Improving access to healthcare in rural communities - IoT as part of the solution

Full Text

Title: **Improving access to healthcare in rural communities - IoT as part of the solution**

Authors: **I. K. Poyner and R. S. Sherratt**

Biomedical Engineering, University of Reading, UK,
i.poyner@pgr.reading.ac.uk
r.s.sherratt@reading.ac.uk

Conference: International Conference on Technologies for Active and Assisted Living (TechAAL 2019)
Publisher: IET
Location: London
Conference Date: 25 March 2019
Accepted Date: 21st January 2019
Published Date: not yet published
pp.: not yet assigned
DOI: not yet assigned

Keywords: IoT, healthcare, remote, rural, constrained.

Abstract

AAL has benefitted tremendously from the near-ubiquity of powerful smartphones and very high data rates available over broadband and mobile networks. However, this is beyond the reach of many users. IoT systems offer the potential to extend some of the benefits to disadvantaged users. Such solutions will need to secure personal health information and provide a sufficient quality of service even when operating constrained user devices and communications.

1 Introduction

Technologies such as low-cost computers and broadband communications are enabling novel healthcare services that can help people, young and old, reduce the impact of chronic conditions, such as diabetes, cognitive challenges and dementia. In some cases, a user may share information in a controlled manner with other people who can provide support, such as family members, carers and organisations who have legal safeguarding obligations to user, such as social services.

However, communities in rural areas or developing countries may be inadvertently excluded from these transformative benefits because communications are not available, systems are unaffordable, or services have not been regionalised to make them easier for a user to understand in their native language.

Even within developed countries, broadband and 4G mobile services are not ubiquitous – in the UK around 860,000 premises cannot get broadband that meets the Government's Universal Service Obligation and only 64% of the UK's geographic area can receive 4G services [1]. Over 24 million Americans lack access to broadband infrastructure, with adoption at 69% in rural areas, compared to nearly 98% in urban areas [2]. Globally, there are 3.9 billion people not connected to the internet, with most living in rural areas.

Usability issues (including language and configuration) and affordability are even greater barriers than lack of access to communications, according to the United Nations [3]. In many developing communities, smartphones are too complex for some users, especially if the smartphone does not support the user's native language or script, is too expensive, not supported by the network and requires too frequent charging, where power is not always available. As an example, in Rwanda 92% of the population are within 3G coverage and internet should be affordable to around 32% of households (based upon the assumption that cost is less than 5% of total expenditure), yet only 9% of households had access to the internet. The Government of Rwanda recognises that low computer literacy is a major obstacle to becoming a "Smart Nation" (less than 9% of over 15-year olds are computer literate) [4].

IoT (Internet of Things) technologies could partially mitigate these issues. Low cost devices with long battery life and a simple (disappearing) user-interface may be more appropriate than smartphones. Wireless network base-stations with a range of 10-15km and costing from around £400 [5] may enable communities to enjoy at least some of the healthcare benefits being deployed in western urban communities.

In this paper we look at four use cases, the users of the services, requirements on the system, constraints encountered by traditional technology and how IoT technologies can address some of the constraints.

2 Use cases

Four use cases are considered:

1. Elderly person coping with early onset dementia living in a rural environment. Generally fit and active, but who may occasionally become disoriented in unfamiliar surroundings or poor visibility when outdoors.
2. A teenager with Type 1 diabetes undertaking a multi-day expedition in a wilderness area with remote supervision (Duke of Edinburgh Award), who becomes dangerously confused when blood sugar levels are not under control.
3. An adult with Down's Syndrome living independently (supported living) and suffering with high blood pressure.
4. A midwife supporting pregnant women in several villages in a developing country. In some of the least developed countries there is a significant gender digital divide with only one in seven women using the internet compared with one in five men. The gender digital divide in Africa appears to have grown significantly over the past five years [6].

Some common characteristics amongst these use cases are:

- End-user device management and ergonomics - the user may at times suffer from physical and/or cognitive impairments and not always be capable of operating a device (such as a smartphone) or be relied upon to charge the device daily. For some people, technology will be alien and so mass-market health and fitness devices and apps would be wholly inappropriate. Some users may be highly independent and resent any outward 'tag' and so may favour a sensor that blends into other objects or garments (e.g.: walking stick or jacket).
- Communications - the user will regularly not be within coverage of in-home Wi-Fi or 3G/4G mobile communications. Two-way communications may be beneficial for carers to support users. This is particularly important for the midwife case who could send reminders and ante-natal advice.
- Duty of care and availability – the primary user of the data is generally not the wearer of the device, but people who can provide assistance, such as carers, supervisors or family members. They may have a legal obligation to safeguard the individual and so need to know that the monitoring system is functioning correctly.

- Privacy of personal information - carers and supervisors may have a need to know the person's pattern-of-life and status, such as location, glucose level, blood pressure, temperature etc. However, carers should only have access to the information they require for their particular role to safeguard the individual and should not have access to privileged information that GPs or guardians may have.
- Confidentiality - such information could make an individual highly vulnerable if it was accessed by inappropriate people or organisations.
- Consent management – the individual, or their legal guardian, must be able to control the information that can be accessed by carers, supervisors and family members. Associated with this is the identity management of both users and devices across the end-to-end service.

3 Requirements

This section explores four segments of an IoT system [7], namely the user device (sensor), wide area communications, carer services and overall system requirements.

Within a home or healthcare environment there is ample opportunity to generate an abundance of data from multiple sensors, either worn by or implanted within the user, and ambient sensors, such as sensors in chairs, bed and bathroom.

A complication in our use cases, where users may be outside of their homes, compared to AAL-at-home or smartphone-based systems is that there is no gateway device or decision measuring unit [8]. Such a device typically provides processing power to perform data collection and protocol conversion from multiple heterogenous sensors, aggregation and filtering, local analysis of the data and triggering of alarms when required, implement security protocols and encryption, establish high-bandwidth communications, etc. Instead, these functions must be performed either within the low-power user device or at the system level.

3.1 User-device requirements

Mass-consumer health and fitness apps and devices, often based upon smartphones, have grown rapidly because they serve a large and affluent section of society. In contrast, AAL users have very different usability challenges and may have very little disposable income or be reliant upon stretched social services to provide care. For these users, it is critical to consider:

- Safety, especially where the device may be in close contact with the user and communicating over a wide-area, needs to comply with safety regulations, such as specific absorption rate (SAR) of RF energy absorbed by the human body.
- User-centred design [9], such as a disappearing user interface, where the user is unable to directly configure the device. This avoids a user inadvertently misconfiguring the device. Configuration needs to be completed via a remote connection or second device (network, Bluetooth, NFC, USB etc.), which needs to support the carer's native language or dialect.
- Ergonomically the device should be virtually invisible in the user's mind, so reducing the risk that that they remove the device. This could be achieved by incorporating the device into a walking stick, pendant or clothing etc.
- Long-life battery, to overcome the user not remembering to recharge the device. Ideally, maintenance of the device (battery replacement) should be annual, or monthly. This becomes even more important in communities that do not have reliable power supplies for routine recharging of devices. This will require a trade-off with how much information is processed and transmitted.
- Secure by design, as the user may be unable to input passwords or deal with other authentication methods, such as biometrics, especially when confused. Initial configuration and enrolment of the device would likely need to be completed by the service provider.

3.2 Communications requirements

Hospital and nursing home environments can draw upon high-fidelity monitoring systems, technicians to configure and rectify devices, reliable power supplies, high-speed networks under their own administration and, as importantly, trigger intervention by medical staff or carers at short notice. In such data-rich environments, expected monitoring rates are shown in Table 1 [10],[11],[12].

Application	*Target data rate*	*Latency*	*Packet size (Bytes)*
Video / Medical imaging	< 10 Mbps (e.g., Standard Video)	< 100 ms	
EMG	1.536 Mbps (8kHz sample, 16-bit ADC, 12 channels)	<250 ms	16.3
Capsule Endoscope	1 Mbps	-	
Audio	1 Mbps	< 20 ms	
Deep Brain Stimulation	< 320 Kbps	< 250 ms	
ECG	192 Kbps (6 Kbps, 32 channels)	<250 ms	17
EEG	86.4 Kbps (300Hz sample, 12-bit ADC, 24 channels)	<250 ms	16.3
Motion sensor	35 kbps	250 ms	16.3
Drug Delivery	< 16 Kbps	< 250 ms	
Blood Pressure	13.2 Kbps	10 ms	16.4
Respiration	3.2 Kbps	40 ms	16
Glucose level	< 1 Kbps	240 sec	15.1
Skin Temperature	120 bps	60sec	17.0
$Sp0_2$ blood saturation	16 bps	250 ms	16.4

Table 1: Unconstrained monitoring rates

In contrast, for remote users, especially when they are outside of their home, compromises need to be made where lower granularity of data or less frequent updates are provided but must still be sufficient to assure the carer of the user’s condition. From the example use cases, it may be acceptable for the user’s location and temperature, together with blood glucose level or blood pressure level, to be updated once per 30 minutes. Readings outside of an expected range could trigger more frequent monitoring or could add other parameters to the updates.

Geo-location is an important parameter for the remote monitoring a mobile user, which is generally not a factor for hospital or home AAL systems. Different methods for geo-locating a sensor are available (triangulation from base stations; GPS although it can be power and processing hungry, etc.), but typically co-ordinates can be provided in 9 bytes (GPS format of 3 bytes each for latitude, longitude and altitude) or 7 bytes (AIS reports 28-bit longitude, 27-bit latitude) [13].

Reliability of the communications channel may be required, including assured delivery of messages, known freshness and error correction.

Depending upon the system, it may be necessary for bi-directional communications, such as to provide reliable delivery, request different monitoring parameters or rates, patching software and renewing security associations (including revoking the device).

3.3 Carer services

The user information needs to be actioned by emergency services, social carers or family members when there is a problem. Otherwise, the data may be stored centrally to provide a ‘pattern of life’ of what is normal for the user or shared as depersonalised information with researchers in order to build a population-scale database for different conditions.

The critical aspect is that the system is handling and storing personal health information (PHI) of particularly vulnerable people. Safeguarding data in compliance with EU GDPR (General Data Protection Regulations) and/or US HIPAA (Health Insurance Portability and Accountability Act) laws must be a fundamental design consideration from the outset.

For many carer organisations, re-using existing applications and services (as used on Wi-Fi/internet/3G-enabled services) may be the most efficient approach as the carer workforce does not need to be trained to operate or respond to two systems. Also, all the data, security, audit logs and system administration are on a single system.

Existing applications would need to recognise that IoT-enabled sensors and communications will have much sparser data, there may be extended periods when no data is received, and it may be more difficult to send requests to end-user devices. These technical challenges will affect the decision making (by automated algorithm or human carer) as to whether the user needs to be contacted in person.

3.4 Overall system requirements

As mentioned earlier, the legal requirements to protect PHI discriminates healthcare systems from many other IoT systems. Other applications may have a commercial need to secure data in transit, but the impact of security vulnerabilities of healthcare information systems are high [14], [15] and so they need to demonstrate compliance to best practice, security and privacy of data guidelines [16]. The following factors must be addressed during the initial design and throughout the life of the system [17]:

- Confidentiality – data is accessible only to those who have the right to know.
- Integrity - assurance that data has not been tampered with or modified in any way to undermine its authenticity.
- Availability – having timely access to information.
- Identity management - management of user identities across the end-to-end architecture, hence associating health information with the right individuals.
- Nonrepudiation of origin.
- Consent management - enables users (or guardians) to provide and manage their consent preferences, which serves as a basis for governing access to and usage of their individual identifiable health information.

For GDPR compliance, the UK ICO (Information Commissioner’s Office) [18] advocates the seven ‘foundational principles of privacy by design’ developed by the Information & Privacy Commissioner of Ontario [19] which lists seven principles, four of which are very relevant to IoT:

- Privacy as the default setting.
- Privacy embedded into design.
- End-to-end security.
- Respect for user privacy.

Implementing security in a very constrained system, without a gateway device and where the sensor has limited processing power and the communications are limited, requires very careful selection of the encryption algorithm to ensure that it remains robust even with intermittent connections and without needing end-user interaction [20], [21], [22]. It may be that currently ‘*no security approach provides the perfect solution [for constrained devices]* ’[23]. However, if the sensor and communications are both contained within the user device then this overcomes the vulnerability of sensor to gateway transfer seen in more traditional AAL systems (Bluetooth or Wi-Fi is typically used to secure the link). Work in this area includes the NIST (US National Institute of Science and Technology) lightweight security project for IoT [24], the IETF working group addressing authentication in constrained environments [25], and other potential techniques such as encompression [26].

In addition to security, managing a system based upon constrained devices deployed into a highly variable environment with limited communications will always be challenging. The system has to manage FCAPS (fault, configuration and remote reprogramming, accounting, performance and security) [27], localisation of mobile devices, prioritisation of messages (e.g.: routine, high priority, emergency), reliability, remote calibration, scalability and interoperability across homogeneous devices.

4 LPWAN communications options

Low-power wide area networks (LPWAN) potentially enable IoT devices to communicate over long distances (several kms) with low or no networking charges and at very low energy (e.g.: can run off an AA battery for several years). A few base stations within a rural community could service dwellings over a wide area. The base stations could alert local carers and first responders and could reach regional services either by landline (where available) or a network of base stations (although aggregating messages on LPWAN systems can lead to overload).

Prioritisation and assured delivery of messages may be important for some health services. In addition, downlink capability may be important for several reasons such as for carers to send reminders to take medication, handshaking between devices to establish security associations and for system administrators to patch or update user devices.

Considerations in choosing an LPWAN will include:

- Overall capital and operating costs, including licences and base stations;
- Range, and how it deals with hills or buildings blocking line of sight;
- Reliability, to assure important messages are delivered and to avoid users rejecting the system;
- Data rate for individual devices, constraints on the duty cycle of transmitting, and the overall system capacity.
- Energy consumption, to avoid having to recharge or replace batteries in user devices;
- Security to protect PHI in transit;
- Open standard versus proprietary solutions to avoid being locked into a vendor and potentially losing the investment should the vendor discontinue the system. An open system may also enable a community more freedom to deploy their own system rather than relying on having to buy a service.

Table 2 provides an indicative performance of the leading current and planned LPWAN technologies. Compared to cellular technologies, LPWANs use more sensitive receivers to enable greater range (up to 40dBm, or 10,000 times more sensitive) [28]. However, as with many networking protocols, there are trade-offs between range, data rate and energy consumption. In addition, any community-based service would need to consider the cost of user-devices and base stations, together with reliability and complexity in maintaining the system. Other factors to consider include local geography blocking signals, national regulations on licensing and maximum usage of frequency bands, and contention with other local users (too many messages will cause collisions, resulting in a decrease in throughput).

LPWAN	*Range (km)*	*Two-way*	*Data rate*	*Packet size (Bytes)*
NB IoT	15	Y	60 - 250 kbps (30-170 kbps down)	Variable
EC-GSM-IoT	15	Y	70 – 240 kbps	Variable
LTE Cat-M1 eMTC	15	Y	375 kbps	Variable
Ingenu RPMA	5 – 6 (>500 km star)	Y	624 kbps up 156 kbps down	Variable up to 10Kb
LoRaWAN	5 - 15	Y	250 bps to 50 kbps	59 to 250 B
Symphony Link (LoRa)	10	Y	Similar to LoRaWAN	256 B
Weightless -W	~ 2	Y	200 bps – 1 Mbps	10 B +
Dash 7	5	Y	167 kbps	256 B
SigFox	10	4/day	100 - 600 bps	12 (max 14 packets per day)
nWave		N	100 bps	2 – 20 B

Table 2: Indicative LPWAN performance

The first four systems (NB-IoT, EC-GSM-IoT, LTE CatM1, and 5G) are 3GPP (3rd Generation Partnership Project) standards that (will) operate from existing mobile phone base stations using licensed spectrum. As this research is focussed on areas underserved by traditional cellular coverage, they are only included for comparison.

NB-IoT (Narrowband-IoT), or Cat-NB, was approved by the 3GPP in June 2016 and is being rolled out by major network operators (e.g.: Vodafone within the UK). With links of up to 250kbps, it aims to be more cost-effective than 3G/4G networks for M2M (machine-to-machine) applications. NB-IoT fits into 180KHz of spectrum and so operators have the option of deploying on a GSM carrier spectrum where 4G has not been rolled out [29].

EC-GSM-IoT (Extended Coverage Global System for Mobile Communications Internet of Things) and LTE-M (eMTC and LTE CatM1) provide high speed communications over mobile network spectrum. They are likely to be deployed only by existing carriers.

5G networks are expected to be rolled out starting in 2019, although initial deployments will be to dense urban areas. Coverage may be better than existing 3G/4G networks but are still unlikely to be economically viable in many rural areas.

Ingenu RPMA (random phase multiple access) is a proprietary standard with range of up to 50 km line of sight or 5-10 km without line of sight. Message acknowledgement improves reliability and helps to fulfil duty-of-care requirements. The number of access points required to serve an area is purported to be significantly lower according to Ingenu, although its energy consumption may be higher. However, roll-out appears to depend upon Ingenu and its partners, which may prevent for community-led deployments.

LoRa (Long Range) is promoted by the LoRa Alliance, but the underlying transceiver chip is proprietary to Semtech, the originators of LoRa. LoRa operates in the unlicensed ISM spectrum (Industrial, Scientific and Medical – 433MHz and 868 MHz in EU) and is the basis of LoRaWAN and Symphony Link. It is bi-directional and base stations and end nodes are available from several companies relatively cheaply, so making it highly suitable for community use.

LoRaWAN aims for devices to operate for several years on a single battery, dependent upon the messaging rate and distances. Typical configuration is in a star-of-stars network to relay messages to a network server [30]. There are a growing number of demonstration networks, including 16 gateways around Reading [31]. Base stations cost around £400 (or can be built upon a Raspberry Pi for around £200) and so may be affordable for community networks.

Link Lab's Symphony Link is a proprietary system operating in the ISM band that uses the LoRa standard chipsets for the PHY (physical layer) but not the LoRaWAN MAC (media access control). It has an adaptive data rate, supports packet acknowledgement and provides privacy using AES and TLS encryption. It is more expensive than LoRaWAN products, but purports to offer improved performance, which could be suitable for a service which requires high quality of service. Weightless is an open standard with three sub-standards; -N is unidirectional, -P and -W are both bi-directional. -N and -P operate in the sub-1GHz unlicensed spectrum, whilst -W operates in the TV spectrum, but has higher power consumption. Range is lower than other technologies above and so may not be suitable for dispersed communities.

Dash7, derived from ISO18000-7, is a proprietary, open source system. Originating from military logistics and RFID tags, it is suited for BLAST traffic (bursty, light, asynchronous, stealth and transitive). Due to limited range its use for community services is limited.

SigFox is a proprietary standard and is widely deployed in Europe. It is connectionless, optimised for uplink communications and in ideal rural environments, the range can be over 30km. However, its uplink packet size is limited to 150 messages of 12 bytes per day. The downlink channel is even more constrained to four messages of 8 bytes per day. In areas served by SigFox, it could provide simple health status, but it would be difficult to provide a reliable health service based on SigFox or a service requiring two-way messaging.

Nwave's marketing is focussed on parking solutions, claiming to have twice the range and an order of magnitude lower power compared to LoRa. Similar to SigFox, it is too constrained to be useful for healthcare.

Satellite-based IoT communications shows great potential, with over 18 different constellations at varying stages of development. However, many of these proposed systems may not achieve operations and of those that do, the pricing structure may be prohibitive for all but the most affluent of rural residents. Power consumption may also be problematic.

5. Future work

The cost of implementing a community IoT healthcare access system needs to be assessed for specific countries. The overall cost will be sensitive to base station costs, the number of access points required to cover a given region, licensing costs and the specialist skills required to implement a system.

After down-selection of the LPWAN, power consumption analysis needs to be completed to estimate the battery life. Then lightweight security protocols will be assessed, leading to a candidate architecture for a prototype system to be built. The aim is to trial the IoT system where it can be compared to a more pervasive AAL capability, such as SPHERE [32].

Depending upon market maturity, satellite links may be investigated, such as the Lacuna system. This would be dependent upon the openness of the operators to divulge information and to participate in a research project.

5 Conclusions

LoRa (LoRaWAN and Symphony Link), Weightless-P and RPMA may be suitable for a community-based healthcare monitoring service. However, further work is required to determine costs, complexity, battery life and security. Additionally, commercial constraints, such as any dependency to buy a service from a national provider, need to be considered for any underserved community.

6. Acknowledgements

This research is funded by the University of Reading Research Endowment Trust Fund.

7. References

[1] Ofcom, "Connected Nations Update October 2018," Ofcom 2 October 2018.

[2] Federal Communications Commission, "2018 BROADBAND DEPLOYMENT REPORT," Federal Communications Commission, Washington, D.C. 2 February 2018.

[3] M. J. ITU Deputy Secretary-General, "The Commonwealth of Nations and United Nations Perspectives: Bridging the Health and Technology Sectors with the Global Goals," in *71st World Health Assembly "Creating a digital Health Dynamic for Universal Health Coverage 2030"*, Geneva, 2018.

[4] ITU, "ICTs, LDCs and the SDGs Achieving universal and affordable Internet in the least developed countries," 2018.

[5] The Things Network, "List of Gateways," 2019.

[6] ITU, "ITU COUNCIL CONTRIBUTION TO THE HIGH-LEVEL POLITICAL FORUM ON SUSTAINABLE DEVELOPMENT (HLPF)," ITU 8 March 2018.

[7] ITU, "ITU-T Y.2060 Overview of the Internet of things," 2012, pp.

[8] M. Ghamari, B. Janko, R. Sherratt, W. Harwin, R. Piechockic, and C. Soltanpur, "A Survey on Wireless Body Area Networks for eHealthcare Systems in Residential Environments," *Sensors,* vol. 16, p. 831, 2016.

[9] ISO, "9241-210: 2010. Ergonomics of human system interaction-Part 210: Human-centred design for interactive systems," *International Standardization Organization (ISO). Switzerland,* 2009.

[10] C. Cordeiro and M. Patel, "Body area networking standardization: present and future directions," in *Proceedings of the ICST 2nd international conference on Body area networks* Florence, Italy: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2007.

[11] M. Shu, D. Yuan, C. Zhang, Y. Wang, and C. Chen, "A MAC protocol for medical monitoring applications of wireless body area networks," *Sensors (Basel, Switzerland),* vol. 15, pp. 12906-12931, 2015.

[12] M. S. Akbar, H. Yu, and S. Cang, "IEEE 802.15.4 Frame Aggregation Enhancement to Provide High Performance in Life-Critical Patient Monitoring Systems," *Sensors (Basel, Switzerland),* vol. 17, p. 241.

[13] United States Coast Guard, "AIS Standard Position Report," 2017.

[14] N. S. Abouzakhar;, A. Jones;, and O. Angelopoulou, "Internet of Things Security: A Review of Risks and Threats to Healthcare Sector," 2017.

[15] J. M. Blythe, S. Michie, J. Watson, and C. E. Lefevre, "Internet of Things in Healthcare: Identifying key malicious threats, end-user protective and problematic behaviours," *Frontiers in Public Health*.

[16] IOT Security Foundation, "Establishing Principles for Internet of Things Security," 2016.

[17] I. K. Poyner and R. S. Sherratt, *Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people*: Institution of Engineering and Technology.

[18] Information Commissioner’s Office (UK), "Information Commissioner’s Office," 2017.

[19] Information & Privacy Commissioner of Ontario, "Privacy by Design," 2013.

[20] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal,* vol. 4, pp. 1250-1258, 2017.

[21] H. Suo, J. Wan, C. Zou, and J. Liu, *Security in the Internet of Things: A Review*.

[22] ETSI, "ETSI TR 118 508 V1.0.0 (2014-07) Analysis of Security Solutions for the oneM2M System " July 2014 2014.

[23] IETF, Garcia-Morchon, S. Kumar, and M. Sethi, "State-of-the-Art and Challenges for the Internet of Things Security draft-irtf-t2trg-iot-seccons-08," 2017.

[24] NIST, "Report on Lightweight Cryptography," 28 March 2017 2017.

[25] IETF, "An architecture for authorization in constrained environments draft-ietf-ace-actors-07," 22 October 2018 2018.

[26] M. Zhang, M. M. Kermani, A. Raghunathan, and N. K. Jha, "Energy-efficient and Secure Sensor Data Transmission Using Encompression," in *2013 26th International Conference on VLSI Design and 2013 12th International Conference on Embedded Systems*, 2013, pp. 31-36.

[27] ITU, "X.700 : Management framework for Open Systems Interconnection (OSI) for CCITT applications," 10 September 1992 1992.

[28] Link Labs, "A comprehensive look at Low Power, Wide Area Networks ", 2016.

[29] Vodafone, "Narrowband IoT," 2018.

[30] IETF, "RFC 8376 Low-Power Wide Area Network (LPWAN) Overview Draft," 31 May 2018 2018.

[31] The Things Network, "The Things Network Reading."

[32] SPHERE, "SPHERE," 2018.