Stratix

Internet of Things in the Netherlands

Applications, trends and potential impact on radio spectrum

REPORT

Report commissioned by
Ministry of Economic Affairs, the Netherlands

Hilversum, September 2015

Management Summary

The omnipresence of sensors, actuators and electronic processing power in, on and around many common goods, objects and devices and the exchange of information between them and with external services is often called the 'Internet of Things' ('IoT'). Wireless communication plays an important role in this trend. Although the bandwidth demand for such devices does not have to be very high compared to for instance the high data volumes for video and other media, the total demand of IoT devices might have an effect on radio spectrum use.

The Ministry of Economic Affairs is currently updating its frequency policy vision document (succeeding the 'Nota frequentiebeleid 2005'). The fast growth of connected devices may require specific attention with regard to spectrum use and policy in the coming years. This inquiry focusses on applications, technology and spectrum policy issues and trends regarding IoT with the focus on application areas that are likely to have the largest impact in the following five to ten years.

The emerging "Internet of Things" consists of a large and extremely diverse group of applications. Already emerging and growing application fields for IoT include home automation, automotive, personal care and assisted living. Other application areas such as institutional health care, industry and manufacturing, smart cities and agriculture show growth, although adoption seems slower.

At this moment, applications in IoT often form distinct, standalone ecosystems or technically isolated 'islands'. There is a multitude of standardisation efforts, but in most areas no definite standard has yet emerged. This lack of widely applied standards forms a bottleneck for large scale introduction and deployment of IoT. We expect market standards to consolidate in the coming years. Government can play a role in facilitating discussion between Dutch companies on IoT standardisation and the exchange of information about standards involvement.

Communication

Internet of Things devices operate and communicate with each other at different operational scales. We can distinguish 'personal area network', 'local area networks', 'metropolitan area networks', and 'wide area countrywide macro networks'. An important driver for the success of IoT is the availability of 'ubiquitous connectivity' *on those various scales*, since that ideally offers the ability to use the most suited and easy to implement form of communication in every situation and location. Connectivity in both licensed and license exempt spectrum and in both operator and end-user controlled networks plays a role at every 'operational scale' mentioned above.

Introduction of IoT may start as 'nice to have' implementation of simple sensors and straightforward applications. However, over time dependency of consumers, businesses and society on IoT and on underlying wireless communication might grow unnoticed. Another issue is ownership and control over information from devices. IoT devices are likely to be a part of the personal environment. They connect to web based servers, and local applications are offered as 'cloud based services'. Attention for privacy and security is needed regarding the introduction of IoT.

Wide area networks

Wide area networks, primarily consisting of operator owned public mobile GPRS and LTE networks in licenced spectrum, play a major role in providing connectivity at a macro scale with countrywide coverage. These networks and related licensed spectrum is under administration of an operator, allowing for control of network density, usage levels, and quality of availability and service. Those networks give the IoT application providers or application users connectivity to devices without the need to worry about local network details. Coverage and availability of public mobile networks become more important once more applications depend on them. Especially in rural areas (indoor) coverage might pose additional challenges for some applications.

Metropolitan area

For applications on a metropolitan scale, both license exempt spectrum (mainly 868 MHz) and licensed spectrum play a role, and both local networks under control of the IoT service provider and operator networks are used. There is a recent uptake of attention for low power IoT applications that use the 868 MHz licence exempt spectrum band for metropolitan area networks. Availability of such sub-1 GHz spectrum is expected to be vital for the further growth of Internet of Things on a ‘smart city’ scale, and it is expected that there will be a significant uptake in usage of this spectrum in the coming years. This will probably increase the amount of interference. Additional spectrum in the sub-1GHz band could solve this. It is recommended to closely monitor the uptake of usage in the sub-1 GHz license exempt spectrum, and look for other spectrum for license exempt use in this range. One option is the 915-921 MHz spectrum since this gives the possibility for a band that is harmonised in a large part of the world.

Personal and local area networks

In both *personal area networks* and *local area networks* license exempt spectrum, and especially the 2.4 GHz ISM band, is widely used for IoT. However, the 2.4 GHz spectrum is already crowded and further increase in use is expected, which can impact the suitability for Internet of Things applications. Especially for non-critical or indoor applications the 5 GHz ISM band is an important alternative, and also there are developments that aim to use the 60 GHz band. Preferably, those alternatives are used for further growth of IoT applications in the personal and local area networks. One course of action is to encourage usage of the 5 GHz band, as is current policy.

Critical Applications

Many IoT devices use shared, license exempt spectrum. This poses a challenge for critical applications since the available spectrum is expected to become even more crowded. Often there are demands for specific spectrum allocation for specific critical applications. However, designating spectrum per application causes fragmentation and inefficient spectrum use. We recommend investigating the possibility to designate shared, license exempt spectrum for critical applications in general to facilitate those critical applications. Conditions for this spectrum should be such that the use of the band remains limited enough to provide a high degree of availability, without introducing too severe barriers for use.

Spectrum harmonisation

Harmonisation of spectrum policy is important for the Internet of Things since it allows manufacturing of devices that can be utilised and shipped on a worldwide scale. Also, devices sold in a certain region will be carried around the world and ordered online in other regions. This might cause unwanted interference in regions with other spectrum designations. Additional spectrum for IoT will need to be harmonised preferably worldwide, but at least at European level.

Monitoring and enforcement

Growth in the number of devices and the variety of protocols in shared spectrum will make monitoring and enforcement more difficult. Spectrum use may vary greatly in location and time and (local) spectrum impact is very difficult to predict. The role of the regulator and monitoring agency might (need to) shift towards earlier phases in the manufacturing process by following and steering worldwide standardisation of spectrum use where possible, and monitoring of potential bottleneck situations and quickly adapt policy, regulation and enforcement accordingly.

Table of contents

Management Summary 2
Table of contents 5
1 Introduction 8
1.1 Background and context 8
1.2 Scope 8
1.3 Research questions 8
1.4 Research methodology 9
1.5 Covering the research categories 10
2 The Internet of Things 12
2.1 Introduction 12
2.2 Architectural concepts 13
2.3 Growth of IoT 14
2.4 Added Value of Connected Devices, M2M and IoT 15
2.5 Issues 15
3 IoT applications: overview and trends 17
3.1 Home automation and smart buildings 17
3.2 Healthcare (care and cure) 20
3.3 Automotive and Transport 26
3.4 Industry and manufacturing 28
3.5 Smart Cities 31
3.6 Utilities: Energy and water 34
3.7 Agriculture 36
3.8 Observations and trends 37
4 Technology overview and trends 41
4.1 Introduction 41
4.2 Characteristics of connectivity 41
4.3 Communication technologies 43
4.4 Platforms, ecosystems and alliances 51
4.5 Trends and observations 54
5 Radio spectrum and IoT 56
5.1 Communications “as a service” vs “user operated” 56

5.2 Role of licensed exempt spectrum ... 56
5.3 Role of Licenced spectrum ... 57
5.4 Harmonisation ... 58
5.5 Spectrum bands ... 58
5.6 Summary ... 62
6 Spectrum policy and the Internet of Things ... 63
6.1 Policy of the European Commission ... 63
6.2 United Kingdom ... 64
6.3 Germany ... 64
6.4 United States ... 65
6.5 Other countries ... 66
6.6 Policy trends and lessons learned ... 67
7 Analysis ... 69
7.1 Connectivity needs of future applications ... 69
7.2 Determining potential spectrum bottleneck situations ... 70
7.3 Spectrum implications ... 72
7.4 Stakeholders ... 74
7.5 Spectrum policy memo 2005 from today's perspective ... 79
7.6 Monitoring and enforcement ... 80
8 Conclusions and Recommendations ... 82
References ... 86
Acknowledgements ... 88
Annex A Examples of emerging Applications ... 89
A.1 Home Automation ... 89
A.2 Emerging Applications in Healthcare (care and cure) ... 90
A.3 Automotive and Transport ... 93
A.4 Industry and manufacturing ... 94
A.5 Smart Cities ... 94
A.6 Utilities: Energy and water ... 97
A.7 Agriculture ... 97
Annex B Communication Protocols ... 99
B.1 Communication protocols for low power, small area ... 99
B.2 Communication protocols for low and medium power, medium area ... 101
B.3 Technologies supporting medium power, medium area ... 103

B.4 Technologies supporting low power, wide area 105

B.5 Technologies for supporting medium power, wide area 107

B.6 Application layer protocols 108

1 Introduction

1.1 Background and context

The phrase ‘Internet of Things’ indicates a technical, economical and general application area related to the ‘third wave’ of connectivity: after connecting locations and connecting persons via mobile devices, the third wave connects ‘things’. IoT as a trend includes the development of interaction and intelligence that goes beyond ‘Machine to Machine’, or ‘M2M’, communication. Developments in IoT currently move in a fast pace, and various players see new opportunities. The number of connected IoT devices is growing and the potential for more connected devices is high too. Although in general the bandwidth demand per device does not have to be as high as, for example, smartphones streaming videos, the total demand by millions of devices might have an effect on radio spectrum.

The ministry of Economic Affairs is currently updating its policy vision document (succeeding the ‘Nota frequentiebeleid 2005’ that covers the 2005-2015 period). Developments in IoT may require attention with regard to spectrum policy in the coming years. As such, the ministry commissioned a study of new and upcoming technologies and their potential impact on the use of spectrum. Aspects of the Internet of Things that may affect spectrum utilisation include trends regarding the application areas of IoT and the increasing uptake of small devices and sensors in various application areas.

This report gives an overview of IoT applications and trends, and the potential impact on radio spectrum and possible consequences for radio spectrum policy.

1.2 Scope

Internet of Things is a broad area of exploration. The number and diversity of applications, devices and technologies is high. This inquiry focusses on application, technology and spectrum policy issues and trends regarding IoT, and more specific those applications that use wireless communication, with the focus on application areas that will likely be most influential in the Netherlands in the following five to ten years.

IoT trends can have a potential impact on other policy areas including areas such as number plans, net neutrality, vulnerability and dependency of ICT infrastructure, as well as more general issues like privacy. This is outside the scope and focus of this document.

1.3 Research questions

The research questions are divided in these categories:

Developments and trends

- What are the developments and trends regarding the IoT?
- Which promising applications does IoT make possible in various (business) sectors and what opportunities it offers to consumers and citizens in the Netherlands?

Connectivity need

- What is the connectivity need of these promising applications and of the IoT in general?
- What technical requirements do IoT applications impose on the wireless communications infrastructure?

Inventory of IoT telecom policy in other countries

- How do other (European) countries facilitate IoT applications in their spectrum policy?

Translation to spectrum policy to stimulate IoT applications

- How can the Dutch spectrum policy facilitate IoT applications? Are there other issues that are possibly related to the development of the IoT that directly relate to spectrum policy?

The following paragraph summarises in what chapter which different research questions are covered, resulting in combined analysis in chapter 7 and conclusions and recommendations in chapter 8.

1.4 Research methodology

The research that has led to this report consisted of the following components. Figure 1 shows a schematic view of our approach.

In an initial orientation phase a quick scan was done, leading to a long list of IoT applications in a wide variety of areas, a long list of IoT protocols and technologies and a long list of stakeholders and stakeholder types.
Based on the long lists of the first phase, a selection was made of the most promising areas and technologies and a more in-depth analysis of current situation[1], and trends was made from three different perspectives:

- **Trends in applications and use** (IoT applications, usage and user groups), see chapter 3,
- **Technology developments and trends** (IoT protocols, platforms, ecosystems and alliances), see chapter 4 and chapter 5, and,
- **Spectrum policy** (EC spectrum policy and relevant examples of IoT spectrum country policies), see chapter 6.

For this research a combination of sources were used, publicly available information on internet, reports and white papers, and information from a number of interviews that were held. An overview of the main sources used can be found in the References and Acknowledgement sections.

[1] In this phase a number of interviews were carried out with user and branch organisations, application vendors, network service providers and standards organisations.

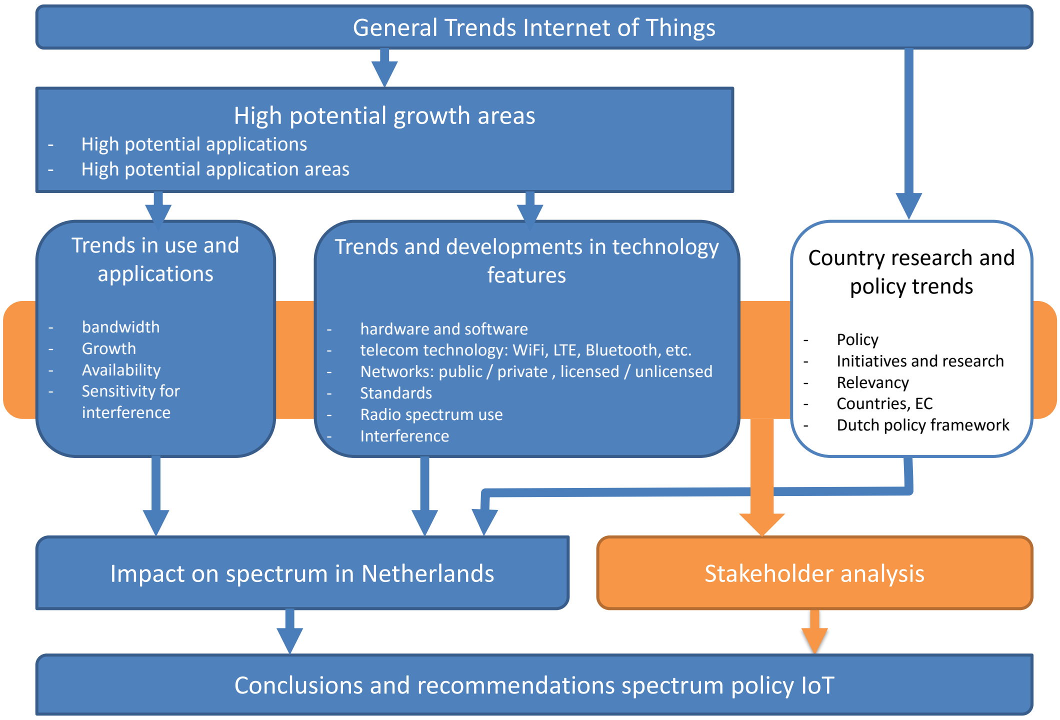

General Trends Internet of Things
High potential growth areas
- High potential applications
- High potential application areas
Trends in use and applications
- bandwidth
- Growth
- Availability
- Sensitivity for interference
Trends and developments in technology features
- hardware and software
- telecom technology: WiFi, LTE, Bluetooth, etc.
- Networks: public / private , licensed / unlicensed
- Standards
- Radio spectrum use
- Interference
Country research and policy trends
- Policy
- Initiatives and research
- Relevancy
- Countries, EC
- Dutch policy framework
Impact on spectrum in Netherlands
Stakeholder analysis
Conclusions and recommendations spectrum policy IoT

Figure 1: schematic overview of research steps and their relations

1.5 Covering the research categories

This paragraph summarises in which sections the five research categories are covered.

Developments and trends of IoT

Chapter 2 provides background information about IoT. The trends and developments regarding to applications and sectors are addressed in chapter 3. Trends with regard to the development of relevant software, hardware and platforms for IoT are addressed in chapter 4. Chapter 3 focusses on the sectors where most "promising" application areas currently are and where a significant growth or effect on spectrum in the Netherlands can be expected.

Connectivity need of IoT

The currently used technologies, spectrum and connectivity requirements of the different applications and application areas are briefly discussed in chapter 3. Their general connectivity requirements to wired and wireless telecommunication infrastructure and an estimate of the expected growth are addressed in chapter 7.

Chapter 4 provides an insight in the various technologies used for IoT (grouped by technology type, not by application or sector). Chapter 5 provides an overview of the available and commonly used frequency bands for IoT.

Inventory of IoT telecom policy in other countries

Chapter 6 provides a brief overview and analysis of initiatives and spectrum policy decisions taken by neighbouring countries.

Translation to spectrum policy to stimulate IoT applications

Chapter 7 analyses the consequences of emerging applications in the different sectors to spectrum and spectrum policy in the Netherlands by using scenarios. Spectrum policy recommendations and other policy issues are given in chapter 8.

2 The Internet of Things

2.1 Introduction

The term "Internet of Things"[2] is used in multiple ways with various, slightly different meanings. An exact definition or scope of "Internet of Things" cannot be given. It extends the ongoing trend in areas such as telemetry, automatic (remote) control and M2M (Machine to Machine) communication in which machines or other objects exchange information automatically.

Usually "Internet of Things" points to the trend that nowadays more and more 'Things' exchange information with each other and with external processes and applications via Internet or other networks: objects are equipped with sensors and computing power to process and transmit data from those 'sensors' to other objects or to 'big data' servers connected to the internet. Such ubiquitous connectivity of machines and objects and the (worldwide) distribution, aggregation and processing of information that is derived from this connectivity is associated with the term 'Internet of Things'.

Connected objects

Objects forming the internet of things usually consist of regular, tangible objects, enhanced with the following components:

- Sensor, actuator and/or presentation capabilities
- Processing capabilities
- Communication capabilities

Many objects are 'mobile' in a sense that they can easily be moved around, which leads to a number of additional characteristics of IoT objects. Specifically if it concerns small objects, this means that the sensors, processing capability and communication radios must be small and lightweight compared to the object. So IoT device can usually, but not always be characterised as:

- a low power device,
- sensing small amounts of (relevant) data based on time or other triggers (for example temperature, pressure, etc.), and/or
- performing a simple action and/or presentation task (for example lock or unlock a door, or switch a light on or off).

One important driver behind the current and expected growth of 'the Internet of Things' is that sensors, actuators, transmission devices, and processing power in general have become (much) smaller, are cheaper to produce, and use less energy than twenty years ago. Integrated circuits (chips) used in sensors, actuators and transmission devices are getting cheaper, smaller and more energy efficient. Below a certain price it becomes increasingly feasible to add sensor-chips to all kinds of objects. Moreover fixed and wireless networks provide low cost connectivity everywhere, which is another important condition.

[2] The term Internet of Things was first documented in 1999.

To get a grip on what IoT entails, and what the spectrum use might be, this report starts with a focus on emerging IoT applications in chapter 3. This gives an overview of the kind of applications, the communication technologies they use, and an indication of the expected number of future devices. From this an indication of the total spectrum utilisation for communication and possible bottlenecks can be derived.

2.2 Architectural concepts

The communication need (and thus the spectrum need) of IoT devices or applications depends, among others, on the way the devices interact with each other, and on the various paths this information travels.

This is related to a so called 'architecture' of a specific application or device. To complicate things, no single communication architecture is used, but – depending on the specifics of the application and choices made by manufacturers – various architectures are used.

Some devices are IP capable and connect directly to an IP network or the internet, while others use (IP or non-IP) protocols to connect to a gateway or controller, either directly or via a mesh (see Figure 2).

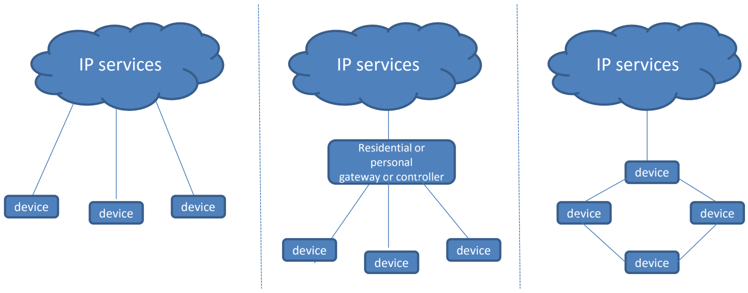


Figure 2: Examples of high level architectural concepts for IoT applications

In some cases data uses one wireless connection, in other cases multiple connections are used. This can place an extra load on the spectrum, for example, wearable devices (like bracelets) use a short distance communication method (such as Bluetooth) to communicate with a smartphone that acts as a 'gateway', from where another communication type (such as Wi-Fi or LTE) is used to communicate to some service on the internet.

Another aspect of architectural approaches is the location of intelligence and processing in the network: Raw data can be sent to servers via the internet (also referred to as 'the cloud' or 'cloud solutions') for further processing, or raw data can be processed locally in the device, and only resulting parameters (alerts, a summary, etc.) are sent.

The trends of low power and small sensors with communication capabilities make it easier to develop and deploy services that both (1) use intelligent devices itself, (2) that use processing power elsewhere on the internet. This also allows for a combination of intelligence in devices and/or servers, with intelligence, aggregation and processing or control in local gateways.

Each design choice has implications on the way data communication is organised, for the amount of data that is exchanged via different (wireless) networks, and thus on the spectrum use of that application.

2.3 Growth of IoT

Although the increase of the number of connected devices is widely recognised, predictions about the uptake on the longer term (5-10 years) vary, and although IoT devices generally do not use much data, the total use of data is expected to grow fast.

Gartner places the 'Internet of Things' on the top of the 'Hype cycle'[3] for emerging technologies (see Figure 3). According to Gartner, IoT is currently at the 'Peak of Inflated Expectations', which it describes as "early publicity produces a number of success stories — often accompanied by scores of failures". Gartner expects that in 5 to 10 years the trend will reach maturity where mainstream adoption starts to take off.

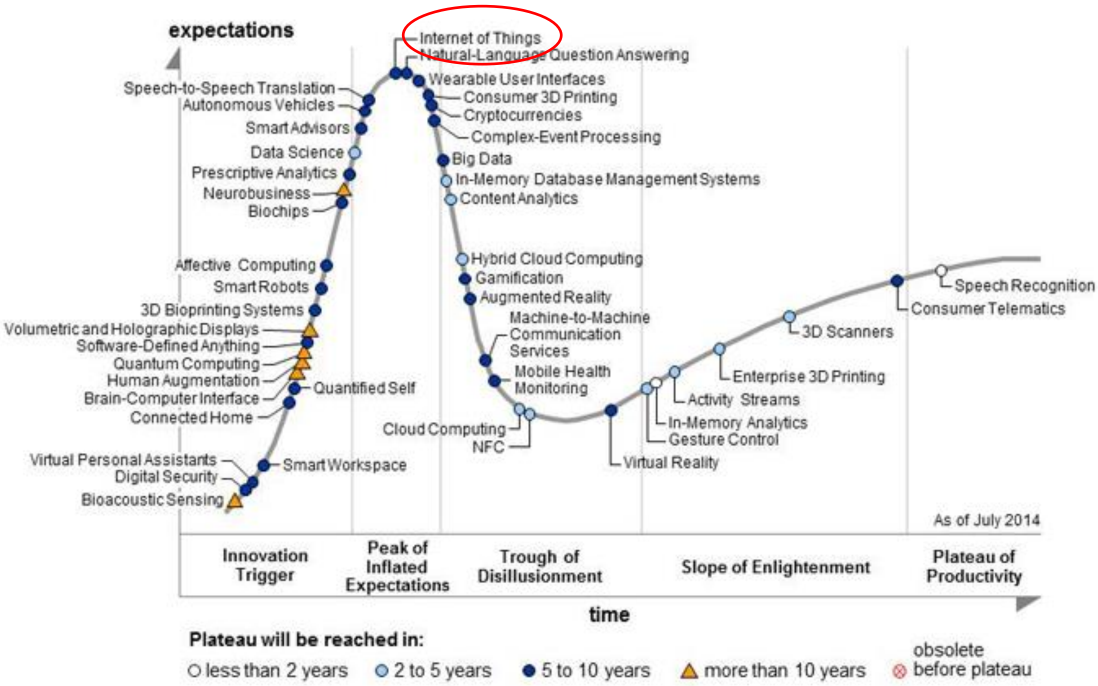


Figure 3: Gartner Hype Cycle for emerging technologies, august 2014

This reflects the state of the technology eco-systems that are currently visible: There are many different ecosystems, many of which designed for a specific use case, that not yet have converged to a small number of 'best practices' or 'technology platforms'.

[3] http://www.gartner.com/newsroom/id/2819918

The findings in this report show a large variety of ideas and upcoming potential successful applications, platforms and protocols, and thus illustrate this position. Furthermore, during the few months research period for this report alone of only 10 weeks, several reports and forecasts of research companies and announcements and news items from a variety of industry players were published.

2.4 Added Value of Connected Devices, M2M and IoT

Real-time, combined information from sensors and the ability to use of actuators can create additional value in different ways, for example by improving cost efficiency, enabling new business models, increasing safety or by increasing general well-being.

There are several examples of potential efficiency improvements. IoT applications can relay information about the object itself (status, location) that allows for easier 'asset management' (in the form of tracking, stock status, knowing when repair or replacement is needed). Or it can relay information about its environment (depending on the types of sensors) which – when combined – can be transformed into useful information on which can be acted (either by human interaction, or via automated rules). However, placing sensors, processing power and the ability to communicate on objects increase the cost of those objects. This means that for largescale deployment there is a trade-off between the added value and the costs.

Implementation of IoT concepts leads to the introduction of new or advanced services such as flexible maintenance based on the actual use. It can change business models, for instance with business and pricing models based on usage or result of the use of a tool instead of a business and pricing model that is based on selling or leasing the tool itself. The availability of to communicate relatively undisturbed at the relevant scale is a condition for the development and success of such new business models.

IoT applications can be utilised for societal benefit and increase general well-being, improving comfort, healthcare and wellness, safety, security, environment and ecological values.

2.5 Issues

A number of other issues related to IoT are not directly connected to telecom or spectrum usage, but are relevant for the deployment of new services, and might indirectly impact communication. Although issues such as usability of 'big data', possible privacy implications, health effects and environmental impact are outside the primary focus of this research, we will briefly address some of them here.

The large scale introduction of devices like sensors is often connected to both "open data" (data being freely available from various sources) and "big data" (related to the question how to manage, extract and manipulate large amounts of unordered data). The aim of both trends is to enable new solutions and business models by providing some kind of added value. In its simplest form a platform collects structured data from a set of well-known sensors and processes this data to present it visually or in some other way, or combines data from several sources to detect patterns or statistical relations.

If the data gathered becomes more 'open', data from multiple sources becomes available (both owned and from sources owned by others), and the number of (different types of) sensors grow, the *amount of data* collected becomes larger and more unstructured. The question arises how to use this data for something useful, and how to perform (automated?) analysis on this data.

Connecting and analysing this data requires smarter tools and large processing capacity than are usually associated with those kinds of 'big data' collections. In the coming years a large effort has to be made developing those tools and creating ways to (effectively) handle this data.

Privacy is an important issue in a connected world, where sensors not only communicate directly to their owner, but send information to internet-based cloud solutions as well. This is specifically relevant for IoT, as omnipresent sensors gather data unnoticed and at an unprecedented scale. If this is combined with central storage and 'big data' tools this can be particularly invasive and potentially intrusive. Similarly, devices could potentially relay business information to the outside. Although there is privacy protection to some extend by law, there are a number of possible problems with that. First is the fact that devices can communicate with services in other countries, which makes it harder to enforce privacy rules.

Another aspect related to this is security. At the simplest level, the communication from and to objects should be secure (i.e. you should be able to rely on the fact that it has not been tempered with, that data sent is received and that actuators cannot be operated by unauthorised persons). At a higher level: servers can be hacked, giving persons not intended to see the data insight in (personal or company) sensor data. Servers containing larger amounts of data might form an attractive target. The trustworthiness of the data itself is a key aspect to take into account. At a larger scale, when (open) data from multiple sources is gathered and combined, this becomes more complex since it is not always clear of a source of data can be trusted.

If data is gathered from sensors owned by the gathering party (or sensors of a known party), it is likely that information about the status of the sensor is available (i.e. does it need service, what is the battery status, might there be factors influencing the reading (like temperature or other environment conditions). From this and other 'circumstantial' information a judgement can be made about how trustworthy the data is, and if necessary information can be post-processed to compensate for any known systematic deviations. However, in the more futuristic vision where open data is abundantly available, and others have access to the sensor data, some choices have to be made: Is access given to information before or after processing?

These issues are relevant for IoT in the coming years. In this report the main focus will be on issues related to wireless communication and spectrum use.

3 IoT applications: overview and trends

This chapter describes emerging applications and the protocols and networks they use. This gives an indication about expected types of devices and their applications, the communication needs of those devices. From this, a coarse estimate about the number of devices that use similar spectrum can be made (see chapter 7).

Based on public sources, a first inventory of IoT applications that are already in use or are being developed today, public reports[9][12], and information obtained from a variety of interviews, a number of promising areas for IoT can be identified: Home automation, healthcare, automotive and transport, industry and manufacturing, smart cities, utility companies and agriculture.

In this chapter for each of these areas typical examples of emerging applications are described, and an overview is given of used technology, stakeholders, trends and bottlenecks, connectivity need and an estimate of connectivity growth for this area. A broader list of example applications can be found in annex A. Please keep in mind that the examples in this chapter or in the annex are not meant to be exhaustive or complete and that the IoT landscape is developing very fast.

There are several common stakeholder types that can be identified across every sector. These general stakeholder types are summarised in chapter 3.8 and are described further in chapter 7. For each application area only additional specific stakeholders are described in the relevant paragraph.

The final paragraph of this chapter describes observations and overall trends based on the emerging applications.

3.1 Home automation and smart buildings

Introduction

Home automation, (‘Domotics’) and building automation entails the concept that many functions for control and automation already present in your home (and possible new ones) are connected and interact with each other. This creates possibilities for easy control and coordination functionality and flexible automation through the use of sensors and intelligent algorithms.

Examples of emerging Applications

One clear emerging application in the field of home automation is the introduction of smart *Connected lights* and switches. Basic applications include traditional light-switches that are supplemented with a ‘wireless’ switch that allows lights to be controlled using a remote or an app on your tablet. This allows automated switching of lights (on/off) and – for more elaborate implementations - use of trigger-based lighting schemes (depending on mood, timer, activity, number of people present, etc.).

In recent years the most visible are media appliances that have become 'connected' like *connected Radio's, TV's, Media Centers and Game consoles,* etc. Next to communication and syncing of audio and other media streams (that may in itself not be regarded as 'Internet of Things'), they can communicate with connected lights to create an *"immersive lighting experience that matches the action on-screen*", and send for instance usage and even sensor data.

Smart appliances like kitchen appliances, washing machines and dryers form another area where connected devices will start to replace traditional, non-connected devices in the coming years. A variety of examples are already emerging.

Ovens can be pre-heated when on your way home, and temperature and other oven settings can be controlled using your tablet or smartphone. Some ovens have internal camera's to watch the meal without opening the door, and even allow sharing of your creations on social media[4]. Modern high-end washing machines come with a Wi-Fi connection that allows for control and status monitoring from an app. Energy companies provide *'smart thermostats'* such as Toon and Nest. These thermostats are sometimes capable of controlling or monitoring other home equipment such as lighting or washing machines.

Other examples of other emerging applications include *gardening sensors* and devices to take care of the condition of soil for flowers and plants (sensors are placed in the ground near plants and send their information to a gateway in which data is collected and analysed), *Automated blinds and sunshades*, connected *Smoke and carbon monoxide detectors*, *smart doorbells* (taking a picture of anyone nearing the door or entering), and automatic window and door locks[5].

Office building automation for lighting and climate control (*havac)* often use wired solutions. However, where wireless solutions are used similar protocols like home automation are used in addition to proprietary standards in license exempt spectrum.

Typically all those applications communicate with a gateway or control station using one of a variety of technologies including ZigBee, Wi-Fi, Z-Wave, and a number of other (proprietary) protocols. The gateway itself is connected to the home network using Ethernet or Wi-Fi, and is accessible via a web-interface on a computer or smartphone apps.

Technology and stakeholders

The idea of home and building automation already exists for many years, and there are a number of (mainly wired) protocols defined in the last twenty years. Although wired connections are used for example for security, the recent growth in application is driven by the miniaturisation of control electronics and radio's (allowing small transceivers to be placed inside lightbulbs or behind existing switched) and often use wireless connections for communication between a gateway and transceivers/actors.

There is a large variety of protocols/standards used for communication related to home and building automation. Wi-Fi is often used for many appliances in the house, especially for

[4] http://www.telegraph.co.uk/technology/news/11307950/Connected-ovens-and-the-smart-home-of-the-future.html

[5] Even *'pet doors'* for dogs and cats.

transporting larger amounts of data and status updates of various machines. Other protocols used (with lower bitrates and lower session setup-times) are ZigBee, Z-Wave and EnOcean.

Additional to the common stakeholder types that we have come across in every sector and are discussed in chapter 7, there are some stakeholders specific to home automation:

Construction industry include project developers, building companies and contractors, which are all involved in building projects. In The Netherlands this is a large sector that might have power in adopting and promoting new technologies for smart buildings.

Real estate owners own the property and may appreciate added value that home automation may add to their property.

Residents associations: They protect the interest of home owners and promote home-related products (such as the Dutch 'Vereniging Eigen Huis').

Trends and bottlenecks

For all lights in a home or office to be controlled remotely regular switches will have to be replaced or amended. Since most people don't overhaul their entire wiring and lighting scheme on a regular bases, it is most likely that for most households the growth in connected lights will start with only specific use-case, starting with lights or armatures when they see fit, for example for 'mood lighting' (lights that can be adapted for various moods or activities) in the living room. At this stage there are no signs that new build houses are 'readily' equipped with home automation features. For buyers of new lighting systems it is often unclear what system or (open) communication protocol to choose if you want the certainty that parts are still available in ten years' time. The large variety of suppliers and protocols plays a role in the decision: People would like one remote or 'app' to control all your lights. At this moment this often means buying all lights from the same vendor, which is inconvenient and hampers competition. A future in which lighting consists of specific closed ecosystems is therefore unwanted since it means vendor-specific dependency and lock-in. This suggests that widespread introduction of (affordable) integrated 'connected lighting' systems might take a number of years, when standards are more common and consolidated.

Next to the difficulty to choose a standard or protocol when building houses, the choice to implement such a system is up to the builder of the house. At that phase there is (at this moment) often no 'urgency' to act.

Residents are able to modify their houses to include applications and devices, like purchasing connected gadgets and appliances).

Connected appliances are expected to become the standard for mid- and high-end devices in the coming years. For example Electrolux and Samsung announced they will ship all their appliances from 2016 onwards with communication possibilities.

Currently there is a competition to provide the 'home automation gateway': various parties offer gateways and additional services. A trend worth noting is that in some cases functionality of this gateway is moved towards centralised servers, while home automation is a typical example where most of the functionality can easily (and technically more logically) be placed at the homes. This might pose additional risks regarding privacy and security.

Connectivity need and connectivity growth estimate

Home and building automation uses wireless communication on a residential range: between devices and one or a number of gateway devices. For most application and device types the amount of exchanged data is limited: simple information such as temperature, light or humidity is measured, simple tasks such as on, off, up, down or lock or unlock are performed. However applications where video streams are used such as remote security cameras exchange considerably higher amounts of data. QoS requirements of home automation applications vary greatly.

The average number of wireless connected devices due to the introduction of IoT applications in family homes can only be estimated very roughly. Kitchens have an average life expectancy of 15 to 20 years, dish washers and microwave ovens 9 years, refrigerators 13 years and washing machines 5 to 15 years and dryers 13 years. Assuming that mid- and high-end devices (that will become connected from 2017 onwards) have a market share of 60% and every household has five relevant appliances, in the Netherlands that means that the total number of connected appliances will grow with over two million devices every year, for an installed base of over 240 million by 2025 (or 3 per household).

Take-up of smart lighting might continue to depend on (stand-alone) products for the next (~5) years, limiting the number of 'smart bulbs' to just a few (2-10) per household. Practical market standards[6] will become clear in the coming years paving the way for widespread introduction of more elaborate systems, involving build-in lights in houses in about 5-10 years. Roughly estimated there might be 2-10 connected bulbs on average per home around 2020, 10-20 in ten to fifteen years' time.

A very rough 'estimate' of other wireless home automation devices related to home automation in 2025 is an average of 10-15 low data intensity and 3-7 high data intensity devices per household, including high data intensity devices like TV's, Media Centers, and other controllable media devices including digital set top boxes.

Other devices that are likely to become connected by 2015 are a number of low data intensity devices like smoke detectors (2-4 per home), 1 remote control device for home automation, anti-theft or door indicators, blinds, sun screens, door and window locks, per-room thermostats (2-5), inside atmosphere monitoring (temperature and humidity meter), and devices like 1 smart heating or air-conditioning device, 1 outside temperature meter and/or wind meter, 2 garden or outdoor lights, motion detectors, smart door bells, door mats, or mail box indicators.

3.2 Healthcare (care and cure)

Health is a subject of broad interest for many people, and involves various organisations.

Hospitals already use sensor devices for monitoring of patients for diagnostics with sensors connected to bedside machinery, limiting the mobility of patients. Hospitals expect that

[6] Either because a couple of large players or standards emerge (that give confidence of long ter support) between which to choose, or because generic gateways 'talking' to lights of various protocols become easily available for mainstream users (and not only for enthusiasts as is the case now).

sensor-technology can significantly further decrease the need for hospital visits, since use of sensors that patients can use at home allow for more remote diagnostics. Some estimates state that a reduction of 30-70% of all visits (patients visiting the hospital in person for routine procedures and consults) can be achieved in about ten years. This is good for the hospital (physical resources can be directed at patients that do need to be there to be taken care of) and for the patient (hospital visits for regular checks take up time and can cause additional load on already burdened patients). Also, IoT can allow for (more) care to take place at home, while being remotely monitored.

Broadly (health)care can be categorised into three flavours:

- Institutional healthcare (in or by hospitals or GP's)
- Home-based healthcare (like elder care)
- Personal health (prevention, health and fitness related devices for consumers)

As we will see the introduction of mainly low cost consumer devices, and the extension of monitoring by doctors of a patient at home will mix those areas, and the lines between these categories are somewhat arbitrary.

Emerging Applications in Institutional Healthcare

The main emerging field in hospitals is the use of wireless diagnostic devices measuring the condition of patients. This widens the scope of monitoring (not only in the hospital bed) and allows for longer time-traces of various parameters concerning a person's health.

The Radboud UMC in Nijmegen carried out a pilot in which wireless diagnostics devices were used for alerting, monitoring and assisting COPD patients. This solution can also be of benefit to patients with diabetes, asthma and heart failures. The Radboud UMC also works together with Philips Medical Systems on a platform called Hereismydata that combines data from different healthcare apps with hospital patient data to create a complete set of personal medical data.

Hospitals start (at a moderate scale) to provide their patients with connected *wireless diagnostics devices* like patches that continuously measure ECG, heart rate, respiratory rate, sin temperature, etcetera, to monitor their patients at a distance. Those sensors fit into a small 'patch'[7] so to cause minimal obstruction for the patient and keep the patient mobile.

In the future, wireless diagnostics using small sensors allow *doctors to monitor patients at home* effectively *extending hospital care to the home environment'*, allowing patients to leave the hospital some days earlier whiles still being 'connected' to the hospital.

Wireless diagnostics can be combined with *patient tracking:* The location and status of patients in the hospital can be tracked in real-time, for instance using Wi-Fi connected wristbands. Patients can more easily walk around and be notified when it is their turn at some facility. This kind of application increases the efficient flow of patients while keeping the patient 'ambulant' (no need to wait, patients can walk around until summoned) and thus increasing patients wellbeing.

[7] For example 'Vital Connect health-patches' are placed on the patient's chest and communicate via Bluetooth to a phone or other portable 'relay' device from where data is send to a platform using for example Wi-Fi or LTE.

Other examples are around sixty thousand *AED's (Automatic External Defibrillators)* that might in due time record ECG data[8] and send this information in real-time to a specialist in the hospital, using a public mobile network.

Combining information and making it accessible is of vital importance, and various parties are working on developing and testing the demands for such a *medical information platform*.

Emerging Applications Home Care

A wide variety of applications is emerging that can facilitate home care.

To allow the elderly to be able to stay at home for a prolonged time technology can play an important role. Already widely used are *wireless alarm-buttons* that are worn around the neck and use GPRS or SMS to send an alarm to health officials when the button is pressed. More sophisticated examples are *Motion and fall detecting sensors* to detect if a person have fallen and are immobilised, and then send an automated alert. Already there are sets of sensors commercially available that monitor presence, humidity, temperature and movement. A home gateway forwards the information to a server on the internet where the data is stored.

GreenPeak offers a 'Senior Lifestyle System' that uses a number of sensors and alarms throughout the house, connected to a gateway via ZigBee. This allows for example for fall detection and the possibility to send an alarm in case of an emergency, while also monitoring of health, eating habits. and sleeping patterns. This information can be shared with family or care givers. The system 'learns' the regular behaviour and can send an alert (to a smartphone or via email) when irregular behaviour is detected.

In the Netherlands (with a population of 17 million) there are over 5 million people that structurally need medical attention or have a chronic disease, of which approximately 50 percent need some form of medicine, care or attention on a regular basis. It is to be expected that most of those will in the future be aided in their daily lives using IoT-technology, in the form of both sensors monitoring their specific condition, and smart technology to streamline medicine intake. This can be done using *Smart Wireless Pill Boxes* that remind patients to take their medicine, '*Smart injection trackers'* for diabetes patients that collect insulin injection history and allows data to be shared with the doctor if needed, and *wireless heart monitors* for arrhythmia patients that collects data of the heart (ECG) and send it to a mobile external monitor device.

Emerging Applications Personal Care

Smart-devices for personal care are becoming cheaper and more popular by the day. Individuals use these devices to monitor their own health or sports performance. Chipsets and other hardware components are becoming cheaper, making these tools affordable for everyone. Moreover, many of these devices communicate with one's tablet or smartphone. The penetration of smartphones and tablets in the Netherlands is quite high, which makes using the smart-tools easier as well.

The most popular applications include various types of Fitness and activity tracking. *Fitness and activity wristbands and other health tracker devices* exist for a couple of years already.

[8] http://www.wos.nl/nieuws/item/20140117-nominatie-m2m-services-voor-kpn-channel-award/

Especially fitness trackers are becoming more popular every day[9] and the sale numbers will likely increase in the upcoming years[10]. Fitness trackers track movements (for example the number of steps a day), as well as monitor sleep and intensity of movement, walking or running. They mostly communicate with a smartphone or tablet using Wi-Fi or Bluetooth or ANT, on which users need an app to view the collected data. To complete the health tracking experience for the users, the same manufacturers of fitness wristbands are offering *smart scales.* These scales communicate with a smartphone and combine the data from the fitness tracker using. They sometimes have extra features like BMI calculation and calorie charts.

Other examples include *baby monitoring devices* that monitor sleep activity, skin temperature and body position and send notifications to the parent's smartphone when things appear not to be right, for example to prevent 'sudden infant death syndrome'.

Most of these gadgets communicate using Bluetooth with a smartphone or a base station that uses Wi-Fi.

Technology and stakeholders

Devices use a variety of technologies, dependent on situation, technical background of the suppliers and legislation situation of the target market. Often mainstream technologies are used like Bluetooth and ZigBee to connect personal area sensors with some gateway or relay-device, also using DECT and Wi-Fi and Z-Wave for indoor communication as well as Wi-Fi and 3GPP public mobile networks for connecting those gateways to the back-end. For application use inside hospitals access to wireless networks can be generally controlled by the hospital. However, in case of usage of communication outside the hospital, for example when using third party networks or a residential (home) network of, it is not always clear which stakeholder is primarily responsible for the present and future availability and quality of the wireless connection and related (fixed) Internet connection. This means an additional challenge when using critical wireless medical devices outside the hospital.

Institutional healthcare include special stakeholders like hospitals, certification institutions and insurance companies:

Hospitals: They not only provide medical care, but also conduct research and work together with device manufacturers to develop IoT technology. This makes these stakeholders possible enablers of IoT in this sector.

Insurance companies: Insurance companies determine what kind of healthcare is (and what is not) paid for. They have to balance *effectivity* with the *cost* of a certain medicine, tool, or equipment. If insurance companies understand IoT and are willing to partly reimburse the costs of use of such tools, then they are enablers as well.

Certification intuitions: Medical devices have to meet strict requirements regarding regulatory, interoperability, and health and safety, and new methods have to be tested thoroughly.

[9] According to research carried out by Samsung, in December 2014 at total amount of about 52,000 fitness and activity trackers were sold in the Netherlands.

[10] Revenues of wearables in the Netherlands in 2014 are estimated to be about 105 million Euro, almost three times higher than revenues in 2013, see Statista, "wearables-sales-revenue-by-european-countries"

Additional to the stakeholders already mentioned above, other relevant stakeholder categories include:

Home care service providers: (in Dutch: "thuiszorg") provide care at home for elderly and other people with special needs.

Family care givers: (in Dutch: "mantelzorgers"), supporting a recovering, handicapped, or elderly family member or friend.

Other care givers: people who work in elderly homes or work as home care nurses.

For personal care a variety of technology and protocols are used varying from personal area network technology such as Bluetooth, BLE, Wi-Fi and cellular to proprietary protocols and technologies such as Nike+.

In this sector the end-user, technology multinationals like Google and Apple, and social media are most relevant stakeholders.

Trends and bottlenecks

The basic technology is ready, and ´IoT´ applications start to appear for a large variety of healthcare related activities, but there are a number of bottlenecks.

Hospitals are starting to pilot and adopt new technology. However, hospitals and health practitioners are highly trained to work using certain well-tested and well-documented procedures, equipment and medicine, which helps to create a high quality health system. This can delay introduction of new equipment (often with good reasons including demands about testing). Information from interviews indicates that the traditional reluctance of the health sector (including hospitals and health insurance companies) for changes in proven methods, models and (business) roles is slowly shifting towards an approach where the possibilities of enhanced healthcare combined with money saving aspects of new technologies become the driver of a more pragmatic attitude towards introduction and adoption.

Extending institutional healthcare to the patient's home brings challenges in the way doctors work, since currently patients are dismissed when the doctor sees no further need to stay hospitalised, but institutionalised monitoring at home may create a larger 'grey' area of responsibility.

In home care, the societal shift that elderly stay living at home until a higher age and the changing position of family care givers might lead to a new approaches towards home care. This can be seen both as opportunity for growth of IoT applications and as a potential bottleneck for uniformity and standardisation. In some situations in rural areas lack of the availability of broadband connectivity might form a bottleneck for introduction.

The sector of personal health devices is expected to grow tremendously in the following years[11]. In personal healthcare, most devices are "nice to have" gadgets and don't face harsh regulatory regimes. Wearables are no danger for public health and easier to introduce

[11] See GFK forecast, http://blog.gfk.com/2015/05/the-global-wearables-market-sales-forecasts-and-trends/

and sell. Thus, adoption of personal care items is mostly up to marketing, price and availability of technology, giving the consumer (end-user) the choice of adoption. By communicating about devices to each other in social media, end-users are promoting their used IoT gadgets as well. Technology multinationals like Huawei, Samsung, Google, Apple, and many others are playing a part in this sector. They offer devices, software, cloud-based web interfaces and sometimes connectivity and their decisions can define the market. Moreover, customer loyalty to some brands, like Apple, is high so it is possible that loyal customers would buy anything from these brands, including wearables and other gadgets.

Connectivity need and connectivity growth estimate

IoT applications for health and care vary greatly in connectivity demand and in typical operational ranges and amount of data that is transported. Many wearables only need to operate at a personal range, because they use a smart phone or wearable gateway as intermediate hub. Other applications need to operate at local range, for instance inside a home or hospital. Additionally, some applications may need mobile connectivity and nation-wide or even larger coverage if ‘always on’ functionality is needed for travelling users.

Extending institutional healthcare to the patient’s home implies that communication with monitoring devices should be available and reliable: when the patient is not in the hospital there is no control over network availability. This may create an extra demand on spectrum and network availability, both for public mobile networks (posing demands on coverage and availability, also indoor) as well as for license free spectrum when sensors communicate locally with a gateway[12].

In interviews the suggestion was made that for critical health applications dedicated radio spectrum may be needed when licence exempt spectrum becomes crowded more in the future.

Institutional care

In the Netherlands there are about 4 million hospitalisations a year (in 2012) nation-wide. It might be conceivable that by 2025 patients will receive at least some form of monitoring device, plus in many cases an additional medicine related IoT device, potentially leading to hundred thousand up to millions of devices.

[12] For instance using Bluetooth and/or Wi-Fi. The gateway itself is connected to the hospital using fiber, ADSL or Docsis. This means local fixed infrastructure should be at hand before introduction of such solutions.

Home-care

In the Netherlands there are about 5 million chronical illness patients (diabetes, heart, other). They might not all use IoT for their health, but an estimation of 50% of the patients using at least 1 device, will give about 2.5 million devices in this sector in 2025.

In 2025, according to CBS there will be about 1 million people of 80 years or older in the Netherlands and most of them will be living in their own homes. They will be using devices like health monitors and sensors, and might use about 1-3 such devices per person, which will give a total of 1 to 3 million devices.

Personal care

Assuming several fitness trackers, baby or child tracking devices, scales and toothbrushes are used in 2025, this could result in 2-10 connected personal care devices per household.

3.3 Automotive and Transport

Introduction

Many applications regarding logistics and management of vehicles in automotive and transport can indeed be regarded as (or moving towards) IoT-functionality. Today the tracking and tracing of vehicles is already common in the logistics and transport sector for fleet management and logistic purposes. Newer generations of cars are equipped with more and more sensors for car and motor management, some of which use wireless communication. Other applications include ITS and 'connected car' functionality, e-Call, and remote control of automatic guided vehicles. The 'ITS plan The Netherlands 2013-2017' [1] aims to provide better real-time traffic and warning information and the introduction of e-Call. Also, a number of pilots are conducted in the Netherlands under the FREILOT project, for example in Helmond with connected trucks that gain additional information about traffic lights they approach or even get priority at some traffic lights to increase traffic efficiency. This paragraph focuses on applications in cars and transport systems.

Emerging Applications

Car manufacturers like BMW and Volkswagen equip their (high-end) cars with sensors for *remote car management functions*, for example motor management. This information is transmitted using public mobile networks. The car manufacturers or dealers use this information to offer additional services like maintenance planning.

An upcoming application is 'Emergency call', or *e-Call*, to automatically warn an emergency call-centre in case of an accident. Introduction of e-Call will become mandatory from March 2018 onwards. Since the functionality should work throughout the EU, most manufacturers consider using public mobile networks for communication. This might pose additional demands to such networks in terms of availability and coverage: vehicles need to be able to connect whenever an accident happens, also in rural areas.

Future cars are envisioned to drive (semi-)automatically and cooperatively by exchanging information with cars in front of the vehicle and with roadside infrastructure. *Intelligent Transport Systems* include driving assistance, collaborative driving, cooperative awareness, road hazard warning, increasing both traffic efficiency (by managing collective speeds of trains of vehicles), and safety. For fast communication between cars manufacturers plan to use a low latency version of 802.11, 802.11p. A dedicated 50 MHz spectrum band is standardised in the 5.9 GHz band. Definitive ITS standardisation is ongoing but not completed, and e-Call legislation is expected.

Vehicle-to-vehicle and infrastructure-to-vehicle communications poses high demand on the used technology because of the need to share information between a ‘random’ set of cars, meeting on roads and moving at high speeds (with regard to the infrastructure and to other vehicles). The communication needs to be fast (i.e. the communication channel needs to have a low latency). A specific frequency band is designated for this application to prevent unwanted interference.

Connectivity need and connectivity growth estimate

Already manufacturers of high-end cars connect their cars using cellular technology, and with the introduction of e-Call it is expected that from 2017 onwards all new cars will be connected, with approximately 400.000 new cars being sold in the Netherlands each year.

Next to cellular connectivity, cars might communicate in other ways, including using 5.9 GHz for ITS purposes. Large scale introduction of ITS in new cars is however not expected in the near future and might take up to 5 years or more.

Coverage is an important factor for many automotive applications. Local spectrum demand is likely to peak at traffic jams or (almost) accident situations, and accidents also happen in rural areas where coverage is less dense.

For time critical car to car applications availability of interference free short range spectrum, also in these situations, is vital.

Technology and stakeholders

A variety of technologies, protocols and frequency bands are used for automotive applications[2]. Many existing and emerging applications including e-Call use mobile (GPRS/LTE) networks.

Specifically critical car-to-car communication like collaborative driving and automatic breaks pose stringent demands on communication: it should be low latency, and work with a high client velocity. Since communication needs to be trustworthy, the 5,855-5.925 spectrum is standardised for such ITS applications, of which 30 MHz is specifically allocated for road safety ITS applications[11]. For use in ITS standardisation, efforts have focused on 802.11p/WAVE to meet those stringent demands. The other 40 MHz is reserved for less critical communication and future ITS applications, although for many of the (non-critical) applications envisioned, other means of communication like public mobile networks might also suffice.

Other wireless applications operating in the (non-critical part of) ITS spectrum include automatic toll collection at toll-roads in Portugal, Austria and France.

The following stakeholders are most relevant: drivers, the EC, and car manufacturers represent the general stakeholder types that apply in most application areas (see also chapter 7).

Drivers (as a user, or as a victim of a road accident) will benefit the most from implementing safety related application like e-Call. The driver is in many cases the customer who decides to purchase IoT devices in his or her car.

The EC made implementing e-Call mandatory pushing the adoption of in this sector.

Car manufacturers are able to implement devices in their cars and can possibly accelerate the adoption in this sector.

Trends and bottlenecks

In interviews conducted for this research the application area of Automotive and Connected Cars was mentioned as one of the areas likely to adopt sensors and automation relatively fast. Reasons behind this include the relative low (and shrinking) costs of the technology compared to the costs of a vehicle as a whole, the life cycle of a vehicle, upcoming legislation regarding e-Call, and the successful uptake of navigation systems and other driving assisting applications. The number of vehicles with IoT applications is expected to grow fast to reach about 100 million in Europe in 2030[13].

A potential bottleneck is the lack of standardisation or legislation, especially Europe-wide or globally of application protocols, allocated frequency bands, and especially the attention for (and potential weaknesses of) security, safety and privacy aspects.

3.4 Industry and manufacturing

Introduction

For decades large parts of the equipment in industrial environments uses data communication for operating, managing and monitoring purposes, using systems as SCADA and Programmable Logic Controllers. This paragraph focuses on applications in industry that use sensors, actuators and output devices and particularly applications that (are likely to) use wireless connections. Most common buzzwords to describe the Internet of Things trends in this area are ‘Industrial Internet (of Things)’ and ‘Industry 4.0’. This refers to a wide range of connections of industrial machine sensors and actuators to local processing, to the Internet, and to connections in, to and between industrial networks. The Industrial Internet faces challenges such as the need for more precision and timing optimisation, adaptability and scalability, security, maintainability and extendibility (updates and meeting changing requirements), and flexibility.

The “Smart Industry, Dutch industry fit for the future”[3] report describe potential threats such as hacking and information theft, both positive and negative aspects of internationalisation and standardisation. The resulting Dutch Action Agenda Smart Industry

[13] http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/

[4] stresses the importance of strengthening the foundation of knowledge, skills and ICT parameters by development of technical solutions, business models and forms of cooperation that simplify the exchange and use of data.

The cost effective and flexible deployment of 'IoT' capabilities such as monitoring and remote management creates an opportunity to introduce new business models for industrial applications. This is seen in a change from buying or hiring equipment to 'using the equipment as a service', where a pricing model is used based on how many times and for what purposes the equipment is actually used.

In the long term this will result in *'smart assembly and factory'* with better connections between enterprise networks and manufacturing, further optimising availability of assembly lines, precision and reliability *and* with better real time 'dashboard monitoring' of factory performance, use of resources, security threats etcetera.

Emerging Applications

Some of the most visible application fields of the Industrial Internet are mentioned *predictive maintenance* and *remote asset management, improved worker productivity*, and *improved safety and working* conditions.

Another example are *Automatic Guided Vehicles*, indoors or at container terminals, especially when combined with intelligence in the network and use of combined sensor information.

Industrial applications include a wide range of applications ranging from unmanned aerial vehicles to inspect pipe lines to monitoring food safety using sensors. An example[14] from oil and gas company Shell are the *Smart Well,* with sub-surface sensors and flow control devices monitored and controlled from the surface, and 4D seismic surveys.

Dutch water management authorities (Dutch: 'Waterschappen') were early adopters of M2M in measuring water levels and controlling pumps in reclaimed land ('polders'). Another example is Thames Water Utilities Limited, a major UK water and wastewater services utility company using *sensors, analytics and real-time data to respond more quickly to leaks, changing weather conditions* and other potentially critical situations.

Location tracking of vehicles and equipment using GPS and sending location (and other) information via gprs to a centralised coordinator is already common practice in fleet management applications, and in the transport and logistic sector in general. In practice there is a trend that all kinds of tools are (getting) connected for monitoring, asset management and maintenance purposes, like *robot welding machines* communicating using GPRS and *tightening tools with sensors, intelligence and wireless remote communication* via ZigBee or other protocols.

Connectivity need and connectivity growth estimate

The number of installed wireless IoT devices in industrial automation reached 10.3 million in 2014, and expected to grow to more than 40 million in 2020, according to research firm Berg

[14] Other examples include *4D Seismic Acquisition* surveys reservoir dynamics using sensors throughout the field on the seabed, and the *Smart Mobile Worker,* where workers use a tablet device and a helmet camera to discuss situations with field experts in the head office.

Insight. Operational ranges are often local or metropolitan for in-house or on-site wireless connectivity, but also wide area networks are used when machines directly communicate with suppliers or maintenance companies. Industrial applications tend to optimise for robustness and reliability so in most cases use wireless communications for non-critical purposes, but also here applications often start as 'nice to have' and slowly may become critical from a business continuity perspective[2][10].

Technology and stakeholders

Industrial applications are typical large scale but at a static location, and specific for the kind of manufacturing that is taking place[15]. Relevant stakeholders in industry are: Industrial companies, industrial internet consortia, governments and ICT standards development organisations.

Industrial companies (factories) that deploy IoT in their processes and sometimes develop their own IoT solution using their in-house R&D. These could be multinationals or SMEs.

Industrial Internet Consortia that develop standards and protocols especially for industrial purposes. Examples are the Industrial Internet Consortium (founded in 2014 by industry players such as such as AT&T, Cisco, General Electric, IBM, Intel and SAP and academic and government institutions) with the goal to accelerate the development, adoption and wide-spread use of Industrial Internet technologies and the Open Interconnect Consortium (founded in 2014 by Cisco, GE Software, Intel, Mediatek and Samsung), to strive for more standardisation of open IoT platforms and protocols.

Governments can decide to fund the national industry or to fund research to make industries more high tech and adoptive to IoT.

ICT Standards Development Organisations develop standards and protocols for industrial purposes, these organisations are mostly international organisations that include large multinationals[16].

Trends and bottlenecks

Manufacturing is expected by some to be one of the largest segments of the IoT market in revenues[17]. In manufacturing and industrial environments, with relatively low mobility of equipment and with a need of high robustness and availability of tools, much of this is wired. Wireless communication is mainly used for non-essential communication, or when other communication is difficult and robustness by design is possible.

A potential bottleneck for further introduction of Industrial Internet of Things applications is the variety of standards and their interpretation, both of existing industry automation and data exchange standards, as well as emerging M2M and IoT specific standards. Currently the interoperability between many 'islands' of manufacturing and industrial application platforms

[15] Trends such as rapid advances in 3D printing may change this since production facilities become more flexible.

[16] Examples of protocols developed by such organisations are OneM2M, covering requirements, architecture, API specifications, security solutions and mapping to other industry protocols such as CoAP, MQTT and HTTP. The Fieldbus standard (IEC 61158) has a variety of implementation standards including HART.

[17] Some estimates state that by 2020 manufacturing will form between 15% and 27% of the IoT market, http://iot-analytics.com/iot-market-segments-analysis/

is still an issue but as is shown above there is a slow trend towards more uniformity of interfaces.

The Dutch Action Agenda Smart Industry stresses the importance of strengthening the foundation of knowledge, skills and ICT parameters and it carries out research programme aimed at the development of software tools, with a view to chain cooperation, standardisation and interoperability, and building on a robust and secure ICT infrastructure for Smart Industry.

Both governments and multinational industrial companies are possible enablers of IoT in industry. By funding R&D or initiating and coordinating industrial consortia, like Germany[18], Finland[19] and the Netherlands[20] do, these governments are possible enablers of IoT. Multinationals have their own R&D, take part of consortia that decide on which protocols and standards to develop and adopt for Industrial IoT, and have negative power to governments and mobile network providers to push these standards to be implemented. Finally, multinationals are also the end-users that ultimately will use the technology.

3.5 Smart Cities

Introduction

A ‘Smart city’ is an urbanised area that utilises contextual, real-time information from different sectors and technology systems to achieve sustainability, increase well-being and productivity of those within it. Applications range from smarter traffic management; bringing people to their destination fast and with less distance driven in the city, to efficient garbage collection and recycling to increased safety and security.

Emerging Applications

In-city traffic management

Although not new, the ability to use fine-grained information from sensors and dispatch it in real-time to drivers creates further progress in *smart traffic management* to optimise the flow of traffic, reducing congestion in cities. If this information is combined with information about available parking spaces optimal traffic advice can be dispatched to vehicles to create *smart parking*[21]. Although, at the moment, it primarily works with digital panels like DRIP’s (Digital Road Information Panels), in the future this information can be directly dispatched to the navigation systems in the car.

Nedap offers a variety of sensors for smart traffic and smart city applications, including sensors under each parking bay to detect available parking spots on the street, relaying the information (“available” or “occupied”) to a central hub using a low power communication protocol in the 868 MHz band. This can reduce the time cars need to find a parking spot, reducing overall traffic.

[18] http://www.bmbf.de/de/9072.php

[19] http://valtioneuvosto.fi/artikkeli/-/asset_publisher/tutkimus-suomesta-teollisen-internetin-piilaakso?_101_INSTANCE_3wyslLo1Z0ni_groupId=10616&_101_INSTANCE_3wyslLo1Z0ni_languageId=en_USn

[20] http://www.smartindustry.nl/over-smart-industry/initiatief/

[21] For example Nedap offers such a system using low power protocol in the 868 MHz band.

There are a number of ideas for *'connected bikes'*, including GPRS-enabled GPS-trackers[22]. Another application in current development (can be pre-ordered from 2015) is a 'smart solar powered bike lock[23]' that automatically opens when you are near, based on local Bluetooth communication from your smartphone to the lock. The lock also communicates using public mobile networks so it can be remotely unlocked, allowing for your bike to be shared with friends. An additional feature can be crash-detection, similar as is proposed for cars, to detect (to) sudden movements indicating a crash and to send an alert.

City environment and safety

Managing the flow of waste is aided by wireless *container fill-level monitoring devices*, creating an intelligent system for the recollection of urban waste. Information about filling levels for glass, paper, and trash-containers, together with GPS location information, is sent to centralised planning tools to optimise the route of garbage collecting cars. This increases efficiency, reduces unnecessary trips of collection trucks, and prevents the situation where trash containers are full and people place their garbage directly next to the container, attracting bugs and birds. Those systems use a variation of wireless communication technologies, like public mobile networks or private networks based on 802.11.4.

City *street lights* have to be switched on and off at night. New connected lights allow for smarter lighting schemes, that switch not only depending on time, but also on weather conditions, and that allow for street lights to become brighter when persons or vehicles are near and dimmed otherwise. This reduces electricity use while keeping enough lights for safety[24], and at the same time helps to reduce the amount of ambient background light.

Air quality is a major concern in many cities. Often city officials monitor air-quality using a network of (tens of) measuring-modules containing sensors that are placed throughout the city. In the Netherlands, there is a network of about 100 air quality measuring stations that are spread throughout the country. However, with the advent of cheaper sensors and programmable hardware modules it is now possible for people to have access to measurement equipment themselves. In a project in Amsterdam[25] a Do It Yourself *'Smart Citizen kit' for air quality measurement* is offered to hundreds of people. The system, based on Arduino[26] and open source software, includes sensors that measure humidity, noise, temperature, CO, NO_2 and light intensity in a neighbourhood. Once the kit is put together, the sensors are placed outside windows or on balconies and connect to the internet using Wi-Fi. The data is collected on a central server, creating a fine-grained network of (citizen owned) pollution sensors. The 'Smart Citizen' project is an example of how IoT, due to cheaper sensors and the availability of communication networks (using people's Wi-Fi), can help citizens to be better informed and to actively participate in their community.

[22] Connected cycle uses pedals that can be attached to any bike, see http://connectedcycle.com/#about

[23] http://www.gizmag.com/skylock-solar-powered-bike-lock/32157/

[24] There are appr. 3 million street lights in the Netherlands. Once connected smarter lighting schemes become possible.

[25] http://waag.org/en/project/smart-citizen-kit

[26] Systems such as Arduino and Raspberriy Pi, combined with low cost sensors, allow for many hobbyist and Do It Yourself-solutions, as well as provide a widely used prototyping platform.

Tourism

Personalised and real-time tourist information, based on, and adapted for, the needs of a specific tourists, helps tourists find the way. The city of Amsterdam[27] plans a pilot *"iBeacon and IoT Living Lab"* in 2016 that uses Bluetooth based iBeacons for personalised direction information combined with other information on your smartphone. Another example is the development of *dynamic (real-time) signs* that can be programmed to show personalised location of special events, public transportation, or any other sign related activity. *Smart and personal roadside advertisement*, although not yet as sophisticated as envisioned in the science fiction movie 'Minority report', is becoming a reality. Shops detect repeat visitors (for example using the ID of always on Wi-Fi phones) and use facial recognition techniques[28] to determine what to offer and advertisement display relevant information based on certain parameters measured from sensors.

Connectivity need and connectivity growth estimate

The smart city is a large and crowded area where potentially many "things" can be connected. The number of devices that might in principle be connected in the next one or two decades include about three million public street lights, hundred thousands of sensors for smarter traffic redirection (including for example parking bay occupancy sensors[29]), ten thousands of (underground) waste bins, and thousands of sensors for monitoring city environment including air quality, sound, temperature, etc. The streetlights, although large in number, will only briefly communicate during switching, but the waste-bins and other sensors are likely to communicate more frequently and using more data. Other (consumer-driven) applications like connected bikes (there are about 1.1 bike per person), might add another hundred-thousand to maybe millions of connections in the next five to ten years.

In many cases wide area networks are used, but also metropolitan size networks for specific applications or even smaller range networks are used, for instance for communication between parking sensors and a gateway that combines and relays information from all parking sensors in a street.

Technology and stakeholders

Most smart city applications use available communication technologies like Wi-Fi, Bluetooth, Sigfox, Lora, and cellular technology like GPRS and LTE. Applications and devices are developed by different parties, that don't always work together. Some applications are commercially introduced, while others make part of larger government initiatives.

In "smart cities" municipalities play a special role since they (among others) manage traffic, parking and air quality in and around the city. Municipalities can push technologies and make use of IoT themselves to manage the city.

[27] http://amsterdamsmartcity.com/projects/detail/id/104/slug/ibeacon-living-lab

[28] http://www.theguardian.com/business/2013/nov/03/privacy-tesco-scan-customers-faces

[29] For example, in the city of Amsterdam there are about 100 thousand parking spaces, around 15 thousand of which are located in the city center.

Trends and bottlenecks

The number and diversity of IoT applications in the field of smart cities is growing. Governments are starting to see the advantage of the use of technology to support air quality, security and traffic management. Therefore, it is expected that the growth of IoT in smart cities will continue. A combination of a crowded city and large use-cases potentially has impact on other users in the same spectrum, such as citizens and companies.

Although municipalities can profit from IoT and it is to be expected that they will become an important enabler of smart cities, at this stage awareness about possible advantages might not always be there, and solutions are implemented only if a clear short term benefit exists. Integration of real-time information from different sub-sectors is ultimately the goal of efficient working smart cities. This is however a challenge because decisive organisations and parties do not particularly work together. There is development of IoT on different levels, municipalities, telecom operators, central government, and even innovative start-ups do not work together for a seamless integrated system.

3.6 Utilities: Energy and water

Introduction

The way energy and other utilities operate their networks is changing, driven by the ‘energy revolution’ in which energy is not only transported from large plants towards homes and businesses, and energy (from for example solar panels on homes) is fed back into the net at many decentralised points. The aim is to save energy and use more renewables. Decentralised storage can help to reduce peak-load on the energy network.

Better insight helps utilities to operate their networks more efficiently, and gives consumers the possibility to safe on energy by looking at that consumption.

Examples of emerging applications

Smart meters give more fine grained insight in electricity, water and gas consumption over time and makes introduction of varying electricity fees (depending on total availability of energy) possible. The ‘smart electricity meter’ installed by utilities records energy consumption and sends this information periodically to the grid operator. The smart energy meters acts as a hub for water and gas meter. The installation of smart electricity and gas meters in homes is underway, with grid operators aiming to offer installation to all homes in the Netherlands by 2020. For smart meter readout in the Netherlands both a CDMA-450 MHz and commercially available GPRS services are used.

Another trend is to add automation and sensors to the energy grid itself, for example in distribution nodes, to early detect failures and for maintenance scheduling. The vision is that gradually the networks change to become a *“smart grid”* in which various actor and users on the energy grid communicate to each other or to a centralised system to optimise *demand and supply* of energy. The availability of network connectivity will become more important in the future, especially for real time energy grid management purposes. The electricity grid-operators plan on using a dedicated network for their critical applications in a dedicated (450 MHz spectrum) band, see below.

Electric cars pose a challenge for grid operators and electricity producers. Optimal charging strategy prevents peak loads (i.e. prevent cars from being loaded at the same time energy is needed for other processes). For this coordination, and thus communication, can be used using smart charging points for electric cars that combining local creation of energy from the sun[30] with storage of energy to significantly decrease the load on the energy grid and reduce transport loses. Batteries of parked cars can be used as a storage medium for electricity.

Connectivity need and connectivity growth estimate

Smart meters will be installed in the upcoming years, with the aim that 80% of the 7.6 million households have a smart meter installed before December 2020. Next to smart meters further automation is planned of regional and local distribution by connecting the (approximately 40.000 in the Netherlands) automation substations. A similar number is likely for each of other utility elements such as sewage plants, pumps, and reservoir level detections.

The availability of network connectivity will become more important in the future with the introduction of smart grids, especially for real time energy grid management purposes.

In most cases wide area networks are used, although technically other solutions and network types (metro, local) could be used.

Technology and stakeholders

For the large scale deployment of the Automatic Meter Reading infrastructure by the utility companies an automatic meter the Dutch net companies plan to use both CDMA 450 (estimated 4 million meters) and public GPRS/LTE networks (estimated 3 million meters). Rollout is planned to take place before the end of 2020, by which time almost all homes need to be connected. The utility network companies see the ability to control the communication network as a key asset for future introduction of smart grid. Control over their network allows for redundancy in the communication network, and network planning can be adapted as they see fit.

For other parts of the system, including further automation of the electricity substations (approximately 40.000 in the Netherlands), both CDMA, and GPRS/LTE are used (next to DSL) for fault detection.

Relevant stakeholders include *utility companies* (electricity, gas and water production and distribution companies), *consumers*, alternative, mostly locally organised *energy cooperatives*, specialised *utility network providers* such as Utility Connect, *technology vendors* for distribution of electricity, gas and water, consumer meter *equipment vendors*, and local water management authorities (that control waste and sewer and drainage systems).

Trends and bottlenecks

The bulk of connections in this field will be the 7 million meters to be placed in homes between 2015 and 2020 as a result of European and country legislation and promotion.

[30] https://www.stedin.net/over-stedin/pers-en-media/persberichten/wereldprimeur-utrecht-laadpaal-maakt-opslag-zonneenergie-mogelijk

IoT innovations may enable or accelerate application development and deployment for monitoring, operation and automation of network distribution and other utility elements.

Potential drivers and bottlenecks are mainly related to trends in legislation and acceptation of smart meters in homes, trends in energy prices, trends in local energy production (for instance using solar cells) and in awareness towards economic and ecologic aspects of energy, water and waste handling.

In the Dutch energy sector, grids are regionally distributed and have different owners with different opinion upon which communication technology to adopt for smart grids. This might be a potential bottleneck to fully implemented and utilised smart grids in the following years.

Consumers however, are already adopting smart thermostats and other energy related devices that are offered by energy companies (not grid owners) and other companies.

3.7 Agriculture

Introduction

In agriculture and farming, many activities dependent on external factors such as weather conditions, and availability of water and other resources. Monitoring such conditions provides farmers a tool to take control of their environment and optimise farming results. Sensors of all kinds and sizes offer such tools for farmers. The trend is to connect the sensors to the Internet in order to be able to easily collect relevant data and quickly react to the given information. The uptake of "smart farming" is further stimulated by the growing attention for environmental issues and regulations for CO_2 emissions, manure quota, etcetera. The combination of fragile environmental conditions, economies of scale, globalisation and a growing world population require farmers to be more efficient.

Examples of emerging applications

Applications related to *Precision Farming* aim to improve yield, harvest and livestock well-being, while staying competitive in worldwide business.

To gain more yield using less resources high tech hardware is being applied in arable farming. It started by measuring yield using camera's and GNSS position technology, and gradually becomes more complex by adding sensors and camera's to control the different processes in the farm (i.e. using differ amounts or kinds of fertiliser based on measurements of earlier that year). An example is the *van den Borne* potato farm in the Netherlands, which uses a drone and many cameras in the field to collect data and adjust irrigation and pesticides.

Farmers monitor activity and location of livestock using sensors to collect data and send it to a server that is accessible via an app on the farmer's smartphone or laptop. Such real-time and detailed monitoring allows the farmer to monitor condition of the livestock and detect diseases early on. Other examples of sensors in livestock management include sensors in milking machines, and sensors and actuators in feeding machines.

Other examples are sensors (using amongst others, 433 MHz, 866 MHz and 2.4 GHz bands) to measure lighting, CO_2, humidity and temperature in greenhouses, sensors in forests to measure temperature and concentration of certain gases to predict risk of forest fires, and sensors, cameras and GPS on a collar on Rhinos[31] to protect them against poachers.

Connectivity need and connectivity growth estimate

Indoor in stables and barns local networks are most likely to be used for communications, outside on the fields there are several options: wide area networks, metropolitan area networks, or local networks with scattered access points.

In 2014, there were about 65 thousand farming business in the Netherlands, the majority of which are animal farms. With 2.5 million dairy animals in total, the potential of the connected cow (or other dairy animal, like goats or sheep) is quite high.

Technology and stakeholders

Several sensor technologies are used. Sound, temperature, humidity or the presence of a chemical gas in the environment are the most common sensors. These sensors are being connected to an online system 'in the cloud', or locally to enable the farmer to obtain the relevant data and use it to make informed decisions about what steps to take. Sensors in this field are both wired and wireless, many use cellular technology (2G, 3G and 4G), Wi-Fi, RFID, in some cases Bluetooth, and a number of propriety protocols in ISM-bands.

Relevant stakeholders in this sector are farmers and farmers' associations, the device manufacturers and connectivity providers.

Trends and bottlenecks

The number of initiatives, devices and applications for further connect sensors in farming is growing and offering various opportunities for farmers. They aim to improve the work process, quality and efficiency, and to save water and energy. Worldwide, the expectations of automation in agriculture are high[32].

Networks in many rural areas do not (yet) provide sufficient bandwidth for online cloud based data intensive applications[5] and might form a potential bottleneck. Spectrum and telecom policy aimed at improving the availability and quality of broadband access in rural areas may ease the introduction of IoT solutions in agriculture.

3.8 Observations and trends

Many applications and ideas under development

It is clear that many new ideas and products under development, and even more are being contemplated for the future. There is a large and very diverse group of IoT applications in development. The common factor is that it involves some kind of sensors and actors that collect data and (try to) do something useful with this data. Sometimes, this means elaborate 'big data like' analyses, but more often the data is processed in a more old

[31] http://www.nu.nl/gadgets/4092312/slimme-camera-neushoorns-moet-stroperij-tegengaan.html
[32] https://www.visiongain.com/Report/1460/Industrial-Internet-Market-Report-2015-2025

fashioned way. Companies gradually start to introduce new business models around connected devices.

Typical operating ranges

The wide range of applications roughly can be divided into four 'operational ranges', related to the average distance between communicating devices involved.

Generally, wide range networks provide communication between devices that are scattered in a wide range or that move around in larger areas (countrywide or even worldwide). Metropolitan range networks cater for wireless communication in limited areas such as a city. Local range networks cater for wireless communication inside buildings between devices or to gateways to fixed networks. Personal range networks connect sensors and wearables with smart phones or personal gateways.

Operational range of the IoT device is an important factor for choice of communication network. Technically and economically, the shortest wireless connection is often best suited for purpose. However, other requirements regarding power consumption, device size and cost, communication reliability and availability, etcetera, lead to choices about what network to use. In chapter 4 more information on the technology choices and networks used can be found.

Applications consist of separate domains

Currently many emerging applications form closed ecosystems ('stove pipes' or 'silos') of (very) specific applications. Applications operate within their own domain, and interaction with other domains is limited. In practice this means each application or application area has its own ways of working, protocols and platforms.

Success of applications

One characteristic of some of the most successful applications appears to be the fact that those applications are introduced 'bottom up' with enthusiastic users being first adapters.

For applications involving multiple players or applications that involve strict regulation, introduction is often not so easy. Examples are *health applications*, where people use all kinds of trackers and devices to monitor sports accomplishments, but where innovators have to convince hospitals, doctors and insurance companies, and where decisions about introduction take a longer time*.* Introduction of the smart meter is obliged by law to make people aware of their energy usage, that are now slowly being deployed, but where enthusiast voluntarily use all kinds of smart thermostats that serve a similar role like Toon.

The difficulty is that it is hard to predict which of the promising new application will become successful. In the coming months and years many solutions, standards and alliances might prove unsuccessful: it will be impossible to develop or maintain them, or they will merge into larger standards. The inevitable disappointment of a part of the users will be a necessary step towards workable standards and best practices.

Stakeholders

There are several common stakeholder types that can be identified across every application area. These stakeholder types are:

- end users: the people that directly use or operate IoT devices, or companies or organisations representing those people,
- IoT enhanced service providers: companies or institutions that provide services to end users, and use IoT applications to enhance or improve this service,
- fixed and mobile connectivity providers: companies that provide and/or manage network connectivity for IoT applications,
- device or hardware manufacturers: companies that develop and manufacture IoT devices,
- software developers or integrators: companies that develop, manufacture, combine or integrate software for IoT applications,
- policy makers or regulators: governmental institutions related to governments that develop and enforce policies,
- standards bodies or platform alliances: institutions that develop standards, protocols or 'best practices', and
- IoT process certifiers or financiers: non-governmental institutions that certify or finance services or applications that are likely to be enhanced or improved using IoT applications.

The future developments of IoT applications are accelerated or decelerated by a combination of all these stakeholders. In chapter 7 a further analysis of the general stakeholder types and their roles is given.

Connectivity need

Many of the emerging applications use only a limited bitrate to function, and often at this stage do not require a specific high availability connection. This is likely to change. There are a number of examples where availability and coverage will play an important role. For example for critical applications in healthcare availability is vital for the system to be trusted and used to monitor vital life-function or to regulate medicine-flows. For e-Call, coverage of public mobile networks is important, since cars move both in cities (where bystanders can alert emergency services) as well as in rural areas where there might be no people nearby.

The large number of devices at both personal/residential area scales, and at metropolitan/macro scales, make that in the future thousands of devices might compete for the same connectivity and/or spectrum. IoT depends on the existence of 'ubiquitous connectivity', i.e. the omnipresent availability of fit-for-purpose communication options that can be chosen from. The availability of network and communication options for every operational scale will plays an important role in the uptake of IoT. Implications for connectivity need and use of radio spectrum are most likely to occur in those situations where usage in one or more 'operational scales' is relatively high and multiple applications compete for the same spectrum, such as ''urban area family home during peak hours'[33].

[33] This case forms a 'typical' example of a 'high impact' situation with a diverse combination of applications.

Based on the information from this chapter, in chapter 7 an outlook for spectrum implications for this case is given.

Communication technology

With the large scope of applications a large variety of communication mechanisms and protocols can be found for use for IoT. Manufacturers choose the communication mechanisms based on a combination of technical requirements, on ease of implementation, and on availability (of both spectrum and hardware for communication, or of ready-to-use operator networks). The success of IoT depends largely on the fact that communication is cheap, and that IoT manufacturers/providers can choose the appropriate way of communicating as they see fit.

Public Mobile networks (mainly GPRS and recently LTE) are chosen not only for mobile applications (like in cars), but also for applications that are placed outside the owners premises. This gives the owner the possibility to control communication of its devices without the need to worry about local network details: once a sim is inserted devices can be placed almost anywhere, and with international M2M contracts suppliers do not need to worry about different mobile contracts for different countries.

For a large group of applications the fact that they can communicate autonomously, without the need for a third party wireless connectivity provider, is important. This reduces complexity and administrative overhead. In many of the applications described communication technologies in licence exempt bands provide this autonomy.

Low power RF communication techniques for sensors in for example the 868 MHz band are used to connect distributed sensors to a centralised ‘hub’ (creating a local ‘cell’ with a diameter of typically 1km under the control of the sensors owner), that in itself is connect to some server using an IP backbone (which can be fixed or wireless).

For local IP based communication often Wi-Fi is chosen for private as well as for professional and industrial applications. Local communication for sensors and switches often use technologies like ZigBee, Bluetooth or simple product-specific protocols in 868 MHz spectrum.

4 Technology overview and trends

4.1 Introduction

Wireless connected devices and applications are a combination of technology components: There is the hardware of the devices itself, there is the application software and firmware that runs on the devices, there are servers, and wireless and wired communication, sometimes via gateways, between the devices.

For this research with its focus on radio spectrum implications the most important component to consider is the communication and connectivity component. The aim of this chapter is to provide an overview of the technologies used in communication for IoT. Paragraph 4.2 discusses the characteristics of connectivity and paragraph 4.3 gives an overview of the different communication protocols that exist and emerge. However emerging trends and standards in the other components are indirectly also important, as they influence communication trends. Paragraph 4.4 describes platforms and ecosystems regarding generalised hardware and software (middleware) for applications.

4.2 Characteristics of connectivity

The growth of the number of connected devices depends (amongst others) on the availability of low cost wireless connectivity. Protocols specifically tailored to be used for low power applications are developed to allow those devices to communicate.

Range and coverage

Often the data is transported over small distances, in personal area networks, or home networks, and can then be possibly aggregated with larger data streams over backhaul or long distance connections. This means for many applications multiple modes of communication are used. Both fixed and wireless connectivity providers in many cases play a role in at least those long distance backhaul connections.

Coverage can play an important role for some applications. There where communications uses some local network, the network can be dimensioned by the party also using the local IoT application. However, when moving to other areas, one becomes dependent on the availability of networks there. The public mobile networks in the Netherlands have a good coverage, and with the roaming agreements connectivity is available throughout the EU and large parts of the world. However, especially in rural areas, coverage might pose a problem.

Choice of the exact communication architecture depends on a number of requirements. Low power communication is vital for battery operated devices.

Other factors include usability requirements (ease of use and implementation) and cost.

Data, data formats and application protocols

In general, IoT devices ('Things') communicate only small amounts or bursts of information compared to other (internet) traffic such as online video streams, with logical information content of one information burst is in most cases in the order of one byte to kilobytes[34]).

The resulting amount of data traffic however can vary considerably, depending on the application, the number of devices involved, the used data formats and application protocols. Also the interval between bursts varies considerably (from once or several times per month to many times in a minute). What adds complexity is that many devices have busy or quiet periods with less or more bursts and devices may sleep or be turned off.

ICT applications tend to start lean and mean at the time of introduction, but new functionality is likely to be added for device updates, or new or updated applications, causing similar devices and applications to exchange more data or to exchange data more frequently after each update. For many devices it is possible to distribute new firmware to the devices over the same wireless connection.

Wireless communication of data

Data is sent in messages that contain, in addition to the data itself, information such as addresses of sender or receiver. Apart from messages containing data there is additional traffic, for instance related to 'keep alive' signals, registration or deregistration of devices.

Various types of message exchange can be distinguished: dependent on used hardware, protocols and applications a device may use one or a combination of the following strategies, each with a different impact on traffic:

- broadcasting their information without any check or confirmation whether the information is actually received,
- 'listen before talk' to minimise the chance of interference,
- wait for a confirmation message and otherwise resend the message,
- sending the message using adapted transmission speed or using adapted transmission power, that fit the circumstances,
- only send information when a request for information is received from a gateway or controller, send information via neighbouring devices that resend the message,
- send information via a proxy or gateway that itself is a wireless device[35],
- using or not using specific broadcast or multicast technology to optimise transmission of similar messages to multiple recipients,
- generally only receive messages, generally only send messages or both receive as well as send messages.

Cognitive Radio, multiband devices and whitespaces

Some devices have multiple radio's in them, suited for a variety of bands and protocols. This means the device itself can choose the band or protocol most suited (depending on a number of rules). For example, a device using cognitive radio could 'sense' various bands and choose

[34] This does not include applications with streaming data such as surveillance cameras, media streaming devices etc.
[35] For instance a Bluetooth device that communicates with a car kit that communicates via a mobile network

a free band. Already some smaller – devices have the technical ability to operate on different radio bands or even multiple network technologies[36].

Such developments are of importance for future spectrum efficiency. However, for the current very low power sensors that drive IoT, implementation of multiple radios is at this stage not obvious since it puts strain on antenna design, power consumption and cost of a device.

Technologies, protocols and ecosystems

Various protocols are used, each with their own characteristics to serve specific applications, work in specific circumstances, and each with their own types of messages they need to exchange.

Technology ecosystems are slowly forming around protocols and clusters of manufacturers and/or users[37]. Specialised low power protocols and networks are in development, while other applications use existing protocols or networks.

The remainder of this chapter gives an overview of the existing and emerging network and protocol technologies and standards.

Addressability

One of the major success factors of the internet is uniformity of the middle part of the addressing and session protocols, allowing worldwide addressability of computers. The combination IP, HTTP(S) and HTML is now the absolute standard for web services, and worldwide addressing and interaction is successfully standardised. The IPv4 address space is almost entirely used by existing IP equipment. This means all devices on the internet are in principle reachable using the internet.

For IoT this is slightly different. The number of devices that form the 'Internet of Things' is of a much larger magnitude. In some cases the devices are IP capable and can be connected to an IP network like the Internet directly. Theoretically IPv6 can cater for the address space but then addressing takes up a relatively large amount of bandwidth and resources compared with the few bits that are interchanged by devices. In other cases, the sensor devices are not IP capable and use some low level, low overhead protocol to talk with a gateway. The gateway usually is connected and addressable using IP, but the individual devices are not.

4.3 Communication technologies

Communication is the 'glue' that binds all the sensors, actuators, presentation devices, management platforms and databases together to form 'the Internet of Things'.

[36] http://www.pcworld.com/article/2038054/panasonic-creates-multiband-m2m-chip-with-20year-lifespan.html

[37] For instance in lighting and home automation around the protocols ZigBee and Z-wave, and in the automotive industry around the emerging ITS standardisation efforts.

4.3.1 Ranges of communication

The Internet of Things involves communication between devices at various levels, and application can involve multiple communication methods. A coarse distinction in communication can be made based on the reach of communication:

- **Wireless wide area 'macro' networks**: For communication using connectivity over larger area's (countries or larger), for example using macro networks like operator controlled mobile networks (or sometimes even satellite communication).

- **Metropolitan Area Networks**: Communication between devices on a more localised, metropolitan area (up to a couple of kilometres) in an area.

- **Wireless Local Area Networks**: Communication between devices in your home, office or workplace form a 'Local Area Network'.

- **Personal Area Network (PAN)**: Personal devices that you carry around and connect on a 'personal scale' form a Personal Area Network.

Although these scales of operation give an indication of the type of networks used, often certain technologies can also be used at other scales: public GPRS networks form a large-distance network, but larger scale networks could in principle also provide the connectivity of devices that operate at a smaller scale. For example, GPRS is also used for static devices for other reasons, like control over network connectivity[38]. Choice of a specific network technology is based on a combination of various aspects, including the reach of a network, cost, availability, manageability, and uniformity (or diversity) viewed from the perspective of the device 'operator'.

An example of devices forming a Personal Area network are wearables and wristlets connected via Bluetooth to your phone, which collects data and acts as your personal 'hub' and control centre.

Local networks in the context of the Internet of Things are networks connecting local sensors to each other or a (homecentric) hub which you control from your tablet, for example using Wi-Fi. For wider areas either single cell networks (for static devices or devices within a restricted area) or countrywide 'macro' networks are a logical choice.

Various supporting technologies are emerging. In the following paragraphs the most common protocols and underlying technologies are described briefly.

4.3.2 Wireless wide area 'macro' networks

Cellular mobile networks

Cellular networks are already used for many applications today, usually for applications that involve mobile devices that moved over larger distances or are scattered over multiple sites.

[38] For example smart meters were introduced to give users insight in energy-usage. In practice, data is transferred out of your home using GPRS, while you access the server containing the date using the internet from your home.

Especially for those applications where the cost of wireless communication is relatively low compared to the whole product (for instance in vending machines) or in cases where access to a cellular mobile network can be used for other purposes, the relatively high costs of the SIM and connections and high energy consumption is less important.

In recent years the subscription prices for 'M2M' sims that use in the order of 1-2 MB's of data per month have been declining, making it more feasible to connect more devices (like millions of smart meters) using cellular networks.

A challenge faced by some parties is the need to physically replace the SIM when switching operators. A number of initiatives are taken to make switching easier, like using softSIMs that are reprogrammable, or by allowing M2M operators to use their own (shared) MNC so that they can effectively work as an MVNO[39], and manage their own sims.

There is an effort to develop a *Low Power LTE* or *LTE MTC (Machine Type Communication*) variant, but this effort is currently still in research and prototyping phase[40]. It is for instance not yet clear how Low Power LTE solves the challenge of catering the combination low transmission power and longer transmission distances while co-existing with other LTE devices. Introduction of the first LTE low power features is expected in the coming years (3GPP release 13 and further).

Although LTE is mostly used for such operator owned networks in licenced spectrum, LTE as a technology can be used for private LTE networks in licence exempt or locally licenced band like the 3.5 GHz band in the Netherlands[41].

Characteristics:

- Standard: 3GPP and GSMA, GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G)
- Frequency bands: 800MHz/900MHz/1800MHz/1900MHz/2100MHz/2600MHz
- Operating Range: Up to 35km for GSM; Networks covers country or wider.
- Data Rates (download): 35-384kps (GPRS/EDGE), up to 3-10Mbps (LTE)

Other

Others include WiMAX (although in the Netherlands no WiMAX networks are operational) and Satellite as an alternative macro network that plays a role for niche applications for instance for devices that are scattered in (very) rural areas, like for monitoring pipelines or electric wire networks that stretch hundreds of kilometres across remote areas (total market estimated at only 3 million units in 2014 and mainly serves a ´niche' market).

4.3.3 Metropolitan Area Networks

This segment of communication technology is an upcoming area of communication. It is used to accommodate communication for low power (battery powered) devices on a distances up

[39] In the Netherlands the possibility to allow M2M operators to use a subset of an MNC's was introduced in 2014, creating dedicated (sub)imsi ranges for large-scale M2M applications.

[40] http://www.rethinkresearch.biz/articles/huawei-demonstrates-pre-standard-lte-m-vodafone-targets-cellular-iot/

[41] Using LTE for such a network positions such a network in the 'metropolitan area' category.

to a couple of kilometres (so using less power than the regular GPRS or LTE networks, and communicating further away than conventional WLAN's)[42].

These kind of networks, that can be operated in shared licence exempt spectrum, are also distinct from the 'WAN macro networks' with respect to operation and management: they can operate stand-alone or be operated by local users, such as a municipality or company without the need of a contract with a third party. This freedom of operation is an important driver for easy to implement applications on a local scale.

As we will see, some technologies suited for such networks can also be used to implement macro networks (and the other way around: LTE in local or licence exempt spectrum can be used to create local owned metropolitan or street level networks).

LoRa/LoRaWAN

LoRaWAN (Long Range Wide Area Network, known as Lora) is a low power communication technology developed by the company Semtech and standardised in the LoRa Alliance (founded in March 2015).

LoRa aims at low power applications that only need to send a relative small amount of data. Such networks allow for applications such as sensors that can run on batteries for a number of years.

A LoRa network typically consists of a gateway that communicates to the sensors using the LoRa protocol. The gateway itself is connected to a backend using for example a fixed Ethernet connection or LTE.

Currently there is much interest for such low power networks that operate at a longer scale since they are more suited for M2M and IoT then for example the LTE macro networks.

Recently a city network based on LoRa has been introduced in Amsterdam[43]. Apart from local use KPN is now considering rolling out a nation-wide LoRa network in the Netherlands. In this case, LoRa technology is used to create a 'macro network', in which case it plays a different role.

Characteristics:

- Standard: LoRa
- Frequency band:868 MHz (EU) / 915 MHz (US)
- Operating Range: 2-5km (urban environment), 15km (suburban environment)
- Data Rates: up to 50kbps.

SigFox

SigFox is a low power technology for wireless communication to a diverse range of low-energy objects such as sensors and M2M applications that need to send a relative small

[42] https://machinaresearch.com/news/with-3-billion-connections-lpwa-will-dominate-wide-area-wireless-connectivity-for-m2m-by-2023/

[43] http://thethingsnetwork.org/

amount of data. Such networks allow for applications such as sensors that can run on batteries for a number of years.

A SigFox network consists of cells with a central gateway that communicates to the sensors. The gateway itself is connected to a backend using for example a fixed Ethernet connection or LTE. It allows for transport of small amounts of data over ranges up to 50 kilometres. The technology was developed by the French company SIGFOX founded in 2009. Major players are Samsung, Airbus, Telefonica, SK Telecom and NTT. Currently there is much interest for such low power networks that operate at a longer scale since they are specifically suited for low power (battery powered) devices.

In the Netherlands Aerea operates a SigFox network that covers a large part of the country. The network evolves from a metropolitan network to a low power WAN macro network, in which case it can play a different role by providing coverage in large parts of the country and possible nomadicity functionality[44]. Recently Tele2 and Aerea formed a partnership in the Netherlands to provide SigFox network access for Tele2 M2M customers.

Characteristics:

- Standard: SigFox,
- Frequency band: 868MHz in Europe and 915MHz in the U.S.,
- Operating Range: 3-10km (urban environments), up to 50km (rural environments),
- Data Rates: up to 1kbps.

Other

Other candidates for use on metropolitan ranges are Weightless, 'On-Ramp Wireless' and Wireless M-Bus (Metering Bus, for communication between meters for water, gas, electricity on one side and the data concentrators on the other side).

4.3.4 Wireless Local Area Networks

Communication in the 'local area' range is used for various 'Internet of Things' signalling and switching of devices, such as for home and building automation. The main protocols include Wi-Fi and ZigBee. Within these networks, a difference can be seen between specifically designed (very) low power protocols, and more general protocols for higher bandwidths.

Wi-Fi

The IEEE 802.11 standards, more commonly known as 'Wi-Fi', evolved to a standard used by virtually every laptop and phone. It is the technology behind most wireless local area networks in homes, offices, and other environments. Popularity started in 1999 with the IEEE 802.11b standard, but is since extended providing more bandwidth and using the 5 GHz bands. Wi-Fi is the most ubiquitous wireless technology today.

Characteristics:

- Standard: Based on 802.11n (most common usage in homes today)

[44] This means that a device is still connected and addressable for communication when it is moved from one area to another.

- Frequency band: 2.4 GHz and 5 GHz bands
- Operational Range: Approximately 50m
- Data Rates: up to 600 Mbps (latest 802.11-ac standard could offer up to 1Gbps)

Low Power Wi-Fi (under development)

IEEE 802.11ah (sometimes referred to as 'low power Wi-Fi') is currently being developed and aims for low energy applications in extended range networks, such as groups of sensors, stations or M2M applications in a larger area. IEEE 802.11ah uses sub 1 GHz license-exempt bands, to enable low power utilisation and longer working ranges.

Characteristics:

- Standard: IEEE 802.11ah; expected to be finalised in 2016;
- Frequency bands: Under discussion, various sub GHz ISM bands proposed;
- Operational range: up to approximately 1 km;

ZigBee

ZigBee is a protocol for low power, small distance (10-100 meter) communication of small amounts of data with 250 kbps. It is based on an IEEE 802.15.4 standard. It supports a mesh topology which enables transporting data over larger distances by passing through data from device to device. Typical applications are wireless light switches, lighting settings such as mood lighting or adaptive lighting, remote displays of meters and sensors, traffic management systems, and other consumer and industrial equipment. The ZigBee protocol suite includes profiles for different application types including smart energy, building automation, health care and remote controls for television and set top boxes (this last profile is known as RF4CE and was standardised in 2009 as part of ZigBee. Major players in this field NXP, Philips (Hue lighting system), Panasonic, Sony and Samsung.

Characteristics:

- Standard: ZigBee 3.0, based on IEEE802.15.4
- Frequency bands: 2.4GHz
- Operational Range: 10-100m
- Data Rates: 250kbps

EnOcean

EnOcean is a protocol for use in industry, transportation, logistics and smart homes. The system uses an energy harvesting technology used in building automation systems in which the energy from pressing the button is used for the wireless communication.

Characteristics:

- Standard: ISO/IEC 14543-3-10
- Frequency bands: 868 MHz (Europe), 902 MHz (North America), 928.35 MHz (Japan), 315 MHz (US)
- Operational Range: 30m inside buildings
- Data rates: 125 kbps

Z-wave

Z-wave is a protocol developed primarily aimed at home automation applications such as lighting, smoke alarms, remote controls and home appliances. The technology is designed for low power transmission of small data packets at relatively low speeds up to 100 kbps.

Characteristics:

- Standard: Z-Wave Alliance ZAD12837 / ITU-T G.9959
- Frequency bands: 868 MHz / 900MHz (ISM)
- Operational Range: 30m
- Data Rates: 9.6/40/100kbit/s

DECT Ultra Low Energy

DECT Ultra Low Energy is a low energy variant of the DECT protocol that is used for cordless (home) telephones. The 'ULE' variant was introduced in 2011 and uses the 1.9 GHz band. The standard aims to enable home automation, security, healthcare and energy monitoring applications that are battery powered and can easily connect to the web using the large number of existing DECT enabled modems and be managed using a smartphone app.

Characteristics:

- Standard: DECT ULE, ULE Alliance (cooperation between ETSI and DECT Forum)
- Frequency band: 1.9 GHz band
- Operating Range: over 50 meters in buildings and up to 300 meters in the open air.
- Data rate: up to 1 Mbps

Thread

Thread is a new protocol developed by Nest Labs of Google in collaboration with Samsung. The protocol is IP(v6)-addressable IEEE 802.15.4 based protocol with mesh communication. Thread has support for over 250 devices on a network. In May 2015 Google introduced the Brillo platform which is designed to work with Thread and an SDK named Weave.

Characteristics:

- Standard: Thread, based on IEEE802.15.4 and 6LowPAN
- Frequency band: 2.4GHz (ISM)
- Range: N/A
- Data Rates: N/A

Other

Other protocols include Dash7 (an open source RFID-standard for wireless sensor networking for applications that do not want to use comparable but in some respects less open standards such as ZigBee and Z-Wave), and INSTEON (a dual-mesh RF and PowerLine technology for home automation).

4.3.5 Personal Area Network (PAN):

Short range, low power communication protocols are used for local communication forming Personal Area Networks for connecting devices in one's direct vicinity. Technologies used for such communication includes Bluetooth, Wireless USB, and NFC, although for example ZigBee can fall in this category too.

Bluetooth

Bluetooth is a low power, low range communication protocol that connects devices in each other's direct vicinity, like mobile phones or laptops to each other or to other peripherals like sensors. Three variants of Bluetooth technology can be roughly distinguished. Bluetooth Low Energy (which is the current standard) was introduced in the Bluetooth standard in 2010 (version 4.0) and marketed as 'Bluetooth Smart'. The technology is faster and more energy efficient than earlier Bluetooth implementations over comparable distances. *iBeacon* is a technology based on Bluetooth used for indoor localisation and beacons. It uses Bluetooth technology to achieve simple RFID/NFC like functionality over larger distances (centimetres to over 100 meters) and enables use for navigation in buildings by using location ID's / UUID as predefined waypoints or reference points.

Characteristics:

- Standard: Bluetooth 4.2 core specification
- Frequency band: 2.4GHz (ISM)
- Operational Range: 50-150m
- Data Rates: up to 1Mbps

Radio Frequency ID (RFID)

Radio Frequency Identification is a relatively cheap way to identify objects using tags that can be 'interrogated' using low power radio signals to detect the identification code of the tag. Two systems are most common: Systems with an active reader and a passive tag (with a tag that uses the interrogation signal to produce a response and does not need batteries), and systems with an 'active tag and reader', which uses a tag that actively responds or sends an ID. Most RFID systems use standardised ISM bands.

Characteristics:

- Standards: Variety of standards. include ISO, IEC, ASTM International, the DASH7 Alliance and EPC-global.
- Frequency bands:
  - 120–150 kHz (10cm) can be used license free worldwide
  - 13.56 MHz (10cm-1m) can be used license free worldwide
  - 433 MHz (1-100m)
  - 865-868 MHz (Europe) and 902-928 MHz (North America) (1-12m).
- Data Rates: 100–420kbps

Near Field Communication (NFC) is a term used for a more elaborate form of communication using similar technology principles as RFID, but not only used for identification but for more elaborate two way communication. Examples are interrogation of sensors, or storing and retrieving information in tags.

Similar to RFID, different communication types can be distinguished: passive communication and active communication. In the case of passive communication the target device answers an initiator device without the need of an internal power source: the target device draws its operating power from the initiator-provided electromagnetic field, so no batteries are needed in the target device. In the case of active communication initiator and target devices generate their own RF fields.

Characteristics:

- Standard: ISO/IEC 18000-3
- Frequency band: 13.56MHz (ISM)
- Operational Range: 10cm
- Data Rates: up to 420kbps

Non-wireless identification methods

There are identification mechanisms and protocols using 'machine readable identification tags', such as barcodes, QR codes that do not directly affect frequency use, but certainly have an impact indirectly to data traffic and spectrum use because the use of such methods generates wireless traffic.

Others

Others include a number of IEEE 802.15.4 based standards (WirelessHART, Modbus wireless, MiWi, and ISA100.11a), ANT (aimed at the communication of sports and fitness sensors to a display unit such as a watch or cycle computer), Wireless USB, and a number of other proprietary or system-specific protocols.

4.4 Platforms, ecosystems and alliances

Recently several attempts to organise, structure and standardise the Internet of Things have emerged. These 'platforms' make it easier to develop applications by providing functional building blocks that can easily be reused by application builders. In this paragraph a number of noteworthy platforms and ecosystems are described in three categories:

1. *Hardware oriented application platforms and ecosystems*: physical systems consisting of a set of chips and physical interfaces (sockets such as) on a circuit board,
2. *Software oriented application platforms and ecosystems*: operating systems or middleware that provide software interfaces that can be used as a basis for application software,
3. *Other alliances, organisations and ecosystems*: they promote or develop combinations of software and/or hardware standards or best practices.

4.4.1 Hardware oriented platforms and ecosystems

Prototyping and flexible implementation hardware platforms

There is a wide variety of hardware prototyping platforms. One of the most commonly used is *Arduino*, a compact open source single-board microcontroller for building small interactive devices (with board sizes varying from less than 2 cm to more than 10 cm) that can sense, control and interact. Other examples of similar prototyping platforms are *Beaglebone* and *Raspberry Pi*. Often those platforms run Linux or some other small footprint operating system for embedded devices. All platforms have variants allowing developers to choose the most suited devices, based on factors including size, processing power, power consumption, flexibility towards wireless capabilities, memory, programming languages, and cost.

Wireless System on Chip (SoC) platforms

Modules with RF and IP capabilities combined on one chip are created by manufacturers like *Texas Instruments*, *Gainspan, Wiznet, Nordic Semiconductor,* and others. These solutions allow companies to add wireless communication features to devices without having the need to have extensive RF expertise and going through lengthy certification processes.

4.4.2 Software oriented platforms and ecosystems

There are many different approaches towards extendible software platforms for applications. Roughly we can distinguish platforms for devices, such as firmware platforms or light operating systems, platforms for gateways or application controllers, and platforms for cloud solutions. Below for each of these categories some examples are given.

Software platforms for devices

Embedded devices require specific software since they need to cope with the low power, and often low memory and processing power of those devices. The platform supports a variety of communication options, like Bluetooth Low Energy and Wi-Fi.

Dedicated operating systems and firmware platforms include a number of open source platforms such as *TinyOS* or *LiteOS,* lightweight operating systems originally developed for sensor networks, other small footprint Linux or BSD based systems, and for example *Thingssquare Mist,* a lightweight open source firmware platform that works with multiple microcontrollers with a range of radios. Recently Google announced an Android-based embedded operating system called ‘Brillo’, to be available in the second half of 2015. It interworks with the protocol Weave.

Software platforms for server based ‘cloud’ solutions

Internet-based platform provide an internet based server side with which devices can communicate and act as central point in ’cloud’ solutions for managing devices, monitoring connections, and collecting data . Specific applications or analytics services can be applied using those platforms. Variants include data broking platforms, application design environments and platforms for machine learning. Examples are *Carriots* an application hosting and development platform and *Nimbits,* a “Data Logging Service and Rule Engine Platform for connecting people, sensors and software to a server on the internet and one another”. *Jasper* is a management platform for provisioning, diagnostics, billing, etc. that is used in a variety of industry sectors. IBM in march 2015 announced its '*cloud-based open platform for Industries'*.

There are a number of open source initiatives to combine control over home automation devices from various vendors. Example are the open source platforms *Domoticz* and *Domotiga*, both platforms that can run on simple hardware like a raspberry pi and aim to connect devices of multiple home automation vendors into one simplified control application. Both allow the various devices to be controlled from a single App on a smartphone or tablet. An advantage of such a system is that the platform can run independent from the various manufacturers, preventing a (practical) lock-in.

Software platforms for gateways or distributed applications

Examples of platforms for gateways or distributed applications are The *Intel IoT Gateway Development kit*, a combination of a hardware and software platform for gateway development, *Nitrogen*, a platform that aims to connect devices together into applications, and the Huawei Internet of Things Solution aimed at interworking with LiteOS operating system for devices and a management tool for gateways, applications and data.

Several middleware platforms aimed at technical application areas such as robots and sensors, sensors (*SensorBus, SensorWare*), etcetera, probably fit in this category.

Application layer protocols

A broad range of application layer protocols including session protocols, data structuring languages etcetera, is used. Examples[45,46] are existing protocols such as *HTTP* (known as the protocol for webpages), *REST* and *SNMP* (Simple Network Management Protocol, used for managing switches, printers etcetera). Most of the currently widely used data, session and application protocols such as HTTPS do not fit[47] well with the requirements that are generally associated with IoT: low power, long duty cycle, and small messages. Specific M2M and IoT oriented protocols are developed such as *COAP* for very simple electronic devices and *MQTT*.

Apple introduced a *Homekit* as a common protocol and API for home automation devices. Google recently announced the protocol *Weave.* Both aim to be a library of high level terms and commands to be used universally among supported devices.

4.4.3 Alliances and organisations

There are several alliances and organisations related to IoT (see figure 4 for a non-exhaustive overview) and recently many more initiatives, consortia, alliances and platforms have been announced.

Standard groups such as ITU, IEEE, ETSI and specific standards groups and consortia such as the Wi-Fi alliance and the LoRa Alliance define and promote protocols or platforms mentioned earlier in this chapter, while also user or sector specific consortia promote introduction of application in specific fields. Examples of this are described in chapter 3.

[45] http://embedded-computing.com/articles/internet-things-requirements-protocols/

[46] http://postscapes.com/internet-of-things-protocols

[47] "Why HTTP is not enough for the Internet of Things", IBM (2013)

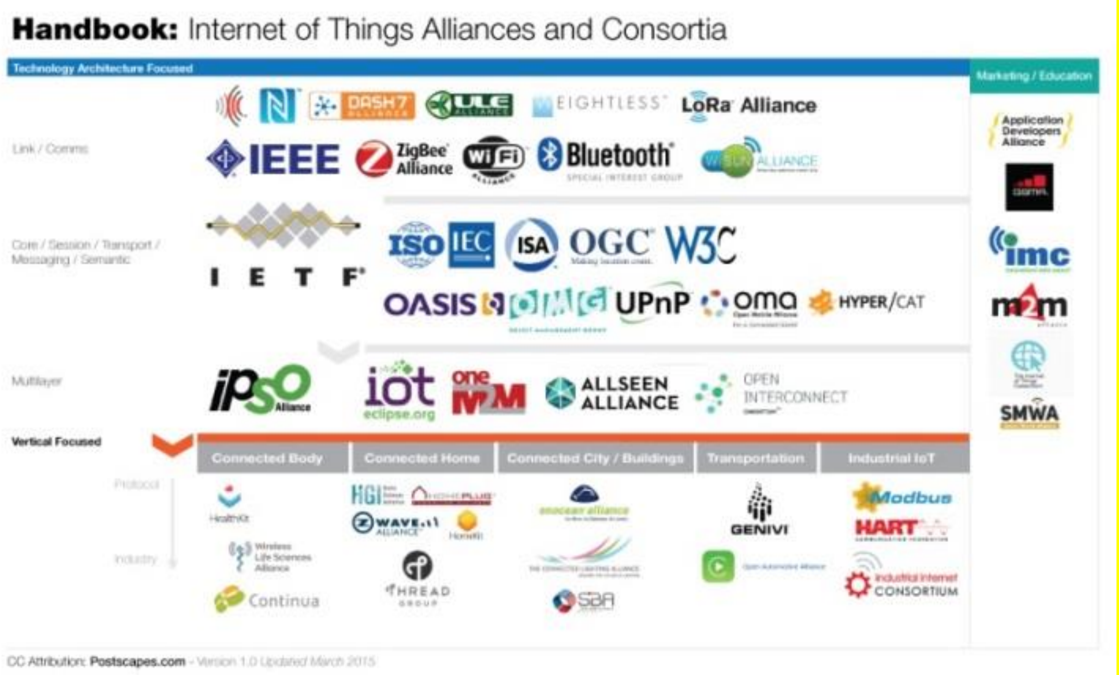


Figure 4: Overview of alliances and consortia (source: Postscapes.com)

4.5 Trends and observations

The Internet of Things is already a technical reality, but consists of a large variety of ecosystems, protocols and devices. There is still a wide variety of transport and transmission protocols that is used for or aimed at IoT, and currently even more protocols and platforms are introduced or announced. A de-facto standard or 'typical use' has not (yet) emerged.

There are many proposed candidate protocols that potentially could be used, and the amount and variety of proprietary and open protocols, standardisation efforts and standard bodies and consortia is not yet consolidating.

This large diversity makes it difficult to allow the promise of simple, ubiquitous connectivity and interworking between many different sensors, actuators and applications to become reality.

This (at least partly) explains why the emerging applications are often 'bottom up' and relative small scale: such a wide variety of choice makes it hard for (large scale) implementations of IoT to take place, since it is unclear if an investment in a system will still be supported in ten year time.

For consumer products, with lifecycles of only a couple of years, this is sometimes less of a problem. However, also for consumers, long term certainty is needed, for example as is the case in home automation: Although stand-alone switches are easy to replace, implementation of fully automated lights in new build homes will only become the standard once the needed Home Automation systems are mature and standardised.

It is to be expected that in the coming years, as the market matures, de facto market standards, will become clear, paving the way for longer term implementations.

One of the dilemmas is where data collection, aggregation and intelligence ideally should be placed in the architecture. There is a trend from centralised intelligence in clusters of servers back to distributing intelligence toward the nodes (this trend is sometimes called *'the fog' or 'edge computing'*), running apps (more) locally, self-learning, and in real time (since a high latency connection to a centralised server might not always be the best option for decentralised sensors and devices).

5 Radio spectrum and IoT

For data exchange of devices and other components, several wireless communication options exist, with different characteristics. Relevant characteristics include what spectrum is available (like available bandwidth and radio carrier frequency, high versus low). And possible legally imposed restrictions for use (i.e. is a license needed, is this license uniquely given to one party, or is the spectrum license-exempt). Other characteristics relate to the organisation of the communication. Based on those characteristics, and on other factors like (expectation of) interference of other users, availability of (low cost) radio chipsets, operators or manufacturers of M2M devices choose one or multiple communication options, and a multitude of spectrum bands, for their applications. For wireless communication between 'things' different types of networks and spectrum each play their role.

5.1 Communications "as a service" vs "user operated"

Depending on the application, either 'communication as a service', with an external party managing the service, or 'user/device operated' communication where the user or the solution itself is managing the service (giving autonomy over the connectivity), or a combination of the two, is used.

In the wide range of (possible) applications both operator controlled network services and 'stand-alone' communication solutions are widely used. Both have their technical and practical advantages. For some cases both modes might suffice (giving the developer choice of communication channel) or both are needed (for example using local communication via a user operated Wi-Fi network and also using an operator controlled backhaul via DSL or LTE).

For innovation and development of low power wireless devices, it is important that developers can choose from both kinds of communication as they see fit, so that ultimately they choose the "best solution for their application"[48].

5.2 Role of licensed exempt spectrum

Licence exempt frequency bands can be used without the need for a licence or authorisation and therefore play an important role in a large number of applications. Unlicensed or shared bands can be used by everyone, under the right set of conditions (often limitations apply regarding power or duty-cycle, and sometimes unlicensed bands are designated for specific applications).

The main feature of this spectrum is that it is a shared medium, and users can use it without licence. Because of this, this spectrum plays an important role in the success of many wireless applications, since it allows end-users to simply 'buy' a system and start using it without any further fuss.

[48] Off course, what is technical the most suitable solution might not always be chosen, for other reasons. This also depends on who is the ultimate customer.

However, sharing also means the same spectrum is used for different devices, protocols and ranges of communication. This leads to (sub)eco systems within one band that influence each other. Within one ecosystem, coexistence is easier to implement since the protocol can take into account existence of other devices using the same protocol. However, a multitude of ecosystems in the same band means it is harder to avoid interference. Also, the one that uses the band most or sends with the most power can have a large impact on other ecosystems that make less heavily use of that band (for example, the enormous use of Wi-Fi for broadband can have more impact on other applications in that band than the other way around).

Specifically at a personal, residential, and street-level scale, the availability of licence exempt spectrum is key: communication at a local scale is best handled locally, and the license exempt spectrum like the ISM bands plays this role in many of the emerging IoT devices (just as it does for local wireless broadband).

Licence exempt spectrum provides an autonomous, low cost way to connect devices and that is easy to implement. Also, it requires no administrative overhead, and can therefore facilitate an easy way for manufacturers and innovators to enter a market with products that can be sold 'as is' without further registration.

This type of licence exempt spectrum plays a key role in further enhancing growth of IoT, and the long term availability of (relatively) interference free, licence exempt spectrum is vital for IoT to keep growing. It is vital that developers of applications have such license free spectrum at their disposal, and that there is certainty that that specific spectrum stays available for at least the next 10 to 15 years[49].

5.3 Role of Licenced spectrum

Licensed bands give the licensee the exclusive right to use that band. This gives operators of networks the possibility to control the network to a high degree and to optimise efficiency with regard to used protocols, availability and redundancy, QoS, admission of devices, etcetera.

Countrywide licensed spectrum plays a major role for operator-controlled macro-networks such as GPRS and LTE networks. Those networks play a role mainly for those applications that are mobile and for those that need to operate at various places outside the owners' (local) area. Because of their countrywide network coverage and (global) roaming agreements mobile operators fulfil the role of countrywide, Pan-European, or worldwide connectivity service provider. New releases of LTE aim at low power devices (low power LTE), and some of those features may already become available in the coming years.

Local licences spectrum, like the 3.5 GHz band, can be used for private LTE networks. This gives a company or organisation a high level of control over the network and spectrum usage at a local level. The main advantage is that the network infrastructure can be built

[49] Of course spectrum is often hard to free once successful: the large amount of applications currently using 2.4 GHz and 868 MHz spectrum will make it virtually impossible to reassign those frequencies for other purposes.

specifically for the needs of the organisation, for example in terms of redundancy of network elements and local coverage.

5.4 Harmonisation

Harmonisation of spectrum, preferably worldwide, is an important success factor for IoT applications. It reduces development cost and reduces the need to create different types of products for different markets. Also, it allows for devices to be easily transported and used throughout the world.

A similar issue plays a role in smartphones (that use a wide variety of bands that are only partially harmonised). Smartphones have been 'multiband' for many years and can switch to other frequencies when necessary.

However, for IoT the problem of harmonisation is specifically vital, since the devices need to be small and low power. They cannot easily be equipped with multiple radio's and antennas. The 2.4 GHz (and the 5 GHz) are widely used bands that are largely harmonised throughout the world. In the sub-1GHz range, slight variations exist, like the 868 MHz spectrum in Europe that plays a similar role as the 915 MHz in the US and Japan, causing fragmentation of the market (i.e. devices are either sold for 868 MHz or 915 MHz). Although from a technical perspective, devices manufactured for one band can sometimes use both bands, this is not allowed. There are developments towards more hardware flexibility regarding the use of different spectrum bands.

5.5 Spectrum bands

The following paragraphs give an overview of the most common radio spectrum bands for IoT applications, grouped by the categories 'license exempt' spectrum, 'application specific' spectrum, and 'licensed' spectrum.

5.5.1 License-exempt spectrum

There are a number of license exempt bands[50] available for (amongst others) use of short range devices and sensor networks. For IoT the most commonly used licence exempt bands are the 433 MHz band, the 868 MHz band, and the 2.4 GHz band. There are a number of other (smaller) bands, but they do not appear to play a major role.

433 MHz

The 433.05-434.790 MHz spectrum is used for a range of low power devices like weather stations and outdoor temperature sensors, remote controls for toys, remote car key locks etcetera.

[50] https://www.agentschaptelecom.nl/sites/default/files/brochure-vergunningsvrije-radiotoepassingen.pdf

868 MHz

The 863.0 - 870.0 MHz is used for a large array of applications. Typical use of this band includes RFID/NFC, SRD's, LoRa, SigFox, and a (large) number of proprietary or application specific radio protocols, for communication over ranges varying from a few meters to up to hundreds of meters. The spectrum is harmonised for use within Europe.

Some parties mention unwanted interference between for example RFID-readers and communication systems in this spectrum. For now, there seems to be sufficient spectrum in this band, although additional (sub-GHz) licence-exempt spectrum is on the wish list for future expansion: A number of stakeholders, including manufacturers, expect the pressure on this spectrum to increase in the coming years, due to both growth of local communication applications and traffic as well as the advent of low power wider range networks.

At this stage, there are a number of initiatives (both in the Netherlands and in a number of other countries) to roll out countrywide operator controlled networks for SigFox and Lora. Such large scale networks can increase the pressure on this band since they coexist with the other applications and networks that make use of the same band.

Licencing (as one might consider in case of scarcity) is not an option: the fact that this spectrum is licence-exempt is likely to be one of the key drivers for IoT and metropolitan scale networks, so limiting the ease of use would harm IoT introduction. One way to deal with this is to designate additional similar sub GHz spectrum for those kinds of applications and networks. To prevent the new spectrum from getting crowded early on, additional technical restriction could be put in place, like reduced allowed power or duty cycles.

2.4 GHz (2.412 – 2.472 GHz)

The main protocols used in this band are IEEE 802.11 (Wi-Fi), IEEE 802.15.4 (ZigBee), and Bluetooth, and there are a number of other proprietary or application specific protocols (for example used for some types of smoke detectors and motion alarms). Use of Wi-Fi in the 2.4 GHz band is very attractive because of the availability of standard compliant hardware and firmware.

However, the 2.4 GHz is under pressure due to its success since this spectrum is widely used by many users and devices for wireless local broadband and industrial applications experience increasing challenges to meet the demand for higher bandwidths and service availability in this ever more crowded spectrum. Some parties mention interference and operation problems in this band concerning SRD's. There are reports that future interference from neighbouring LTE might reduce the effective amount of useful spectrum in this band[51].

[51] See "LTE and 2.4GHz SRDs interference issue and policy recommendation", Green Peak (2015)

Other licence-exempt bands

5 GHz

The 5 GHz band is available for licence exempt use and is mainly seen as the band to relieve the crowded 2.4 GHz band for wireless broadband (using 802.11n/ac, allowing wider channels up to 160 MHz). The expected usage mainly involves high-bandwidth applications, although Wi-Fi enabled IoT applications might also use this spectrum.

Restrictions related to military use and radars apply for (a large) part of this band. This limits the flexibility of devices and products in this band. In practice this means that to use the entire band a DFS-system that switches away from a part of this band if radar is detected is mandatory in access-points.

Even for professional users it is not always clear what the chances are that temporary or permanent unavailability of spectrum due to DFS obligation will occur. Providing better information about the (expected) availability in place and time[52] throughout the Netherlands could help removing this barrier in some cases. Other parts of the band are restricted to in-door use only. It is unclear whether enforcement of this restriction is feasible, especially for the growing numbers of consumer devices that are also used outside.

60 GHz spectrum

The potential use of 60 GHz spectrum (57-66 GHZ in Europe[53]) has gained attention recently and is being considered for high-bandwidth, short distance communication. This is mainly driven by proposals for wireless multimedia-streaming within a room from for example a home theatre PC to the TV, eliminating the need for Ethernet-cables around the TV. Proposed protocols include 802.11 ad and WirelessHD both aiming to provide data rates of multiple gigabits per seconds over short distances. Although bands vary slightly throughout the world, there is a large overlap of 5 GHz of harmonised bandwidth worldwide.

915 MHz

The 902-928 MHz band, designated for SRD's in the US and Japan is not in use for SRD's in Europe, but plays a similar role in the US and Japan as the 868 MHz spectrum in Europe.

Spectrum under consideration

Additional license exempt spectrum for SRD's is under consideration of CEPT and others. For example, the 3 MHz 700 MHz duplex gap is proposed for future use of SRD's. Other spectrum under consideration for usage for SRD's and IoT-like applications is the 870-876 MHz and 915-921 MHz spectrum. In the Netherlands and in some surrounding countries this spectrum is at this moment designated for military use. Throughout Europe, this use of this last spectrum band is currently fragmented, but alignment in (parts of) Europe might be possible. The UK recently announced it would make this spectrum available for short range devices

[52] For example, the likelihood that part of the spectrum is not available depends on the presence of radar systems using that frequency. In locations where radars are expected, this might pose a problem, while in other locations it might not. An indication of the (expected) percentage of time spectrum cannot be used at some locations would help.

[53] For an overview see http://www.digikey.com/en/articles/techzone/2013/jul/high-speed-60-ghz-wireless-connectivity-finally-takes-off

(see paragraph 6.2 about the UK). CEPT [18] concludes that "*while there are several administrations where implementation of the SRD Recommendation will be problematic or partial, there remain a number of administrations where full implementation is possible*". A major advantage of this spectrum is that this band can pose an opportunity to create a band that is uniform throughout a large part of the world (including Europe, the US, and Japan).

5.5.2 Licensed spectrum for public mobile networks

Licensed spectrum for public mobile networks play an important role in providing countrywide (and even worldwide) connectivity, mostly in the form of 3GPP-based networks operated by the telecom operators. The most commonly used bands in the Netherlands are 800 MHz, 900 MHz, 1800 MHz, and 2100 MHz bands, with 2.6 GHz networks currently being deployed. For M2M the most used bands are the lowest frequency bands since they provide the best (reaching to indoor) coverage.

For many years M2M and IoT communication using cellular spectrum was based on GPRS technology. Currently (with the introduction of LTE networks in recent years and with the increased availability of cheap LTE chipsets) applications start to become LTE ready and capable of more efficient spectrum use (with modems being backwards compatible). However this kind of technology evolution is relatively slow considering the long life span of many M2M and IoT devices.

5.5.3 Spectrum for specific applications or use cases

For some applications specific spectrum is assigned. The advantage of dedicated spectrum for a specific application is that the risk of unwanted interference can be reduced.

However, spectrum allocated for specific application brings a large challenge in terms of spectrum efficiency and adds significantly to spectrum fragmentation.

5.9 GHz for ITS

In the case of Intelligent Transportation Systems (ITS), for instance for car to car communication, the 50 MHz (5.875 – 5.925 GHz) is assigned. The proposed protocol is 802.11p/WAVE, a slim version of 802.11 to reduce latency in car-to-car communication. Part of this band is specifically dedicated to critical ITS applications.

450 MHz for smart metering

In the Netherlands, a 450 MHz CDMA network is being deployed for smart meter readout and for future smart grid applications. This spectrum is not officially designated for this purpose and can potentially be used for other M2M applications next to smart-meter readout.

401-406 MHz for medical implants

Use of spectrum between 401-406 MHz, of which 402-405 MHz is harmonised and standardised[54] in large parts of the world, is reserved for (very) low power and low range medical implants use with the "Medical Implant Communication Service", MICS.

5.6 Summary

Various spectrum bands (both licence exempt and licenced) are used by IoT applications. This can be explained by a combination of practical, and technical reasons, as well as some historical and economic reasons. Many M2M and IoT devices have a life span of several years to decades, some bands are application specific, there are different bands for licensed and license free spectrum, and also the different operational scales (personal area, residential area, wide area) ideally require different radio spectrum for short range and wide range applications.

Licence exempt spectrum plays an important role in IoT, and various protocols described in this paragraph depend on licence exempt spectrum. Both the availability of high frequency spectrum (2.4 GHz, 5 GHz) as well as sub-GHz spectrum is vital. It allows manufacturers to create devices that operate and communicate autonomously (without third party connectivity provider) at a local (depending on the application) scale. The sub 1 GHz band (currently mainly the 868 MHz spectrum) is used for low power metropolitan networks (for example using LoRa, SigFox, or other, proprietary low power protocols). The availability of such a band is important for the advent of low power sensors on a street, large building, or city wide scale. The 2.4 GHz band is mainly used for local area networks, using Wi-Fi, and personal area networks, using for example Bluetooth. The availability of multiple options for license exempt spectrum use gives the opportunity to use the most 'fit for purpose' communication mode for a given application.

The spectrum for the public mobile (LTE and GPRS) networks plays a major role providing coverage for mobile devices and coverage outside the domain of the IoT application provider. This type of spectrum use also allows for detailed control over the network parameters by the mobile service providers, since this operator has exclusive usage rights for this spectrum. Mobile operators are planning to implement specific LTE feature for M2M to allow for low power usage ('cat 0 devices') in the coming years, with further enhancements being made up to 2022 with the possible introduction of further 'low power LTE' features aimed specific at low cost low energy devices. This might make LTE low power an attractive communication option for certain low power applications as well, competing with the current low power metropolitan networks that use license free spectrum, giving IoT service providers a choice of network technology.

[54] www.etsi.org/deliver/etsi_en/301800_301899/30183901/01.03.01_60/en_30183901v010301p.pdf

6 Spectrum policy and the Internet of Things

This chapter gives an overview of lessons learned in other countries that have researched possible impact of Internet of Things applications on radio spectrum policy or already changed or introduced spectrum policy specifically with IoT in mind. This chapter provides a description of spectrum policy solutions and an overview of how other countries facilitate IoT in their spectrum policy.

6.1 Policy of the European Commission

EU spectrum policy regarding short range devices is defined according to the 2006/771/EC decision [13]. The EU has given the CEPT a mandate to investigate the European short range situation in order to make changed in this decision. The last time was in 2013 and the goal of the update was *"…widening the scope of the Decision with least constraining usage conditions and allow for as much flexibility as possible for manufacturers and users."* [14]

The update resulted in changing the definition of some application categories like road transport and traffic telematics, adding new categories like active medical implants, and changing the frequency regimes of several bands from *non-specific* to more specific bands, like 401-406 MHz band for medical implants. The implementation deadline for member states was set on 1st of July 2014 [15].

CEPT has compiled a recommendation document for the member states in May 2015 [17]. They observe that most IoT applications make use of spectrum in the category "non-specific short range devices". Especially, the 868 MHz ISM band is commonly used (as is the case in the Netherlands), and is likely to be used even more in the following years. CEPT has identified two spectrum issues regarding to this band, both regarding adjacent high power bands due to probably GSM and LTE bands in several member states:

"The adjacent frequency bands below 862 MHz and above 870 MHz may be used by high power systems. Manufacturers should take this into account in the design of equipment and choice of power levels."

"The adjacent frequency bands below 915 MHz and above 876 MHz as well as 921 MHz may be used by high power systems. Manufacturers should take this into account in the design of equipment and choice of power levels."

The CEPT recognises the need to keep the 868 MHz frequency, due to all installed devices in this band, since *"otherwise the performance, reliability and functionality may decrease significantly due to competition with other applications in the same band which generates a less reliable, less predictable spectrum environment."*[18].

At this moment the CEPT [19] is considering M2M spectrum possibilities in the 700 MHz band. Specifically the 733-736 MHz / 788-791 MHz band, which is 2x3 MHz duplex gap in this band that is considered internationally suitable for M2M and was proposed in the APT band plan[55] for this purpose. The decision is not yet approved.

CEPT [16] investigates the possibilities for designating the 5.725-5.875 MHz band to wireless industrial applications and looks into compatibility issues with existing applications working in this band such as non-specific short range devices (for example alarms and wireless CCTV camera's, video electronics for both professional and consumer markets) and a number of other specific applications (satellite and fixed broadband wireless access).

6.2 United Kingdom

Ofcom has carried out several consultations and studies regarding short range devices, M2M and IoT starting in 2014 with a consultation for the 870-876 MHz band and the 915-921 MHz band [20][21] and ending in a consultation statement *Promoting investment and innovation in the Internet of Things* in January 2015 [22][23]. The consultation in 2014 was based on the recommendations of the CEPT report 189 with the intention to make the 870-876 MHz band and the 915-921 MHz band available for short range devices (see chapter 5 for the situation in the Netherlands). This resulted in both bands being made available in the UK. Ofcom concludes that this current initiative is sufficient for the short to medium term.

Ofcom is currently exploring possibilities to make spectrum available between 55 and 68 MHz band and possibilities for liberalising license conditions for mobile spectrum to support IoT. However, Ofcom recognises that on the long term, as the IoT sector develops, more spectrum might be needed in the future, and therefore they will continue to monitor IoT spectrum use, especially in the license exempt bands to help identify new needs for spectrum. Other bands (next to the once mentioned above) that might be suitable for IoT applications and can play a role in the future are a subset of license exempt bands, a subset of bands that are used for business radio, or (TV) white spaces between 470 to 790 MHz band could be suitable for IoT [22].

6.3 Germany

Germany has commissioned a study "Channel Access Rules for SRDs" on the coexistence of SRD applications [24] and is now contemplating actions. The main conclusions and recommendations of this research were 1) that in most cases the available bandwidth for SRD applications is sufficient and 2) that *"a significant part of SRD applications will be single-carrier systems due to cost and complexity limitations"*. Furthermore, 3) SRD applications that require low latency and high reliability (like industrial automation) cannot efficiently be operated in coexistence with applications that use random access schemes. Therefore the SRD band should in the case of low latency and high reliability applications only be used in the protected areas or use high data rate standards with guaranteed access, and 4), that there might be a need for a small exclusive portion of spectrum to very sensitive applications (like special alarms) since there is no guarantee of use in the ISM bands. The most recent version of the available spectrum for SRD use is published in 2014 [25]. Recently (May

[55] http://ec.europa.eu/DocsRoom/documents/8270/attachments/1/translations/en/renditions/native and http://stakeholders.ofcom.org.uk/binaries/consultations/iot/responses/Qualcomm.pdf

2015) Germany has auctioned the 700 MHz, 900 MHz, 1800 MHz and 1.5 GHz spectrum[56] to cope with growth of demand for mobile.

6.4 United States

The FCC (Federal Communications Commission) has a technology advisory working group dedicated convened to research the impact of IoT on communication networks and came with recommendations in December 2014 [26][27][28]. Regarding to spectrum, the main findings of this research were that the rate of demand of spectrum of short range devices can be met under certain conditions:

- the FCC continues to encourages the use of spectral efficiency and increase the availability of spectrum for PAN/LAN networks on a *timely basis*
- that industry adopts spectrum efficient technologies for IoT
- that the upstream links of smartphones, PC's and tablets (which are used as proxy's/gateways) will continue to grow
- the rate of deployment of small cell technology continues
- they high throughput rate (video streams) is offloaded close to the device

The main concern is that IoT growth can only be facilitated if short-range spectrum availability remains well ahead of the demand. Further, connectivity in rural areas (where there is less availability of wireless and fixed broadband than in the rest of the country) may need special attention of the commission.

Furthermore, according to the group, there is no unique allocation of spectrum for IoT required, however, the FCC should periodically examine its spectrum policy to ensure sufficient short-range spectrum, and accommodate the growth of upstream links of the proxies in wide area networks. The periodic analysis and the FCC plans should be concrete and timely communicated with the industry to guide industry planning related to IoT.

The workgroup links the stimulation of growth of IoT to the availability of unlicensed spectrum that is suitable for PAN/LAN range services (not limited to IoT).

To stimulate IoT growth, the FCC should focus on the availability of unlicensed spectrum suitable to a range of PAN/LAN services (including, but not limited to IoT).

The FCC has already broad legislation[29] for unlicensed spectrum, but is now taken actions to set up a future roadmap for unlicensed services by forming a workgroup in April 2015 to study this issue[30].

The FCC has recognised the necessity to take other IoT related actions next to spectrum issues [31], like broadband availability in rural areas and net neutrality legislation [32].

[56] Bundesnetzagentur website – Project 2016, Az:BK1-11/003

6.5 Other countries

Finland

In Finland, the government has conducted a research to investigate Industrial Internet, which indirectly refers to IoT[57]. The main conclusions of this report include measures to stimulate the use of industrial internet like using 5% of all public procurement on alternatives advances the industrial internet.

France

The French ministry of Economic Affairs has announced an industrial plan to integrate the Internet of Things as a sector in the French industrial landscape.

"The plan is designed to make sure the IoT is deeply integrated in the broader industrial landscape, which requires a common understanding and industry-let standards. In order to do so, around 200 stakeholders have been included in the making of the Plan.[58]"

The ministry recognises the importance of the IoT for their economy, in the industrial plan, a potential of 80 billion connected devices in 2020 is given. They recognise that there are some technical difficulties that need to be overcome in order to reach the 80 billion connected devices[59]. There is however no specific actions taken to counter these technical difficulties are.

Italy

The Italian communication authority (AgCom) has conducted an M2M consultation[60] and issued a report IoT[61]. Connected Cars and the Smart home sector are identified as the sectors with the greatest increase and revenue potential for Italy the following three years. Also, AgCom recognises the difference of the character of telecom for IoT services compared to other telecommunication services. AgCom has concluded that adjusting the regulatory regime will be necessary in order to facilitate this market.

One issue of attention is the lack of standardisation (higher level standardisation is needed to ensure that different devices are able to communicate with each other).

Regarding spectrum a main issue is the licensing regime, which is suitable for telecom companies, but not aimed at typical M2M operators, car companies or utilities. Moreover, the nature of IoT and M2M requires simplification of notification obligations to authorities. Agcom further concludes that new authorisation regimes may be needed to ensure that shared usage of spectrum happens in a more flexible and efficient way.

[57] http://valtioneuvosto.fi/artikkeli/-/asset_publisher/tutkimus-suomesta-teollisen-internetin-piilaakso?_101_INSTANCE_3wyslLo1Z0ni_groupId=10616&_101_INSTANCE_3wyslLo1Z0ni_languageId=en_US

[58] http://www.rudebaguette.com/2014/06/19/axelle-lemaire-announced-industrial-plan-connected-objects-made-france/

[59] http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/17608.pdf#page=13

[60] http://blogs.dlapiper.com/iptitaly/?p=56644

[61] http://www.technologyslegaledge.com/2015/04/16/the-iot-scrutinized-by-telecom-regulator/

Regarding the use of mobile networks for IoT applications also some issues are identified: One issue is that many current M2M devices use 2G networks, and shutting down the 2G network might affect already installed M2M and IoT.

Another is the need to prevent lock-in with the telecom operator. Regulations must be adjusted to ensure switching providers is relatively easy, even in this market. Cyber security and privacy of individuals are a priority for the Italian regulator, but the security standards should not be too costly to avoid potential barriers to enter the IoT market.

6.5.1 East-Asia

Other countries have initiated or stimulated IoT initiatives and developments in several ways. An example is South Korea's Songdo[62], which claims to be the first 'smart city' in the world. It was recently built from scratch (2012-2015), but the IoT features are not fully utilised yet, because the number of residents is still limited.

In Japan, the very high quality infrastructure and resident's high use of smartphones are both enablers of IoT. ITS (Intelligent Transport Systems) is being introduced in a number of ways. To improve broadband communication for safety reasons and for tourism, the Japanese radio department wants to make Wi-Fi available for the public in and around government buildings like city halls and museums and other national establishments like national parks and monuments[63].

6.6 Policy trends and lessons learned

General issues and concerns

In the countries discussed, the available spectrum for IoT use is generally regarded sufficient at this moment. However, sufficient spectrum to cope with the growth of IoT in the future is a shared concern.

Some countries consider that an adjustment of spectrum licenses might be necessary in the future to make such licenses also suitable for other parties than the traditional mobile network operators.

Also some countries consider that spectrum sharing in ISM bands may leads to a related possible need for additional rules or etiquette in these bands. For example, there might be a need for a small exclusive portion of spectrum to very sensitive applications since there is no guarantee of use in the ISM bands.

Most sources conclude that international harmonisation is needed to ensure economies of scale.

CEPT sees chances for partial harmonisation of the 915-921 MHz spectrum, and the UK has taken steps towards making this spectrum available for IoT.

[62] http://www.theguardian.com/cities/2014/dec/22/songdo-south-korea-world-first-smart-city-in-pictures

[63] http://www.ptc.org/images/pdf/SF/2014/Iida-Development-of-Mobile-Broadband-and-Spectrum-Policy-Vision.pdf

General observations regarding international spectrum policy

IoT related policy research of the countries that were investigated cover the use of license exempt as well as licensed spectrum. It becomes clear that both public mobile networks and autonomous networks or communication in licence exempt spectrum play a role in IoT. The availability of interference-free license exempt spectrum is an area of concern in a number of countries.

For license exempt spectrum the following generalised observations can be made:

- Short range spectrum, co-existence and sharing of unlicensed spectrum are important topics. A number of countries have commissioned research regarding spectrum use by short range devices, M2M or IoT recently. This indicates a growing international awareness of IoT.
- Specific spectrum policies related to IoT are taken by the following countries:
    - UK made the 870-876 MHz band and the 915-921 MHz available for license free use, according to the CEPT recommendations
    - US acknowledges that license free spectrum is important for growth of IoT and will have the guard bands of the 600 MHz available for license free use

  The CEPT is recently considering the 733-736 MHz /788-791 MHz band for international harmonisation for M2M.For licensed spectrum, mainly used by public mobile networks, some reports point out the need to prevent lock-in with the telecom operator and to reduce bottlenecks for switching between operators.

For the Netherlands, it seems similarly important to look for possible additional spectrum for IoT and short range devices. The 915-921 MHz band possibly allows for a widely harmonised band for IoT (See Spectrum bands) it is interesting to consider the possibilities for use of this 915 MHz spectrum for IoT in the Netherlands.

The potential need for a specialised band for critical applications is observed in some countries. This is also considered a potential issue for future critical applications in the Netherlands (as described in chapter 3), and is an interesting notion that might need further exploration.

7 Analysis

Based on the overviews of application areas and applications, technology, radio spectrum and spectrum policies in the chapters 3 to 6, this chapter describes a combined analysis of the outlook regarding connectivity need of applications in general (paragraph 7.1), determining situations in which a combination of applications and devices may lead to potential spectrum bottlenecks (paragraph 7.2), and possible spectrum implications that may occur in these situations (paragraph 7.3). Furthermore, in paragraph 7.4 a general analysis is given of stakeholders that are related to IoT applications, and their roles and relations. The spectrum memo of 2005 is then discussed from today's perspective in paragraph 7.5, and potential monitoring and enforcement issues are discussed in paragraph 7.6.

7.1 Connectivity needs of future applications

7.1.1 Ubiquitous connectivity

Chapters 3 and 5 illustrate that the availability of cheap and easy implementable connectivity options are vital for the advancement of IoT developments. Communication needs vary between applications (see chapter 3), and various protocols are used in the various available spectrum bands (see chapter 4 and 5). To accommodate the variety of applications and operational scales, there should be a variety of communication technologies available for IoT in order to accommodate the various demands and to ensure real 'ubiquitous connectivity'. Competition between technologies and frequency bands will create an incentive for the market to strive to deliver the most efficient way of communication. Both competition between technologies and competition between networks (operator controlled vs end user-controlled local networks) will add to the choices that IoT manufacturers have. The availability of a variety of communication technologies and options is an advantage since it allows for choosing the solution that is 'most fit for purpose'.

In order to facilitate innovation and development in the field of the 'Internet of Things' from a spectrum point of view, the various types of communication need to be available as a choice for developers. This allows them to either use an existing technology that they deem right, or develop a new technology for a specific spectrum band if needed.

7.1.2 Coverage and availability

For a number of applications described in chapter 3, coverage and availability is, or may become, an important factor.

Coverage plays a role in many applications. For example, home automation the ZigBee gateway should be able to communicate to devices throughout the building. If the application uses a local network in shared spectrum, the network is often under control of the user who can choose to add access points if needed. Interference from the network of the neighbours or from some other network using the same shared spectrum can cause problems in terms of the availability of the communication service.

In case shared licence exempt spectrum is used, the user is itself has only limited possibilities to enforce availability since others are allowed to use the spectrum at the same time.

In case of public mobile networks, the operator is responsible for providing the coverage. Since operators of for example GPRS and LTE networks have a licence for a specific spectrum band they can exercise control over network density and the amount of users. If applications cross country borders, the possibility of roaming is an important differentiator of public mobile macro networks. For example, e-Call relies on those networks to give accurate location information about incidents. In rural areas, where there might be no bystanders, lack of coverage might potentially pose a problem for those accidents happening outside network coverage. Also, e-call should function throughout the EU, making EU-wide roaming vital.

In both cases, using either public networks or local networks, the dependency might grow over time: once people are used to the fact that some system works, processes might be adapted to reflect the new situation, while being unaware of the possible negative implications of the network being unavailable.

7.1.3 Amount of data traffic

IoT devices generally communicate only small bursts of information, but, as discussed in paragraph 4.2, both for individual devices as for accumulated traffic, the amount of data and the related use of radio spectrum can vary considerably.

The total load on the spectrum depends both on the amount of data per communication moment and how often this takes place. This in itself depends on the application, number of devices involved, the used data formats and protocols, and on other ‘overhead’ factors[64].

Although the relevant information that is exchanged is often relatively small (sometimes only a few hundred bytes), and communication is in many cases sporadically, there is a trend that both payload and communication frequency increases over time because functionality and complexity increases with updates and added features.

7.2 Determining potential spectrum bottleneck situations

Even if each individual device does not necessarily use much data or spectrum, the large number of IoT devices that share the same spectrum bands with each other and with other non-IoT applications potentially cause issues[65].

To estimate the impact on spectrum load, the main importance is to define situations when and where many devices that may compete for the same type of spectrum are likely to be found, and then assess possible ‘worst case’ scenarios with regard to traffic exchange including overhead.

[64] Such as addresses of sender or receiver, encryption, and overhead in the communication protocols and procedure itself, for instance related to ‘keep alive’ signals, (de)registration of devices, acknowledgement procedures.

[65] Spectrum is often shared with other applications that do may use a large bandwidth like multimedia streams

Based on the observations on (numbers of) applications and devices described in paragraph 3, in this paragraph we sketch such a situation: a potential (busy) case in 2025 where many active devices compete for radio spectrum to cater their connectivity needs.

Although it is hard to predict exactly what protocols and which spectrum bands will be used, an estimate is made about the 'operational scale' of various applications, and the associated types of spectrum that may be used at such scales.

Roughly four operating scales can be distinguished that relate to the general use of applications and devices at a certain range: personal scale (for instance for wearables communicating with a personal gateway), local scale (for instance for home automation devices communication with a home gateway), metropolitan scale, and macro scale networks (for applications that need connectivity on a wide range, for example cars moving throughout the EU).

In general and from a technical perspective, these operating scales for which applications generally may compete for the same type of spectrum, are the most common fit for the application needs of the three different types of applications: personal, residential and metropolitan or macro operating applications. However there are many reasons why some applications or devices will not fit in this classification: economical or other strategical reasons may lead to other spectrum use. This is for instance comparable with the mobile user: in some cases, some users switch to Wi-Fi for data communication, where others still use the mobile connection even when Wi-Fi is available. An illustrative, more IoT related, example is the home Smart Meter. From a technical perspective one would predict it to have either a fixed connection or a Wi-Fi connection (with VPN security for a connection to the utility company) as most homes already have internet access, in practice tough, most Smart Meters use cellular technology to communicate.

Bottleneck Scenario: Urban area family home during peak hours (6-8 p.m.)

We assume a family household of four persons in a typical street (100 houses) in urban area, and sketch a possible scenario of connected IoT devices by 2025.

On a *personal scale* inhabitants are likely to have personal care devices in their network', like a number of sports and/or health monitors, smart scales or toothbrushes, or devices for toddlers (around 6-10 devices in total in the household), that communicate using some 'personal area network' technology to a personal 'gateway' (such as a smartphone).

Personal scale networks: Assuming an overlap of personal scale networks between only directly neighbouring houses (total of 3-6 houses), a total of between 30 and 60 devices might compete for the same spectrum.

On a *residential scale*, a connected home in 2025 might consist of both applications for home automation and healthcare related applications. An average of three connected appliances and five media-devices might be present. Regarding home automation, connected lighting systems will be present that control anywhere between 5 to 25 lights and an additional number of between 5–15 of other home-automation devices is likely to be present, for a total of connected devices in this household at a residential level in the order of 20-40. In general, they all connect and interact to a home automation gateway or similar device and/or with internet services.

Residential scale networks: Assuming an overlap of residential scale networks between 10-15 houses, a total of between 100 and 500 devices might compete for the same type of spectrum.

At a street level, on average there might be one connected car per two homes, adding additional wireless connections for car-management, e-call, and maybe charging-points depending on the uptake of electric-only cars (500-1500 connections per square kilometre). Other applications are the 'smart city' applications in your neighbourhood, including a number of sensors or actors/switches for controlling streetlights (400-700 per square kilometre). Other applications in the street that are likely to see further connectivity in the coming ten years are sensors for measuring fill levels of underground waste-containers, local energy, water and gas distribution points, measurements of sewage and water drainages levels (for another 50-400 connections per square kilometre). They most likely communicate via some metropolitan or macro scale network with ranges of hundreds of meters or more, either operator-owned or controlled by the municipality (using for example LTE or a low power technology like LoRa or SigFox).

Metropolitan or macro scale networks: Per square kilometre 1000 – 2600 connected devices might be present. Assuming a cell-size of 4 square kilometres, this could mean 4000 or more devices competing for the same type of spectrum at a metropolitan scale.

7.3 Spectrum implications

The previous paragraph describes that a large number of applications will compete for spectrum at the various operational scales. For all of the described operational scales it is to be expected that, in a decade time, the number of wireless communicating devices will grow enormously (estimates vary but growth in number of devices could be as large as tenfold or more compared to today). This will increase overall interference and generally increase background noise levels.

For communication at the personal area scale networks, often the 2.4 GHz ISM band is used. This means that those applications compete with many of the applications that operate on a residential scale using protocols like Wi-Fi and ZigBee. Next to this, the 2.4 GHz ISM band is already under increased pressure from the large success of Wi-Fi for local broadband networks for laptops, tablets and smartphones. From interviews conducted in this research project, it became clear devices already occasionally suffer from unwanted interference, and recent investigations [6] commissioned by Agentschap Telecom indicate that problems in this 2.4 GHz ISM band occur on a regular basis in crowded areas like an urban environment.

With the expected increase in applications competing for this spectrum, the problems are likely to rise and form a potential bottleneck for deployment. However, there are alternatives present, like the 5 GHz band for which devices are readily available, and 60 GHz. For the near future, shifting load from 2.4 GHz to those alternatives might be the easiest way forward.

Although many Personal Area applications use lower power transmission techniques covering smaller ranges than Residential Area applications, they co-exist with each other in the same spectrum bands (2.4 GHz, and alternatively 5 GHz) and in some cases cause unnecessary interference with each other. A discussion for a more efficient separation between spectrum aimed for very local personal scale use and spectrum aimed for residential use may be an option.

While for applications in for example vehicles using a macro network is an obvious choice, for many other (smart city) applications (specifically if power is not a constrained) both metropolitan or macro scale networks can be used, id est using either GPRS or LTE in for example the 800/900 MHz bands, or using a low power sensor technology such as LoRa or Sigfox in the 868 MHz range. For applications that need to operate on batteries for prolonged periods, using low power sensor network technology is most suited. Using the licence-exempt 868 MHz band is vital for providing such low power, larger area, easy to implement, technologies.

Some applications require specific types of networks, while others can ‘choose’ between a number of solutions. Apart from general aspects (such as costs, flexibility, robustness, quality, ease of use), choices are based on factors like a) country- or worldwide coverage, which is a strength of mobile networks, b) on power consumption, which is a strength of low power technologies in the 868 MHz band, and c) on autonomy and flexibility of people and organisations using IoT applications, which is a strength of those technologies that can be implemented and maintained by the IoT application developer or owner rather than with the involvement of a third party as an operator.

For those applications that require a macro network, coverage and availability of that network might be specifically important for critical application (like e-Call). Although coverage is relatively good in the Netherlands, in some rural areas coverage is less dense which poses a challenge for implementation of critical applications in rural areas.

For the operator-owned LTE networks, more spectrum will become available (in the 700 MHz range), and IoT traffic is only a small portion of the total LTE traffic. It is yet unclear whether developments such as LTE Low Power will lead to the need for additional LTE spectrum bands, or whether these solutions can be fitted in already allocated spectrum bands. GPRS and LTE are already an important technology for various types of M2M and IoT applications where power consumption is not the major constraint, and the introduction of low power LTE features by operators in the Netherlands will make LTE a candidate for very low power devices as well.

For many of the metropolitan scale networks, the continued availability of sub GHz spectrum is vital. However, it becomes clear that with the large number of expected devices on a street or metropolitan scale that might use 868 MHz spectrum, the pressure is likely to increase. Additionally, the number of networks operating in the same spectrum 868 MHz spectrum might put further strain in this band (for example, in the Netherlands this spectrum is used by a number of proprietary local applications, as well as SigFox, a city wide Lora network in Amsterdam, and plans from an operator to implement a LoRa network in this same spectrum.

In order to give metropolitan scale applications like those for smart cities or industrial plants the certainty of interference free usage of sub GHz spectrum, it is likely that additional similar spectrum might be needed in the intermediate term. This requires attention and monitoring of the uptake of devices and usage. There are a number of potential bands for use for IoT, and if possible the allocation of additional sub-GHz licence exempt, harmonised spectrum for IoT should be investigated and contemplated (for example the use of 3 MHz duplex gap in the 700 MHz LTE spectrum or the use of 915-921, as described in CEPT [18]).

7.4 Stakeholders

This paragraph describes a general analysis regarding stakeholders that relate to the uptake of wireless IoT applications. From the different application areas and technology areas that were mapped in this research a number of generalised stakeholder types are identified. These stakeholder types are used as a basis for a general analysis of stakeholder types and their roles and actions.

For this analysis the work of Mitchell et al. [21][7] is used, where three attributes are distinguished for analysis of stakeholder roles and their actions:

- *Power*, defined a as relationship between stakeholders where one stakeholder A can get another stakeholder B to do something that B would not have done otherwise;
- *Legitimacy*, defined as generalised perception that actions by a stakeholder are appropriate within a system of norms;
- *Urgency*, the degree to which stakeholder claims call for immediate attention.

Pressures from stakeholders are more successful if these stakeholders accumulate the attributes. Stakeholders with all three attributes ('definitive stakeholders') are considered most effective in getting their priorities accepted. The identifications 'Definitive stakeholder', 'Dominant stakeholder', 'Demanding Stakeholder', etc. in a stakeholder typology diagram (such as depicted in Figure 5) provide a description of likely or potential general behaviour of the stakeholder. Although it is not always possible to define the stakeholders on an equal level, the diagram gives an idea about the perception of the position of the relevant players, and can provide insight into their acts or can visually represent their perceived roles.

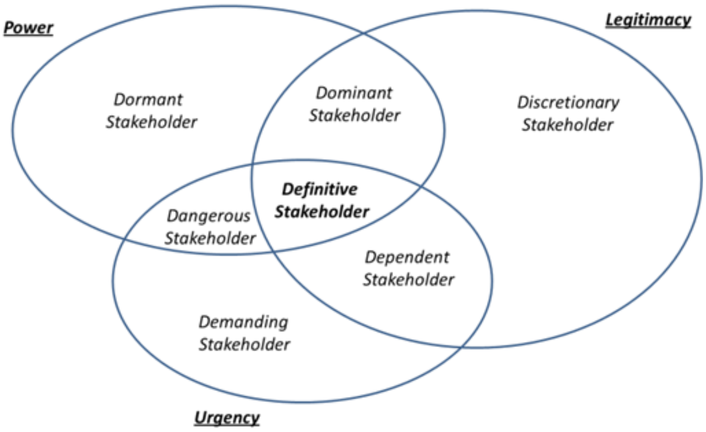


Figure 5: Stakeholder typology (from [21], p. 874)

For different application areas (described in chapter 3) a number of ‘general stakeholder types’ were identified that are similar for a majority of the cases. The generalised stakeholder types are summarised in Table 1 and discussed in more detail below. For each stakeholder type examples from different application areas are given.

Table 1: Stakeholder types related to 'Uptake of Efficient Wireless IoT Applications'

	Example	**Urgency**	**Power**	**Legitimacy**
End user	consumer, resident, citizen, patient, driver	comfort, costs, health benefit, security, flexibility and reliability	Limited: buying, using, choosing	Limited
IoT enhanced service provider	hospitals, car manufacturers, city parking, utility companies	costs, efficiency, improving or extending services	Limited: buying (services), offering (to end users)	Limited
Fixed connectivity provider	cable, fiber or DSL access provider		offer fixed and residential wireless connectivity. possible gateway functionality	
Mobile connectivity provider	LTE or other mobile network provider	Limited: business (subscriptions), network load & overhead	offering wireless connectivity and coverage	Limited: Licensed spectrum can be prioritised and allocated
Device or hardware manufacturer	chip, sensor and actuator manufacturers, gateway maker	Business	offering general & fit for purpose solutions	
Software developer or integrator	Operating system, internet platforms, application	Business	offering general & fit for purpose solutions	
Policy maker or regulator	AT, EZ, EC	limited, only indirect	in some cases: mandating use(eCall)	legislation and enforcement
Standards body or platform alliance	IEEE, 3GPP, ETSI	limited, via businesses	limited, only indirect	defining standard protocols etc.
IoT process certifier or financier	Insurance companies (health, car, home), equipment certification (incl. privacy, health)	in some cases, but only when 'best practice' can be clearly improved	power to mandate, delay, stop introduction	related to regulation and 'safety', 'fairness' and 'solidarity'

The **end user** can have different roles depending on the IoT application: a consumer, in case of consumer products, can have some *power* in choosing which type of product to use, but in many cases such as institutionalised health, connected car or utility applications, where end users have the role of resident, patient or driver, the end user has relatively low power. The *legitimacy* regarding this subject is limited to personal preferences regarding health, privacy and efficiency of home networks, but the implications of those subjects are not always clear to end users. However the *urgency* is in many cases relatively high: the end user in general is aware or convinced of the potential of added comfort, cost efficiency, health benefit, security, flexibility and reliability of IoT applications. In conclusion, because of this combination of lacking power and legitimacy, while having urgency, the end user is positioned as a so-called *Demanding Stakeholder* (see Figure 6).

The **IoT enhanced service provider** is a generalisation of stakeholders that are not the direct end users of IoT applications, but provide services or applications that are enhanced by IoT capabilities, such as car manufacturers, hospitals and care providers, but also utility companies introducing smart meters or governments introducing smart parking systems. The *urgency* for these stakeholders is related to minimising costs, optimising efficiency or improving or extending offered services or applications to end users. These stakeholders have some *power* regarding the uptake of efficient wireless IoT applications: for instance car manufacturers, utility companies and large hospitals can have a considerable impact, but many stakeholders in this category have relatively low power, and are followers dependent on what applications and technology solutions are available on the market. The *legitimacy* is relatively low and limited to specific considerations regarding for instance health risks in hospitals, and considerations regarding how the use of IoT relates to the general feature of the product or service offered. In conclusion, the IoT enhanced service provider can be positioned as a Demanding Stakeholder, but in some cases may be regarded as Dangerous Stakeholder, for instance in case when a high urgency and power to fulfil this urgency leads to less efficient and potentially illegal spectrum use.

A large part of the IoT applications uses personal range wireless networks or residential networks for communication with devices and gateways to fixed access. The **fixed connectivity provider** provides access via fibre, cable or DSL but in many cases also offers wireless residential facilities, for instance with a modem with Wi-Fi capabilities. The uptake of wireless IoT applications poses no immediate *urgency* for this kind of stakeholders: IoT traffic is still only a small part of the total traffic that they transport and distribute. A potential urgency that may occur in the future is addressing the issue of too many devices trying to register at a modem, and this is related to a possible *legitimacy* attribute. The attribute *power* is somewhat difficult to qualify: connectivity is essential for IoT applications and in most applications fixed access networks play a role, but the networks are already there. However the fact that most access providers own and control modems and set-top boxes in homes that may evolve to gateways is an important consideration. This may in the future for example happen for senior healthcare applications. In conclusion, by having power, but lacking legitimacy and the urgency to influence the uptake of IoT, the fixed connectivity provider is positioned as a Dormant Stakeholder.

For applications for which coverage and range is important the **mobile connectivity provider** plays a role and is a stakeholder. Has a limited *urgency*: IoT subscriptions are an emerging business, and may in some cases have limited impact on network load of data traffic and (maybe even more, overhead due to registration and firmware upgrade traffic), but IoT traffic represents only a part of the total and growing amount of data traffic. As countrywide, and – through roaming agreements – worldwide players these providers have *power* to introduce and efficiently deploy IoT applications in their networks. Due to licensing and control of the major parts of their network these stakeholders have a high degree of *legitimacy* in this matter. In conclusion, mobile connectivity providers have the power and the legitimately to influence the uptake of IoT, but lack the urgency, they therefore can be positioned as a Dominant Stakeholder.

One of the most prominent stakeholder types is the **device or hardware manufacturer**: producers of chips, sensors, actuators, gateways and other hardware components that form

IoT applications. Some applications use licensed wireless networks and related technology that are deployed by the mobile connectivity providers, use unlicensed wireless networks and fixed networks that are partly facilitated by fixed connectivity providers, or use specific network technologies in unlicensed bands such as the ISM bands. These stakeholders have a high *urgency,* related to the market potential of growing numbers of efficiently working IoT devices*.* Their *power* is considerable: efficiently use of radio spectrum to transport data is strongly related to the solution they provide. The *legitimacy* is an important factor: hardware has a relatively long life span and in a world market with a variety of spectrum policies these stakeholders try to optimise their market. However, the differences in licensing and spectrum policy pose a great challenge: although it is possible to produce cheap flexible hardware that can theoretically be used in many geographic areas, the licensing and enforcement rules of such hardware is in many cases regarded too complex. In conclusion, by combining all three attributes, the device and hardware manufacturer is positioned as a Definitive Stakeholder, although in some cases this stakeholder may be regarded as a Dangerous Stakeholder.

A strongly related stakeholder type is the **software developer or integrator**, and the attributes *urgency*, *power* and *legitimacy* can be generally regarded as similar to those of the device or hardware manufacturer. However software is much more volatile than hardware in the sense that the life span is shorter, it is more diverse, certification is more difficult and software has the tendency to pragmatically (over)use resources. Already mentioned is the fact that software updates of IoT firmware or software may contribute to a significant part of IoT traffic. In conclusion the software developer or integrator is positioned as a Dangerous Stakeholder.

Policy makers or regulators, government administrations such as the Radiocommunication Agency of the Ministry of Economic Affairs, other radio spectrum regulators such as OFCOM and FCC, and local, provincial, country or EC governments in general form another stakeholder type. The *urgency* attribute is relatively low and indirect: the IoT hype starts to raise interest of governments, but a real sense of urgency will only be generated indirectly, when problems arise, or the market or citizens demand action. *Power* in improving the uptake of efficient wireless IoT applications is a low and indirect attribute. Exceptions are when government administrations are large users of IoT technology (but then they can be regarded as another stakeholder type, IoT enhanced service provider or End user), or when government administrations mandate, strongly promote or enforce the use of IoT. Examples are mandatory introduction of eCall, and in some countries Smart Metering or Road Pricing technologies. The *legitimacy* is obviously an important attribute for this type of stakeholder. In conclusion, the policy maker or regulator is positioned as a Discretionary Stakeholder in case of spectrum policy and allocation, and as a Dormant Stakeholder when mandating IoT use.

Another stakeholder type is the **standards body or platform alliance**, such as IEEE, the ZigBee Alliance and ETSI. In general, *urgency* regarding this subject can be regarded high, but because these are often fragile alliances between different companies and/or governmental organisations, this is not always brought into effect: standards may lead to increasing business for the community as a whole and promoting common interests, but not always for the business and interests of all separate parties and this generally means standardisation processes are slow and tedious. The *power* is limited: defining a standard does not imply that the standard will automatically be widely adopted. The most prominent attribute of this stakeholder type is *legitimacy*. By having legitimacy and sometimes urgency as well the standards body or platform alliances is positioned as a Dependent Stakeholder, but can in some cases also be regarded as a Discretionary Stakeholder.

A final stakeholder type that we consider is the **IoT process certifier or financier.** This category of stakeholders is involved in the introduction of technology in products, services or processes and has a decisive or strongly advising role in this introduction. Examples are insurance companies for healthcare, cars (accidents) or houses (burglary, fire), but also certification organisations related to health and quality requirements, etcetera. These stakeholders have a limited *urgency* regarding the introduction of efficient wireless IoT applications. Only when it is clear that 'best practices' can clearly be improved there will be urgency for adoption. However these organisations in many cases have the *power* to mandate, delay or stop introduction new applications, and have the *legitimacy* to do so. In conclusion, in the IoT process certifier or financier is positioned as a Dominant Stakeholder, and may in some cases be regarded as a Definitive Stakeholder.

Summary and general observations

Figure 6 shows the stakeholders and an illustration of their possible position in terms of power, legitimacy and urgency with respect of the uptake of efficient wireless IoT applications for the generalised situation.

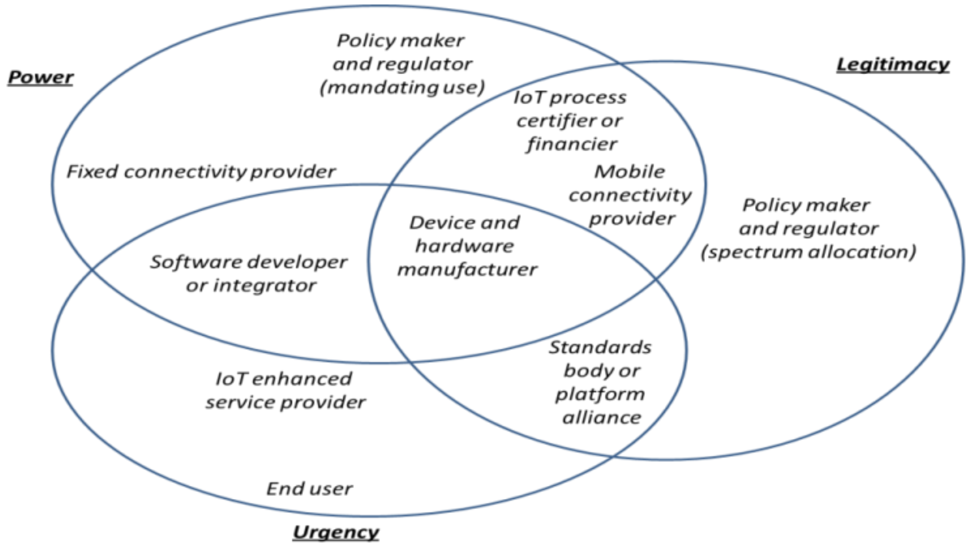

Power
Policy maker and regulator (mandating use)
Legitimacy
IoT process certifier or financier
Fixed connectivity provider
Mobile connectivity provider
Policy maker and regulator (spectrum allocation)
Device and hardware manufacturer
Software developer or integrator
Standards body or platform alliance
IoT enhanced service provider
End user
Urgency

Figure 6: Illustration of stakeholder types related to 'Uptake of Wireless IoT Applications' in typology of Mitchell et al.

A number of observations can be made:

The device and hardware manufacturers often play an important role and have the combination of power, urgency and legitimacy and they, in some cases together with software developers and integrators, contribute most significantly to the uptake of efficient wireless IoT applications (and can therefore be characterised as 'definitive stakeholders').

The IoT enhanced service providers generally have more power than individual end users, but often lack legitimacy, and also (in exceptional cases) sometimes do not yet see the urgency, for instance because the life span of their product and the relative modest place IoT enhanced functionality has in the total product or service.

For manufacturers, developers and service providers, and even end users there is a risk that they bypass the (perceived) *legitimacy* if for some reason they feel the 'urgency' to act and the power is there. This can backfire, since in the end certain products might not be accepted. The combination of awareness, (preferably worldwide harmonised) regulation and enforcement should avoid this.

For connectivity providers, the IoT traffic is relatively unimportant when compared to other traffic, and fixed connectivity providers do not (yet) have a need or possibility to very much control spectrum use as they generally only use unlicensed spectrum. However, IoT will become more important, both businesswise as an opportunity to provide new services, and technically (using more network resources, addressing resources, etcetera). One other challenge is to move the IoT process certifier or financier (such as insurance companies) into an urgent position by clear that IoT application can increase (cost) efficiency.

For policy makers and regulators it is important to be aware of the (differences in) urgency of stakeholders and their power to introduce certain new solutions. In some cases a policy maker or regulator can increase its power to influence IoT trends by mandating certain use of applications, or to facilitate IoT certifiers or financiers and/or standards bodies to move towards the position of 'definitive stakeholder'.

7.5 Spectrum policy memo 2005 from today's perspective

In the spectrum policy memo (Nota Frequentiebeleid) of 2005[8], on which current spectrum implementation in the Netherlands was based, there is specific preference for the use of license exempt spectrum and the objective to lower barriers for usage. Already in 2005 it was expected that there would be a strong increase in the demand for license exempt spectrum and that the allocation of additional frequency space could be a possible solution if this demand keeps growing.

Although the most visible usage of this licence exempt spectrum was (is) the wide availability of high bandwidth local networks using Wi-Fi, such license exempt spectrum also plays a vital role in the current M2M and IoT evolution: As stated before, the availability of spectrum to use without the need of a (third party) contract or without the need for a licencing procedure allows for large numbers of small devices to be sold and operated. In the light of the memo 2005, this means the policy of creating license exempt spectrum with low practical barriers for usage as stated in 2005 should be extended with IoT in mind.

In the memo, the starting point is that spectrum *"should be license exempt"* if it is "*not scarce".* The license exempt spectrum is a key ingredient for the development of IoT. However, scarcity is a relative notion, and the question is what to do if the spectrum (available for IoT) becomes scarce due to an uptake of usage in a specific band, and the allocation of additional frequency space is not possible, another solution that is mentioned in the memo is the introduction of licenses or registration. However, for many of the IoT applications, this will significantly increase the barriers for implementation. The need to have simple to use and to implement spectrum is of such importance for IoT that in case of scarcity in certain bands, and if no similar bands are available, where possible freeing additional (harmonised) spectrum might be the better option.

The memo was written in a time when the importance of IoT applications was still relatively low, although applications such as remote controls and garage door openers are used as examples. One of the possible future areas for discussion is the potential use of (harmonised) dedicated license free frequency space for general critical IoT applications.

The memo mentions related areas where ICT and spectrum come together, regarding the safeguarding of security and transparency, and points to the need for government attention for issues like *"privacy, authentication, safe internet, and avoiding misuse".* The memo 2005 was likely reflecting on internet applications in general, but attention for those issues needs to be extended for the "internet of things", since the effects that the internet of things can have on those issues like privacy are likely to be even more invisible than the effects on privacy of the current regular internet use.

Policy enforcement is an important aspect of the nota 2005, in which it is mentioned that research into acceptable levels of interference for specific applications is needed. We see that 'things' in the Internet of Things communicate at various distances and powers, often in the same frequency band. The application using the highest power and making most use of the band is more likely to cause interference then a low power, low duty cycle application in that same band. The question of acceptable interference levels for specific applications stays, as addressed in the Nota, an important aspect for IoT in the coming years. The quickly changing landscape of types of devices and the number of devices, and the protocols they use, make it hard to follow up on actual interference hotspots. Modelling of potential interference situations using risk analysis combined with practical information (i.e. measurements where possible) can become key to play a proactive role.

7.6 Monitoring and enforcement

For monitoring and enforcement the increase in overall interference and background noise levels, caused by a larger number of devices being used will pose a challenge: combined regular use of all these devices may in some cases cause problems, but also the potential improper or unauthorised use of some of these devices.

Monitoring of spectrum use and early detection of bottlenecks is important tool for adequate enforcement and for spectrum policy updates to ensure long term interference free use of spectrum. In the case of license exempt spectrum, a heavily used frequency band can cause congestion and degradation of the services using that band, even if all players adhere to the rules. Especially for IoT, where license exempt spectrum is used by many devices and the spectrum is also shared with bandwidth-heavy applications (for instance Wi-Fi connections consuming large parts of the locally available radio spectrum): this might cause additional challenges. Monitoring of possible congestion is important to estimate risks of usage of certain bands and to be able to anticipate and timely implement changes in policy or enforcement as adequate counter measures.

The number of devices that travel outside their primary targeted use area is likely to increase. This makes monitoring and enforcement more difficult, since a wide variety of devices might often adhere to other or deviating standards than should be (for example due to other power limits or other spectrum use in the country of production or original use). It will be especially more difficult to enforce regional restrictions for (small and omnipresent) consumer equipment that is likely to travel with travelling persons or can be easily ordered online in other countries. For users it is increasingly difficult to know where and when devices that he or she uses[66] are legal or illegal. This implies that the role of the regulator might (need to) shift towards earlier phases in the manufacturing process. Following and steering worldwide standardisation and harmonisation of spectrum-use where possible might become more important. Also the way spectrum monitoring plays a role in this may change as it has to take into account the increasing number and variety of devices that do potentially not adhere to local standards.

Spectrum scarcity may vary greatly in location and time, and due to diversity of applications, devices and applications the spectrum impact is very difficult to predict. Early prediction and detection of potential bottleneck situations is needed, for instance using models and risk-assessments of potential congested areas to determine the best locations for monitoring of congested situations.

In some cases creating awareness and attention of the main stakeholders involved can already help a great deal: by pointing out where potential bottlenecks may occur in a few years, parties can anticipate and timely adapt by optimising parameters under their control such as network configurations, application settings, organisational dependency on applications and availability of back up connectivity options.

[66] Also, users might not even be aware of all communications once these devices become seemingly ‘insignificant’ parts of day to day products or objects that are transported, carried, bought, used, etc.

8 Conclusions and Recommendations

The 'Internet of Things' consists of many applications that use wired and wireless connections to and between an enormous amount of devices and objects. Many new products are under development, and even more are being considered for the future. They form a large and extremely diverse group of applications. The common factor is that it involves some kind of sensors and/or actors that collect data and do something useful with this data. Already emerging application fields for IoT include home automation, automotive, personal care and assisted living. Short life cycles and cheap and low power sensors actuators and processors, will further drive the use of those applications. Other application areas such as institutional health care, industry and manufacturing, smart cities and agriculture show growth, but for these areas adoption seems slower yet.

General trends

One characteristic of some of the successful applications appears to be that they are introduced 'bottom up' as stand-alone products, rather than 'top down'. This points to the fact that introduction of IoT is less easy in cases that involve multiple stakeholders, large scale deployment, or strict testing and certification conditions. An example for this is the area of *health applications,* where consumers use all kinds of sleep monitors and fitness trackers, but where a top down approach in hospitals requires rigorous testing and strict regulations.

Internet of Things devices operate and communicate with each other at different scales depending on their purpose and design. We can distinguish 'personal area network' (personal devices connecting very locally), 'wireless local area networks' on scales up to tens of meters, 'metropolitan scale networks' with a reach of hundreds of meters up to kilometres, and wide area macro networks, for countrywide or even worldwide communication. Apart from the availability of cheap, low power devices, the success of IoT largely depends on the fact that data communication *on those various scales* is easy to implement and widely available. This availability of 'ubiquitous communication' options at various levels forms an important driver of IoT since it offers the ability to use the most suited and fit for purpose form of communication. Policy should (continue to) aim to lower barriers of use for a multitude of communication options at the various scales to facilitate innovation and development of IoT.

Worldwide market

The market for IoT devices and solutions is a worldwide market. This creates opportunities for Dutch companies, but it also means that competition is worldwide, and gadgets and other devices can be ordered from worldwide competitors via Internet. In order to facilitate such a market, harmonisation of spectrum policy is key, since it allows manufacturing of devices that can be utilised and shipped on a worldwide scale. Also, the other way around, personal devices will be carried around the world and – when harmonisation is insufficient - might cause unwanted interference in regions with other spectrum designations.

Recommendation: Additional spectrum for IoT will need to be harmonised preferably worldwide, but at least at a European level.

Growing dependency

The introduction of IoT may start as ‘nice to have’ implementation of simple sensors that give the IoT operator better insight. However, over time the importance of this real-time information might grow, increasing the dependency on IoT and on communication.

Recommendation: Awareness of the increased dependency on real-time information, and thus of the dependency on telecom and spectrum usage, should be raised.

Standardisation

At this moment, applications in IoT mostly form distinct, standalone ecosystems or economically and technically isolated ‘islands’. In practice this means each application or application area has its own protocols and platforms. There are a multitude of standardisation efforts, but in most areas no definite standards have yet emerged. This makes future interoperability hard to predict. This forms a bottleneck for large scale introduction of IoT, especially for systems with longer life spans. However, this is typical for the current state of development in which IoT is attracting attention from many parties. It is likely that market standards will become less diverse and consolidate in the coming years, and efforts to create open industrywide standards are being made.

Recommendation: Follow standardisation trends to detect possible impact on spectrum policy. Consider facilitating discussion between Dutch companies on goals of IoT standardisation and exchange of information about standards involvement.

Connectivity and spectrum use

Various network technologies and providers can play a role at each of the ‘operational scales’ mentioned above. The larger scale networks could in principle provide the connectivity of devices that operate at a smaller scale, but this is not always the most practical or efficient way. As a rule of thumb, to achieve the most efficient use of radio spectrum the ‘communication scale’ of networks used should match the operational scale of the IoT devices, but spectrum efficiency is often no or only a minor consideration in this matter. Some existing congestion and interference problems in residential areas or companies can be solved using better network planning and configuration.

Recommendation: Increase awareness on efficient spectrum use of applications and devices and promote fair and efficient spectrum use.

Wide area macro networks

Wide area networks, primarily consisting of operator owned public mobile GPRS and LTE networks in licenced spectrum, play a major role in providing connectivity at a macro scale with even worldwide coverage. Apart from wide area coverage, an advantage is that the network and spectrum is under administration of an operator, allowing for control of network density, usage levels, and quality of availability and service. Those networks are used both for mobile objects (vehicles or equipment that are moved around), and for objects of a single party scattered on locations over large areas (such as garbage containers or vending machines), giving the IoT application operator connectivity to its devices without the need to worry about local network details. The currently deployed version of LTE is less suited for very low power applications, but a specific low power version of LTE is under development.

Point of attention: Coverage and availability of the networks might play an even more important role in the future once more applications depend on them. Especially in rural areas (indoor) coverage might pose additional challenges for some applications.

Metropolitan area networks

For applications on a metropolitan scale, both licence exempt spectrum (mainly 868 MHz) and licenced spectrum (either locally or countrywide) can play a role, and both local networks under control of the IoT service provider and operator networks are used.

The 868 MHz licence exempt spectrum band is used for low power metropolitan area networks (as well as networks for number of building automation), creating local networks of one or more cells, each with a diameter of typically 1 km. This network can be under the control of the application operator, giving autonomy of use and removing the need for a third party communication provider. Continued and undisturbed availability of such sub-1 GHz spectrum is vital for the further growth of Internet of Things on a ‘smart city’ scale. At this stage the available spectrum is still relatively free from interference. However, it is expected that there will be a significant uptake in usage of this spectrum in the coming years. This will probably raise the amount of interference. Additional spectrum in the sub-1GHz band could solve this. One option is the 915-921 MHz spectrum since this gives the possibility for a more wide harmonised band. The UK has recently announced it will make this spectrum available In the Netherlands this spectrum is currently designated for military use. Other options include spectrum in the 700 MHz range.

Recommendation: Closely monitor the uptake of usage in the sub-1 GHz licence exempt spectrum, and look for other spectrum for licence exempt use in this range.

Personal and local area networks

In both *personal area networks* and *local area networks* license exempt spectrum, and especially the 2.4 GHz ISM band, is widely used for IoT (for example by Wi-Fi, ZigBee, and Bluetooth). Next to this both 868 MHz and 434 MHz are used for a number of applications.

It is clear that the 2.4 GHz spectrum is already crowded (due to the large success of Wi-Fi for local wireless broadband). Increase in use is expected to put further strain on this band, which can impact the usability for IoT. Attention for this is needed in the near future. Some stakeholders warn of possible future interference due to the (now largely unused) neighbouring LTE TDD band. Separating PAN and WAN area networks can be thought of, however, this might be difficult in practice since the areas of use overlap. Using the 5 GHz ISM band is an important alternative, both for IoT itself and as a means to reduce the pressure on the 2.4 GHz band. There are developments to use the 60 GHz band for (in-room) local communication. Preferably, those alternatives are used for further growth of IoT applications in the personal and local area networks. One course of action is to move broadband traffic to the 5 GHz band (as is current policy).

Recommendation: Monitor the use of 2.4 GHz spectrum and (continue to) bring alternatives like the 5 GHz band for personal and local area networks under attention in order to shift part of the load there.

Critical Applications

Critical applications face a challenge when using shared spectrum that becomes more crowded. This often leads to demands for specific spectrum for an application. However, designating spectrum per application causes fragmentation and inefficient spectrum use. A possible solution is to designate spectrum – for one or more operational scales - for critical applications in general. Conditions for this spectrum should be such that the use of the band remains limited enough to provide a high degree of availability, without introducing severe conditions or licencing. One can think of technical limitations like protocols to use or power or duty-cycle restriction. Another option can be some light form of licencing.

Recommendation: Investigate the possibility to designate shared spectrum for critical applications in general instead of per application.

When IoT devices are secondary users of spectrum (for example, in large parts of the 5 GHz band a device has to leave the spectrum when it detects radar use) the chance and likelihood of the primary usage occurring is not always clear, making the reliability of this band difficult to determine.

Point of attention: The likelihood of unavailability of (parts of) the 5 GHz band should be more clear, for instance by providing estimations of the likelihood of spectrum unavailability at certain locations due to (likely) presence of radar and DFS obligations.

Monitoring and enforcement

Growth in the number of devices and the variety of protocols in shared spectrum makes monitoring and enforcement difficult. Spectrum use (and scarcity) may vary greatly in location and time and (local) spectrum impact is very difficult to predict. In addition, the number of devices that are used outside their primary targeted area and that might not adhere to EU standards (for example due to other power limits or other spectrum being used) is likely to increase: devices are easily ordered online in other countries, and travellers carry devices with them, which makes monitoring and enforcement even more difficult.

Recommendation: The role of governments towards regulation, monitoring and enforcement might (need to) shift towards earlier phases in the manufacturing process by following and steering worldwide standardisation of spectrum use where possible.

Recommendation: Methods for prediction (using congestion-models and risk-assessments of potential congested areas) and detection of potential local bottlenecks are needed. Monitoring smartly chosen (busy) sample situations with regard to spectrum use in order to assess the need of further policy enforcement or policy change is recommended.

Privacy

IoT devices are likely to enter the personal and home environment even further in the coming years. Multiple devices connect to web based servers, and (technically) local applications like home automation are offered as 'cloud based services'.

Point of attention: Specific attention might be needed for privacy and security concerns regarding the introduction of IoT devices.

References

[1] "ITS-Plan the Netherlands 2013-2017" (2013)

[2] "Wireless applications in Transport and Logistics", Stratix commissioned by Telecommunications Agency (March 2015)

[3] "Smart Industry, Dutch industry fit for the future", FME-CWM, Chamber of Commerce, Ministry of Economic Affairs, TNO, VNO-NCW (June 2014)

[4] "Action Agenda Smart Industry the Netherlands", FME-CWM, Chamber of Commerce, Ministry of Economic Affairs, TNO, VNO-NCW (November 2014)

[5] "LTE-dekking in Nederland: Mogelijkheden voor gebieden zonder snelle vaste internettoegang", Stratix, commissioned by Ministry of Economic Affairs (February 2015)

[6] "Research into the License Exempt spectrum of the Netherlands", Strict and Figo (February 2015)

[7] "Societal Impact of Wireless Revolution in the Netherlands and Possible Measures", J.C. Wortmann, J.B. van Meurs, F.B.E van Blommestein, G.B. Huitema, , University of Groningen commissioned by Agentschap Telecom, (March 2014)

[8] "Nota Frequentiebeleid 2005", Ministry of Economic Affairs (2005)

[9] "OECD Digital Economy Outlook 2015", chapter 6, OECD (2015)

[10] "Nut en noodzaak Regional Roaming voor vitale sectoren", Stratix commissioned by Ministry of Economic Affairs, (January 2014)

[11] "Intelligent Transport Systems (ITS); Access layer specification for ITS operating in the 5 GHz frequency band", ETSI EN 302 663 (V1.2.1) (July 2013)

[12] "Industry 4.0 - How to navigate digitization of the manufacturing sector", McKinsey&Company ,McKinsey Digital, (2015)

[13] European Commission Decision "On harmonisation of the radio spectrum for use by short-range devices", 2006/771/EC (2006)

[14] ECC report 44, In response to the EC Permanent Mandate on the "Annual update of the technical annex of the Commission Decision on the technical harmonisation of radio spectrum for use by short range devices", CEPT (2013),

[15] European Commission implementing Decision "amending Decision 2006/771/EC on harmonisation of the radio spectrum for use by short-range devices and repealing Decision 2005/928/EC", 2013/752/EU (2013)

[16] CEPT report 57, "To study and identify harmonised compatibility and sharing conditions for Wireless Access Systems including Radio Local Area Networks in the bands 5350 - 5470 MHz and 5725 - 5925 MHz", CEPT (2015).

[17] ERC Recommendation 70-03, "Relating to the Use of Short Range Devices (SRD)", CEPT (2015)

[18] ECC report 189 "Future Spectrum Demand for Short Range Devices in the UHF Frequency Bands", CEPT (2014),

[19] CEPT (not approved yet), DRAFT ECC report 242, "Compatibility and sharing studies for M2M applications in the 733-736 MHz / 788-791 MHz band"

[20] "Statement on the Authorisation of short range Devices in 870 to 876 MHz and 915-921 MHz", Ofcom (April 2014),

[21] Machina Research, "M2M application characteristics and their implications for spectrum", (May 2014)

[22] "Promoting investment and innovation in the Internet of Things, summary of responses and next steps", Ofcom (October 2014).

[23] "Promoting investment and innovation in the Internet of Things" Consultation document, Ofcom (July 2014),

[24] IMST GmbH "Channel Access Rules for SRD", charged by the BNetzA, Germany) (November 2012)

[25] "Allgemeinzuteilung von Frequenzen zur Nutzung durch Funkanwendungen mit geringer Reichweite für nicht näher spezifizierte Anwendungen; Non-specific Short Range Devices (SRD)", Bundesnetzagentur (2014)

[26] BNA.com (November 2014) "As 'Internet of Things' Evolves, FCC's spectrum Strategy Will Be Put to the Test"

[27] "How will IoT impact communications networks in 5, 10 years" (slide 84-118), FCC TAC (December 2014)

[28] "What impact will IoT have on the network in 3 years, 5 years, 10 years?" (slide 5-19), FCC TAC (June 2014)

[29] "Operation within the bands 902–928 MHz, 2400–2483.5 MHz, and 5725–5850 MHz", §15.247, FCC (1985)

[30] "Roadmap for future unlicensed services" (slide 47-50), FCC TAC (April 2015)

[31] "Keeping up: FCC Focusing on the Internet of Things", SmartGridNews.com (July 2015)

[32] "FCC to address broadband gaps impending Internet of Things", Fiercebigdata.com (February 2015)

[33] "Internet of Things – From Research and Innovation to Market Deployment", Ovidiu Vermesan and Peter Friess (2014)

[34] "Future use of Licence Exempt Radio Spectrum", J. Burns, S. Kirtay, P. Marks, for the UK spectrum policy forum (July 2015)

[35] "How China is scaling the Internet of Things", Insight Report from the GSMA Connected Living Programme (July 2015)

[36] "Unlocking the potential of the Internet of Things", McKinsey (June 2015)

[37] "The 2015 Vodafone M2M Barometer" (July 2015)

Acknowledgements

We would like to thank the following parties for sharing information and ideas:

- ASML;
- Actility;
- Domotica Platform Nederland;
- ETSI;
- GreenPeak;
- KPN;
- Nedap;
- Philips Lighting and Philips Medical systems;
- Philips standards and Intellectual Property;
- Radboud UMC;
- Tele2;
- Vodafone;
- ZigBee Alliance.

Annex A Examples of emerging Applications

In order to get insight in the uptake of current and future emerging applications a list of potential applications was created for this research. This annex contains examples of emerging applications in various fields.

A.1 Home Automation

Examples of emerging Applications

In recent years the most visible are media appliances that have become 'connected' like connected *Radio's, TV's, Media Centers and Game consoles* etc. Next to communication and syncing of audio and other media streams (that may in itself not be regarded as 'Internet of Things'), they can communicate with connected lights to create an *"immersive lighting experience that matches the action on-screen."*[67], and send for instance usage and even sensor data to each other and the internet. This illustrates the difficulty to define the scope of the Internet of Things.

Connected lights and switches typically start with simple tasks or systems being automated and 'connected' (like the traditional light-switch that is supplemented with a 'wireless' switch that allows lights to be controlled using a remote or an app on you tablet) but can end in highly integrated applications in which multiple systems of different kinds are connect (like a home cinema set and audio system that controls lights in order to create the right atmosphere that fits the movie or music). Typical applications include automated switching of Lights (on/off) and the implementation of trigger-based lighting schemes (depending on mood, timer, activity, number of people present, etc.). Controlling the lights takes place via a gateway or control station connected to the home network using Ethernet or Wi-Fi, and that controls the lights using one of a variety of technologies including ZigBee, Wi-Fi, Z-Wave, and a number of other (proprietary) protocols. Many early adapters have simple 'remote controlled' lights in living rooms. Remote switches to be placed in the power line or behind regular wall switch have been available for years. More recently stand-alone solutions became readily available and become mainstream with starter sets available at electronics and home supply shops, like Philips's 'Living Lights' and Belkin's 'WeMo LED lighting'.

Smart appliances like kitchen appliance, washing machines and dryers form another area where devices are getting connected in the coming years. Ovens can be pre-heated when on your way home, and temperature and other settings can be controlled using your tablet or smartphone. Some ovens have internal camera's to watch the meal without opening, and even allow sharing of your creations on social media[68]. Modern high-end washing machines come with a Wi-Fi connection that allows for control and status monitoring from an app.

[67] http://www.cnet.com/news/sharknado-2-syncs-with-philips-hue-for-smart-bulb-light-show/, http://www.electronichouse.com/daily/home-lighting/syfy-channel-sync-philips-hue-lighting-12-monkeys-tv-series/

[68] "By 2016, all of Electrolux's appliances will follow a set of protocols that allow them to communicate with other connected devices and appliances from the likes of LG, Sony, Panasonic, Sharp and Microsoft." http://www.telegraph.co.uk/technology/news/11307950/Connected-ovens-and-the-smart-home-of-the-future.html

Connected appliances are becoming the standard in the coming years. Typical they are replaced typically somewhere between 5 -15 years[69].

Energy companies provide *'smart thermostats'* such as Toon and Nest. These thermostats are sometimes capable of controlling or monitoring other home equipment such as lighting or washing machines.

Although still more in its infancy there are various connected *gardening sensors* that are placed in the ground near plants and send their information to a gateway in which data is collected and analysed to monitor the condition of soil for flowers and plants.

Automated blinds and sunshades can be found in many houses (although not mainstream, since many people don't mind closing them by hand). Modern versions are remote controlled by either a 'remote' or using an app on smartphone or tablet. They include features like automatic closing and opening on triggers, like time of day or sunshine.

Smoke and carbon monoxide detectors are getting connected[70], first to each other, (an alarm in one room triggers the alarm in an adjacent room warning persons there), later via a gateway (using for example Z-wave or ZigBee), (an alarm triggers email or sms alert when away from home). In almost all homes typically a couple of detectors are present per home. 'Connected detectors' might probably not become main stream soon, mainly because people are unlike to invest in a 'domotics gateway' just to fit the smoke detectors. More likely people will at some point have a gateway for other purposes (like lights), and then gradually add smoke detectors using the same gateway.

Other emerging applications include *smart doorbells* (taking a picture of anyone nearing the door), automatic locks (opening the door using a tag or smartphone), and *'pet doors'* for dogs and cats. They might be more for hobbyist and enthusiasts, with probably a low adoption in the coming years.

A.2 Emerging Applications in Healthcare (care and cure)

A.2.1 Institutional healthcare

Examples of emerging Applications

When it comes to hospital healthcare, there are many applications that can be regarded 'Internet of Things' and that are already used today. Some use is still in a pilot phase but other applications are already daily practice.

Hospitals start (at a moderate scale) to provide their patients with connected *wireless diagnostics devices* like patches that continuously measure ECG, Heart Rate , Respiratory

[69] http://www.cbsnews.com/news/kitchen-appliances-how-long-do-they-last/, http://stevesmallman.com/wp-content/uploads/2013/05/NAHB-Lifetimes.pdf , http://www.nachi.org/life-expectancy.htm

[70] https://shop.smartthings.com/#!/products/smoke-detector-and-carbon-monoxide-alarm

Rate and Skin Temperature to monitor their patients at a distance. Those sensors fit into a small 'patch'[71] so to cause minimal obstruction for the patient and keep the patient mobile.

Wireless diagnostics using small sensors allow *doctors to monitor patients at home* effectively *extending hospital care to the home environment'*. This makes it possible for some patients to leave the hospital early while still being under doctors supervision.

Wireless diagnostics can be combined with *patient tracking*[72]*:* using Wi-Fi connected wristbands patients in the hospital can be followed and notifications can be send when it is their turn at some facility. This increases the flow of patients, while keeping the patient 'ambulant' (no need to wait, patients can walk around until summoned) and thus increasing patients wellbeing.

In the *operation room*, operative tools are connected to be able to track all tools during the operation and more important, after it. *Asset tracking* is usually used in industries, but now in healthcare as well.

Around sixty thousand *AED's (Automatic External Defibrillators)* are available at many public places throughout the country. Right now they are often stand alone. However, modern Defibrillators record ECG data[73] and send this information in real-time to a specialist in the hospital, using a public mobile network. This allows for an earlier determination of the best treatment than is the case in traditional treatments where this information is available later. The expectation is that the public AED's will be connected with the supplier to schedule maintenance (to make sure all AED's available are ready for use) and to alert the back-office when it is used for an emergency.

A.2.2 Home-Care

Examples of emerging Applications

Senior Lifestyle Monitoring

For the elderly to be able to stay at home for a prolonged amount of time technology can play an important role. A number of applications is emerging that can facilitate this.

Motion Sensors are placed in the patients' home to detect movement. It's mostly used to track if a person has fallen in their homes to be able to go there on time to help. There are sets of sensors already commercially available that monitor presence, humidity, temperature and movement. They last about 10 years on one battery and can be attached in several spots of the home, for example to the fridge door and the bathroom door. A home gateway forwards the information to a server on the internet where the data is stored. The data is then used to detect eating and sleeping patterns and send warnings or information to family care givers, for instance when dehydration may occur. Other examples that are already widely used are *wireless alarm-buttons* that are worn around the neck use GPRS or SMS to

[71] For example 'Vital Connect health-patches' are placed on the patient's chest and communicate via Bluetooth LE to a 'relay device' from where the data is send to a platform using for example Wi-Fi or LTE.

[72] See for example the Ekahau RTLS patient tracking

[73] http://www.wos.nl/nieuws/item/20140117-nominatie-m2m-services-voor-kpn-channel-award/

send an alarm to health officials when the button is pressed, and *RFID tags* in clothes, 'watches' or shoe inlays[74] that transmit GPS locations used by care institutions for localising people with Alzheimer's disease.

Long-term illnesses

In the Netherlands (with a population of 17 million) there are over 5 million people with some chronicle illness, of which approximately 50 percent need some form of medicine, care or attention on a regular basis. It is to be expected that most of those will in the future be aided in their daily lives using IoT-technology, in the form of both sensors monitoring their specific condition, and smart technology to streamline medicine intake.

Examples include *Smart Wireless Pill Boxes*[75] that remind patients to take their medicine based on the prescription, for example using audio-signals, connection to a smartphone-app or SMS. '*Smart injection tracker'* for diabetes patients (approximately 800.000 in the Netherlands) that connects insulin pens to smartphones using Bluetooth. The application collects the data and forms a database, so that injection history can be accessed later and can be shared with the doctor if needed. And *wireless heart monitors* for arrhythmia patients (around 300.000 patients in the Netherlands) that collect and store data of the heart (ECG) and send it to mobile external monitor device.

A.2.3 Personal care

Introduction

This includes devices, tools and applications that individuals can buy at the store and use for personal care, or health related care. Examples include fitness wristbands, smart-scales, and smart baby monitors. This is a growing group of smart-devices that is becoming cheaper and more popular by the day. Many of these devices communicate with one's tablet or smartphone. The penetration of smartphones and tablets in the Netherlands is quite high, which makes using the smart-tools easier as well.

Examples of emerging Applications

Fitness and activity tracking

Fitness and activity wristbands and other health tracker devices exist for a couple of years already, Fitbit for example is founded in 2007. Fitness trackers track movements (for example the number of steps a day), as well as monitor sleep and intensity of movement, walking or running. They mostly communicate with a smartphone or tablet using Bluetooth, on which users need an app to view the collected data. Some have extra features that are not fitness related, like alarm clocks, or e-mail and phone call notifications.

To complete the health tracking experience, manufacturers of fitness wristbands also offer *smart scales.* These scales communicate with a smartphone and combine the data from the fitness tracker using Wi-Fi or Bluetooth 4.0.

[74] http://www.gpssmartsole.com/

[75] For example AdhereTech (http://adheretech.com/) and 'Ubox' (http://my-ubox.com/)

Besides the dedicated devices to activity tracking, there are hundreds of smartphone applications worldwide that track walking, running, cycling, and sleeping, they are mostly free of charge.

Baby monitoring

Gadgets like the *owlet baby sock*, *mimo baby monitor*, and the *sproutling baby monitor* are popular for baby monitoring. These devices monitor sleep activity, skin temperature and body position for example and send notifications or alarms to the parent's smartphone when things appear not to be right. Pacif-I monitors the baby's temperature at all times and communicate this with the parents smartphone, while pixi smart diaper monitors hydration and infection via a smartphone. There are specialised devices like the Pacif-I (*smart pacifier*), SunFriend, iSwimband and Pixi *Smart Diaper* which specialise in specific conditions, like swimming pools, or monitor sun exposure.

Most of these baby gadgets communicate using Bluetooth with a smartphone or a base station that uses Wi-Fi.

A.3 Automotive and Transport

Examples of emerging Applications

Car manufacturers like BMW and Volkswagen equip their (high end) cars with sensors for *remote car management functions*, like motor management. This information is transmitted using public mobile networks. The car manufacturers or dealers use this information to offer additional services like maintenance planning.

Emergency call, or *eCall*, is an application in cars to automatically warn emergency call-centres in case of an accident. The European Parliament decided to make introduction of E-Call in new cars mandatory from March 2018 onwards. Since the functionality should work throughout the EU, most manufacturers consider using public mobile networks for communication.

Future cars are envisioned to drive (semi) automatically and cooperatively by exchanging information with cars in front of the vehicle and with roadside infrastructure. *Intelligent Transport Systems* include driving assistance, collaborative driving, cooperative awareness, road hazard warning, increasing both traffic efficiency (by managing collective speeds of trains of vehicles), and safety. *Collaborative driving* is still being developed. For fast communication between cars manufacturers plan to use a low latency version of 802.11, 802.11p. A dedicated 50 MHz spectrum band is standardised in the 5.9 GHz band. Definitive ITS standardisation is ongoing but not completed, and e-Call legislation is expected.

Vehicle-to-vehicle and infrastructure-to-vehicle communications poses high demand on the used technology because of the need to share information between a 'random' set of cars moving at high speeds (with regard to the infrastructure and to other vehicles). The communication needs to be fast and have a low latency.

A.4 Industry and manufacturing

Examples of emerging Applications

The applications of the Industrial Internet that are mentioned most commonly are *predictive maintenance* and *remote asset management,* and *applications that improve worker productivity, safety and working conditions*[76].

An example is Thames Water Utilities Limited, a major UK water and wastewater services utility company using *sensors, analytics and real-time data to respond more quickly to leaks, changing weather conditions* and other potentially critical situations. Other applications range from unmanned aerial vehicles to inspect pipe lines to sensors for monitoring food safety. An example from oil and gas company Shell[77] are the *Smart Well,* with downhole sensors and flow control devices monitored and controlled from the surface.

More application can already be seen in practice: examples are for instance *robot welding machines with sim cards* for remote monitoring[78] and *tightening tools*[79] *and other tools with sensors, intelligence and wireless remote communication* via ZigBee or other protocols for monitoring, asset management and maintenance purposes. Other examples are *Automatic Guided Vehicles using* sensor information and intelligence in the network.

In the long term this will result in *'smart assembly'* with better connections between enterprise networks and manufacturing, further optimising availability of assembly lines, precision and reliability, *'the visual factory'* with better real time 'dashboard monitoring ' of factory performance, use of resources, security threats etcetera, '*Plant-wide Visibility'* where globally dispersed production sites are integrated, and better standardisation and uniformity of '*plant alarms an event resolution*'[80].

A.5 Smart Cities

Examples of emerging Applications

In-city traffic

Although not new, the ability to use fine-grained information from sensors and dispatch it in real-time to drivers creates further progress in *smart traffic management* to optimise the flow of traffic, reducing congestion in cities. If this information is combined with information about available parking spaces optimal traffic advice can be dispatched to vehicles to create *smart parking*. Although, at the moment, it primarily works with digital panels like DRIP's (Digital Road Information Panels), in the future this information can be directly dispatched to the navigation systems in the car. In order to detect available parking bays on the street

[76] http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf
[77] http://www.mcrockcapital.com/uploads/1/0/9/6/10961847/mcrock_industrial_internet_of_things_report_2014.pdf
[78] http://www.mac-solutions.co.uk/en/success-stories/73-talk2m-enables-remote-monitoring-and-control-of-robot-welding-machines
[79] http://resource-center.desouttertools.com/my/download.php?itemId=126496905&itemName=EAP-EDP_EN_User_Manual_6159936431-05.pdf&itemSize=2300249&itemContentType=application/pdf
[80] http://www.industrial-ip.org/en/industrial-ip/internet-of-things/how-the-internet-of-everything-will-transform-industries

sensor are placed under each bay, relaying the information ("available" or "occupied") to a central hub using a low power communication protocol, for example in the 868 MHz band[81]. Another example are *connected parking meters*[82] that allow drivers to find open parking spots. Amsterdam uses *intelligent traffic direction signs*[83] around their stadium and concert hall area to optimise the traffic flow at the start and finish of major events.

The city of Utrecht[84] uses technology to *enforce a low emission-zone* using an automatic system consisting of detectors for number plate recognition, a system that checks a database to determine type of cars, and visual warning systems (signs or drips) to warn a driver of a car in real-time if it enters the centre zone unauthorised.

There are a number of ideas for *'connected bikes'*, including GPRS-enabled GPS-trackers (connectedcycle.com). Another application in development is a 'smart solar powered bike locks'[85] that automatically opens when you are near, based on local Bluetooth communication from your smartphone to the lock. The lock also communicates using public mobile networks so it can be remotely unlocked using a smartphone, allowing for your bike to be shared with friends. An additional feature can be crash-detection, similar as proposed for cars, to detect (to) sudden movements indicating a crash and to send an alert.

City environment and safety

Managing the flow of waste is aided by wireless *container fill-level monitoring devices*[86], creating an intelligent system for the recollection of urban waste. Information about various filling levels for glass, paper, and trash-containers, together with GPS location information, is send to centralised planning tools to optimise the route of garbage collecting cars. Such a system increases efficiency, reduces unnecessary trips of collection trucks, and prevents the situation where trash containers are full and people place their garbage directly next to the container, attracting bugs and birds. Those systems use various wireless communication technologies, like public mobile networks or private networks based on 802.11.4.

City *street lights* have to be switched on and off at night. New connected lights allow for smarter lighting schemes, that switch not only depending on time and on weather conditions, and that allow for street lights to become brighter when persons or vehicles are near and dimmed otherwise, thus reducing electricity use while keeping enough light for safety[87]. Such smarter schemes help reduce the total amount of ambient background light in modern cities.

Air quality is a major concern in many big cities. Often city officials monitor air-quality using a network of (tens of) measuring-modules placed throughout the city. In the Netherlands, there is a network of about 100 air quality measuring stations that are spread throughout

[81] For example Nedap offers such a system operating in a specially developed low power protocol in the 868 MHz band. LoRa, SigFox, and other low power networks can be used for those kind of applications, too.

[82] http://sfpark.org/how-it-works/

[83] https://www.rijkswaterstaat.nl/zakelijk/magazines/wegeninfo/juli_2013/samenwerken_aan_verkeersmanagement.aspx

[84] http://www.nu.nl/utrecht/3915153/utrecht-checkt-kentekens-vieze-autos-milieuzone.html

[85] http://www.gizmag.com/skylock-solar-powered-bike-lock/32157/

[86] Sintelur and Enevo One are examples of detector system that wirelessly communicate to a backend server. As an extra 'gimmick', the latter communicates its status using Twitter: https://twitter.com/trashcanlife

[87] There are approximately 3 million street lights in the Netherlands that might become connected in such a way that smarter lighting schemes become possible.

the country. However, with the advent of cheaper sensors and programmable hardware modules it is now possible for people to have access to measurement equipment themselves. In a project in Amsterdam[88] a Do It Yourself *'Smart Citizen kit' for air quality measurement* is offered to hundreds of people. The system, based on Arduino[89] and open source software, includes sensors that measure humidity, noise, temperature, CO, NO_2 and light intensity in a neighbourhood. Once the kit is put together, the sensors are placed outside windows or on balconies and connect to the internet using Wi-Fi. The data is collected on a central server, creating a fine-grained network of (citizen owned) pollution sensors. The 'Smart Citizen' project is an example of how IoT, due to cheaper sensors and the availability of communication networks (using people's Wi-Fi), can help citizens to be better informed and to actively participate in their community.

Tourism

Besides facilitating to its residents, cities facilitate many visitors from outsides. IoT is bringing new features to allow this to happen. *Personalised and real-time tourist information*, based on, and adapted for, the needs of a specific tourist, can make a city attractive.

The City of Amsterdam[90] plans a pilot *"iBeacon and IoT Living Lab"* in 2016 that uses Bluetooth based iBeacons for personalised direction information combined with other information on your smartphone. The plan is to create a zone in which the application will guide tourists and users to relevant locations, using points of interest and location information of the user. In the future *dynamic (real-time) signs* can be programmed to show personalised location of special events, public transportation, or other relevant information. Ideas are for example 'Pointsigns' that rotate to show visitors the way to go. The signs are programmable and use internet connectivity (using Ethernet or wireless connectivity using for example LTE). This project gives an idea what personalised dynamic road-signs might look like in the near future.

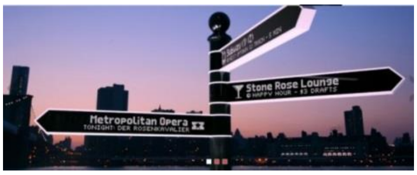


Figure 7: Artist impression of Pointsign (source: pointsign.com)

Smart and personal roadside advertisement is becoming a reality. Shops detect repeat visitors (for example using the ID of always on Wi-Fi phones) and use facial recognition techniques[91] to determine what to offer. Advertisement signs are equipped with sensors to display relevant information based on certain parameters.

[88] http://waag.org/en/project/smart-citizen-kit

[89] Systems such as Arduino and Raspberry Pi, combined with low cost sensors, allow for many hobbyist and Do It Yourselve-solutions, as well as provide a widely used prototyping platform.

[90] http://amsterdamsmartcity.com/projects/detail/id/104/slug/ibeacon-living-lab

[91] http://www.theguardian.com/business/2013/nov/03/privacy-tesco-scan-customers-faces

A.6 Utilities: Energy and water

Examples of emerging Applications

Smart meters give more fine grained insight in energy consumption over time and makes introduction of varying electricity fees (depending on total availability of energy) possible. The 'smart electricity meter' installed by utilities records energy consumption and sends this information periodically to the grid operator. The smart energy meters acts as a hub for water and gas meter. The installation of smart electricity and gas meters in homes is underway, with grid operators aiming to offer installation to all homes in the Netherlands by 2020. For smart meter readout in the Netherlands both a CDMA-450 MHz and commercially available GPRS services are used. In the utility room, information from the water and gas meter is transferred to the e-meter.

Another trend is to add automation and sensors to the energy grid itself, for example in distribution nodes, to early detect failures and for maintenance scheduling. The vision is that gradually the networks change to become a *"smart grid"* in which various actor and users on the energy grid communicate to each other or to a centralised system to optimise *demand and supply* of energy.

The need to charge electric cars poses a challenge for grid operators and electricity producers. Optimal charging strategy prevents peak loads (i.e. prevent cars from being loaded at the same time energy is needed for other processes). For this coordination, and thus communication, can be used using smart charging points. Combining local creation of energy with local storage of energy can significantly decrease the load on the energy grid, and brings an advantage in itself that the energy does not need to be transported so transport losses are reduced. Examples are charging points for electric cars, that can use locally generated power from the sun[92] when available, and at the same time allow the battery of the car to be used as a storage medium for electricity.

Some utility companies experiment with marketing *smart thermostats* that can be controlled from outside the home and can control home automation features.

A.7 Agriculture

Examples of emerging applications

One of the most trends in the agricultural sector is precision farming: applications are being used to improve yield, harvest and livestock well-being, while staying competitive in worldwide business. Lack of availability of broadband in rural areas can cause issues when using those novel technologies. Currently sometimes removable USB hard disks are used to collect and transport data daily or weekly in cases broadband is lacking.

Precision farming

[92] https://www.stedin.net/over-stedin/pers-en-media/persberichten/wereldprimeur-utrecht-laadpaal-maakt-opslag-zonneenergie-mogelijk

To gain more yield, and use less resources, more and more high tech applications are applied in arable farming. It started by using satellite positioning technology and gradually became more complex by adding sensors and camera's to control the different processes in the farm like solutions for automated seeding and recording harvesting data. An example is the *van den Borne* potato farm in the Netherlands which uses a self-made drone and cameras in the field to collect data and adjust irrigation and pesticides to the crops.

Other examples include wine farmers that use *connected sensors*[93] to measure temperature of the soil and humidity and send the data to an online system, and use in fishery where water temperature and dissolved oxygen levels are monitored and send to the farmer's phone. The European Union is backing initiatives in this area like sensorfish.eu.

Livestock monitoring

Farmers keep an eye on the well-being. Data is collected using sensors on the livestock or in stables and data is send to a server and is accessible via an app on the farmer's smartphone or tablet using the 2.4 GHz band. Such real-time and detailed monitoring allows the farmer to monitor condition of the livestock and detect diseases early on.

There are many initiatives in this area, like the EU funded *precision livestock farming*[94] project (started in 2012) that "*develops management tools aimed at continuous automatic monitoring of animal welfare, health, environmental impact and production in real-time."*. Several devices were developed during this project, one of them is the *pig cough monitor*, which isolates the sound of coughing in a piggery. The data is accessible via the internet and enables the farmer to detect diseases in the piggery, before a mass spread. The same device is altered and used in poultry farms to detect stress levels of poultry and to detect respiratory infections in young calves. Other examples are the *eCow farmBolus*or the *Nedap Smarttag health monitoring* using a neck or leg tags, sensors in milking machines, sensors in feeding machines, activity monitors, and air quality.

In the Netherlands Vitelec and other companies build sensors networks (using ISM bands 433 MHz, 868 MHz or 2.4 GHz) in the field of Greenhouse farming to measure lighting, CO_2, humidity and temperature in the Greenhouse[95].

Besides specific applications generic systems are used to manage and localise equipment to prevent theft, manage the use of resources like water and electricity, or cameras to guard the property. Real-time fleet management solutions are used to monitor transportation of agricultural products. The *Nano Ganesh modem*, which is installed on water pumps, monitor the use of scarce water in farming.

Forestry and wildlife

Sensors are being used measure temperature and concentration of certain gases in forests where fires occur frequently in the summer[96], and sensors are used to protect wildlife animals from poachers (for example using a camera and GPS collar on Rhinos[97]).

[93] http://newsroom.cisco.com/video-content?type=webcontent&articleId=1275685
[94] http://www.eu-plf.eu/
[95] https://www.t-mobile.nl/zakelijk/htdocs/page/zakelijke-oplossingen/m2m/segmenten/publieke-infrastructuur.aspx

Annex B Communication Protocols

B.1 Communication protocols for low power, small area

Short range, low power communication protocols are used for local communication such as in **Personal Area Networks** for connecting devices in one's direct vicinity.

Radio Frequency ID (RFID) and Near Field Communication (NFC)

Radio Frequency Identification is a relatively cheap way to identify objects using tags that can be ‘interrogated' using low power radio signals which will result in detection of the identification code of the tag. Two systems are most common: Systems with an active reader and a Passive Tag (ARPT), with a tag that does not need batteries but uses the interrogation signal to produce a response, and systems with and active Reader and an active Tag (ARAT), which uses a tag that actively responds or sends an ID. Most RFID systems use standardised ISM bands.

Characteristics:

- Standards: Variety of standards for different industries and usage. Relevant standardisation organisations include ISO, IEC, ASTM International, the DASH7 Alliance and EPC-global.
- Major Players:
- Frequency bands, ranges and use: Bands RFID runs on:
  - 120–150 kHz (10cm) can be used license free worldwide
  - 13.56 MHz (10cm-1m) can be used license free worldwide
  - 433 MHz (1-100m), defence applications
  - 865-868 MHz (Europe) and 902-928 MHz (North America) (1-12m).
- Data Rates: 100–420kbps
- Installed Base: It is expected that around 150 Billion (150.000.000.000) RFID tags will be deployed in this decade.

Near Field Communication (NFC) is a term generally used for a more elaborate form of communication using similar technology principles as RFID for more elaborate two way communication. Examples are interrogation of sensors and storing and retrieving information in tags. Similar to RFID, both passive communication and active communication can be distinguished.

Characteristics:

- Standard: ISO/IEC 18000-3
- Major Players:
- Frequency band: 13.56MHz (ISM)
- Operational Range: 10cm
- Data Rates: 100–420kbps
- Installed base: The number of NFC-enabled devices exceeded 500 million in 2014,

[96] http://www.libelium.com/wireless_sensor_networks_to_detec_forest_fires/

[97] http://www.nu.nl/gadgets/4092312/slimme-camera-neushoorns-moet-stroperij-tegengaan.html

Bluetooth

Bluetooth is a low power, low range communication protocol that connects devices in each other's direct vicinity, like mobile phones or laptops to each other or to other peripherals like sensors. Three variants of Bluetooth technology can be roughly distinguished. Although specifically aimed for short range communication involving mobile handsets, the first versions of Bluetooth up to version 3.0 were – compared with current practice – not very energy efficient.

Bluetooth Low Energy (Bluetooth 4.0, BLE, Bluetooth Smart, Wibree): In 2006 Nokia introduced Wibree which was merged into the main Bluetooth standard in 2010 in version 4.0 and marketed as 'Bluetooth Smart'. The technology is faster and more energy efficient than the earlier Bluetooth implementations over comparable distances.

iBeacon is a technology that uses a simplified version of Bluetooth 4.0, where senders transmit an ID called UUID which can be recognised by iBeacon supporting devices such as smart phones. This enables for instance use for navigation in buildings by using senders as predefined waypoints or reference points.

Characteristics:

- Standard: Bluetooth 4.2 core specification
- Frequency band: 2.4GHz (ISM)
- Operational Range: 50-150m (Smart/BLE)
- Data Rates: 1Mbps (Smart/BLE)
- Installed Base: unknown, estimates are billions.

Nike+

Nike and Apple developed the Nike+ technology for personal exercise monitoring. It is a proprietary technology, only working on Nike and Apple devices.

Characteristics:

- Standard: Proprietary
- Frequency band: 2.4 GHz
- Operational range: up to 10 meters
- Data Rates: up to 272 bps

Non-wireless identification methods

There are identification mechanisms and protocols using 'machine readable identification tags', such as barcodes, QR codes that do not directly affect frequency use, but certainly have an impact indirectly to data traffic and spectrum use because the use of such methods generates wireless traffic. An example is self-scanning of products in supermarkets with wireless devices.

Wireless USB

Wireless USB (WUSB) was designed to operate in the 3.1 to 10.6 GHz frequency range. Data rates that can be achieved vary between 480 Mbit/s at distances up to 3 metres and 110 Mbit/s at up to 10 metres.

Characteristics:

- Standard: Wireless USB Promotor group
- Major Players:
- Frequency bands: 3.1 GHz–10.6 GHz
- Operational Range: 3 – 10 meter
- Data Rate: 53-480 Mbit/s

B.2 Communication protocols for low and medium power, medium area

Communication in the 'Local Area' range are used for various 'Internet of Things' signalling and switching of devices, such as for home and building automation. The main protocols include Wi-Fi (which) and ZigBee. Within these networks, a difference can be seen between specifically designed (very) low power protocols, and protocols like Wi-Fi, that is a more general protocol that supports higher bandwidths.

ZigBee

ZigBee is a protocol for low power, small distance (10-100 meter) communication of small amounts of data with 250 kbps. It is based on an IEEE 802.15.4 standard. It supports a mesh topology which enables transporting data over larger distances by passing through data from device to device. Typical applications are wireless light switches, lighting settings such as mood lighting or adaptive lighting, remote displays of meters and sensors, traffic management systems, and other consumer and industrial equipment. The ZigBee protocol suite includes profiles for different application types including smart energy, building automation, health care and remote controls for television and set top boxes (this last profile is known as RF4CE and was standardised in 2009 as part of ZigBee by four consumer electronics companies: Sony, Philips, Panasonic, and Samsung).

Characteristics:

- Standard: ZigBee 3.0, based on IEEE802.15.4
- Major players: Philips (Hue lighting system), NXP, Sony, Panasonic, Samsung
- Frequency bands: 2.4GHz
- Operational Range: 10-100m
- Data Rates: 250kbps
- Installed Base: In 2014 there were an estimated 315 million ZigBee devices in the field.

Z-wave

Z-wave is a protocol developed primarily aimed at home automation applications such as lighting, smoke alarms, remote controls and home appliances. It was developed by Danish company ZenSys that formed the Z-Wave Alliance in 2005. The technology is designed for transmitting small data packets at relatively low speeds up to 100 kpbs, so that power consumption is kept relatively low. Z-Wave operates in the 900 MHz frequency range and is sharing this frequency range only with some cordless telephones and other consumer devices.

Characteristics:

- Standard: Z-Wave Alliance ZAD12837 / ITU-T G.9959
- Major players:
- Frequency bands: 900MHz (ISM)
- Operational Range: 30m
- Data Rates: 9.6/40/100kbit/s
- Installed base: As of 2014, the Z-Wave installed base is estimated to include over 25 million interoperable products.

Thread

Thread is a new protocol developed by Nest Labs of Google in collaboration with Samsung. The protocol uses 6LoWPAN, which in turns uses the IEEE 802.15.4 wireless protocol with mesh communication similar to ZigBee. Thread however is IP(v6)-addressable. It has support for over 250 devices on a network. In May 2015 Google introduced a platform which is designed to work with Thread.

Characteristics:

- Standard: Thread, based on IEEE802.15.4 and 6LowPAN
- Major Players: Google, Samsung
- Frequency band: 2.4GHz (ISM)
- Range: N/A
- Data Rates: N/A
- Installed Base: only recently introduced.

EnOcean

EnOcean is a protocol for use in industry, transportation, logistics and smart homes. The system uses an energy harvesting technology used in building automation systems in which the energy from pressing the button is used for the wireless communication.

Characteristics:

- Standard: ISO/IEC 14543-3-10
- Major Player: Siemens
- Frequency bands: 868 MHz (Europe), 902 MHz (North America), 928.35 MHz (Japan), 315 MHz (US)
- Operational Range: 30m inside buildings
- Data rates: 125 kbps
- Installed Base: As of 2015, EnOcean-based products are installed in over 250,000 buildings around the world. More than 20 million devices installed globally.

Other:

WirelessHART

WirelessHART is a wireless variant of the HART protocol using IEEE 802.15.4 standard radios in the 2.4 GHz ISM band. It is aimed at industrial applications. It uses a self-organising and self-healing mesh architecture. Major players include Siemens, Hitathi, Mitsubishi and Alstom.

Modbus wireless

Modbus wireless is a wireless application of the industrial Modbus protocol, using IEEE 802.15.4 standard radios in the 2.4 GHz ISM band.

MiWi

MiWi is a proprietary protocol based on IEEE 802.15.4 for small, low power (personal area network devices. It is claimed that MiWi protocol stacks are small foot-print alternatives (3K-17K) to ZigBee (40K-100K)

ISA100.11a

This is a standard described as "Wireless Systems for Industrial Automation: Process Control and Related Applications" standardised by the International Society of Automation (ISA) aimed at industrial applications. The protocol uses IEEE 802.15.4 for the physical layer.

Protocols that are used as building blocks in more than one technology

IEEE 802.15.4 specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs) and is the basis for protocols such as ZigBee and 6LowPan (and WirelessHART, MiWi, ISA100.11a).

6LoWPAN ('IPv6 over Low power Wireless Personal Area Networks') is a higher level protocol that allows IPv6 packets to be sent over IEEE 802.15.4 based networks. It is defined in RFC6282 (RFC 4919) and is used over a variety of other networking media including Bluetooth Smart, ZigBee or low-power RF (sub-1GHz).

B.3 Technologies supporting medium power, medium area

Wi-Fi

The IEEE 802.11 standard, more commonly known as 'Wi-Fi', evolved to a standard used by virtually every laptop and smartphone and is the technology behind almost every wireless local area networks in homes, offices, and many other environments worldwide. Popularity started in 1999 with the IEEE 802.11b standard providing a maximum bandwidth of 11 Mbps using the 2.4 GHz band, but is since extended providing more bandwidth and using the 5 GHz bands.

Characteristics:

- Standard: Based on 802.11n (most common usage in homes today)
- Major players:

- Frequency band: 2.4GHz and 5GHz bands
- Operational Range: Approximately 50m
- Data Rates: 600 Mbps maximum. 150-200Mbps is more typical, depending on channel frequency. Latest 802.11-ac standard could offer 500Mbps to 1Gbps.
- Installed base: Wi-Fi is the most ubiquitous wireless technology today, with Wi-Fi shipments passing the ten billion mark in January 2015. Analysts predict that by the end of 2020 there will be an installed base of 212 billion Wi-Fi devices connected, some 30 billion of which will be connected "autonomous things".

Low Power Wi-Fi (under development)

IEEE 802.11ah (sometimes referred to as 'low power Wi-Fi') is a version of 802.11 that is currently being developed that aims for use in extended range Wi-Fi networks, and for low energy applications such as cooperating groups of sensors or stations in a larger area. IEEE 802.11ah uses sub 1 GHz license-exempt bands, to enable longer working ranges than the 2.4 GHz and 5 GHz bands used in other existing IEEE 802.11 variants. The standard is expected to be finalised and published in 2016.

Characteristics:

- Standard: IEEE 802.11ah
- Major Players: Qualcomm
- Frequency band: 0.9 GHz (700MHz/863-868 MHz in Europe, under discussion, 916.5-927.5 MHz in Japan, with eleven 1MHz channels. 755-787 MHz in China, with thirty-two 1 MHz channels.)
- Operational range: up to approx. 1 km
- Data rates: specs aims for throughput of 150 Kbits/s (for a 1 MHz band).
- Installed Base: not yet introduced.

DECT Ultra Low Energy

DECT Ultra Low Energy (ULE) is a low energy variant of the DECT (Digital Enhanced Cordless Telecommunications) protocol that is used all over the world for cordless (home) telephones. The ULE variant was introduced in 2011. DECT ULE uses the 1.9 GHz band. The standard has been created to enable home automation, security, healthcare and energy monitoring applications that are battery powered and can easily connect to the web using the large number of existing DECT enabled modems and be managed using a smartphone app.

Characteristics:

- Standard: DECT ULE, ULE Alliance
- Major Players:
- Frequency band: 1.9 GHz band
- Operating Range: over 50 meters in buildings and up to 300 meters in the open air.
- Data rate: up to 1 Mbps[98]

[98] http://www.lsr.com/white-papers/technical-overview-of-dect-ule

DASH7

DASH7 is an open source RFID-standard for wireless sensor networking originally designed for military use, but now aimed for commercial applications that do not want to use comparable but in some respects less open standards such as ZigBee and Z-Wave.

Characteristics:

- Standard: DASH7 Alliance, ISO/IEC 18000-7
- Frequency: 433 MHz unlicensed ISM band/SRD band
- Range: up to 2 km
- Data Rates: up to 200 kbit/s

INSTEON

INSTEON is a dual-mesh (RF and Powerline) technology for home automation invented around 2005 by Smartlabs, Inc.

Characteristics:

- Standard: proprietary Smartlabs
- Frequency bands: 902 to 924 MHz
- Data rates: average 180 b/s, instantaneous 13kbits/s
- Operating range: up to 45 meters unobstructed line-of-sight
- Installed Base: roughly around 100 million units worldwide

ANT and ANT+

ANT is a technology working in the 2.4 GHz band aimed at the communication of sports and fitness sensors to a display unit such as a watch or cycle computer. An extended version of the protocol, ANT+, enables devices to be interoperable in a managed network.

Characteristics:

- Standard: ANT
- Frequency bands: 2.4 GHz
- Operational range: up to 30 meters
- Data Rates: ~20 kbps
- Installed Base: worldwide installed base of 150M+

WeMo

Belkin WeMo is a proprietary protocol for power switches for lights and home appliances using a Wi-Fi connection.

B.4 Technologies supporting low power, wide area

LoRa/LoRaWAN

LoRaWAN (known as Lora) stands for Long Range Wide Area Network and is a low power communication technology standardised in the LoRa Alliance (founded in march 2015). The technology enables bi-directional low data rate communications over long distances by battery operated sensors and actuators for M2M and IoT applications. A LoRa network typically consists of a gateway that communicates to the sensors using the LoRa protocol. The gateway itself is connected to a backend using for example a fixed Ethernet connection or LTE.

Characteristics:

- Standard: LoRaWAN
- Major players: Cisco, IBM, Bouygues Télécom (France), KPN (Netherlands), Swisscom (Switzerland), Belgacom (Belgium), Eastnet (South Africa)Frequency: Various
- Operating Range: 2-5km (urban environment), 15km (suburban environment)
- Data Rates: 0.3-50 kbps.
- Installed base: Still in introduction phase, several tens of thousands devices worldwide.

SigFox

SigFox is a low power technology for wireless communication to a diverse range of low-energy objects such as sensors and M2M applications. A SigFox network consists of cells with a central gateway that communicates to the sensors, while the gateway itself is connected to a backend using some other technology (fixed or wireless). It allows for transport of small amounts of data over ranges up to 50 kilometres.

Characteristics:

- Standard: Sigfox
- Major players: Samsung, Airbus, Telefonica, SK Telecom and NTT
- Frequency: 900MHz (868MHz in Europe and 915MHz in the U.S.)
- Operating Range: 3-10km (urban environments), 30-50km (rural environments),
- Data Rates: 10-1000bps
- Installed Base 2015: approximately 300,000 devices are connected in Europe.

Weightless

Weightless is an open, low power technology for exchanging data between a base station and hundreds of devices. The protocol is developed by the UK company Neul. It uses narrow band technology and working in license exempt sub 1GHz spectrum. There was an effort to create Weightless-W that would use Tv-white spaces. However, this was deemed to be no longer an opportunity with TV frequency space becoming less and leaving less whitespaces..

Characteristics:

- Standard: Weightless Special Interest Group (Weightless SIG), Neul
- Frequency band: 868MHz, 915 MHz, 458MHz (UK)
  Operating range: 10km

On-Ramp Wireless

On-Ramp Wireless is a solution for low-power wide area scalable sensor networking and location tracking for industrial sensor networking, building control, energy management and location tracking.

Characteristics:

- Standard: On-Ramp is working in the IEEE 802.15.4k standards group
- Major players: utility companies
- Frequency range: 2.4 GHz
- Operating range: 50 km (30 mile)
- Data rates: low, similar to Sigfox, Lora etc.

Wireless M-Bus

Wireless M-Bus is a set of European (ETSI) standards for Automatic Meter Reading at sub 1 GHz. M-Bus, short for Metering Bus, defines the communication between meters for water, gas, electricity on one side and the data concentrators on the other side.

Characteristics:

- Standard: European standard NEN-EN 13757-4:2013, EN13757-3:2004, dedicated application layer, ETSI EN 300 220 v2.3.1
- Frequency range: 868 MHz, 169 MHz, 433 MHz[99]
- Operating range: < 2km, at line of sight
- Data rates: 16.384 kbps / 66.6 kbps

B.5 Technologies for supporting medium power, wide area

Cellular mobile networks

Cellular networks are already used for many M2M and IoT applications today, usually for applications that involve mobile devices that are moved over larger distances or are scattered over multiple sites.

Especially for those applications where the cost of wireless communication is relatively low compared to the whole product (for instance in vending machines) or in cases where access to a cellular mobile network can be used for other purposes, the relatively high costs of the SIM and connections and high energy consumption is less important.

In recent years the subscription prices for ‘M2M’ sims that use in the order of 1-2 MB’s of data per month have been declining, making it more feasible to connect more devices (like millions of smart meters) using cellular networks.

There is an effort to develop a *Low Power LTE* variant, but this effort is currently still rather in research and prototyping phase[100]. It is for instance not yet clear how Low Power LTE

[99] http://www.emcu.it/WirelessMBUS/Wireless_M-BUS_Solutions_and_more.pdf
[100] http://www.rethinkresearch.biz/articles/huawei-demonstrates-pre-standard-lte-m-vodafone-targets-cellular-iot/

solves the challenge of catering the combination low transmission power and longer transmission distances while co-existing with other LTE devices.

Characteristics:

- Standard: 3GPP and GSMA, GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G)
- Frequency bands: 800MHz/900MHz/1800MHz/1900MHz/2100MHz/2600MHz
- Operating Range: 35km max for GSM; 200km max for HSPA
- Data Rates (typical download): 35-170kps (GPRS), 120-384kbps (EDGE), 384Kbps-2Mbps (UMTS), 600kbps-10Mbps (HSPA), 3-10Mbps (LTE)
- Installed base: An estimated 200 million mobile connections used for M2M in 2014.

Satellite

Although the majority of upcoming IoT applications will be based on terrestrial technologies, some applications, for instance with devices that are scattered in rural areas in many different countries can benefit the use of satellite data communication. Satellite M2M/IoT is important for niche markets such as the energy sector, for instance for monitoring pipelines or electric wire networks that stretching hundreds of kilometres across remote areas.

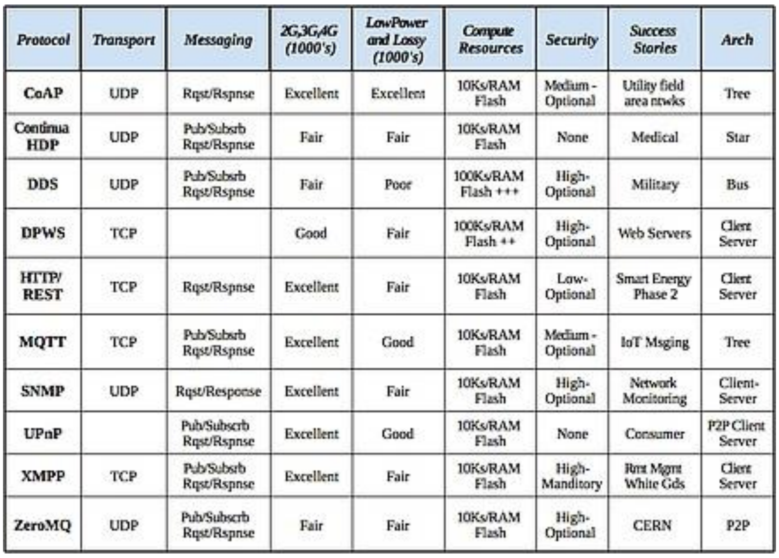
Characteristics:

- Major players: satellite companies (Eutelsat)
- Frequency bands: primarily L-Band (and sometimes others such as the Ku-band[101])
- Operating range: whenever there is reasonable line of sight to the south
- Data rates: up to 160 Kbps/terminal[102]
- Installed base: the total market for satellite communication for M2M and IoT applications is estimated at 3 million units in 2014.

B.6 Application layer protocols

A broad range of application layer protocols including session protocols, data structuring languages etcetera, is used for IoT applications. Examples are already longer existing protocols such as *HTTP* (Hyper Text Transfer protocol, famous as the protocol that internet browsers use), *REST* (Representational State Transfer, a set of workable constraints for hypertext and hypermedia applications) and *SNMP* (widely used for switches, printers etc.). Others are more M2M and IoT oriented protocols such as *COAP*, the Constrained Application Protocol aimed for use in very simple electronic devices and *MQTT (*a light-weight messaging protocol for applications with low bandwidth and small code footprint with a name that is derived from Message Queuing Telemetry Transport although message queueing is no longer a required standard feature of the protocol). An overview of features of a selection of the IoT application layer protocols is given in Figure 8.

[101] http://offcommnews.com/article/forecast-for-satellite-m2m/
[102] http://www.eutelsat.com/files/contributed/news/media_library/brochures/EUTELSAT_SMARTLNB_M2M_1014.pdf



Protocol	Transport	Messaging	2G,3G,4G (1000's)	LowPower and Lossy (1000's)	Compute Resources	Security	Success Stories	Arch
CoAP	UDP	Rqst/Rspnse	Excellent	Excellent	10Ks/RAM Flash	Medium - Optional	Utility field area ntwks	Tree
Continua HDP	UDP	Pub/Subsrb Rqst/Rspnse	Fair	Fair	10Ks/RAM Flash	None	Medical	Star
DDS	UDP	Pub/Subsrb Rqst/Rspnse	Fair	Poor	100Ks/RAM Flash +++	High-Optional	Military	Bus
DPWS	TCP		Good	Fair	100Ks/RAM Flash ++	High-Optional	Web Servers	Client Server
HTTP/ REST	TCP	Rqst/Rspnse	Excellent	Fair	10Ks/RAM Flash	Low-Optional	Smart Energy Phase 2	Client Server
MQTT	TCP	Pub/Subsrb Rqst/Rspnse	Excellent	Good	10Ks/RAM Flash	Medium - Optional	IoT Msging	Tree
SNMP	UDP	Rqst/Response	Excellent	Fair	10Ks/RAM Flash	High-Optional	Network Monitoring	Client-Server
UPnP		Pub/Subscrb Rqst/Rspnse	Excellent	Good	10Ks/RAM Flash	None	Consumer	P2P Client Server
XMPP	TCP	Pub/Subsrb Rqst/Rspnse	Excellent	Fair	10Ks/RAM Flash	High-Manditory	Rmt Mgmt White Gds	Client Server
ZeroMQ	UDP	Pub/Subscrb Rqst/Rspnse	Fair	Fair	10Ks/RAM Flash	High-Optional	CERN	P2P

Figure 8: Non exhaustive overview of application level protocols (source: embedded-computing.com)

CONTACT

Stratix

Stratix B.V.
Villa Hestia - Utrechtseweg 29
1213 TK Hilversum

Telefoon:	+31.35.622 2020
E-mail:	office@stratix.nl
URL:	http://www.stratix.nl