

**This item is the archived peer-reviewed author-version of:**

Flexible multimodal Sub-Gigahertz communication for heterogeneous Internet of Things applications

**Reference:**

Famaey Jeroen, Berkvens Rafael, Ergeerts Glenn, De Poorter Eï, Van den Abeele Floris, Bolckmans Tomas, Hoebeke Jeroen, Weyn Maarten.- Flexible multimodal Sub-Gigahertz communication for heterogeneous Internet of Things applications  
IEEE communications magazine / Institute of Electrical and Electronics Engineers [New York, N.Y.] - ISSN 0163-6804 - 56:7(2018), p. 146-153  
Full text (Publisher's DOI): <https://doi.org/10.1109/MCOM.2018.1700655>

# Flexible Multimodal Sub-Gigahertz Communication for Heterogeneous Internet of Things Applications

Jeroen Famaey<sup>1</sup>, Rafael Berkvens<sup>1</sup>, Glenn Ergeerts<sup>1</sup>, Eli De Poorter<sup>2</sup>, Floris Van den Abeele<sup>2</sup>,  
Tomas Bolckmans<sup>2</sup>, Jeroen Hoebeke<sup>2</sup>, and Maarten Weyn<sup>1</sup>

<sup>1</sup> IDLab, University of Antwerp – imec, Antwerp, Belgium

<sup>2</sup> IDLab, Ghent University – imec, Ghent, Belgium

**To realize low-power and low-cost wireless communication over long distances, several wireless standards using sub-1GHz frequencies have recently been proposed, each with their own strengths and weaknesses in terms of coverage, energy consumption and throughput. However, none of them are currently flexible enough to satisfy the requirements of future dynamic and heterogeneous IoT applications. To alleviate this, a novel architecture that uses a multimodal device for flexibly employing a variety of heterogeneous sub-1GHz wireless networks is proposed. It greatly increases the network flexibility, resilience and performance. A device design is presented together with an abstraction layer that combines the different networks into a single flexible virtual network substrate. The article elaborates on the qualitative advantages of this approach. Measurement-based simulation results show advantages in terms of energy efficiency, with significant reduction in energy use compared to a single-technology solution in a representative IoT track and trace scenario. Finally, the article identifies several open research challenges that need to be resolved to fully realize this vision of flexible multimodal communication for demanding IoT applications.**

## I. INTRODUCTION

Low-power and low-cost wireless communication over long distances is central to the Internet of Things (IoT) vision. To meet these requirements, a plethora of new low-power wireless networking standards have been proposed during the last five years. Many recent communication technologies targeting IoT connectivity employ sub-gigahertz (sub-1GHz) frequency bands (e.g., 433 MHz and 868/915 MHz). Sub-1GHz frequency bands allow significantly increased range and penetration, at the cost of reduced bandwidth. This makes them highly suitable for massive long-range low-throughput IoT applications. Despite focusing on long-range and low-power connectivity, these sub-1GHz communication technologies have widely varying characteristics. On the one hand, Low-Power Wide Area (LPWA) network technologies offer a throughput of a few hundred bits per second at a range of tens of kilometers (e.g., LoRa [1] and Sigfox [2]). On the other hand, wireless sensor networks (WSNs) provide throughputs of hundreds of kilobits per second at ranges up to at most a few kilometers (e.g., IEEE 802.15.4g [3], IEEE 802.11ah [4], and DASH7 [5]). More recently, 3GPP has introduced cellular-based IoT communication technologies (e.g., NB-IoT [6]). As they use licensed spectrum, they provide increased reliability and indoor penetration, albeit at a higher deployment and operational cost. This extreme variety and differentiation has

led to significant fragmentation and heterogeneity in the IoT landscape.

Currently, heterogeneous IoT networks exist as independent silos. An IoT device connects to one network, with very specific characteristics that only satisfy the requirements of a subset of applications. However, the limited capabilities of each separate technology are not sufficiently flexible to satisfy the requirements of advanced IoT applications. An application may require long-distance communication at one point, but higher throughput at another. To alleviate this, we argue that the walls that exist between these networks need to be torn down. Multimodal IoT devices that support multiple network technologies can dynamically select which network to connect to, based on their current application requirements, network availability, link quality, and environmental conditions. Through effective coordination and management across networks, such a multimodal approach promises significantly increased flexibility, reliability, and performance.

In this article we present our vision of a flexible multimodal IoT device that can seamlessly switch between the different available heterogeneous networks. An end-to-end network management substrate coordinates operations across these networks. Together, the device and management substrate offer flexible communication, enabling advanced applications.

Figure 1 illustrates the flexibility of the proposed multimodal device and management approach for an industrial track and trace application. Such an application aims to connect a company's physical assets to the Internet in order to track them, collect usage and maintenance data, and control actuators. In the company warehouse, a higher throughput technology (e.g., IEEE 802.15.4g) can be used to provide indoor connectivity and over-the-air software updates. A backup long-range network (e.g., LoRa) can be used to provide site-wide connectivity. Once the assets are loaded onto a truck, they can switch to ad-hoc short range communications for local coordination, and an LPWA network for back-end communication.

In the remainder of this article, we first offer a motivation for multimodal management of heterogeneous sub-1GHz wireless technologies. Subsequently, the architecture of the proposed multimodal IoT device and network manager are presented. The advantages of our solution are highlighted based on evaluation results obtained from a prototype multimodal IoT device. Finally, the open research challenges are identified and conclusions drawn.

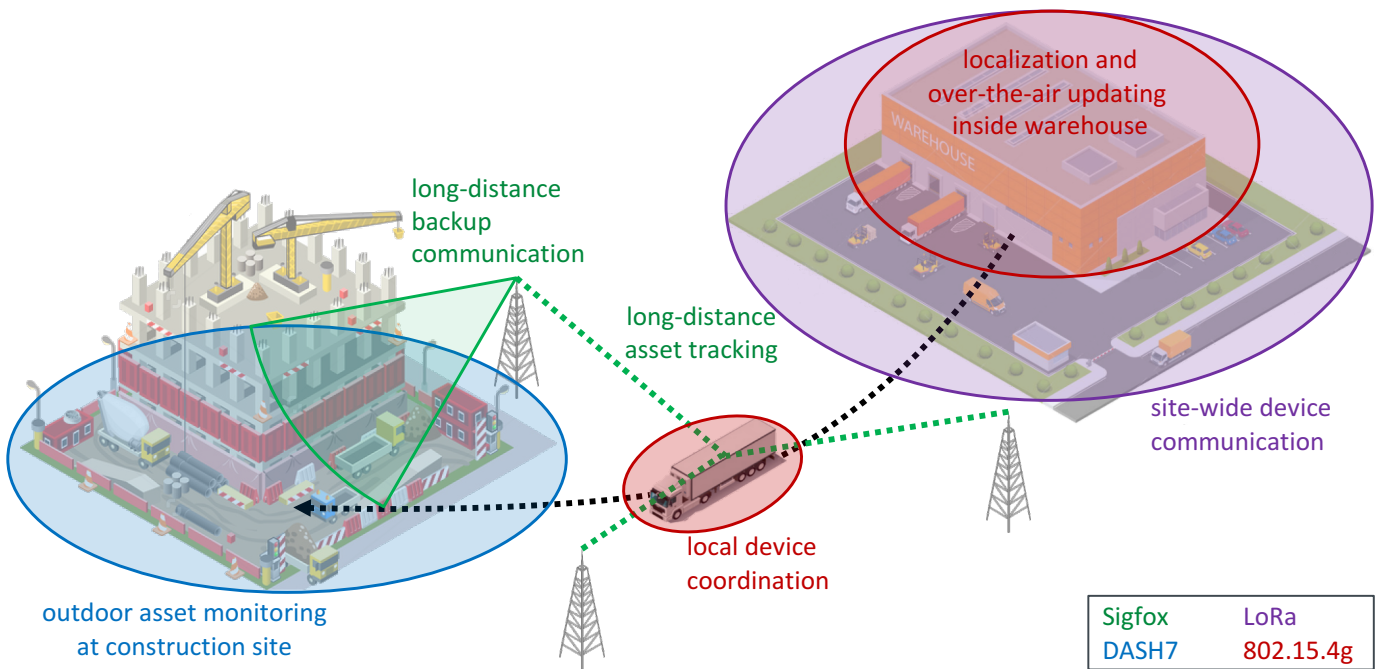


Fig. 1. An industrial track and trace scenario illustrating the flexibility of the proposed multimodal IoT solution. A multimodal track and trace device attached to assets can adapt its choice of communication protocol based on the context and location of the asset, including when it's stored in the warehouse, being transported by a truck, or in use at a construction site.

## II. MULTIMODAL COMMUNICATIONS FOR IOT

The need for a flexible multimodal communications solution for the IoT is clearly demonstrated by the widely varying characteristics of available low-power communications technologies. Table I compares the most popular sub-1GHz wireless technologies for IoT. They share the goal to provide long-range and energy-efficient connectivity to massive IoT applications. However, they provide different trade-offs. LoRa [1] and Sigfox [2] offer the longest range up to tens of kilometers at the cost of significantly lower throughput of only hundreds of bits per second. NB-IoT offers a similar range, but its use of licensed spectrum allows it to achieve higher throughput [6]. In contrast, IEEE 802.15.4g (Wi-SUN) [3] and IEEE 802.11ah (Wi-Fi HaLow) [4] focus on high throughput applications, offering up to hundreds of kilobits or even megabits per second, but at a relatively low coverage area of around 1 km. Finally, DASH7 [5] provides a middle ground in terms of both throughput and range. Combining several such technologies in a single device would therefore greatly increase flexibility, offering the combined characteristics and advantages of multiple wireless technologies.

The idea of multimodal devices able to seamlessly switch from one network to the other is not new, and is generally referred to as *vertical handover*. The first widely known solution in this area was the IEEE 802.21 standard for Media Independent Handoff (MIH). It supports vertical handovers among various wired and wireless network technologies [7]. However, MIH focuses on traditional high-throughput networks. More recently, ETSI standardized the cross-vertical machine-to-machine (M2M) service layer [8]. It targets interoperability at the service layer, independent of the underlying network infrastructure [9]. Such an approach could hide the

multimodality from the perspective of the IoT applications, but does not address the challenges related to managing the selection and usage of the network interfaces nor the service layer signaling over constrained low-power networks. Batalla *et al.* proposed an extensible virtualization platform as a basis for a multi-stack IoT gateway based on IEEE 802.15.4 [10]. It currently supports ZigBee, Idsecom and 6LoWPAN, but their design is modular and can be extended to other technologies. The design makes use of virtual machines for the different technology protocol stacks, and the transmission of the baseband chip sequence to the physical layer of the single radio for modulation. As such, it is resource intensive and only suited for the infrastructure side of IoT networks as it cannot easily be ported to battery-powered devices. In addition, multimodality is enabled at the MAC and higher layer, but not at the physical layer, a prerequisite to support different sub-1GHz network technologies.

IoT networks are characterized by severe energy and resource constraints, which significantly complicates signaling, coordination, and network detection. Traditional solutions for vertical handover management [7] introduce too much signaling and control overhead to be applicable to multimodal IoT devices. Moreover, the vision and solution proposed in this article are complementary to existing approaches for IoT. Our solution can benefit from standardization [8], [9], which is focused on architecture and protocol aspects, as well as hardware virtualization platforms [10] to support multiple protocol stacks at the infrastructure side. In this article, we focus on the intelligence and management challenges in the end-to-end network convergence layer, paying specific attention to the extreme resource scarcity and heterogeneity of sub-1GHz wireless networks. This requires methods for coordi-

TABLE I  
COMPARISON OF THE MOST COMMON SUB-1GHZ WIRELESS IOT COMMUNICATION TECHNOLOGIES BASED ON EUROPEAN REGULATION

	Bandwidth	Modulation & Coding	Maximum TX power (dBm)	Maximum range (km)	Data rate	Max. payload size (bytes)
<b>LoRa</b>	125 kHz	CSS	14	15	0.25 – 5.4 kbps	59 – 250
<b>Sigfox UL</b>	100 Hz	DBPSK	14	50	100 bps	12
<b>Sigfox DL</b>	600 Hz	GFSK	27	50	600 bps	8
<b>NB-IoT</b>	180 kHz	OFDMA	23	15	20 – 250 kbps	85
<b>IEEE 802.15.4g</b>	7.8 – 500 kHz	FSK, OFDM, O-QPSK	14	1	40 – 800 kbps	2047
<b>IEEE 802.11ah</b>	1 – 16 MHz	OFDM	14	1	0.15 – 346 Mbps	2304
<b>DASH7</b>	25 – 200 kHz	GFSK	14	5	9.6 – 166.7 kbps	256

nation and network detection with extremely low signaling and radio utilization overhead. Additionally, it requires vertical handover strategies that take into account the heterogeneous characteristics of different sub-1GHz wireless technologies.

### III. COORDINATED HETEROGENEOUS IOT NETWORK ARCHITECTURE

In this section, the components of the envisioned heterogeneous low-power IoT network are described. The architecture, as depicted in Figure 2, involves multimodal IoT devices equipped with actuators and sensors, communicating with one or more IoT application providers. Communication takes place over several independently owned and operated low-power networks, some of which may be public and even offer their own cloud data platforms with proprietary APIs (e.g., Sigfox) and some of which may be private, possibly operated by the IoT application provider itself. At the heart of our approach are (i) the multimodal IoT device with its network convergence layer (NCL), and (ii) the virtual network operator with its heterogeneous network controller (HNC). The NCL provides an abstraction over the different available networks towards the device's applications. It autonomously determines which network to use. The HNC enables coordinated management across the different available networks. Together, the NCL and HNC enable IoT applications to intelligently make use of several low-power networks in a transparent manner, providing significant added value compared to using those networks independently. The approach results in increased flexibility and resilience. Flexibility is increased by allowing a single device to connect to different networks. It can then combine the advantages of all of them, based on the changing needs of the application. In terms of resilience, on-the-fly multimodal data forwarding allows the device or network manager to select a different network in reaction to link quality degradation or even complete loss of connectivity.

#### A. Multimodal IoT device

The proposed multimodal IoT device contains multiple wireless communications protocol stacks, which should preferably share the same radio chip and antenna. Sharing the same radio chip and antenna allows for a smaller form-factor and reduced costs, which is very important for many IoT applications. However, this is not always feasible due to licensing (e.g., only the Semtech-licensed radio chip can be used for LoRa), certification (e.g., as required to use the Sigfox

network), and frequency band constraints. The NCL allows IoT devices to intelligently make use of the available networks and their resources. It provides a virtual abstraction on top of the different network interfaces, making the process of network selection and protocol stack adaptation fully transparent to the IoT applications running on the device. Moreover, it provides a northbound interface that allows applications to announce the QoS requirements of the data to be transmitted. The three core tasks performed by the NCL are detailed below.

#### 1) Standard-based data encapsulation

The different radio technologies are all characterized by their own layer 2 frame formats. In order to avoid fragmentation at the higher layers and to create uniformity towards applications, the NCL introduces a data encapsulation method on top of these layer 2 formats, based on open IETF standards [11]. The 6LoWPAN adaptation layer provides compression and fragmentation services to reduce the transmission overhead and to satisfy the minimal IPv6 datagram size requirement. For the application layer, the Constrained Application Protocol (CoAP) is used. CoAP is a specialized web transfer protocol for use with constrained nodes and networks. Devices structure their data and actions as resources identified by URIs. By issuing GET, PUT, POST and DELETE requests, information can be retrieved, resource states can be changed or operations can be performed. In order to minimize overhead, CoAP uses a short 4-byte base header as well as a binary format for encoding message options in the CoAP requests and responses. This results in typical CoAP message sizes of around 10 bytes, excluding the application payload. The resulting stack has a low footprint and transmission overhead, but still has some limitations. In the best case, 6LoWPAN can compress the 48 bytes of the IPv6 and UDP header down to 6 bytes, which, together with the CoAP header and payload, still introduces too much overhead for LPWA technologies with very limited payloads such as SigFox. Therefore, Static Context Header Compression (SCHC), as being standardized by the IETF LPWAN working group, is used [12]. SCHC exploits the fact that most protocol header fields remain the same across packet transmissions between a device and its back-end. Therefore, a common context is stored in the LPWAN device and the network. This context consists of a list of rules. Each rule has a unique identifier and provides a packet header template and compression actions such as omitting or abbreviating header fields. The rule that best matches an outgoing packet is selected and the corresponding compression is applied. Using SCHC, packets can be compressed down to

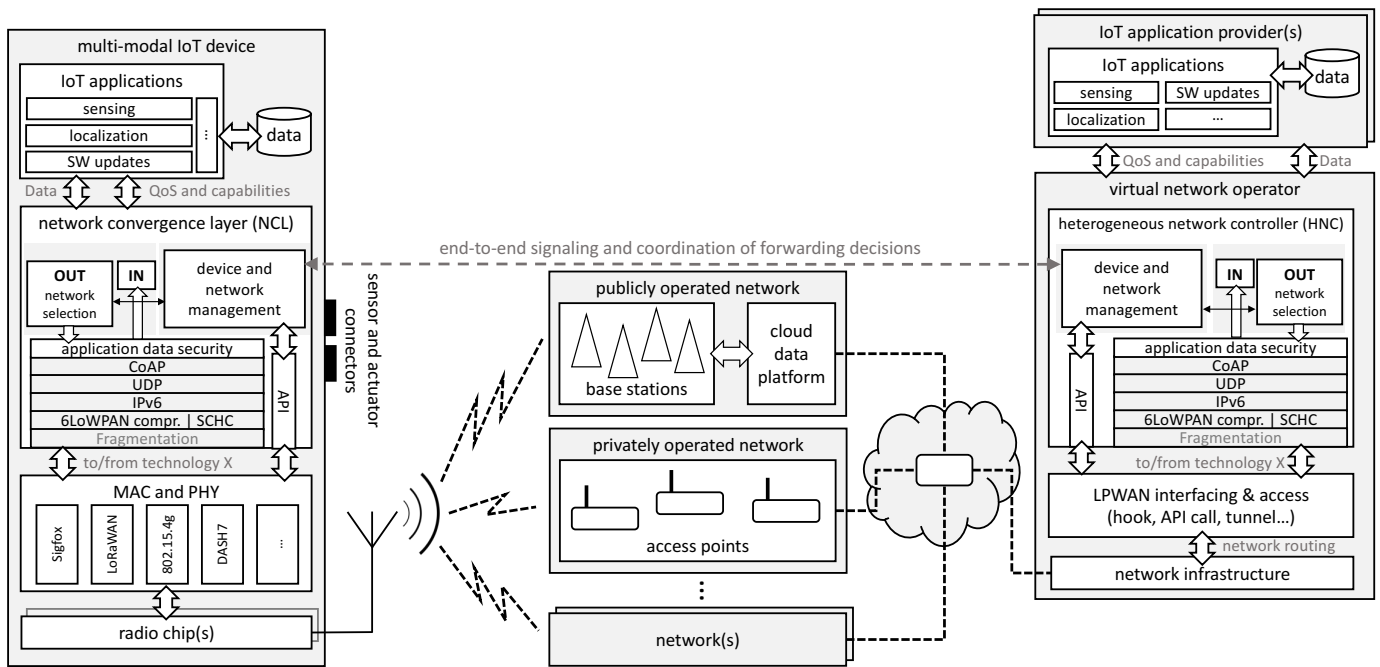


Fig. 2. Overview of the envisioned multimodal IoT network architecture, showing the interactions among the multimodal IoT device, several independently operated wireless access networks, and the virtual network operator. The virtual operator provides an abstraction layer on top of various heterogeneous networks, while signaling between the device and operator allows them to coordinate handovers. The network convergence layer (NCL) leverages on open standards to hide the complexities of coexisting MAC and PHY layers towards the application layer.

a few or even a single byte (i.e. only the rule ID).

## 2) Device and network management

The ability to use multiple wireless technologies requires the provisioning of additional management functionalities as well as signaling. From a radio resource point of view, the device must comply with duty cycle requirements in the sub-1GHz frequency band across technologies as well as keep track of mandatory resource allocations for downlink traffic. Part of the required information is obtained via an API towards the lower layers. With respect to network management, appropriate mechanisms such as polling and polling frequency in order to detect available networks, possibly complemented with over-the-air activation to obtain network access, must be supported for some of the technologies. Finally, with respect to protocol stack management, the transmission of data over a selected technology may trigger specific protocol stack configurations such as fragment size settings or retransmission timeouts. The required signaling between the devices and the virtual network operator must be limited and runs over the standard-based protocol stack. The knowledge available in the management component is also exposed to the applications via an application-facing API, which provides information about the resources of the available networks. This information can be used by applications as a trigger to for example transmit data, initiate a software update, or change the update frequency of localization messages. Of course, in many cases, applications are static and will not be able to adjust their behavior to changes in the available network resources. Such non-adaptive applications are instead able to signal their QoS requirements to the NCL, which are then used to drive the network selection process.

## 3) Network selection

The network selection component's main responsibility is to autonomously select which network technology to use for each data transmission, and to determine the most suitable moment to perform the transmission. For this, the NCL takes into account QoS requirements coming from the applications. Two different levels of requirements have been identified, namely global requirements across applications and application-specific requirements. At the global level, one can for instance define an upper boundary to the energy consumption in order to meet lifetime requirements or define how frequently the back-end must be polled for the presence of any available downlink traffic. At the application level, applications can enrich the data that needs to be transmitted with specific QoS requirements. Identified QoS requirements include:

- An upper bound on the transmission delay, in order to enable buffering of traffic in anticipation of the availability of a more energy efficient network or to indicate that data must be sent instantaneously.
- Whether the data transfer is bidirectional (e.g. data transfer followed by an acknowledgement or expecting a response).
- Whether it is a one-time transmission or periodic transmission with a given periodicity, to better align polling for alternative networks with data transmission needs.
- What the complete size is of the entire transaction (e.g., for performing a firmware update).
- The desired reliability, possibly resulting in multiple transmissions of the same message or request for an acknowledgement.

Based on this QoS information and the information retrieved from the management component about available networks, their resources, and duty cycle restrictions, a decision is made on when to transmit the data and over which technology. When the data is ready to be transmitted, it is handed over to the protocol stack, which will apply security, compression and fragmentation mechanisms suitable for the selected network technology.

As evidenced by prior work on network selection and vertical handovers (e.g., IEEE 802.21 [7]), the problem of seamlessly handing over the device's connection among heterogeneous networks is far from trivial. This is further complicated by the constrained nature of sub-1GHz network technologies, as it requires methods for network detection, signaling and coordination that are extremely efficient in terms of network resource and energy consumption.

### B. Virtual network operator

The virtual network operator is responsible for providing a unified interface between the IoT application server (e.g., running in a cloud data center) and the different heterogeneous networks. As such, its HNC performs a function similar to the NCL at the device side. The virtual network operator role can be taken up by a physical network operator (that offers multiple technologies), the IoT application provider (that may use its own private network in combination with a public network), or a separate entity. The main HNC functions are described below.

#### 1) Interfacing between virtual and physical network operators

The virtual network operator enables operation over a variety of sub-1GHz networks with different properties. The network management component keeps track of all managed networks and devices, whereas the network interfacing and network access component enables the exchange of data over these networks. For publicly operated networks such as Sigfox, the interfacing can be as simple as implementing the necessary hooks to a Cloud platform. For private multi-gateway deployments, the different gateways must be registered with the management component and secure communication channels for data and signaling must be established. Signaling consists of several aspects: (i) the retrieval of radio resource usage, (ii) the presence of devices in the network or their activation to use a network, (iii) the availability of downlink slots, (iv) the arrival time and signal strength of messages, and (v) the distribution of device specific information such as device identifier and temporary session keys towards all gateways.

#### 2) Data encapsulation and routing

The virtual operator implements a similar protocol stack as the device, as well as similar stack management mechanisms for all registered devices. Data is passed from the application provider to the stack, together with QoS requirements. Based on radio resource usage, presence of downlink slots, and knowledge about available networks for the destination device, a decision is made on which technology will be used for downlink communication and the required data encapsulation is applied. Alternatively, the virtual operator may terminate the

stack at the network layer and exchange IPv6 packets with the application providers.

## IV. EVALUATION

In this section, we quantify the advantages of coordination in heterogeneous IoT networks. An initial hardware prototype is used to illustrate the advantage of a multimodal IoT device in terms of energy efficiency and the feasibility of the protocol stack is assessed.

### A. Energy efficient multimodal IoT device

In this section, we compare the energy consumption of a multimodal IoT device with that of a traditional single-technology device. We assume a track and trace scenario where the multimodal device is attached to an asset that is transported between locations. The device monitors the environment and sends sensor readings and location coordinates at fixed (pre-configured) intervals, with a total payload of 27 bytes per message. It uses LoRa (with spreading factor 12) for communication when on the road, while attempting to use DASH7 when near a site or warehouse. To achieve this, the device polls for DASH7 availability at certain intervals. The polling interval can be smaller than the data transmission interval, as the device may want to change to DASH7 as fast as possible (e.g., for over-the-air software updates, or to synchronize temporarily stored data). The evaluation combines real hardware energy measurements with a simulated communications environment.

The measurements were performed using our initial single-antenna single-radio multimodal IoT device prototype, as depicted in Figure 3. It consists of a Silicon Labs EZR32 System on Chip (SoC) combined with the Semtech SX127X radio and an RF switch. This allows it to dynamically switch between different network technologies. Currently, it supports LoRa, Sigfox and DASH7, while support for IEEE 802.15.4g is underway. Energy consumption measurements on the prototype were conducted using the Keysight N6705B DC Power Analyzer. The energy consumed by LoRa for data transmission of the track and trace payload is measured as 563.55 mJ, while DASH7 transmission and polling uses 3.44 mJ (including acknowledgment reception). The measured energy values are subsequently used in a Python-based simulation model. In this simulation, the asset and attached multimodal tracking device are loaded onto a truck that drives around and comes within reach of a local DASH7 network with a certain probability (i.e., DASH7 availability). Two sensor and location data transmission intervals are evaluated (i.e., 600 s and 3600 s). Moreover, the polling interval to detect the availability of DASH7 is varied from 5 s (i.e., to detect the network in near real-time), up to 600 s (i.e., the same value as the lowest evaluated transmission interval).

Figure 4 depicts the results for both data transmission intervals. For the longer transmission interval (i.e., 3600 s), polling for DASH7 availability will use relatively higher energy, as less energy is consumed for data transmission. In this case, only very long polling intervals (600 s and more) will result in an energy reduction compared to pure LoRa



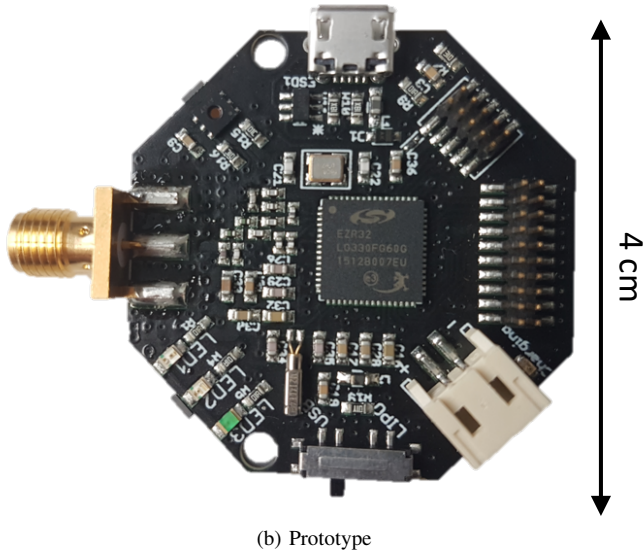
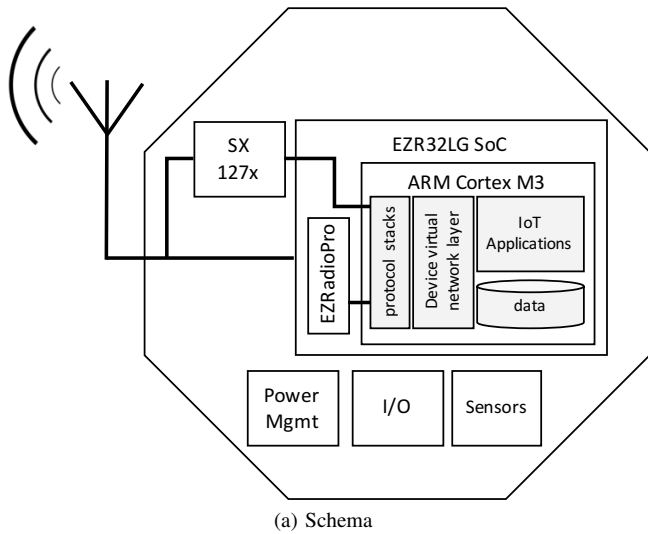


Fig. 3. Single-antenna multimodal sub-1Ghz IoT device prototype, supporting Sigfox, LoRa, DASH7 and IEEE 802.15.4g

when the DASH7 network is only sporadically available (i.e., less than 40 % of the time). In a more transmission heavy scenario, as depicted in Figure 4a, a polling interval of as low as 60 s will already improve energy consumption compared to the single-technology scenario if DASH7 is available at least 10 % of the time. For example, for a 600 s data transmission interval, a polling period of 60 s and a DASH7 network availability of 25 %, the multimodal solution already uses 18 % less energy than a LoRa single-technology device. This increases to a 43 % reduction when DASH7 is available 50 % of the time. In summary, the results show that a polling-based technology detection method is sufficiently energy-efficient if the transmission rate is high and there is no need for low latency handovers. In order to perform energy-efficient low-latency (in the order of a few seconds) handovers, more novel passive technology detection methods are needed.

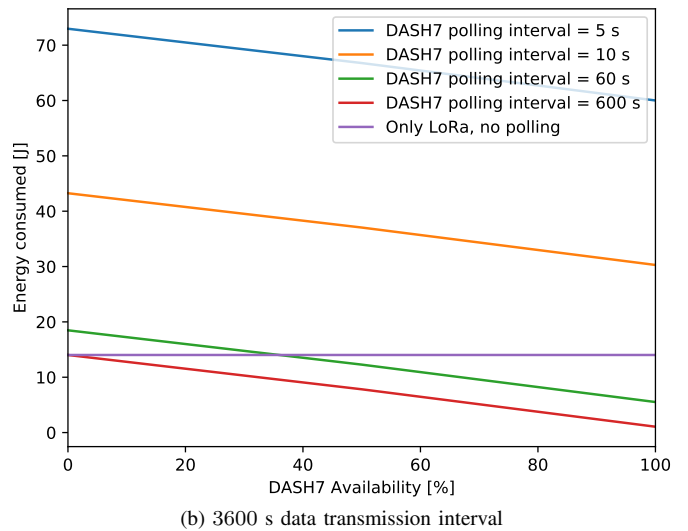
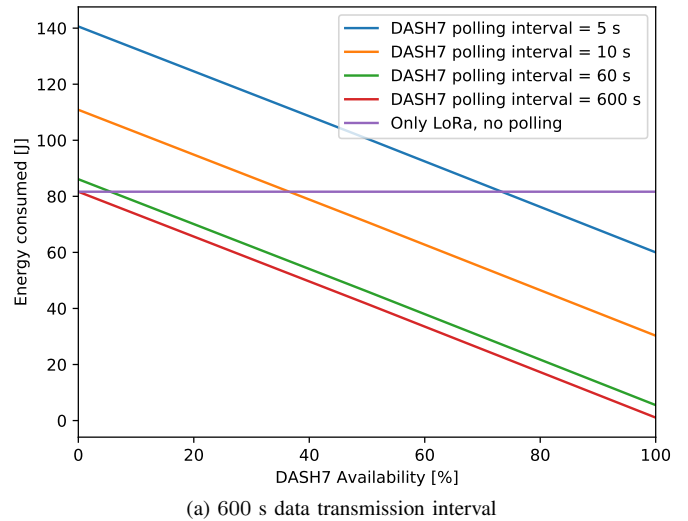


Fig. 4. Energy consumption comparing different DASH7 polling intervals with a single-technology solution (LoRa only) as a function of DASH7 network availability

### B. Static context header compression

In this section, we present results of the SCHC component of the multimodal IoT device. Figure 5 shows the realized architecture in combination with the SCHC performance. The protocol stack consists of LightWeight IPv6, PicoCoAP and an implementation of the SCHC draft for IPv6 and UDP. A LoRaWAN gateway is deployed and connected to the public The Things Network (TTN). An IPv6 subnet is associated with the gateway and the device has a statically configured address in this subnet. The device sends CoAP messages with a payload of 12 bytes to an application server. The virtual network operator interfaces with this public LoRa network, retrieving the messages generated by our nodes. SCHC decompression is applied, after which the resulting CoAP packet is routed further or directly handed over to the application.

Five different scenarios have been evaluated: (i) the payload is sent directly over LoRaWAN, (ii) the IPv6 packet is sent uncompressed over LoRaWAN, (iii) SCHC is used, but the

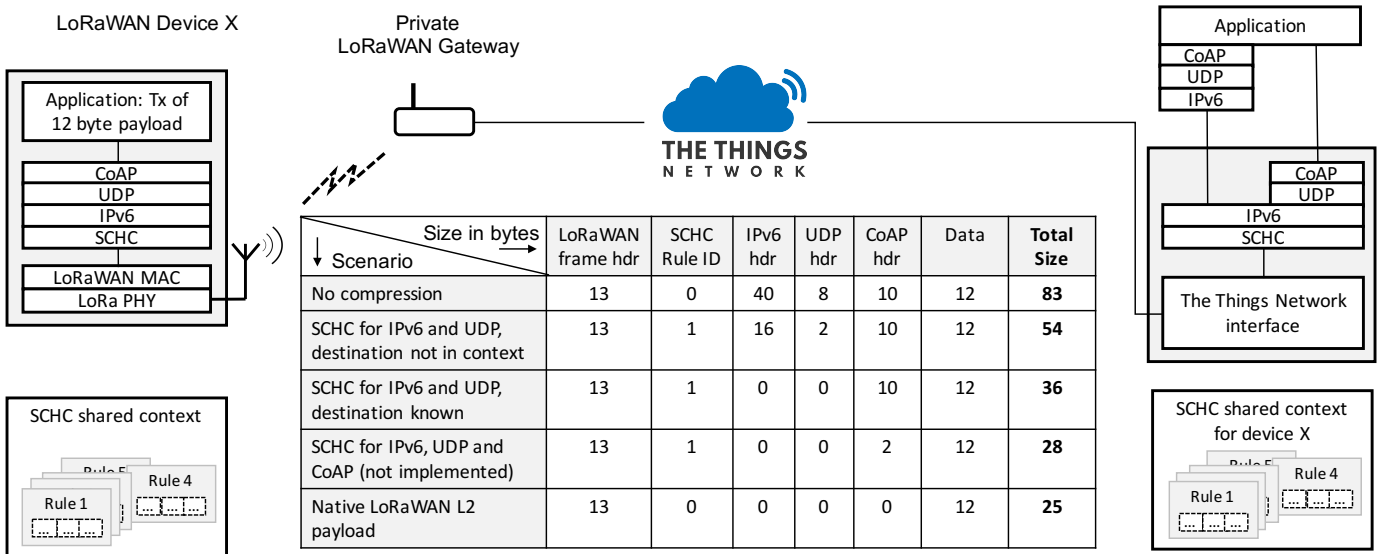


Fig. 5. Overview of the realized IPv6 over LoRaWAN architecture that uses SCHC to achieve compressions from 83 bytes down to 28 bytes depending on the scenario, compared to 25 bytes for a native LoRaWAN payload.

rule is not able to compress the destination IPv6 address (e.g., a situation where the device interacts with multiple different parties), and (iv) SCHC is used and the entire IPv6/UDP packet can be compressed (i.e., a situation where the device interacts with a known party), and (v) a theoretical scenario, where SCHC is used to also compress the CoAP header.

Depending on the scenario, different compression ratios can be achieved as shown in Figure 5. No compression results in a total size of 83 bytes compared to 25 bytes for a native LoRaWAN L2 transmission. For LoRa networks using spreading factor 10, 11 or 12, this is problematic. For these settings, the maximum layer 2 payload is only 51 bytes, making IPv6-based communication impossible. Using SCHC, the size can be reduced to 54, 36 or 28 bytes respectively, depending on the specific scenario. As such, the best SCHC compression provides a full CoAP/UDP/IPv6 stack header at a mere 10% overhead. Of course, this can only be achieved in the presence of rules that allow most header fields to be omitted. The ability of using such rules is strongly related to the heterogeneity of the traffic. More heterogeneous traffic either requires more rules or more generic rules where not all header fields can be omitted. In addition, if not known at deployment time, the installation of these rules must be done over-the-air and comes at a signaling cost.

## V. OPEN RESEARCH CHALLENGES

Achieving the vision of a coordinated heterogeneous IoT network consisting of a multitude of smart multimodal devices requires several research challenges to be addressed. This section surveys the most closely related state of the art and identifies major open research questions in key areas.

### A. Multimodal communication and management

Packet forwarding, vertical handovers and management of multi-technology sub-1GHz networks has only received very

limited attention in research. Recently, Taneja [13] presented a conceptual framework for interworking of IEEE 802.11ah and LoRa, focusing on resource management issues. However, this work did not address challenges related to protocol stack design, network and stack management. With respect to efficient and standard-based packet forwarding on top of LPWA networks, initial progress is made by IETF through the specification of SCHC. However, no solutions to install the SCHC context have been defined, the specifications only consider single-technology devices and security has not been considered at all. In the context of multimodal LPWA networks, additional research is needed to align application security across different technologies, dynamically install or learn the SCHC context, and disseminate context across the managed networks and their gateways. Also, with respect to network management, several open challenges remain. Here, solutions are needed to easily incorporate novel LPWA networks into the virtual operator system, to commission devices and immediately enable their operation across a variety of networks. Finally, innovations in network management are needed to expose relevant management APIs from the LPWA networks and devices towards the operator for proper management and signaling.

### B. Minimal-overhead technology detection

Shorter-range technology detection can be done through periodic polling (cf. Figure 4) combined with long-range LPWA network usage as a fall-back. However, this approach does not scale towards larger numbers of technologies and is not energy efficient. Alternative low-level approaches such as matched-filter detection, waveform-based sensing and cycle-stationary feature detection [14] are very accurate, but can only be applied using pre-decoded information which is not available in most LPWA radios. Furthermore, they typically have large memory and computational requirements, making them less suited for embedded devices. For constrained devices, an alternative approach is to utilize simple RSSI-based



energy detection features [15] (i.e., power, idle times, periodicity, transmission times, packet gaps) to identify technologies with different Medium Access Control (MAC) mechanisms. However, existing technology recognition solutions do not take into account sub-1GHz specific aspects, such as the limited detection bandwidth of many sub-1GHz radios, the longer packet transmission duration (requiring longer sampling times) and the possibility to do technology recognition even in the presence of overlapping packet transmissions. As such, there is a need for novel, efficient sub-1GHz technology detection and recognition methods to allow devices to make informed decisions about when to switch between technologies. A possible research direction is to trigger the switch passively by incorporating an RFID scanner (e.g., UHF Gen-2) in the hardware design.

## VI. CONCLUSION

This article presents a novel heterogeneous IoT network architecture that provides applications with a flexible virtual network abstraction on top of a variety of low-power IoT networks with varying characteristics. This allows the device and network manager to achieve seamless handovers across technologies in line with dynamic application requirements and network quality. The advantages of this approach include greatly increased flexibility, resilience, energy-efficiency, and combined indoor-outdoor coverage. Preliminary measurements and simulations already show the promise of the proposed solution, with a reduction in energy consumption even when using an energy-intensive polling-based handover technique. Several challenges still remain to be addressed in order to fully realize this vision, both in terms of multimodal network communication and management, as well as passive energy-efficient technology detection methods.

## ACKNOWLEDGEMENT

Part of this research was funded by the Flemish FWO SBO S004017N IDEAL-IoT (Intelligent DENSE And Long range IoT networks) project, and by the ICON project MuSCLe-IoT. MuSCLe-IoT is a project realized in collaboration with imec, with project support from VLAIO (Flanders Innovation and Entrepreneurship). Project partners are imec, Flash Private Mobile Networks, Engie M2M, Sensolus and Aertssen.

## REFERENCES

- [1] 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, p. 1466, 2016.
- [2] B. Reynders, W. Meert, and S. Pollin, "Range and coexistence analysis of long range unlicensed communication," in *23rd International Conference on Telecommunications (ICT)*, 2016.
- [3] K.-H. Chang and B. Mason, "The IEEE 802.15.4g standard for smart metering utility networks," in *IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, 2012, pp. 476–480.
- [4] V. Baños Gonzalez, M. S. Afaqui, E. Lopez-Aguilera, and E. Garcia-Villegas, "IEEE 802.11ah: A technology to face the IoT challenge," *Sensors*, vol. 16, no. 11, p. 1960, 2016.
- [5] M. Weyn, G. Ergeerts, R. Berkvens, B. Wojciechowski, and Y. Tabakov, "DASH7 alliance protocol 1.0: Low-power, mid-range sensor and actuator communication," in *IEEE Conference on Standards for Communications and Networking (CSCN)*, 2015, pp. 54–59.
- [6] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An overview," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, 2017.
- [7] G. Lampropoulos, A. K. Salkintzis, and N. Passas, "Media-independent handover for seamless service provision in heterogeneous networks," *IEEE Communications Magazine*, vol. 46, no. 1, pp. 64–71, 2008.
- [8] TS 102 690, "Machine-to-Machine communication (M2M); functional architecture," European Telecommunications Standards Institute (ETSI), Sophia Antipolis, France, Standard, 2011.
- [9] P. Guillemin, F. Berens, M. Carugi, M. Arndt, L. Ladid, G. Percivall, B. De Lathouwer, S. Liang, A. Bröring, and P. Thubert, "Internet of Things standardization – status, requirements, initiatives and organisations," in *Internet of Things – Converging technologies for smart environments and integrated ecosystems*, O. Vermesan and P. Friess, Eds. Aalborg: River Publishers, 2013, ch. 7, pp. 259–276.
- [10] J. M. Batalla, G. Mastorakis, C. X. Mavromoustakis, and J. Zurek, "On cohabitating networking technologies with common wireless access for home automation system purposes," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 76–83, 2016.
- [11] I. Ishaq, D. Carels, G. K. Teklemariam, J. Hoebcke, F. V. d. Abeele, E. D. Poorter, I. Moerman, and P. Demeester, "IETF standardization in the field of the Internet of Things (IoT): A survey," *Journal of Sensor and Actuator Networks*, vol. 2, no. 2, pp. 235–287, 2013.
- [12] A. Minaburo, L. Toutain, and C. Gomez, "LPWAN static context header compression (SCHC) and fragmentation for IPv6 and UDP," Internet Engineering Task Force, Internet-Draft draft-ietf-lpwan-ipv6-static-context-hc-10, Feb. 2018, accessed on March 20, 2018. [Online]. Available: <https://datatracker.ietf.org/doc/draft-ietf-lpwan-ipv6-static-context-hc-10>
- [13] M. Taneja, "802.11ah - LPWA interworking," in *IEEE NetSoft Conference and Workshops (NetSoft)*, 2016, pp. 441–446.
- [14] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 40–48, 2008.
- [15] H. Zhang, X. Chu, W. Guo, and S. Wang, "Coexistence of Wi-Fi and heterogeneous small cell networks sharing unlicensed spectrum," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 158–164, 2015.