The wireless Internet of Things: Spectrum utilisation and monitoring

Commissioned by:
Radiocommunications Agency Netherlands

Project number:
2016.032

Publication number:
2016.032-1618 v2.3

Date:
Utrecht, 31 October 2016

Authors:
Tommy van der Vorst MSc
Jasper Veldman MSc
Jan van Rees MSc

Management summary

In this study, we analyse the current and future impact of wireless Internet of Things[1] (IoT) connectivity on the radio spectrum. The main research questions are:

1. Which issues will be caused by the utilisation of spectrum below 1 GHz by wireless IoT applications, and what are possible solutions for overcoming these issues?

2. What are obstacles affecting the oversight and regulatory enforcement of wireless IoT applications, how can these be overcome, and how can monitoring contribute?

This study is mainly concerned with impact related to three core tasks of the Dutch Radiocommunications agency: (1) ensuring that spectrum is managed between applications and is used effectively, (2) to ensure adherence of spectrum usage to regulations through monitoring and enforcement, and (3) to ensure the reliability of critical (wireless) infrastructure.

Findings

Long-range, large scale deployments of IoT networks have the highest impact on the spectrum. The main technologies for LPWA (low-power, wide area) IoT in licensed spectrum are LTE-M1 (LTE Cat MTC), LTE-M2 (NB-IoT) and (future) 5G IoT. In unlicensed spectrum, LoRaWAN (based on spread spectrum) and SIGFOX (ultra narrowband) are the most prominent technologies for LPWA IoT that are currently being deployed in the Netherlands.

We are expecting very fierce competition between the licensed and unlicensed technology families, where the main contention points will be (1) price of device, (2) time to market and (European, countrywide) network coverage, and (3) reliability and security. We do not expect the market to standardize on either solution. We also expect different technologies for LPWA IoT to co-exist in unlicensed bands for the near future.

Based on our analysis we expect that there will be between 8.6 and 52.1 million LPWA devices in the Netherlands in 2024. Most of the devices are expected to be in the categories *agriculture and environment* and *smart buildings.* Monitoring the trade flows of these devices will not be an easy task due to the diverse supply chains of LPWA IoT devices.

Deployment of LPWA IoT networks in licensed spectrum is expected to be gradual and smooth. Neither LTE-M1 nor LTE-M2 appear to be bound by concurrent usage issues, as these standards provide very good means for power control and concurrent access. The situation regarding IoT networks in unlicensed spectrum below 1 GHz is much more complex. The 863-870 MHz band, in particular the frequencies around 868 MHz, appear to be very popular for all technologies currently deployed at scale.

The impact of short range IoT usage in unlicensed spectrum is expected to be limited: a very high level of frequency re-use is possible for short range applications. The regulatory framework may however not be adequate in the light of large-scale deployments of long-range technologies, such as for LPWA IoT. Two new scenarios of interference are of particular interest:

[1] The Internet of Things is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. [33]

- The scenario where short range devices are close to a base station of a long range network, and cause interference that harms long range communication in the whole long range cell.
- A scenario where there is interference between different long range technologies in the same spectrum.

At the wider scale, monitoring is an instrument that provides information on the overall health of the spectrum with respect to its intended usage. At the more local level, monitoring can be used as a tool to troubleshoot local problems, or (by sampling various locations) to obtain a more detailed view on the spectrum health.

Conclusions

Which issues will be caused by the utilisation of spectrum below 1 GHz by wireless IoT applications, and what are possible solutions for overcoming these issues?

- We expect that the currently available spectrum is sufficient to handle the expected connectivity demand for wireless IoT.
- The use of unlicensed spectrum for mission-critical communications presents a risk with respect to televulnerability.
- Many short-range IoT applications do not necessarily need to use spectrum below 1 GHz.
- LPWA IoT networks in the unlicensed bands are limited in efficiency due to the fact that current duty cycle regulations limit the downlink capacity and hence the network to perform e.g. power control.
- The usage of different kinds of technology for LPWA IoT in unlicensed spectrum leads to additional interference and suboptimal usage of the spectrum.

What are obstacles affecting monitoring and enforcement of wireless IoT applications, how can these be overcome, and how can monitoring contribute in solving this issues?

- Problems resulting from interference with and between LPWA IoT transmissions will be primarily local and intermittent.
- Monitoring trade flows of devices containing LPWA IoT technology is difficult due to the diversity of supply chains.
- We expect interference from IoT devices that are imported from countries outside of Europe, and use the 902-928 MHz band, on current applications in that spectrum.
- Traditional monitoring instruments can, to a limited extent, be reconfigured for monitoring wireless IoT spectrum usage. We suggest augmenting traditional monitoring with monitoring based on IoT network operator data, SDR nodes, and specialised IoT monitoring nodes.

Recommendations

- We recommend the Dutch Radiocommunications Agency to instruct operators and user groups to educate (potential) users of IoT LPWA connectivity in unlicensed spectrum about the possible (future) risks regarding availability and reliability.
- Operators of LPWA IoT networks in unlicensed spectrum should be encouraged to further densify their network.
- We recommend the Agency to investigate the possibilities for using data from the IoT network operators for monitoring purposes.
- We recommend the Agency not to allocate additional spectrum for LPWA IoT at this point.

Managementsamenvatting

In deze studie wordt de huidige en toekomstige impact van draadloze *Internet of Things*[2] (IoT)-connectiviteit op het radiospectrum geanalyseerd. De hoofdvragen voor het onderzoek zijn:

1. Welke knelpunten worden veroorzaakt door het gebruik van spectrum onder de 1 GHz door draadloze IoT-toepassingen, en wat zijn mogelijke oplossingen hiervoor?

2. Welke knelpunten zijn er te identificeren bij het toezicht op IoT toepassingen, welke oplossingen zijn hiervoor, en wat is de rol van monitoring daarbij?

Deze studie betreft voornamelijk impact die relevant is ten aanzien van de drie kerntaken van het Agentschap Telecom (AT): (1) spectrummanagement, (2) toezicht op spectrumgebruik, en (3) het waarborgen van de betrouwbaarheid van kritieke (draadloze) infrastructuur.

Bevindingen

Grootschalige IoT-netwerken met hoog bereik hebben de grootste impact op het spectrum. De belangrijkste technologieën voor LPWA (laag vermogen, hoog bereik) IoT-connectiviteit in gelicenseerd spectrum zijn LTE-M1 (LTE Cat. MTC), LTE-M2 (NB-IoT) en toekomstige 5G IoT-technologie. In ongelicenseerd spectrum zijn LoRaWAN (gebaseerd op spread-spectrum-technologie) en SIGFOX (ultra-narrowband) de belangrijkste technologieën, welke op dit moment in Nederland tevens op grote schaal zijn uitgerold.

We verwachten sterke competitie tussen gelicenseerde en ongelicenseerde technologieën, waarbij (1) prijs van devices, (2) time-to-market en (Europese, landelijke) dekking, en (3) betrouwbaarheid en veiligheid de belangrijkste twistpunten zijn. We verwachten niet dat de markt standardiseert op een van beide oplossingen. We voorzien dat in de ongelicenseerde band verschillende technologieën voor LPWA IoT naast elkaar zullen blijven bestaan.

We verwachten dat er tegen 2024 in Nederland tussen 8.6 en 52.1 miljoen LPWA IoT-devices zullen zijn. Het merendeel van deze devices zal een toepassing vervullen in de agricultuur en 'smart building'-categorieën. Het monitoren van de handelsstromen van de devices is geen eenvoudige taak, omdat de waardeketens van de LPWA IoT-devices zeer divers zijn.

We verwachten dat de uitrol van LPWA IoT-connectiviteit in de gelicenseerde banden geleidelijk verloopt. Doordat de LTE-M1 en LTE-M2-standaarden voorzien in goede mogelijkheden voor power control en gelijktijdige toegang lopen deze netwerken voorlopig niet tegen knelpunten aan ten aanzien van gelijktijdig gebruik. Voor technologieën in ongelicenseerd spectrum verwachten we dat wel. De 863-870 MHz band, specifiek enkele frequenties rondom 868 MHz, blijken het meest populair voor deze technologieën.

We verwachten dat de impact van *short range* inzet van wireless IoT beperkt is: er is binnen de huidige reguleringskaders bij gebruik op korte afstanden en met lage vermogens een zeer hoge mate van hergebruik van spectrum mogelijk. Grootschalige LPWA IoT-netwerken worden wel beperkt door de reguleringskaders. Twee scenario's met betrekking tot interferentie zijn hierbij relevant:

---

[2] Het Internet of Things is een wereldwijde infrastructuur voor de informatiesamenleving, die geavanceerde diensten mogelijk maakt door het verbinden van (fysieke en virtuele) dingen, gebaseerd op bestaande en evolverende, interoperabele informatie- en communicatietechnologie. [33]

- Het scenario waarbij een *short range* device zich dichtbij het basisstation van een *long range* netwerk bevindt, en interferentie veroorzaakt die connectiviteit in de hele netwerkcel beperkt;
- Het scenario waarbij er interferentie plaatsvindt tussen verschillende typen *long range* technologieën binnen hetzelfde spectrum.

Op hoog aggregatieniveau kan met monitoringinstrumenten een beeld worden vekregen van het spectrumgebruik in relatie tot het beoogde gebruik. Op meer lokaal niveau kunnen met monitoringinstrumenten problemen worden opgelost en een meer gedetailleerd beeld worden geschetst van het spectrumgebruik.

Conclusies

Welke knelpunten worden veroorzaakt door het gebruik van spectrum onder de 1 GHz door draadloze IoT-toepassingen, en wat zijn mogelijke oplossingen hiervoor?

- We verwachten dat het nu beschikbare spectrum afdoende is om aan de verwachte vraag voor draadloze IoT-connectiviteit te voldoen.
- Het gebruik van ongelicenseerd spectrum voor kritieke toepassingen levert risico's op ten aanzien van telekwetsbaarheid.
- Voor veel *short range* IoT-toepassingen is er geen noodzaak om spectrum onder de 1 GHz te gebruiken.
- LPWA IoT-netwerken in ongelicenseerd spectrum worden beperkt in hun efficiëntie door huidige regulering ten aanzien van duty cycle. Dit komt omdat hierdoor de capaciteit in het downlinkkanaal wordt beperkt, waardoor de netwerken minder goed in staat zijn om (bijvoorbeeld) aan *power control* te doen.
- Het gebruik van verschillende technologieën voor LPWA IoT binnen hetzelfde ongelicenseerde spectrum leidt tot nieuwe interferentiescenario's en suboptimaal gebruik van het spectrum.

Welke knelpunten zijn er te identificeren bij het toezicht op IoT toepassingen, welke oplossingen zijn hiervoor, en wat is de rol van monitoring daarbij?

- Eventuele problemen die het gevolg zijn van interferentie tussen en met LPWA IoT-transmissies zullen primair lokaal en intermitterend zijn.
- De grote diversiteit in de waardeketens voor IoT-devices maakt het monitoren van handelsstromen zeer lastig.
- We verwachten interferentie van IoT-devices die worden geimporteerd uit regio's buiten Europa, en daardoor gebruik maken van de 902-928 MHz frequentieband, op de huidige toepassingen in die band.
- Traditionele monitoringinstrumenten kunnen, tot op zekere hoogte, worden gebruikt voor monitoring van draadloze IoT-toepassingen. We stellen voor om deze instrumenten aan te vullen met monitoring gebaseerd op data van IoT netwerkoperatoren, SDR-nodes, en gespecialiseerde IoT-monitoringnodes.

Beleidsaanbevelingen

- We bevelen het AT aan om operatoren en gebruikersgroepen te instrueren om (potentiële) gebruikers van IoT LPWA in ongelicenseerd spectrum voor te lichten over de risico's ten aanzien van beschikbaarheid en betrouwbaarheid.
- Operatoren van LPWA IoT-netwerken in ongelicenseerd spectrum moeten worden aangemoedigd om hun netwerk verder te vermazen.
- We raden het AT aan te onderzoeken of gegevens van IoT-netwerkoperatoren kunnen worden gebruikt ter ondersteuning van haar taken.

- We adviseren het AT om op dit moment geen aanvullend spectrum voor LPWA IoT te alloceren.

Table of contents

1 Introduction

In this study, we analyse the current and future impact of wireless IoT connectivity on the radio spectrum. The results support policy decisions on allocation, regulation, monitoring and enforcement of spectrum usage. The Dutch Radiocommunications Agency has formulated the following main questions for this study:

1. Which issues will be caused by the utilisation of spectrum below 1 GHz by wireless IoT applications, and what are possible solutions for overcoming these issues?

2. What are obstacles affecting the oversight and regulatory enforcement of wireless IoT applications, how can these be overcome, and how can monitoring contribute?

The main questions are further detailed into the following sub questions:

1. What will be the demand for spectrum below 1 GHz for wireless IoT applications, and how can this be demonstrated?

2. Are there opportunities for increasing the efficiency of spectrum utilisation of wireless IoT applications, in order to reduce the load on the spectrum?

3. What are the consequences for current users of a frequency band when the band is opened up for wireless IoT applications?

4. How can spectrum utilisation by wireless IoT devices be monitored? Given different levels of scale (wide, metropolitan, personal and local area), what is the best monitoring approach at each level? How can these approaches be embedded in the current monitoring processes for short-range devices?

5. How can trade flows of wireless IoT devices be mapped? How can regulatory bodies become aware of illegitimate wireless IoT devices as early as possible?

1.1 Context

IoT has experienced a considerable growth over the last year. The role of wireless communication is key in this process. IoT is used for smart meters [21] [37] [91], street lights [72], monitoring crops [38] and connecting cars [10]. Connecting all these things to the internet via a fixed internet cable is often not possible and, in many cases, not economically feasible. Wireless communication is more flexible and, following the introduction of specialised hardware components, in many cases less expensive.

There are several reasons to start looking into wireless IoT connectivity. In this paragraph we list the most important concerns, and how they relate to IoT applications.

Usage of unlicensed spectrum for critical applications

As current mobile networks do not yet provide a suitable solution for connecting very low-power devices, connectivity options that do meet the requirements have arisen in unlicensed spectrum. In the Netherlands, there are now two (nationwide) deployments of LoRa and one nationwide deployment of SIGFOX, co-existing in the same frequency band. As both technologies have not yet reached widespread use, there do not yet seem to be many issues regarding interference. However, it is expected that if the number of devices on the networks increases, so will interference. There are also concerns regarding the capacity of the networks themselves.

There is a concern that users who adopt LoRa or SIGFOX based devices will at first experience a well-working network, but will later run into serious problems as the networks grow in popularity, and the unlicensed band becomes congested. Locally, various other uses of the unlicensed spectrum may cause additional issues with LoRa and SIGFOX, while these technologies may initially appear to provide highly reliable communications. Operators themselves indicate that they will not and cannot offer SLAs on connectivity over unlicensed bands. [71]

While LoRa and SIGFOX could also be deployed and used in private bands, these are different between countries. The operators of the LoRa and SIGFOX networks that are currently deployed rely on the fact that the unlicensed band is harmonised over multiple countries, because it (1) lowers device costs as there are less different bands to support, and (2) allows for seamless roaming between countries, which is important for use cases such as international 'track and trace'.

Competing, incompatible technologies in unlicensed spectrum

Competition between networks is seen as positive from an economic point of view. However, for networks in the unlicensed frequency bands, competition between a large number of players and different kinds of technology may actually lead to the least favourable outcome, where none of the networks performs as desired. There is a strong suspicion that spread-spectrum based technologies (such as LoRa) and ultra-narrowband technologies (such as SIGFOX) are not 'good neighbours' in scenarios with a large number of nodes.

Short range technology being applied for long range

Of particular interest are *low power wide-area (wireless access) networks* (LPWA) for IoT. An LPWA network is designed to allow wireless long range communications at low power levels. LPWA networks are typically designed to connect devices and actuators that need to operate for a long time on limited power supply, and that require only very low bit rate communications. [30] With LPWA IoT, we refer to LPWA technologies and networks that are specifically designed to facilitate connectivity with the internet (or to private networks, but using internet technologies) and are called LPWA IoT networks.

While LPWA IoT networks typically transmit over long distances, some of the available LPWA technologies do use short range frequency bands. Using technology with extremely large link budgets and well-placed base stations, the networks are able to achieve long distance communications while adhering to short range regulations. This appears to be in contradiction with the definition of 'short range device' as used by CEPT and ETSI, which *"is intended to cover the radio transmitters which provide either unidirectional or bi-directional communication which have low capability of causing interference to other radio equipment"*. (ERC Recommendation 70-03, [15])

LoRa and SIGFOX are examples of technologies that stretch the limits of frequency bands that were initially intended for short range applications to realise long range coverage. This is achieved by using technology that allows for large link budgets, and by using relatively high-placed base stations. As a consequence, a single short-range device transmitting at the same power (or higher power, in the case of RFID readers) with a line of sight to a base station has the potential to disrupt all communications to that base station.

Another issue is power control. Regulations for usage of the unlicensed bands imposes limits on the maximum duty cycle (e.g. the amount of time it is allowed to send compared to the amount of time it is required to remain 'silent') of a single transmitter. In the long-range networks, the restrictions apply equally to the devices as well as the base stations. Nevertheless, the base stations are expected to communicate with a very large number of devices (for downlink traffic) as well as the need for additional 'air time' to transmit power control commands. Therefore, such networks are much worse at managing power than their licensed counterparts.

1.2 Reading guide

We start out in chapter 2 by describing the methodology employed to answer the research questions. In chapter 3 we will briefly introduce the different relevant platforms and technologies for wireless IoT. In chapter 4, we discuss the demand for wireless IoT connectivity in terms of device volume. In chapter 5, the different technologies are analysed with respect to spectral efficiency, which leads to an outlook on IoT connectivity capacity. In chapter 6, we discuss potential interference issues and the role of monitoring for enforcement. Finally, in chapter 7, we summarize our findings as answers to the research questions.

Throughout the report, references to literature are displayed between brackets. A list of references as well as a glossary explaining abbreviations can be found at the end of the report.

2 Research methodology

Figure 1 provides a schematic overview of the research methodology employed in this study. The main objective of this study is to analyse the impact of wireless IoT on the spectrum. The impact is a function of demand (from devices that require connectivity) and supply (the networks and technology that can provide said connectivity). Both are modelled separately, and then combined geographically to model impact.

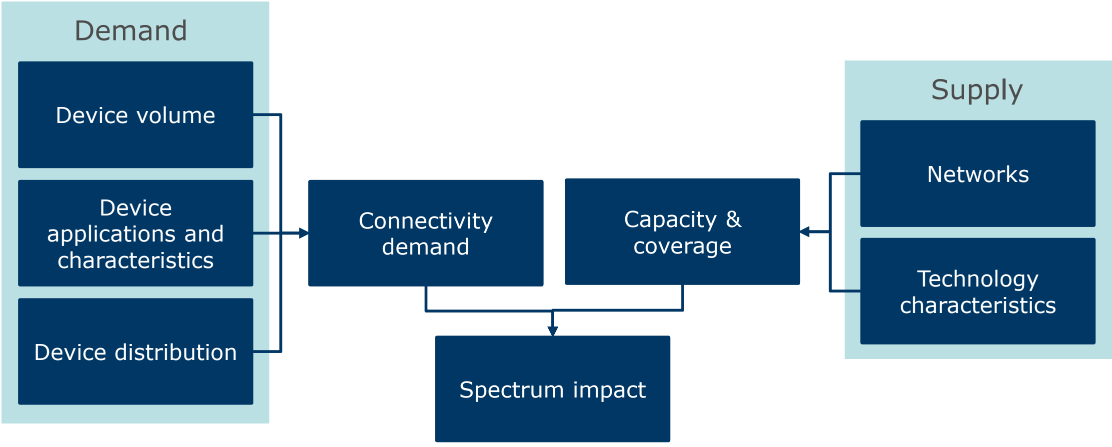

Figure 1 Schematic overview of research methodology

2.1 Modelling demand

Figure 2 gives an overview of the methodology used for modelling the demand side. From literature, we obtain projections for device volumes and the distribution of devices over applications. This leads to absolute estimates of devices per application. From statistical and topographical data, we distribute the devices geographically over the Netherlands. The model includes various assumptions that translate the statistical data to device distributions, in the form of "x% of households will have a device of type Z" that are based on literature. Infrastructural data is used for certain kinds of devices (e.g. street lighting, cars, et cetera). Based on the distribution data, devices are spread out over the map, based on the geographical distribution data. This data set then contains individual devices, which can be mapped to network coverage in the following step.

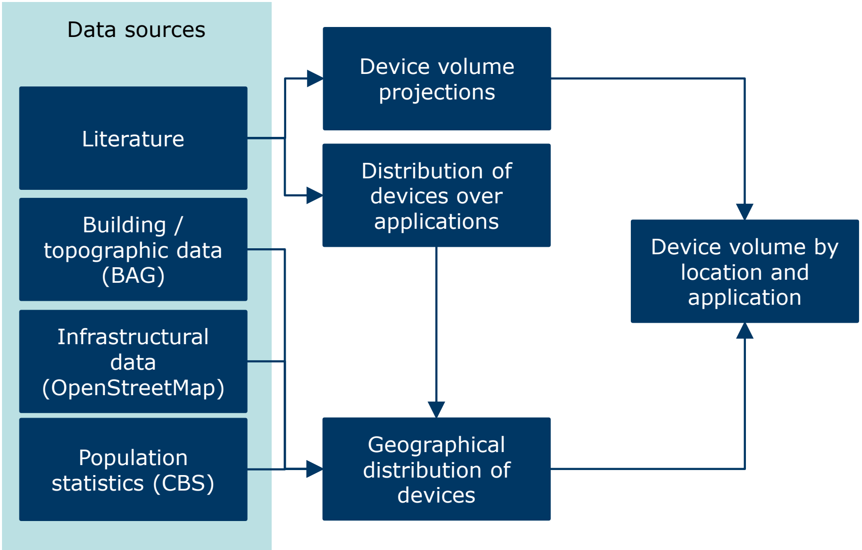

Figure 2 Schematic overview of the methodology used for modelling the device volume

In our modelling, we distinguished different types of applications. The specific way in which devices were modelled in the main categories is discussed below.

Smart buildings

For modelling the *smart building* device category we used the municipal database of addresses and buildings (*Basisregistraties Adressen en Gebouwen* (BAG)). The BAG contains all the addresses and buildings in the Netherlands including their coordinates. We randomly selected addresses from the BAG and simulated placement of a device within a range of 5 meters of the coordinates of the address. The offset was used to spread the devices through a house.

Agriculture and environment

The *agriculture and environment* devices are modelled based on the type of land in a location. OpenStreetMap provides a map of the Netherlands where every location is classified based on the type of land. To model the devices we selected all the relevant types of land such as farm, grass, farmland, meadow and orchard. One problem was that some of these types of land could occur within cities (for instance, grass), whereas devices within city boundaries are classified as 'smart city' devices. Therefore we used the information of the Statistics Netherlands (CBS) about the location of municipalities to exclude all the *agriculture and environment* land within city centres.

Utility

For modelling the *utility* devices we used the addresses from the BAG again. We randomly selected addresses and used their coordinates to plot a utility device. Contrary to the *smart building* devices we did not apply an additional offset to the location.

Consumers

For modelling the *consumer* devices we also used the BAG. We again randomly selected addresses from the BAG and placed a *consumer* device within 20 meters of the address. The range is wider than for smart building devices, as these devices (such as bikes and pet tracking devices) are more likely to be outside the building than inside.

Logistics

The logistics devices are modelled based on the map of OpenStreetMap that contains all the roads in the Netherlands. We randomly placed *logistics* devices along the roads contained in OpenStreetMap. We did not make a distinction between the different types of roads such as highways or streets.

Smart cities

The *smart city* devices fall apart in two categories: *street lighting* and *parking and waste*. We therefore used both data from the OpenStreetMap and CBS. For the street lighting we used the roads map from OpenStreetMap, which we again used to randomly add devices along the way.

For modelling the *parking and waste devices* we only used the roads from OpenStreetMap located in the city centres. These devices are expected to be in the city centres, because they have often a shortage of parking spots and can benefit the most of a better waste management.

Industrial

For modelling the industrial devices we used the BAG again. In the BAG each address is assigned to one or multiple functions. An address can for instance have a residential function, industrial function or educational function (or even both a residential and industrial function). We selected only the addresses from the BAG with an industrial function and used their coordinates to randomly place devices.

Indoor/outdoor

Because coverage of LPWA IoT networks differs greatly between indoor and outdoor, devices need to be classified into either category. In Table 1 each type of device is assigned to either outdoor or indoor.

Table 1 Classification of devices to indoor or outdoor based on application

Type	Indoor/outdoor
Smart buildings	Indoor
Agriculture and environment	Outdoor
Utility	Indoor
Consumers	Indoor
Logistics	Outdoor
Smart cities	Outdoor
Industrial	Indoor

Note that due to the sheer size of the resulting data set, we used random sampling on the data sets to generate particular results.

2.1.1 Trade flows

Besides modelling the projected demand of the IoT-devices we also make an attempt to identify the trade flows for IoT devices. Our approach for identifying trade flows starts out with desk research, starting from the different currently deployed IoT LPWA platforms (such as Aerea and The Things Network). From this starting point we compiled a list of different stakeholders, such as chip and module manufacturers, and their roles. This information was then used for determining the trade flows and relevant stakeholders.

2.2 Modelling supply

For the purposes of this study, we modelled the current and (potential) future coverage and capacity of the relevant LPWA IoT networks in the Netherlands. The coverage estimation is primarily based on the structure of the network.

Reasoning about capacity

The concept of *capacity* in the context of (public) wireless telecommunications networks refers to the total amount of data that can be transmitted or received over the access part of such a network. Capacity can be calculated either from a given location, or as an aggregate average over a larger area. Capacity is determined by three aspects, as is shown in Figure 3.

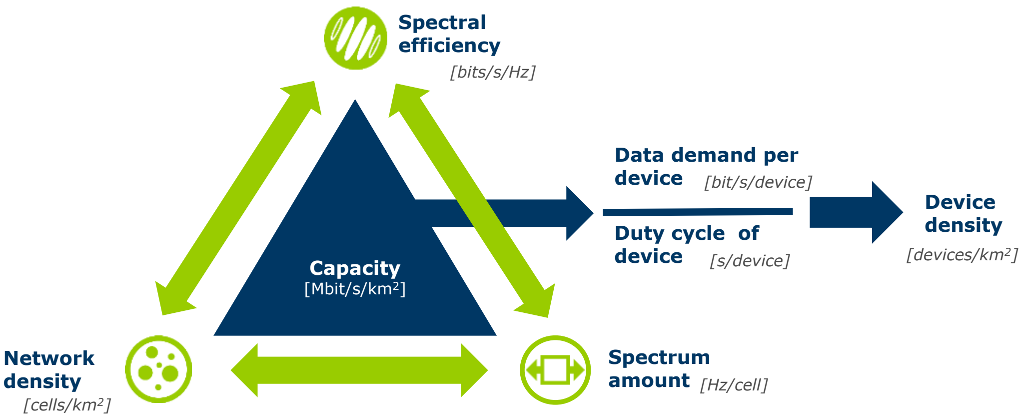

Figure 3 The relationship between network density, spectral efficiency, amount of spectrum and capacity

The amount of spectrum that is required to transfer an amount of data depends on the *spectral efficiency*[3] of the technology used for transmission, as well as the specific configuration of the network and user equipment. The capacity at a given location can be increased either by increasing the amount of spectrum used, or by employing a more spectrally efficient technology, which can simply send more data given the same amount of spectrum. The total capacity available at a particular location is always shared with other users connected to the same base station: the area served by a single base station is called a 'cell'. Making cells smaller therefore is another way of improving capacity, as it reduces the number of users that share the same capacity.

The size of a LoRaWAN or LTE cell is determined by the distance that the radio signals can travel before they become too 'weak' to be properly received and interpreted. Using a radio signal propagation model we estimate the area within which the signal strength for LoRa and LTE is within operational limits, as they are defined in the LoRa standard as well as confirmed

[3] Note that in this report, *spectral efficiency* refers to the efficiency of a *single* technology or application in isolation. Spectral efficiency can also be analysed at the systems level, where it refers to the efficiency of spectrum usage by *all* applications operating in a certain spectrum, including interaction effects between applications that reduce practical spectral efficiency to levels lower than the spectral efficiency of a technology/application in isolation.

during field tests. [62] The propagation model used is the Hata-Okumura COST 321-model.[4] The Hata-Okumura model takes receiver height, base station height, signal path length, transmit power and centre frequency as input, and calculates the median path loss (in dB) to be expected over that propagation path. For our purposes, the model was inverted to calculate the maximum distance at which the median path loss is still above a certain value. The software used to calculate network coverage using these models was developed earlier by Dialogic and Inwilution for the Dutch Radiocommunications Agency, originally to calculate the capacity of GSM, UMTS and LTE networks. [14]

Modelling LTE capacity

For LTE-based networks, we used the exact methodology as detailed in [14], with minor adjustments following from the specific characteristics of LTE-M1 and LTE-M2. For LTE, the minimum signal level is -115 dBm measured for a subcarrier.[5] LTE-M provides an increased link budget (e.g. between 11.5 – 20 dB) which allows for weaker signals (and therefore provides better coverage). However, LTE-M devices may transmit at lower transmit power to conserve energy. [36]

The Dutch antenna registry contains detailed information about antennas for LTE. Data about base stations in The Things Network are freely available from the website of The Things Network. KPN does not publish data, but did indicate that it would re-use sites in their mobile networks. From the Dutch antenna registry, we hence selected the top x highest[6] sites operated by KPN and having LTE-20 antennas, and assumed a LoRa deployment close to existing LTE antennas.

Modelling LoRaWAN capacity

For LoRaWAN, the minimum signal strength depends on the level of error correction employed. The LoRaWAN standard defines several 'modulation levels' which provide different levels of error correction. Error correction improves the odds of a message being interpretable by the receiver, but comes at the cost of adding redundancy, which reduces the amount of useful information that can be transmitted given the same spectrum usage level.

The signal strength at the receiver is diminished by signal strength losses accrued by the signal in transit ('path loss'). The maximum acceptable path loss values were varied between different scenarios. The base scenario was chosen to be outdoor LoRa coverage using SF7 modulation – this requires a minimum signal strength of -137 dBm at the receiver. A second scenario is where the current network provides *indoor* LoRa coverage, at SF12 modulation. The latter requires a minimum signal strength of -123 dBm at the receiver. Both scenarios were also calculated with expanded networks (i.e. more base stations). Additionally, all scenarios were calculated assuming either a single, omnidirectional antenna at each site, or

---

[4] An overview of and comparison between propagation models is given in [59]. The Hata-Okumura model was chosen because it is relatively simple (e.g. compared to [16]) works reasonably well in both the LTE and LPWA IoT scenarios under study here. Note that while Hata-Okumura cannot be used to estimate median path loss on link distances shorter than 1 kilometre, we do not expect such to occur in these scenarios.

[5] See [14]. The average signal level for an LTE subcarrier must be above -115 dBm. An LTE deployment in 10 MHz of spectrum has 601 subcarriers. Therefore a single carrier has a signal strength 27,8 dB below the total power of the band.

[6] Antennas registered with exactly the same coordinates were considered a 'site'. Operators generally register exactly equal coordinates when antennas are on the same pole. In most cases, a single site has three antennas for a particular band, which may be at different heights. The average height of all antennas at a site was used as the reference height.

sectoral antennas at each site (in the case of KPN, we assumed the configuration of its LTE-20 deployment for LoRa). For LoRa we further assume a centre frequency of 868 MHz, and transmit power at 14 dBm EIRP.

For both technologies we assume a receiver height of 1.5 metres, For LTE, the software tool assumes 'perfect' power control and hence separation between cells. For LoRa, power control was assumed to be imperfect and coverage cells overlap. For modelling outdoor conditions, we use the 'open area' flavour of the Hata-Okumura model for outdoor modelling, which is most appropriate given the topography of the Netherlands. For modelling indoor conditions, we use the 'urban' flavour of the Hata-Okumura model, adding an additional path loss of 13.2 dB resulting from the device being indoors.

3 Platforms and networks

In this chapter, we describe the networks for LPWA (low-power, wide-area, wireless access) IoT connectivity that currently exist or are expected to be deployed in the Netherlands during the time horizon of this study (five years).

3.1 What is the wireless IoT?

ITU defines the Internet of Things (IoT) as *a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.* [33] A key aspect of the IoT is that it creates a mirrored, digital representation of physical objects, as depicted in Figure 4. Due to the nature of the devices as well as the applications envisioned for the IoT, it is expected that a significant portion of the connections that make up the IoT will be wireless.

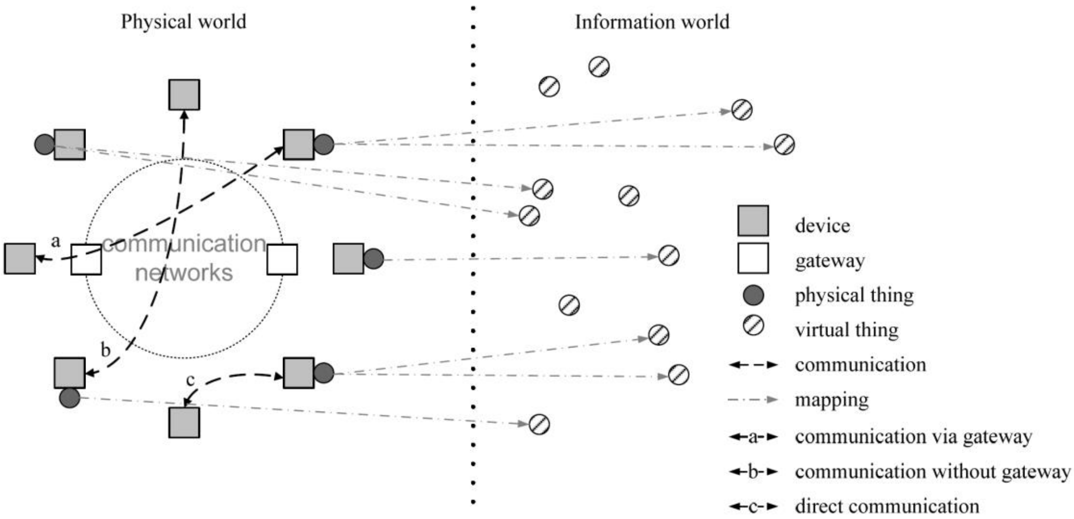

Figure 4 Technical overview of the Internet of Things, as defined by ITU. [33]

In a report published late 2015, Stratix provides an overview of technologies most likely to be implemented in the Netherlands to meet the demand for IoT connectivity. Stratix distinguishes different levels of scale, ranging from *personal* and *local* to *metropolitan* and *wide* area networks. The report also describes back-end platforms and other elements of the IoT value chain. [65] Figure 5 gives an overview of different technologies for IoT connectivity, ordered by scope (wide area vs. local area) and spectrum type. In the report of Stratix the technical description of all the non-LPWA technologies can be found.

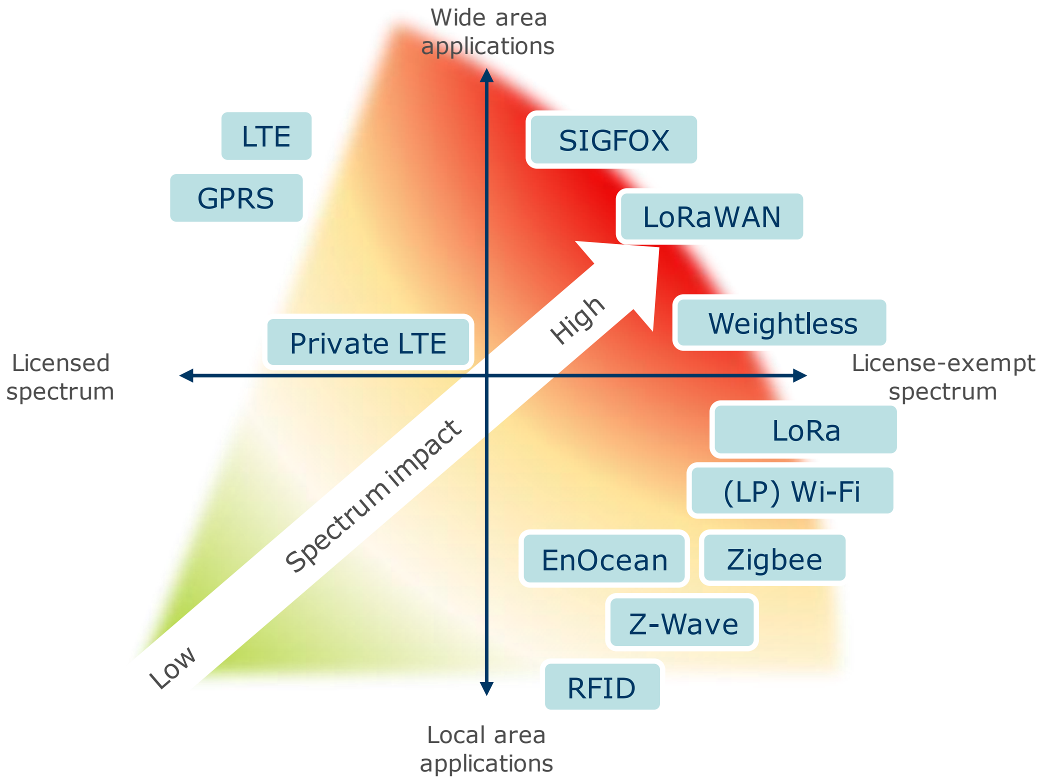

Figure 5 Overview of technologies for wireless IoT connectivity, by spectrum type and scope

In this study, we are mainly concerned with those technologies and deployments that may have consequences related to three core tasks of the Dutch Radiocommunications agency: (1) ensuring that spectrum is managed between applications and is used effectively, (2) to ensure adherence of spectrum usage to regulations through monitoring and enforcement, and (3) to ensure the reliability of critical (wireless) infrastructure. We are therefore focusing on the radio access part of IoT connectivity solutions. Second, we limit our scope (at least in this chapter) to the 'newcomers'. Third, and most importantly, we focus on those deployments that have the potential to either encounter a capacity issue, or the potential to run into interference.

In our description of platforms and networks for LPWA IoT connectivity, we make a clear distinction between deployments in licensed and deployments in unlicensed spectrum. First of all, the two types of deployments vary greatly in the dynamic regarding technology selection and adoption. While both are driven by standardization processes and backed by large companies, there appears to be a much greater level of consensus about the road forward for licensed deployments than for unlicensed deployments, where several new players are entering the market and pushing their (proprietary) technologies.

3.2 IoT LPWA in licensed spectrum

In licensed spectrum, IoT LPWA standards are primarily developed and implemented by the organisations that are already involved in the development and implementation of mobile networks. For operators of mobile networks and vendors of mobile network equipment, the existing platforms provide a good starting point for provisioning LPWA IoT connectivity. The main technical engineering challenges are to allow the existing standards to work in low-power use cases, while maintaining as much compatibility with, and as much as the performance of existing standards as possible.

Development of mobile-based LPWA IoT connectivity is focused on the following design goals:

- Simplifying standards and thereby hardware requirements, to allow devices to be built at a cost lower than $5.
- Providing long-range coverage, even more so than existing mobile networks, at the expense of data throughput.
- Providing low-power operation, such that a device will be able to operate for 10 years on a single battery given it transmits only a few messages per day.

The main technologies for LPWA IoT in licensed spectrum are those currently developed or under development by the 3GPP. These technologies are designed as add-ons to currently existing mobile cellular networks, employing parts of spectrum currently allocated to these networks. The first addition to the LTE standard in the direction of LPWA IoT connectivity are the 'category 1' (introduced in Release 8) and 'category 0' (Release 12) device categories. These categories define profiles for low-power, low-cost devices with reduced connectivity needs.

As the cost, power and connectivity of category 0 and category 1 device profiles still exceeds the typical requirements for true IoT devices, new standards are in development aimed at even lower cost, lower power and lower bitrate scenarios. Currently there are two separate tracks of standardization within 3GPP regarding cellular LPWA IoT, of which the technology is usable within the time horizon for this study. Both are evolutions of current LTE technology under the label 'LTE Category M', which comes in two flavours:

- **LTE-M1.** LTE-M1 is an evolutionary upgrade for LTE, which provides an LTE compatible RAN technology optimized for LPWA IoT. LTE-M1 was first released in 3GPP Release 12 in Q4 2014, and is also known as LTE *Cat MTC*. [28] Further optimizations (e.g. regarding control of device sleep) will be included in Release 13, whose specifications were completed in Q1 2016.

- **LTE-M2.** 3GPP RAN Release 13 contains a new narrowband radio interface, officially referred to as 'LTE Category NB1', and also (previously) known as 'Narrowband 1' and 'NB-IoT'. [28] Standardization started in Q4 2015 with specifications to be completed by Q2 2016. Two solutions were being proposed: (1) a solution based on narrow-band FDMA in the uplink and narrow-band OFDMA in the downlink, and (2) a 200 kHz narrow-band evolution of LTE. [45]

  In June 2016 the LTE-M2 proposal has been approved for 3GPP Release 13, with the following improvements over LTE-M1:

  - Reduced device bandwidth of 200 kHz in downlink and uplink
  - Reduced throughput based on single PRB operation
  - Provide LTE coverage improvement corresponding to 15-20 dB compared to regular LTE[7] [45]

[7] According to Nokia, *"coverage is increased by simply operating in 200 kHz or 1.4 MHz compared to 20 MHz; yielding 20 dB and 11.5 dB improvement respectively. LTE-M further allows output power to be reduced by 3 dB for lower implementation cost. Furthermore, control and data signals can be repeated to reach the required coverage enhancements."* [45]

Table 2 provides an overview of the different 3GPP LTE RAN standards relevant for M2M and IoT connectivity. In addition to the above, there is ongoing standardization work for 5G, which consists of the next generation of technology after LTE-M1 and LTE-M2. The focus in 5G is on the usage of higher frequency bands and new forms of orthogonal frequency-division multiplexing (OFDM). The ITU hopes to standardize 5G in 2020, but the technologies related to IoT are expected to only become usable at a large-scale by 2022. [66] [77] Early phase 5G deployments focus on the use of very high frequency bands to provide high throughputs. Therefore, we are not including them in this study.

Table 2 Overview of the different LTE RAN standards and device categories for M2M and IoT [56]

Parameter	Release 8 LTE Cat-4	Release 8 LTE Cat-1	Release 12 LTE Cat-0	Release 13 LTE-M1	Release 13 LTE-M2
Downlink peak rate (Mbps)	150	10	1	<1	~0.2
Uplink peak rate (Mbps)	50	5	1	<1	~0.2
Max. no. of down-link spatial layers	2	1	1	1	1
Number of UE RF receiver chains	2	2	1	1	1
Duplex mode	Full	Full	Half	Half	Half
UE receive band-width(MHz)	20	20	20	1.4	0.2

LTE-M1 can be deployed alongside current LTE deployments, as it simply uses resource blocks within an existing LTE carrier. For LTE-M1, these resource blocks are in-band and restricted to a designated 1.4 MHz sub band. LTE-M2 can be deployed either in-band (like LTE-M1, utilizing resource blocks in a 200 kHz sub band), in an LTE carrier guard band, or stand-alone (usually as a replacement of one or more GSM carriers). It would also be possible to deploy a stand-alone LTE-M2 carrier alongside a 3G band – this requires the 5 MHz wide 3G band to be ‘squeezed’ to 4.2 MHz. [46]

The migration from GSM-based machine-to-machine communication

There appears to be general consensus among (at least) Dutch mobile network operators that eventually, GSM and UMTS networks will be switched off in favour of LTE. This requires machine to machine equipment, which currently operates primarily over GSM, to migrate to LTE or one of the other IoT connectivity options.

The strategies of the different operators regarding this migration are varied in nature. KPN has indicated that it sees LoRa and (future) LTE-M1 based connectivity as a solution for different market segments, where LoRa serves the lower end and LTE-M1 serves the higher end, which is currently served by GSM. KPN expects the LoRa network to be operational for at least ten years. While heavily investing in LoRa, Orange has indicated that it sees LoRa primarily as a stop-gap measure *“as ETSI gets to grips with standardising cellular technology in the form of NB-IoT”*. [43]

Both Vodafone and T-Mobile have embraced LTE-M2. [69] [83] Vodafone sees LTE-M2 as the best technology for LPWA networks, due to the usage of licensed spectrum, availability of reliable bandwidth and the open standard.

In the context of migration from GSM, another development of interest is that of Extended Coverage GSM (EC-GSM). EC-GSM extends the coverage of existing GSM networks at the expense of throughput. EC-GSM is an evolutionary addition to GSM access network technology, which in June 2016 has been standardized in the 3GPP GERAN Release 13.

EC-GSM is mainly important for indoor deployments of devices, such as smart meters. In the Netherlands, smart meters are connected either over a CDMA450 based network, over GSM or LTE. The latter is (currently) operated by Vodafone, which is one of the frontrunners for LTE-M1 and LTE narrowband. We therefore do not expect EC-GSM to play a role of significance in the Dutch smart meter use case.

Roaming

For LTE-M1, the situation regarding international roaming is similar to that of 'normal' LTE. Operators will have to agree on roaming conditions and the devices will have to support different frequency bands between countries. While supporting different frequency bands will make devices slightly more expensive (compared to single-frequency devices), it is still our expectation that devices will generally support multiple frequencies. Recently, U-Blox introduced the first device module for LTE-NB (which, as we will see, is aimed at even less complex devices), which already supports three RF bands chosen such that the module can be used in most geographic regions. [81] The main engineering challenge is not the reception of signals at the different frequencies, but rather to implement filtering of signals on the device chipset in the cheapest way possible. LoRa and SIGFOX face a similar issue as they too operate in frequency bands that are relatively far apart (433 MHz and 868 MHz, for instance).

Localisation

The LTE-M1 standard does not provide specific support for time-of-arrival based localisation of devices. We expect that LTE-M1 devices will typically be equipped with a GPS receiver in order to provide highly accurate position measurements.

3.2.1 Future technologies

5G technology is due to be standardised by ITU in 2020 and consists of two main components:

- Use of higher frequency bands to achieve throughput of 10 Gbps
- Use of a new modulation[8] variant to allow for optimum combination of three very different types of traffic: broadband, IoT and V2X[9]. Currently various candidate technologies are being considered and evaluated in the 3GPP standardisation process.

A new modulation variant or alternative waveform can be used in the existing mobile bands and especially in the sub 1 GHz band to provide long range and access for a large number of devices

[8] Specifically an improved version of OFDM, which is the modulation technology currently used in LTE.

[9] V2X (Vehicle-to-X) is a term used to refer to vehicle-centric communications, either to other vehicles (V2V) or to infrastructure (V2I). V2X is a specific focus topic in 5G standardisation.

3.3 IoT LPWA in unlicensed spectrum

Unlicensed spectrum is a very attractive option for the deployment of IoT LPWA networks for several reasons. First, deployment in unlicensed spectrum is completely separated from existing operators of a mobile network operator, and is also an option for newcomers who do not currently own licensed spectrum suitable for deployment of LPWA IoT technologies. Second, the availability of harmonised unlicensed spectrum across different countries enables roaming[10] opportunities without requiring devices to support a large number of frequency bands. Third, unlicensed spectrum is often readily available at no cost, and also does not require the completion of lengthy procedures to acquire a license.

3.3.1 LoRaWAN

LoRa is short for Long Range and is promoted by the LoRa Alliance, an organisation whose members are among others KPN, Orange and Swisscom. The technology of LoRa is based on spread spectrum modulation and typically uses channels between 125 and 500 kHz wide. The focus of LoRa is on low bitrates, low costs for the devices, a long battery life and a large link budget (Figure 6). The latter is necessary to bridge long distances within the restrictions of the unlicensed spectrum.

The LoRaWAN specification defines medium access control (MAC) for large-scale public deployments of LoRa. For clarity, we will mention 'LoRa' whenever a statement applies to the technology disregarding deployment, and 'LoRaWAN' when a statement is specific to large-scale public deployment of LoRa using the LoRaWAN MAC protocol.

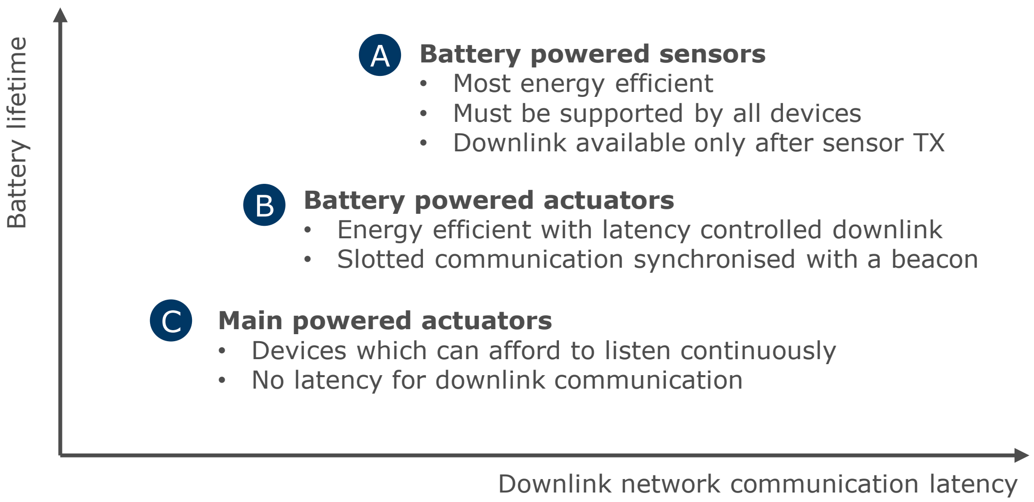

Figure 6 Types of devices distinguished in the LoRa standard [40]

LoRa can be used in multiple frequency bands but the current focus is on the 868 and 915 unlicensed bands. Within the 868 MHz band, LoRaWAN defines ten channels, of which eight can be used with different data rates (from 250 kbps to 5.5 kbps), a single high data rate channel (at 11 kbps) and a single FSK channel at 50 kbps. [40]

[10] The roaming situation for LPWA IoT networks in unlicensed spectrum is similar to the traditional situation in mobile networks: users can either take subscriptions on individual national platforms and 'roam' themselves, or they can take a subscription with an operator that has roaming agreements in place, allowing more seamless/automatic roaming.

ETSI regulations impose duty cycle restrictions (which, importantly, apply to both the base station as well as the device) and a maximum output power of 14 dBm (with the exception of the G3 band, which allows for 27 dBm). There are no restrictions on maximum transmission or channel dwell time. [40]

3.3.2 SIGFOX

SIGFOX uses ultra-narrow-band, instead of a spread spectrum based modulation as seen with LoRa. By choosing ultra-narrow channels with a width of about 100 Hz, SIGFOX creates a large number of channels within up to 1 or 2 MHz of unlicensed spectrum. Due to the use of Software Defined Radio receivers, the hardware requirements for devices are rather low, as an SDR receiver can receive an ultra-narrow channel even if it is slightly off-frequency.

3.4 Other wireless IoT technologies

Several other wireless technologies for IoT connectivity exist. These technologies are not discussed in depth in this study, as their impact on spectrum usage is limited by nature, and/or the technologies fulfil a very specific niche purpose, or the technologies are already in widespread use for non-IoT applications (e.g. Wi-Fi).

3.4.1 Very low power / radio-powered, near-field

RFID

RFID (Radio Frequency Identification) is a technology that is primarily intended to allow wireless, automated identification of objects, such as freight or identification cards. Bidirectional communication is also possible, for instance to perform transactions (e.g. with contactless payment or public transit cards). An RFID *tag* is a very small and low-cost radio transmitter that transmits information that can be related to the object it is attached to.

Active RFID tags are typically battery-powered and continuously or periodically transmit information, whereas passive RFID tags only transmit upon request, and typically do so using energy provided to it wirelessly by an RFID reader. In order to provide the energy required to the tag, an RFID reader has to transmit electromagnetic waves at relatively high power compared to typical power levels used for radiocommunications. RFID communication is typically very short ranged, from several centimetres to a metre (for passive RFID tags) to a few metres (for active RFID tags).

EnOcean

EnOcean is a technology for short range (30 – 300 metres) wireless IoT connectivity. Like RFID, it uses energy from radio waves to power a device’s transmitter, however unlike RFID, it collects the energy over a longer period of time. EnOcean can operate in various frequency bands, including 868 MHz (in Europe), 902 MHz (USA and Canada), 928 MHz (Japan) and 2.4 GHz (worldwide). EnOcean provides bi-directional communication and data rates up to 125 kbit/s, using ASK and FSK modulation. [22]

3.4.2 Low-power, small area

Bluetooth

Bluetooth is a wireless technology that allows short-range (10 - 100m) communications at low to medium speeds (1 – 3 Mbit/s) in unlicensed bands. Bluetooth was primarily intended as a ‘wire replacement’ technology for low-bandwidth accessories such as computer mice, phone headsets and car kits. The more recent Bluetooth ‘Smart’ (also known as Bluetooth ‘Low Energy’) standard provides Bluetooth functionality for devices that need to operate on low power, which is highly relevant for IoT applications. While the classical versions of Bluetooth operate using a frequency-hopping spread spectrum modulation, Bluetooth Smart operates using direct-sequence spread spectrum. [7]

Kleer

Kleer is a technology designed specifically for wireless streaming of lossless audio in simultaneous operation with Wi-Fi and Bluetooth in the 2.4 GHz ISM band. It was designed by Daimler for use inside cars, where end-user Wi-Fi and Bluetooth devices are present that would otherwise potentially disrupt audio streaming over Wi-Fi or Bluetooth. [50]

Mesh-based

ZigBee (IEEE 802.15.4) provides short-range connectivity for low-power, low-complexity devices. While the low power requirements limit the transmission distance for ZigBee to between 10 and 100 metres (line of sight), it provides communication over longer distances using *mesh networking*. In a mesh network, all nodes participate in routing and delivering traffic to its destination. Note that this also requires nodes to transmit and receive much more traffic than the node itself needs to transmit and receive.

3.4.3 High-power, short range

Wi-Fi

Wi-Fi (IEEE 802.11b/g/a/n/ac) is a technology family that facilitates short-range (typically up to 100 metres) broadband connectivity. Wi-Fi operates in the unlicensed 2.4 GHz and 5 GHz frequency bands, using channels of between 10 and 40 MHz wide. While Wi-Fi uses more energy and is more complex to implement than technologies such as LoRa and SIGFOX, it is still an interesting choice for IoT applications, mainly because Wi-Fi is widely deployed, and Wi-Fi technology is widely available. There are also various solutions on the market that allow for cheap and relatively easy integration of Wi-Fi capabilities in devices, such as modules based on the the popular esp8266 chip, providing Wi-Fi connectivity at less than $2 hardware cost. [25] Various initiatives exist to increase the range and/or decrease the power usage of Wi-Fi, further improving its suitability for IoT applications. [89]

3.4.4 Low-power, wide-area

Weightless

A frequently mentioned competitor for SIGFOX and LoRa is Weightless. Weightless is an open standard for LPWA IoT devised by the Weightless Special Interest Group (SIG). Table 3 shows the different variants of the Weightless standard.

Table 3 Overview of the different Weightless standards for LPWA IoT [86]

	Weightless-N	Weightless-P	Weightless-W
Directionality	1-way	2-way	2-way
Feature set	Simple	Full	Extensive
Range	5km+	2km+	5km+
Battery life	10 years	3-8 years	3-5 years
Terminal cost	Very low	Low	Low-medium
Network cost	Very low	Medium	Medium

Weightless-N is an open standard and uses an ultra-narrowband technology. It has a claimed range of several kilometres in urban environments and very lower power consumption. Weightless-N uses a different binary phase shift keying (DBPSK) digital modulation scheme to transmit within narrow frequency bands using a frequency hopping algorithm for interference mitigation. Weightless-N only allows for one-directional communication.

Weightless-P is presented as an ultra-high performance LPWA connectivity technology for IoT. Similar to Weightless-N it uses a narrowband modulation scheme but with bidirectional communications capabilities. Weightless-P uses both Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA) in 12.5 KHz wide channels. The range of Weightless-P is ca. two kilometres while the data rate is adaptive between the 200 bps and 100 kbps, depending on device link quality.

Weightless-W is based on a LPWA star network architecture operating in TV white space spectrum on frequencies between 470 and 790 MHz. Since shared access to white space spectrum for IoT is currently only available in a limited number of regions, Weightless recommends users to consider Weightless-P technology instead. Weightless-W is able to deliver data rates from 1 kbit/s to 10 Mbit/s depending on the link budget.

As of today, Weightless has not seen deployments in the Netherlands. Internationally Weightless has been deployed at city-scale, e.g. in London (Weightless-N). [87]

Satellite-based

Satellite-based machine-to-machine communications have been in use already for several decades and are offered globally (incl. over the Netherlands). Satellite-based M2M and/or IoT services are of great interest for applications that are either very remote or highly mobile (e.g. ships, airplanes). These services are currently offered by companies such as Orbcomm [49], Inmarsat, Globalstar and Iridium. Upgrades of existing constellations are anticipated or already in progress.

We expect new satellite based initiatives in the near future, in particular operating in low earth orbits (LEO) and using small satellite constellations (nanosats or cubesats). There are various initiatives such as OneWeb (who plans to operate 640 satellites in a LEO constellation), O3B, ViaSat Netherlands, Leosat, EightyLEO and Magnitude Space have initiatives in various stages of development.

3.5 Overview

The different platforms for LPWA IoT are all optimised for low-power usage, aiming to allow devices to operate as long as ten years of operation on a single battery. All are focused on low data rates and pay special attention to increase coverage to include indoor use cases, as well as optimized access in scenarios with a very large number of devices. Figure 7 gives an overview of the design goals of the technologies discussed.

	SIGFOX	LoRa	clean slate cIoT	NB LTE-M Rel. 13	LTE-M Rel. 12/13	EC-GSM Rel. 13	5G (targets)
Range (outdoor) MCL	<13km 160 dB	<11km 157 dB	<15km 164 dB	<15km 164 dB	<11km 156 dB	<15km 164 dB	<15km 164 dB
Spectrum Bandwidth	Unlicensed 900MHz 100Hz	Unlicensed 900MHz <500kHz	Licensed 7-900MHz 200kHz or dedicated	Licensed 7-900MHz 200kHz or shared	Licensed 7-900MHz 1.4 MHz or shared	Licensed 8-900MHz 2.4 MHz or shared	Licensed 7-900MHz shared
Data rate	<100bps	<10 kbps	<50kbps	<150kbps	<1 Mbps	10kbps	<1 Mbps
Battery life	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years
Availability	Today	Today	2016	2016	2016	2016	beyond 2020

Figure 7 Overview of technologies for LPWA IoT connectivity [45]

SIGFOX and LoRa are the most prominent technologies for LPWA IoT that are currently being deployed in the Netherlands. Both technologies already have quite extensive coverage via the networks of The Things Network (LoRa), KPN (LoRa) and Aerea (SIGFOX). LoRa and SIGFOX see increasing interest, even from industries that appear to want to use it for critical applications. Energy metering is one of such applications and has seen deployment already [21] [37] [91]. Nevertheless it is not of relevance to the Netherlands, as Dutch smart meters will be connected exclusively over networks in licensed spectrum (e.g. through a CDMA450 network or over public GPRS/LTE networks). [9] Nevertheless we expect other critical applications to appear in the Netherlands, such as monitoring railway shunts. [79]

While initially lagging, the 3GPP appears to have finally managed to standardise a variant of LTE that fits the demand for LPWA IoT connectivity. The momentum behind the technology appears to be very high, with operators such as Vodafone [70], Deutsche Telekom and AT&T backing the technology. Several operators also have announced plans to deploy the technology, including T-Mobile in the Netherlands. [80]

We are expecting very fierce competition between the licensed and unlicensed technology families, where the main contention points will be (1) price of device, (2) time to market and coverage, and (3) reliability and security. We do not expect the market to standardize on either technology – rather, the competition will be about the division of applications between either licensed or unlicensed connectivity. Within the domain of licensed connectivity, competition is expected between operators as there currently is on mobile connectivity in general. In the unlicensed domain, there will be competition between SIGFOX and LoRa, where only a single deployment of either technology is expected to remain in the race, with The Things Network perhaps additionally fulfilling a niche for hobbyists and enthusiasts.

Operators and vendors in either camp put different emphasis on localisation functionality. Proponents of LoRa say LoRa allows for rather precise localisation using time-of-arrival methodologies, which does not require additional hardware on the device side. Indeed, time-of-arrival localisation is a lot more difficult to do with SIGFOX, as it uses very narrow signals. LTE-M1 and LTE-M2 do not provide specific support for time-of-arrival localisation, although it may be possible to implement in a future release.

Nevertheless, localisation using time-of-arrival methods still requires the proper reception of a LoRa message by at least three synchronized base stations, which may become an issue when the LoRa network becomes more crowded. We also suspect that use cases that require localisation may either only require very coarse localisation (e.g. which base station picked up the signal) or will use highly precise GPS based localisation anyway.

The sheer size of the LTE-M2 deployment planned by T-Mobile (12.000 sites) as well as the fact that LTE-M2 modules are already becoming available [81] clearly illustrate that while LoRa and SIGFOX may have had a head start regarding coverage and availability, LTE-M2 may quickly close the gap. In addition, while LTE-M2 modules are expected to be more expensive than their LoRa and SIGFOX counterparts, LTE-M2 seems to be the most promising technology from a technical point of view, especially concerning reliability and security.

While currently not evidenced in practice, we do see uncertainty regarding the future reliability of these technologies, especially facing large-scale deployments with a large number of devices. While LoRa and SIGFOX may be marketed as being low-cost and only for non-critical applications, we are unsure whether customers truly understand the risks of the technology. We expect that even though initial deployment of applications based on unlicensed LPWA IoT connectivity will be isolated, customers will gradually integrating such applications further into their business processes, and gradually become more reliant on the connectivity (e.g. [9] describes future applications of data obtained from smart meters).

4 Demand

The impact of wireless IoT on the spectrum is highly dependent on the total number of active transmitters, and therefore the volume of IoT devices. In this chapter we model the current and future market volume of IoT devices. A distinction is made between the different types of applications and the geographical dispersion of the devices in the Netherlands.

4.1 Total device volume

IoT has experienced a considerable growth over the last year. In all the sectors the number of IoT network connections has grown with double digits, as can be seen in Figure 8.

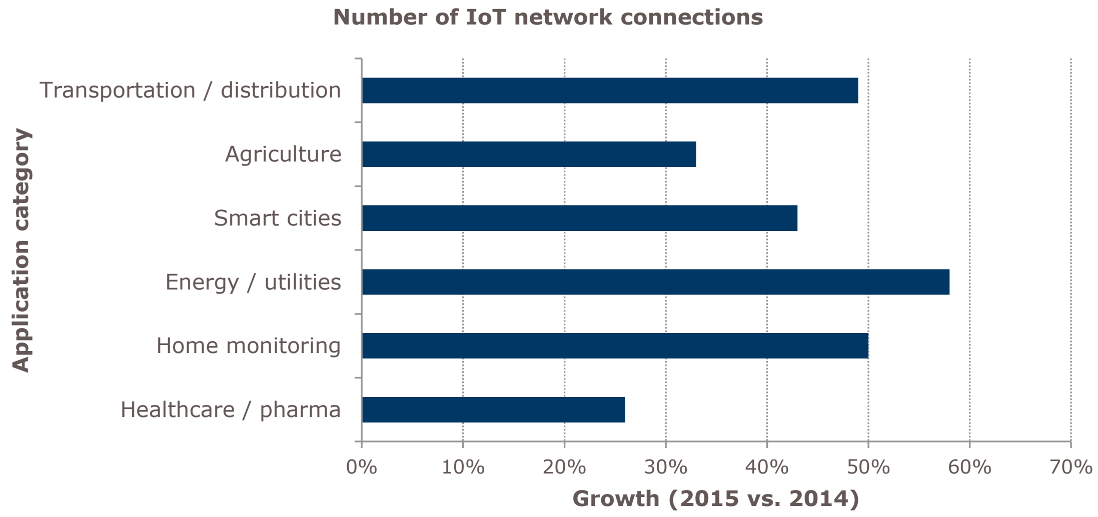

Figure 8 Growth of IoT network connections in 2015 [82]

Our focus with respect to device volumes for this study is on LPWA IoT devices. As discussed, these devices have the greatest impact on the spectrum and other users, as obviously their use of particular (unlicensed) spectrum is noticeable in a (much) larger geographical area than short range devices.

Market volumes for short range devices have already been studied in-depth in earlier research commissioned by the Radiocommunications Agency. [71]. In this study, a distinction is made between wireless devices in households[11] controlled with and without smartphone/tablet. In Table 4 an overview is given for the number of households with a smart device, controlled with a smartphone/tablet, for both 2015 and 2020.

[11] More specifically, households in terraced houses. Terraced houses are also called row houses or linked houses due to sharing of the side walls.

Table 4 Number of households with smart device controlled with smartphone/tablet [71]

Device	Number of households (2015)	Number of households (2020)
Smart thermostats	600,000	2,690,000
Security camera	380,000	2,000,000
Smoke detector	290,000	2,530,000
Distance controlled lighting	290,000	2,140,000
Shutter or blinds	170,000	1,050,000
Baby monitor	170,000	580,000
Dishwasher/washing machine	90,000	620,000

In Table 5 the number of households owning wireless devices controlled without smartphone/tablet is given.

Table 5 Number of households with smart device controlled without smartphone/tablet [71]

Device	Number of households
Wireless equipment around computer	2,640,000
Wireless headphones, microphones, speakers, Hi-Fi sets	1,570,000
Wireless switch for light	980,000
Wireless remote controls for car, garage etc.	830,000
Wireless weather station	710,000
Wireless thermostat	540,000
Wireless alarm	440,000
Wireless equipment related to health	300,000
Wireless device to control household electronics central	170,000

The above figures cannot be directly translated to the volumes of short range device below the 1 GHz. First of all a household can have multiple devices within one category. For instance, a household can have multiple wireless switches for the lights or multiple wireless microphones. Second, not all the devices operate on the sub 1 GHz frequency band. A weather station operates at both the 433 MHz and the 2.4 GHz frequency band. Despite the inconsistencies, the figures give a good initial overview of the market volume.

4.1.1 Current volume

For the estimation of the current volume we take figures from market studies into account but also information from vendors, manufacturers and resellers of LPWA devices.

Operator figures

KPN, operator of a Dutch LoRa network with nationwide (outdoor) coverage, recently announced that, in the short term, it expects to connect at least 1.5 million devices. [79] Applications recognized by KPN include (among other things) dike monitoring, parking space sensors as well as meters for gas, electricity and water consumption. [71] KPN is also conducting experiments with more critical applications, such as railway shunts. [79]

Market studies

A lot of market studies about the market volume of IoT are available. However, these market studies do not all have the same scope. For instance, McKinsey [42] looks at all the objects connected to the internet, while Ericsson estimates the market volume for both cellular and non-cellular IoT devices [24]. In our estimation we look specifically at the market volume of LPWA devices, the scope of our research as defined earlier.

Only a few market studies look specifically at the market volume for LPWA devices. Pyramid Research and Strategy Analytics estimated that the worldwide market volume of LPWA devices was roughly 20 million (Pyramid Research [51]) till 60 million (Strategy Analytics [31]) devices in 2015. They do not make a distinction between LoRa, SIGFOX or NB-IoT.

The market studies only give the volume for the whole world, a distinction between countries or even continents is not made. For converting the global market volume into a market volume for the Netherlands, two different methods are used. The first method is to take the Dutch share in the total world population, which is around 0.23%. The second method is to look at the Dutch part of the global GDP, which is roughly 0.74%. In Table 6 an overview is given for the estimates of the current volume of LPWA collections in the Netherlands.

Table 6 Market volume of LPWA devices in the Netherlands

Organisation	Volume based on % of world population	Volume based on % of GDP
Pyramid Research	46,000	148,000
Strategy Analytics	138,000	444,000

Sales figures

The sales information from vendors, manufacturers and resellers can be used to validate the estimates from the market studies. However, the information from the vendors is not reliable enough to validate the estimates. Most of the vendors did not want to share their sales numbers, but they did not hesitate to mention that there is an enormous potential for LPWA devices. Only a few vendors provided us with rough estimates of their sales figures. The sales figures varied from 1,000 – 10,000 LPWA devices per vendor in the past year for Western Europe. A breakdown towards the different countries was not made. Despite the lack of good sales figures, the information can be used to give guidance to the estimates of the market studies. The 444,000 LPWA devices quoted by Strategy Analytics seems to be way too high. The sales figures would be substantially higher, despite the fact that we only spoke to a few vendors.

4.1.2 Projections for the future

For the projections for the future more market studies are available. A lot of organisations have made their own projections for the future. The main difficulty in comparing these projections is the unit of analysis. In Table 7 an overview of the different projections is given.

Table 7 Projections of global market volume IoT devices

Organisation	Projection	Year	Technology	Ref.
Machina	3.78 billion	2024	SIGFOX, LoRa, NB-IoT	[41]
Analysys Mason	3.1 billion	2023	SIGFOX, LoRa, NB-IoT	[53]
Strategy Analytics	5.1 billion	2022	SIGFOX, LoRa, Cellular LPWA technologies	[31]
Pyramid Research	860 million	2020	SIGFOX, LoRa, NB-IoT	[51]
Huawei	2 billion	2020	Zigbee, Bluetooth, Wi-Fi, SigFox, Lora, NB-IoT	[32]
Ericsson	15.7 billion	2021	All IoT technologies, both cellular and non-cellular	[24]
McKinsey	20-30 billion	2020	All objects connected to the internet	[42]

Especially the studies by Analysys Mason and Strategy Analytics are relevant as they both give an estimate for the whole range of years, instead of only one year. In Figure 9 an overview of their projections is given. We extrapolated both projections towards 2024 so that a comparison with the study of Machina Research is possible [41]. The extrapolation is based on the growth rate of both projections.

The extrapolation leads to a forecast of 3.76 to 7.22 billion LPWA devices in 2024. The prediction of 3.76 billion devices comes close to the 3.78 billion devices as estimated by Machina Research [41]. The forecasts of Analysys Mason and Strategy Analytics differ almost 3.5 billion devices. One explanation for the huge difference can be the timeline of the projections. The growth of the market volume of IoT devices is expected to follow an s-curve. The case can be that both Analysys Mason and Strategy Analytics reach ultimately the same number of IoT devices but that the prediction of Analysys Mason is lagging. However, the growth rate of Analysys Mason is in 2022 roughly 35%, which is only marginally larger than the 29% of Strategy Analytics. Thus the prediction of Analysis lags behind the prediction from Strategy Analytics, but not enough to explain the difference of 3.5 billion devices.

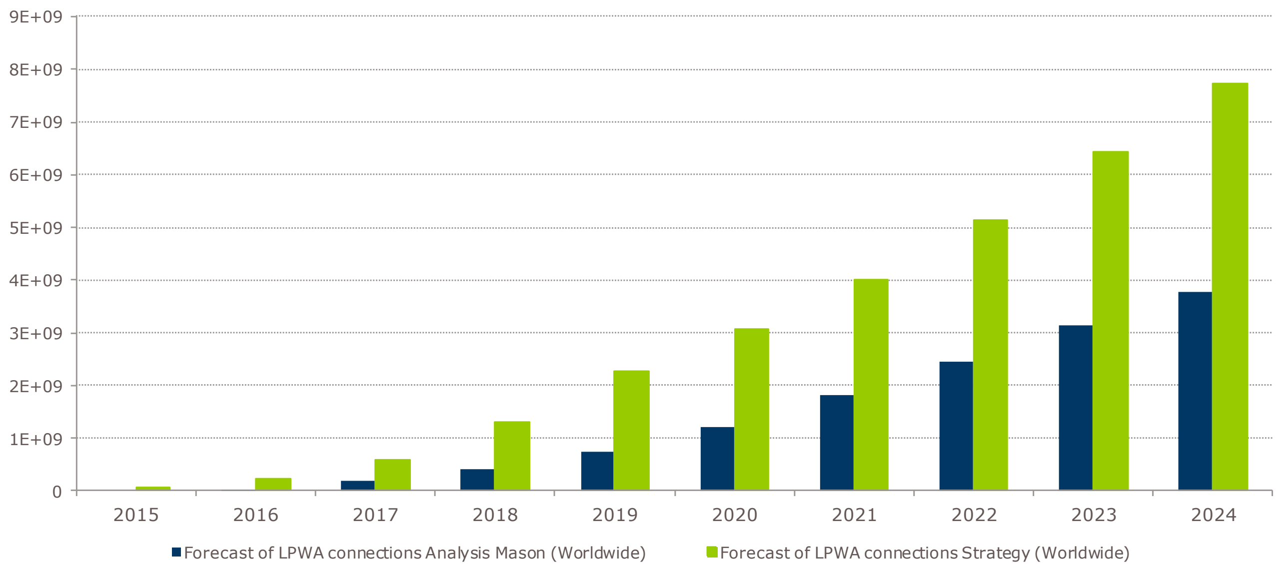

Figure 9 Estimate of the worldwide volume of LPWA devices for 2015-2024

Just like the previous paragraph we used the Dutch share in the world population and the GDP to convert the volumes of the global market into the Dutch market volume. In Figure 10 an overview of the projections is given. In 2024 there will be between 8.7 and 52.1 million LPWA devices in the Netherlands.

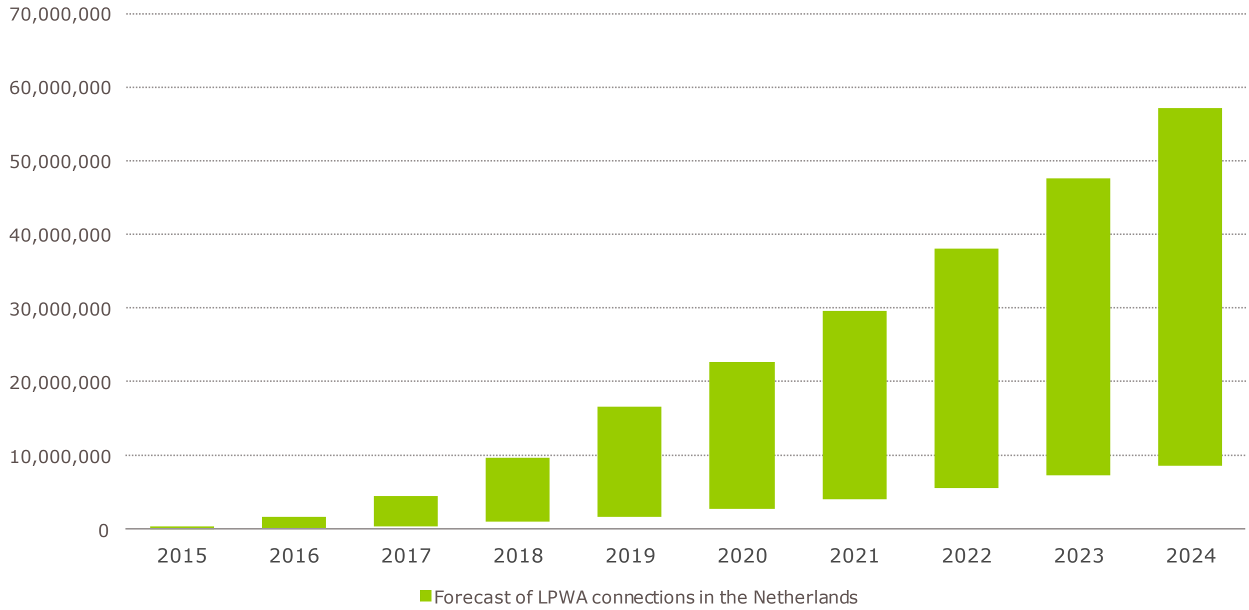

Figure 10 Estimate of LPWA devices in Netherlands for 2015-2024

4.2 Applications

The breakdown into different applications will be used for the modelling of the devices in the next paragraph. Both Analysys Mason and Strategy Analytics give a breakdown towards the different applications, as can be seen in Table 8.

Table 8 Share of applications in LPWA devices by Strategy Analytics (left) and Analysys Mason (right)

Type	Share
Home Automation	20.60%
Office Security	15.60%
Maintenance	15.40%
Other	14.40%
Vehicles	7.40%
Building Automation	7.10%
Remote/Green Technology	5.40%
Retail Outlets	5.00%
Smart metering / Utilities	4.20%
Consumer Electronics	3.50%
Transportation	0.90%
Office Metering / utilities	0.40%

Type	Share
Smart buildings	24.90%
Agriculture and environment	23.60%
Utility	17.70%
Consumers	12.50%
Logistics	9.60%
Smart cities	8.60%
Industrial	3.00%

The first things that stands out is the categorization by both firms. The study of Strategy Analytics has five additional categories compared to Analysys Mason. There are also some substantive differences in the tables. Strategy Analytics estimates that roughly 5% (both office and smart metering) of the LWPA-devices will be used for utilities, while Analysys Mason expects a share of almost 18%. Both estimates are nowhere near the prediction of Pyramid Research that in 2024 45% of the LPWA devices are smart meters. Another noticeable difference is the application *agriculture and environment* which has a substantial share of ca. 24% in the prediction of Analysys Mason. However, the application has only a minor share in the forecast of Strategy Analytics as Remote / Green Technology.

We will use the breakdown of Analysys Mason for the modelling in the next paragraph. They have a clear demarcation of the different applications and contrary to Strategy Analytics they have elucidated their breakdown in the forecast. They see for each application the following use cases:

- **Smart Buildings:** smoke alarms, white goods
- **Agriculture and environment:** land monitoring, livestock monitoring, forest monitoring
- **Utility:** gas and water meters
- **Consumers:** bicycles, pets
- **Logistics:** container tracking, refillable tanks and bottles
- **Smart cities**: street lighting, parking, waste management
- **Industrial:** indoor asset tracking, pipeline monitoring

4.2.1 Critical applications and televulnerability[12]

The use of LoRa and SIGFOX devices may pose a problem when used for certain critical applications. In France, SIGFOX has won a tender to connect more than 100,000 boilers of e.l.m. leblanc to remotely monitor boiler performance and optimize required and preventive maintenance. [8] The benefit for leblanc is that maintenance work can be done way more efficient. However, if SIGFOX gets hacked (which is not unlikely given the limited security), and fake or false reports are send by the boilers, leblanc will have a lot of work to fix these problems.

Similar issues can be expected when the SIGFOX frequency band is full and the messages cannot be sent anymore. Companies that become (completely) dependent on the information from LPWA devices may have a problem when the frequency band is full. Therefore it is of utmost importance that companies know the limitation of long-range LPWA devices (especially SIGFOX and LoRa) before integrating them into their organisation.

In the Netherlands, KPN also recognizes various opportunities related to infrastructure (e.g. gas, electricity and water meters, as well as railway shunts) for its LoRa network, but also indicates that it intends to 'hold back' on pushing use for critical applications. [79] It is questionable whether KPN and its customers will be able to assess the criticality of the applications at deployment time; in many cases, we expect the reliance on IoT data to increase over time.

4.2.2 Localisation

Operators of LPWA IoT networks recognize localisation as an important use case on their networks. Critical use cases and/or cases that require detailed location information (within 10 metres accuracy) will generally use devices that have localisation hardware built-in (e.g. based on GPS or another GNSS). Due to the power requirements of GNSS hardware, such devices will also likely end up using the more power-hungry (but also better performing) wireless IoT connectivity options.

For less critical applications, and applications that require less accuracy for localisation, the low-power networks provide means for localisation without requiring specific device hardware. First of all, SIGFOX and LoRa networks can locate devices by identifying the base station(s) that picked up messages from the device, and use a form of triangulation based on (among others) signal strength measurements. According to Link Labs, the accuracy of this method is limited, unless there is a near direct line-of-sight between the transmitter and the receiver. [39]

More accurate localisation can be achieved using time-of-arrival measurements, where the network attempts to measure the distance travelled by the radio signals themselves. This approach has been tried before in the context of GSM localisation (e.g. for emergency calling, such as 911 in the US). However, it only works in networks that use signals above a certain minimum bandwidth. As Link Labs puts it, *"To measure radio range you need enough energy in the direct path to detect it, and you need enough bandwidth to resolve what is a reflected signal and what is not."* [39] This requirement makes time-of-arrival localisation infeasible for SIGFOX networks (which use ultra-narrowband signalling). SAGEM reports that time-of-arrival localisation is feasible in LoRa – this conclusion however only appears to hold for networks with relatively dense networks (having an average inter-site distance of only 1700

---

[12] With this term we refer to the risks related to telecommunications service availability for crisis organisations. For an elaborate discussion, see [85].

metres), while combining time-of-arrival measurements with RSSI (signal strength) measurements, and assuming the reception of a single signal by at least ten gateways. [60]. Neither of these requirements appear to be currently met by LoRa networks in deployment in the Netherlands.

4.3 Trade flows

One part of this study is to identify how trade flow of wireless IoT can be mapped and how regulatory bodies can become aware of illegitimate wireless IoT devices as early as possible. In this paragraph both subjects will be discussed.

4.3.1 Mapping trade flows of wireless IoT

Mapping trade flows of wireless IoT devices is not an easy task. The first issue is the diversity of devices that can be bought. The Things Network, one of the LoRa networks in the Netherlands, has on their website a list of more than 20 different devices that can be used on their network. [75] The devices vary from complete nodes to communication chips. On the website of SIGFOX a similar list of transceivers and development kits can be found. [64]

The aforementioned devices however form only a small part of the IoT-ecosystem. The list consists of chips and modules that are mostly suited for developers or manufacturers. End-users often do not want to buy a simple module or communication chip, they want to buy a turnkey device. For example, a smart water meter with a remote controlled valve. End users can buy such a turnkey device either directly from the manufacturer or from a solution provider, where the latter also provides the connectivity with the wireless network. In Figure 11 an overview of the ecosystem is depicted.

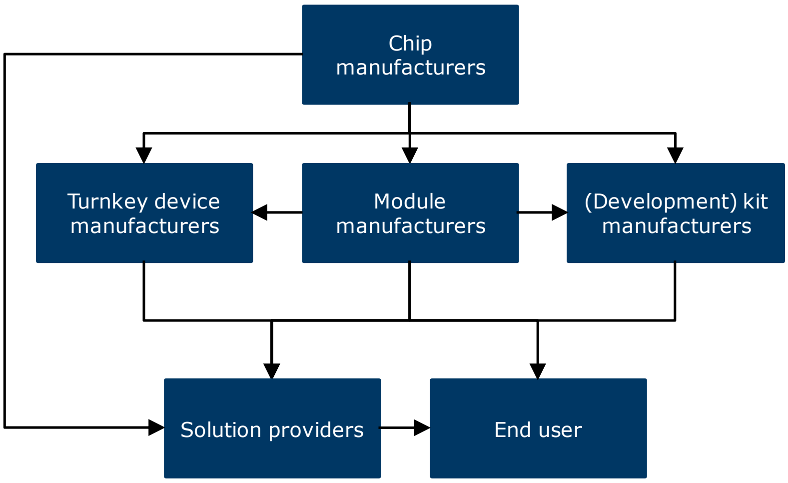

Figure 11 Ecosystem for IoT devices

The devices as listed on the website of The Things Network are related to the chip, module and (development) kit manufacturers. Their focus seems to be on hobbyists who want to test the possibilities of the LoRa-network, especially since the use of the network is free of charge. The necessary gateways are placed by sponsors or financed via crowd funding.

KPN on the other hand, who also operates a LoRa-network in the Netherlands, is headed in the direction of solution provider. For instance, they collaborate with Ziut and HR Groep who use the LoRa-network for respectively services on street lighting and street furniture. [36] The use of their network is also not free of charge. Aerea, responsible for the SIGFOX-network, has a business model similar to KPN's.

The most relevant and biggest trade flows for the end users are the ones from the manufacturers of turnkey devices and the solution providers. Most of the end users want to buy a device that directly works, only the hobbyists buy modules and development kits. In Figure 12 an overview of the supply chain from the chip manufacturers towards the solution providers is given.

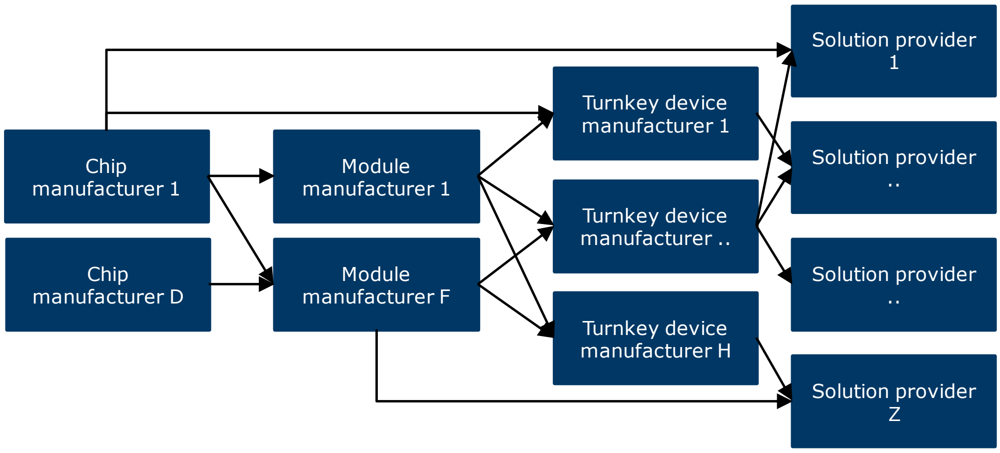

Figure 12 Supply chain from chip manufacturers towards solution providers

In Table 9 a short overview of relevant stakeholders is listed. The table contains all the manufacturers of radio chips and a subset of module and turnkey manufactures and the solutions providers.

Table 9 Brief overview ecosystem IoT market

Company	Technology	Manufacturer
Atmel	SIGFOX	Radio chip, module
Silicon Labs	SIGFOX	Radio chip
ON Semiconductor	SIGFOX	Radio chip
Texas Instruments	SIGFOX	Radio chip, development kit
Semtech	LoRa	Radio chip
Microchip	LoRa	Radio chip
HopeRF	LoRa	Radio chip
Embit	LoRa	Module, development kit
Modtronix	LoRa	Module, development kit
Adafruit	LoRa	Module, development kit
MultiTech	LoRa	Module
SODAQ	LoRa	Module, development kit
Atim	SIGFOX	Module, turnkey device
Capturs	SIGFOX	Turnkey device
Hydroko	SIGFOX	Turnkey device
Adeunis	SIGFOX, LoRa	Turnkey device
Ziut	LoRa	Solution provider, turnkey device

The number of chip manufacturers is relatively small compared to the other groups of eco-system participants. For LoRa and SIGFOX there are respectively three and four manufacturers of radio communication chips. Monitoring their trade flows should give a good insight in the total market volume of IoT devices. However, the chip manufacturers cannot easily pinpoint their volumes to different countries and applications. A chip manufacturer can for instance sell chips to a turnkey device manufacturer in Germany who sells their products in whole Europe.

The solution providers and turnkey device manufacturers have a better overview of the number of sold products in the different countries. However, there are numerous companies who offer turnkey devices or solutions. On the website of SIGFOX already 46 different manufacturers of turnkey devices are listed. In Figure 13 the trade-off between knowledge about volume versus location is shown. The chip manufacturers such as Semtech and Silicon Labs have a good overview of the volumes of LPWA devices, but do not know where the devices end-up. Ziut, a solution provider, has a good overview of their devices in the Netherlands, but does know the number of devices from other companies.

KPN and Aerea are the most interesting companies in this context - they both have an LPWA-network in the Netherlands and should know how many devices are active on their network. Based on contracts with the solution providers and end-users they can even predict the amount of new IoT devices on the network.

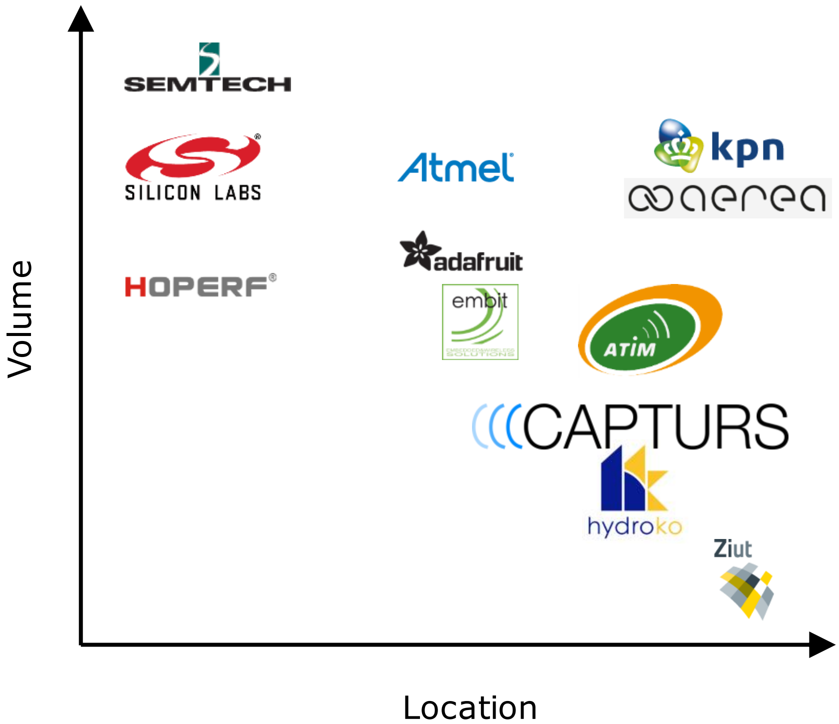

Figure 13 Volume versus location and application of IoT devices: who knows what?

4.3.2 Awareness of illegitimate wireless IoT devices

Illegitimate wireless IoT devices can pose a problem for the development of IoT. Devices with a too high power output or duty cycle can cause interference on the 868 MHz frequency band.

Before a device can make use of the LoRa-network of KPN it has to be certified by the LoRaWAN-alliance. The certification prevents the entrance of illegitimate devices to the network. However, not each individual device is certified and it is unclear how the certification is enforced – it seems appropriate to use a device ID or another kind of address for this purpose, but such a check is probably not airtight. Illegitimate devices can therefore likely still enter the network.

A possible bigger problem is the import of illegitimate IoT devices from completely different markets. IoT devices from the USA often operate in the 902 – 928 MHz frequency bands and can cause uplink interference on the existing cellular network in the Netherlands in the 902-915 MHz. Similar problems can happen with certain types of cordless phones from the USA. Tracking these types of devices is very difficult because consumers can import these devices themselves via the USA or take these devices with them after a holiday. AT does not have the resources available to check every device that enters the European market through the Netherlands on its specifications. More efficient market surveillance can be performed based on intelligence on illegal devices through the ICSMS system, which notifies market surveillance authorities about products that do not comply with harmonised standards.

The third option would be to track the device when the actual interference occurs, via the monitoring network. We will discuss this further in paragraph 6.3.

4.4 Geographical distribution

For modelling the distribution of the devices we use the breakdown of Analysys Mason and the lower bound of the estimation from paragraph 4.1.2 (ca. 8.6 million devices in 2024). The lower bound is used to give a realistic representation in the model while at the same limiting the necessary computing capacity. In Table 10 an overview of the number of devices per application is given.

Table 10 Number of LPWA devices per application

Type	Relative share	Devices
Smart buildings	24.90%	2,161,000
Agriculture and environment	23.60%	2,047,000
Utility	17.70%	1,532,000
Consumers	12.50%	1,080,000
Logistics	9.60%	831,000
Smart cities	8.60%	748,000
Industrial	3.00%	263,000
Total	**100%**	**8,661,000**

In Figure 14 a sample result of the modelling can be seen. The figure contains roughly 6,000 points of all the seven categories. In the city centre mostly the smart buildings, smart city and utility devices are present, while the agriculture and environment devices are situated in the rural areas. In the bottom left of the picture a few industrial devices can be seen, in the middle of the industrial area.

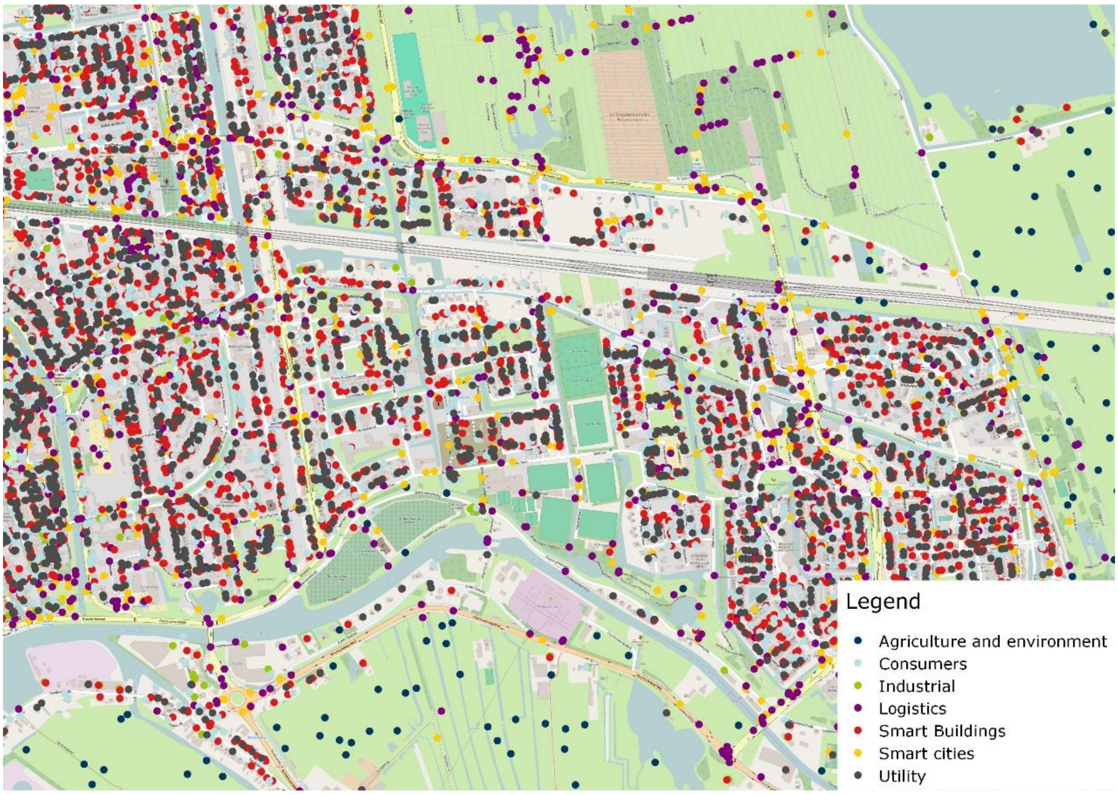

Figure 14 Example of modelled geographical dispersion of LPWA IoT devices (shown here for the city of Gouda)

In Figure 15 a heatmap of the devices through the Netherlands is shown. Based on the heatmap it can be stated that especially in the megalopolis in the west of the Netherlands, the *Randstad*, most of the devices can be found. Note that this map does not necessarily also indicate potentially problematic areas with respect to interference or capacity issues, as there are other users of the same frequency bands that need to be taken into account (see our discussion in chapter 6).

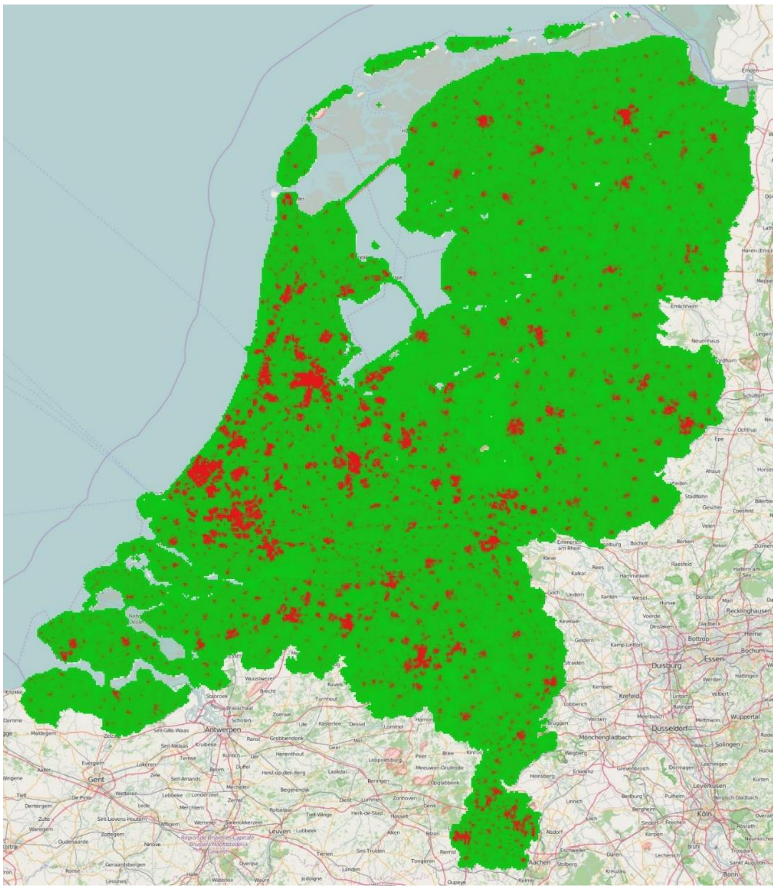

Figure 15 Heatmap of LPWA devices

We also made a histogram of the number of devices per square kilometre as can be seen in Figure 16. The highest number of devices per square kilometre is almost 10,000. The number of devices per square kilometre is centered around the 100 devices per square kilometre.

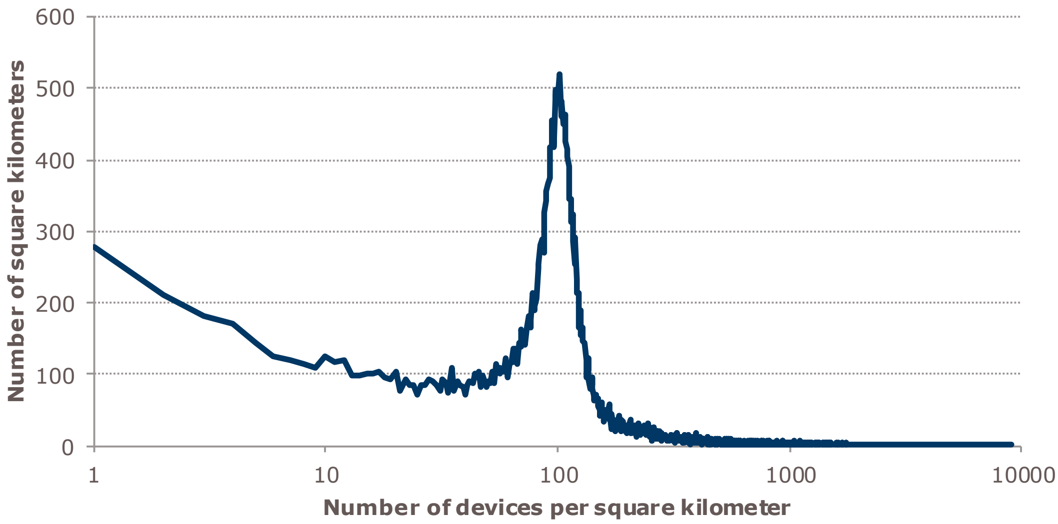

Figure 16 Histogram of the modelled number of devices per square kilometre

4.5 Overview

Based on our analysis we expect that there will be between 8.6 and 52.1 million long range LPWA devices in the Netherlands in 2024. Most of the devices are expected to be in the categories *agriculture and environment* and *smart buildings*, although there is a significant difference between the studies. Monitoring the trade flows of these devices will not be an easy task due to the diverse supply chain of LPWA IoT devices. The chip manufacturers have for instance a good overview of the total number of devices, but not in which country they are sold. For the solution providers and the turnkey device manufacturers the situation is the other way around. The best option would be to contact KPN (LoRa) and Aerea (SIGFOX) because they can see how many devices are connected to their network. We expect that most of the devices can be found in the west of the Netherlands, in the *Randstad*.

5 Spectrum impact

In this chapter, we analyse the impact on the spectrum resulting from the usage of wireless IoT devices on the platforms discussed in the earlier chapters. We will first discuss the way these technologies use the spectrum: how efficient are they, and what are other relevant characteristics? Second, we will discuss coverage of the networks. Finally, we will model the capacity of the network to find where certain thresholds may be exceeded, now and in the future.

5.1 Spectrum utilisation

For most IoT applications, it is expected that there will be more uplink (device-to-network) than downlink traffic (network-to-device). First of all, sensors will typically transmit data at intervals, while actuators will only be controlled irregularly. Second, we expect actuators to be primarily connected in more traditional ('machine-to-machine') ways, as reliability and two-way communication is more important for these devices compared to sensors, for which the LPWA IoT networks are very well suited.The primary concern regarding spectrum utilisation of LPWA IoT is therefore the uplink.

Downlink traffic also is much less of a concern as it can be coordinated more easily from the network side, whereas coordination between the traffic transmitted from a large number of end user devices (which are also constraint in various ways) is a much more difficult problem.

5.1.1 IoT LPWA in unlicensed spectrum

SIGFOX

SIGFOX is based on ultra-narrowband technology. SIGFOX messages are transmitted in a narrow-band channel, which is inside the 868 MHz unlicensed spectrum. Messages are modulated using ultra-narrowband GFSK, using 100 Hz of bandwidth. Effectively, in for example a 200 kHz part of spectrum used by SIGFOX, there would theoretically be up to 2,000 channels. However, adjacent channels are difficult to use due to frequency drift and adjacent channel interference issues, which reduces the number of (simultaneously) usable channels. A SIGFOX transmitter will choose a channel at random for the transmission of each message – a SIGFOX receiver will receive for example a full 200 kHz frequency band, demodulate all messages and filter out those messages it is interested in.

Studies show that ultra-narrowband sites with 10.000 users each sending several short messages over the course of a day require about 200 non-adjacent channels of 100 Hz. Therefore, in this scenario, a frequency band of 40 kHz would be sufficient.[13]

[13] This figure is calculated as follows. Assuming a device on average transmits 4 KB per day in 12 byte transmissions (using three retransmissions per message). This translates to 111 messages being sent using 333 transmissions per day, each taking approximately 1 s. Assuming 10.000 users, this translates to 38.5 transmissions/second on average. At 40 simultaneous messages and an Aloha utlisation rate of 0.2, 200 channels are required. Assuming channels are 100 Hz wide and cannot be adjacent (hence are effectively 200 Hz wide) this leads to 200 x 200 Hz = 40 kHz of spectrum (or 80 kHz when six retransmissions are used).

Following the same logic, a 125 kHz frequency band would be able to accommodate 318 simultaneous users, assuming the system would load the band for 50% as there are also other users in the same unlicensed spectrum.

In a study performed by Real Wireless, ultra-narrowband LPWA technologies are compared with spread spectrum technologies. Following the estimates by Real Wireless, a 200 kHz channel should be able to provide an uplink throughput of 50 kb/s, for 500 simultaneous users using channels of 100 Hz at 100 bits per second each. [52]

LoRaWAN

LoRa uses a proprietary and patented implementation of *chirp* spread spectrum (CSS) modulation. [61] A key property of the modulation technology used by LoRa is that a trade-off can be made between resiliency of a message against interference, throughput and the amount of 'air time' (spectrum) used. The trade-off takes the form of different *modulation types* which all LoRaWAN certified devices are required to support. The LoRaWAN standard further dictates that devices follow instructions from the network regarding the modulation to use as well as the amount of power to use when transmitting.

In order to maximize the network performance and spectral efficiency, LoRa networks and devices should ideally transmit at the modulation level which includes the least error correction but can still get the message across. The most efficient modulation level is known as 'SF7' in the LoRa standard. The level with the highest level of error correction capability is 'SF12'.

The relationship between the wanted data bit rate, symbol rate and chip rate for LoRa modulation can be expressed as follows: [62]

$$R_b = \frac{BW}{2^{SF}} * SF$$

In this formula, R_b represents the bit rate in bits per second. BW is the modulation bandwidth (in Hz) and SF represents the spreading factor (which varies between 7…12).

Table 11 shows the different spreading factors available at 125 kHz and the associated indicative performance figures in terms of bandwidth, range and time on air. Note that there are also modulation variants that use additional bandwidth (e.g. "SF7BW250" is LoRa in 250 kHz of spectrum using a spreading factor of 7).

Table 11 LoRaWAN protocol spreading factors (SF) versus data rate and time-on-air [48]

Spreading factor (at 125 kHz)	Bit rate (bps)	Range (km; indicative)	Time on air (ms) for 10 bytes application payload
SF7	5.470	2	56
SF8	3.125	4	100
SF9	1.760	6	200
SF10	980	8	370
SF11	440	11	740
SF12	290	14	1,400

As The Things Network provides data on both signal strength, signal to noise ratio and modulation rate for each message it received, it is possible to make an assessment of whether the network is actually capable of optimizing the performance in the way described. Note that while The Things Network is operational and the data used is directly from the live network, the network is still used relatively little. As discussed earlier for SIGFOX, it is likely that the number of collisions will increase as the number of nodes grows, and hence the efficiency of the network will start to decline.

In the Netherlands, LoRaWAN operates in the 867 to 869 MHz spectrum. As can be observed in Figure 17, The Things Network appears to be primarily active at the 868.1, 868.3 and 868.5 MHz frequencies. [74]

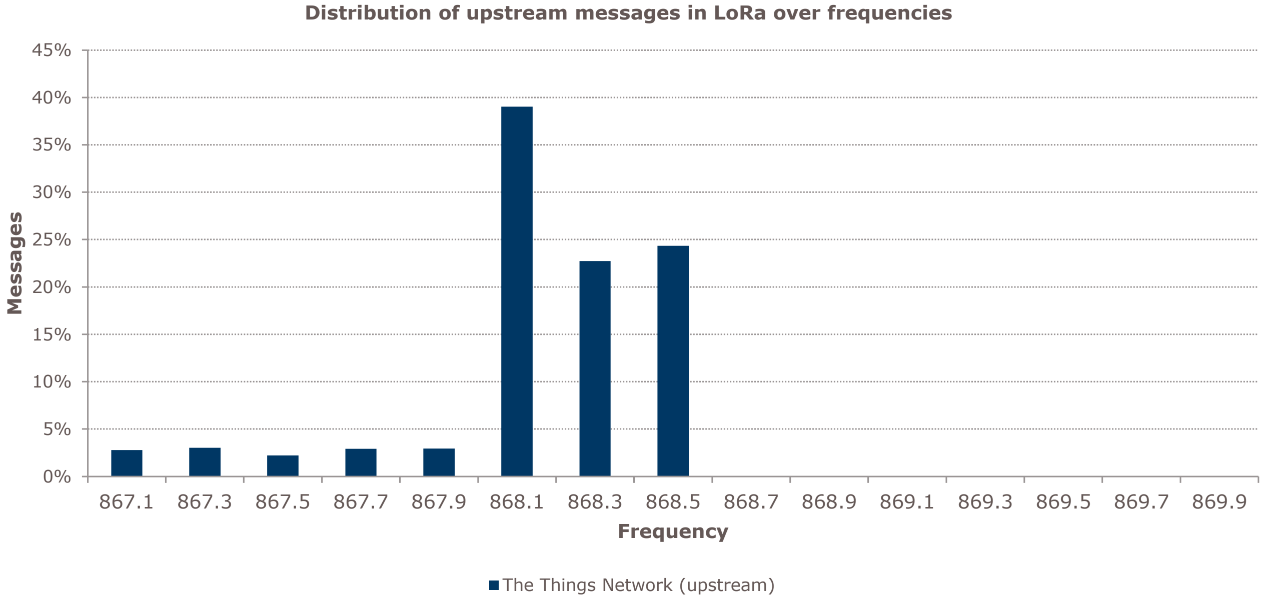

Figure 17 Distribution of messages received by the Things Network over different LoRa channels. [74]

Figure 18 shows the modulation rates observed in The Things Network in May 2016. Note that the data set also contained data on transmissions outside the Netherlands. The chart also does not show transmissions in the 433 MHz and other bands in which LoRa operates (in other countries). Yet it is interesting to see that only a few LoRaWAN channels are actually used while the technology allows for as much as 31 channels in the 863-870 MHz band (excluding high power and alarm channels and depending on national regulation).

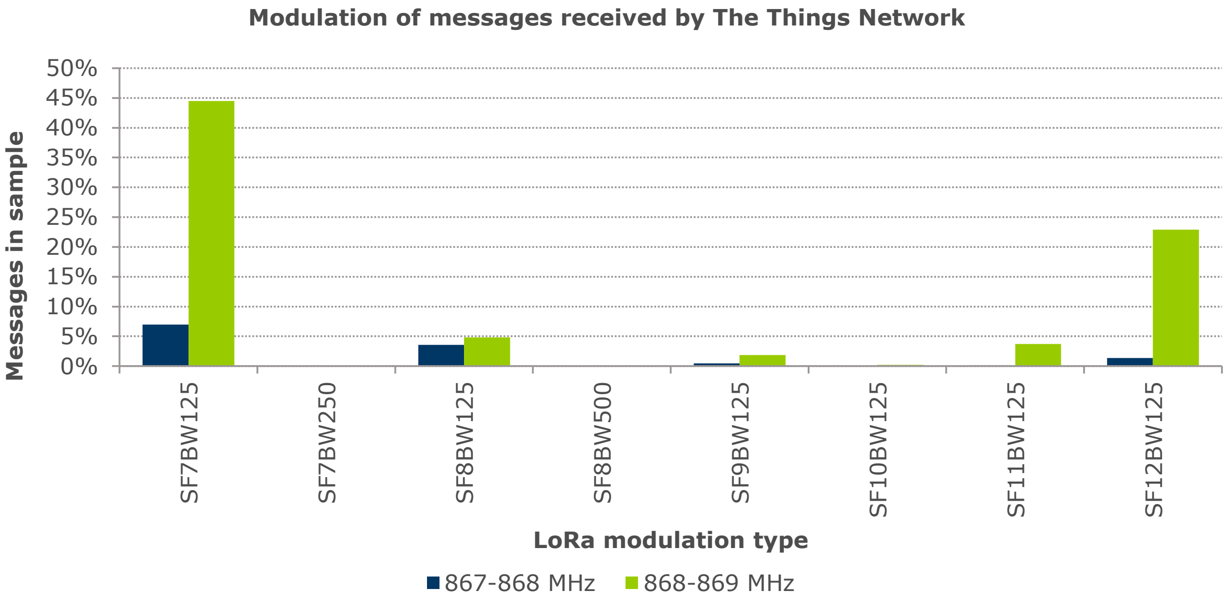

Figure 18 Modulation rates observed in The Things Network [74]

Figure 19 and Figure 20 show the distribution of modulation rates used for messages received by The Things Network, distinguished by the different signal-to-noise ratios observed. About 24% of the total traffic observed in the Things Network during our observation is SF12 traffic. From Figure 20 it is clearly visible that a large fraction of those messages are sent even while the signal-to-noise ratio is rather high. Additionally, the majority of messages is received at high signal-to-noise ratios (see Figure 19). This finding makes us wonder whether the network is actually capable of steering devices towards lower modulation levels, even at these early, low levels of total network usage.

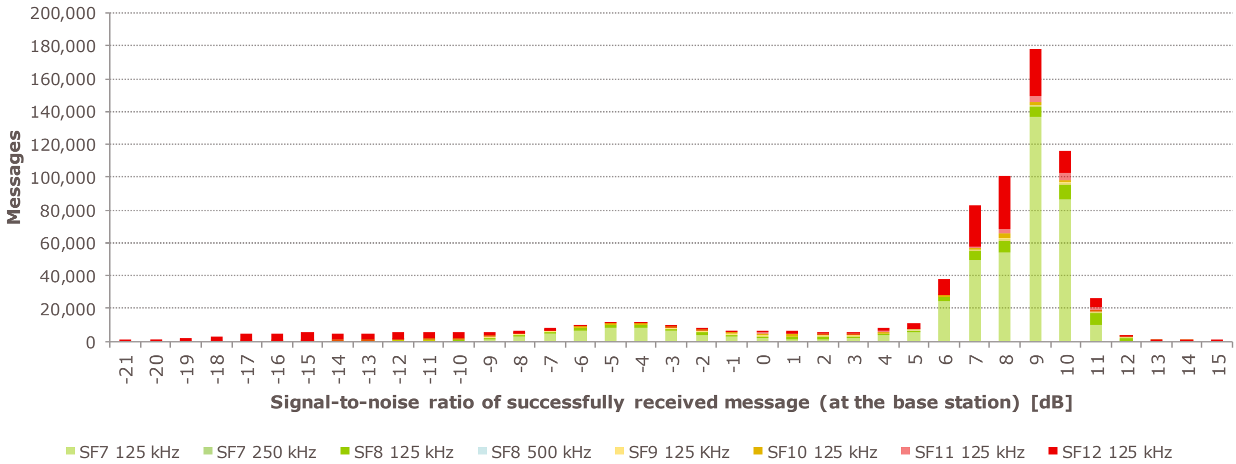

Figure 19 Modulation types observed in the Things Network in May 2016 for messages received at different signal-to-noise ratios (expressed in absolute number of messages). [74]

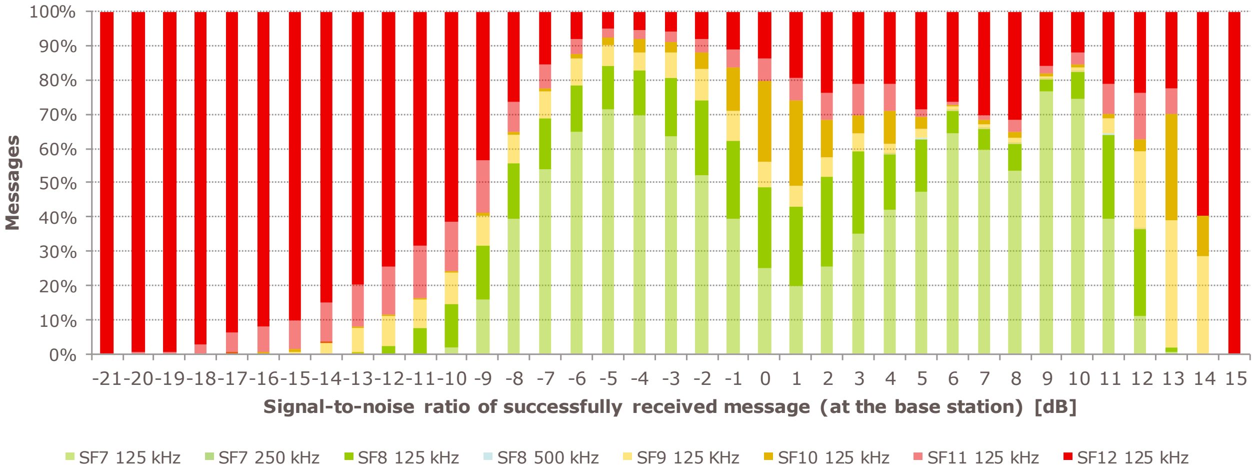

Figure 20 Modulation types observed in the Things Network in May 2016 for messages received at different signal-to-noise ratios (expressed as percentage of messages in signal-to-noise ratio bucket) [74]

5.1.2 IoT LPWA in licensed spectrum

LTE-M1 is primarily an evolutionary addition to the LTE technology stack currently deployed by operators, it is relatively easy to deploy. An operator can more or less apply a software update to their base stations. LTE-M1 makes use of existing LTE resource blocks, effectively using a virtual 'sub band' of 1.4 MHz wide.

LTE-M1 can in theory be deployed in any band where LTE can be deployed. It is however unlikely that low power devices will support all bands, which would imply hardware that supports frequencies between 450 MHz and 5.2 GHz. Instead, it is expected that devices will implement only the lowest LTE bands, as this provides the best coverage.

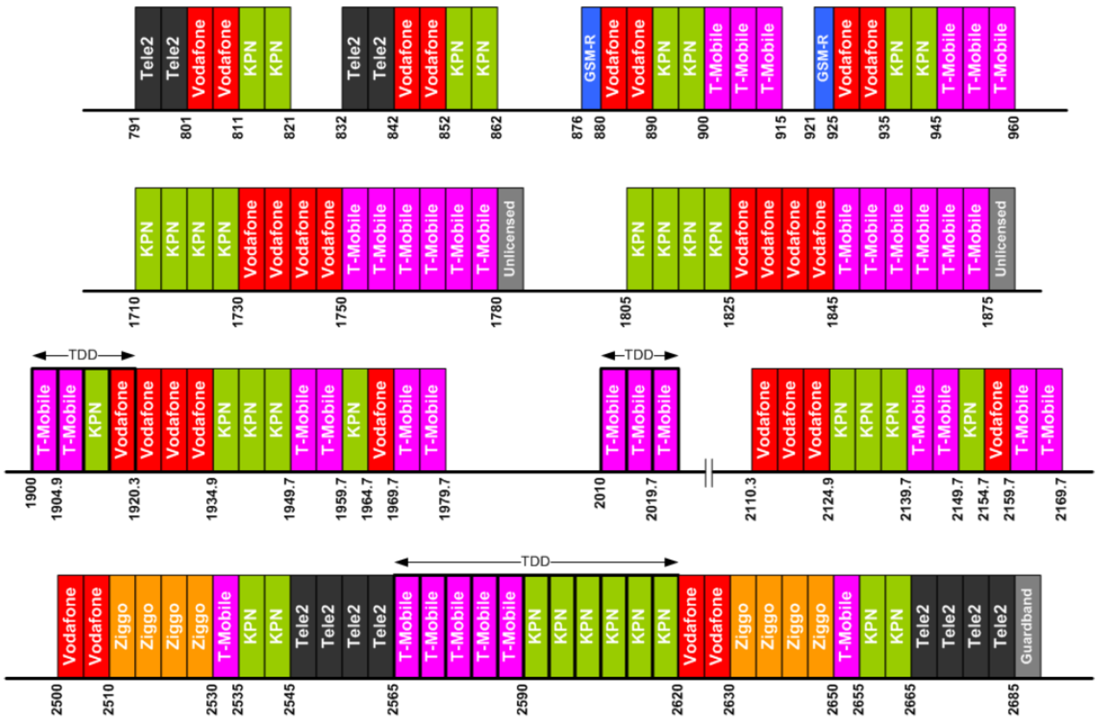

Figure 21 Overview of spectrum allotted in the Netherlands by provider [78]

In the Netherlands, deployments of public mobile networks start at about 800 MHz. Figure 21 shows the current spectrum allocation between the operators in the Netherlands. While this picture does not show what technologies are used by the operators in the different frequency bands, it does give an indication of the potential for LTE-M1 deployment. Operators can either choose to deploy LTE-M1 in the same band as existing LTE deployment, or they can choose to 'overlay' LTE-M1 onto spectrum that is currently used for GSM.

If Dutch operators are to deploy LTE-M1 in their networks, they are expected to do so in the lowest 1.4 MHz frequency band that they have available and have currently allocated to LTE, as the lower bands have the best characteristics with respect to coverage. Table 12 shows the frequency bands in which the four Dutch mobile network operators are expected to deploy LTE-M1.

Table 12 LTE networks in the 800 and 900 MHz frequency bands in the Netherlands [3]

Operator[14]	Lowest LTE band available	Lowest LTE centre frequency[15] (downlink)
KPN	LTE-20	816 MHz
T-Mobile	LTE-8	950 MHz
Tele2	LTE-20	800 MHz
Vodafone	LTE-20	806 MHz

Note that the operators can, in the future, also deploy more than 1.4 MHz of capacity for LTE-M, either in the bands listed above, or in higher LTE bands.

Like LTE-M1, LTE-M2 is primarily an evolutionary addition to the LTE technology currently deployed by operators. LTE-M2 uses existing LTE resource blocks and can therefore easily be deployed alongside LTE or LTE-M, in a 200 kHz wide sub band. Deployment however may require hardware upgrades, depending on the vendor. The reason is that for LTE-M2 it was decided to use different modulation techniques, whereas LTE-M1 simply uses 'regular' LTE radio access technology, albeit restricted to 1.4 MHz of spectrum.

The first LTE-M2 products are expected to be widely available in the market in (early) 2017. The first device module for LTE-M2 has recently been announced. [81] On the very same day of the T-Mobile announcement, Vodafone made a statement saying that it too regards LTE-M2 as the best technology for LPWA IoT connectivity. [70]

As discussed earlier, the Dutch mobile network operators will likely deploy LTE-M2 alongside their existing deployment of LTE, using the same base stations. The situation for LTE-M2 is similar, although it may be the case that deployment is slower and only possible at certain sites due to the fact that in some cases, hardware upgrades are required in addition to software upgrades. Vodafone expects that in the Netherlands 95% of their base stations will be able to support LTE-M2 with a software upgrade [83].

[14] The names of the operators listed correspond to the following legal entities: KPN B.V. (KPN), T-Mobile Netherlands B.V. (T-Mobile), Tele2 Mobiel B.V. (Tele2) and Vodafone Libertel B.V. (Vodafone).

[15] Centre frequency of the current frequency band, which is between 10-20 MHz wide.

In the Netherlands, operator T-Mobile has recently announced plans to deploy LTE-M2 on as much as 12.000 sites in the 900 MHz band, where T-Mobile currently has a deployment of LTE (see Table 12). [80]

Concurrent use

Compared to the capacity of unlicensed technologies, the estimates provided by vendors of solutions that operate in licensed spectrum are an order of magnitude higher. Ericsson and Huawei have announced support of as much as 200.000 and 100.000 devices per cell respectively for LTE-M2.

Simulations performed by ZTE in support of the standardization of LTE-M2 show that at an average message length between 100 and 280 bytes, 50.000 devices with 50.000 messages per hour in a 200 kHz channel is feasible for LTE-M2 without much degradation (see Figure 22 and Figure 23 for modelled uplink and downlink performance, respectively).

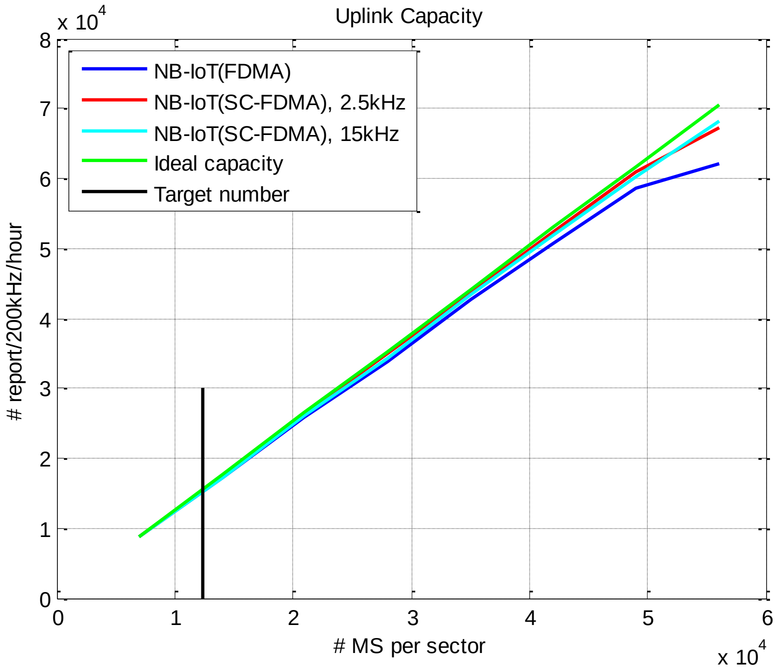

Figure 22 Modelled uplink capacity, comparison between NB-IoT (SC-FDMA) and NB-IoT (FDMA). Note 'MS' refers to 'mobile subscribers' (number of devices). [90]

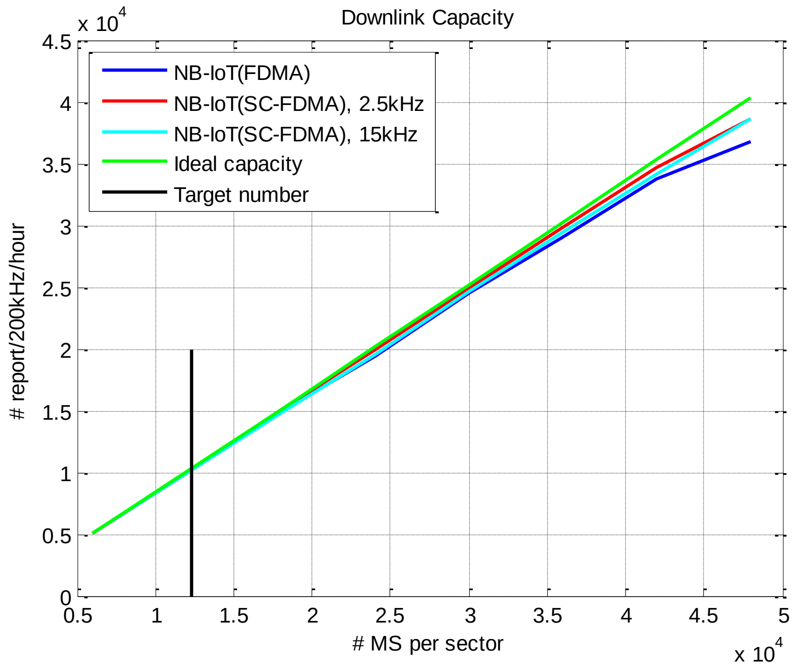

Figure 23 Modelled downlink capacity, comparison between NB-IoT (SC-FDMA) and NB-IoT (FDMA) [90]

At 40.000 devices, ZTE estimates as much as 50.000 uplink reports per hour per LTE-M2 band (200 kHz). Translating this to throughput (assuming messages between 100 and 280 bytes) the effective uplink throughput is 21.1 kbps in total. This throughput is comparable to the (theoretical) throughput in LoRa. As LTE-M2 is able to exert better power control and suffers less interference (as it operates in licensed spectrum) it is however more likely to actually achieve the theoretical maximum than LoRa. Further LTE has permanent availability of the downlink, versus just 1% of the time for the unlicensed technologies. This provides more capacity for acknowledgements, and reduces the need to send the same message many times to increase the likelihood of reception.

Note that above 50.000 devices per sector, the rate of failure starts to increase (Figure 24), imposing a limit on the number of devices per cell. In contrast to the technologies in the unlicensed band, there is no limitation on the downlink side as there is no limit on duty cycle.

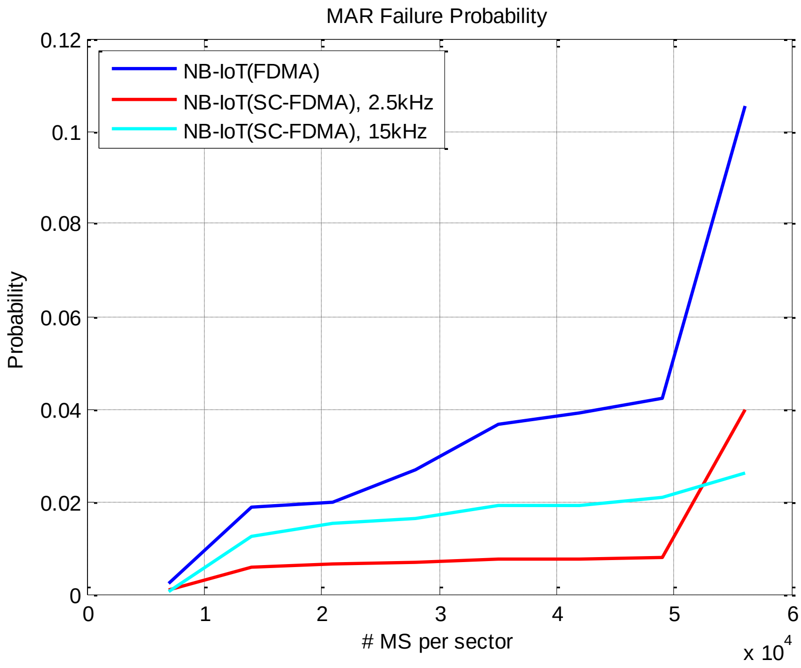

Figure 24 Modelled MAR (message arrival) failure probability, comparison between different forms of LTE-M2 [90]

The simulations performed by ZTE provide confidence in the ability of LTE-M1 and LTE-M2 to support large numbers of devices per cell. Neither LTE-M1 nor LTE-M2 appear to be bound by concurrent usage issues, as these standards provide very good means for power control and concurrent access. While both are capacity-bound, operators can easily (and even dynamically) allocate other spectrum in their possession to IoT. Also new frequency bands are expected to become available in the near future that are usable for LTE.

When comparing the maximum number of devices per cell and corresponding cell sizes between LTE and other technologies (such as LoRa and SIGFOX) it should be noted that LTE cells, given the same sites, may be up to a third smaller due to the fact that many LTE networks use sectorised antennas. While other technologies may also use sectorised antennas, LTE has the advantage that typically sectorised antennas are already deployed.

5.2 Coverage

5.2.1 IoT LPWA in licensed spectrum

LTE-M1

Figure 25 shows the estimated aggregated capacity of an initial deployment of LTE-M1 by three Dutch mobile network operators, assuming a deployment in the lowest 1.4 MHz of spectrum available to each operator (which is LTE band 20 for all operators except T-Mobile, whose lowest LTE spectrum is in band 8).

Note that capacity is expressed as *average attainable bit rate* (Mbit/s) per km^2. The estimate is as such corrected for the fact that receivers further away from a base station will be able to attain a lower speed than receivers close to a base station. In these estimates, we did not take into account the effect of an extremely high number of nodes (i.e. the estimates should be regarded as the capacity at the moment of go-live of the networks, and is likely to degrade slightly when the number of devices active in the network reaches a certain threshold; see paragraph 5.1.2).

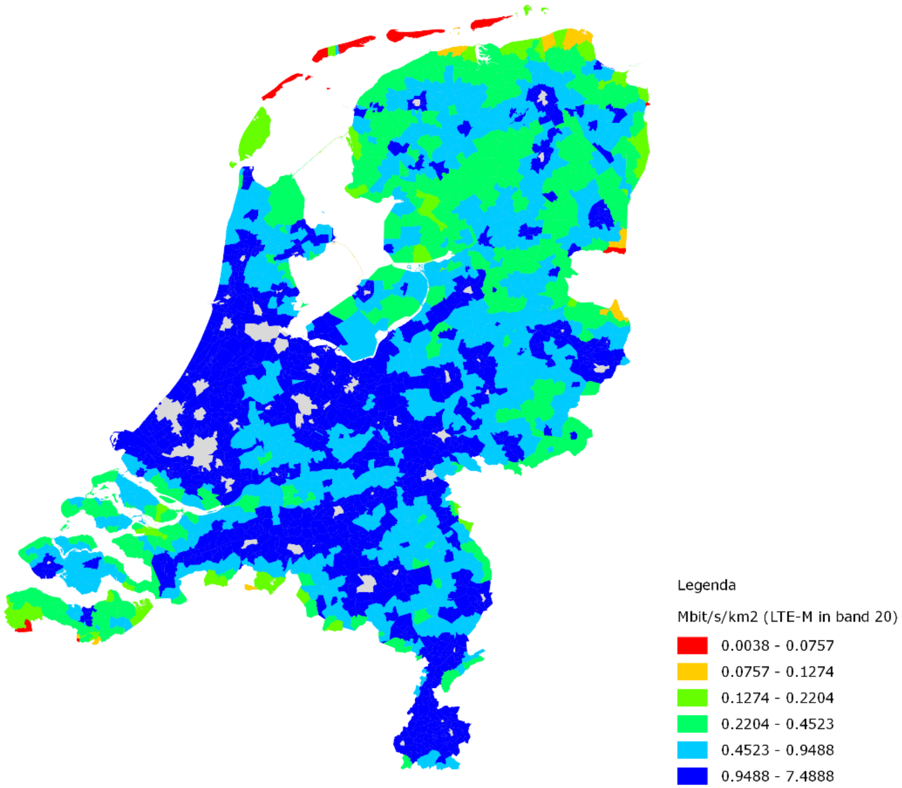

Figure 25 Estimated aggregate capacity of initial deployment of LTE-M1 by three Dutch mobile network operators in the lower parts of LTE band 20. [3] [14]

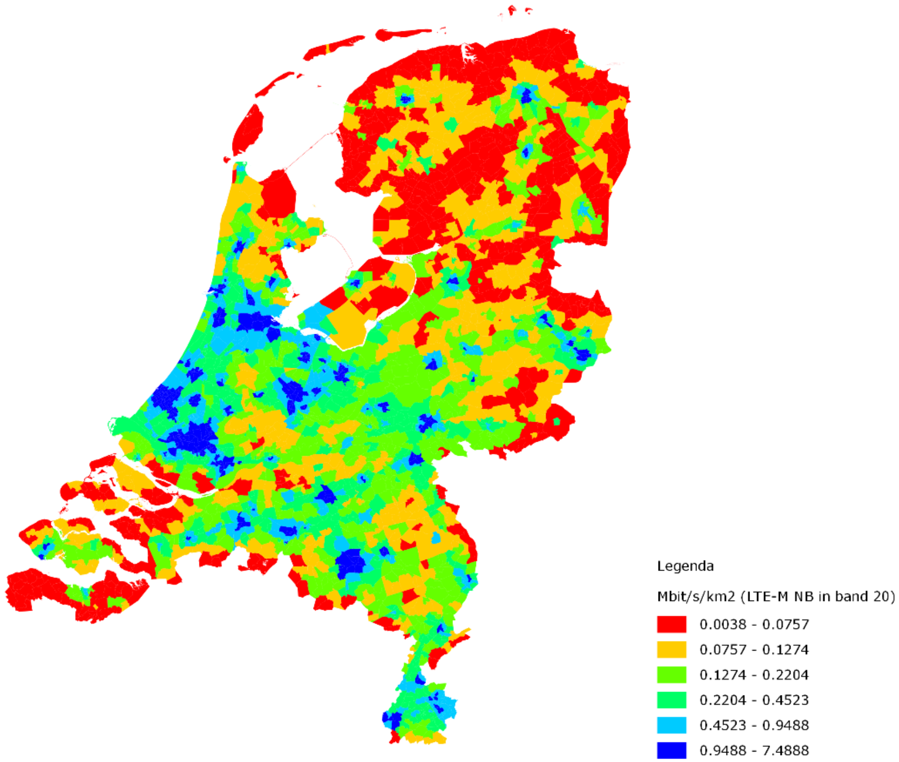

Figure 26 Estimated aggregate capacity of initial deployment of LTE-M2 by three Dutch mobile network operators in the lower parts of LTE band 20. [3] [14]

LTE-M2

Figure 26 shows the estimated aggregate capacity of an initial deployment of LTE-M2 by three Dutch mobile network operators, assuming a deployment in the lowest 0.2 MHz of spectrum available to each operator (which is LTE band 20 for all operators except T-Mobile, whose lowest LTE spectrum is in band 8).

Note that capacity is expressed as *average attainable bit rate* (Mbit/s) per km^2. The estimate is as such corrected for the fact that receivers further away from a base station will be able to attain a lower speed than receivers close to a base station. In these estimates, we did not take into account the effect of an extremely high number of nodes (i.e. the estimates should be regarded as the capacity at the moment of go-live of the networks, and is likely to degrade slightly when the number of devices active in the network reaches a certain threshold; see paragraph 5.1.2).

Note that operators can roll out a second band (allocating more to LTE-M2 and less to regular LTE) and can do so dynamically. It is also possible to overlay LTE-M1 or LTE-M2 (and also regular LTE) on GSM.

5.2.2 IoT LPWA in unlicensed spectrum

LoRaWAN

Two LPWA LoRa networks have (or are expected to have) widespread network coverage in the Netherlands during the time horizon of this study: The Things Network and KPN LoRa. In addition there are several regional and local initiatives.

The Things Network (LoRaWAN)

The Things Network (TTN) is an open source, free initiative to deploy a network to connect sensors and actuators to an open, internet-based platform. TTN will provide neutral and free access and is open for anyone. Service is provided 'as-is' and may be used for any purpose, including commercially.

Devices can connect to TTN either over an existing internet connection (e.g. using residential Wi-Fi or a mobile network), or can use wireless-access provided by TTN gateways, hosted by volunteers (either individuals or non-profits) and necessarily operating in unlicensed spectrum. Currently, TTN appears to have standardized on LoRa for LPWA wireless access. TTN is a global initiative, with gateways currently active in various different countries. In the Netherlands, TTN has deployed gateways operating in the 868 MHz frequency band.

TTN is organised in so-called communities, which are usually grouped by city or region. Figure 27 shows TTN LoRa gateways active in the Netherlands as of May 2016.

Figure 27 LoRa gateways in The Things Network located in Netherlands as of May 2016

Deployment of base stations ('gateways') is coordinated by TTN in communities. Coverage in communities is typically quite decent as of June 2016 (as for instance can be seen in Figure 28, showing coverage in Utrecht), although TTN is far from nationwide coverage.

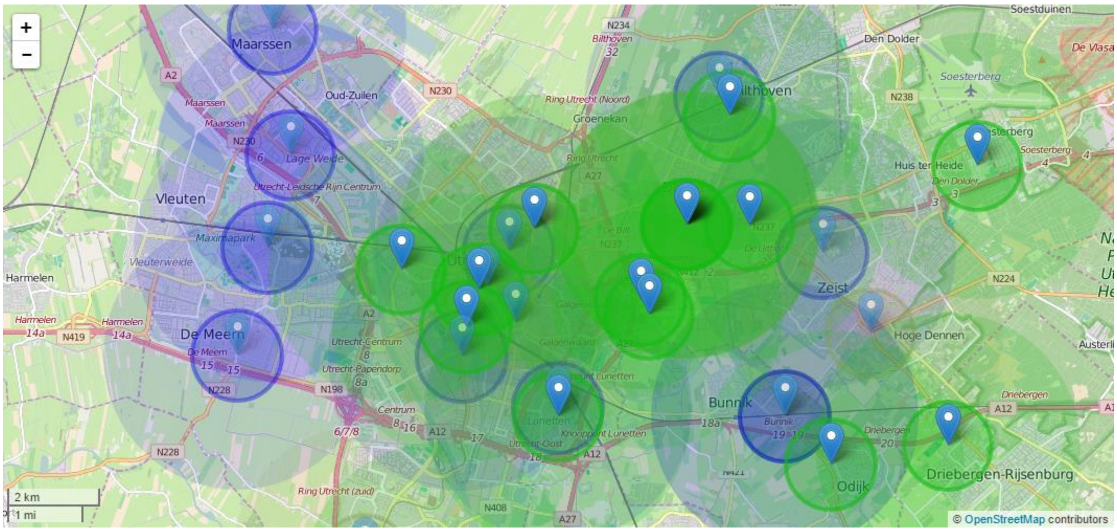

Figure 28 The Things Network coverage in Utrecht, as reported by TTN (June 2016) [76]

KPN LoRa

KPN, the Dutch incumbent operator for fixed and wireless telecommunications, is deploying a nationwide LPWA IoT network based on LoRa. KPN deploys LoRa gateways on sites that it also uses for its other services (e.g. its mobile and paging networks).

In addition to LoRa, KPN currently also offers machine-to-machine communication solutions, typically based on GSM/GPRS, 3G and LTE, as well as paging services (which are also commonly used to relay sensor data to technical staff, for instance).

KPN has deployed a LoRa network providing (according to KPN) nationwide, outdoor coverage. KPN is planning to eventually provide indoor coverage as well. Plans to further accelerate the deployment of LoRa were presented by KPN in 2015, and aimed at a deployment with 641 sites in June 2016. Figure 29 displays the (target) coverage of the network. KPN later indicated they will increase the number of sites to about a thousand to also achieve acceptable indoor coverage.

End of May 2016 (440 sites in total)	End of June 2016 (641 sites in total)

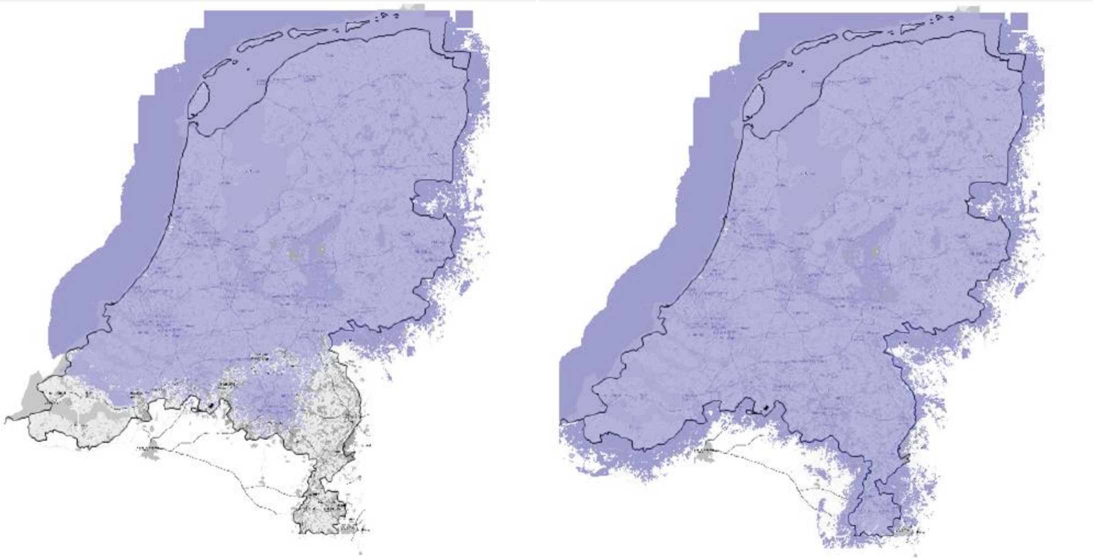

Figure 29 KPN deployment plans for LoRa in the Netherlands, showing planned coverage for the end of May 2016 (left) and end of June 2016 (right) [35]

After the planned deployment, KPN will likely further increase the number of sites locally to maintain network performance.

The KPN network operates on the same frequencies as the Things Network (868 MHz). KPN has indicated that while their base stations may also receive traffic destined for the Things Network, they have not yet encountered issues of interference with The Things Network.

KPN requires devices active on the LoRa network to obtain certification following the LoRaWAN standard. Among others, this would guarantee that the devices obey power and modulation control exercised by the LoRa network to maximize network performance and scalability.

While KPN expects to be able to keep up the network performance in the face of a growing number of nodes, we doubt that the network will be able to perform the required power and modulation control. First of all, both forms of control are restricted by the maximum duty cycle imposed on the downlink, which means that the network may simply not have enough time to send control messages to all nodes in time. Second, power control in LoRa may be too slow for regulating the power of mobile (moving) nodes. To illustrate: a UMTS (3G) network performs power control as much as 1500 times per second[16] whereas the bands in which LoRa operates only allows a duty cycle of at most 1%. Nevertheless, KPN regards mobile nodes as an important use case, evidenced by the importance it puts on the localization abilities in LoRa.

Large-scale, short-range deployments of LPWA IoT

An interesting opportunity for further deployment for KPN's LoRa network is to equip KPN CPEs for DSL and fibre access with a short-range LoRaWAN base station. This would create a very fine-grained network and could solve indoor coverage issues (at least for consumers).

A similar initiative is ongoing in the UK, using CPE-like modules developed by Archos. [6] It would of course require new CPEs that are equipped with a LoRaWAN transceiver module, which is expensive. KPN currently already runs a public Wi-Fi network from the CPEs, which shows it has the infrastructure in place to deploy such services.

Regional and local LoRa networks

M2MServices, a provider of IT & telecom solutions, is deploying a LoRa network in Westland, a region in the western part of the Province of South Holland. The M2MServices cooperates with the company MCS, which started the program Sensoring Success. The goal of the program is to develop tangible and viable IoT-applications. The focus of M2M services is on the manifold presence of horticulturists in the Westland, who can benefit from better sensoring applications. The potential coverage of the network is 12.000 companies and 40.000 households. The complete network should have been deployed at the end of June 2016.

Other smaller LoRa deployments exist for instance in Eindhoven [11], Rotterdam [12] and Geleen [13]. In the coming years we expect that similar networks may be deployed at the regional or local level.

SIGFOX

In the Netherlands, a nationwide deployment of SIGFOX is operated by Aerea. Aerea is a relatively new player on the Dutch telecommunications market, and operates a network with close to nationwide coverage, using SIGFOX technology. [2] Aerea has recently joined a partnership with Tele2, operator of a Dutch LTE network, who will offer access through the Aerea network as a part of its M2M solutions, and will allow its customers to flexibly choose between LTE-based or SIGFOX-based access. [67]

Aerea is part of the SIGFOX partner network, boasting (as of June 2016) a coverage of 1.2 million km^2 in 20 countries (of which most are in Western Europe, with roll-out in process in the United States as well as Brazil), covering a population of 316 million. [63] Among others, SIGFOX appears to be of great interest to utilities in order to connect smart meters. [68]

Not much is known about the exact deployment of Aerea's network. From the coverage map (Figure 30), it appears that the number of sites is significantly lower than the 600+ sites deployed in the KPN network. People familiar with the matter suggest that Aerea (as of January 2016) operates about 50 sites in the Netherlands, and is planning to increase the number of sites to 300.

---

[16] A UMTS frame is transmitted in 10 ms and consists of 15 'Transmit Power Control' commands, which tell the user equipment what level of power to use when transmitting. This results in a power control frequency of 1500 Hz (15/10ms).

Figure 30 SIGFOX coverage as reported by Aerea for the Netherlands (May 2016) [63]

5.3 Capacity

As discussed in the earlier paragraphs, the capacity of wireless IoT networks is limited in two ways. First, there is an upper limit to the number of devices that can be active concurrently. Before this limit is reached, efficiency and reliability decrease while the number of devices increases. Second, capacity is limited simply by channel bandwidth, due to theoretical limits (i.e. the Shannon theorem) but also by duty cycle regulations, as well as the modulation and error correction mechanisms used by the different technologies.

Combining the device volume estimates with the knowledge about the behaviour and characteristics of the different technologies and networks discussed in this chapter, we can now answer the question whether supply meets demand. We modelled the expected number of devices per cell for both the LTE and LoRa networks[17]. A cell is defined as the area served by a single base station antenna[18]. In cells where the number of devices reaches a certain threshold, issues will arise. When exactly a cell will become too 'crowded' depends on various factors not included in the model, such as the number of messages that the devices send on average, the average payload size, usage patterns over the course of a day, and so on.

[17] While the methodology can also be applied to model SIGFOX capacity, we did not have enough information about the network and devices to do so at this point.

[18] Multiple antennas may be used for e.g. diversity reception, MIMO and beamforming – this is considered as one 'logical' antenna for our purposes. User equipment in LTE-M1 and LTE-M2 only uses a single antenna and does not support MIMO.

5.3.1 LTE-M1 and LTE-M2

Using data from the Dutch antenna registry, the coverage and capacity of LTE networks can be modelled – earlier research performed by Dialogic for the Radiocommunications Agency provides a methodology and software tool for doing so. [14].

While we are interested in LTE-M1 and LTE-M2 deployments, none of the Dutch operators appears to have already deployed such a network. Additionally, the antenna registry does not require registration of details that would allow us to see which antennas have either or all of the LTE-M variants enabled. Therefore, we need to make a few assumptions in order to model LTE-M1 and LTE-M2 capacity. First, we assume that operators will deploy LTE-M1 and LTE-M2 in-band in the lowest frequency bands currently available to them. Second, we assume that they do this using a software upgrade on all of their base stations, which implies that the same antennas are used with the parameters as listed in the registry (e.g. regarding height, transmit power, directionality and location).

Figure 31 shows the modelled coverage of the LTE network of operator KPN in band 20, which consists of more than 11,000 cells. As the link budget for LTE-M1 is equal to that of 'regular' LTE, coverage will be similar (although it may vary slightly depending on which part of the carrier is enabled for LTE-M1). For LTE-M2, the link budget is actually larger, and coverage will be better. Nevertheless this will only be noticeable near the edges of the covered area and deeply indoors, as coverage is nearly 100% over land in the Netherlands.

We subsequently randomly assigned each of the four mobile operators a quarter of the simulated devices. Each operator will hence connect roughly 2.15 million IoT devices. Figure 32 shows a histogram of the resulting modelled number of devices per cell. The majority of the cells contains no more than 1,000 devices. T-Mobile is the only operator where we find more than a few cells that contain over 10,000 devices. The cause for this deviation is the limited coverage of T-Mobile (as of February 2016) in the LTE 8 band - we expect T-Mobile's coverage to have improved since. Especially their cells near the edge of the Netherlands were, at the time, relative large and therefore contain a lot of devices in our modelling.

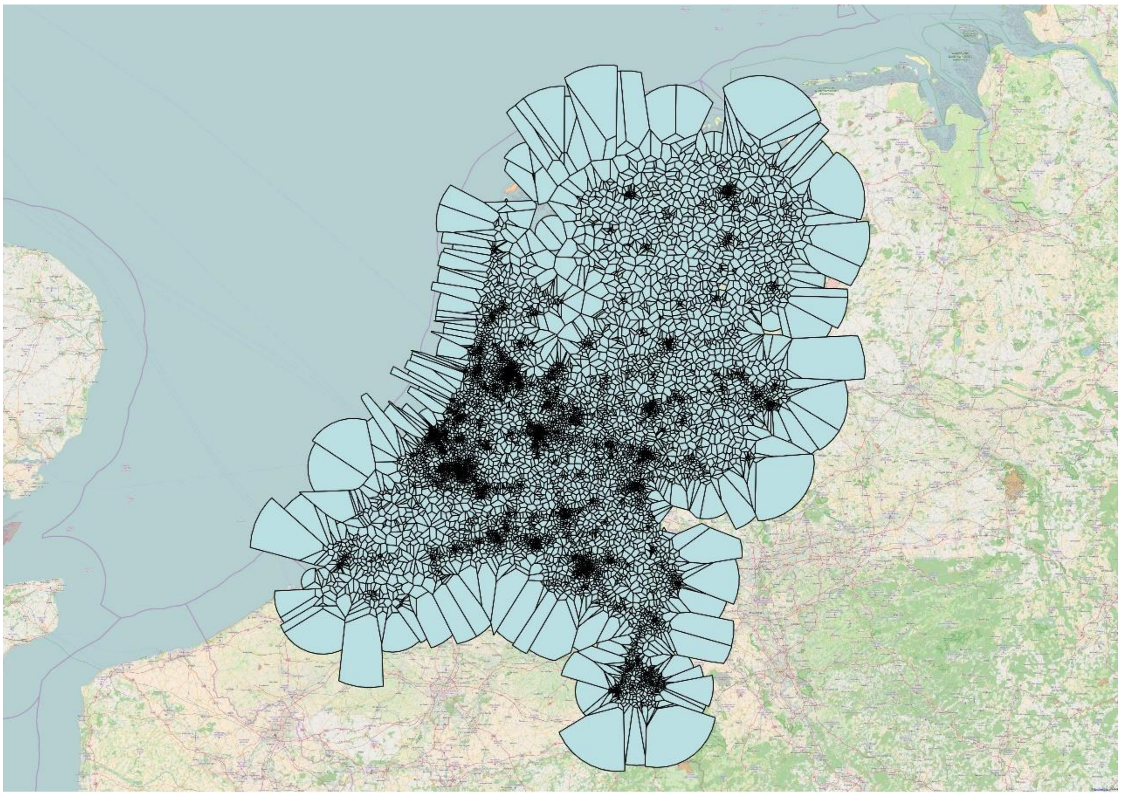

Figure 31 Modelled coverage of the LTE network operated by Dutch operator KPN in LTE band 20.

As discussed in paragraph 5.1, an LTE-M cell should be able to accommodate roughly 50,000 devices. [90] The maximum estimated amounts of 18,000 to 19,000 devices per cell of T-Mobile are still well below this threshold, so no problems are expected.

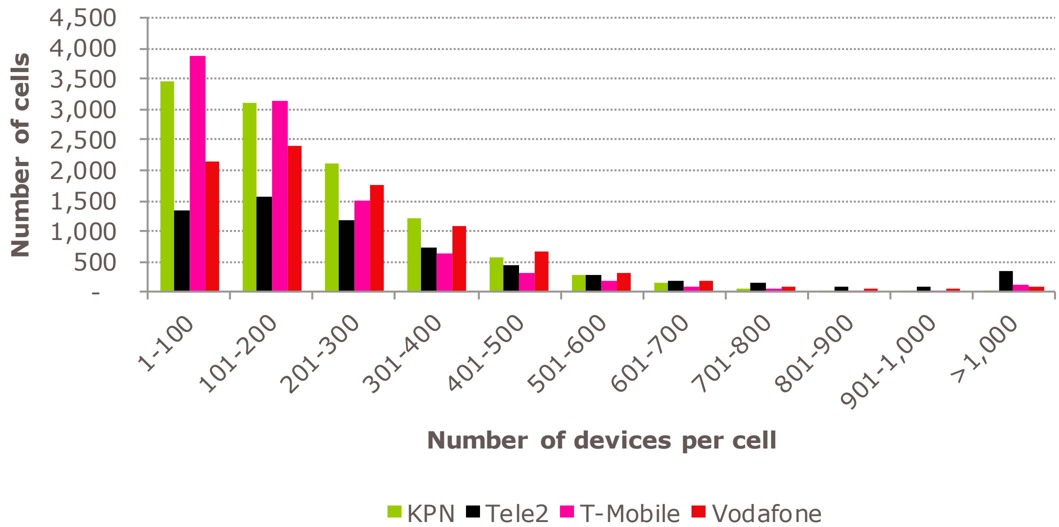

Figure 32 Histogram of the modelled number of device per cell (for LTE-M2)

5.3.2 LoRAWAN

KPN is currently the only operator who has a nationwide coverage with their LoRa network. We therefore use their network as an example in estimating the impact of LoRa-devices. The coverage of the LoRa-network is not as easy to construct because less information is available. While we could still use the tool that was used above for modelling LTE coverage, we had to include different scenarios varying on the following dimensions:

- **Number of sites.** KPN initially announced that it would deploy LoRa on 600 sites. They later indicated they will increase the number of sites to about a thousand to also achieve acceptable indoor coverage. (see 3.3.1)

- **Antennas:** It is not known whether KPN uses antennas that are sectorised or omnidirectional. All scenarios were hence calculated assuming either antenna type.

- **Desired coverage type:** KPN has almost reached complete outdoor coverage, but in some case (smart metering) indoor coverage is also necessary. We calculated scenarios for outdoor as well as indoor coverage.

- **Spreading factor:** LoRa devices can use different spreading factors. A lower spreading factor means a higher data rate, but also a lower coverage. As discussed earlier, there is uncertainty about whether the network will be able to 'steer' devices into using the most efficient spreading factor possible, and regarding the performance in the light of a high amount of concurrent users. We therefore assumed the worst and the best spreading factor in different scenarios.

In addition the assumptions described in the methodology section apply.

Table 13 shows the different scenarios and simulation results. The first five columns show scenario parameters whereas the latter three show the resulting coverage. The last column shows the total area covered divided by the total (land) area of the Netherlands. This figure is purely indicative: due to the nature of LoRa overlap between the different antennas will occur, so a coverage of 1x the Netherlands does not imply full coverage everywhere in the Netherlands (but more likely coverage in only a small part with overlap).

Table 13 LoRa simulation scenarios and results

Antenna type	Sites	Coverage	Spreading factor	Antenna gain (dBi)	Average cell area (km2)	Total area covered (km2)	Number of times the Netherlands
Omni	600	Indoor	SF12	5	42	25,297	0.61
Omni	600	Indoor	SF7	5	6	3,848	0.09
Omni	600	Outdoor	SF12	5	11,313	6,788,100	163.40
Omni	600	Outdoor	SF7	5	1,718	1,030,937	24.82
Sectoral	600	Indoor	SF12	5	14	25,182	0.61
Sectoral	600	Indoor	SF7	5	2	3,830	0.09
Sectoral	600	Outdoor	SF12	5	3,794	6,757,441	162.66
Sectoral	600	Outdoor	SF7	5	576	1,026,259	24.70
Sectoral	1,000	Indoor	SF12	5	13	39,364	0.95
Sectoral	1,000	Indoor	SF7	5	2	6,046	0.15
Sectoral	1,000	Outdoor	SF12	5	3,450	10,261,045	247.00
Sectoral	1,000	Outdoor	SF7	5	529	1,573,660	37.88

In Figure 33 the outdoor coverage for 1,000 directional antennas which can receive devices with the most efficient (but least resilient) form of modulation for LoRa (SF7) is given. The coverage is almost 38 times the surface of the Netherlands with an average cell area of 529 km^2. Also the indoor coverage for 1,000 directional antennas that are capable of receiving devices with SF12 modulation is given. The coverage is 0.95 times the surface of the Netherlands, with an average cell area of 13 km^2.

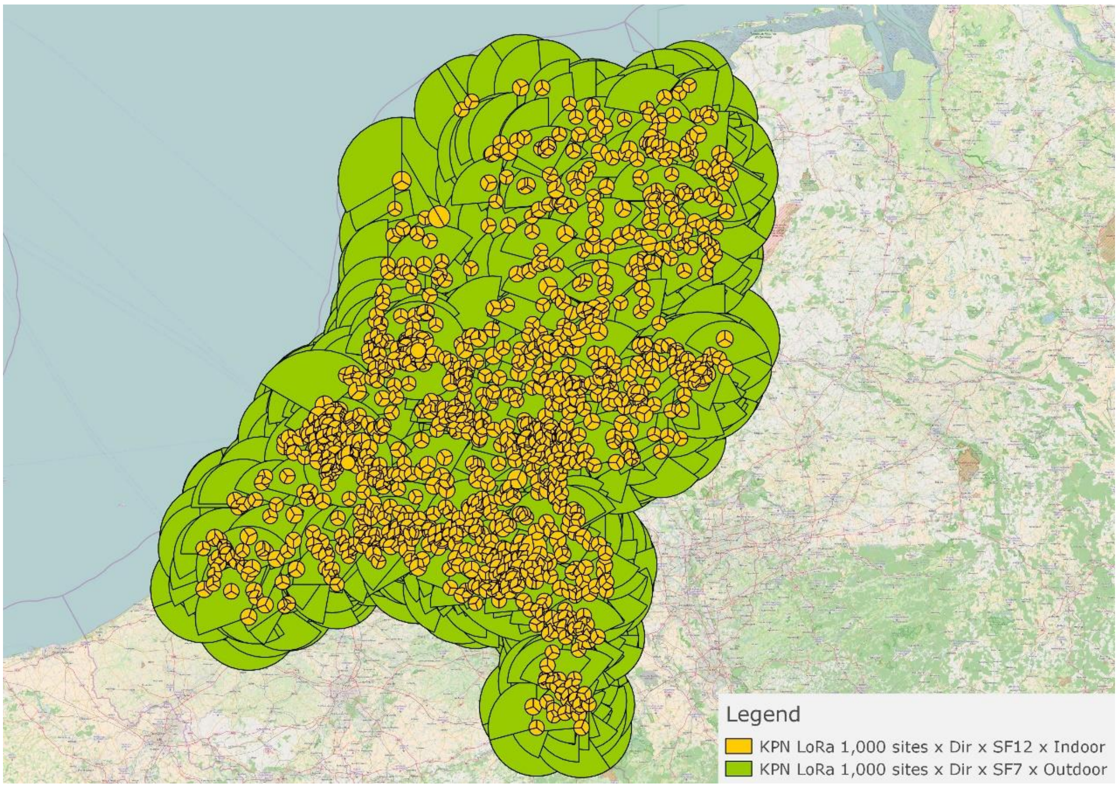

Figure 33 Modelled coverage (example) for KPN LoRa using directional antennas on 1,000 sites.

Impact

The impact on the LoRa-network is difficult to determine. First of al there is not an unambiguous maximum number of devices per cell, and second there is significant overlap between the cells. Figure 34 and Figure 35 show the total number of cells broken down by coverage requirement (indoor vs. outdoor).

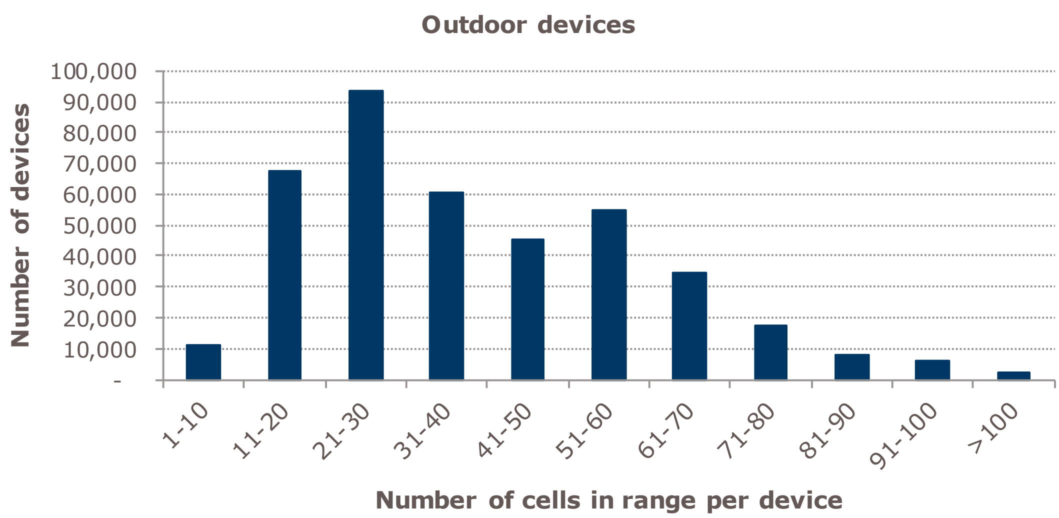

Figure 34 Histogram of modelled number of 'visible' cells per device (LoRa, outdoor)

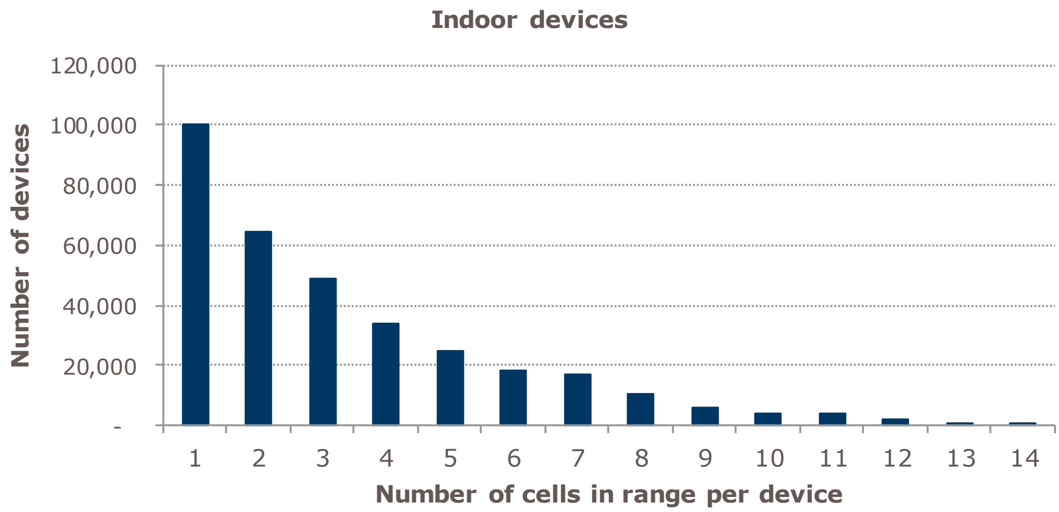

Figure 35 Histogram of modelled number of 'visible' cells per device (LoRa, indoor)

At any given point, a single LoRA device can be in range of multiple different base stations (in different 'cells'). If at least one of these base stations is not 'overcrowded' (i.e. in range of more than a certain amount of active devices), messages transmitted from the LoRA device will be successfully picked up by the network. The more base stations a device can reach, the higher its changes of successfully transmitting a message. However, if the coverage area of these base stations overlaps significantly, it is less likely that one of the base stations is not overcrowded while the other ones are. Increasing the number of base stations therefore should alleviate capacity issues, but only up to a certain point: as base station coverage starts to overlap, capacity increases only marginally.

To calculate the maximum number of devices a LoRa network can support, we first calculate the percentage of cells that are overcrowded given our expected distribution of devices over the different cells. We then calculate a lower and upper bound for the estimated success rate of a device transmission. In the pessimistic scenario, we assume that being in reach of multiple base stations does not improve a device's chance of transmitting successfully relative to the case where it only 'sees' a single base station. Under this assumption, the 'success rate' for a single device is equal to the overall success rate. Table 14 shows the estimates for various total device volumes and maximum number of devices per cell.

Table 14 Modelled percentage of devices experiencing impaired connectivity, assuming a pessimistic scenario where cell overlap provides zero benefit.

Total device volume	Maximum number of devices per cell			
	20,000	30,000	40,000	50,000
1 million	3.2%	0.8%	0.2%	0.0%
2 million	27.2%	8.5%	3.2%	1.0%
3 million	68.7%	27.2%	12.4%	5.8%
4 million	89.5%	54.5%	27.2%	15.3%
5 million	95.5%	79.4%	46.9%	27.2%
6 million	97.5%	89.5%	68.7%	42.5%
7 million	98.3%	94.1%	82.9%	60.9%
8 million	98.8%	96.2%	89.5%	75.8%

In the optimistic scenario, we assume that each additional base station that is in reach of a device provides another chance of successful transmission (e.g. if the global rate of success is 80%, and the device is in range of two base stations, its chances of successfully submitting a message to the network are 100% - $(100\% - 80\%)^2$ = 96%). The outcomes in Table 15 depict the failure rates in the favourable scenario.

Table 15 Modelled percentage of devices experiencing impaired connectivity, assuming an optimistic scenario where cell overlap provides maximal benefit.

Total device volume	Maximum number of devices per cell			
	20,000	30,000	40,000	50,000
1 million	0.4%	0.1%	0.0%	0.0%
2 million	4.5%	1.2%	0.4%	0.1%
3 million	17.9%	4.5%	1.8%	0.8%
4 million	35.8%	11.8%	4.5%	2.3%
5 million	51.9%	24.7%	9.4%	4.5%
6 million	64.2%	35.8%	17.9%	8.1%
7 million	72.2%	46.6%	27.8%	14.3%
8 million	78.5%	55.5%	35.8%	22.1%

Assuming a failure rate of 5% is acceptable, the KPN LoRa network should be able to deal with between 2-4 million active devices. The estimates shown in Table 14 and Table 15 indicate that at 3 million devices and assuming a maximum of 40,000 devices per cell, between 1.8% and 12.4% of the devices will experience connectivity failures. Having a large amount of cell overlap alleviates, but does not solve the capacity issues. The network operator will hence have to create smaller cells as the total device volume increases.

5.4 Overview

Deployment of LPWA IoT networks in licensed spectrum is expected to be gradual and smooth. In many cases, operators will use existing spectrum to deploy LTE-M1 or LTE-M2. Deployment will, for most operators, be a matter of a software upgrade, and will almost instantly provide nationwide, indoor coverage. Neither LTE-M1 nor LTE-M2 appear to be bound by concurrent usage issues, as these standards provide very good means for power control and concurrent access. While both are capacity-bound, operators can easily (and even dynamically) allocate other spectrum in their possession to IoT. Also new frequency bands, such as the 700 MHz band, are expected to become available in the near future that are usable for LTE.

An interesting question is whether the current operators will make an attempt to migrate existing machine-to-machine applications to the new LTE-based standards. Of particular interest are the users of the CDMA-450 network operated by Utility Connect and KPN. Today, this network is primarily used to read electricity and gas meters. In theory, this network can be upgraded to LTE in the same band (which in LTE is band 31).

The situation regarding IoT networks in unlicensed spectrum below 1 GHz is much more complex. The 863-870 MHz band, in particular the frequencies around 868 MHz, appear to be very popular for all technologies currently deployed at scale. In other parts of the world, these technologies also operate in the 902-928 MHz bands (North America) or in the 915-921 MHz bands, which is currently also under investigation for reallocation in Europe.

6 Interference, monitoring and enforcement

In this chapter, we analyse the different platforms for wireless IoT on their performance in practice, where they are used by a large number of concurrent users, and (in some cases) operate in spectrum that is also used for other purposes. First, we will discuss the behaviour of each technology in the light of concurrent use. Second, we will discuss interference between different applications in the same frequency band, which may or may not be other LPWA IoT applications. Finally, we will discuss how interference issues can be monitored by the Radiocommunications Agency for enforcement.

6.1 Multiple access

Multiple access refers to a situation where multiple transmitters *of a single application* want to make use of the same spectrum (same frequency band, same time period and not spatially separated). In order to prevent interference between different transmitters, wireless applications typically implement a form of medium access control (MAC). In this paragraph we explore the differences between multiple access control for LPWA IoT in licensed and unlicensed spectrum.

6.1.1 LPWA IoT in licensed spectrum

In licensed spectrum, only a single operator is ever allowed to transmit in a particular frequency band. If licenses for spectrum overlap in terms of frequencies, they are usually either spatially separated (e.g. one user is only allowed to transmit in places where the other is not active, or at a very low transmit power) or temporally separated from other licensed applications. Note that spectrum is usually licensed to the network operator only – end users may use certified (generally available) equipment to connect to public mobile networks.

Cellular networks are designed to efficiently allocate spectrum resources between users within the frequency bands in which a network operates. Typically, only a small portion of the spectrum used is 'random access' (e.g. intended for uncoordinated, user-originated communications) whereas all other spectrum is allocated by the network. In LTE, spectral capacity is divided in so-called *resource blocks*, which is basically a time slot in which a user terminal is allowed to transmit on a single subcarrier within an LTE frequency band.

Due to the fact that resource usage is almost completely controllable by the network, cellular networks (and LTE in particular) support very high amounts of concurrent use. In fact, below a certain number of devices, simulations suggest that multiple access is not concurrency- but rather capacity bound (see e.g. Figure 22 and Figure 23).

While cellular networks are typically designed to have greater capacity than is demanded most of the time, it is possible for operators to make trade-offs between users or applications on a wireless network in cases of congestion.[19]

[19] Note that this may be subject to net neutrality regulations if the service offered is 'internet access', which may or may not be the case for an IoT network. [54]

6.1.2 LPWA IoT in unlicensed spectrum

Like in licensed spectrum, multiple access for users of the same application is an issue that needs to be dealt with. In addition, different applications in unlicensed spectrum generally do not coordinate multiple access with each other (as opposed to for instance multiple base stations in a network operating in licensed spectrum). Regulation is in place to ensure that even in such a situation, eventually transmitters will have a chance to make an attempt to transmit. Regulations generally demand that transmitters in unlicensed bands use relatively low transmit power, and limit their *duty cycle* (percentage of time that the transmitter is transmitting). In some cases, there are additional requirements (e.g. to 'listen before transmit'). The different technologies for LPWA IoT each deal differently with these requirements in order to facilitate multiple access for their own users and cohabitation with other users.

SIGFOX

Although transmitters typically only send short messages and choose a random channel to do so, it becomes increasingly likely for collisions to occur when the number of devices increases. In order to mitigate the effects of a collision, SIGFOX transmitters typically send each message three or six times, each time at a different channel. While this decreases the efficiency of the spectrum usage per message, it increases the chances of the receiver actually being able to read the message transmitted.

Figure 36 shows the result of a simulation of the behaviour of SIGFOX, when 1000 devices are transmitting within 1 minutes with a configured redundancy of three retransmissions. Figure 37 shows how many collisions are likely to occur when the number of devices increases, in a scenario where devices are configured to always perform three transmissions. [88]

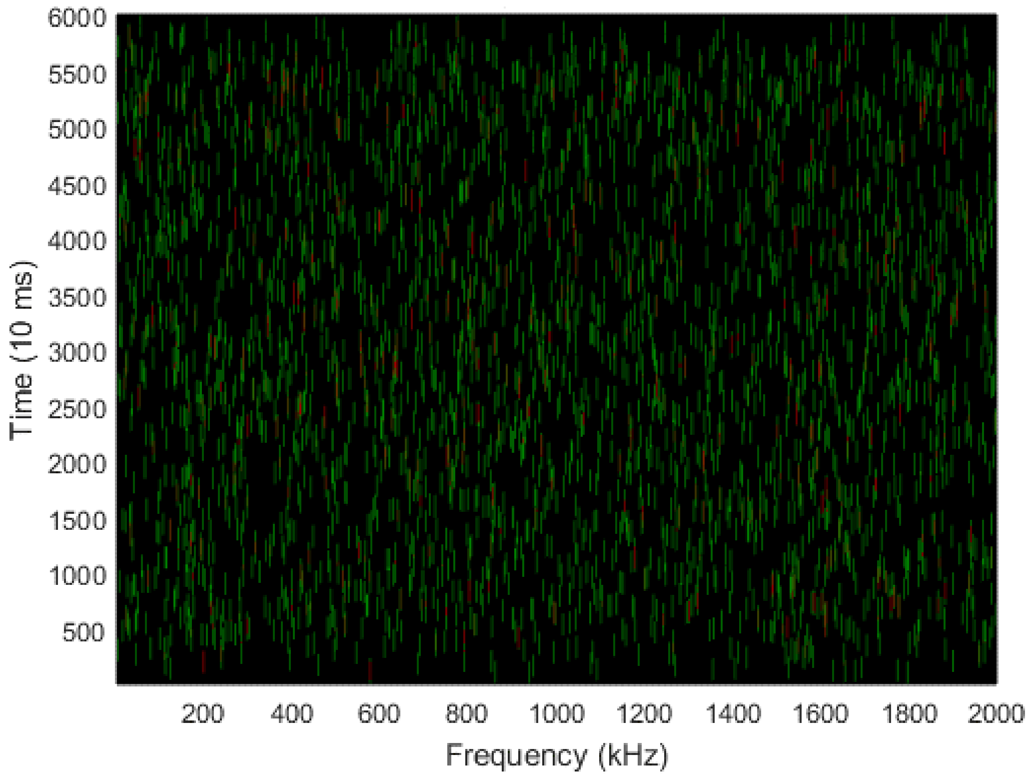

Figure 36 SIGFOX behaviour simulation in 200 kHz with 1000 devices transmitting randomly within 60 seconds (3 retries) [88]

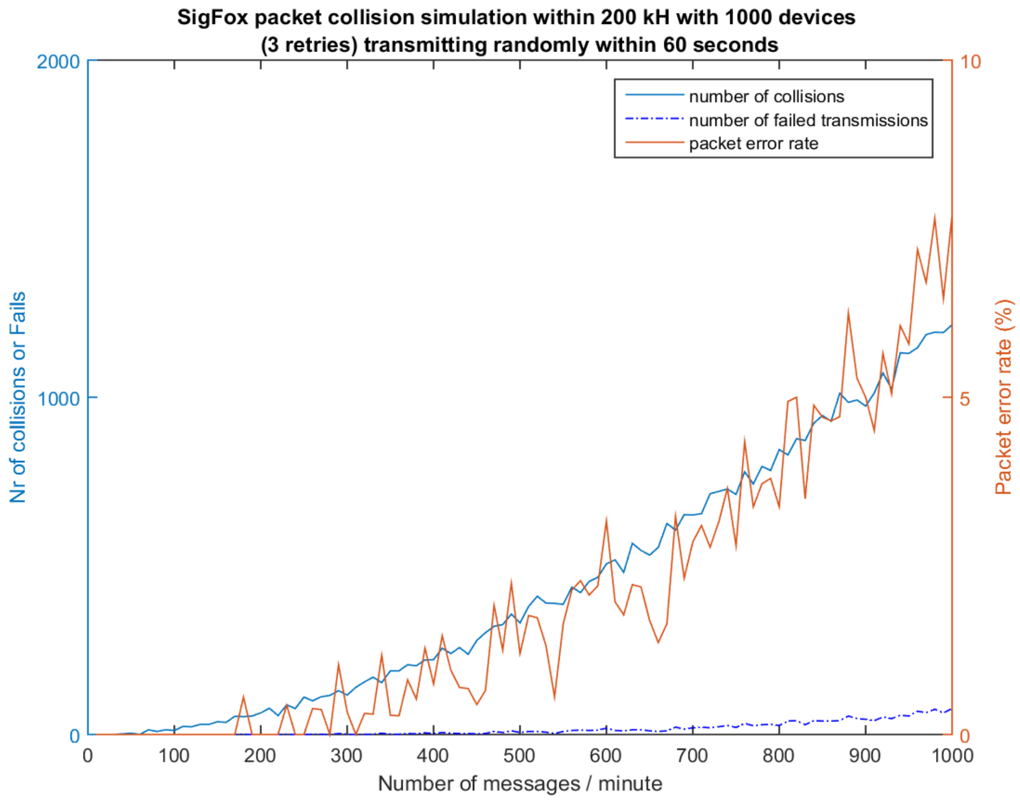

Figure 37 Number of collisions in SIGFOX simulation in 200 kHz with 1000 devices transmitting randomly within 60 seconds (3 retries) [88]

The simulated performance of SIGFOX shows that the system is quite resilient to errors resulting from collision from other SIGFOX transmitters. As the number of collisions increases, the number of SIGFOX messages that are not received stays relatively low. Figure 38 shows the behaviour of the technology with up to 10.000 devices each transmitting once during a minute. Note that this simulation does not take into account other types of interference or signal attenuation that may further degrade the packet error rates.

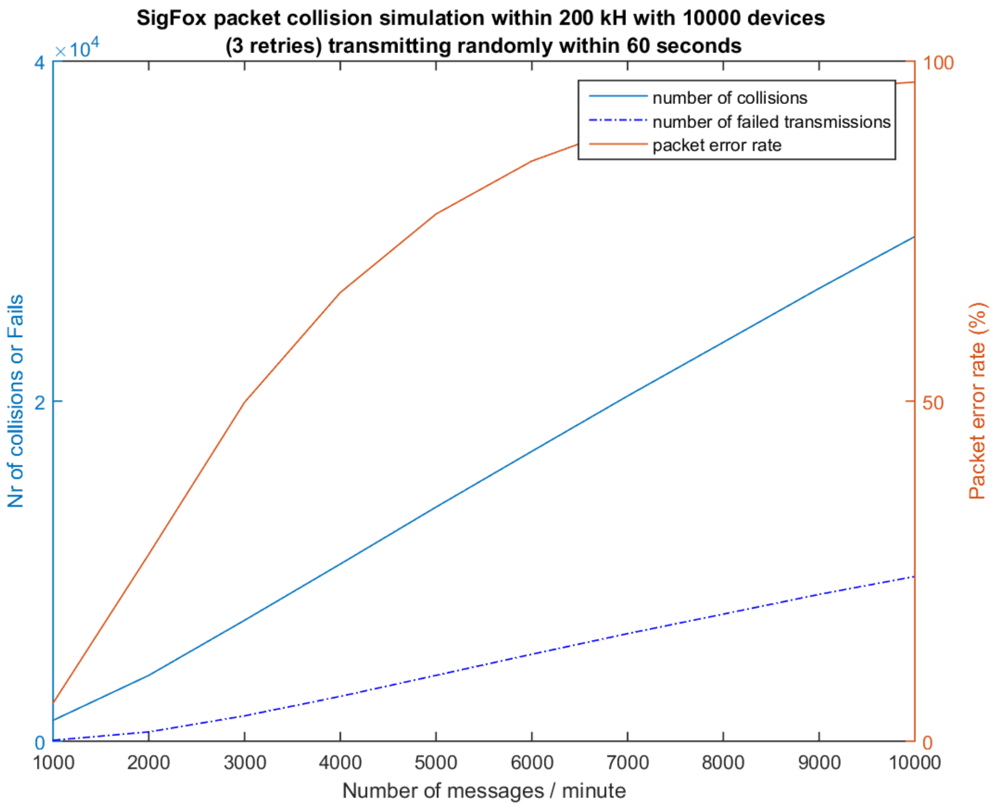

Figure 38 Number of collisions in SIGFOX simulation in 200 kHz with up to 10.000 devices transmitting randomly within 60 seconds (3 retries) [49]

Note that these simulations concern a theoretical situation with only a single base station. Adding more than one base station will further increase the chances of receiving a message (even while also further increasing geographical coverage, thereby increasing the chance of other collisions). Note also that the simulations assume that channels are perfectly separated. As an online commenter to the results remarks: "*A 1 PPM crystal error (i.e. if using a TCXO) results in 868 Hz of carrier frequency error. Your simulation should assume that any two adjacent in freq [sic] packets will likely collide at a minimum*". [49]

An important difference between SIGFOX and LoRaWAN is that while LoRaWAN can and will dictate the power that devices should use to transmit to the network, SIGFOX cannot, and does not have to. Having power control makes LoRaWAN a better neighbour (at least in theory) for other users of unlicensed spectrum as the devices in the network can use lower transmit power when this is sufficient. On the other hand, the LoRaWAN network does have to send periodic power control commands to devices.

LoRaWAN

As for SIGFOX, simulations were performed regarding the impact of collisions between multiple LoRaWAN users. Figure 39 and Figure 40 show the results of these simulations for a scenario where devices transmit at a random spreading factor or the highest (SF12) spreading factor, respectively. Note that the former is not a realistic scenario, as the devices will choose their spreading factor either at command of the network, or by configuration. The latter scenario is strictly a worst-case scenario, in which all devices in the network use the least efficient modulation rate. [88]

Note that even while in the best case there are 31 channels that devices can choose from, it appears the LoRaWAN standard dictates the use of three specific channels for sign-on and device calling features.

As is the case for SIGFOX, adding additional base stations would increase the chances of a message being picked up by at least one base station in the network. In the case of LoRa, it might even enable the use of lower spreading factors and increase overall network performance, depending on the network's ability to coordinate power control and the amount of overlap in coverage between base stations.

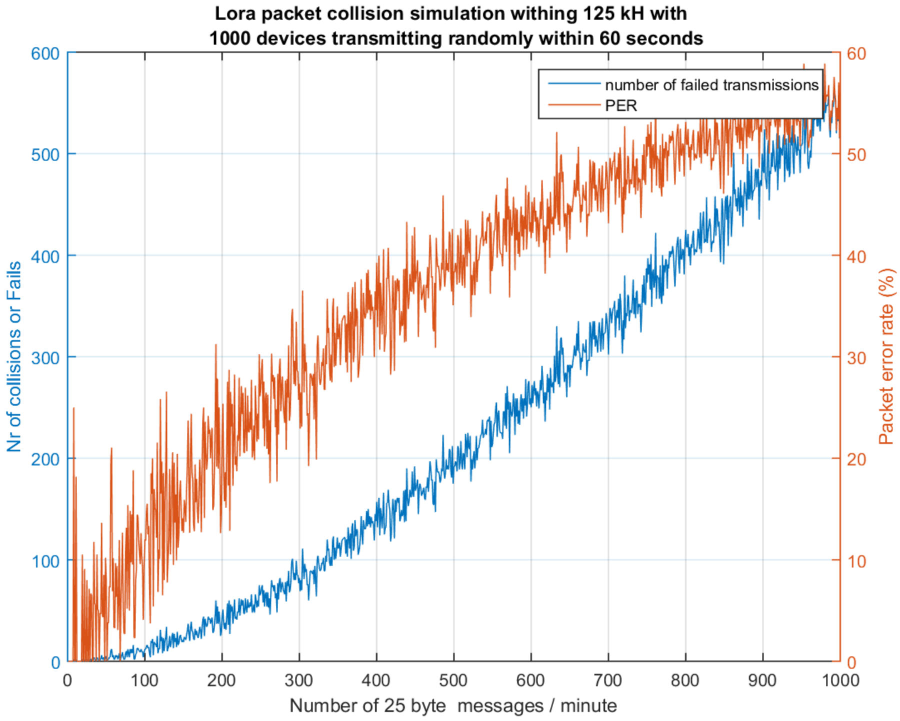

Figure 39 LoRa packet collision simulation within 125 kHz with 1000 devices transmitting randomly within 60 seconds using a randomly selected spreading factor [88]

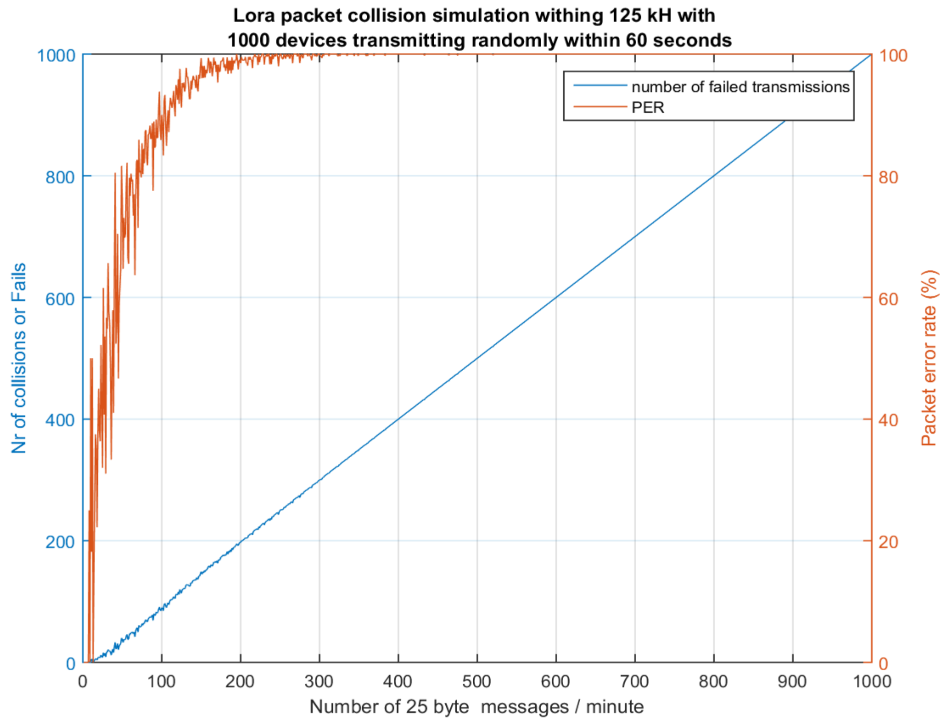

Figure 40 LoRa packet collision simulation within 125 kHz with 1000 devices transmitting randomly within 60 seconds using SF12 (worst case scenario) [88]

The study performed by RealWireless referenced earlier for SIGFOX also provides useful results regarding the number of simultaneous users possible in LoRa. Real Wireless found that the number of simultaneous users in a spread spectrum environment is around 60 to 70 per base station – above this number of users, the base station noise rises quickly above usable levels (Figure 41). Note that Real Wireless assumes 'perfect' power control which, as discussed earlier, the power control in LoRaWAN is not. Imperfect power control causes transmissions from different devices to arrive at the base station at different power levels.

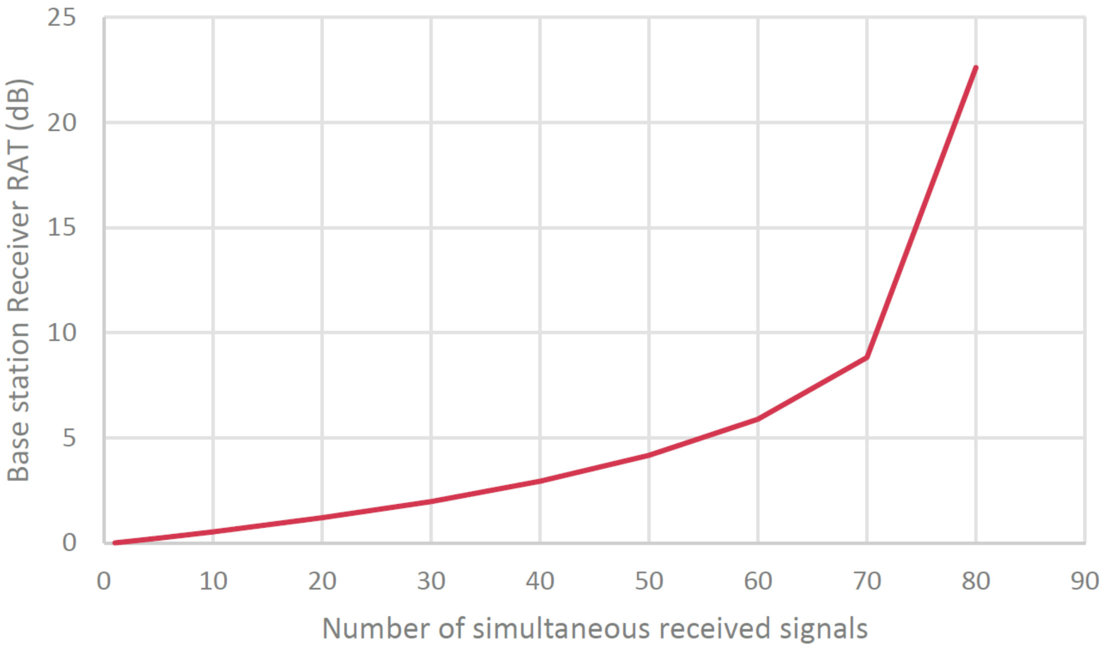

Figure 41 Base station noise rise simulation for multiple uplink transmissions with perfect power control [52]

From the simulations, it appears that SIGFOX is a superior technology when it comes to multiple access, at least under static conditions. Ultra-narrowband modulation effectively divides a frequency band in a large number of channels, which (when all users distribute their traffic over all channels equally) significantly lowers the chance of a collision. The downside of ultra-narrowband is that a message takes a relatively long time to transmit. For mobile (moving) devices, the signal may fluctuate while transmitting, decreasing the chances of proper reception.

The performance of LoRa in multiple access scenarios depends greatly on the modulation type and transmit power chosen by the transmitting devices. Unlike SIGFOX, LoRaWAN provides the network with means to dictate both parameters to the devices (although at a certain moment the device may choose to increase transmit power or use a more resilient modulation). A second point of concern is that as the duty cycle regulations also apply to the LoRa base stations, the time these base stations have to regulate power and control modulation of devices is very limited. For mobile clients, power control will likely be too slow to allow for the most appropriate modulation type (e.g. that with the lowest possible level of redundancy) to be used.

6.2 Interference

When multiple access control (see paragraph 6.1) fails, or transmitters of different applications do not coordinate spectrum usage between each other, interference may occur. Interference is a situation where two or more radio transmitters attempt a transmission, but where either or all transmissions may fail to be received properly because spectrum usage overlaps in time, space and frequency bands (either fully or partially during transmission). The result of interference is 'wasted spectrum capacity' – no useful information was transferred during the time the interference took place, and the transmitters will generally make an attempt at retransmission if they have the means to detect that interference has occurred.

In this chapter, we will explore different scenarios for interference. First of all, there may be interference between different LPWA IoT networks – as there is generally no more than one

LPWA network active in a licensed spectrum, this is primarily a concern in unlicensed spectrum. Second, and again typically only in unlicensed spectrum, there may be interference between existing other users.

6.2.1 Interference between LPWA IoT networks

LPWA IoT technologies for use in unlicensed spectrum are typically designed for operation with very generous link budgets – this followed from the limited transmit power allowed in the unlicensed bands. A consequence is that a large fraction of the area covered by a cell is subject to very high path loss, as shown in Figure 42 from a study performed by RealWireless. [52]

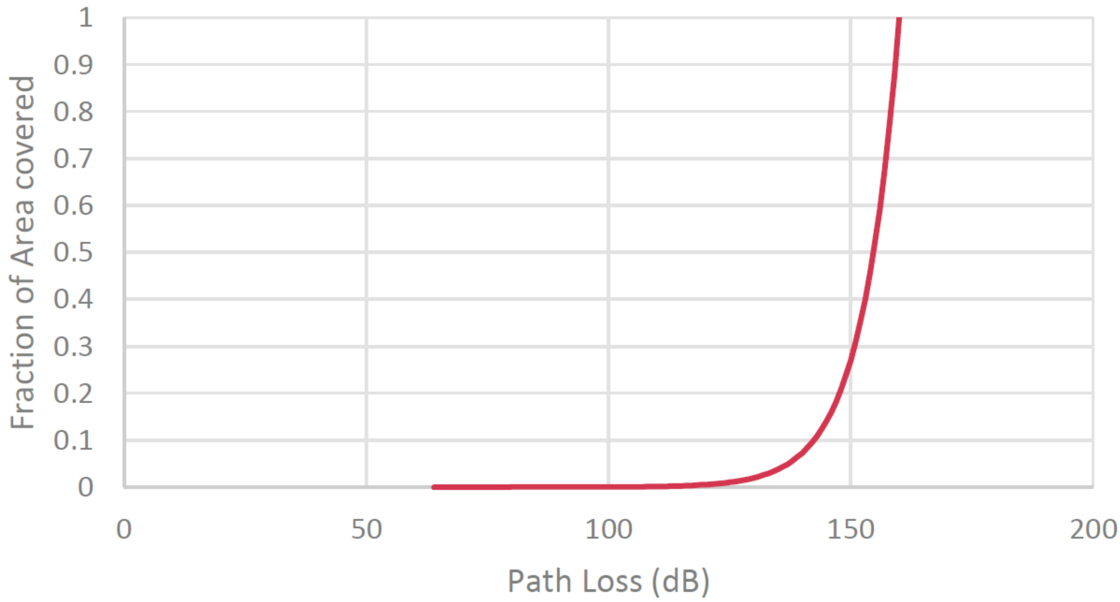

Figure 42 Fraction of a cell covered with increasing path loss following from simulation [52][20]

The skewed distribution of path loss over coverage area is a primary reason for interference between ultra-narrowband and other types of systems (e.g. between SIGFOX and LoRa). The main reason for this is that interference will be at relatively high levels of power for a majority of users (as many users operate at high levels of path loss, as demonstrated in Figure 42). RealWireless have analysed interference between ultra-narrowband and (chirp) spread spectrum systems and distinguish six different interference scenarios, as shown in Table 16.

[20] RealWireless assumed an urban Hata model with 20 m base station antenna height and the end-point devices at a height of 1.5m with a penetration loss of 15dB, and circular coverage.

Table 16 Interference scenarios between ultra-narrowband and spread spectrum users [52]

	Victim Systems	
Aggressor Systems	UNB	Spread Spectrum
Own network UNB	Re-transmission strategy part of normal operation. Dimensioned to contain clash probability to acceptable levels	N/A
Other network UNB	Increased uplink clashes can be mitigated by using more channels and additional base station processing. Frequency re-planning may be needed to avoid interference.	Difficult to avoid impact of multiple simultaneous interference across wideband carrier. Impact worse on uplink, reducing range with the potential for some nearby interferers to block base station receiver.
Own network Spread spectrum	N/A	Intra-system interference will constrain (uplink) capacity – particularly with imperfect power control. Splitting users into 'near' and 'far' groups on different frequency channels can reduce impact but may not be feasible for mobile/nomadic end-points.
Other network Spread spectrum	Difficult to avoid impact of multiple simultaneous interference across all overlapped UNB carriers. Impact worse on uplink, reducing range with the potential for some nearby interferers to block base station receiver. Co-located base stations employing power control would mitigate interference – making deployment co-ordinated.	Difficult to avoid impact of multiple simultaneous interference across all overlapped carriers. Impact worse on uplink, reducing range with the potential for some nearby interferers to block base station receiver. Co-located base stations employing power control would mitigate interference – making deployment co-ordinated.

RealWireless suggest that spread spectrum systems are more likely to be a 'bad neighbour' to other users of unlicensed spectrum. [52] Figure 43 shows a simulation of the number of users blocked, given an increasing number of simultaneous interferers. At 40 simultaneous interferers, which is an achievable, realistic estimate, already (at least) 66% of the users is blocked.

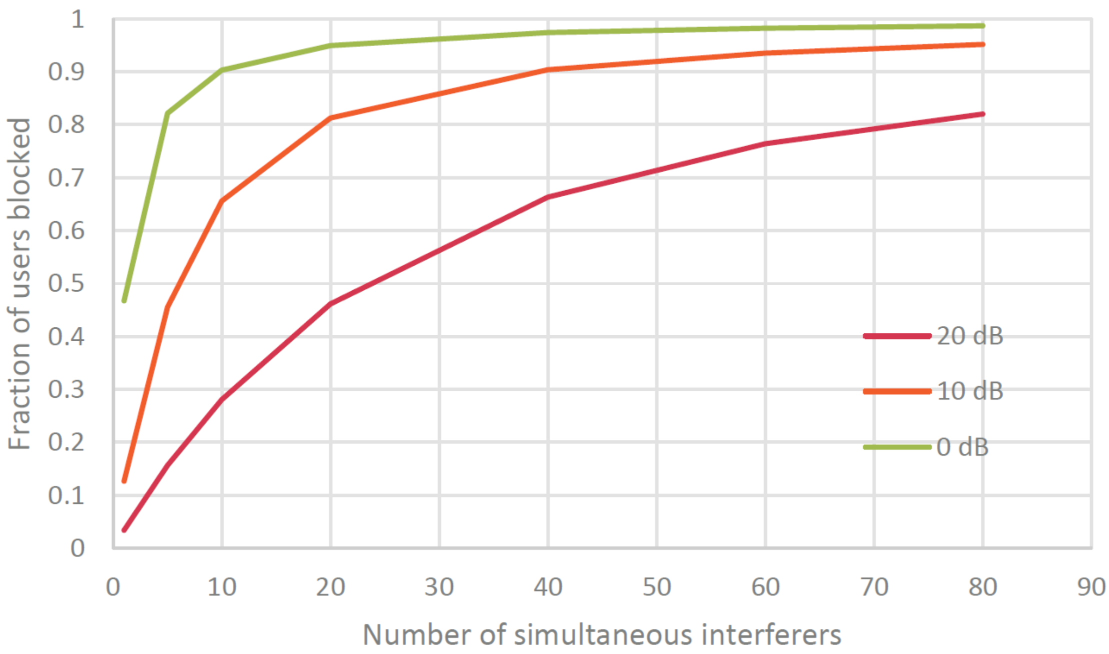

Figure 43 Modelled fraction of users blocked as the number of simultaneous interferers increases [52]

6.2.2 Interference between LPWA IoT networks and existing users

Traditionally, unlicensed spectrum has been used for short range applications – the technology that brought the generous link budgets that allow for long range applications has only become available recently. Interference in the unlicensed bands (at least those of interest for LPWA IoT) has generally been either very local, or the result of users not adhering to the regulatory limits. With traditional methods for monitoring, the only way to detect local interference is with either using a very dense monitoring network, or using mobile monitoring nodes. Interference caused by non-adherence to regulation is easier to detect if the interference is the result of excessive transmit power.

Even with the limitations on (current) monitoring capabilities in unlicensed bands and the detectability of interference, data from the monitoring systems of the Dutch Radiocommunications Agency provides useful insights in the situation in the unlicensed bands to which the LPWA IoT networks are attracted. Figure 44 up to and including Figure 46 show measurements of the 863-870 MHz bands performed in November of 2015. Horizontally the figures show different parts of the band (with a resolution of 5 kHz). Vertically shown is time, ranging from 0 minutes (midnight) to 1440 minutes (midnight the next day) with one minute resolution. The colouring indicates the level of power used during that time interval. From the figures, several interesting patterns can be observed:

- *Frequent/strong signals.* In Figure 44, several signals can be seen that are present frequently, and also relatively strong (around 30 dB above the noise floor).
- *Cyclic signals.* The upper part of the band shown in Figure 44 shows repeating patterns. Figure 45 also shows repeating patterns, which alternate between different frequencies within the band.
- *Full duty cycle signals*. Figure 46 shows that near Schiphol, several frequencies were in use for almost 24 hours consecutively at 100 kHz of bandwidth.

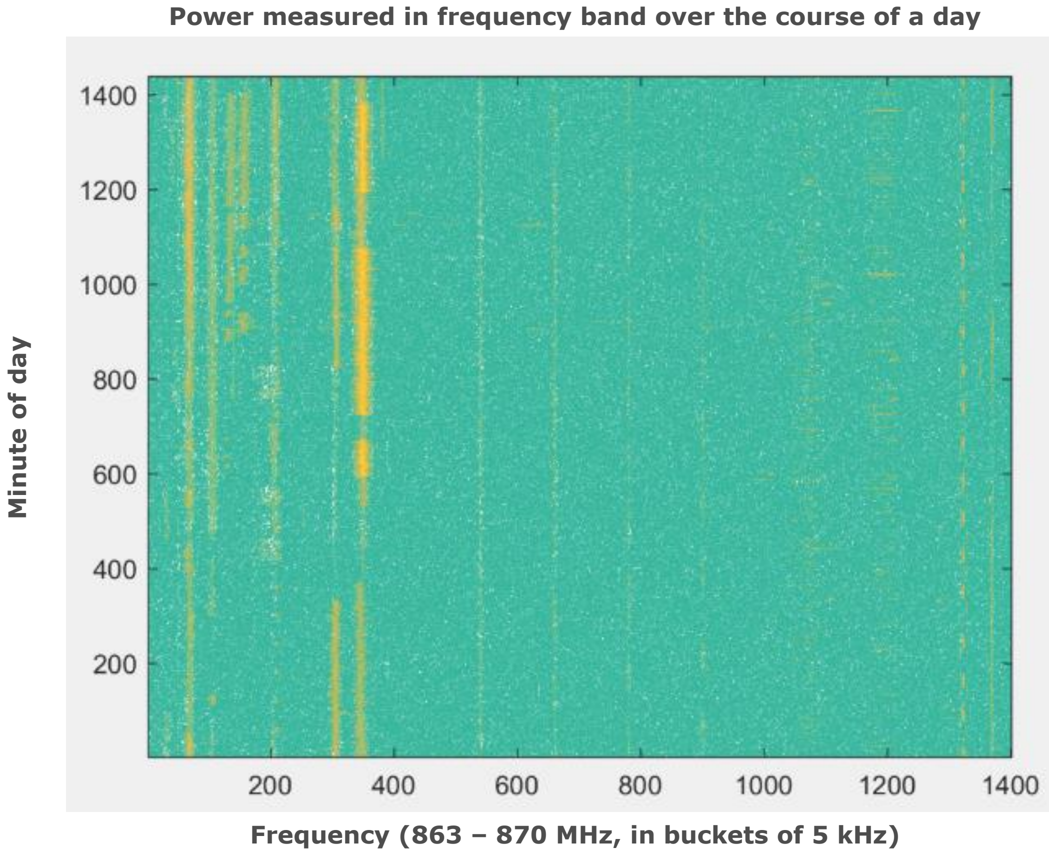

Figure 44 Measurement of the 863-870 MHz frequency band over the course of a day in Breda on November 27th 2015

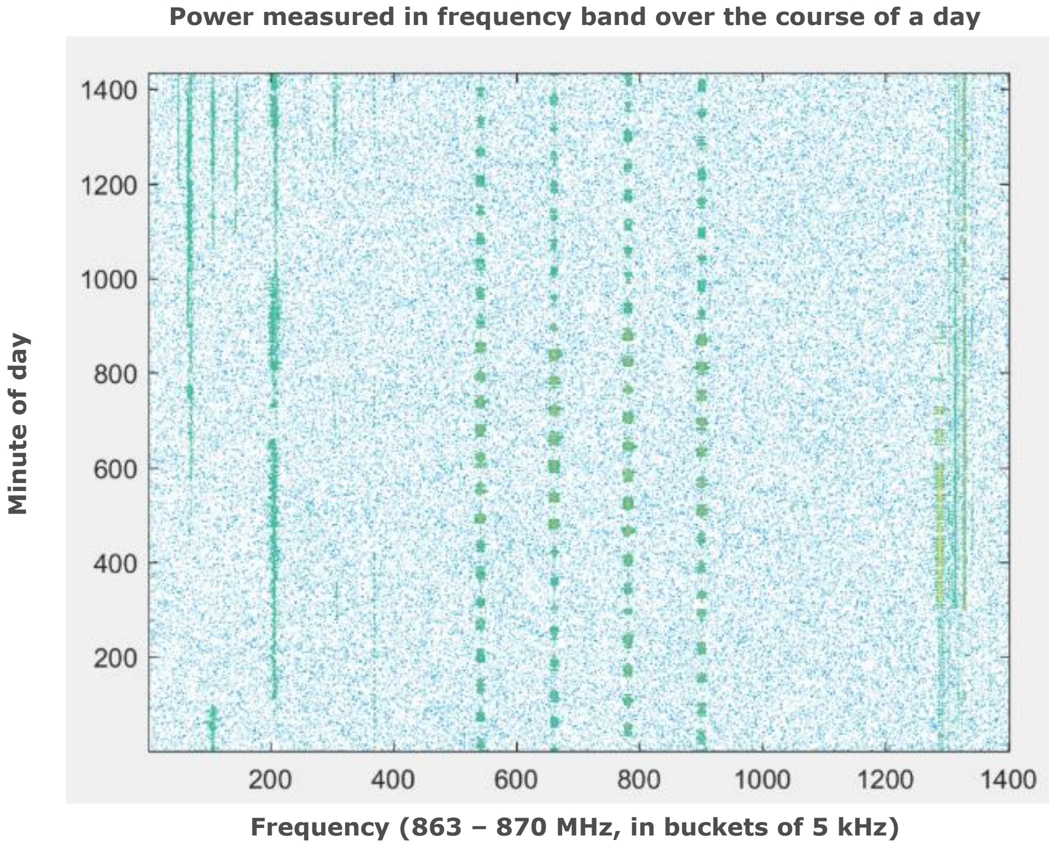

Figure 45 Measurement of the 863-870 MHz frequency band over the course of a day in Axel on November 27th 2015

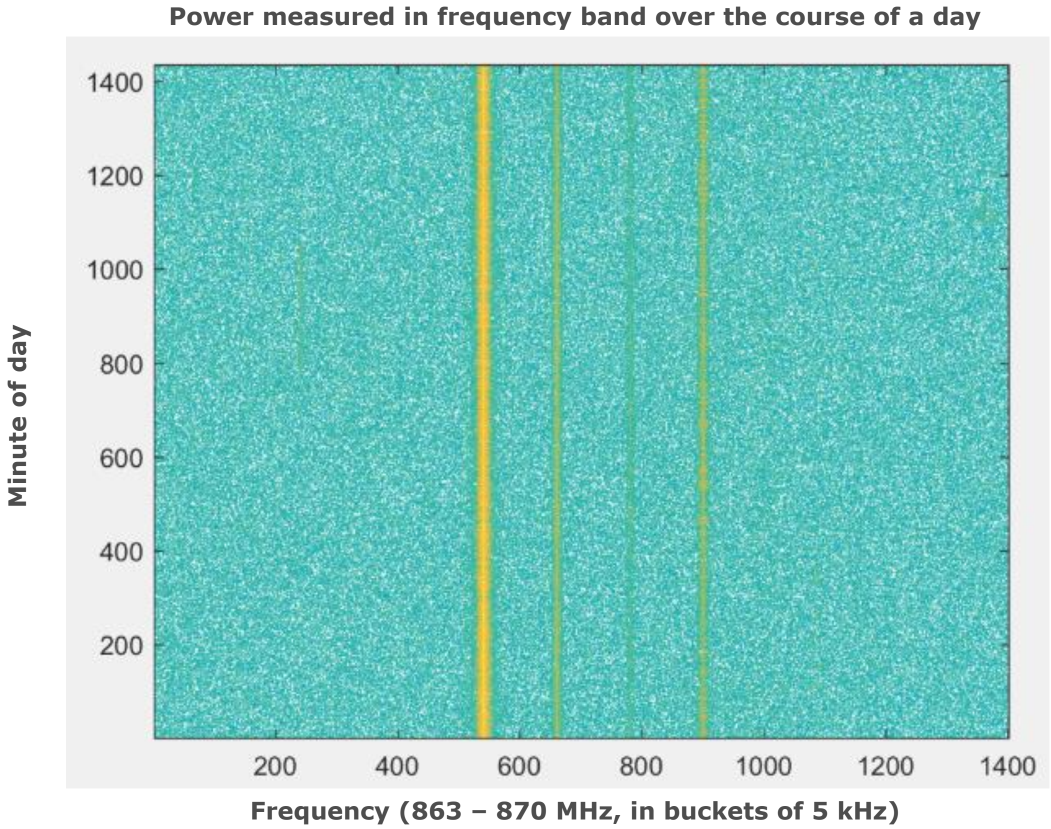

Figure 46 Measurement of the 863-870 MHz frequency band over the course of a day at Schiphol on November 26th 2015

In general, quite a number of channels in the 863-870 MHz band show occupation all across the day. In-between these channels there are still many channels available which do not show any frequent occupation. A few channels show more intensive usage during daytime than at night.

The distribution of signal power levels seems to be relatively consistent over different monitoring nodes. Figure 47 shows the distribution of signals as measured in Hoek van Holland on November 27th, 2015, and is representative for the other measurement nodes on that day. Most samples are below 20 dbµV/m and only a very small percentage shows much higher values.

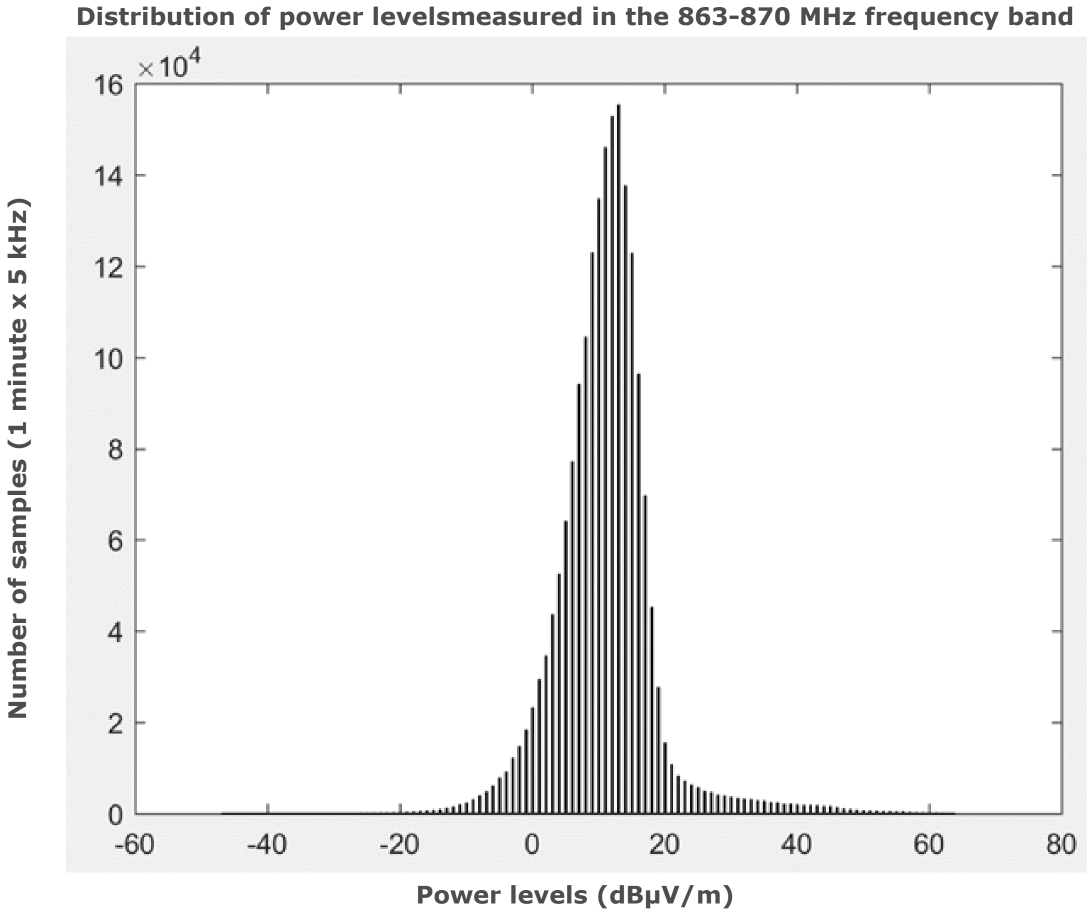

Figure 47 Distribution of signal power levels as measured in Hoek van Holland on November 27th, 2015. Horizontally shown is the signal level in dBµV/m. Vertically shown is the number of samples (total number of samples is 1,440 x 1,400 = 2,016,000).

All patterns displayed can point to different types of users. A recent report by Telecompaper [71] suggests different users and device volumes for unlicensed spectrum applications. From both sources we suspect the following to be the most important origins of interference in the context of LPWA networks:

- *Cordless microphones*. These typically exhibit a 100% duty cycle (e.g. transmit continuously over long periods of time), and can be fully legitimate.

- *Long-range cordless telephones*. Like microphones, cordless long-range telephones transmit continuously during very long time periods. It appears that cordless phones are currently available in the Netherlands and meet the applicable regulations even though elsewhere the same devices seem to be capable to operate at levels as high as 500 mW. Some vendors provide external antennas to increase the range. It isn't known if there are instructions on how to 'unlock' the higher transmit power on phones where it is disabled to comply with regulations.

Needless to say, the unlicensed bands contain a very large number of different device types of varying quality. In general, many illegitimate origins of interference will be devices that are certified for operation in countries other than the Netherlands, and are imported. In some cases, imported devices are allowed to operate in the Netherlands but at lower power levels. Some of these devices allow users to change the transmit power from software.

Legitimate sources of interference include RFIDs, as discussed earlier. These do not seem to appear in the measurements obtained from the monitoring network. Nevertheless we expect the interference caused by RFIDs to be very local and also quite prominent in the places where RFID readers are active. LPWA networks will likely directly notice RFID readers close to base stations.

Note that in this paragraph, we have primarily focused on the 863-870 MHz frequency band. We expect the situation to be similar for the 433 MHz bands. Nevertheless, this band is less attractive for IoT applications due to the fact that it is less wide and requires larger antennas.

6.2.3 Interference from RFID

In Europe, RFID is used in the 868 MHz frequency band, which is also used for short range applications, and is also one of the frequency bands used by LPWA IoT networks. RFID uses relatively high power transmissions, in order to power the transmitter in the RFID tag. The high power transmissions may locally cause issues with other applications using the unlicensed frequency band.

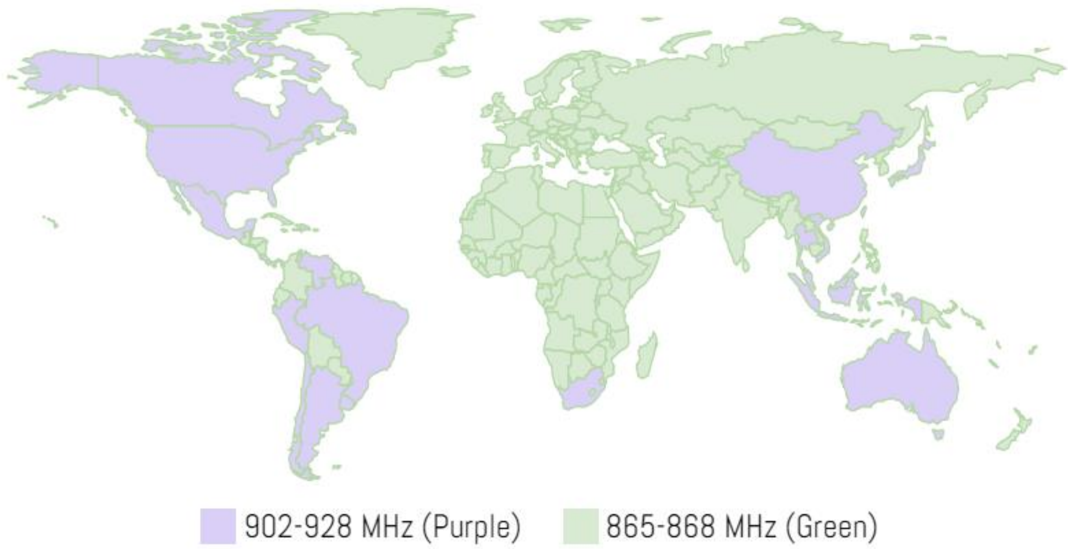

Figure 48 Overview of frequency bands in use for RFID around the world as of 2014 [57]

Aggravating the issue is the fact that many RFID tags operate either in the 902-928 MHz and 865-868 MHz frequency ranges (see Figure 48), whereas the former (in the Netherlands) needs to be read exclusively using equipment in the latter band, which is a range also designated to other unlicensed applications. As the frequencies do not match, the power required to read a tag is much higher than necessary if the tag would be read out at the design frequency. Allowing the use of tags in the 915-921 MHz range would be beneficial for a variety of RFID users (especially because of 'source tagging' – where a good is tagged at the beginning of the value chain). [19] [20]

Possible mitigations

At the European level, there is a push to free the 915 – 921 MHz frequency band, which currently in the Netherlands is used for military and security-related purposes. [5] The band is of particular interest as it would be globally available and highly suited for RFID usage (together with GSM-R as the primary user[21] - ETSI is performing studies to find out whether RFID and GSM-R can co-exist in the 915-921 MHz band [26]).

The CEPT has made a recommendation (ECC 70-03) to set out the general positon on common spectrum allocations for SRDs for countries within the CEPT [15]. Specifically for the 915 – 921 MHz frequency band the status of the implementation by each of the countries within the CEPT (at the moment of writing this report) is given in Figure 49. If a country has implemented the recommendation of the CEPT, IoT services can be deployed.

The information is based on appendix 1 of the ECC recommendation 70-03, a supplementing questionnaire of the ECC [18], and information gathered by GS1 [29]. Several countries have not implemented the recommendation of the CEPT but (1) do not use the band at all, (2) use the band for non-critical applications such as PMR/PAMR or (3) use the band for critical applications like governmental security. Some countries are considering splitting the band, and allowing usage of parts of the band under certain conditions.

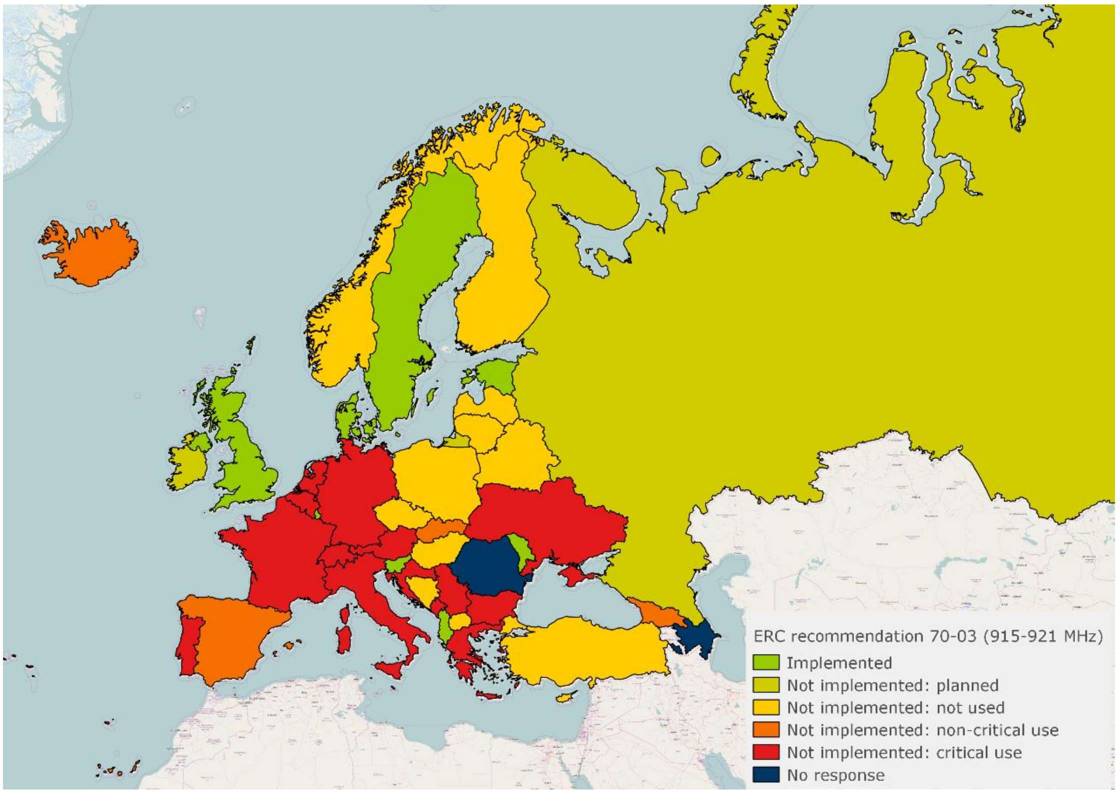

Figure 49 Usage of 915-921 MHz frequency band in Europe [18]

6.3 Spectrum monitoring

In this paragraph we discuss how a regulator can monitor the impact of IoT on the spectrum. First of all, we discuss the objectives for monitoring. Second, we will describe existing and new monitoring instruments and their relevance for monitoring IoT. Finally, we will devise a monitoring strategy.

[21] In order to guarantee an interference-free coexistence between the two systems, ETSI ERM TG34 has developed mitigation techniques in STF 397 Phases 1 and 2 defined in Technical Specifications TS 102 902 and TS 102 903.

6.3.1 Objectives

The main objective of monitoring is to verify whether the available spectrum for radio communications is used appropriately at any given time and any location to which spectrum regulations apply. Spectrum monitoring hence concerns three dimensions: frequency, time and place. The Dutch Radiocommunications Agency currently has a monitoring network in place that can collect information on all three dimensions.

In this paragraph, we will discuss strategies for monitoring wireless IoT applications and their impact on the spectrum. As discussed earlier in this report, the impact of wireless IoT on the spectrum differs greatly between long range and short range applications. We will therefore discuss the two levels separately, and consider the following monitoring objectives:

1. Obtain information on spectrum utilization by IoT applications (supporting spectrum management)

2. Obtain information on the spectral efficiency of the IoT applications (supporting standardisation work)

3. Detect generic issues related to the use of spectrum by IoT applications (supporting enforcement and spectrum management)

4. Troubleshoot specific issues related to interference caused by or harming IoT applications (supporting enforcement)

We will discuss each monitoring objective in more detail below.

Obtaining information on spectrum utilization by IoT

Knowing the utilization of spectrum available to IoT applications is crucial in determining future policy action regarding spectrum allocation. As discussed earlier, we expect capacity issues to appear primarily in unlicensed bands, as in licensed bands, operators currently have ample space to support growth of IoT, and have the required spectrum under their sole control. In the unlicensed spectrum however, over-utilization may not only cause a capacity problem, but also degrade performance for existing users.

In order to be able to monitor the spectrum utilization of IoT applications in unlicensed bands, measurement need to be made in the relevant bands. High-level measurements indicating the average level of power in the band over fixed intervals of time provide a very useful starting point to obtain insights in the development of the band's usage over time. Such measurement however do not provide further information on the type of usage in the band (e.g. is increased usage caused by IoT or by other applications using the same band). Knowing which application is using a band is however not always possible. Nevertheless, the transmissions performed by the handful of IoT technololgies currently in use can be identified and (to some extent) decoded using state-of-the-art monitoring equipment.

Obtaining information on the spectral efficiency of IoT

As spectrum is a scarce resource, the regulator ideally would like the users of the spectrum to use as little spectrum for an application as possible. In order to gain insight in the efficiency of spectrum usage by IoT applications, one should therefore monitor the total volume of useful payload, and compare it to the spectrum that was used in order to transmit that data; the more useful data was transmitted given the same amount of spectrum, the better. This can be measured either for a single application in isolation, or for a system of IoT networks as a whole.

In licensed spectrum, there are only a handful of technologies available for IoT (mainly the LTE-M standards). The efficiency characteristics of these standards are known and as the spectrum is fully under control of the operator, efficiency does not vary much between deployments and specific situations. Monitoring such deployments probably only requires obtaining information on the specific variants of technology currently deployed.

For unlicensed spectrum, monitoring spectral efficiency is more difficult. A system that monitors spectral efficiency must somehow 'know' about the the useful data being transmitted by an IoT application in order to be able to judge whether the spectrum utilisation observed is acceptable. While it would in some cases be possible to decode IoT transmissions and measure (useful) payload length, the efficiency is still unknown, as one would need to know the exact destination of the message (e.g. to estimate propagation path length) as well as correlate other transmissions (e.g. retransmissions) and know whether a message was received properly or not.

Detecting generic issues related to the use of spectrum by IoT

We expect the following three key issues to emerge in the unlicensed bands following wireless IoT adoption:

- ***The mix of short range and long range usage***
  Short range usage can still be increased even in a highly loaded band. The key consequence is that the short range is becoming shorter due to high interference levels and the re-use of the spectrum increases until every home, or every room is re-using the same spectrum.

  Long range use is suffering a lot from interference caused by other users, especially if those other users are close to one of the main nodes of an IoT network. A short range user close to a long range node can easily cause very high uplink interference degrading the long range system.

- ***The mix of different long range systems in the same band segment***
  Different Long Range system can be deployed in the same band segment. For example the band segment 868.0 – 868.6 MHz[22] which according to ERC Recommendation 70-03 is the main band segment allowing 1% duty cycle instead of 0.1%. An example thereof is an IoT network technology such a LoRa which focuses on three prime channels in the 868.0 – 868.6 MHz for international compatibility across Europe. Multiple systems have already been deployed and more are likely to be deployed over the coming years. These systems do impact each other, especially transmissions from high locations such as network base stations. Among the most vulnerable users are the IoT networks using sensitive receivers at high towers trying to achieve very high link budgets for long reach. An increased noise floor due to uplink interference will impact the achievable range of these Long Range systems. Over time the range will continue to decrease due to an increasing interference level.

- ***The mix of different long range systems using different technologies in the same band segment***
  Different LPWA IoT networks using the same technology in the same band are expected to better be able to co-exist than networks that use different types of technology (e.g. spread-spectrum and ultra narrowband). To overcome this the networks would have to evolve to be better able to deal with interference, as well as to

[22] The regulation in the Netherlands has extended this to 865 – 868.6 MHz.

control power levels much better than they currently do. The design of such an evolved protocol however is bounded by the requirement to achieve low-cost in combination with a very long battery life time and only 1% downlink duty cycle. The current system design trade-offs are more focussed on achieving battery life time and low-cost implementation rather than towards the most efficient use of the spectrum.

For spectrum monitoring purposes the first real IoT spectrum issues are likely to be concentrated around the most vulnerable users, which are IoT networks with high antenna positions and targeting very long range and very good link budgets. Initially such a deployment works, but with increasing usage of the band more and more service degradation should be anticipated in terms of reduced reach and an increasing message failure rate. Since it should be anticipated that many IoT business use cases which initially seem complementary will gradually become mission critical, this represents a potential risk with potentially major consequences.

Troubleshoot specific issues related to interference caused by or harming IoT applications

In specific environments and situations, issues may arise from the usage of IoT applications that require intervention from the regulator. A monitoring system can aid in localisation of such issues and resolving them. Again, the situation for unlicensed bands is much more difficult than that for the licensed bands. While licensed-band usage of IoT applications may cause interference, this is then likely due to the specific equipment involved (e.g. interference of 900 MHz LTE on television distribution networks). In licensed bands, there may be different types of issues. Whereas generic issues could still be measured from the IoT network side, this may be impossible for highly local issues that only occur at the device side.

6.3.2 Instruments

The Dutch Radiocommunications Agency currently has several instruments at its disposal for monitoring and enforcement. In this paragraph, we discuss how these existing instruments can be employed to serve the objectives discussed in the previous paragraph. We also suggest a set of new instruments that could further improve monitoring capabilities.

Spectrum monitoring network

The Dutch Radiocommunications Agency currently operates a network of about 15 spectrum monitoring nodes, located across the Netherlands (the 'Landelijk Meetnet Telecom' or LMT). Each node is equipped with high-quality software defined radios (SDRs) that can be configured to collect data on specific frequency bands in specific time frames. The monitoring network currently provides the data 24/7 at a 5 kHz and 1 minute resolution.

The licensed bands that are usable or used for IoT are currently already monitored by the network, as they are subbands of licensed bands currently in use for mobile networks. The bands are however not monitored at a very detailed level which would allow assessment of real system usage and capacity issues.

Assuming technologies such as LTE NB-IoT are likely to emerge over the coming years the mobile operators have several options to integrate this into their existing LTE network. For example, just allocating 180/200 kHz (basically one LTE resource block) for LTE-M2 out of a total 10 MHz of an LTE-800 carrier would be a possible approach. There seems to be no immediate requirement for Agentschap Telecom to start very detailed usage monitoring of that particular 200 kHz since the mobile operator can manage the capacity aspects as well as the (internal) interference issues.

Additional and more detailed spectrum monitoring of those band segments used by large-scale IoT networks for long range would be recommended. Examples of current actual usage are the following:

- LoRa, message length of 46 – 1,150 ms chirping over 125 kHz
- SIGFOX, message length of about 1 second with a channel of 100 Hz

If actual monitoring of IoT networks would be required then the following has to be made measurable:

- **Occupation of 125 kHz channels at a resolution of 50 ms (LoRa)**. 50 ms would be the time resolution required to see how many timeslots are still available. This would require 1,200 times as many samples in time compared to the current 1-minute resolution.
- **Occupation of 100 Hz channels at a time resolution of 1 second (SIGFOX).** This implies a 50 times narrower filtering (compared to 5 kHz today) and 60 times as many samples in the time domain. So 3,000 times as many samples.

This increased resolution in both the time and frequency domain results in 1,200 to 3,000 times the number of measurement samples. If measured at the same time it would imply 100 Hz and 50 ms and that would increase the total number of measurements by a factor 60,000. It would be recommended to do this only for those frequencies used intensively for IoT networks and in time before the IoT networks run into real problems. As long as the spectrum load is low this would not be necessary.

Mobile measurement nodes

The mobile spectrum measurement system adds additional information with respect to the dimension place but by the character of the measurement type the measurement is just at a particular time and place, not continuously at every place. It basically provides a complementary snapshot of the spectrum usage.

The current monitoring network is unable to identify specific uses of the unlicensed bands. It is however possible to identify and decode LoRaWAN transmissions using commonly available, inexpensive SDR (software defined radio) hardware. [58] The LoRaWAN modulation and protocol specifics have been reverse-engineered, and information on how to decode the radio transmissions is readily available. [34] Software for decoding is readily available. [55] Figure 50 shows an example of a captured LoRa transmission, showing the 'chirp' modulation employed. For SIGFOX, we have not found readily available software modules for decoding, although we expect it to be technically feasible to capture SIGFOX traffic as well.

While protocols may be decodable, the information that can be gathered is still limited. For instance, it may not be possible to derive the destination node from decoded transmissions. A monitoring node cannot know which node(s) of an LPWA network will pick up a transmission it has seen, and in what conditions it will receive it. An additional difficulty is that transmissions are expected to be infrequent and short-lived for most IoT applications, which makes it difficult for a mobile node to identify and track individual devices.

The recommended strategy for monitoring IoT using mobile measurement nodes would be to periodically visit those areas expected to have the highest number of devices (using, for instance, the model we presented in paragraph 4.4).

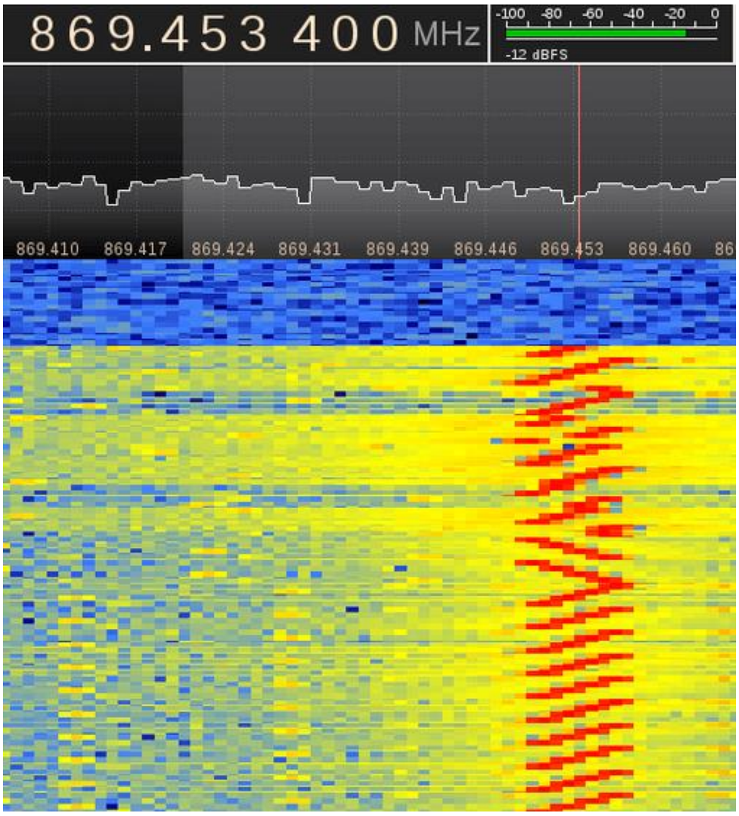

Figure 50 Capturing LoRaWAN communications using an SDR [58]. Horizontally shown is the spectrum between 869.410 MHz and 869.463 MHz. Vertically shown is the time. The colors indicate measured power levels at a specific frequency and time.

IoT network operator data

Operators of IoT networks can collect various measurements about transmissions being received or being made by the network. Most operators will already have monitoring systems in place, in order to detect malfunctions in the network, or for billing purposes. Relevant attributes that can be measured by the networks at the message level are the following:

- Message origin (customer ID, device node ID)
- Receiving/transmitting base station (base station node ID)
- Message payload length
- Radio characteristics, e.g. received signal strength (RSSI) or signal strength used for transmission, SNR ratio
- Modulation type used for transmitting the message
- Approximate location of the node (in case the network supports localisation without specific devic support)

In addition to data related to IoT traffic from and to the network, the network's base stations may be capable of measuring other activity in the band used. LoRa receivers will for instance also receive messages destined for other LoRa networks if both networks operate in the same channels. As many base stations use software defined radio (SDR) receivers, it may be possible to distill various other interesting details about spectrum utilisation within the receiving range of the base station, such as average utilisation by others, noise and power levels.

IoT measurement nodes

A possible way to obtain information on IoT network spectrum utilisation is by placing measurement nodes connected to the IoT network itself. As the hardware is relatively cheap and requires little power, deploying a large number of measurement nodes is possible. Using such a low-power IoT node, various measurements are possible:

- Periodic transmission or (confirmation of) reception of a message. A central server measures the number of messages that have successfully reached the network (or the device) and at what radio conditions (if the network provides this data).
- Periodic measurement of spectrum characteristics, particularly utilisation.
- Measurement of the device configuration parameters received from the network (e.g. regarding modulation type, transmit power).

A more expensive node could be equipped with a software defined radio to measure even more detailed characteristics of the spectrum, such as:

- The number of collissions that appear to occur
- Other users of the spectrum (other IoT or different applications)
- Use of other frequency bands (e.g. other unlicensed spectrum, or licensed spectrum).

While the Radiocommunications Agency could of course deploy such modules by themselves, it could also look for other large scale deployments of IoT devices, and try to collaborate. If for instance a large deployment of IoT devices is done in a municipality for waste management purposes, the agency could request to add software to the devices that would transmit measurement data at times the devices do not have to transmit any other data for their original purpose. Finally, the agency could make available a service where devices (or networks) could voluntarity submit measurement data.

6.3.3 Spectrum monitoring strategy

Given the monitoring objectives and the monitoring instruments available, we can now devise a *strategy* for monitoring IoT spectrum usage. Table 17 gives an overview of each objective and indicates which instrument would be best suited for supporting that monitoring activity.

Table 17 Spectrum monitoring objectives and the instruments appropriate for achieving them

	National measurement network	Mobile measurement nodes	IoT network operator data	IoT measurement nodes
Wide/metro area	√		√	
Local/personal area		√		√
Resolution	Spatial: Low; Spectral: High; Temporal: High	Spatial: Medium; Spectral: High; Temporal: Low	Spatial: High; Spectral: Medium; Temporal: Medium	Spatial: High; Spectral: Low; Temporal: Medium
1 Spectrum utilization by IoT	√			√
2 Spectral efficiency of IoT		√	√	
3 Detect generic issues related to IoT	√	√	√	√
4 Troubleshoot specific interference issues		√		

Legend: Spatial resolution, Spectral resolution, Temporal resolution; Low, Medium, High

Obtaining information on spectrum utilization by IoT

With respect to the first objective (measuring spectrum utilisation by IoT), the measurement network that is already in place can be used, with minmum reconfigurations. The primary issue with using the measuring network for this purpose is that it lacks spatial resolution – there are only a small number of nodes. Depending on the type and height of the antenna, a node will likely be able to 'cover' only an area of at most a few square kilometres.

As the measurement network is not able to measure utilisation at local levels of scale, it should preferably be augmented by a more distributed (but perhaps less precise) measurement system, with a very large number of nodes.

Obtaining information on the spectral efficiency of IoT

In order to measure the spectral efficiency of IoT networks, data is needed at the network level, specifically about the amount of *useful* data that is being transmitted, in order to be able to make a fair comparison to spectrum utilisation. A similar analysis was performed in this study (paragraph 5.1.1), by comparing data on messages sent and received by the Things Network (Figure 18) with radio signal characteristics observed by the base stations in that network for each message (as shown in Figure 19 and Figure 20).

The agency can either collect this data from the IoT network operators, or use mobile network nodes (combined with decoding software) to obtain the data themselves. The former requires cooperation of the operators, the latter requires the agency to obtain the necessary hardware and software. Additionally it may be technically challenging to decode IoT protocols especially when encryption is used.

Detecting generic issues related to the use of spectrum by IoT

With respect to the detection of issues, all monitoring instruments are relevant. Each instrument however detects different issues. The national measurement network can detect issues that are generic, such as high levels of illicit usage of unlicensed bands. Mobile measurement nodes can detect almost all issues, but can only do so in a very limited area – care must be taken to position the mobile measurement nodes at the right places (mobile measurement nodes could for instance periodically perform measurements near airports or seaports, where IoT devices may be used and where the RF environment is expected to be very noisy due to the use of other wireless technologies, such as RFID). Network operators detect issues themselves as part of their monitoring of their own network. Finally, measurement devices could be deployed to detect issues at a very local level.

- The mix of short range and long range usage
- The mix of different long range systems in the same band segment
- The mix of different long range systems using different technologies in the same band segment

Troubleshoot specific issues related to interference caused by or harming IoT applications

Mobile measurement nodes are the only instruments appropriate for performing troubleshooting of specific issues. This requires high-precision measurements (with SDRs) and can always be done on-demand.

As the number of devices is expected to increase significantly, the question is how the Agency can organise itself to only act on the most relevant issues. In order to make monitoring of specific issues more pro-active, the agency could consider opening a service or online form where (users of) IoT devices could submit evidence of interference. Combined with software to cluster and filter these reports, the mobile monitoring nodes can be directed more efficiently to the locations where the urgency is the highest.

6.4 Overview

The impact of short range IoT usage in unlicensed spectrum is expected to be limited. Following the rules set out in ERC Recommendation 70-03 [15], a very high level of frequency re-use is possible for short range applications. Studies performed by the ECC appear to indicate that the regulation is efficient and that there is no shortage of spectrum. Specific applications that require high power, such as RFID, may however lead to issues. [17] [19] [20]

While the frequency plan as well as regulation have been tailored and efficient for short range applications, we have reason to suspect that the regulatory framework may not be adequate in the light of large-scale deployments of long-range technologies, such as those envisioned for LPWA IoT. The adoption of such technologies creates new scenarios for interference. Two scenarios are of particular interest:

- The scenario where short range devices are close to a base station of a long range network, and cause interference that harms long range communication in the whole long range cell. In the long term, this may cause the coverage and reliability of long range networks to decline unpredictably over time.

- A scenario where there is interference between different long range technologies in the same spectrum.

At the wider scale, monitoring is an instrument that provides information on the overall health of the spectrum with respect to its intended usage. At the more local level, monitoring can be used as a tool to troubleshoot local problems, or (by sampling various locations) to obtain a more detailed view on the spectrum health.

In the future, we expect monitoring to become more relevant as three key issues emerge in the unlicensed bands:

- The mix of short range and long range usage.
- The mix of different long range systems in the same band segment.
- The mix of different long range systems using different technologies in the same band segment.

An alternative could be to obtain information from the IoT network providers in terms of the number of messages and the message duration per location.

7 Conclusions

In this chapter we return to the research questions for this study and summarize our findings for each.

7.1 Main research questions

7.1.1 Which issues will be caused by the utilisation of spectrum below 1 GHz by wireless IoT applications, and what are possible solutions for overcoming these issues?

We expect that the currently available spectrum is sufficient to handle the expected connectivity demand for wireless IoT.

LPWA IoT is primarily used by applications that need to send or receive small messages at an infrequent basis. Networks in licensed spectrum have ample room for (dynamically) allocating spectrum to IoT. LPWA IoT networks in the unlicensed bands will face decreasing efficiency resulting from an increasing noise floor, but can mitigate this and scale up by increasing network density. There are opportunities to transform the current long range networks to short range networks, for instance by adding base stations to consumer modems (CPEs).

The use of unlicensed spectrum for mission-critical communications presents a risk with respect to televulnerability.

While we expect early users of LPWA IoT networks to understand the risks and start out with deploying non-critical applications, we expect their dependence on the data generated by these applications to grow over time.

Mission critical applications should be aware of the inherent risks of using unlicensed spectrum and take appropriate measures to mitigate those risks. The easiest way to do so is to use an LTE-M-based service provided by a mobile network operator in licensed spectrum. Alternatively, dedicated infrastructure can be deployed. In the current situation, there is room in both the P(A)MR bands as well as in spectrum currently allocated for private GSM (the 1.875–1.880 and 1.780-1.785 MHz bands, which are also the DECT guard bands). These bands are suitable for deploying dedicated infrastructure for LPWA IoT in indoor and localised (on private property) scenarios. Technologies such as SIGFOX can be deployed in very narrow spectrum (12.5 kHz) and provide sufficient capacity for most applications. Alternatively private LTE-M deployments can be used in spectrum of at least 200 kHz. The licensed, private frequencies can be reused as long as the applications are geographically limited to a particular area.

Many short-range IoT applications do not necessarily need to use spectrum below 1 GHz.

There are several options for IoT connectivity in higher bands (e.g. 2.4 GHz or 5 GHz) that can also provide more bandwidth. Especially in the 5 GHz band, there is ample capacity. Hardware modules that provide low-cost connectivity exist and new initiatives are undertaken to develop technologies that reduce power consumption.

LPWA IoT networks in the unlicensed bands are limited in efficiency by duty cycle regulations.

The efficiency of the networks could be greatly improved if the networks could send (power) control messages more often than they can do now. However, relaxing the duty cycle constraint will also increase interference between users of the unlicensed networks, which in turn may actually decrease efficiency. It could however be worthwhile to further detail the duty cycle requirements (e.g. by setting Ton/Toff-requirements).[23]

The usage of different kinds of technology for LPWA IoT in unlicensed spectrum leads to additional interference and suboptimal usage of the spectrum.

Currently, there are three large-scale LoRaWAN deployments in the Netherlands, and one large-scale SIGFOX deployment. The former uses spread spectrum modulation whereas the latter is based on ultra narrowband technology. Simulations and studies show that networks with different types of technologies exert more interference on each other than they do on other networks using the same technology.

7.1.2 What are obstacles affecting the oversight and enforcement of wireless IoT applications, how can these be overcome, and how can monitoring contribute in solving this issues?

Problems resulting from interference with and between LPWA IoT transmissions will be primarily local and intermittent.

The current monitoring infrastructure available to the Dutch Radiocommunications Agency cannot be used to detect such issues on forehand. It can however be used to monitor the behaviour of large scale LPWA IoT networks. Reconfiguration of the measurement network is necessary to be able to distinguish different transmission types.

Local problems can be monitored primarily using mobile measurement nodes. Software defined radio technology should make it possible to interpret much of the LoRa and SIGFOX traffic, although identifying the source and destination of specific transmissions may still be challenging.

Monitoring trade flows of devices containing LPWA IoT technology is hard due to the diversity of supply chains.

LPWA IoT radio modules are expected to be found in many different kinds of products that previously did not have radio capability within the next five years. This substantially increases the number of trade flows to monitor. Although the devices are subject to certain certifications (most importantly CE), they do not provide easy ways to identify the wireless capabilities of a device. Operators of LPWA IoT networks do require certification (e.g. 3GPP certification for LTE, or LoRaWAN certification for LoRa).

There are several types of actors in the LPWA IoT value chain that may have valuable information regarding trade flows. Chipset vendors will be able to give accurate estimates of global device volume, but will not be able to further detail it to applications or countries. Intermediate parties such as the operators and turnkey device providers may be able to provide this level of detail. Network operators can also provide very useful data on noise levels and other users in the unlicensed bands. Additionally data from these networks can

[23] Ton is the maximum time a device is actively transmitting, Toff is the minimum time a device is not transmitting.

be used to measure the efficiency of the network (e.g. whether the right modulation type is used given the signal and noise levels observed).

We expect interference from IoT devices that are imported from countries outside of Europe, and use the 902-928 MHz band, on current applications in that spectrum.

Many LPWA IoT devices will operate in the 902-928 MHz range, which is a very popular unlicensed band for use outside of Europe, especially in the US, with broader global support for specific sub-bands. We also expect devices to appear on the market that will allow users to easily configure radio parameters (such as transmit power) to exceed the regulatory limits applicable in Europe.

A combination of (reconfigured) existing monitoring instruments combined with novel monitoring instruments is best suited for monitoring spectrum impact of wireless IoT.

Traditional monitoring instruments can, to a limited extent, be reconfigured for monitoring wireless IoT spectrum usage. We suggest augmenting traditional monitoring with monitoring based on IoT network operator data, SDR nodes, and specialised IoT monitoring nodes.

7.2 Sub research questions

7.2.1 What will be the demand for spectrum below 1 GHz for wireless IoT applications, and how can this be demonstrated?

Based on our analysis we expect that there will be between 8.6 and 52.1 million LPWA devices in the Netherlands in 2024. Most of the devices are expected to be in the categories *agriculture and environment* and *smart buildings*, although there is a significant difference between the studies.

We expect that the currently available spectrum is sufficient to handle the expected connectivity demand for wireless IoT.

Deployment of LPWA IoT networks in licensed spectrum is expected to be gradual and smooth. In many cases, operators will use existing spectrum to deploy LTE-M1 or LTE-M2 (NB-IoT). Deployment will, for most operators, be a matter of a software upgrade, and will almost instantly provide nationwide, indoor coverage. Neither LTE-M1 nor LTE-M2 appear to be bound by concurrent usage issues, as these standards provide very good means for power control and concurrent access. While both are capacity-bound, operators can easily (and even dynamically) allocate more spectrum within the same or another band in their possession to IoT. For example, LTE-M2 only takes 200 kHz out of a typical 10 MHz LTE carrier, so scaling up is possible. Additionally, new frequency bands are expected to become available in the near future that are usable for LTE. The 700, 800 and 900 MHz frequency bands are the most likely candidates for deployment of LTE-based IoT connectivity.

An interesting question is whether the current operators will make an attempt to migrate existing machine-to-machine applications to the new LTE-based standards. Of particular interest are the users of the CDMA-450 network operated by Utility Connect and KPN. Today, this network is primarily used to read electricity and gas meters. In theory, this network can be upgraded to LTE in the same band (which in LTE is band 31).

There is sufficient unlicensed spectrum for IoT networks below 1 GHz to meet future demand, provided that the networks implement efficiency measures and interference mitigations. The 863-870 MHz band, in particular the frequencies around 868 MHz, appears to be very popular for all LPWA IoT technologies currently deployed at scale. If the networks do not change, demand is likely to outgrow capacity for two reasons. First of all, the networks currently appear to rely heavily on three specific channels, leaving others unused. Second, increasing use of the unlicensed frequency bands will slowly increase the noise floor, which primarily affects long-range systems that rely on low noise floors to achieve low-power connectivity. In order to scale up, the networks will have to start making more efficient use of all available channels, as well as further densify.

In other parts of the world, LPWA technologies also operate in the 902-928 MHz bands (North America) or in the 915-921 MHz bands, which is currently also under investigation for reallocation in Europe. This provides challenges with respect to enforcement (e.g. preventing illegitimate transmissions in these bands which in the Netherlands are used for other purposes).

7.2.2 Are there opportunities for increasing the efficiency of spectrum utilisation of wireless IoT applications, in order to reduce the load on the spectrum?

The different platforms for LPWA IoT are all optimised for low-power usage, aiming to allow devices to operate as long as ten years of operation on a single battery. All are focused on low data rates and pay special attention to increase coverage to include indoor use cases, as well as optimized access in scenarios with a very large number of devices.

The main concern regarding spectral efficiency relates to the usage of short range technology for long range communications, as is the case for LoRa and SIGFOX (and other technologies that use unlicensed spectrum). LTE-based networks are much better capable of allocating spectrum to and managing multiple access between concurrent users, and scale much better than the short range technologies. The main reason for this is that power control in the short range technologies is non-existent, or limited due to the fact that downlink transmissions are bound by duty cycle limits. Increasing the duty cycle for all users would not improve this situation.

Solutions to this problem are either to migrate to connectivity using licensed bands, or by significantly increasing the density of the networks that provide connectivity in unlicensed bands. Ultimately, these networks will thereby become short range networks (consider however the possibility of adding LoRa base stations to every residential internet modem – operators have done this before with Wi-Fi).

A short term suggestion for LoRa is to improve the use of all channels available in the unlicensed spectrum. We currently see much usage concentrated on frequencies, while the standard and devices support a wider range of frequencies.

7.2.3 What are the consequences for current users of a frequency band when the band is opened up for wireless IoT applications?

The impact of short range IoT usage in unlicensed spectrum is expected to be limited. Following the rules set out in ERC Recommendation 70-03 [15], a very high level of frequency re-use is possible for short range applications. Studies performed by the ECC appear to indicate that the regulation is efficient and that there is no shortage of spectrum. Specific applications that require high power, such as RFID, may however lead to issues. [17] [19] [20]

While the frequency plan as well as regulation have been tailored and efficient for short range applications, we have reason to suspect that the regulatory framework may not be adequate in the light of large-scale deployments of long-range technologies, such as those envisioned for LPWA IoT. The adoption of such technologies creates new scenarios for interference. Two scenarios are of particular interest:

- The scenario where short range devices are close to a base station of a long range network, and cause interference that harms long range communication in the whole long range cell. In the long term, this may cause the coverage and reliability of long range networks to decline unpredictably over time.

- A scenario where there is interference between different long range technologies in the same spectrum.

7.2.4 How can spectrum utilisation by wireless IoT devices be monitored? Given different levels of scale (wide, metropolitan, personal and local area), what is the best monitoring approach at each level? How can these approaches be embedded in the current monitoring processes for short-range devices?

In order to be able to monitor long range IoT networks, specific adjustments have to be made to the resolution of measurements in the monitoring network. An alternative could be to obtain information from the IoT network providers in terms of the number of messages and the message duration per location.

7.2.5 How can trade flows of wireless IoT devices be mapped? How can regulatory bodies become aware of illegitimate wireless IoT devices as early as possible?

Monitoring the trade flows of these devices will not be an easy task due to supply chain of the LPWA devices. The chip manufacturers have for instance a good overview of the total number of devices, but not in which country they are sold. For the solution providers and the turnkey device manufacturers it is the other way around. The best option would be to contact KPN (LoRa) and Aerea (SIGFOX) because they can see how many devices are connected to their network. We expect that most of the devices can be found in the west of the Netherlands, in the *Randstad*.

7.3 Policy recommendations

We recommend the Dutch Radiocommunications Agency to instruct operators and user groups to educate (potential) users of IoT LPWA connectivity in unlicensed spectrum about the possible (future) risks regarding availability and reliability.

Currently, the agency educates users on the risks of using Wi-Fi and we feel that LPWA IoT should be treated similarly.

The agency should also keep in touch with the operators of networks operating in unlicensed spectrum in order to verify how they are marketing their services.

Operators of LPWA IoT networks in unlicensed spectrum should be encouraged to further densify their network.

We expect many of the issues related to LPWA IoT to be resolved when the network's use of the unlicensed bands returns to short range usage.

We recommend the Agency to investigate the possibilities for using data from the IoT network operators for monitoring purposes.

Using the data, the agency can draw conclusions related to the efficiency of the networks (e.g. is the right type of modulation used given the radio circumstances observed). Additionally the networks can provide useful information about the conditions in the unlicensed bands, at much higher precision than the agency can currently measure.

We recommend the Agency not to allocate additional spectrum for LPWA IoT at this point.

For compatibility with RFID tags from outside of Europe we do recommend conforming to the European standard of allocating the 915 – 921 MHz frequency band. Interference from RFID tags originating in other regions may of course still cause interference in the 902-915 MHz range.

Glossary

Term	Description
3GPP	**3rd Generation Partnership** A collaborative organisation responsible for the development of mobile phone standards, most notably the 3G, 4G and 5G standards families.
ASK	**Amplitude Shift Keying** A method for transmitting data over a carrier signal by modulating the amplitude of that signal.
CPE	**Customer Premises Equipment** Equipment located at the customer's premises necessary to provide connectivity to a network.
DECT	**Digital Enhanced Cordless Telecommunications** A European (ETSI) standard for digital cordless telephones.
EIRP	**Equivalent Isotropically Radiated Power** Measure of power emitted by a transmitter, expressed as if the transmitter was isotropic (evenly emitting power in all directions).
FSK	**Frequency Shift Keying** A method for transmitting data over a carrier signal by modulating the freqnecy of that signal.
GFSK	**Gaussian Frequency Shift Keying** Specific form of FSK for transmitting digital data over a carrier signal, but without instantaneously changing the frequency of the carrier signal for each transmitted symbol.
GS1	**Global Standards One** GS1 is the international non-profit organization behind the global system for bar-coding.
IoT	**Internet of Things** The network of physical devices, vehicles, buildings and other items, embedded with electronics, software, sensors, actuators, and network connectivity, that enable these objects to collect and exchange data.
LPWA	**Low-Power Wide Area (Wireless Access)** Communications technology that allows devices to transmit and/or receive data over long distances, with very low power requirements.
LTE	**Long Term Evolution** A 3GPP-developed standard for high-speed wireless communication for mobile phones and data terminals.
M2M	**Machine-to-Machine** Autonomous communcation between two machines.
MCL	**Minimum Coupling Loss** A parameter to describe the minimimum loss in signal between the basestation and user-equipment in the worst case.

OFDM **Orthogonal Frequency-division Multiplexing**

A method for transmitting data over a carrier signal that is used in various standards for wireless and mobile communication, including 4G.

RAN **Radio Access Network**

The part of a mobile communications network that provides connectivity between a user terminal or device and the first wireless access point (base station) of the network operator.

RFID **Radio Frequency Identification**

Technology for automatic, wireless identification and tracking of objects.

RSSI **Received Signal Strength Indication**

A measurement of the power present in a received radio signal.

SDR **Software Defined Radio**

A radio transmitter and/or receiver that can be configured for specific radio technologies fully in software.

SRD **Short Range Device**

A radio transmitter device that has low capability of causing harmful interference to other radio equipment (ECC Recommendation 70-03)

UE **User Equipment**

UMTS **Universal Mobile Telecommunications System**

A 3GPP-developed standard for high-speed wireless communication for mobile phones and data terminals.

V2X **Vehicle-to-X**

Communication from and to vehicles.

V2V **Vehicle-to-Vehicle**

Communication between vehicles.

V2I **Vehicle-to-Infrastructure**

Communication between a vehicle and a telecommunication network or other infrastructures.

References

[1] ACM (2016). *Telecommonitor vierde kwartaal 2015.* [acm.nl]

[2] Aerea (2016). *Aerea levert het grootste Internet of Things netwerk van Nederland.* [aerea.nl]

[3] Agentschap Telecom (2016). *Antenneregister*. Obtained on February 25, 2016.

[4] Agentschap Telecom (2016). *Nationaal Frequentieregister. Bestemming frequentieband 863.0 MHz - 870.0 MHz (NFP2014_MS_863_870_M).* [nfr.agentschaptelecom.nl]

[5] Agentschap Telecom (2016). *Nationaal Frequentieregister. Bestemming frequentieband 915.0 MHz - 921.0 MHz. (NFP2014_MS_EX_AMS_915_921_M)* [nfr.agentschaptelecom.nl]

[6] ARCHOS (2016). *PicoWAN, a network operator, majority-owned subsidiary of ARCHOS, announces its launch of a collaborative network based on LoRA in the Internet of Things.* [archos.com]

[7] Bluetooth SIG (2011). *Bluetooth Low Energy Regulatory Aspects*. [bluetooth.org]

[8] Business Wire (2016). *SIGFOX and e.l.m. leblanc to Connect 100,000+ French Boilers to Enable Predictive, Even Remote, Maintenance* [businesswire.com]

[9] CGI (2016, forthcoming). *Risks related to the use of wireless communications for smart meters in the Netherlands.*

[10]Cisco (2013). *The smart and connected vehicle and the internet of things.* [nist.gov]

[11]Computable (2015). *Draadloos Eindhoven rolt IoT-netwerk uit.* [computable.nl]

[12]Computable (2015). *Intermax rolt LoRa-netwerk uit in Rotterdam.* [computable.nl]

[13]Computable (2015*). Xilion start LoRa-initiatief in Geleen.* [computable.nl]

[14]Dialogic (2016). *Mobile network capacity model*. Publication number 2015.121.1601 v33.

[15]ECC (1997). *ERC Recommendation 70-03. Relating to the use of Short Range Devices (SRD).* [erodocdb.dk]

[16]ECC (2000). *ERC report 68. Monte-Carlo simulation methodology for the use in sharing and compatibility studies between different radio services or systems.* [erodocdb.dk]

[17]ECC (2012). *ECC report 182, Survey about the use of the frequency band 863-870 MHz.*

[18]ECC (2012). *FM (12) 092. Results of the questionnaire regarding the existing usage in the frequency bands 870-876 MHz / 915-921 MHz.* [cept.org]

[19]ECC (2013). *ECC Report 200, Co-existence studies for proposed SRD and RFID applications in the frequency band 870-876 MHz and 915-921 MHz.* [erodocdb.dk]

[20]ECC (2014). *ECC Report 189, Future Spectrum Demand for Short Range Devices in the UHF Frequency Bands*. [erodocdb.dk]

[21]Emerce (2016). *Antwerpen krijgt slimme meter voor water.* [emerce.nl]

[22]EnOcean (2016). *EnOcean - Wireless Sensor Solutions powered by Ambient Energy for Buildings, Smart Homes, Industrial Automation and the Internet of Things. Radio technology*. [enocean.com]

[23]Ericsson (2015). *Accelerating IoT.* [gsacom.com]

[24]Ericsson (2016) *Ericsson Mobility Report On the Pulse of the Networked Society* [ericsson.com]

[25]Espressif. *ESP8266EX.* [espressif.com]

[26]ETSI (2012). *ERM RFID / GSM-R.* [etsi.org]

[27]ETSI (2014). *Low throughput networks (LTN): use cases for low throughput networks.* [etsi.org]

[28]FierceWireless (2016). *LTE prepares for the IoT age.*

[29]GS1 (2014). *Regulatory status for using RFID in the EPC Gen 2 band (860 to 960 MHz) of the UHF spectrum, 31 October 2014.*

[30]GSMA (2015). *Low power wide area networks.* [gsma-future-uit-networks.com]

[31]GSMA (2016). *Mobile internet of things low power wide area connectivity.* [gsma.com]

[32]Huawei (2016) *NB-IoT, Trusted IoT in action.* [gsacom.com]

[33]ITU (2012). *Overview of the Internet of things. Recommendation ITU-T Y.2060.* [itu.int]

[34]Knight, M. (2016). *Reversing LoRa: exploring next-generation wireless.* [jailbreaksecuritysummit.com]

[35]KPN (2015). *LoRa. Versnelling Roll-out LoRa.*

[36]KPN (2016). *LoRa: verbindt apparaten efficiënt.* [kpn.com]

[37]Lace (2015). *The largest LoRaWAN smart meter deployment in the world – LOESK to install 400 thousand LoRaWAN-compatible electricity meters beginning this year.* [lace.io]

[38]Link Labs (2016). *IoT Agriculture Use Cases & Apps To Plant Seeds For Your Ideas.* [link-labs.com]

[39]Link Labs (2016). *LoRa Localization.* [link-labs.com]

[40]LoRa Alliance (2015). *LoRaWAN. What is it? A technical overview of LoRA and LoRaWAN.* [lora-alliance.org]

[41]Machina Research (2015).*Global M2M market to grow to 27 billion devices, generating USD1.6 trillion revenue in 2024.* [machinaresearch.com]

[42]McKinsey (-) *The Internet of Things: Sizing up the opportunity* [mckinsey.com]

[43]Mobile Europe (2016). *Orange's LoRa networks set to go live, but will the tech's success be shortlived?* [mobileeurope.co.uk]

[44]Näslund, J. (2015). *Low power wide area solutions. The central role of the operator and how to fit with other radio technologies.* [gsma.com]

[45]Nokia Networks (2015). *LTE-M – Optimizing LTE for the Internet of Things. White paper.* [nokia.com]

[46]Nokia Siemens Networks (2012). *WCDMA Frequency Refarming: A Leap Forward Towards Ubiquitous Mobile Broadband Coverage.* [nokia.com]

[47]OECD (2015). *Digital Economy Outlook 2015*. [oecd.org]

[48]Orange (2015). *LoRa device developer guide.* [orange.com]

[49]Orbcomm (2016). *Orbcomm satellite network.* [orbcomm.com]

[50]Pfeiffer, E., Rashwan, M., Biebl, E., and Napholz, B. (2015). Coexistence issues for a 2.4 GHz wireless audio streaming in presence of Bluetooth paging and WLAN. *Advances in Radio Sciences, 13, 181-188* [adv-radio-sci.net]

[51]Pyramid Research (2016) *Low Power Wide Area Internet of Things: Market Forecasts and MNO Approaches* [researchmoz.us]

[52]RealWireless (2015*). A Comparison of UNB and Spread Spectrum Wireless Technologies as used in LPWA M2M Applications*. [realwireless.biz]

[53]Rebbeck, T., Mackenzie, M. & Afonso, N. (2014) *Low-powered wireless solutions have the potential to increase the M2M market by over 3 billion connections.* [iotbusinessnews.com]

[54]Regulation (EU) 2015/2120 of the European Parliament and of the council. [europa.eu]

[55]RevSpace (2016). *Decoding LoRa.* [revspace.nl]

[56]RF Wireless World (2016). *LTE Cat0 for M2M | LTE-M Rel Cat-0 Cat-1 Cat-4.* [rfwireless-world.com]

[57]RFIDinsider (2014). *UHF RFID Frequency Regulations* [atlasrfidstore.com]

[58]RTL-SDR.com (2016). *Decoding the LoRa protocol with an RTL SDR*. [rtl-sdr.com]

[59]Saeed et al. (2013). *Performance Analysis and Comparison of Radio Frequency Propagation Models for Outdoor Environments in 4G LTE Network.* [diva-portal.org]

[60]SAGEMCOM (2016). *Location-Enabled LoRa™ IoT Network: "Geo-LoRa-ting" your assets.* Presentation by T. Lestable, PhD at M2M Innovation World.

[61]Seller, O. (2015). *US20160094269 A1: Wireless communication method, submitted by Semtech Corporation* [google.com]

[62]Semtech (2015). LoRA Modulation Basics. *Application note AN1200.22*. [semtech.com]

[63]SIGFOX (2016). *Coverage.* [sigfox.com]

[64]SIGFOX (2016). *Hardware solutions.* [sigfox.com]

[65]Stratix (2015). *Internet of Things in the Netherlands: Applications, trends and potential impact on radio spectrum.* [rijksoverheid.nl]

[66]Techradar (2014). *Super-ultra-fast 5G to land in Europe in 2022*. [techradar.com]

[67]Tele2 (2015). *Aerea nieuwe M2M-partner Tele2.* [tele2.nl]

[68]Telecompaper (2015). *Cofely to connect 100,000 smart meters over Sigfox network.* [telecompaper.com]

[69]Telecompaper (2016). *T-Mobile, Huawei showcase NB-IoT based smart parking.* [telecompaper.com]

[70]Telecompaper (2016). V*odafone: NB-IoT beste technologie voor LPWA-netwerken.* [telecompaper.com]

[71]Telecompaper, Strict & Figo (2016). *Research into Market Usage of License-Exempt Equipment in the Netherlands.* Report commissioned by Radiocommunications Agency Netherlands. [agentschaptelecom.nl]

[72]Telensa (2016). *Telensa PLANet: Intelligent lighting for smart cities.* [telensa.com]

[73]The Things Network (2015). *The Things Network Manifesto.* [github.com]

[74]The Things Network (2016). Messages received by The Things Network between May 8th 2016 (10:00) and May 20th (11:00) CET, obtained through the public REST API. [thethingsnetwork.org]. Note that this API has now been superseded by a streaming API based on the MQTT protocol, which does not provide a way to enumerate all messages received by the network. Administrators of the Things Network have indicated that they are looking into creating ways to perform analysis and monitoring using the new backend.

[75]The Things Network (2016). *Nodes*. [thethingsnetwork.org]

[76]The Things Network (2016). *The Things Network Utrecht.* [thethingsnetwork.org]

[77]TIA (2015). *5G Whitepaper 2015.* [tiaonline.org]

[78]TNO (2015) Monitor Draadloze Technologie 2015. Trends en ontwikkelingen in de mobiele sector.

[79]Tweakers (2016). *KPN gaat 1,5 miljoen apparaten aansluiten op landelijk dekkend lora-netwerk.* [tweakers.net]

[80]Tweakers (2016). *T-Mobile gaat KPN beconcurreren met netwerk voor internet-of-things* [tweakers.net]

[81]U-Blox (2016). *World's first cellular NB-IoT module combines easy, affordable, global connectivity with over 10 years' battery life for low data rate IoT applications.* [u-blox.com]

[82]Verizon (2016) State of the Market: Internet of Things 2016. Accelerating innovation, productivity and value. [verizon.com]

[83]Vodafone (2016) *Enabling the Internet of Things with NB-IoT*. [vodafone.com]

[84]Vosselman, A. (2016). SIGFOX: Vergelijkbare systemen. [nl.wikipedia.org]

[85]Vriezekolk, E. (2016). *Assessing Telecommunication Service Availability Risks for Crisis Organisations.* [utwente.nl]

[86]Weightless SIG (2015). *Choosing the right standard*. [weightless.org]

[87]Weightless SIG (2015). *Smart City IoT network deployment in London*. [weightless.org]

[88]Weyn, M. (2016). *Low power wide area networks.* [wesdec.be]

[89]Wi-Fi Alliance (2016). *Wi-Fi Alliance® introduces low power, long range Wi-Fi HaLow™.* [wi-fi.org]

[90] ZTE (2015). *Capacity evaluation for in-band operation.* 3GPP TSG RAN WG1 Meeting #83, R1-156624.

[91] ZTE (2016). *ZTE releases LoRa-based smart meters.* [zte.com.cn]

Contact:
Dialogic
Hooghiemstraplein 33-36
3514 AX Utrecht, The Netherlands
Tel. +31 30 215 05 80
Fax +31 30 215 05 95
www.dialogic.nl/en