From Micro to Macro IoT: Challenges and Solutions in the Integration of IEEE 802.15.4/802.11 and Sub-GHz Technologies

From Micro to Macro IoT: Challenges and Solutions in the Integration of IEEE 802.15.4/802.11 and Sub-GHz Technologies

Luca Davoli, *Member, IEEE,* Laura Belli, Antonio Cilfone, and Gianluigi Ferrari, *Senior Member, IEEE*

***Abstract*—Research efforts in the field of Internet of Things (IoT) are providing solutions in building new types of "network of networks," going beyond the technological barriers due to intrinsic limitations of the constrained devices typically used in this context. Thanks to the improvement in communication/networking protocols and the hardware cost reduction, it is now possible to define new IoT architectures, combining the "Micro" IoT paradigm, based on short-range radio technologies (e.g., IEEE 802.15.4 and IEEE 802.11), with the rising "Macro" IoT paradigm, based on Sub-GHz radio technologies. This allows the implementation of scalable network architectures, able to collect data coming from constrained devices and process them in order to provide useful services and applications to final consumers. In this work, we focus on practical integration between Micro and Macro IoT approaches, providing architectural and performance details for a set of experimental tests carried out in the campus of the University of Parma. We then discuss challenges and solutions of the proposed Micro-Macro integrated IoT systems.**

***Index Terms*—Internet of Things, IEEE 802.15.4, Sub-GHz technology, IEEE 802.11, Integration, Challenges.**

I. Introduction

THE Internet of Things (IoT) paradigm can be defined as a "*network of networks*" of interconnected devices, generally denoted as Smart Objects (SOs), cooperating to collect data and provide services to users. SOs are extremely heterogeneous and differ in term of connectivity interfaces, battery, processing and memory capabilities, as well as for dimensions, costs, and hardware features. Research is going beyond hardware and protocol barriers, providing several solutions for building IoT networks and opening a new challenge: the definition of effective paradigms and mechanisms aimed at integrating the IoT in common people's life.

The above challenges are very complex from a communication perspective, as they involve all layers of the protocol stack. A few illustrative issues to deal with are the following: (i) selection of SOs connectivity; (ii) mechanisms for automatic endpoints discovery; (iii) resource representation; (iv) final users application design; and (v) modeling the interaction between SOs and people [1]. Moreover, the growing interest of companies, research centers, and governments on IoT technologies and devices has led to the new Web of Things (WoT) paradigm [2], [3], where all physical things are accessible and manageable through Web technologies, integrating objects to the Internet and enabling new forms of interaction between devices (Machine-to-Machine, M2M) [4] and between humans and things (Human-to-Machine, H2M), as shown in several WoT-oriented IoT testbeds recently deployed [5], [6].

Regardless of the specific application scenario, the dominant communication technologies in IoT systems are wireless [7], for both SO-to-SO communications and user access. Referring to the available wireless communication solutions for the IoT, it is possible to classify the existing solutions into two main categories:

- Micro IoT, which provides services in personal areas;
- Macro IoT, which provides services in wide areas, such as a user's district or a metropolitan area.

Micro IoT relies on devices with short-range communication capabilities,[1] such as IEEE 802.15.4 [8], IEEE 802.11 [9], [10], Bluetooth Low Energy (BLE) [11], and Radio Frequency Identification (RFID) [12]. Moreover, Micro IoT SOs are generally constrained devices, with strict limitations in terms of battery consumption and processing capabilities. In the presence of large-scale coverage requirements, constrained devices have to be organized in hierarchical multi-hop networks with dynamic topologies. This highly complicates system design and reduces its robustness.

The emerging scenario of Smart Cities has then encouraged researchers to investigate a new type of IoT applications, here denoted as Macro IoT, where the coverage of wide areas, without relying on multi-hop connections, is required. Macro IoT radio technologies are characterized by transmission ranges on the order of hundreds of meters/kilometers. Considering this Smart City perspective, Micro IoT technologies are not the most attractive solution. Cellular networking (with 3G/4G and the upcoming 5G standards) is an attractive option to provide connectivity to all SOs deployed in urban areas [13]. Moreover, focusing on the specific IoT requirements, the 3GPP has recently completed the standardization of the Narrowband-IoT (NB-IoT), a new LTE-based narrowband technology optimized for IoT [14]. Another possibility relies on the adoption of the

L. Davoli, L. Belli, A. Cilfone and G. Ferrari are with the Internet of Things (IoT) Lab, Department of Engineering and Architecture, University of Parma, 43214 Parma, Italy (e-mail: luca.davoli@unipr.it, laura.belli@unipr.it, antonio.cilfone@unipr.it, gianluigi.ferrari@unipr.it). L. Davoli, L. Belli and G. Ferrari are also with things2i s.r.l., a spin-off company of the University of Parma, 43124 Parma, Italy.

[1]To be more precise, IEEE 802.11 could be considered as a short/medium-range radio communication technology, whereas RFID is a very short-range communication technology. For the sake of simplicity, in this paper we refer to *short-range* radio technologies in the presence of a transmission range within 100 m.

Low-Power Wide Area Network (LPWAN) paradigm, which is based on the use of Sub-GHz frequency bands, trading low data rate for long-range connectivity, spanning from hundreds of meters to tens of kilometers. In [15], the authors comprehensively discuss the advantages of the LPWAN paradigm for long-range IoT Smart Cities applications, in terms of effectiveness, efficiency, and architectural design.

In this paper, we propose a new hybrid architecture aiming at combining the benefits of both Micro and Macro IoT paradigms. More specifically, low-power and long-range devices (i.e., Sub-GHz devices) act as collectors (e.g., gateways) for short-range Micro IoT networks, extending the potentialities of Micro IoT "islands," and creating a highly scalable IoT architecture which allows to better address the complexity of the requirements of WoT scenarios.

The remainder of this paper is organized as follows. In Section II, an overview on the radio technologies here considered for Micro and Macro IoT scenarios is presented. In Section III, the components of the Micro/Macro integrated IoT architecture are described. Section IV presents illustrative IoT use cases, considering different possible off-the-shelf implementations and experimentally investigating their performance. Finally, in Section VI we draw our conclusions.

II. Related works

Considering the *Micro IoT* context, the most representative short-range communication devices can be summarized as follows.

- IEEE 802.15.4 devices, adopting IPv6 addresses in application scenarios where the number of network nodes tends to increase, such as extensive industrial monitoring (i.e., Industrial IoT [16]). For this reason, they need an adaptation layer (e.g., the compression layer IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) [17]) to be able to communicate (using IP) with small packet sizes, low-power consumption, and other optimizations required by the limited capabilities of these SOs [18].
- BLE devices, using the low-power version of the Bluetooth protocol, are one of the latest entries in the IoT arena, being generally deployed in personal area applications (i.e., for proximity sensing or beaconing) [11]. A significant advantage of these devices is that they can directly communicate with the majority of smartphones, which have an integrated Bluetooth interface.
- IEEE 802.11 devices, forming Wireless Local Area Networks (WLANs), are widely used in several IoT testbeds for their easy integration with existing infrastructures and built-in IP network compatibility [19].

These short-range devices are generally organized in subnetworks with different topologies (i.e., star, tree-based, ring, mesh, etc.). Because of their resource constraints, they typically need to be connected to the rest of the IoT world through a more powerful node which acts as a gateway, providing high level functionalities such as: data aggregation, automatic service discovery, and resource discovery.

Considering the *Macro IoT* paradigm, there are two main classes of approaches. The first one relies on the use of cellular networks (e.g., 3G/4G and upcoming 5G), which will likely play a fundamental role in new IoT systems, being able to provide ubiquitous connectivity in wide areas and allowing direct use of smartphones. However, pushing cellular connectivity into SOs presents several limitations, related to the enormous number of IoT SOs that could be simultaneously connected to a single cellular base station, thus compromising the overall system performance. Another cellular network-based approach is represented by the "capillary networks" paradigm [20], [21], in which constrained devices composing local—or capillary—networks are connected using short-range radio access technologies to a more powerful component, denoted as Capillary Gateway. This component connects local networks to the global communication infrastructure through a wide-area cellular network, transporting data to an IoT Cloud service, which, in turn, aggregates collected data and manages devices and gateways. The Cloud often acts as the collection environment for heterogeneous IoT applications and, because of this, vendors and providers have now developed several platforms to manage and build applications for the IoT data flow. Some examples are the Cisco Jasper management platform [22] and the IBM Watson IoT platform [23].

The second Macro IoT solution is represented by LPWANs, which rely on Sub-GHz communication bands and guarantee long-range communication [24]. LPWANs represent an alternative to collect data coming from SOs in scenarios where a reliable cellular coverage is missing (e.g., rural areas) or when a connection to the Internet/Cloud infrastructure is not required (e.g., over-dimensioned). Sub-GHz devices guarantee extended coverage: from hundreds of meters to a few kilometers in urban areas, up to tens of kilometers in open space. They can be organized in networks with star topologies, avoiding multi-hop communications. The drawback of this Macro IoT solution is the low data rate, with respect to Micro IoT. Available communication technologies in LPWANs are the following.

- DigiMesh: this LPWAN communication technology relies on a proprietary routing protocol (developed by Digi) that automatically creates a mesh network among all nodes, allowing them to be addressed in an easy and straightforward way [25]. DigiMesh-enabled nodes can act as forwarders as well as endpoints, thus allowing both point-to-point and multi-hop communications from source to destination.
- LoRa: this LPWAN communication technology has been designed and patented by Semtech Corporation [26]. While the PHY layer of LoRa is proprietary, the rest of the protocol stack, denoted as LoRaWAN, is kept open [27]. LoRa-based networks typically have a star-of-stars topology, where the endpoints are connected via a single-hop link to one or more gateways which, in turn, are connected to a common sink, denoted as NetServer, via standard IP. LoRa gateways forward messages between endpoints and the central NetServer. Unlike cellular systems, LoRa endpoints are not required to be associated with a gateway to get access to the network, but only to the NetServer. Thus, gateways act only as bridges and simply forward to their associated NetServer

all successfully decoded messages sent by any endpoint, after adding some information regarding the quality of the reception.

- SIGFOX: this is one of the first LPWAN technology proposed for IoT scenarios [28]. SIGFOX stack protocol specifications are proprietary and unavailable (there is no publicly available documentation), but SIGFOX-enabled gateways are claimed to be able to handle up to a million connected objects, with a coverage range of 30÷50 km in rural areas and 3÷10 km in urban areas.

In order to preserve energy and to guarantee long-range communications, SIGFOX devices have some limitations, namely: the maximum message size is 96 bits and the maximum number of transmitted messages per day per SO is 140. This limitation is also due to the European regulation governing the 868 MHz band, which imposes a transmission duty cycle not higher than 1%. On the other hand, the flaw of the LoRaWAN architecture is that it requires the presence of two distinct entities (the LoRa gateway and the server) that need to be separated and to cooperate through a backhaul. These components can be redundant, as in many IoT scenarios it is possible to define architectures in which the functionalities of the LoRaWAN gateway and NetServer components are centralized and handled by a single entity. As described in [29], although a single LoRaWAN NetServer can potentially serve millions of devices sending a few bytes of data per day per SO, the system scalability is limited. In fact, most of devices, especially those with higher upload traffic needs, should be located in the proximity of the server. Another limitation is related to the fact that, in dense networks, the NetServer cannot acknowledge each message received by any device.

III. Micro and Macro IoT Integration

In order to combine the benefits of both short- and long-range communications for IoT applications, in this work an integration between Micro and Macro IoT technologies is proposed. In Fig. 1, a graphical mapping over a data rate/-transmission range plane, of possible Micro and Macro IoT technologies is shown. To the best of our knowledge, in the literature there is no work related to the integration of these worlds.

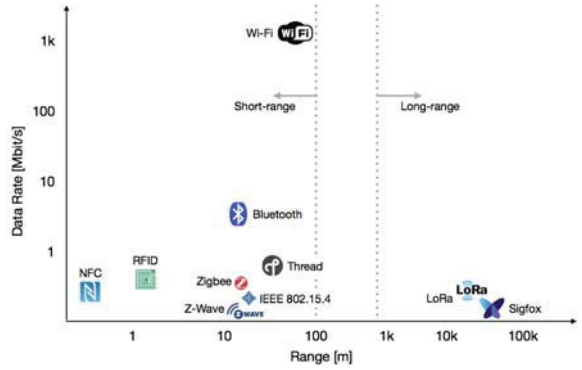


Fig. 1: Possible Micro and Macro IoT radio technologies.

In our proposed architecture, as shown in Fig. 2, Micro IoT "islands" are composed of short-range devices, typically constrained in terms of processing capabilities and energy resources. As shown in Fig. 1, Micro IoT radio technologies (short-range) are heterogeneous in terms of data rate and power consumption. For instance, some technologies have low data rate (e.g., IEEE 802.15.4), whereas others have high data rate (e.g., IEEE 802.11). Micro IoT SOs typically collect information on the environment in which they are deployed and, in order to limit on-board processing (thus saving energy), forward the acquired data to a dedicated device, denoted as μHub, placed at the border of the corresponding Micro IoT region.

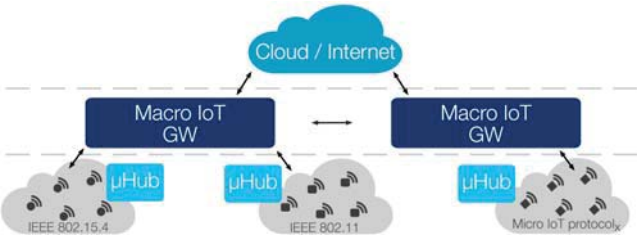


Fig. 2: The proposed integrated architecture, in which different Micro IoT subnetworks (e.g., based on IEEE 802.11 and IEEE 802.15.4) connect, through their local Micro IoT μHubs, to a Macro IoT gateway.

This latter device, which acts as a Micro IoT collector (e.g., a border router), aims at collecting data coming from all components in its subnetwork, following the principles of the emerging Fog Computing paradigm [30]. Periodically, the collector forwards aggregated (and, if needed, compressed) data to other high performance remote processors (denoted as *Macro IoT gateways*), placed far from Micro IoT regions.

The considered Micro IoT collectors work at the application layer and are in charge of collecting data from different types of devices (similarly to what is done by an application gateway) and further forwarding them (e.g., to the Cloud). As anticipated above, these Micro IoT collectors are also denoted as μHubs (as a hub is typically a gateway for heterogeneous data). Their presence allows to completely decouple the local behavior of Micro IoT subnetworks from the behavior of the remote Macro IoT gateways, making the overall architecture dynamic and scalable. In fact, if a particular application requires the deployment of a new Micro IoT subnetwork (i.e., to collect a new type of data with a different short-range IoT technology), the local Micro IoT collector only has to publish its presence through service discovery mechanisms. Thanks to this new communication paradigm—which does not require any additional PUSH-like or POST-like operations from local gateways—the Macro IoT gateway will be automatically notified when a μHub appears with an associated new Micro IoT "island" and will simply start managing new incoming data.

As previously stated, the μHub is typically more powerful than the SOs of its Micro IoT island, as it can locally collect data and preliminary process them. Even though, in principle, in some cases the μHub would not need to share its collected data with other processing units (namely, Macro IoT gateways

or the Cloud), there can be data processing operations that cannot be done locally by each single μHub, but need to be performed by Macro IoT gateways—this is the case, for example, of operations to be carried out on data collected over a large geographic area. The proposed architecture, with intermediate μHubs and centralized Macro IoT gateways, is very flexible and supports this operational mode. More precisely, it can be interpreted as a "multi-layer" architecture, where information flowing from Micro IoT regions can be locally processed (fully or partially) at μHubs and/or combined at centralized Macro IoT gateways. This allows to provide final users with heterogeneous and rich services. For example, there could be need to collect environmental data without compressing them: this could hinder the feasibility of local processing at μHubs (for storage constraints), thus forcing forwarding towards Marco IoT gateways. On the other hand, there could be the need for a fast local feedback on Micro IoT regions (e.g., for real-time machine control), according to a Fog paradigm: in this case, data have to be processed locally at μHubs to avoid networking delays.

A. Wi-Fi and IEEE 802.15.4 Subnetworks

As previously mentioned, according to our vision, short-range Micro IoT subnetworks fit heterogeneous application scenarios, such as: smart parking, smart lighting, environmental monitoring, proximity detection, and so on. An example of a Micro IoT region, as shown in Fig. 2, is given by an IEEE 802.15.4 subnetwork, composed by a multitude of constrained devices—battery-powered, duty-cycled and with short-range connectivity. These SOs continuously collect environmental data through their on-board sensors and, because of their constraints, sensed data are not locally processed but are forwarded to the nearest Macro IoT gateway.

Another example of Micro IoT network, as shown in Fig. 2, is given by an IEEE 802.11 subnetwork. As in the IEEE 802.15.4 case, the Wi-Fi devices (e.g., smartphones, tablets, etc.) are generally battery-powered and able to collect data from their on-board sensors. IEEE 802.11 devices then send collected data to Cloud/Fog processors through the Wi-Fi Access Point (AP) which they are connected to, with a data rate higher than that of IEEE 802.15.4 devices.

According to an IoT-oriented perspective, both IEEE 802.15.4-based and IEEE 802.11-based subnetworks and, in particular, their μHubs, should integrate proper self-configuration mechanisms, with the aim to minimize human intervention, in terms of network deployment and proper service advertisement [31]. On the other hand, μHubs should also provide IoT-defined mechanisms at the application level such as, for example, the Resource Directory (RD) module defined in the Constrained Application Protocol (CoAP) [32]. CoAP is a REST-based web transfer protocol tailored to constrained (battery-power- and processing power-limited) IoT devices. CoAP can be interpreted as a light version of HTTP. More precisely, it includes several HTTP functionalities, but has been redesigned (and not simply directly derived from HTTP) to suit constrained devices. In fact, it runs on top of UDP/IP (i.e., each CoAP message fits into the payload of a UDP datagram). Overall, CoAP is very flexible and can be used with both IPv6 and IPv4 (as layer three protocols). In the case of IPv6 adoption, in IEEE 802.15.4 devices CoAP is directly applicable on top of the 6LoWPAN protocol suite. If IPv4 is adopted, then CoAP can be applied on top of various protocol stacks (including IEEE 802.11).

B. The Micro IoT μHub Module

As already highlighted, the key needs for efficient data dissemination in IoT scenarios are: (i) the need to connect and integrate different technologies, in order to switch from Micro IoT environments (IEEE 802.15.4/IEEE 802.11) to Macro IoT ones (Sub-GHz); and (ii) the need for SOs with enriched network capabilities and able to act as "bridges" between Micro and Macro IoT environments (as shown in Fig. 2). Each bridge, i.e., a μHub, has to support protocols suitable for Micro IoT devices (e.g., CoAP) and, eventually, can also support more complex protocols (such as HTTP) in order to be compliant with WoT principles. Moreover, each μHub has to: (i) act as a local gateway, collecting data coming from devices in its controlled subnetwork and possibly making these data available if queried by external clients; and (ii) actively forward its temporary stored data to a more powerful (remote) data sink. More precisely, the μHub acting on the frontier of an IEEE 802.15.4 subnetwork needs to be equipped with a (short-range) IEEE 802.15.4 interface, to receive data from its subnetwork, and with a (long-range) Sub-GHz interface, which allows the transmission of aggregated data to a remote location. Instead, the μHub acting on the border of an IEEE 802.11 subnetwork needs to primarily act as a Wi-Fi AP for the nodes composing its subnetwork. Moreover, this μHub should be able to collect sensed data coming from the devices in its subnetwork.

C. The Macro IoT Gateway

Trying to keep Micro IoT subnetworks as simple as possible, data processing should be moved outside them. Therefore, "frontier" μHubs need to forward their aggregated data to a high layer sink, able to process them, as well as to possibly outsource (part of) this processing to other high performance infrastructures [33], [34].

An example of high layer concentrator is represented by the proposed Macro IoT gateway, which is RESTful [35] and runs a Java CoAP server as a front-end application interface on which external clients can address CoAP requests. Moreover, the Macro IoT gateway manages a simple RD (namely, a sort of "white pages" of the resources available in the network), maintaining a list of the supervised μHubs and their CoAP resources that can be queried through CoAP requests. The RD can be thus queried on its CoAP resource *well-known/core* by an external client, obtaining the list of available μHubs and their resources. The core of the Macro IoT gateway has been defined in such a way that, as shown in Fig. 3, when an external client sends a CoAP REQuest (CREQ) addressing a known μHub (step 1), the Macro IoT gateway encapsulates the CoAP REQuest's Payload (CREQ-P) in a Sub-GHz REQuest

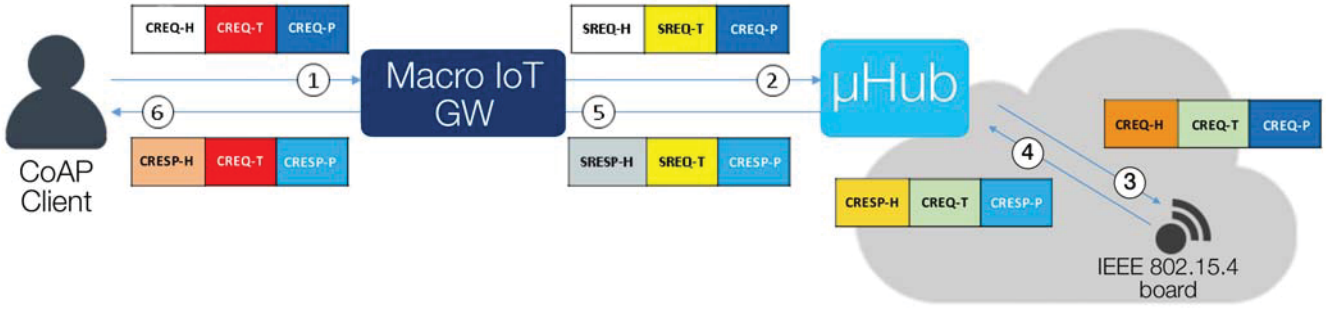


Fig. 3: Messages exchange triggered by a CoAP request (CREQ) sent by an external CoAP client, and targeting a CoAP resource maintained by a short-range IEEE 802.15.4-based board. Each CoAP packet is composed of an Header (CREQ-H/CRESP-H), a Token (CREQ-T/CRESP-T), and a Payload (CREQ-P/CRESP-T), as well as each Sub-GHz packet is composed of an Header (SREQ-H/SRESP-H), a Token (SREQ-T), and a Payload, which always corresponds to the CoAP Payload.

(SREQ) and then forwards it to the targeted μHub (step 2) through a long-range communication.

When the μHub receives the SREQ, it extracts the CoAP REQuest's Payload (CREQ-P) and uses this as if it had come directly to the μHub, maintaining all the properties and attributes provided by the requesting client. Then, the μHub sends a new CoAP request (with the received payload) acting on the proper CoAP resource (step 3) and, when a CoAP RESPonse is obtained (CRESP, shown in step 4), it encapsulates the obtained CoAP RESPonse's Payload (CRESP-P) in another Sub-GHz packet (Sub-GHz RESPonse, SRESP) that, because of its structure, exactly matches the previous self-defined request (through the Sub-GHz REQuest token field SREQ-T, inserted to maintain a perfectly matching request/response, if required by the CoAP attributes of the original request). Finally, the Sub-GHz packet will be sent back to the Macro IoT gateway (step 5), which extracts the CRESP-P and, using the original CoAP request object (through the CREQ-T field), sends the CRESP to the client (step 6), in a totally transparent way. In fact, all external entities, sending CoAP requests to the IoT system, are unaware of the existence of this backbone encapsulation and the architecture still remains dynamic, flexible and scalable.

In Fig. 4, the protocol stacks used in Sub-GHz Macro IoT devices (left) and in IEEE 802.11 and IEEE 802.15.4 Micro IoT devices (right) are shown. It can be observed that the considered Sub-GHz devices are characterized by proprietary protocols for network, transport, and application layers. At the opposite, being based on public standards at low layers (IEEE 802.11 and IEEE 802.15.4), Micro IoT devices share the same protocols at the application and transport layers. However, at the lower layers they adopt different protocols: for IEEE 802.11-based devices, PHY and MAC layers are proper of the standard itself [9], with the adoption of IPv4 at network layer; for IEEE 802.15.4-based devices, we adopt IPv6 at the network layer, on top of 6LoWPAN, which, in turn, acts as an intermediate "compression" layer for lower IEEE 802.15.4 layers [8].

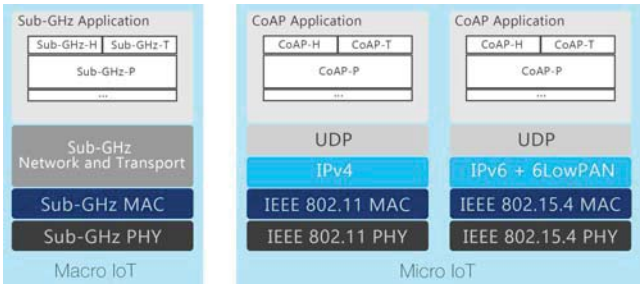


Fig. 4: Considered protocol stacks for Macro (Sub-GHz) and Micro (IEEE 802.11 and IEEE 802.15.4) IoT devices.

D. End-to-End Security among IoT nodes

One of the key aspects of an IoT architecture like the one shown in Fig. 3 is the security required by its different actors. In particular, one needs to address the aspects of authorization and authentication to access data provided by different Micro IoT regions (e.g., for privacy purposes). A possible approach can rely on an IETF initiative specifically addressing authorization in IoT, namely Authentication and Authorization in Constrained Environments (ACE) [36], in which ideas and principles of OAuth are re-used. Other end-to-end solutions that try to guarantee confidentiality of the information exchanged between sensors/actuators and external clients without having to put trust in services are represented by OSCAR [37] and object security [38]. The latter approach refers to a self-contained information container with protected content which does not need be associated with a specific session and consists of a header, a payload (potentially encrypted), and an integrity verification tag. Furthermore, it allows caching services and serving multiple clients with the same object, also adopting different data representations (e.g., Javascript Object Signing and Encryption (JOSE) [39], JSON Web Token (JWT) [40], IoT-OAS [41]).

IV. A Low Cost Hardware Implementation

The architecture proposed for the integration between Micro and Macro IoT technologies can be adapted to several practical situations. As a relevant example, we propose an IoT monitoring architecture that can be deployed in medium/large areas,

such as a university campus. The services built and provided to users through this deployment include traffic control, environmental monitoring and sensing. Moreover, IEEE 802.11-based networks can be adopted to deploy an indoor monitoring system, e.g., a Wi-Fi-based surveillance system, that controls the main entry points of the buildings in the university campus.

A. Vehicle Traffic Control Scenario

In our IoT-oriented vehicle traffic control scenario, as shown in Fig. 5, in order to detect transiting cars, each lane in the main road is controlled by a set of SOs equipped with proximity/vibration sensors and with an IEEE 802.15.4 radio interface. In the same way, both bicycle lanes and the pedestrian sidewalk can be monitored through different SOs. Specific SOs are in charge of turning street lighting on at sunset. Adhering to the proposed hybrid Micro/Macro IoT approach, the events produced by each of these constrained nodes need to be sent to the proper μHub, which collects data coming from all components of its subnetwork. The μHub is also equipped with a camera module, in order to periodically take a picture of the road section, send it to a remote user (in our case, the Macro IoT gateway) which can check the current traffic conditions and choose the proper route (due to aggregated data sent by μHubs, e.g., cars and trucks counter).

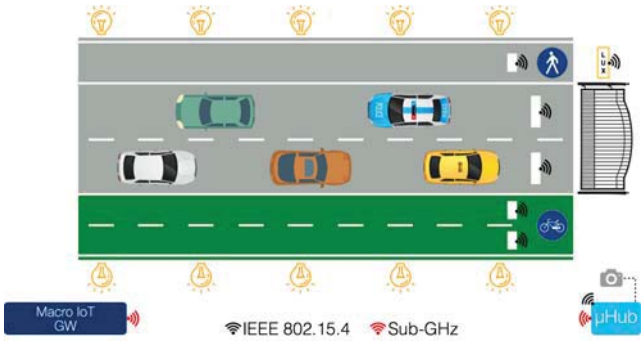


Fig. 5: Vehicle traffic control scenario deployment.

As shown in Fig. 6, the local IEEE 802.15.4 μHub is composed by a Raspberry Pi 3 Model B (Fig. 6.a) with a camera module and two network interfaces: a XBee Sub-GHz radio module (Fig. 6.b), needed to send the aggregated data to the Macro IoT gateway, and an IEEE 802.15.4 dongle. In our implementation, we select the Memsic TelosB mote (shown in Fig. 6.c)—a possible alternative is represented by the OpenLabs 802.15.4 radio module, shown in Fig. 6.d, which can be directly attached to the Raspberry Pi. The IEEE 802.15.4 interface enables the μHub module to receive information from the constrained SOs (in our implementation, Zolertia Z1 boards, as shown in Fig. 6.e), each sensing a street lane.

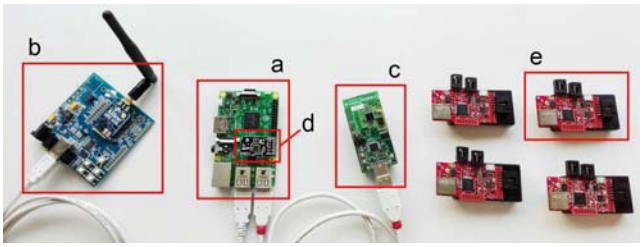


Fig. 6: Traffic Monitoring Micro IoT system. The μHub is composed by (a) a Raspberry Pi 3 Model B, (b) a XBee Sub-GHz dongle, (c) an IEEE 802.15.4 Telos B dongle or, as a possible alternative, by (d) an OpenLabs 802.15.4 radio module. In the same figure, (e) a few constrained nodes (Zolertia Z1 with IEEE 802.15.4 radio interface), to be positioned on the lanes of the road, are shown.

Moreover, an important role is played by the gateway, composed by a Raspberry Pi 3 Model B, equipped with a XBee Sub-GHz module. The task of the gateway is to forward data and images to the data collector, according to a static and pre-configured routing table.

B. Smart Sensing and Monitoring Scenario

In this scenario, instead, each building of the university campus is supposed to be monitored, in order to maintain a high security level and to guarantee personnel (i.e., teachers, students, administrative staff, etc.) to work in a secure and protected environment. In order to do this, the following operational assumptions are reasonable:

- windows need to be obscured in the presence of direct sunlight and external high temperature;
- firefighters should intervene in case of fire detection;
- doors need to be surveilled to detect unauthorized intrusions.

For this application, the vigilance team might install a presence sensor on each door, jointly with a security camera (e.g., an IP camera) that takes a snapshot of the intruder if the presence sensor detects an unexpected movement [42]. In this case, the sensor-equipped module and the IP camera are both connected to the same Wi-Fi AP, which corresponds to a Wi-Fi μHub. As shown in Fig. 7, when an unauthorized intrusion is detected, the movement sensor-equipped device notifies the μHub about the intrusion (step 1). The μHub then simultaneously performs the following operations: (i) it sends a message notification to the vigilance team and to the user of the "burglarized" office (step 2a); (ii) it commands the IP camera to take a snapshot and, once the picture is received (step 2b), it sends it to the vigilance team and to the user of the "burglarized" office (step 2c) (in this way, the data rate of the Sub-GHz communication can support the forwarding of the picture without introducing long delays); and (iii) it starts to locally store the video streaming captured by the IP camera and transmitted through the Wi-Fi connection to the Wi-Fi μHub (step 3). Later, when the user arrives to the "burglarized" office with the vigilance team, after having already received a first picture of the intrusion, he/she can view the complete video stream locally stored into the μHub. With this approach,

according to the infrastructure and to the Sub-GHz data rate constraints, there is no need to transmit the captured stream between the Sub-GHz devices.

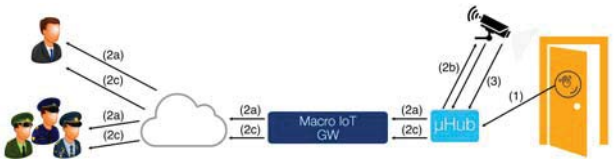


Fig. 7: Smart surveillance scenario.

As can be seen in Fig. 8, the deployed local IEEE 802.11 μHub is composed by a UDOO device [43] (Fig. 8.a) already providing an on-board Wi-Fi radio (Fig. 8.b), and further equipped with a XBee Sub-GHz radio dongle (Fig. 8.c) needed to forward data sensed by on-board accelerometers of the IEEE 802.11-based TI SimpleLink Wi-Fi CC3200 boards [44] (Fig. 8.d), which correspond to the surveillance devices, to the Macro IoT gateway.

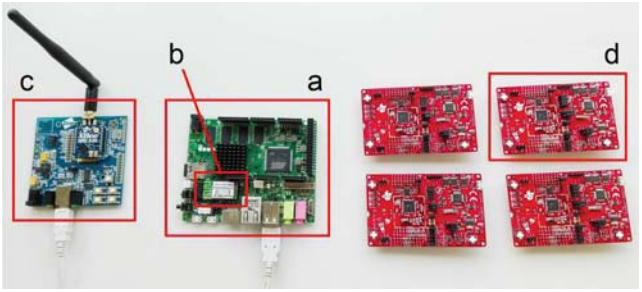


Fig. 8: Smart surveillance μHub composed by (a) a UDOO board with (b) integrated Wi-Fi radio, (c) a XBee Sub-GHz dongle. In the same figure, (d) a few IEEE 802.11-based boards, representing the nodes that made environmental sensing and alerting into the university's buildings, are shown.

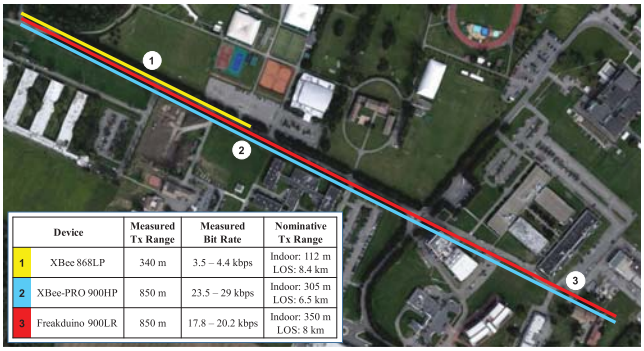
In both the described use-cases, the Macro IoT gateway is assumed to be, as mentioned before, a high performance board. More precisely, one can use a PC equipped with an XBee Sub-GHz board to receive aggregated data coming from all μHubs.

Table I shows in detail the SOs employed to implement the described use-cases, with the corresponding per-item costs. The number of used devices (denoted as either x or y) depends on the scale of the Micro/Macro IoT scenario at hand. Moreover, in Table I the costs required to deploy an IEEE 802.15.4-based Micro IoT region (μHub + constrained IEEE 802.15.4 nodes) and an IEEE 802.11-based Micro IoT region (μHub + constrained Wi-Fi nodes) are also detailed.

V. Experimental Performance Evaluation at the University of Parma Campus

Since Micro IoT scenarios have been thoroughly investigated in the literature [45], [46], in this work we focus on the evaluation of Macro IoT systems and technologies. As shown in Table I, various Sub-GHz boards are available, characterized by different features and costs. Among many options, we selected the following three boards: (i) the Digi XBee 868LP, (ii) the XBee-PRO 900HP, and (iii) the Freakduino 900LR. In order to make a comprehensive performance analysis of these boards, we conducted experimental tests and measurements in the campus of the University of Parma. This particular location cannot be strictly considered as an urban area, as buildings are quite distant from each other and there are several free space areas with trees and no relevant obstacles.

In order to plan the deployment of Macro IoT systems, the first step is to determine the maximum transmission distance that can be reached by a Sub-GHz board. In Fig. 9 the map of the considered portion of the university campus is shown, together with the corresponding obtained maximum measured transmission ranges (together with measured data rates) for the considered Sub-GHz devices.



	Device	Measured Tx Range	Measured Bit Rate	Nominative Tx Range
1	XBee 868LP	340 m	3.5 – 4.4 kbps	Indoor: 112 m LOS: 8.4 km
2	XBee-PRO 900HP	850 m	23.5 – 29 kbps	Indoor: 305 m LOS: 6.5 km
3	Freakduino 900LR	850 m	17.8 – 20.2 kbps	Indoor: 350 m LOS: 8 km

Fig. 9: Transmission ranges and data rates obtained with the selected Sub-GHz boards in the campus of the University of Parma.

In Table II, we extend the results of Fig. 9, showing, for each Sub-GHz device, the measured distance for each allowed value of transmission power. All the measurements have been obtained sending a known sequence of bits a sufficiently large (from a statistical point of view) number of times. The maximum distances are determined in correspondence to a packet delivery ratio (PDR) equal to 90%.

TABLE II: Maximum transmission range, for each Sub-GHz board, as a function of the transmission power.

	Power		
Device	14 dBm	24 dBm	27 dBm
XBee 868LP	340 m	—	—
XBee-PRO 900HP	405 m	850 m	—
Freakduino 900LR	395 m	700 m	850 m

In our tests, the boards were configured using the available transmission power levels. More precisely, the considered power levels are the following: 14 dBm, which is a power level available for all boards (in particular, it is the highest level for the XBee 868LP); 24 dBm, which is allowed by the XBee-PRO 900HP and Freakduino 900LR; and, finally, 27 dBm, which is supported only by the Freakduino 900LR. The overall settings of each Sub-GHz node can be summarized as follows.

- XBee 868LP:

TABLE I: Smart Objects deployed in the use-case implementation.

	Device	Micro/Macro	Data rate [bps]	Coverage	No.	Per item cost
A	Zolertia Z1	Micro (IEEE 802.15.4)	250k	Indoor: 25 m Outdoor/LOS: 60 m	x	$69.95
B	TI CC3200 LaunchPad	Macro (IEEE 802.11)	16M	Indoor: 40 m Outdoor/LOS: 90 m	y	$29.99
C	Raspberry Pi 3	Micro/Macro	12M	Indoor: 10 m	1	$27.99
D	UDOO	Micro/Macro	—	—	1	$115.00
S_1	XBee 868LP		10-80k	Indoor: 14-112 m$^{\alpha}$ Outdoor/LOS: 0.64-8.4 km$^{\alpha}$		$61.20
S_2	XBee-PRO 900HP	Micro/Macro	10-200k$^{\beta}$	Indoor: 305-610 m Outdoor/LOS: 6.5-14 km	1 + 1	$97.67
S_3	Freakduino 900LR		40-250k	Indoor: 350 m Outdoor/LOS: 8 km		$39.00
I_1	TelosB	Micro (IEEE 802.15.4)	250k	Indoor: 30 m Outdoor/LOS: 100 m	1	$87.10
I_2	OpenLabs 802.15.4 radio	Micro (IEEE 802.15.4)	250k	Indoor: 25 m Outdoor/LOS: 90 m	1	$12.00

LOS: Line-of-Sight. $^{\alpha}$Depending on RF antenna type. $^{\beta}$Depending on firmware type.

Cost of an IEEE 802.15.4-based Micro IoT region (μHub + constrained IEEE 802.15.4 nodes):

$$cost_C + cost_I + cost_S + cost_A \cdot x = \begin{cases} cost_C + cost_{I_2} + cost_{S_3} + cost_A \cdot x = \$78.99 + \$69.95 \cdot x & \text{Min} \\ cost_C + cost_{I_1} + cost_{S_2} + cost_A \cdot x = \$182.76 + \$69.95 \cdot x & \text{Max} \end{cases}$$

Cost of an IEEE 802.11-based Micro IoT region (μHub + constrained Wi-Fi nodes):

$$cost_D + cost_S + cost_B \cdot y = \begin{cases} cost_D + cost_{S_3} + cost_B \cdot y = \$162.00 + \$29.99 \cdot y & \text{Min} \\ cost_D + cost_{S_2} + cost_B \cdot y = \$212.67 + \$29.99 \cdot y & \text{Max} \end{cases}$$

  - transmit power: 14 dBm;
  - antenna gain: 2 dBi;
  - receiver sensitivity: -101 dBm @ 80 kbps;
  - transmitter and receiver height: 1.5 m;
  - central bandwidth frequency: 868 MHz;
  - bandwidth: 150 kHz;
- XBee-PRO 900HP:
  - transmit power: 14 dBm, 24 dBm;
  - antenna gain: 2 dBi;
  - receiver sensitivity: -101 dBm @ 200 kbps;
  - transmitter and receiver height: 1.5 m;
  - central bandwidth frequency: 906 MHz;
  - bandwidth: 150 kHz;
- Freakduino 900LR:
  - transmit power: 14 dBm, 24 dBm, 27 dBm;
  - antenna gain: 2 dBi;
  - receiver sensitivity: -101 dBm @ 20 kbps;
  - transmitter and receiver height: 1.5 m;
  - central bandwidth frequency: 906 MHz;
  - bandwidth: 240 kHz.

After analyzing the performance of different Sub-GHz technologies, we decided to select the XBee-PRO 900HP board, as it guarantees the best trade-off between coverage and data rate. In fact, it allows to achieve the same performance of the Freakduino 900LR, using half of the transmission power.

As second step of our evaluation, we have investigated the performance, in terms of data rate, with multiple communication hops in an outdoor scenario. In Fig. 10, the considered network deployment in the university campus is shown, together with the two multi-hop paths that the packets are forced to follow, in order to reach the data collector from the endpoints. We evaluated the performance of the deployed system, taking into account the data rate measured during the transmission of images. In particular, images with different dimensions have been considered—namely, 15 kB, 170 kB and 900 kB—in order to test the performance in various traffic load conditions.

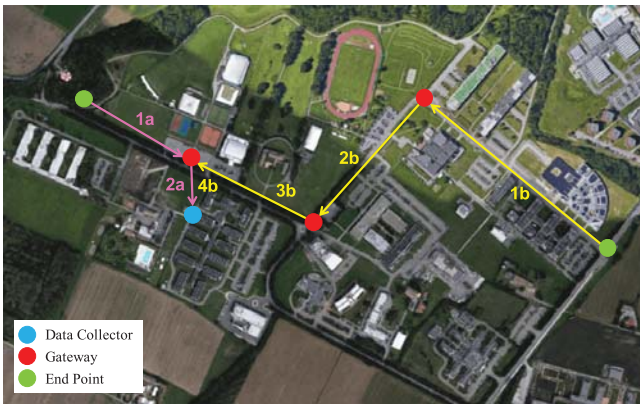


Fig. 10: Setup of multi-hop Sub-GHz communications in the campus of the University of Parma.

In Fig. 11, the experimental (line with stars) results are compared with the theoretical results. The latter results are

obtained by observing that the data rate with n hops can be approximated as R/n, where R is the source data rate (dimension: [bps]). The value R/n can be considered as an upper bound on the data rate, under the assumption that every relay node waits to receive the whole packet stream (associated with an image transmitted by the source) and then forwards it to the next node, rather than forwarding each single incoming packet. We measure the average data rate as a function of the traversed hop. As shown in Fig. 11, the experimental results are close to the theoretical ones. The gap between theory and experiments tends to increase for increasing values of the number of hops.

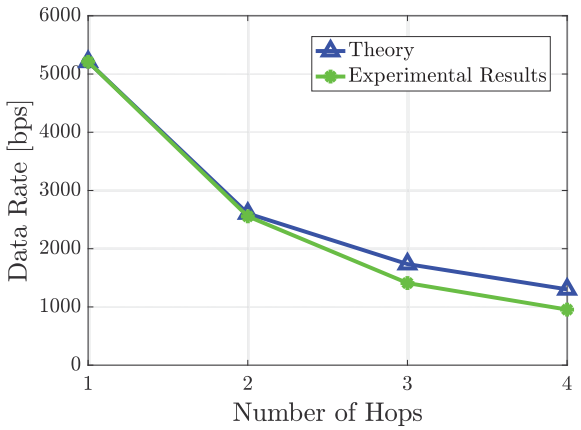


Fig. 11: Measured data rate, as a function of the number of hops, obtained with the selected Sub-GHz boards in the campus of the University of Parma.

As anticipated in Table II, the overall maximum transmission range (850 m) is obtained with two configurations: XBee-PRO 900HP @ 24 dBm and Freakduino 900LR @ 27 dBm. In Fig. 12, it can be observed that, regardless of the used device and transmission power, the PDR remains equal to 100% until the maximum transmission range, in correspondence to which it drops to zero very quickly. Therefore, there is no graceful degradation but, rather, a Sub-GHz link is either perfectly reliable or absent. This also justifies our previous choice of measuring the maximum range in correspondence to a PDR equal to 90%.

VI. Conclusions and Future Works

In this paper, we have introduced a novel approach to combine short-range IoT networks, here denoted as Micro IoT, with more recent long-range LPWANs, here denoted as Macro IoT. The proposed architecture relies on novel components, denoted as μHubs, with double interfaces: one is dedicated to the Micro IoT scenario and uses short-range radio technologies (IEEE 802.15.4 or IEEE 802.11), while the other interface provides long-range (Sub-GHz) connectivity, in order to communicate and deliver data to distant Macro IoT gateways. The proposed architecture, besides being low-cost, is highly scalable and fits with the requirements of typical applications related to Smart Cities scenarios. Two practical

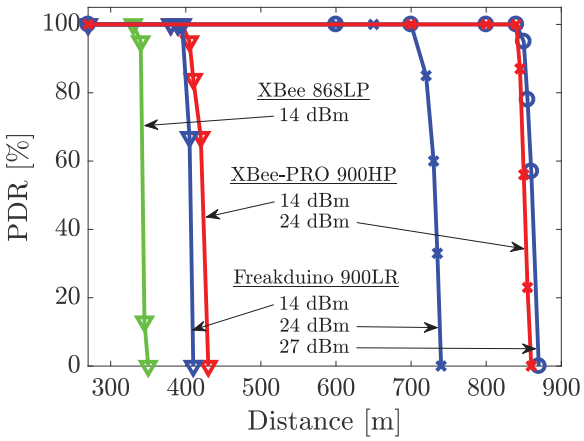


Fig. 12: Experimental PDR, with the selected Sub-GHz boards, as function of the transmission power.

use cases, applicable to a university campus, have been considered and experimental results (for Sub-GHz communications) have been presented. The main drawback of the proposed IoT-oriented architecture is the data rate limitation enforced by Sub-GHz devices. In other words, the Macro IoT portion of the architecture is the bottleneck. This constraint limits the number of possible applications which can be built and the type of data which can be collected (i.e., sensors data and simple images can flow efficiently, whereas video streams cannot be supported). However, this limitation can be mitigated by the μHubs themselves, which can store locally large data, as described in Subsection IV-B.

As a future work, we plan to test the architecture with other Sub-GHz technologies (i.e., with LoRa- or SIGFOX-based devices), also exploring different environmental (propagation) conditions. Another interesting extension consists in building new μHubs able to support other Micro IoT technologies, e.g., BLE. Finally, local storage in the μHubs makes our system interesting also from the point of view of recent theoretical advances in the area of local caching for future efficient device-to-device communications [47], [48].

References

[1] L. Belli, S. Cirani, A. Gorrieri, and M. Picone, "A Novel Smart Object-Driven UI Generation Approach for Mobile Devices in the Internet of Things," in *Proceedings of the 1st International Workshop on Experiences with the Design and Implementation of Smart Objects*, ser. SmartObjects '15, 2015, pp. 1–6.

[2] S. Duquennoy, G. Grimaud, and J. J. Vandewalle, "The Web of Things: Interconnecting Devices with High Usability and Performance," in *2009 International Conference on Embedded Software and Systems*, May 2009, pp. 323–330.

[3] D. Guinard, V. Trifa, F. Mattern, and E. Wilde, *From the Internet of Things to the Web of Things: Resource-oriented Architecture and Best Practices*. Springer Berlin Heidelberg, 2011, pp. 97–129.

[4] S. Cirani, L. Davoli, M. Picone, and L. Veltri, "Performance Evaluation of a SIP-based Constrained Peer-to-Peer Overlay," in *2014 International Conference on High Performance Computing Simulation (HPCS)*, July 2014, pp. 432–435.

[5] S. Mayer, M. Schalch, M. George, and G. Sörös, "Device Recognition for Intuitive Interaction with the Web of Things," in *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication*, ser. UbiComp '13 Adjunct, 2013, pp. 239–242.

[6] L. Belli, S. Cirani, L. Davoli, A. Gorrieri, M. Mancin, M. Picone, and G. Ferrari, "Design and Deployment of an IoT Application-Oriented Testbed," *Computer*, vol. 48, no. 9, pp. 32–40, Sept 2015.

[7] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of Wireless Sensor Networks towards the Internet of Things: A Survey," in *SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks*, Sept 2011, pp. 1–6.

[8] "IEEE Standard for Low-Rate Wireless Networks," *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, pp. 1–709, April 2016.

[9] "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pp. 1–2793, Mar 2012.

[10] "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pp. 1–3534, Dec 2016.

[11] "Bletooth Low Energy." [Online]. Available: https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy

[12] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, April 2012, pp. 1282–1285.

[13] R. Ratasuk, A. Prasad, Z. Li, A. Ghosh, and M. A. Uusitalo, "Recent advancements in M2M communications in 4G networks and evolution towards 5G," in *2015 18th International Conference on Intelligence in Next Generation Networks*, Feb 2015, pp. 52–57.

[14] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," in *Wireless Communications and Networking Conference (WCNC), 2016 IEEE*. IEEE, 2016, pp. 1–5.

[15] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 60–67, October 2016.

[16] "Industrial Internet of Things." [Online]. Available: https://www.accenture.com/us-en/labs-insight-industrial-internet-of-things

[17] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," Internet Requests for Comments, Internet Engineering Task Force, RFC 6282, September 2011.

[18] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," Internet Requests for Comments, Internet Engineering Task Force, RFC 4944, September 2007.

[19] L. Kriara, M. K. Marina, and A. Farshad, "Characterization of 802.11n wireless LAN performance via testbed measurements and statistical analysis," in *2013 IEEE International Conference on Sensing, Communications and Networking (SECON)*, June 2013, pp. 158–166.

[20] J. Sachs, N. Beijar, P. Elmdahl, J. Melen, F. Militano, and P. Salmela, "Capillary networks–a smart way to get things connected," *Ericsson Review, September*, vol. 9, 2014.

[21] O. Novo, N. Beijar, M. Ocak, J. Kjällman, M. Komu, and T. Kauppinen, "Capillary networks-bridging the cellular and IoT worlds," in *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*. IEEE, 2015, pp. 571–578.

[22] "Cisco Jasper Platform." [Online]. Available: https://www.jasper.com/

[23] "IBM Watson IoT Platform." [Online]. Available: https://developer.ibm.com/iotplatform/

[24] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, and M. Pettissalo, "On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology," in *2015 14th International Conference on ITS Telecommunications (ITST)*, Dec 2015, pp. 55–59.

[25] "Wireless Mesh Networking: ZigBee vs. DigiMesh." [Online]. Available: http://www.digi.com/pdf/wp_zigbeevsdigimesh.pdf

[26] "Semtech Corporation." [Online]. Available: http://www.semtech.com/wireless-rf/lora.html

[27] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A Study of LoRa: Long Range & Low Power Networks for the Internet of Things," *Sensors*, vol. 16, no. 9, pp. 1466–1484, 2016.

[28] "Sigfox." [Online]. Available: http://makers.sigfox.com

[29] K. Mikhaylov, J. Petäjäjärvi, and T. Haenninen, "Analysis of capacity and scalability of the LoRa low power wide area network technology," in *European Wireless 2016; 22th European Wireless Conference; Proceedings of*. VDE, 2016, pp. 1–6.

[30] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. ACM, 2012, pp. 13–16.

[31] S. Cirani, L. Davoli, G. Ferrari, R. Leone, P. Medagliani, M. Picone, and L. Veltri, "A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 508–521, Oct 2014.

[32] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," Internet Requests for Comments, Internet Engineering Task Force, RFC 7252, June 2014.

[33] L. Belli, S. Cirani, L. Davoli, L. Melegari, M. Mónton, and M. Picone, *An Open-Source Cloud Architecture for Big Stream IoT Applications*. Springer International Publishing, 2014, pp. 73–88.

[34] L. Belli, S. Cirani, L. Davoli, G. Ferrari, L. Melegari, M. Montón, and M. Picone, "A Scalable Big Stream Cloud Architecture for the Internet of Things," *International Journal of Systems and Service-Oriented Engineering (IJSSOE)*, vol. 5, no. 4, pp. 26–53, Oct 2015.

[35] R. T. Fielding, "Architectural Styles and the Design of Network-based Software Architectures," Ph.D. dissertation, University of California, Irvine, 2000, aAI9980887.

[36] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE)," Internet Engineering Task Force, Internet-Draft draft-ietf-ace-oauth-authz, Mar. 2017, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-ietf-ace-oauth-authz

[37] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "OSCAR: Object security architecture for the Internet of Things," *Ad Hoc Networks*, vol. 32, pp. 3–16, 2015.

[38] J. Mattsson, G. Selander, and G. A. P. Eriksson, "Object Security in Web of Things," in *Proc. of the Workshop on the Web of Things*, Berlin, Germany, June 2014.

[39] R. Barnes, "Use Cases and Requirements for JSON Object Signing and Encryption (JOSE)," Internet Requests for Comments, Internet Engineering Task Force, RFC 7165, April 2014.

[40] M. Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," Internet Requests for Comments, Internet Engineering Task Force, RFC 7519, May 2015.

[41] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios," *IEEE Sensors Journal*, vol. 15, no. 2, pp. 1224–1234, Feb 2015.

[42] L. Davoli, L. Belli, A. Cilfone, and G. Ferrari, "Integration of Wi-Fi mobile nodes in a Web of Things Testbed," {*ICT*} *Express*, vol. 2, no. 3, pp. 96–99, 2016, special Issue on {ICT} Convergence in the Internet of Things (IoT).

[43] "UDOO Board." [Online]. Available: http://www.udoo.org

[44] "SimpleLink Wi-Fi CC3200 SDK." [Online]. Available: http://www.ti.com/tool/cc3200sdk

[45] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella, "Performance study of IEEE 802.15. 4 using measurements and simulations," in *Wireless communications and networking conference, 2006. WCNC 2006. IEEE*, vol. 1. IEEE, 2006, pp. 487–492.

[46] C. P. Kruger and G. P. Hancke, "Benchmarking Internet of Things devices," in *Industrial Informatics (INDIN), 2014 12th IEEE International Conference on*. IEEE, 2014, pp. 611–616.

[47] M. Ji, G. Caire, and A. F. Molisch, "Wireless Device-to-Device Caching Networks: Basic Principles and System Performance," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 1, pp. 176–189, 2016.

[48] ——, "Fundamental Limits of Caching in Wireless D2D Networks," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 849–869, 2016.