoRa data rate(s), mitigates the impact; as a matter of fact, $T_{E2E,LW}$ remains comparable with the over-the-air duration of actual LoRa messages (as better highlighted in the next section). Additionally, when more consecutive advertize and scan slots are available for the regular BM traffic before a new segment is transmitted, collisions occur more frequently, as confirmed by the higher Ploss, LW value resulting from shorter $T_{ADV,LW}$.

From the BM traffic point of view, the simulation results confirm that, when update rate typical of IoT applications is considered (i.e., one LoRaWAN message per minute or slower), the proposed overlaid approach does not significantly affect the overall performance and all the metrics show values aligned with the results obtained when the LoRaWAN traffic is completely absent.

VI. EXPERIMENTAL EVALUATION

A proof-of-concept prototype has been implemented for verifying the feasibility in a real-world scenario.

A. Experimental Test Bench

In particular, the BM and DIN/DINR nodes have been realized around the nRF52840-DK from Nordic Semiconductor. The latter is a single-board development kit based on the 52840 SoC, integrating a 32-bit ARM

Cortex-M4F @ 64 MHz, 256 KB RAM, 1 MB Flash, a 128-bit AES CCM accelerator and a 2.4 GHz transceiver, satisfying BLE L1 specifications. Almost all the general-purpose Input/Output pins (GPIOs, which can also be mapped to communication peripherals) are accessible via edge connectors. Moreover, the board includes a SEGGER J-Link debugger/programmer and a 2.4 GHz PCB antenna. The firmware leverages on the "nRF connect SDK" (version 1.7.0), which natively supports a BM stack, running under the Zephyr real-time operating system [34]. Different from other BM nodes, the DINs and DINRs are also connected to an RN2483 module from Microchip (operating in the EU868 spectrum region) via a UART serial link at 57.6 kb/s. The RN2483 LoRaWAN stack has been paused and the embedded SX1276 radio device (from Semtech) has been directly addressed using the "*radio tx*" and "*radio rx*" AT-like commands of the module interpreter. In this way, it has been possible to transmit and receive the LoRaWAN L1 frame to be processed and analyzed by the nRF52840 purposely designed firmware. Indeed, the original BM stack has been enhanced by adding functionalities derived from the open source LoRaWAN stack from Semtech,[1] in order to manage the LoRaWAN L1 payload (including the messages of the joining procedure) in the DIN and DINR nodes.

Additionally, the DIN and DINR firmware also pulses GPIO lines to signal when:

1) T_{U1}: a LoRaWAN uplink message is generated at the DIN;
2) T_{U2}: uplink is received at the DINR;
3) T_{U3}: it is transferred to the LoRa radio in the DINR;
4) T_{D1}: a LoRaWAN downlink message is received at the DINR;
5) T_{D2}: downlink is arrived at the DIN.

In particular, three E5818A LXI trigger boxes from Agilent have been used to provide UTC referred timestamps of the T_{U1}-T_{U2}-T_{U3} and T_{D1}-T_{D2} instants. In particular, the trigger boxes are disciplined via the PTPv1 protocol by a ML30 Hirschmann, the latter receiving a UTC reference from a TimeMachine TM1000A GPS-based network time server. Due to the use of NTP protocol on the TM1000A, an overall accuracy in the millisecond range is expected [35]. The testbench has been arranged in the Industrial facility building of the Faculty of Engineering, deploying BM nodes in different laboratories, as depicted in Fig. 11. A block diagram of the testbench is depicted in Fig. 12.

Since the RN2483 is compliant with the LoRaWAN L1 (i.e., LoRa radios), it is straightforward collecting the LoRaWAN (uplink and downlink) frames using a standard GW connected to a LoRaWAN backend. During real-world experiments, a Laird RG186 GW has been connected to the "The Things Stack" (TTS) (community edition). TTS is a crowdsourced, open, and decentralized LoRaWAN backend managed by the "The Things Network" community. From the TTS console and/or by means of subscription to well-known topics managed by a MQTT Broker, it has been possible to access live log of the frames received and transmitted by the

[1]Available at: https://github.com/Lora-net/LoRaMac-node (accessed on Feb. 21, 2024).

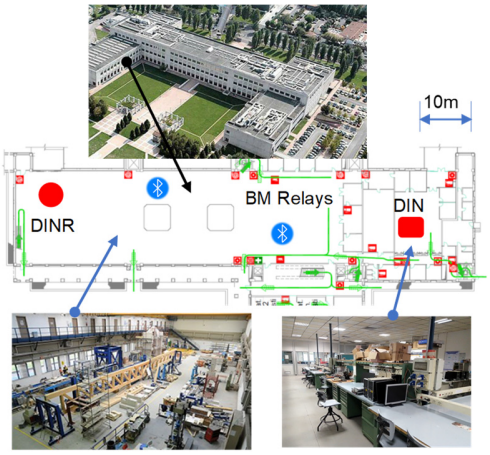


Fig. 11. Deployment of DIN, DINR, and BM relay nodes in the Industrial facility building of the Faculty of Engineering at the University of Brescia.

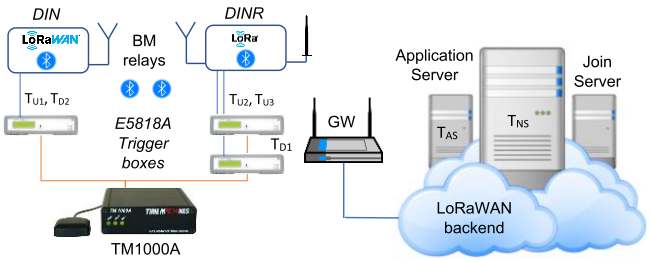


Fig. 12. Block diagram of the experimental test bench.

GW, the NS, and the AS. In particular, other than enciphered payload, timestamps related to the reception of the frame in the GW, the NS, and the AS and information about the estimation of the received signal strength indication (RSSI) and the signal-to-noise ratio (SNR) are available. Despite the GW timestamps are from a free running counter, the other two timestamps (T_{NS} and T_{AS}) are UTC time synchronized.

During the experiment, a set of 100 consecutive LoRaWAN transactions, consisting of the confirmed uplink (40 B LoRaWAN payload, 13 B LoRaWAN header) followed by the acknowledgment downlink (empty LoRaWAN payload, 13 B LoRaWAN header), have been collected. The DIN update rate is 60 msg/h, while the BM network has been setup considering the parameters in Table I and it consists of the DIN, the DINR, and two intermediate relays, implementing three hops (nodes have been properly shielded to ensure linear topology).

B. Experimental Results

Availability of the aforementioned timestamps permits to evaluate the following metrics.

1) $\Delta_{DIN,DINR} = T_{U2} - T_{U1}$: the time interval the uplink needs to travel across the BM network; this metric is comparable with the previously introduced $T_{E2E,LW}$.
2) $\Delta_{DINR,LW} = T_{U3} - T_{U2}$: the time interval needed to process the LoRaWAN message at the DINR.
3) $\Delta_{NS} = T_{NS} - T_{U3}$: the time interval before the NS receives (and stores) the uplink frame.
4) $\Delta_{AS} = T_{AS} - T_{NM}$: the time interval before the AS receives (and stores) the uplink frame.

TABLE V
REAL-WORLD EXPERIMENTAL RESULTS

	Avg [s]	Std [s]	Avg [s]	Std [s]	Avg [s]	Std [s]
SF	**7**		**9**		**12**	
$\Delta_{DIN,DINR}$	0.787	0.058	0.775	0.052	0.778	0.053
$\Delta_{DINR,LW}$	0.057	<0.001	0.057	<0.001	0.057	<0.001
Δ_{NS}	0.133	0.006	0.329	0.006	2.466	0.044
Δ_{AS}	0.209	0.005	0.209	0.005	0.210	0.006
$\Delta_{LW,DINR}$	5.037	0.009	5.152	0.008	6.139	0.020
$\Delta_{DINR,DIN}$	0.247	0.060	0.238	0.056	0.258	0.060

5) $\Delta_{LW,DINR} = T_{D1} - T_{NM}$: the time needed to receive the downlink at the DINR since the reception of the uplink in the NM.
6) $\Delta_{DINR,DIN} = T_{D2} - T_{D1}$: the time interval the downlink needs to travel across the BM network; this metric is comparable with the previously introduced $T_{E2E,LW}$.

Results for different SF values are resumed in Table V, in which the average and standard deviation values are reported. The metrics $\Delta_{DIN,DINR}$, $\Delta_{DINR,LW}$, and $\Delta_{DINR,DIN}$ do not depend on the SF value, but are only function of the BM network configuration and traffic. On the contrary, Δ_{NS} is affected by the LoRaWAN frame air duration, while Δ_{AS} can change due to the actual server load of the LoRaWAN backend. In any case, agreement with results obtained by authors themselves using similar regular LoRaWAN infrastructure exists [36]. It can be noticed that RX1 window is selected by the NS for SF = {7, 9}, since TTN default value is $T_{RX1} = 5$s, while RX2 is preferred for SF = 12. It can be also highlighted that $\Delta_{LW,DINR}$ is lower than simulation results, due to the absence of other interfering BM traffic sources.

VII. CONCLUSION

IoT-like applications demand for standardized approaches to network and security management. A typical example is the LoRaWAN solution, whose specifications not only describe the protocol, but also define the backend. In this work, the ideas of tunneling, encapsulation, and overlay networks, consisting of nodes and logical links constructed on an existing network has been proposed for transferring LoRaWAN protocol across a BM network. Such an approach is particularly useful in mixed critical scenario, since it permits to have a redundant communication path for critical traffic, which requires different QoS with respect to non-critical traffic. The obtainable performance and the feasibility of the proposed approach have been evaluated by means of both simulation and real-word experiments. As regards the LoRaWAN critical traffic transported over the redundant BM channel, results from simulations and experiments are comparable with findings reported in literature about the BM performance (as in [33] and [34], just to mention a few). The packet loss in the redundant BM link is in the order of 1% even when demanding regular BM traffic is present (four flows updating every 2 s, which consent to stress the BM challenges related to the flooding [37]; therefore, the overall delivery success is improved by almost two orders of magnitude. However, the message payload can affect the time performance, due to the BM segmentation, extending trip-time up to 2.5 s for an advertize time of 200 ms. Therefore, the proposed approach permits to reliably and effectively receive messages from devices unreachable by the LoRaWAN GW. On the other hand, when the overlaid LoRaWAN critical traffic moved along the redundant channel is sporadic (update rate of 1 min or higher), it has very little, if any, influence on the possibly coexisting BM traffic. In other words, metrics of interest as the trip-time and the Ploss are close to values obtained without any overlaid traffic (in the order of 1% and 300 ms in the simulated scenario consisting of 4 BM application data streams updated every 2 s).

Future Works

A future development, supported by the very good results presented in this work, will be the design of an integrated electronics for the dual interface node (DIN and DINR).

Additionally, the proposed approach suggesting the implementation of a redundant link for improving availability and survivability could be also carried out using other mesh technologies, like those based on the IEEE802.15.4 radios (as Zigbee, just to mention one).

APPENDIX

In this Appendix the fundamentals of the considered wireless communication solutions are given.

A. LoRa and LoRaWAN

LoRaWAN specifications are oriented to describe the upper protocol layers and are different from LoRa, which is a proprietary physical layer (layer L1) exploiting an enhanced version chirp spread spectrum modulation. In particular, LoRa chirp bandwidth BS $\in$ {125, 250, 500} kHz is fixed, whereas the chirp duration TS is divided into 2^{SF} intervals so that TS·BS $= 2^{SF}$, where SF $\in \{7, \ldots, 12\}$ is a tunable parameter named Spreading Factor. Discontinuities in the frequency trajectory can occur at the edge of one of such intervals, so that SF bits can be coded using a single frequency trajectory. Since frames transmitted using different SF are also quasi-orthogonal, SF selection can be considered as the selection of a virtual channel, allowing for frame overlapping in time and frequency. When BS = 125 kHz, as typically occurs in Europe, the data rate ranges from about 0.3 to about 5.5 kb/s, depending on the SF.

In LoRaWAN the use of LoRa radios is not compulsory, but in the case, the payload length is limited depending on the SF (242 B @ SF7 and SF8; 115 B @ SF9, 51 B @ SF10, SF11, and SF12). The LoRaWAN Data Link layer (L2) is based on pure ALOHA, even if channel activity detection (CAD) is permitted to implement listen before talk (LBT) medium access strategy. The star network topology is adopted, so that each node is one hop away from the GW, i.e., the device(s) tunneling the wireless messages to/from the backend, usually deployed in the cloud, by means of wired connections. In mandatory Class A (considered in this work), the data exchanges are started by the end device (uplink direction); two receiving windows (RX1 and RX2, for downlink) are opened after intervals T_{RX1} and $T_{RX2} = T_{RX1} + 1$ s from the end of the uplink frame. Optionally, the RX2 window can

be prolonged for continuous listening (in Class C operation), or downlink Beacon messages are scheduled for synchronization and supporting additional unsolicited downlinks (in Class B operation).

LoRaWAN also defines logical entities in the backend. Network management is in charge of a single network server (NS), even if roaming is possible, that provides acknowledgment of confirmed messages and enables adaptive data rate strategies (e.g., depending on the channel quality). The message content is opaque for the NS, that only checks the integrity by means of a network wide key. The uplink/downlink traffic is directed/originated to/from the AS, which takes care of message encryption/decryption by means of an application key and allows for the end user application integration (typically by means of a message-oriented middleware or REST APIs). Finally, latest release of the standard also includes a JS for managing the security keys.

B. Bluetooth Mesh

BM, initially released in 2017, exploits the same physical and data link layers of the BLE standard. Other than the legacy uncoded data rate of 1 and 2 Mb/s, new features inherited from the 5.0 release of the specs include the coded data rate at 500 and 125 kb/s (for longer range); moreover, advertising messages (transmitted on one of the three primary advertising channels, i.e., 37, 38, and 39) may embed a reference to a secondary advertising channel (randomly chosen among the other 37 BLE channels), thus extending the amount of exchanged data. An additional periodic advertising is also permitted, for contacting unconnected devices and allowing for their synchronization.

Mesh functionalities are empowered by additional upper layers. The bearer layer defines the advertising bearer, leveraging on the BLE advertising and scanning features to exchange PDUs, and the generic attribute profile (GATT) bearer, for ensuring backward compatibility with device not supporting BM. Above, there is the network layer, analyzing device addresses (unicast, multicast, and virtual) and taking care of relay and proxy functionalities. The lower transport layer takes care of messages delivery (if they are acknowledged or unacknowledged) and is also in charge of managing PDUs fragmentation (max unsegmented payload consists of 15 B; otherwise, 32 segments of 12 B each are permitted). The upper transport layer manages authentication, encryption and decryption data coming to/from the access layer. It is also in charge of managing transport control messages (friendship, heartbeat, etc.). The access layer specifies the application data format and supervises the encryption/decryption process at the upper transport layer. The remaining layers (foundation models and model) are concerned with the proper setup of parameters defining the way the network is configured and managed; three models actually exist: server, client, and control.

From the system architecture point of view, a node that has joined the network (via the provisioning procedure) can have additional functionalities: 1) when behaving as a relay, it can retransmit messages received on advertising bearers; 2) if it is a low-power node, operation occurs with low duty-cycle to minimize consumption; 3) if it is a friend node, it acts as a sort of proxy for low power nodes; 4) finally, a provisioner node can supervise the joining procedure for a new device entering the BM network. Some words must be spent about the way messages are delivered, i.e., the managed flooding [38]. It is based on the previously introduced advertising procedure, in which a message is asynchronously transmitted over the three primary channels, with an interspace time consisting of fixed and random parts. If a relay node is not the intended destination of a message, it inserts the message in a forwarding queue. In this way, there is no need for identifying a route toward the destination. The available bandwidth is a problem [39] and, in order to limit the traffic burden, a time to live (TTL) parameter exists; each time the same message is sent, the TTL is decreased so that flooding can occur only if TTL $>$ 1 (and maximum value is TTL $=$ 127). Reliability can be improved by means of retransmission; source and relay nodes can be configured to repeat the same message a predefined number of times, at a predefined time interval.

As a consequence, BM performance strictly depends on the values that the advertize and scan intervals assume (T_{ADV} and T_{SCAN}, respectively), other than the number of retries at the network level (dictated by the Network Transmit Count -NTC- and Relay Transmit Count -RTC-, respectively). For a certain number M of segments and N of relays, the minimum delivery time T_{MIN} occurs when the first transmission of the very last segment is gathered, and all the replicas of previous segments have been already transmitted. In this case, the time $T_{\mathrm{PROP},M\_\mathrm{First}}$ needed to propagate the last segment along the relays can be modeled as in the following:

$$T_{\mathrm{PROP},M\_\mathrm{First}} = T_{\mathrm{ADV}} + \sum_{i=1}^{N} \left(T_{\mathrm{RX},i} + T_{\mathrm{RAND}} + T_{\mathrm{ADV},i}\right) \quad (3)$$

where T_{ADV} and $T_{\mathrm{ADV},i}$ are the source and ith relay advertize time, respectively; $T_{\mathrm{RX},i}$ is the time required to match the advertising channel; and an additional random delay in the range $T_{\mathrm{RAND}} \in [0, 10]$ ms is imposed by specs for "desynchronizing" transmissions. The time $T_{\mathrm{PROP},0,\ldots,M-1}$ needed to complete the transmissions of previous segments can be modeled as in (4); in particular, it depends on the maximum number of retries along the transmission path

$$T_{\mathrm{PROP},0,\ldots,M-1} = (M-1)\cdot \max\left\{[(\mathrm{NTC}+1)\cdot T_{\mathrm{RN}}], \left[(\mathrm{RTC}i+1)\cdot T_{\mathrm{RR},i}\right]\right\} \quad (4)$$

where T_{RN} and $T_{\mathrm{RR},i}$ are the retry time for the message source and the ith relay (including the random term). Therefore, T_{MIN} can be expressed as in (5), leveraging on the simplified model in [37]. It must be highlighted that other neglected issues (as node buffer overflow) can further increase the latency

$$T_{\mathrm{MIN}} = T_{\mathrm{PROP},M\_\mathrm{First}} + T_{\mathrm{PROP},0,\ldots,M-1}. \quad (5)$$

In order to provide an upper bound, authors evaluate the time T_{MAX} for a successfully received message when only the last replica of all the segments is received and $T_{\mathrm{RX},i} = 20$ ms and $T_{\mathrm{RAND}} = 10$ ms, meaning that propagation of the last

segment requires $T_{\text{PROP},M\_\text{Last}}$ as in the following:

$$T_{\text{PROP},M_{\text{Last}}} = T_{\text{PROP},M\_\text{First}} + (\text{NTC} \cdot T_{\text{RN}}) + \sum_{i=1}^{N} (\text{RTC}i \cdot T_{\text{RR},i}). \tag{6}$$

As a consequence, despite improbable, T_{MAX} can be estimated as in the following:

$$T_{\text{MAX}} = T_{\text{PROP},M\_\text{Last}} + T_{\text{PROP},0,\ldots,M-1}. \tag{7}$$

ACKNOWLEDGMENT

The authors would like to thank Dr. E. Mondini for the help during simulations and experimental tests.

REFERENCES

[1] G. Fortino, C. Savaglio, G. Spezzano, and M. Zhou, "Internet of Things as system of systems: A review of methodologies, frameworks, platforms, and tools," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 1, pp. 223–236, Jan. 2021.

[2] S. Kumar, *Fundamentals of Internet of Things*. Boca Raton, FL, USA: CRC Press, 2021.

[3] M. Urbina, T. Acosta, J. Lázaro, A. Astarloa, and U. Bidarte, "Smart sensor: SoC architecture for the industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6567–6577, Aug. 2019.

[4] G. Cena, S. Scanzio, M. G. Vakili, C. G. Demartini, and A. Valenzano, "Assessing the effectiveness of channel hopping in IEEE 802.15.4 TSCH networks," *IEEE Open J. Ind. Electron. Soc.*, vol. 4, pp. 214–229, 2023.

[5] E. Sisinni, D. F. Carvalho, and P. Ferrari, "Emergency communication in IoT scenarios by means of a transparent LoRaWAN enhancement," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10684–10694, Oct. 2020.

[6] M. B. Attia, K.-K. Nguyen, and M. Cheriet, "Dynamic QoE/QoS-aware queuing for heterogeneous traffic in smart home," *IEEE Access*, vol. 7, pp. 58990–59001, 2019.

[7] P. Ferrari et al., "On the use of LoRaWAN and cloud platforms for diversification of mobility-as-a-service infrastructure in smart city scenarios," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–9, 2022, doi: 10.1109/TIM.2022.3144736.

[8] LoRa Alliance. (May 2023). *Multicast D2D Communication Technical Recommendation TR012 Version 1.0.0*. Accessed: Feb. 2024. [Online]. Available: https://resources.lora-alliance.org/

[9] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, and A. Chehab, "LoRaWAN security survey: Issues, threats and possible mitigation techniques," *Internet Things*, vol. 12, Dec. 2020, Art. no. 100303.

[10] J. R. Cotrim and J. H. Kleinschmidt, "LoRaWAN mesh networks: A review and classification of multihop communication," *Sensors*, vol. 20, no. 15, p. 4273, Jul. 2020.

[11] J. Tournier, F. Lesueur, F. L. Mouel, L. Guyon, and H. Ben-Hassine, "A survey of IoT protocols and their security issues through the lens of a generic IoT stack," *Internet Things*, vol. 16, Dec. 2021, Art. no. 100264.

[12] F. S. D. Silva et al., "A survey on long-range wide-area network technology optimizations," *IEEE Access*, vol. 9, pp. 106079–106106, 2021.

[13] S. Kajioka et al., "A QoS-aware routing mechanism for multi-channel multi-interface ad-hoc networks," *Ad Hoc Netw.*, vol. 9, no. 5, pp. 911–927, Jul. 2011.

[14] J. Rao and S. Vrzic, "Packet duplication for URLLC in 5G dual connectivity architecture," *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Barcelona, Spain, Apr. 2018, pp. 1–6.

[15] A. J. Onumanyi, A. M. Abu-Mahfouz, and G. P. Hancke, "Cognitive radio in low power wide area network for IoT applications: Recent approaches, benefits and challenges," *IEEE Trans. Ind. Informat.*, vol. 16, no. 12, pp. 7489–7498, Dec. 2020.

[16] S. Sendra, L. Parra, J. M. Jimenez, L. Garcia, and J. Lloret, "LoRa-based network for water quality monitoring in coastal areas," *Mobile Netw. Appl.*, vol. 28, no. 1, pp. 65–81, Jul. 2022.

[17] A. I. Griva et al., "LoRa-based IoT network assessment in rural and urban scenarios," *Sensors*, vol. 23, no. 3, p. 1695, Feb. 2023.

[18] I. Cappelli, A. Fort, M. Mugnaini, S. Parrino, and A. Pozzebon, "Underwater to above water LoRaWAN networking: Theoretical analysis and field tests," *Measurement*, vol. 196, Jun. 2022, Art. no. 111140.

[19] M. Ballerini, T. Polonelli, D. Brunelli, M. Magno, and L. Benini, "NB-IoT versus LoRaWAN: An experimental evaluation for industrial applications," *IEEE Trans. Ind. Informat.*, vol. 16, no. 12, pp. 7802–7811, Dec. 2020, doi: 10.1109/TII.2020.2987423.

[20] D. Magrin, M. Capuzzo, A. Zanella, L. Vangelista, and M. Zorzi, "Performance analysis of LoRaWAN in industrial scenarios," *IEEE Trans. Ind. Informat.*, vol. 17, no. 9, pp. 6241–6250, Sep. 2021, doi: 10.1109/TII.2020.3044942.

[21] E. Sisinni, D. F. Carvalho, P. Ferrari, A. Flammini, and M. Gidlund, "Adding redundancy to LoRaWAN for emergency communications at the factory floor," *IEEE Trans. Ind. Informat.*, vol. 18, no. 10, pp. 7332–7340, Oct. 2022, doi: 10.1109/TII.2021.3124054.

[22] A. Aijaz, "Infrastructure-less wireless connectivity for mobile robotic systems in logistics: Why Bluetooth mesh networking is important?" in *Proc. 26th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2021, pp. 1–8.

[23] Y. Liu, M. Kashef, K. B. Lee, L. Benmohamed, and R. Candell, "Wireless network design for emerging IIoT applications: Reference framework and use cases," *Proc. IEEE*, vol. 107, no. 6, pp. 1166–1192, Jun. 2019, doi: 10.1109/JPROC.2019.2905423.

[24] M. J. Faber, K. M. van der Zwaag, W. G. V. dos Santos, H. R. D. O. Rocha, M. E. V. Segatto, and J. A. L. Silva, "A theoretical and experimental evaluation on the performance of LoRa technology," *IEEE Sensors J.*, vol. 20, no. 16, pp. 9480–9489, Aug. 2020, doi: 10.1109/JSEN.2020.2987776.

[25] Q. Guo, F. Yang, and J. Wei, "Experimental evaluation of the packet reception performance of LoRa," *Sensors*, vol. 21, no. 4, p. 1071, Feb. 2021, doi: 10.3390/s21041071.

[26] U. Coutaud, M. Heusse, and B. Tourancheau, "LoRa channel characterization for flexible and high reliability adaptive data rate in multiple gateways networks," *Computers*, vol. 10, no. 4, p. 44, Apr. 2021, doi: 10.3390/computers10040044.

[27] L. Bhatia, P.-Y. Chen, M. Breza, C. Zhao, and J. A. McCann, "IRONWAN: Increasing reliability of overlapping networks in LoRaWAN," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10763–10776, Jul. 2022, doi: 10.1109/JIOT.2021.3125842.

[28] H. Leong Goh, K. Kiong Tan, S. Huang, and C. W. de Silva, "Development of bluewave: A wireless protocol for industrial automation," *IEEE Trans. Ind. Informat.*, vol. 2, no. 4, pp. 221–230, Nov. 2006, doi: 10.1109/TII.2006.885186.

[29] J. Kjellsson, A. Elisabeth Vallestad, R. Steigmann, and D. Dzung, "Integration of a wireless I/O interface for PROFIBUS and PROFINET for factory automation," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4279–4287, Oct. 2009, doi: 10.1109/TIE.2009.2017098.

[30] C. Garrido-Hidalgo, T. Olivares, F. J. Ramirez, and L. Roda-Sanchez, "An end-to-end Internet of Things solution for reverse supply chain management in industry 4.0," *Comput. Ind.*, vol. 112, Nov. 2019, Art. no. 103127, doi: 10.1016/j.compind.2019.103127.

[31] R. Narayanan and C. S. R. Murthy, "A routing framework with protocol conversions across multiradio IoT platforms," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4417–4432, Mar. 2021, doi: 10.1109/JIOT.2020.3028239.

[32] N. Paulino, L. M. Pessoa, A. Branquinho, R. Almeida, and I. Ferreira, "Optimizing packet reception rates for low duty-cycle BLE relay nodes," *IEEE Sensors J.*, vol. 22, no. 13, pp. 13753–13762, Jul. 2022, doi: 10.1109/JSEN.2022.3179622.

[33] R. Rondón, A. Mahmood, S. Grimaldi, and M. Gidlund, "Understanding the performance of Bluetooth mesh: Reliability, delay, and scalability analysis," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2089–2101, Mar. 2020, doi: 10.1109/JIOT.2019.2960248.

[34] M. Baert, J. Rossey, A. Shahid, and J. Hoebeke, "The Bluetooth mesh standard: An overview and experimental evaluation," *Sensors*, vol. 18, no. 8, p. 2409, Jul. 2018, doi: 10.3390/s18082409.

[35] D. C. Mazur, R. A. Entzminger, J. A. Kay, and P. A. Morell, "Time synchronization mechanisms for the industrial marketplace," *IEEE Trans. Ind. Appl.*, vol. 53, no. 1, pp. 39–46, Jan. 2017, doi: 10.1109/TIA.2016.2603464.

[36] D. Fernandes Carvalho et al., "A test methodology for evaluating architectural delays of LoRaWAN implementations," *Pervas. Mobile Comput.*, vol. 56, pp. 1–17, May 2019, doi: 10.1016/j.pmcj.2019.03.002.

[37] Á. Hernández-Solana, D. Pérez-Díaz-De-Cerio, M. García-Lozano, A. V. Bardají, and J.-L. Valenzuela, "Bluetooth mesh analysis, issues, and challenges," *IEEE Access*, vol. 8, pp. 53784–53800, 2020.

[38] M. Reno et al., "Relay node selection in Bluetooth mesh networks," in *Proc. IEEE 20th Medit. Electrotechnical Conf. (MELECON)*, Jun. 2020, pp. 175–180.

[39] A. Valenzuela-Pérez, M. García-Lozano, J. L. Valenzuela, D. Pérez-Díaz-de-Cerio, Á. Hernández-Solana, and A. Valdovinos, "On the use of sniffers for spectrum occupancy measurements of Bluetooth low energy primary channels," *Measurement*, vol. 199, Aug. 2022, Art. no. 111573.

Emiliano Sisinni (Member, IEEE) received the M.Sc. degree in electronics engineering and the Ph.D. degree in electronic instrumentation from the University of Brescia, Brescia, Italy, in 2000 and 2004, respectively.

He is currently a Full Professor of Electronics with the Department of Information Engineering, University of Brescia. His research interests include wireless and wired networking for the Internet-of-Things (IoT) applications, with particular attention to Industrial applications.

Alessandro Depari (Member, IEEE) received the M.Sc. degree in electronics engineering and the Ph.D. degree in electronic instrumentation from the University of Brescia, Brescia, Italy, in 2002 and 2006, respectively.

He is an Associate Professor with the Department of Information Engineering, University of Brescia. His current research interests include: sensor signal conditioning and processing, embedded systems, and design and development of systems for mobile health (mHealth) and Internet of Things (IoT) applications.

Alessandra Flammini (Fellow, IEEE) received the Ph.D. (Hons.) degree in physics from the University of Rome, Rome, Italy, in 1985.

After eight years at Ansaldo Industria, Milan, Italy, in 1995, she joined the University of Brescia, Brescia, Italy, where she is a Full Professor of Electronic Measurements. She has authored or coauthored more than 200 international articles. Her current research interests include electronic instrumentation, digital processing of sensor signals, smart sensors, and wired and wireless sensor networks synchronization.

Stefano Rinaldi (Senior Member, IEEE) received the Ph.D. (Hons.) degree in electronic engineering and the Ph.D. degree in electronic instrumentation from the University of Brescia, Brescia, Italy, in 2006 and 2010, respectively.

He is currently an Associate Professor with the Department of Information Engineering, University of Brescia. His research interests include industrial real-time Ethernet network, Internet of Things, time synchronization, smart grids, renewable energy sources, electric vehicles, and cognitive building.

Paolo Ferrari (Member, IEEE) received the M.Sc. degree in electronics engineering and the Ph.D. degree in electronic instrumentation from the University of Brescia, Brescia, Italy, in 1999 and 2003, respectively.

He is currently a Full Professor with the Department of Information Engineering, University of Brescia. His research is about measurement systems for industrial and smart city applications, including performance and security analysis of real-time networks and Internet-of-Things (IoT) applications; wired and wireless sensor networks; and clock synchronization of distributed systems.

Open Access funding provided by 'Università degli Studi di Brescia' within the CRUI-CARE Agreement