Universiteit Leiden

ICT in Business

Addressing Internet of Things Challenges in a Smart City based on a Novel Architectural Approach

Name: Kaylesh Ajodhia
Student-no: s1731033

Date: 18/08/2017

1st supervisor: Prof. dr. J.N. Kok

2nd supervisor: Dr. L.P.J. Groenewegen

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)

Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Acknowledgements

First of all, I want to take this opportunity to express my gratitude to a number of people that have helped and supported me in accomplishing my master thesis. First, I want to thank my first supervisor Prof. dr. Joost Kok for his close supervision, guidance and insightful discussions. I also want to thank my second supervisor Dr. Luuk Groenewegen for providing me a sound review, helping me with the Archimate models and his enthusiasm during the whole process. Next to my university supervisors, I especially want to thank my company supervisor Jos Grond for providing me this research opportunity, his close supervision and insightful brainstorm sessions even though he was in the other part of the world. Next, I also want to thank my colleagues of Cumulocity in providing me meaningful insights of the practical side of the topics. Furthermore, I want to gratefully thank my family and especially my parents, brother and sister-in-law for believing in me, supporting me and making me comfortable with conducting this research as best as possible. Last but not least, I want to thank my close friends Dylan te Lindert, Hugo Brouwer and Sebastian Mulders for their support from the very beginning of the research. Their discussions and brainstorm sessions have helped me a lot during this period.

Abstract

The concept of Smart City has gained its momentum in the course of the years. Many cities around the world have embraced the potential value, and allocated resources for realization purposes. However, the rapid development in this era has resulted in a number of challenges that are restraining the full utilization of a Smart City. Therefore, in this study, we aim to formulate and to investigate an architectural approach that addresses the challenges. The main research question of the study is: *"To what extent can IoT challenges in Smart City be addressed by means of an architectural approach?"* We have answered the research question as follow. First, we describe the concept of Smart City and the Internet of Things (IoT). Second, we identify the challenges of IoT in a Smart City, which can be regarded as scalability and interoperability. Third, we identify the criteria to address these challenges. Fourth, we evaluate a number of architectural approaches based on the criteria. Fifth and final, we propose our novel architectural approach that addresses the challenges. We validate our novel architectural approach in the Volvo Ocean Race case study and an expert validation.

Our main finding is that our proposed architectural approach allows Smart Cities to implement IoT solutions in a scalable and interoperable manner. Our approach includes an agnostic gateway that effectuates interoperability of IoT. Next, we also provide an approach to auto discover objects, which minimizes the human intervention of managing objects in a Smart City. Lastly, we provide an approach through virtualization and clustering techniques that guarantees scalability in terms of performance and availability.

Contents

List of Tables

List of Figures

Chapter 1: Introduction

The central topic of the study is Smart City. The popularity of this concept is growing at a rapid pace. Yet, the challenges are growing as well. In this study, we aim to address the challenges in the area of IoT and provide an architectural approach. The main research question is *"To what extent can IoT challenges in Smart City be addressed by means of an architectural approach?"*. The approach of this study is to identify main challenges, define criteria to address these challenges and evaluate whether a set of current architectural approaches are capable of satisfying these criteria. Based on the findings we will formulate an architectural approach.

1.1 Introduction

In this chapter, we will introduce the main topic of the thesis. First, we will provide background information where we describe the relevance of the topic. Second, the research questions are defined that serves as the fundament of this thesis. Next, the objectives and methodology are described. The methodology section clarifies how the objectives will be reached. We will end this chapter with an outline of this thesis.

1.2 Background

The central topic of this study is Smart City, which can be regarded as a popular phenomenon nowadays. This concept allows cities, with help of innovative technologies, to confront urban challenges such as air pollution and urban density. Many governmental institutions are interested and eager to realize smartness in their city. Next, the academic world has also shed light on this subject and presented an extensive array of literature. The rise in popularity has increased the implementations of Smart City and consequently created a set of challenges. Novel concepts, such as Smart City, generally come with significant challenges that require comprehensive understanding for being alleviated.

In this study, we focus on the challenges related to the deployment of the Internet of Things (IoT). According to various studies, the current deployment approach is not sufficient for the context of Smart City. Several studies exhibited the need for a different architectural approach to achieve the full economic value of a Smart City.

1.3 Research Question

The main research question of this study is as follows:

- To what extent can IoT challenges in Smart City be addressed by means of an architectural approach?

The following questions are formulated to answer the main question:

1. How is IoT involved in Smart City and what are the challenges?
2. What criteria are required to address the IoT challenges in a Smart City?
3. Are existing architectural approaches capable of satisfying the criteria and if not, can a new architectural approach satisfy the criteria?
4. Assuming the architectural approach can satisfy the criteria, can we evaluate it in form of a case study?

1.4 Research Objective

In this study, we aim to provide an architectural approach that is capable of addressing the IoT challenges in a Smart City. This approach should help stakeholders to implement IoT solutions as effective as possible. We believe that IoT has a prominent role in Smart City and will have a certain impact on the effectiveness. Therefore, proper adaption of IoT is a key success factor in this concept. The architectural approach should allow cities to use the full the economic value of a Smart City.

1.5 Research Methodology

As described in the research objective, our aim is to provide an architectural approach. This approach will be provided based on collected data from desk research and interviews. The collected data will allow us to build a theory, in the form of an architectural approach. This research approach can mainly be regarded as an inductive research rather than a deductive research where a theory is tested.

In the first part of the study, we will provide the common outline of each scientific study, namely a literature review of the concept in terms of definitions, current situation, developments and so on. The goal of this section is to create a thorough understanding of the context of this study. We will derive scientific literature from Google Scholar and the library database of the University of Leiden.

In the second part, we will describe how IoT in involved in Smart City and what challenges are present. Again, a literature review will be performed. In addition to that, interviews may also be used to get a practical perspective on this matter and validate the findings of the literature review.

The next step is to define criteria how the challenges can be addressed. These criteria will be derived from a literature review as well. Such criteria may well point to an architectural method, such as SOA, or a specific type of API. The result of this phase is a framework that will be used for comparison purposes.

The framework, derived from the previous phase, will serve as a basis to analyze and evaluate a number of architectural approaches. The strengths and weaknesses will be assessed and an analysis will be performed whether the architectural approaches are in accordance with the criteria and whether it is applied in the most optimal way in the context of Smart City. Given the fact that this study is inductive, the course of the study may be changed during the research based on the findings. So, the result of this phase determines the course of subsequent phases. When it appears that the architectural approaches are not sufficient for the IoT challenges in the Smart City, a new architectural approach will be provided based on the criteria. In other cases, the next phase will be entered. The subsequent phase is dedicated to a case study where the appropriate architectural approach will be validated in a certain context. This has a significant influence in the credibility of the architectural approach. It is, however, imperative that the contextual setting must have the same characteristics of a Smart City. The last phase of the study will be dedicated to an evaluation of the case study. Recommendations and modifications are provided when necessary and suggestions for further research are formulated. Figure 1 illustrates a schematic overview of the study. In addition to that, the deliverables of this study are depicted in Table 1 below. An elaborated version of the deliverables can be found in Appendix I.

Research Question	Deliverable
How is IoT involved in Smart City and what are the challenges?	Description of a Smart City, IoT and the related challenges.
What criteria are required to address the IoT challenges in a Smart City?	Structure of the comparative framework and constraints.
Are existing architectural approaches capable of satisfying the criteria and if not, how can a new architectural approach satisfy the criteria?	Comparative framework, and if applicable, a novel/adjusted/combined architectural approach.
Assuming the architectural approach can satisfy the criteria, can we evaluate it in form of a case study?	Case study where the proposed architectural approach is validated

Table 1. Short version of the deliverables

1.6 Thesis Outline

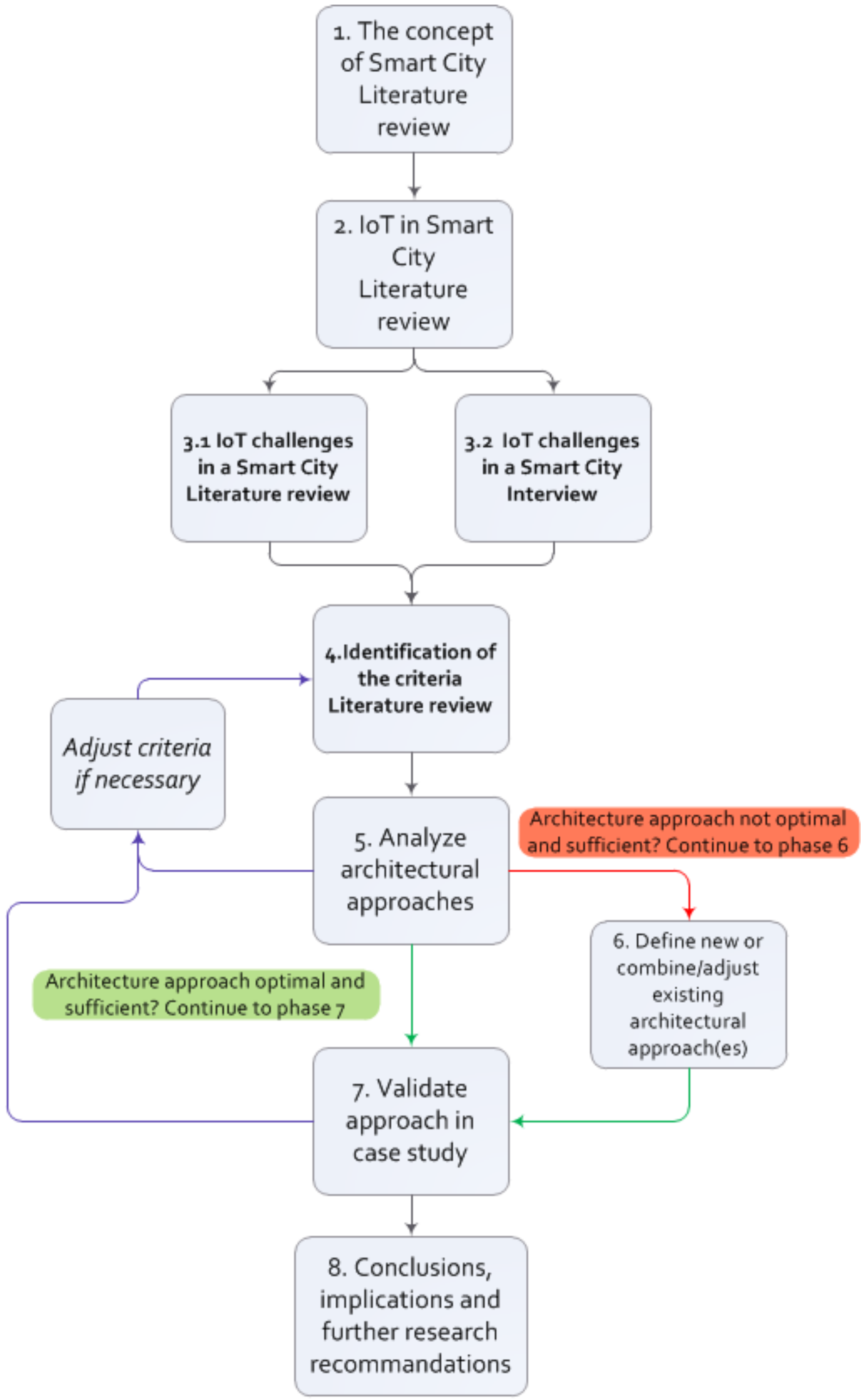

Figure 1. Research framework

The rest of the thesis is structured as follow:

Chapter 2 – *Smart City and IoT* – in this chapter, we will provide a literature review of the Smart City and IoT. A thorough overview of Smart City including the definitions, current situation, developments, application throughout the world will be provided. In addition to that, the involvement of IoT will be described as well as the coherent challenges.

Chapter 3 – *The criteria to address IoT challenges in a Smart City* – in this chapter, we will identify the criteria that address the challenges. In the end, we will provide a framework of the criteria that will be used in the analysis of the architectural approaches.

Chapter 4 – *The analysis of architectural approaches* – in this chapter, we will identify a number of existing architectural approaches and analyze them based on the framework derived from the previous chapter.

Chapter 5 – *The definition of a new architectural approach* – this chapter will provide a new architectural approach when the analyzed approaches are not capable of satisfying the criteria.

Chapter 6 – *Case study* – we will apply the architectural approach from the previous chapter in a case study. A case study is an effective method to validate the architectural approach in a contextual setting. The results of the validation will be used for optimization purposes.

Chapter 7 – *Conclusion* – in the last chapter, we will provide a conclusion of this study. The main conclusion, discussion and limitations and future research will be presented.

Chapter 2: Smart City and IoT

The aim of this chapter is to answer the research question: "*How is IoT involved in Smart City and what are the challenges?*" We have identified scalability and interoperability as main challenges in Smart City since the application of IoT in Smart City will significantly grow (scalability) and city domains have to work in close collaboration to realize the full economic value (interoperability). We argue that an architectural approach is an adequate mean to address these challenges.

2.1 Introduction

In this chapter, we will start with a description of the concept of Smart City and IoT. We will provide three brief cases how Smart City is implemented in order to give an impression how IoT acts as an enabler. Next, we will zoom into the challenges of IoT in a Smart City and will identify the two main challenges on which we will focus in the rest of the study.

2.2 Smart City

Smart City is a concept that is quite popular nowadays. As we have described in the introduction, many governmental institutions are interested in this concept and are eager to realize it in their city. The academic world has also shed light on this subject and presented an extensive array of literature. Yet a clear and consistent understanding of this concept is still missing among scholars and practitioners (L. G. Anthopoulos et al., 2016). This can mainly be underlined by the involvement of practitioners in various disciplines, which have its own perspective on this matter. Some literature references use different terms such as Digital City and Intelligent City. The terms are in general nearly the same but there is, however, a difference. Digital city can be described as "*A digital city is substantively an open, complex and adaptive system based on computer network and urban information resources, which forms a virtual digital space for a city. It creates an information service marketplace and information resource* *deployment center"* (Li Qi & Lin Shaofu, 2001). Ojo argues that Intelligent City lays lies between Smart City and Intelligent City and describes it as "*Intelligent city is conceived as a real city endowed with collaborative, learning, and innovation environments or spaces*" (Ojo et al., 2016). We can argue that Digital City emphasizes on the IT infrastructural part and Intelligent City on the knowledge sharing part by using IT infrastructure as a mean to realize it. The use of various terms in the literature is also a source of confusion regarding this concept.

The concept of Smart City is evolving and the construction of a consistent definition is in progress. Cocchia conducted a systematic literature review on this subject and performed a definition analysis (Cocchia, 2014). The outcome of this analysis is depicted in Table 11, in Appendix II. Table 12 illustrates the analysis of the definitions. The outcome of this analysis is that the main elements of the definitions are citizens/life quality, information technology, infrastructure and environmental impact, respectively. Life quality seems to be the most important element followed by Information Technology, which underlines that Smart City is a combination of the Urban and Information Technology discipline. The definition that will be used in this study is: "*A smart city is a well-defined geographical area, in which high technologies such as ICT, logistic, energy production, and so on, cooperate to create benefits for citizens in terms of well-being, inclusion and participation, environmental quality, intelligent development; it is governed by a well-defined pool of subjects, able to state the rules and policy for the city government and development*" (Dameri, 2016). This definition is chosen since it includes all the important elements of Smart City.

Smart City throughout the decades

It is important to understand how this concept has evolved over the years. Therefore, we provide a brief description on this matter. Three events mainly triggered the Smart City phenomena. The first event is the growing population in urban areas. As can be seen in Figure 2, for the first time in history, more people are living in urban areas rather than rural. This trend is expected to continue and will grow to 6.500 million urban population in 2050 (United Nations, 2014).

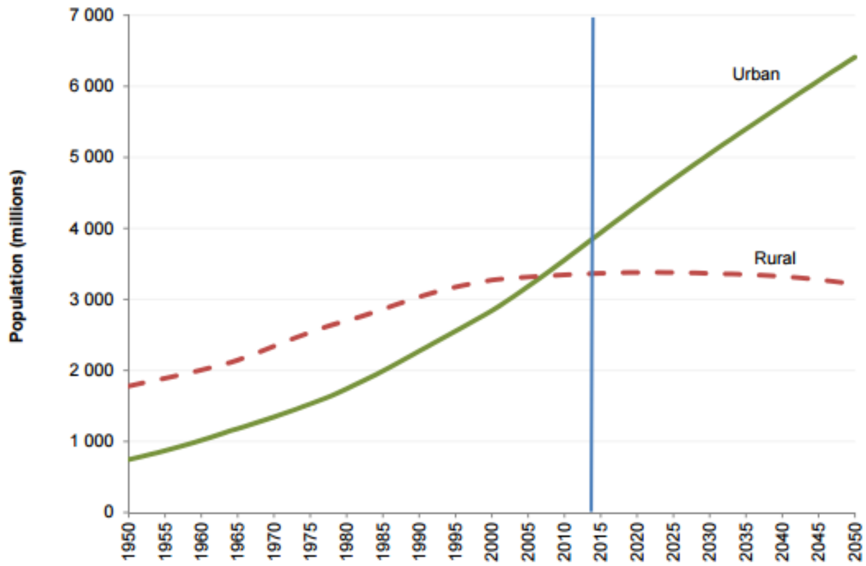

Figure 2. The world's urban and rural populations, 1950-2050 (United Nations, 2014)

This growth has resulted in several challenges for governments. Such as increase in traffic jams, parking problems, CO_2 emission, waste disposal and demand for water and energy resources (Cocchia, 2014; Ojo et al., 2016). As a result, this can badly impact the life quality of urban citizens. Therefore, the growing urban population triggered governments to look beyond the traditional instruments and use a more effective approach to cope with these challenges in a sustainable manner.

The second event that triggered the attention was in the late nineties. As can be observed in Figure 2, the growth of the urban population accelerated significantly in the late eighties. Many countries and institutions were apprehensive about this event and initiated, therefore, amongst other dozens of climate issues, the Kyoto protocol on 11 December 1997. The Kyoto protocol is an international agreement, signed by 192 parties, to reduce the CO_2 emission by five percent against the levels of 1990. This percentage was increased to eighteen percent in 2013 (United Nation Framework Convention on Climate Change, 2016). The agreement forced countries to implement policies and measures to decrease the CO_2 emission. Next to the Kyoto protocol, in the course of the years, a number of agreements, such as the Paris agreement, have been signed by countries to encounter the climate challenges. These events clearly show that climate issues are on the top of world leaders agendas and forces to look beyond the traditional instruments to obtain the agreed objectives.

The third event is the acceleration in the technological era. The technology field can be regarded as an incredibly expeditious discipline in the last decade. The introduction of the internet, in the very beginning of the 21st century, brought the world closer and resulted in a more globalized world. The ICT infrastructure components such as wireless networks, broadband networks, sensors and routers became robust, reliable and cheaper. At the same time, the announcement of the iPhone in 2007 by Steve Jobs has changed the life of people in a certain way. Nowadays, the number of smartphone users hit roughly 2.1 billion and will grow steadily in the following years (Statista, 2014). Internet Service Providers has therefore intensively invested in infrastructural networks to serve the needs of people by connecting them practically 24/7 to the internet anywhere. Besides this, the processing power has also increased significantly in the last decades. Leading chip manufacturers, such as Intel, produced increasingly powerful chips throughout the years. It seems that Intel is following the law of Gordon Moore, which was the co-founder of Intel. The Moore's law states that the computing power of chips will double every two years and will grow exponentially (Gordon E. Moore, 1965).

The increased computing power has opened many doors in the field of computer science and analyses. The increase in computing power made it possible to compute a large set of data in a shorter timeframe. It is nowadays even possible to analyze real-time data. The improvements in the computing power of chips have resulted in many innovative concepts, products and services. Such as, Cloud Computing, Big data, Artificial Intelligence, IoT, and so on. These concepts have evolved in the past years in sophisticated products and services that are adopted by many people and companies.

The accumulation of the three events, described above, has resulted in the creation of the Smart City concept. It first began with the growing population in urban areas and the increase of CO_2 admission in the world. This has consequently raised the awareness of governments and institutions to deal with these challenges. Many scholars and governments agreed that a more creative approach was needed rather than the traditional approach, which was not sufficient to cope with these challenges. The rapid pace of innovative technologies allowed governments to tackle the urban challenges, which has resulted nowadays in the concept of Smart City. Currently, there are more than 800 papers available on this subject (Ojo et al., 2016). This is showed in the graph depicted in Figure 3.

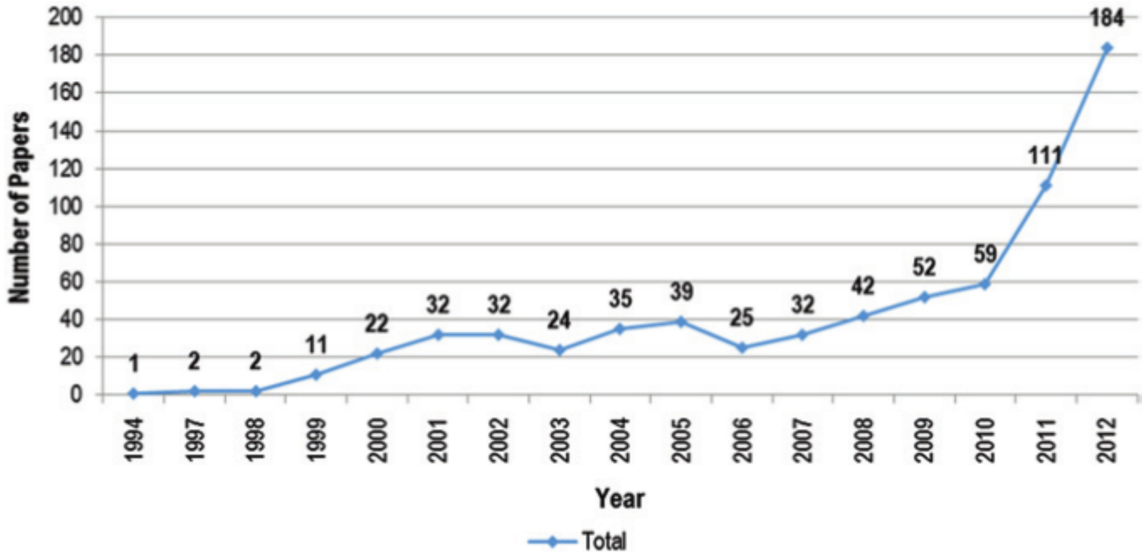

Figure 3. Number of Smart City papers in the last decades (Cocchia, 2014)

Smart City functionalities

The section above provides an analysis of the definition and introduction of Smart City. On top of that, there is some confusion about the actual functions of Smart City. Therefore, this section provides a description of the functions derived from the literature. It is hard to evaluate a Smart City on its performance and rank them. Giffinger was the first scholar that addressed the needs to measure it and identified six dimensions to categorize Smart City functionalities (R. Giffinger, 2007). A few years later, Boyd Cohen an urban strategist and professor, had to deal with this difficulty as well and developed a framework named Smart City Wheel (B. Cohen, 2014). This framework defines six main functionalities with each a set of indicators. The six main functionalities are only a part of the study since the indicators are not relevant. The main functionalities are Smart Economy, Smart Government, Smart People, Smart Living, Smart Mobility and Smart Environment. The Smart City Wheel is depicted in Figure 4. We use these functionalities as a reference to appoint the working areas of a Smart City.

Smart Economy: Stimulates the growth factors of the economy such as productivity, innovation and entrepreneurship.

Smart Government: Enhance the government function by being providing more services, being transparent and enable open public information.

Smart People: Stimulates people's abilities and learning performance by the promotion of the growth mindset rather fixed mindset, flexibility and creativity. A mean to realize this could be through the participations of an online platform. (Central Policy Unit Hong, 2015)

Smart Living: Improve the living environment and quality of citizen's life by making use of innovative technologies such as Big Data and Internet of Things. For instance, the smart heating system that allows people to turn on/off the heater through a smartphone.

Smart Mobility: Improve the cities' transport system including public transport, cycling and walking (Central Policy Unit Hong, 2015). For instance, smart traffic management system and data analysis of traffic flow in a city.

Smart Environment: The main purpose is to provide a sustainable environment by making use of Smart solutions such as the optimization of buildings, implementation of air quality sensors and data analysis of the distribution of Co2 emission.

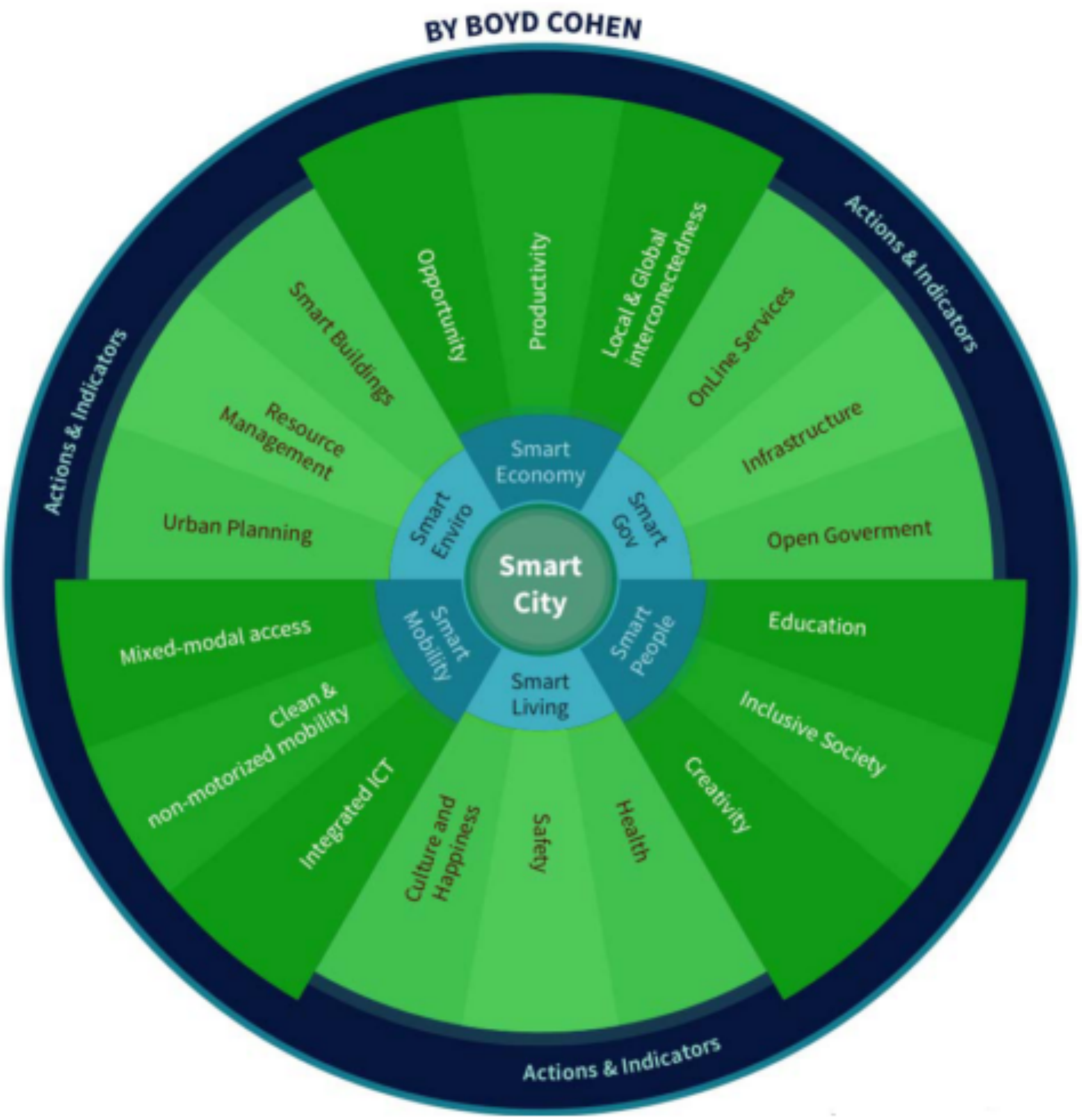

Figure 4. Smart City Wheel (B. Cohen, 2014)

2.3 IoT in Smart City

We have provided a brief description of the concept of Smart City in the previous section. The definition and history is described as well as the main functionalities based on the Smart City Wheel of Cohen. We are interested in the ICT part and in particular the Internet of Things involvement in this concept. Together with Big Data, IoT forms the main technology driving the accelerating adoption of Smart Cities. Therefore, we focus on describing how these two concepts are related.

Brief history

The concept of IoT was introduced almost a decade ago by Kevin Ashton, a British technology pioneer of the MIT. He introduced the concept of creating an internetwork and allow communication between objects. At that time, Kevin Ashton's team was developing a global open standard system for sensors like RFID to stimulate the communication between objects. However, the standardization of the sensor system was not enough to realize the concept. Further improvement and research were needed in the field of communication. Such as, wireless communication, internet infrastructure, the amount of IP addresses, and so on. These hurdles have been solved and improved in the last decades. For instance, IPv6 allowed assigning a large number of IP addresses to devices.

Nowadays, IoT has become a promising technology that has raised the interest of many companies and individuals as well. There are various definitions in the scientific field of IoT. We will use the definition of the International Telecommunication Union (ITC). They define IoT as "*a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies"* (International Telecommunication Union, 2012).

The application of IoT in Smart City

The benefits of IoT can be applied in various industries from the public sector to the industrial sector. In this study, we aim at the contextual setting of a Smart City. As described in the previous section, IoT has a significant contribution in the developments of Smart City by allowing communication and interaction of a wide range of objects via the internet (Zanella et al., 2014). The objects can be regarded as items that are intensively used in the daily life of people. Such as thermostats, garbage cans, parking meters, traffic lights, and so on. IoT allows cities to obtain effectivity and efficiency in daily activities of citizens. In our view, the best way to describe the application of IoT in Smart City is by providing a set of cases. The first case is NYC followed by Singapore and Barcelona.

New York City

New York City (NYC) was one the first big city in the US that implemented Smart City solutions in partnership with the major technology firm Cisco. Currently, it is one of the pioneers of Smart City and has been awarded as 'Best Smart City of 2016' at the Expo World Congress in Barcelona. These strategies resulted in the following Smart solution implementation: LinkNYC, Smart Indoor Lighting, Wireless Water Meters, Responsive Traffic Management, Traffic Light Priority, Smart Waste Management, Water Quality Monitoring, Air Quality and Real-time Gunshot Detection. Three of these implementations are elaborated below.

LinkNYC: This initiative is one of the flagships of NYC where old-fashioned payphones are transformed to smart Kiosks with many functionalities. The key functionalities are: Wi-Fi connectivity, device charger, access to maps and city services and make free phone calls in the whole US. The Kiosk, also called Links, are used more than 21 million times since September 2016.

***Real-time Gunshot Detection*:** This system aims to detect gunshot in the city. Hundreds of sensors are installed on the rooftops in the city that identifies gunshots within 25 meters of its location. The sensors generate an alarm for validation and sends it to the New York Police Department, within a minute, for further actions

Singapore

Singapore is a nation that has been interested in this concept before it was born and taking the Smart City concept to a next level, namely Smart Nation. In the early nineties, the city was already experimenting how IT can be combined with urbanization (Central Policy Unit Hong, 2015).

Virtual Singapore: One of the projects under this program was the implementation of sensors and cameras that collects data from air quality, crowd movements and traffic flow to monitoring public places. The collected data is fed to the platform 'Virtual Singapore', which is a promising platform that provides a virtual representation of the island. This platform is useful for running simulations based on real-time data. Singapore became one of the most successful Smart City in Asia with these projects.

Barcelona

Barcelona is one of the main cities in Europe, next to Copenhagen and Amsterdam, that pursues the objective to become a Smart City and can be regarded as a pioneer of Smart City due to the introduction of the 22@Barcelona district.

Fastprk: One of the projects that is piloted in the district is Fastprk. This is a system that helps drivers to find a parking space and helps a city to deal with parking problems. Fastprk had implemented 1000 sensors in 2012 and reached the number of 50.000 sensors in 2014.

Barcelona Lighting Masterplan: This project installed more than 1000 environmental friendly LED lampposts that also provide Wi-Fi connectivity throughout the city and collects air quality data.

The applications presented in the section above shows in a nutshell how IoT enables innovative solutions for Smart Cities. For instance, Singapore is taking the IoT implementation to the next level by collecting data of the deployed sensors and fed it into a platform that provides a virtual representation of the island. The number of application presented in the paragraphs above are only a tip of the iceberg. The IoT applications in cities are growing on a daily basis.

2.4 Challenges of IoT in Smart City

In the previous section, we have provided some examples of cases to show how IoT is applied in a Smart City. In this section, we will focus on the involved challenges. The literature has provided some valuable insight and identified several challenges. However, we are focused on the challenges related to IoT. As can be observed in the cases from the previous section, the IoT implementations serve various disciplines in a city and have wide coverage ratio. This is a positive characteristic of the current state by offering these disciplines new possibilities. Yet it entails a new dimension of challenges. These challenges will be described in this section.

The context of Smart City and IoT

The context of a city can be regarded as a complex system of various domains that are closely interrelated (Lyle & Harrison, 2014). Each domain has its own perspectives, ICT systems, budget, system owners and challenges. In the case of Smart City, these domains can be regarded as a collection of independent organizations that have a common goal. Some scholars labeled this environment as a system of systems. In case of Smart City, these independent organizations have a common goal to transform the city into a Smart City. However, in order to make this transformation seamless and efficient, these domains have to cooperate and collaborate intensively, otherwise, this transformation will be inefficient, costly and unlikely (IEC, 2014).

Placing IoT in this context reveals the novelties of the concepts. The context of Smart City is relatively new in the era of IoT. According to Sanchez, the majority of IoT deployments are applied in a rather different context (Sanchez et al., 2014). Currently, most of the IoT deployments are exercised in a particular domain. There are, for instance, companies specialized in RFID products in transport domains and companies specialized in sensors for air quality in environmental domains. This indicates that the current IoT deployments are domain tailored and optimized to the context in which they have been tested (Sanchez et al., 2014). As a result, a diverse set of standards, protocols, software and devices have been emerged during the course of the years (Poudel, 2016; Van den Abeele et al., 2015). These findings are in line with the study of the British Standard Institution. Many IoT suppliers offer products and services with their own set of standards and protocols that are compatible with their specific domain requirements. Consequently, almost 100 standards and protocols are being used in Smart City (BSI, 2014). The current state of deployment has, therefore, impact in the realization of a Smart City and can eventually lead to a fragmentation of IoT solutions throughout the whole city. Fragmentation is known for significant implications in terms of scalability and interoperability (IEC, 2014; Poudel, 2016), which is regarded as an imperative attribute in the deployment of IoT on a larger scale, such as Smart City. The next section will zoom in this particular set of challenges.

The fragmentation of IoT solutions in a Smart City

The section above describes the friction of the context of Smart City and the current domain specific deployment of IoT. This has resulted in the fragmentation in IoT solutions that can lead to significant implications in terms of scalability and interoperability.

In the literature, the wide range of standards, protocols, devices and software is regarded as a heterogeneous substance (Elkhodr et al., 2016; Hussain, 2016; Van den Abeele et al., 2015; Zanella et al., 2014). Zanella et al. conducted a study of IoT challenges and regarded the non-interoperability of heterogeneous systems as a major concern (Zanella et al., 2014). The main reason for this is the current state of the market that consists of various (big) players which are trying to push their standard forward and, as a consequence, increasing the non-interoperability between IoT systems. The interoperability of IoT systems is an essential element in the success of a Smart City. According to a study of McKinsey, 40 percent of the economic value can be achieved by making IoT systems work together (McKinsey & Company, 2015). The lack of interoperability has, therefore, severe impact in terms of the achieving the full potential value of IoT in a Smart City economic value (Poudel, 2016).

In addition to that, the lack of interoperability has an adverse effect on scalability since these two attributes are closely interrelated. Severe implications can emerge when IoT solutions are deployed on a larger scale without having the ability to interconnect seamlessly. This line of reasoning has been an interest in the scientific field and a number of studies provided several ideas to address these challenges. Lopez et al. mentioned: *"the fast evolution of the IoT technology is defining new architectures challenges in term of scalability, allocation of resources and efficient discovery"* (Lopez et al., 2013).

In addition to that, Elkhodr et al. suggested a need for a new approach: "*IoT requires standards to enable horizontal platforms that are communicable, operable, and programmable* *across devices, regardless of their make, model, manufacturer, or industry applications*" (Elkhodr et al., 2016). The IEC describes this approach more specifically in the context of Smart City, as: "*A truly "smart" city requires horizontal integration as well as creating a system of systems capable of achieving considerable increases in efficiency and generating new opportunities for the city and its citizens*" (IEC, 2014).

Based on these studies, horizontal integration appears to be a convenient approach to cope with the heterogeneous, scalable and interoperable challenges in the context of a Smart City. Horizontal integration can be regarded as a form of architecture that serves the needs of multiple domains rather than specifically a single domain. This concept is illustrated in Figure 5.

We have developed the model in Figure 5 based on the matrix organizational philosophy. The philosophy was inspired by large manufacturing companies where a number of domains were responsible for the end-product such as a cars or airplanes. Each domain had its own responsibility in terms of assembling a part of the whole product. The responsible team reported directly to the domain manager, which had the overall responsibility. As soon the domain produced their part, it would go the next domain. We can regard this as a chain of activities where several domains have their set of tasks and responsibilities. In the course of the years, people were observing that there was a lack of integration between the domains where managers were only focused on their part of the whole process. This had eventually resulted in poor performance, lack of integration and many inefficiencies (Stuckenbruck, 1979). As a result, the matrix organization was introduced that is, nowadays, widely implemented in many organization. This type of organization has introduced production managers that are responsible for the whole product line instead of only one part of the product. This had eventually resulted in a more efficient organization since the integration of domains were much smoother and there were no islands of domains anymore.

For that very reason, we believe that in order to enable integration of domains that are operating in complex environment, the matrix organization philosophy should be the inspiring factor to realize this.

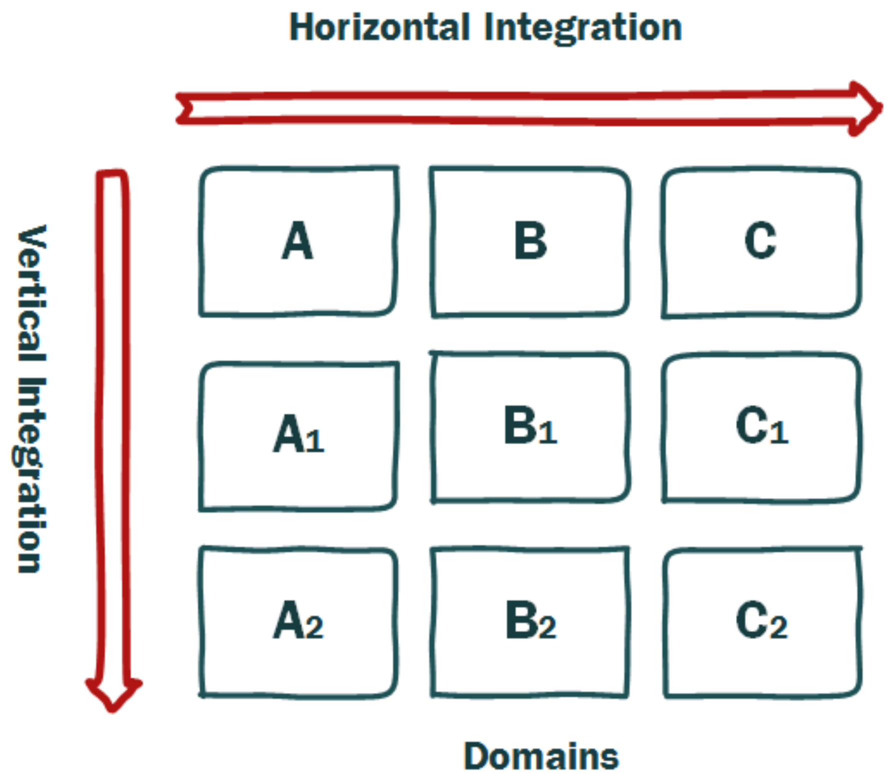

Figure 5. Vertical and horizontal integration

The literature on IoT challenges in Smart City

The previous section describes the deployment challenges of IoT in the context of Smart City. The current deployment of IoT is not sufficient for Smart City and entails some severe challenges. Among the variety of challenges, this study concentrates on scalability and interoperability challenges of IoT solutions. Several studies have done some work in this area and suggested insight and approaches to cope with these challenges. This section describes the current state of literature regarding this subject.

The literature provides clear arguments why the current deployment of IoT is not sufficient for large contexts, such as Smart City. Some studies elaborated this argument and provided architectural approaches and frameworks. Apart from the scientific field, there are a number of initiatives from commercial companies, standardization organizations to governmental institutions that promote the horizontal integration approaches, such as the ISOs 268/SC on smart community infrastructures, IBMs Intelligent Operation Centre and the IoT Cloud Platform Stack from Eclipse. Lopez et al. acknowledges the variety of IoT architectures and describes this as: *"Recently, several projects have designed different IoT architectures depending on their specific applications and requirements. Due to a large heterogeneity of applications and requirements, the architecture approaches differ between the projects resulting in more or less different components and protocols. The IERC (Internet of Things European Research Cluster) recognizes that the architectures diversity is the main factor limiting the advance of the IoT technology"* (Lopez et al., 2013). As described by Lopez et al., several studies provided novel architectural approaches in the context of a Smart City. Yet the majority of these studies have different perspectives on that matter, which has resulted in architectural approaches that are only valid in a particular domain. We argue that these set of approaches are not dealing with the challenges of IoT in a Smart City but rather isolating it for a specific domain.

Moreover, Enterprise Architecture in combination with SOA (Service Oriented Architecture) serves as a strong interest in the literature, such as (L. Anthopoulos, 2015; L. Anthopoulos & Fitsilis, 2014; da Silva et al., 2013; Kakarontzas et al., 2014; Le Vinh et al., 2015). The main focus of these approaches concentrates on how ICT solutions can be implemented as effective as possible by creating alignment between the architectural layers of a Smart city such as city domain layer, application and technological layer. We regard this kind of approaches as vertical integration of the layers in the architecture, as shown in Figure 5. We argue that the interoperability and integration challenges consist on mainly the layers itself rather than the integration of vertical layers.

Besides this, Santana et al. conducted a research where 23 software platforms are evaluated based on relevant criteria derived from the literature (Santana et al., 2016). The most cited challenges in the literature are interoperability and heterogeneity, respectively. However, scalability seems to be a less important element since only three studies addressed this as a severe challenge. This is a cause for concern considering the significant challenges in the growth of IoT and thereby the support of a large range of devices, sensors, users, data, and so on (Lopez et al., 2013). Moreover, as depicted in Table 2, the majority of the platform only serves one or two domains. There is no platform that is applicable in all domains. This evidence is in line with the study of BSI and Lopez, which argues that many IoT suppliers offer products and services that only serve the need for a specific domain (BSI, 2014; Lopez et al., 2013). Table 2 reveals that this is also valid for software platforms that serve for integration purposes. As mentioned in the previous section, this state can eventually lead to a fragmentation of IoT solutions and can have implications in terms of scalability and interoperability for Smart City as a whole.

	City Sensing	Traffic Control	Air Pollution	City Dashboard	Health Care	Safety	Disaster Prevention	Energy Management	Waste Management
GAMBAS		X							
SmartSantander	X	X	X						
Padova Smart City	X			X					
OpenIoT	X								X
WindyGrid	X	X	X		X	X			
ClouT	X	X			X	X	X		
Scallop4SC								X	
Number of Instances	5	4	2	1	2	2	1	1	1

Table 2. Domains of Smart City Systems (Santana et al., 2016)

Scalability and Interoperability as a challenge of IoT in Smart City

The previous section provided a brief analysis of the relevant literature. The main outcome of this section is that a large set of literature is dedicated to Enterprise Architectural approaches. These approaches are, however, not relevant for this study since they are focused on vertical integration between architectural layers. A relative smaller set of studies is dedicated to horizontal integration approaches. Santana et al. performed a thorough analysis and provided clear insight of the current developments as well as the implications. First, the study argues that, currently, scalability can be regarded as a less important element since only a handful studies address this as a severe challenge. Second, the evaluated software platforms are not sufficient in providing a horizontal integrated approach that is suitable for all Smart City domains.

As described the previous section, the studies of (Elkhodr et al., 2016; IEC, 2014; Lopez et al., 2013) addresses the need for a horizontal integrated approach to cope with the heterogeneity of Smart City. The implications of not having such an approach can impact in terms of scalability, interoperability, efficiency and effectiveness. In addition to that, the study of McKinsey (McKinsey & Company, 2015) described that 40 percent of the economic value could be achieved by making IoT systems work together, which implies that the current state of deployment will not be sufficient to get the full potential of IoT in Smart City.

These studies are not in line with the platforms that are analyzed by Santana et al. (Santana et al., 2016), where the most only serve one or two domains and where a handful studies only address scalability. Therefore, we argue that the literature lacks in providing a comprehensive understanding how horizontal architectural approaches across multiple domains of Smart City, can address the interoperability and scalability challenges and thereby achieve the full potential of IoT in Smart City. A horizontal integrated approach focused on addressing all these challenges has not been provided yet in the literature. This allows us to conduct a study on this matter.

2.5 Conclusion

Our main aim of this chapter was to answer the research question: *How is IoT involved in Smart City and what are the challenges?* IoT serves as one the fundamental technology in Smart City and allows cities to achieve effectivity and efficiency in daily activities of citizens. However, there are some frictions in the concept of IoT and context of Smart City that resulted in various challenges. Among the challenges, we have addressed scalability and interoperability as an important challenge and will focus on this during the rest of the study. The next paragraph provides an elaborated summary of this chapter.

In this chapter, we first started to explain the fundamentals of Smart City by providing the definition, outlining the main functionalities based on the Cohen's Smart City Wheel and describing the evolution throughout the decades. Since we are interested in the ICT part of Smart City, we also explained the fundamentals of IoT by providing some cases where cities make intensive use of this concept. The main outcome of this part is that IoT has a significant contribution in the developments of Smart City by allowing communication and interaction of a wide range of objects via the internet. However, the combination of the concepts (IoT and Smart City) have some frictions. The majority of IoT deployments are exercised in a rather different context. This has resulted in a large number of IoT standards, protocols, software and devices that are applied in a Smart City. The wide application of IoT by several city domains has resulted in a certain degree of fragmentation and heterogeneity, which can have, according to several studies, significant implication in terms of scalability and interoperability. The literature acknowledged these challenges and provided some architectural approaches. Santana et al. performed a thorough analysis and provided clear insight of the current developments as well as the implications. First, the study argues that, scalability can be regarded as a less important element since only a handful studies address this as a severe challenge. Second, the evaluated software platforms are not sufficient in providing a horizontal integrated approach that is suitable for all Smart City domains. Therefore, we can argue that the literature lacks in providing a horizontal architectural approach, in form of e.g. a platform, across multiple domains of a Smart City, which addresses the interoperability and scalability challenges for achieving the full potential of IoT in Smart City.

Chapter 3: The criteria to address IoT challenges in Smart City

We aim to answer the research question: *"What criteria are required to address the IoT challenges in a Smart City?"* The main outcome of this chapter is that there are a various number of protocols and standards in the IoT ecosystem. In order to create interoperability, we should embrace all these standards and protocols rather than exclude them. An architectural approach should incorporate mechanisms to realize this. Moreover, we have identified auto discovery and high availability as imperative features to realize scalability.

3.1 Introduction

In this chapter, we will identify the criteria that address the IoT challenges in a Smart City. The identification of the criteria is performed as follow. First, we will analyze the standards and protocol on the technical level, which can be regarded as the lower levels of the OSI model. Second, we will analyze the standards and protocols on the application layers, which can be regarded as the upper layers of the OSI model. Next, we will identify features that are imperative for a scalable and interoperable architectural approach. At the end, we will provide a comparative framework which consists of constraints.

3.2 Standards and protocol in the IoT era

In this section, we will describe which standards and protocols are mainly used in the era of IoT. In order to get a clear view, we will plot the standards and protocols on the layers of the OSI model. First, we will start at with the technical layer that consists of the physical, network, data and transport layer. Second, the application layer will be described that consists the session, presentation and application layer.

Technical layer

As described in the intro of this section, we first have to analyze which standards and protocols are used in IoT. The overview of the analysis is depicted in Figure 6 where we have plotted the standards and protocols on the logical layers of the OSI model. We will only describe the main elements of this layer. Additional information is provided in Appendix III.

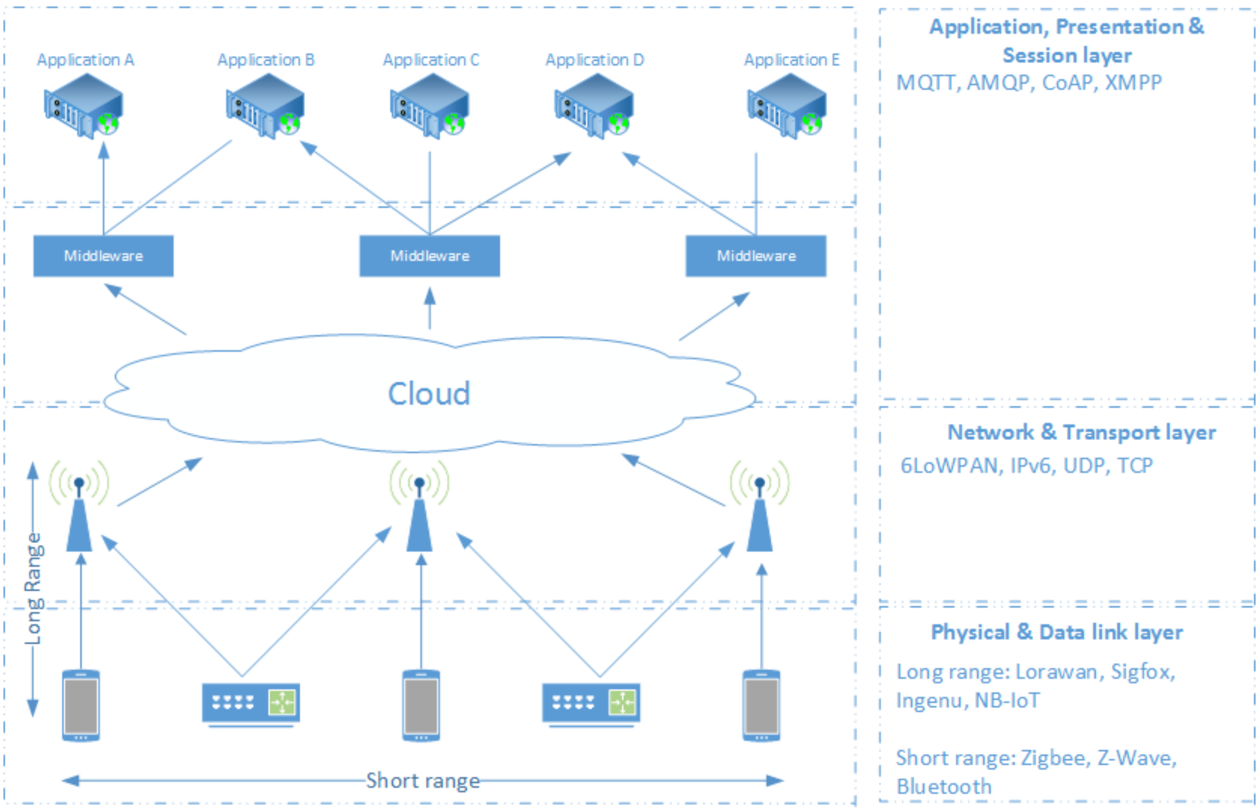

Figure 6. Overview of standards and protocols used in IoT

Starting with the physical and data link layer, there are two types of standards that enable the interconnection of objects. On the one hand, there are short-range standards, such as Zigbee and WirelessHART, that are mainly used in environments where objects are placed in a range within 100 meters. On the other hand, there are standards that enable the communication of objects on a longer range. Both short and long-range standards and protocols are widely used in a Smart City. We will only analyze long range protocols since the connection of short range protocols to the cloud is mostly managed by a local gateway (such as a router), which makes this structure straightforward. Hence, we have provided a description of these standards and protocols in Appendix III.

Long range standards and protocols

The existing cellar networks were not compatible with smart objects, which requires efficient energy consumption. As a result, LPWAN (Low-Power Wide Area Network) was designed to support low-energy objects as well. A number of standards and protocols have been developed in the course of the years. Nowadays, there are mainly two major players in the market, named LoraWan and Sigfox, which is already implemented in several cities as well as whole countries (Zanella & Zorzi, 2016).

Another standard that is gaining popularity is NB-IoT, which is quite different than LoraWan and Sigfox in terms of technology. NB-IoT is an open cellular technology standardized by 3GPP (3rd Generation Partnership Project). It is an extension of the existing LTE network to support low energy and bandwidth devices in the IoT era. To that end, service providers can implement this standard with just a software upgrade. Unlike Sigfox and LoraWan, NB-IoT uses a licensed spectrum that is managed by a telecom operator. According to Gartner, NB-IoT will likely dominate the LPWAN space in a couple of years (Gartner, 2016).

Standards and protocols regarding to IoT scalability and interoperability in a Smart City

In the previous section, we have provided a description of the standards and protocols used in the datalink layer. In this section, we will analyze the standards and protocols regarding to scalability and interoperability. We will analyze the long-range standards and protocols based on five aspects. Namely, network topology, proprietary, spectrums and network type.

	LoraWan	Sigfox	NB-IoT
Network topology	Stars-of-stars	Star	Star
Proprietary	Yes*	Yes	No
Spectrum	Unlicensed	Unlicensed	Licensed
Network type	LPWAN (open cloud)	LPWAN (Private cloud)	Cellular

Table 3. Long range protocols and standard

Network topology

Nearly all protocols make use of star topology, which can be regarded as one of the most suitable topology in LPWAN areas. Each node is connected to a specific gateway that acts as the central point where data is collected and transmitted to the internet. However, LoraWan makes use of a so-called stars-of-stars topology that is somewhat different than a star topology (Adelantado et al., 2017). In this topology, gateways can receive data from multiple nodes, which means an identical package can be received multiple times on a network server. The advantage this topology is when one gateway is not available, the nodes can still send packages to another gateway. The disadvantage of this topology is the requirement of extra server capacity for the deduplication processes (Raza et al., 2017).

Both LoraWan and Sigfox make use of gateways to send data packages from IoT devices to the internet. In case of NB-IoT, gateways are not necessary since existing cellular base stations can be used (Brian Ray, 2017; Peter Gutierrez, 2016). As a result, this decreases the complexity of IoT networks by removing an additional network component. Similar to gateways, base stations also use star topology to connect a bunch of devices to the internet.

Proprietary

Sigfox is proprietary technology that provides an end-to-end solution for its customers. Various companies have partnered with Sigfox to produce compatible devices. These devices are compatible to communicate with a Sigfox gateway, which transmits data to the Sigfox cloud. The cloud environment is fully managed by Sigfox. Customers can then obtain the data from the Sigfox cloud.

The LoraWan technology is open. However, the devices that enable the communication with LoraWan make use of Lora modulation, which is developed and patented by Semtech. Currently, Semtech is the only supplier of these chips, which makes the open standardization of LoraWan questionable (LoRa Alliance, 2017). Nevertheless, the LoRa Alliance has announced that two major chip manufacturers are developing standardized Lora compatible chips.

Contrasted to Sigfox and LoraWan, NB-IoT is an open standard initiated by the standardization body 3GPP, which is also had a significant role in standardizing LTE (Long Term Evolution). This standard is largely supported by a number of large manufacturers such as Intel, Huawei, Vodafone and Nokia (GSMA, 2017). Moreover, Intel has announced a new partnership with major firms like LG, Ericsson, Nokia and Verizon to design IoT devices to support NB-IoT.

The choice of using proprietary or open technology certainly affects scalability and interoperability challenges. Only a number of partner suppliers are allowed to bring devices on the market that are compatible with that specific technology. In that sense, a city that has selected a proprietary technology may be limited in choosing other products and services. In case of open technology, suppliers are allowed to use the technology without any costs or partnerships, which increases the range of products and services that are compatible with that technology.

Spectrum

The main difference between a licensed and unlicensed spectrum is described in Table 4. licensed spectrum is reserved for a specific use and is managed by a certain party such as a mobile carrier. To that end, only one operator is allowed to use a specific frequency band, which makes interferences obsolete and increases, therefore, the reliability. Costs are related when consumers are making use of this spectrum. Unlicensed spectrums are, on the other hand, available for public use without any related costs. However, interference on the frequency bands is possible due to the public use, which decreases the reliability and quality of service.

	Licensed	Unlicensed
Cost	Costs are related to the usage of the spectrum	Publicly available and free to use
Security	Secure	Less secure
Interference	No	Possible
Reliability	High	Medium

Table 4. Licensed and unlicensed spectrum

The use of a specific spectrum is not influencing an IoT architectural approach in terms of scalability and interoperability. However, it does affect certain factors amongst costs, security and reliability of services in a Smart City. When a service is considered as critical (military or hospital services), the use of an unlicensed spectrum may be questionable.

Network type

We describe LoraWan and Sigfox as LPWAN networks and NB-IoT as cellular. The main difference is that LPWAN uses the unlicensed spectrum to enable the transmission of data. The transmission is done by additional gateways that are placed next to the existing cellular networks. The gateways are responsible for collecting data and transfer it to the cloud, which differs per LPWAN supplier. Sigfox has a private cloud where the transmitted data of the gateway is processed and is made available to the customer. LoraWan has, on the other hand, not a specific cloud solution but gave freedom to developers to create own cloud solution by making use of the open LoraWan protocol. Based on that, the business model of Sigfox and LoraWan is rather different since Sigfox aims to provide an end-to-end solution for its customers while LoraWan provides an open protocol that can be used by multiple vendors.

NB-IoT is labeled as a cellular IoT technology and make, in contrary to LPWAN, use of existing Radio Access Network (RAN). Network operators can make base stations NB-IoT compatible with a simple software upgrade (Vodafone, 2016). Therefore, data packages are transmitted directly to the internet without additional network components, which are necessary for LPWAN. Nowadays, there are only a handful suppliers that support NB-IoT, which is mainly caused by the novelty of this technology. However, Gartner predicted that cellular technologies will dominate the long range era in a couple of years (Gartner, 2016).

Application layer

In the previous section, we have described the technical era of IoT based on the OSI model and analyzed them in terms of scalability and interoperability. The next step is to analyze the upper layers, namely the session, presentation and application layer. In this stage, data have to be sent to one or more applications. The data stream of IoT devices in a city can be quite huge and complex to handle. Fortunately, there are a number of standards and protocols that allow us to efficiently send data to specific applications. We will analyze these standards and protocols in terms of interoperability and scalability.

As we have described in the previous section, one of the main core elements of IoT is efficiency. IoT has to deal with constrained devices in terms of bandwidth and energy consumption. In that sense, protocols and standards on this layer require as lightweight design as well. A number of standards and protocols have been proposed in the course of the years, which are described below. We will mainly focus on MQTT, AMQP, CoAP and XMPP. The main elements are depicted in Table 5 and will be used as a basis for the analysis.

Protocol	Transport	QoS options	Architecture	Security
MQTT	TCP	Yes	Publish/Subscribe	TLS/SSL
COAP	UDP	Yes	Request/Response	DTLS
AMQP	TCP	Yes	Publish/Subscribe	TLS/SSL
XMPP	TCP	No	Request/Response Publish/Subscribe	TLS/SSL

Table 5. Comparison of messaging and web transfer protocols (Karagiannis et al., 2015)

MQTT

Stands for Message Queue Telemetry Transport and is a lightweight ISO standard developed by IBM. The standard runs on top of TCP and is based on asynchronous publish-subscribe architecture, which works as follow. When an application is interested in a specific set of data, it subscribes, via a central broker, to the instance that publishes the data (also called topic). The broker will send the topics from the publisher to the subscribers. In this case, the publisher is a sensor that is installed in a city and the end-applications are the subscribers. To that end, this architecture can be regarded as a one-to-many (IBM, 2017b). The use of TCP, in a resource-efficient setting, is questionable since it has several mechanisms that guarantee the reliability of data packages and requires, therefore, more resources of devices (James Stansberry, 2015).

CoAP

Stands for Constrained Application Protocol and is developed by the IETF. The aim of this standard is to extend the existing web technology in order to support low energy constrained devices (Sadasivan et al., 2014). To that end, COAP is designed based on a subset of HTTP and makes use of the same methods (GET, POST, etc.) CoAP uses asynchronous request/response to exchange messages from client to server, which works as follows. When an application is interested in a specific set of data, it requests the data directly from the network instances. The network instance acts on this requests via a response by sending the packages via the UDP protocol. This transport protocol is certainly lighter and suitable for energy-efficient environments. However, UDP is less reliable but CoAP uses its own mechanism on top of UDP to ensure reliability (Karagiannis et al., 2015).

AMQP

Stands for Advanced Message Queuing Protocol and is an open standard which is initially developed for the financial industry. This standard is based on the asynchronous publish-subscribe messaging architecture and is similar to MQTT. However, this standard support a larger exchange of messages in terms of messages per second and has more features such as security. A study of Karagiannis recommends the AMQP standard to build secure and scalable infrastructure over a reliable network and use MQTT standards in constrained environment where energy efficiency and low bandwidth is required (Karagiannis et al., 2015).

XMPP

Stands for Extensible Messaging and Presence Protocol (XMPP) and was standardized by IETF more than a decade ago. It was mainly used for messaging purposes and is known for its efficiency (Tobergte & Curtis, 2013). However, this protocol uses XML messages that increase the computation power and, as a result, also the energy consumption. Moreover, XMPP is extensible and allows the specification of XMPP Extension Protocols (XEP) that increase its functionality (Karagiannis et al., 2015).

Standards and protocols regarding to IoT scalability and interoperability in a Smart City

In the previous section, we have described the main standards and protocols that are used in the application layer. The momentum of these protocols is gained by efficiency in terms of energy and bandwidth. Each protocol has its own strengths and weaknesses and based on that, IoT suppliers select messaging protocols according to their specific requirements. We can, therefore, conclude that there is no one-size-fits-all protocol and standard currently available. In case of a Smart City, where a large number of IoT solutions are implemented, the existence of various application protocols is inevitable. To that end, we should not exclude protocols but rather embrace them in an architectural approach that serves all Smart City domains.

It might be the case that an application and constrained device make use of different application layer protocols (Sutaria & Govindachari, 2013). For instance, an application that uses MQTT messages wants to interact with IoT devices that only support CoAP messages. In this case, certain translation mechanism is required to enable the communication. One can argue that devices and applications should support both MQTT and CoAP protocols. However, as we have emphasized multiple times, IoT devices should be as efficient as possible. Supporting both MQTT and CoAP would not contribute to an energy-efficient device. We should avoid the support of multiple protocols on device levels and shift this to another level (Sutaria & Govindachari, 2013). Therefore, it is essential to have an abstraction layer where the standards and protocols are abstracted in order to allow cross-domain activities in a Smart City. Currently, there are a number of approaches to enable interoperability of various protocols such as gateways, proxies and agents. For instance, a gateway may act as a layer in the architectural approach to enable seamless interoperability amongst heterogeneous objects (Cirani et al., 2014).

3.3 Interoperability and scalability features in the IoT era

The previous section was dedicated to the analysis of standards and protocols in the IoT era. We analyzed which standards and protocols are being used in a Smart City and how they address the challenges of a Smart City. In this section, we will focus on the features that are important in the contribution of interoperability and scalability of an architectural approach in a Smart City. First, we will describe the concept of auto discovery and high availability. At the end, we will shed a light on the discussion of open and proprietary technologies with regard to an architectural approach.

Auto Discovery

Scalability is a key factor in ensuring the effectivity of a Smart City. Gartner has predicted that the number smart objects will reach around twenty billion in 2020 (Gartner, 2017). Manual management of such amounts can become expensive, labor-intensive, inefficient and in some cases even impossible (Perera et al., 2014). Therefore, we should make use of concepts that allows us to manage the tremendous number of objects efficiently. Cirani et al describe these mechanisms as *"A crucial enabler of robust applications and easy smart objects' deployment is the availability of mechanisms that minimize (ideally, cancel) the need for external human intervention for configuration and maintenance of deployed objects*" (Cirani et al., 2014). Auto discovery is such a concept that provide mechanisms to automatically discover objects without human intervention. Therefore, an architectural approach should incorporate components where auto discovery activities are satisfied.

Protocol	Architecture	Auto Discovery	Mechanism
MQTT	Publish/Subscribe	No	N.A.
CoAP	Request/Response	Yes	Multicast/Unicast
AMQP	Publish/Subscribe	Yes	Multicast/Unicast
XMPP	Request/Response Publish/Subscribe	Yes	Multicast DNS (mDNS)

Table 6. The support of auto discovery per protocol

As depicted in Table 6, most of the messaging protocols used in the IoT era incorporated auto discovery mechanisms. However, MQTT is not part of that group. Therefore, additional components have to be implemented in order to discover MQTT objects. In this study, we will adopt the approach of Happ and Wolisz (Happ & Wolisz, 2017). Their study has provided an advertising message string that can seamlessly be integrated with the existing messaging format. In that way, it would be possible to advertise to MQTT brokers on reserved topics.

There are a number of approaches that provided their own auto discovery mechanisms on top of the messaging protocols, such as (Cirani et al., 2014; Kim et al., 2016; Liu et al., 2013; Perera et al., 2014). We argue that this is not the ideal approach since it adds significant complexity. We should rather encourage the use of the native discovery mechanisms of the protocol itself and use additional components when necessary.

High Availability

In this study, we are continuously targeting at abstracting the technical landscape from the Smart City functionalities so that we can make use of the heterogeneous objects in a seamless way. As we have described in the application layer, abstraction can be realized by incorporating an integration layer in the architectural approach. This layer is responsible for the translation and integration of the heterogeneous protocols, which can be regarded as middleware. However, ensuring interoperability in heterogeneous environments generates a new set of challenges that require attention. The downside of integrating various protocols creates a certain degree of dependency. In such architectures, where the integration layer ensures interoperability, a failure can cause huge problems. It might be the case that all connected sensors sending data to an IoT platform won't be able to communicate with certain end-applications. The consequences can 'shut down' a Smart City. Therefore, the integration layer and the IoT platform as a whole should guarantee high availability. Virtualization and clustering is concept that can realize this.

Virtualization and clustering

The introduction of virtualization has created many advantages in terms of scalability and high availability. The hypervisor abstracts the hardware and operating system layer (OS). In this way, virtual machines are not affected by hardware failures since multiple servers can act as one system (Endo et al., 2016). However, in case of hardware failures, the performance will decrease in certain degree since less hardware capacity will be available. In addition to that, high availability is not the only advantage of clustering and virtualization. Servers can be added or removed without affecting virtual machines, which make this concept scalable as well. This concept is depicted in Figure 7.

In the paragraph above, we explained why high availability of the integration layer is an important element in a Smart City. We can argue that virtualization and clustering is a suitable concept that can guarantee high availability as well as scalability in a Smart City.

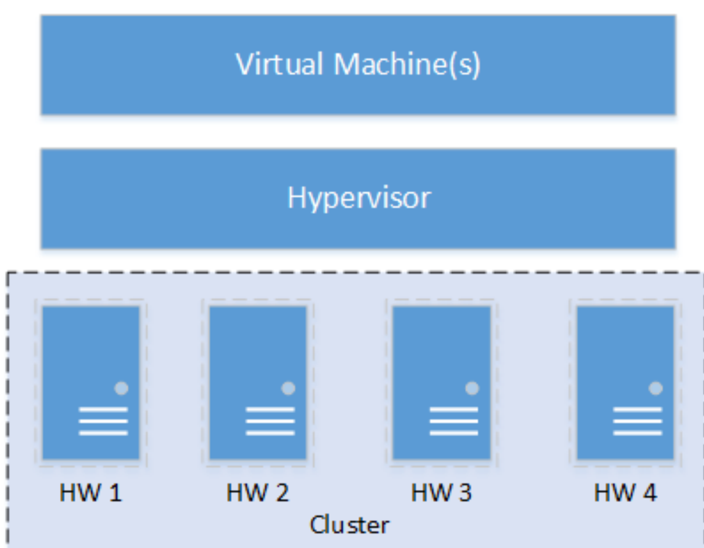

Figure 7. Clustering virtual machines

Open vs. Proprietary platforms

Currently, there are a relatively large number of IoT platforms offered in the market with their own architectural approaches. Some of these platforms are open and driven by standardization organizations or academics and some are proprietary and mostly driven by commercial companies. Sigfox is an example of a proprietary end-to-end solution that manages all layers of the IoT ecosystem.

The debate of open and proprietary standards is still going on in the scientific and commercial world. Both camps have its own reasonable arguments. Proponents of open standards suggest that it encourages interoperability of various technologies and stimulates innovation in certain eras since developers, in the entire world, are allowed to use these standards (Aggarwal et al., 2012). In that sense, open standards tend to decrease security vulnerabilities as well. Proponents of proprietary standards argue higher reliability as well as security. Regarding to security, these arguments are, especially nowadays, not completely valid due to the globalization in the developing communities such as GitHub. Developers throughout the whole world are contributing to the quality and security of software. To that end, we can argue that more intellectual manpower is dedicated to the development of open standards rather than proprietary standards where only a selection of manpower is dedicated to that process.

Shifting the debate to the context of this study brings us back Chapter 2 where we have identified interoperability and scalability as one of the main challenges in a Smart City. Open standards tend to promote interoperability between technologies and thereby guarantees compatibility. This is a major advantage for Smart Cities where we have to deal with heterogeneous environments. Therefore, open standards are suitable for Smart City and should be regarded as the preferred solution.

3.4 Comparative framework

In the previous sections, we have analyzed the standards and protocols in the IoT era and the features that are imperative for an interoperable and scalable architectural approach for a Smart City. The results of the analyses are transformed into constraints in which an architectural approach should comply to ensure interoperability and scalability. The constraints are placed in a comparative framework that will be used in the next chapter to evaluate architectural approaches. We will first start with the technical layer followed by the application layer and features.

1. Technical layer
    a. An architectural approach should support both long and short-range protocols.
    b. Short range protocols and standards (Wi-Fi, Zigbee, Bluetooth) are mostly used in a Wireless Sensor Network (WSN) and are connected to the internet via a gateway. An architectural approach should be able to connect to these gateways to reach the objects. These gateways can be
        i. Long range protocols and standards are used when objects are placed in an environment where a WSN cannot be implemented or when the objects are moving constantly in a wide range. For instance, a city that wants to measure the sea level on dikes or vehicles that are constantly moving throughout the whole city. In this case, objects are connected via an energy efficient and low bandwidth long range protocol directly to a gateway without having an IP address. The gateway is responsible for transforming the specific packages into IP packages. Companies that manage these gateways (such as Sigfox, KPN, T-Mobile) provides API's to customers, which can then use the data that is collected by the objects.

2. Application layer
    a. An architectural approach should support both request/response and publish/subscribe messaging architectures.
    b. An architectural approach should incorporate an integration layer that handles the communication of various application protocols.
        i. There are mainly two messaging architectures that are dominating the IoT era, which can be regarded as MQTT (Publish/Subscribe) and CoAP (Request/Response). The popularity of these protocols is gained by the efficiency in terms of bandwidth and energy, which makes it suitable for the IoT. A lot of IoT suppliers are advocating CoAP or MQTT based on their specific requirements. Therefore, the current IoT era can be regarded as vertical silos that use its own type of architecture based on their specific needs. In case of a Smart City, it is likely that certain domains are using several messaging architectures. In order to gain interoperability, it is important that an architectural approach can handle both messaging architectures.
        ii. According to several studies, the interoperability can be gained by having an integration layer, in form of proxies or (semantic) gateways, which abstracts the messages of CoAP and MQTT (Desai et al., 2015; Thangavel et al., 2014). Therefore, an architectural approach should incorporate an integration layer that can communicate with various application protocols.

3. Auto discovery
    a. An architectural approach should include auto discovery mechanisms to provide scalability.
        i. Auto discovery mechanisms are crucial in providing a scalable architectural approach for a Smart City where a large number of objects are implemented and yet continuously growing. An architectural approach should incorporate an additional layer where the auto discovery mechanisms are satisfied.

4. Open vs. Proprietary
    a. An architectural approach should prefer open standards, protocols, technologies and platforms rather than proprietary solutions.
        i. Interoperability is a key factor in the success of a Smart City. Open technology tends to increase the interoperability since the availability of source codes allows developers to make it compatible with other technologies. Moreover, developer communities such as GitHub are showing strong growth during the last decade. People around the world can now contribute to the quality and security of certain solutions with more intellectual manpower. It is, therefore, nowadays difficult to compete, as a company, with such strong communities and open standards.

5. High availability
    a. An architectural approach should take into account how the availability of the IoT platform can be guaranteed.
        i. An important element of this study is the integration layer in the architectural approach, which is responsible for integrating heterogeneous instances of a Smart City. However, this layer increases the level of dependency since all objects in the city are sending data to this layer where certain translation activities are carried out. Failures on this level can cause huge problems in a Smart City. Therefore, an architectural approach should take into account how the availability can be guaranteed. We have described the virtualization and clustering concept as a possibility to realize this.

	Evaluation	
Constraints	**Architectural approach A**	**Architectural approach B**
1. Support both short and long-range protocols and standards.		
2. Support both request/response and publish/subscribe messaging architecture.		
3. Incorporate an integration layer that handles the communication of various application protocols.		
4. Provide auto discovery of resources		
5. Support open standards, protocols, technology and platforms		
6. Provide high availability		

Table 7. Structure of the comparative framework

3.5 Conclusion

Our main aim of this chapter was to answer the research question: "*What criteria are required to address the IoT challenges in a Smart City?*" In order to answer this research question, we first started to explore the standards and protocols in the IoT era. The OSI model was used as an outline where we first analyzed the lower layer, namely the technical layer. The main outcome was that on this level a number of standards and protocols are used. IoT solution providers select these protocols and standards based on their specific requirements. Therefore, we cannot exclude certain standards and protocols but rather support them. The same argument is also valid in the application layer where a number of standards and protocols are widely used. Therefore, we conclude that there is no one-size-fits-all solution suited for the enormous IoT era. An architectural approach should take this into account and embrace the standards and protocols that serve all Smart City domains. This can be accomplished by an integration layer that can communicate with several standards and protocols. In this way, a horizontal architectural approach could be realized.

In addition to these layers, we also took into account the features that contribute to interoperability and scalability of an architectural approach. Auto discovery, high availability and open source technologies are identified as crucial features to address the challenges.

The answer to the research question is the comparative framework where the results of the analyses, in form of constraints, are placed in. The comparative framework will be used in the next chapter where architectural approaches are evaluated.

Chapter 4: The evaluation of architectural approaches

The aim of this chapter is to answer the first part of research question: *"Are existing architectural approaches capable of satisfying the criteria and if not, how can a new architectural approach satisfy the criteria?"* The main outcome is that the existing architectural approaches are not completely capable of satisfying the criteria of the identified challenges. There are certain factors to consider such as auto discovery and high availability, which is a partially or not addressed by the approaches. Furthermore, the evaluated approaches are not modeled based on a uniform modeling langue and it is not clear how the approaches are adding value to certain Smart City activities.

4.1 Introduction

In this chapter, we will analyze architectural approaches based on the defined constraints. First, we will select four architectural approaches of IoT platforms. Second, each approach will be evaluated based on six constraints that are defined in the previous chapter. The results of the evaluation will be depicted in a table, which provides a clear overview whether the constraints are satisfied or not.

4.2 The selection of architectural approaches

Various IoT platforms have been developed in the course of the years. Some of these platforms are suitable for only a specific domain and some are suitable for multiple domains. We are focused on the latter one since we are aiming at horizontal platforms. However, due to time constraints, we are not able to evaluate all architectural approaches in this area and have selected four platforms, which are OpenIoT, Cumulocity, ClouT/BigClouT and Watson IoT. Our initial aim was to focus only on open-source platforms. However, we have incorporated Watson IoT as well since IBM is considered as a pioneer in the IoT era. Therefore, it is interesting to evaluate the closed Watson IoT platform with respect to the open platforms. In the next section, we will explain the rationale of each platform.

OpenIoT

OpenIoT is a project that is co-funded by the European Commission. The project has developed an award winning open source middleware platform that can be used for a wide range IoT applications. OpenIoT defines its main objective as: "*OpenIoT creates an open source middleware for getting information from sensor clouds, without having to worry about what exact sensors are used.*" (OpenIoT, 2016). Next to that, OpenIoT is focused on managing IoT objects through cloud environments.

We have selected OpenIoT since it is one of the popular open source platform developed by both the academic and commercial world. This is an interesting combination since scientific knowledge and practical insights are combined.

Cumulocity

Cumulocity is founded in 2010 as a spin-off of Nokia in Silicon Valley. Cumulocity offers an independent device and application management platform for IoT services. This platform can deal with the most used IoT related protocols and standards, which allows companies to make use of IoT services disregarding which protocol and standard objects are being used. Cumulocity describes one of its main objectives as: "*Cumulocity strives to remove complexity and allow the benefits of IoT to be exploited rapidly, comprehensively and securely by all organizations.*" (Cumulocity, 2017).

We have selected Cumulocity since their platform is growing rapidly and gaining worldwide attention. Many enterprises have recognized the platform's abilities in creating new business opportunities, increasing customer satisfaction and creating efficiencies in a simplified way.

ClouT/BigClouT

BigClouT is funded by the European Commission and National Institute of Information and Communication Technology of Japan. This project is an extension of the ClouT project that ended in June 2016. The result of this project is a framework to provide data of multiple IoT sources into a uniform way. The BigClouT project uses this framework as a fundament and aims at creating an integrated Smart City platform by making use of IoT, cloud computing and big data. On top of that, BigClouT also provides the ability to perform data analytics activities based on the collected data (BigClout, 2017).

The argument of selecting this platform is twofold. First, the European and Japanese commissions established the BigClouT project after the ClouT project, which indicates that these projects have the support of the involved parties. Second, this platform is specifically targeting Smart Cities whereas the other platforms are applicable in multiple contexts.

Watson IoT

Watson IoT is an IoT platform developed by IBM. This product is the flagship of IBM's IoT solutions. As described in Chapter 2, IBM was one of the key companies in the introduction phase of IoT. We can argue that IBM played a significant role in taking IoT to the next level. Watson IoT aims at providing a platform that can connect to a wide range of devices and gateways, manage these devices and store data from the devices. On top of that, IBM provides a broad variety of features. Such as machine learning, text analytics and Blockchain (IBM, 2017a).

The selection of Watson IoT may be in conflict with the constraints of architectural approach. In Chapter 3, we have defined the constraints and preferred open over proprietary platforms. However, the included number of features might be interesting for a city. Next to that, IBM is one of the leading and innovative companies in the IoT era.

4.3 Evaluation

The results of the evaluation are depicted in Table 8. In the next section, we will analyze the architectural approach in-depth. Each architectural approach is assessed based on six constraints that are crucial for a scalable and interoperable IoT platform. The colors are defined as follow. Red means that the approach does not satisfies the constraints. Yellow means that the approach partially satisfies the constraints. Green means that the constraint is satisfied. We have provided a short summary per platform next to the table that describes the strong and weak points of the platforms.

Evaluation of the platforms

Constrains	OpenIoT	Cumulocity	BigClout	Watson IoT
1. Support both short and long-range standards and protocols	OpenIoT makes use of X-GSN middleware that is more focused on WSN. OpenIoT does not describe how long-range protocols can communicate with the platform	Cumulocity both support short and long-range protocols via device and network agents	Connection are establish via the SensiNact gateway. This gateway is responsible for handling various protocols including short and long-range protocols	Supports both short and long-range protoc However, in some cases, extra components such as proxies, are needed
2. Support both request/response and publish/subscribe messaging architecture	OpenIoT providers wrappers to communicate with request/response and publish/subscribe objects	Cumulocity supports both messaging architectures. However, a HTTP proxy is required to communiccate with CoAP	both messaging architectures are supported by SensiNact gateway	Only supports publish/subscribe messages. Proxies are needed to support request/res messages between the gateway and platfo
3. An architectural approach should incorporate an integration layer that handles the communication of various application protocols	OpenIoT uses the X-GSN middleware layer as an agnostic mean to collect data from various protocol specific objects	Cumulocity offers both centralized and decentralized intergration via device and network agents.	SensiNact gateway can be regarded as an agnostic mean that realizes the interconnection of various protocols	Watson IoT has not a central agnostic integration layer that is responsible for connecting the objects
4. There should be possibilities to auto discover resources	OpenIoT does not include auto discovery mechanisms for objects. However, there are auto discovery mechanism for services based on semantic annotations	Cumulocity does not provide auto discovery mechanisms	Auto discovery is provided based on object specific protocols such as CoAP. However, the MQTT does not support auto discovery mechanisms. Therefore, additional mechanisms are required on top of MQTT. It is not described how MQTT objects are auto discovered	Watson IoT does not provide the ability to discover resources
5. Support open standards, protocols, technology and platforms	OpenIoT is an open-source platform that is free to use. However, the CUPUS component is based on propieraty technology	Cumulocity is an open platform that uses open standards and protocols	The platform is completely open and uses open standards and protocols	The platform is closed and proprietary to IB
6. High availability should be guaranteed	OpenIoT does not describe how high availability can be guaranteed and also does not provide guidelines or best practices	Cumulocity services are mainly offered via the cloud that operates on advanced datacenters	The platform ensures high availability through several open-source cloud solutions	Watson IoT is provided as SaaS (Software a Service). All underlying layers are managed IBM in their advanced data centers

Table 8. Results of the evaluation of the architectural approaches

Summary of the evaluation

OpenIoT

OpenIoT has not yet the potential to be the leading IoT platform. It seems that this platform is focused on WSN environments, which may clarify why long-range are not addressed. Moreover, this platform also lacks in providing auto discovery mechanisms and high availability. A unique feature of this platform is service discovery based on semantic annotations.

Cumulocity

Cumulocity is IoT platform that is gaining its momentum by basically providing accessibility and simplicity. It has the potential to serve as an IoT platform for a Smart City. However, a number of aspects have to be considered. One of them is auto discovery, which is not provided by the platform. Next to that, the support of CoAP objects should be realized without having certain proxies. Nevertheless, a unique selling point of Cumulocity is the simplicity and PaaS services. To that end, customers do not have to manage the underlying hardware layers to make use of an IoT platform and can, therefore, focus on adding value business services.

ClouT/BigClouT

ClouT/BigClout can be regarded as the most potential IoT platform for Smart Cities. The platform satisfies all constraints except auto discovery. This feature is partially provided since the platform does not describe how MQTT objects are discovered. These objects require additional components on top of the protocol. In addition to that, the platform is still in the developing phase and not yet publicly available.

Watson IoT

It seems like IBM Watson is mainly focused on data that is collected by IoT objects. Therefore, we argue that the part of connecting and collecting data from heterogeneous objects is certainly missing. IBM is outsourcing this part to the gateways that are currently available and has not provided an agnostic gateway to cope with the challenges on this level. Despite these drawbacks, IBM Watson provides sophisticated features for data analytics and Blockchain.

4.4 The analysis of architectural approaches based on comparative framework

In this section, we will evaluate the architectural approaches of the selected platforms in-depth. The comparative framework which is defined in the previous chapter will be used as a basis to perform the analysis. We will evaluate how the architectural approaches address the constraints. The constraints are depicted in Table 9. First, we will start with OpenIoT followed by Cumulocity, BigClouT and Watson IoT.

Constraints
1. Support both short and long-range protocols and standards.
2. Support both request/response and publish/subscribe messaging architecture.
3. Incorporate an integration layer that handles the communication of various application protocols.
4. Provide auto discovery of resources
5. Support open standards, protocols, technology and platforms
6. Provide high availability

Table 9. Constraints

OpenIoT

Constraint 1. *Support short and long-range protocols and standards*

Starting with short range protocols, OpenIoT uses the X-GSN (Extended Global Sensor Network) sensor middleware. This open source middleware collects, filters and combine data from virtual and physical sensors to the platform (Medvedev et al., 2015). Next to that, it semantically annotates data so that it can be used for discovery purposes. Figure 8 shows the architecture of the X-GSN. The system that is running X-GSN is connected with the IoT objects and the internet. In order to realize the communication between IoT objects and X-GSN middleware, wrappers are used to transform raw sensor data into a readable X-GSN format. It is important to note that IoT objects should have a supported wrapper to communicate with the middleware.

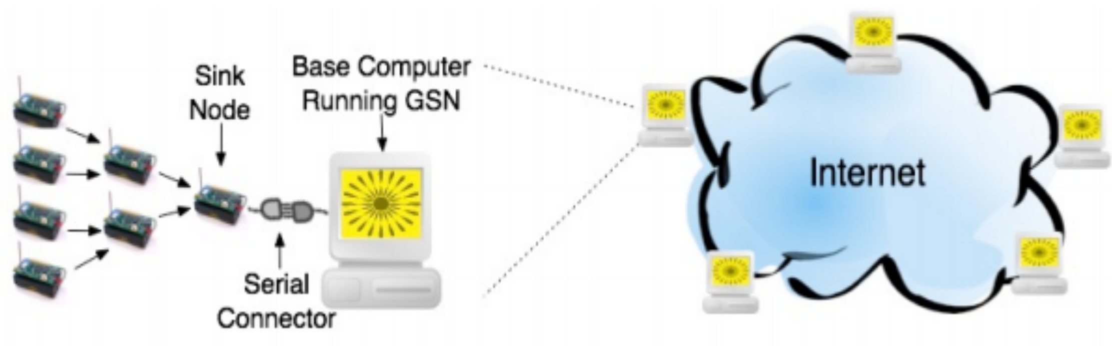

Figure 8. X-GSN middleware for Wireless Sensor Networks (Kefalakis et al., 2013)

OpenIoT argues that developing wrappers for sensors is an effortless job. However, this is not sustainable for a Smart City where a large number of protocols are present.

Regarding to long range protocols, OpenIoT does not describe how constrained objects can connect to the platform. As we can see in Figure 8, OpenIoT only includes wireless sensor networks that are connected via X-GSN. This component is installed on a node that acts a gateway between the platform and physical environment. This approach is not applicable for long-range protocols where gateways are managed by telecommunication companies (such as KPN and T-Mobile), which offers API's to retrieve data. To that end, OpenIoT does not describe how these API's can be fed into the platform. Therefore, we can argue that OpenIoT is more focused on supporting WSN environment rather than environments with constrained objects.

Constraint 2. *Support both request/response and publish/subscribe messaging architecture*

OpenIoT provides wrappers that support both request/response messaging architectures in form of CoAP and HTTP wrappers. Regarding to publish/subscribe, OpenIoT implemented the CUPUS open-source middleware component which consists of publishers, subscribers and mobile brokers. The mobile broker can be installed on mobile devices or, in case of constrained devices, on gateways.

Constraint 3. *An architectural approach should incorporate an integration layer that handles the communication of various application protocols*.

OpenIoT uses the X-GSN middleware layer as an agnostic mean to collect data from various objects disregarding the used protocols and standards. As depicted in Figure 9, we can see that the X-GSN layer is responsible for collecting data from objects and directing it to the cloud. The mobile broker is the CUPUS interface that handles publish/subscribe messages via the X-GSN layer to the platform (Soldatos et al., 2015). To that end, we can conclude that X-GSN acts as an integration layers.

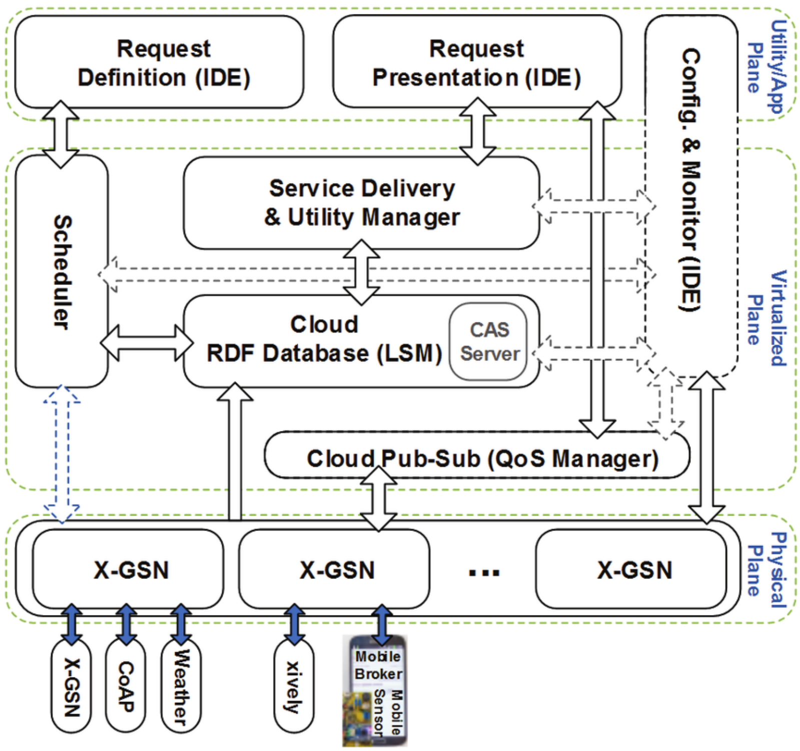

Figure 9. OpenIoT architectural components (Kefalakis et al., 2015)

Constraint 4. *There should be possibilities to auto discover resources*

OpenIoT does not provide auto discovery mechanisms to discover objects. Each object requires registration in the platform before data can be collected. The registration can be done individually or with a bulk import (Arenas et al., 2015). Nevertheless, OpenIoT provides semantic service discovery by annotating collected data based on W3C Semantic Sensor Networks (SSN) ontology and store the annotations in an RDF database in the cloud. In that way, users can then discover services without knowing from which sensor it is derived (Soldatos et al., 2015).

Constraint 5. *Support for open standards, protocols, technology and platforms*

As the name already reveal, OpenIoT is an open-source platform that is free to use. The project is co-funded by the European Commission under the FP7 program. Source codes are available on GitHub where a group of developers are working on the project. The X-GSN middleware, which is a core element the platform, is adopted from the open-source GSN project. However, a drawback of this platform is the use of CUPUS. This publish/subscribe component is open-source but uses its own proprietary protocols and data structures and thereby limiting interoperability (Antonic et al., 2015).

Constraint 6. *High availability should be guaranteed*

OpenIoT does not describe how high availability can be guaranteed and also do not provide guidelines or best practices. It seems that users are responsible for high availability of the systems where the OpenIoT platform is deployed.

Cumulocity

Constraint 1. *Support short and long-range protocols and standards*

The Cumulocity platform establishes communication to objects via agents. The agents are responsible for translating object specific protocols into a single reference protocol which is understandable by the platform (Cumulocity, 2017). There are two types of agents, namely device agents and network agents. Device agents are installed on objects itself and network agents are installed in the cloud. The latter is mainly used for constrained devices that have limited capacity.

We can conclude that Cumulocity support short range protocols since agents can translate specific protocols into a single reference protocol. Moreover, agents can also be deployed on gateways in a WSN. Network agents are suitable for long range protocols. The Cumulocity platform has incorporated pre-integrated connectors to realize the communication with Sigfox, LoraWan and NB-IoT protocols (Cumulocity, 2017). To that end, we conclude that Cumulocity support both short and long-range protocols.

Constraint 2. *Support both request/response and publish/subscribe messaging architecture*

Cumulocity both support request/response and publish/subscribe messaging architectures. REST is used for the former one and MQTT for the latter one. However, Cumulocity has not described the support of the CoAP protocol, which can be regarded as the most suitable IoT protocol for constrained environments. It is, however, relatively simple to communicate with CoAP since it is based on REST. HTTP proxy can be used to communicate with CoAP objects that translate CoAP messages to HTTP compatible messages (Sadasivan et al., 2014).

Constraint 3. *An architectural approach should incorporate an integration layer that handles the communication of various application protocols*

Cumulocity integrates devices, via agents, in both a centralized and decentralized way. The agent can be regarded as an agnostic mean to realize communication disregarding object specific protocols. Device agents can be installed on objects, such as devices and gateway, and can be therefore regarded as decentralized. Network agents are installed in the cloud where multiple devices can connect and can, therefore, be regarded as centralized.

Constraint 4. *There should be possibilities to auto discover resources*

Cumulocity does not provide auto discovery mechanisms. Objects need to be registered manually or via bulk imports. Unlike OpenIoT, the platform also does not provide service discovery.

Constraint 5. *Support for open standards, protocols, technology and platforms*

One of Cumulocity's main philosophies is to provide an open platform where customers and developers are allowed to contribute to the success of the platform. Next, Cumulocity prefers the use of open standards and protocols as well. Cumulocity describes its platform as*: "The Cumulocity IoT platform is open, publicly documented and standards based, which allows customers to innovate full end-to-end solutions rapidly and completely removes the need for organisations to adopt risky "doubling-down" strategies"* (Cumulocity, 2017).

Constraint 6. *High availability should be guaranteed*

Cumulocity offer its services mainly via the cloud that can be accessed through the internet. The advantage of this approach is twofold. First, the infrastructural environment of the platform is not a concern for the customer anymore. Second, Cumulocity is responsible for managing these cloud environments which is part of their main expertise. The latter advantage is an important factor for high availability. Platforms are operated in advanced data centers that ensure scalability, by simply adding or removing servers in a cluster, and ensuring high availability, by adding multiple servers in one cluster.

ClouT/BigClouT

Constraint 1. *Support short and long-range protocols and standards*

The IoT kernel is responsible for the communication between the objects and platform. As depicted in Figure 10, the kernel consists of three components, namely the 1) Uniform Access to IoT devices, 2) IoT Device management and 3) IoT Device Wrapping. The latter is responsible for establishing the connection of the objects via the SensiNact gateway. This component can handle various object specific protocols. The gateway can be installed in a WSN and in the cloud to interact with constrained devices. To that end, we can conclude that platform both supports short and long-range protocols and standards.

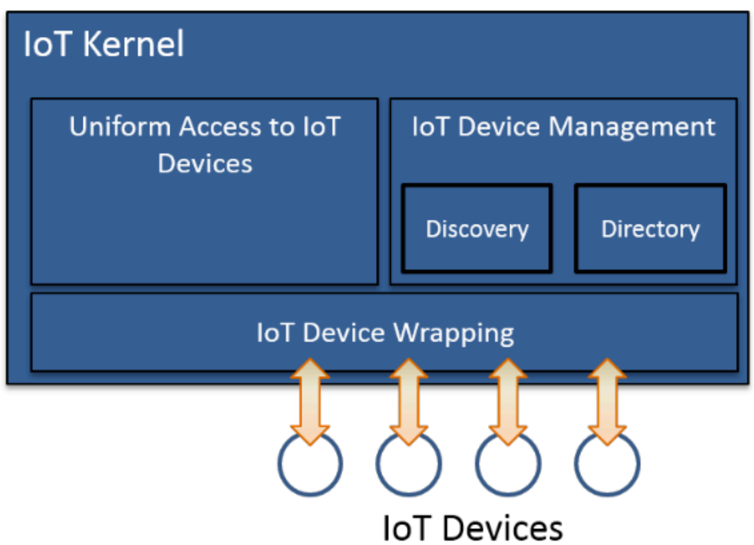

Figure 10. IoT kernel of ClouT (ClouT, 2013a)

Constraint 2. *Support both request/response and publish/subscribe messaging architecture*

ClouT/BigClouT supports both request/response and publish/subscribe messaging architectures. As depicted in Figure 11, the SensiNact gateway consists of two bridges, namely the southbound bridge with object specific protocols like CoAP, Sigfox and MQTT, and the northbound bridge with application specific protocols like HTTP Rest and MQTT agents. The core is responsible for the interconnection of all these standards and protocols.

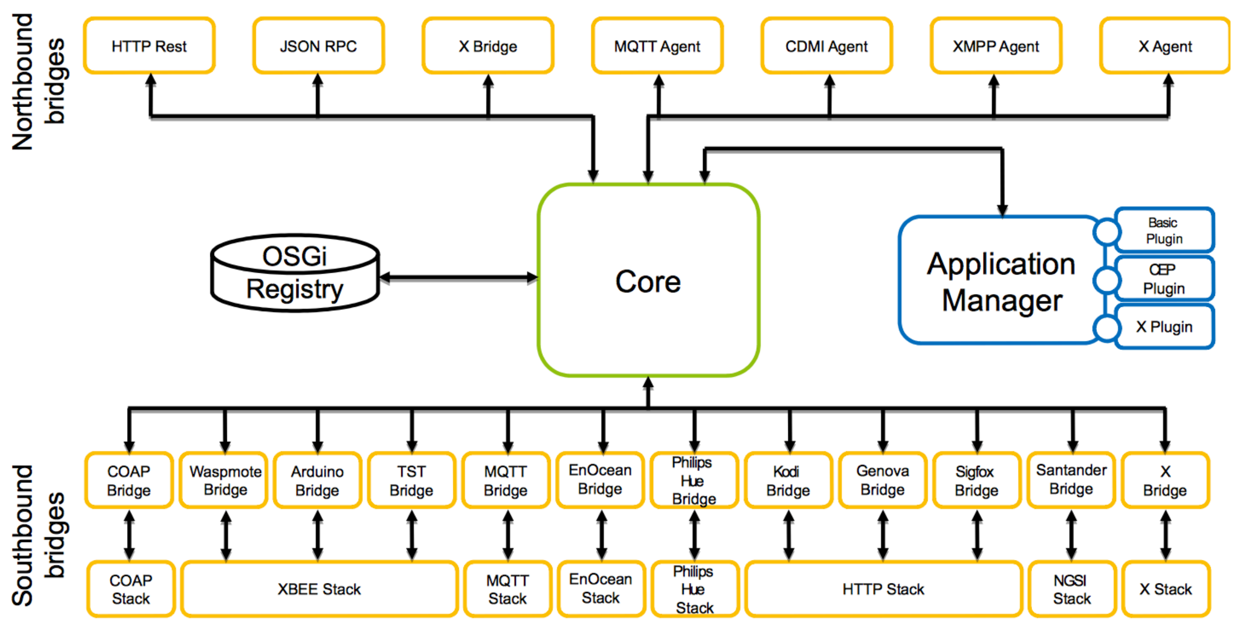

Figure 11. SensiNact Southbound and Northbound bridges (Rémi Druilhe, 2016)

Constraint 3. *An architectural approach should incorporate an integration layer that handles the communication of various application protocols*

ClouT/BigClouT provides an integration layer in form of the SensiNact gateway. As we can see in the figure above, the SensiNact gateway can be regarded as an agnostic mean that realizes the interconnection of various protocols.

Constraint 4. *There should be possibilities to auto discover resources*

ClouT/BigClouT provides auto discovery mechanisms to discover resources. The IoT Device Management is responsible for this activity and is part of the IoT Kernel, which is depicted in Figure 11. Objects are discovered based on the native discovery mechanism of the standard itself. For instance, objects that are using CoAP are discovered via CoAP auto discovery mechanisms, and objects that are using IPv6 are discovered via MDNS/DNS-SD mechanisms (ClouT, 2013a).

There is, however, an important aspect excluded. The native MQTT standard does not support auto discovery mechanisms. Therefore, other mechanisms are required on top of the MQTT standard. ClouT/BigClouT does not describe what mechanisms are implemented to discover MQTT objects.

Constraint 5. *Support for open standards, protocols, technology and platforms*

ClouT/BigClouT is an open platform that is thoroughly documented. The SensiNact middleware, which serves as an important component, is open-source and is publicly licensed by Eclipse Community.

Constraint 6. *High availability should be guaranteed*

ClouT/BigClouT provides mechanisms to ensure high availability. The computing and storage building block is responsible for these activities. The platform makes use of OpenStack solutions, which is an open-source software platform for cloud computing. The Open Stack Swift is implemented to store large amounts of data in a distributed way and thereby ensuring high availability. Next, OpenStack OpenShift is used to provide high availability for infrastructural nodes by making use of hypervisors and brokers (ClouT, 2013b).

Watson IoT

Constraint 1. *Support short range protocols and standards*

The architecture of Watson IoT is rather different than the rest of the analyzed platforms. Watson IoT provides the freedom to use any gateway to connect with the objects. However, an important requirement is that the gateway should support MQTT messages since this is the only supported protocol in the platform (IBM Bluemix, 2017). There are a number of gateways that support short range protocols via MQTT gateways. Regarding to long range protocols, Watson IoT provides the possibilities to connect to Sigfox and LoraWan networks (IBM Bluemix, 2017). To that end, we conclude that Watson IoT supports both short and long-range protocols. However, extra components, such as proxies, are needed to translate any type of messages into MQTT messages, which significantly increases the complexity.

Constraint 2. *Support both request/response and publish/subscribe messaging architecture*

Watson IoT only supports publish/subscribe messages to realize the connection between gateways and the platform. Certain proxies are needed to support request/response messages between the gateway and platform. Therefore, we conclude that both messaging architectures are supported when certain proxies are used.

Constraint 3. *An architectural approach should incorporate an integration layer that handles the communication of various application protocols.*

Unlike the other IoT platforms, Watson IoT has not a central agnostic integration layer that is responsible for connecting the objects.

Constraint 4. *There should be possibilities to auto discover resources*

Watson IoT does not provide the ability to auto discover resources. The platform has transferred these activities to the gateways.

Constraint 5. *Support for open standards, protocols, technology and platforms*

Watson IoT is developed by IBM which is a large technology firm. Therefore, it is obvious that the platform is closed and proprietary to IBM. Therefore, users have to pay to make use of Watson IoT.

Constraint 6. *High availability should be guaranteed*

Watson IoT is provided as PaaS (Platform as a Service). All underlying layers are managed by IBM in their advanced data centers. Therefore, the high availability of the platform is guaranteed.

4.5 Conclusion

Our aim of this chapter was to answer the first part of the research question: *"Are existing architectural approaches capable of satisfying the criteria and if not, how can a new architectural approach satisfy the criteria?"* The focus of this chapter was to analyze whether the architectural approaches are capable of addressing the IoT challenges in a Smart City. In order to answer this part of the research question, we first selected four architectural approaches. These approaches were evaluated based on the constraints which were defined in the previous chapter.

Based on the analysis, we conclude that the evaluated architectural approaches do not satisfy all six constraints. ClouT/BigClouT came out as the most potential platform. However, there is an important point to consider. This platform claims that auto discovery is supported based on object specific protocols such as IPv6, CoAP and MQTT. It is, however, not described how MQTT objects are discovered since it does not include auto discovery mechanisms. Therefore, additional components are required on top of this protocol. It is not described what additional components are implemented. Moreover, this platform is still in the development phase and not publicly available. It is, therefore, questionable whether the auto discovery mechanisms are tested in large heterogeneous environments. In addition to that, none of the architectural approaches, including ClouT/BigClouT which aims to develop a reference architecture for a Smart City, provides a uniform model that illustrates the building blocks in a comprehensible and coherent manner. We argue that a uniform model is an imperative mean to communicate the architectural approach as effective as possible especially for a reference architecture.

Chapter 5: A novel architectural approach

The aim of this chapter is to answer the second part of research question: "Are existing architectural approaches capable of satisfying the criteria and if not, how can a new architectural approach satisfy the criteria?" The main outcome is a model, based on Archimate, that illustrates a technology, application and business layer. Moreover, two functional models are provided. The model shows that our architectural approach is capable of intervening the interoperability and scalability challenges in a Smart City by providing an agnostic gateway, auto discovery capabilities and the assurance of high availability.

5.1 Introduction

In the previous chapter, we have evaluated a number of architectural approaches. The main result was that these approaches were not completely capable of satisfying the constraints. Moreover, the architectural approaches of the platform were not modeled in a uniform way. Therefore, in this chapter we aim to provide a model that a) satisfies the constrains, b) is in accordance with a standardized modeling language and c) shows how business value is created. We will use Archimate because this is a widely used standardized modeling language in the architectural era. Moreover, it is not our aim to define a completely new architectural approach since we do not want to reinvent the wheel. Hence, we will reuse certain components of the evaluated approaches and include them in our novel approach.

We will introduce the novel architectural approach by first starting at the technology layer where the infrastructural components are illustrated and described. Second, we will present the application layer where the gateway and IoT platform is introduced. Next, the auto discovery and high availability approach will be outlined. We will end this chapter with the business layer where we will describe how our novel approach is creating value for Smart Cities.

5.2 Proposed Architectural Approach

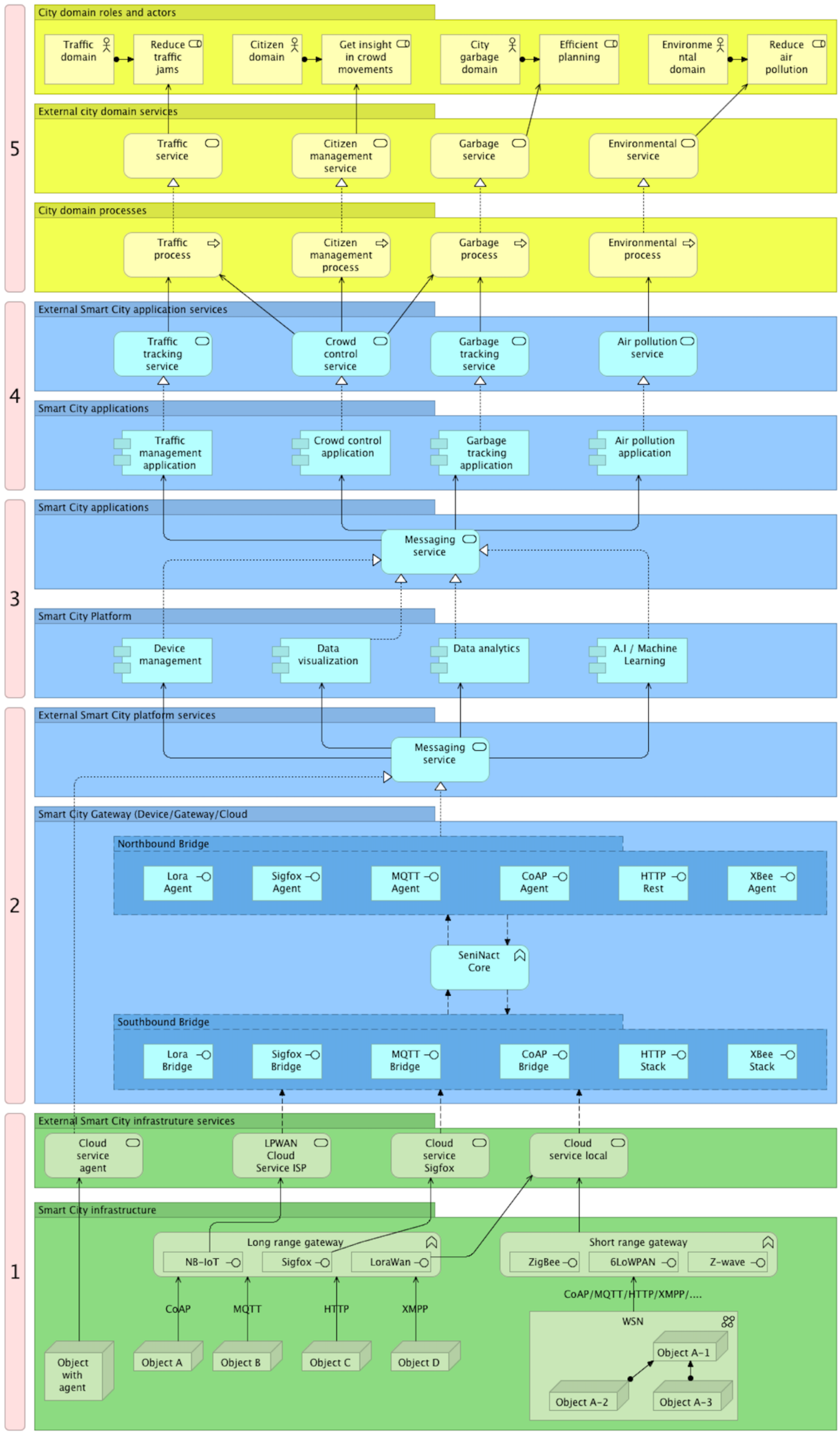

Figure 12 illustrates the novel architectural approach that we have defined based on the constraints and outcome of the evaluated approaches. This model is based on Archimate and consist of three layers. The green layer is the technological layer, the blue layer is the application layer and the yellow layer is the business layer. The activities within the layer result in a set of services that feed the activities in the upper layers.

The following sections will be dedicated to the description of each layer, starting with technology, application and business layer respectively.

5.2 Technology layer

We will start describing our novel architectural approach by the technological layer, which is depicted in Figure 13. This layer consists of the infrastructural components. As we can see on the bottom of the layer, there are a number of objects. We can distinguish these objects in three types. First, the objects that have sufficient battery capacity and processing capabilities. These objects can be provided with agents that serve as a gateway by translating the object specific protocols into a common language. To that end, translation activities are carried out on the edge, which reduces processing capacity in the cloud or local gateway. This approach is adopted from Cumulocity, which is the only evaluated platform that uses agents.

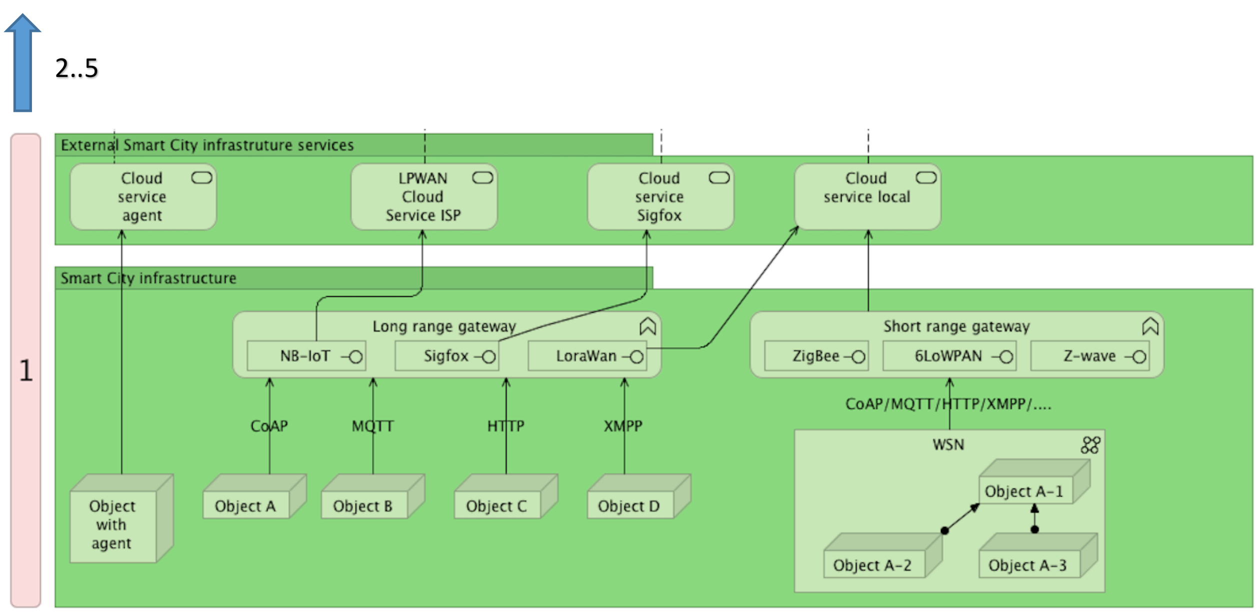

Figure 13. Technological layer

The second type are constrained objects that use short range standards and protocols such as ZigBee and Z-wave. These objects are connected with a local gateway that is placed in a relative short range. The third type are constrained objects that use long range standards and protocols such as LoraWan and NB-IoT. In some cases, it is not possible or feasible to place local gateways. For instance, sensors that are placed on dikes or objects that are constantly moving. These objects are connected with long-range gateways that are often managed by third-parties.

Objects and gateways deliver services, which are depicted on the second layer (External Smart City Infrastructure services). We can see here that service providers are responsible for providing NB-IoT services and Sigfox for Sigfox services. Short range gateways and the objects with agent are connected via common cloud services

5.3 Application layer

The application layer consists of two parts, namely the gateway and the platform itself. We will start with the former one. As ended in the previous section, the objects on the technical layer forward data to the platform in form of services. However, due to the heterogeneity, it is a challenge to fed all data sources in a uniform format to the platform. Therefore, a gateway is required for certain translation mechanisms.

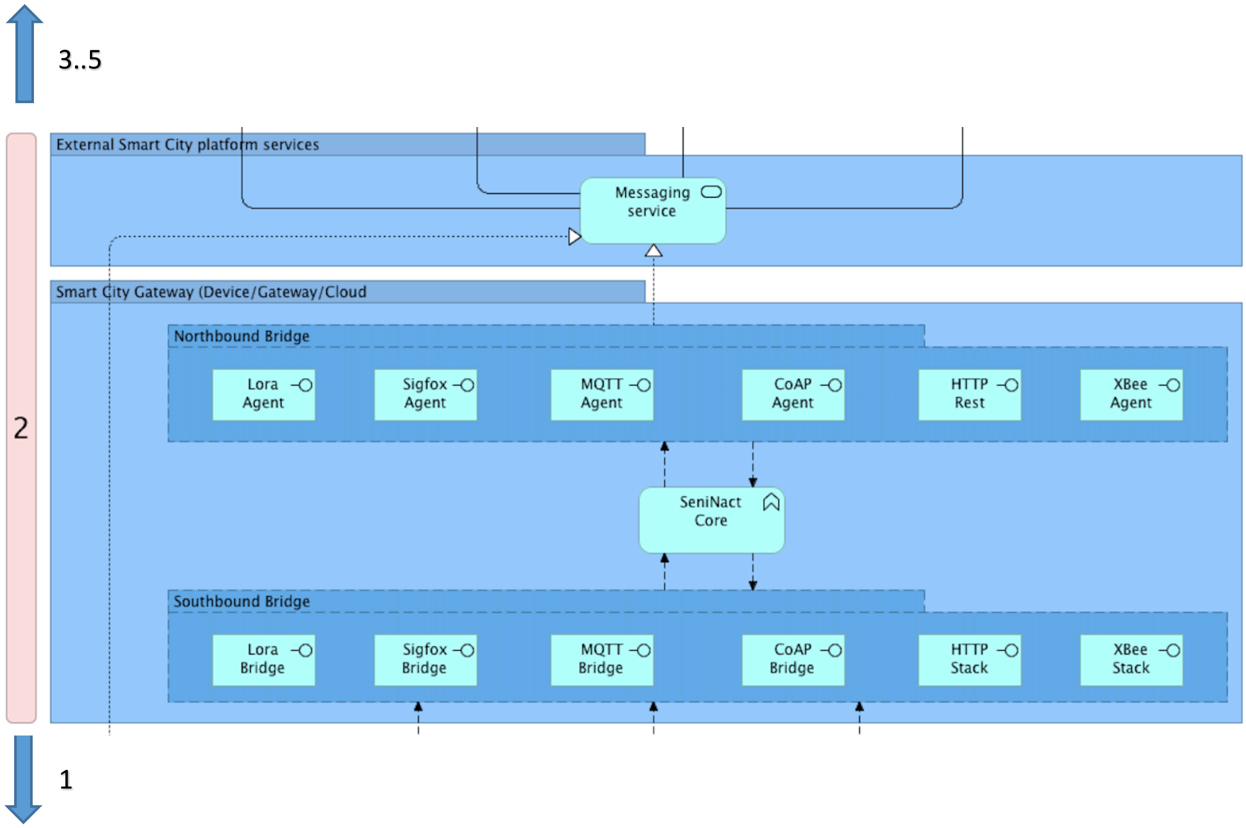

Figure 14. Application layer of the gateway

The SensiNact gateway appears to be the most appropriate gateway in a Smart City. The main reason for this is the number of supported standards and protocols. Next, modules with additional standards and protocols are simple to add, which increases the interoperability and scalability. Therefore, we will adapt the concept of the SensiNact gateway in our architectural approach. This gateway is adopted from the ClouT/BigClouT platform.

SensiNact gateway consists of a Southbound and Northbound bridge. The Southbound bridge is in charge of realizing the interaction of objects and gateway through object specific protocol adapters such as CoAP Bridge and HTTP Stack (Eclipse, 2017). The Northbound Bridge is responsible for sending data to applications through application specific protocols, such as REST API's and MQTT agents (Eclipse, 2017). Next to the bridges, the core component is also an important element. The core is responsible for the coordination and orchestration of data that flows through the gateway. At the end, the activities of the SensiNact gateway results in a messaging services to the IoT platform, which depicted in Figure 15.

The platform is in charge of the management of all underlying activities of the model. We will only focus on device management where auto discovery has a vital role. In Chapter 3, we have identified auto discovery as an important component to realize scalability. In Chapter 4, we have evaluated architectural approaches based on a number of constraints including auto discovery. None of these approaches fully address the auto discovery constraints. Therefore, we will include auto discovery mechanisms in our model that fully addresses the constraints.

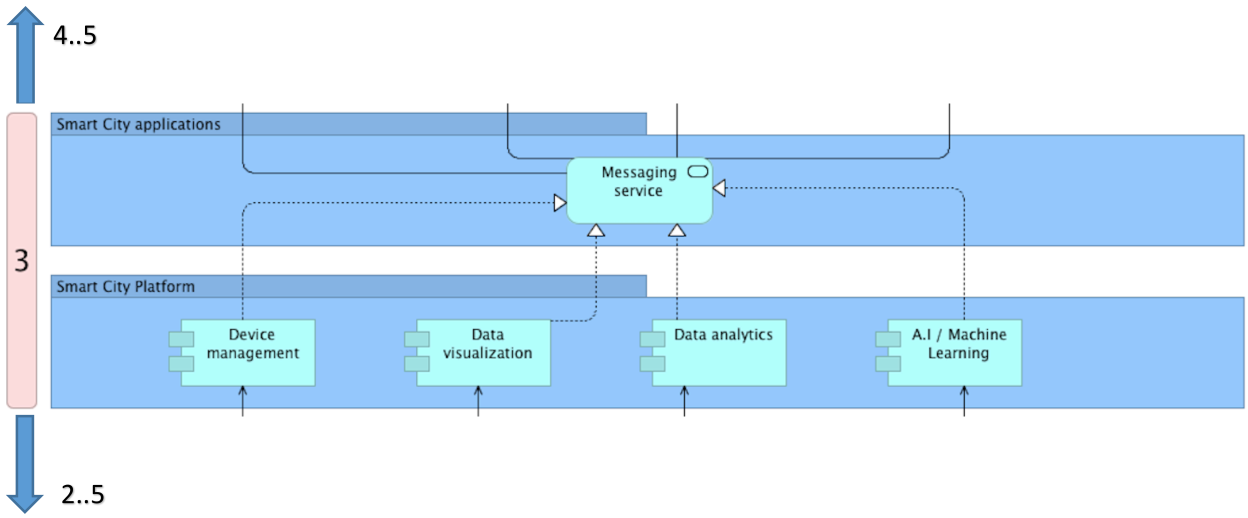

Figure 15. Application layer of the IoT Platform

5.4 Auto Discovery

We will adopt the auto discovery mechanisms that are used in ClouT/BigClouT, which is realized by the SensiNact gateway. SensiNact discovers objects through object specific protocols via protocol adapters in the Southbound Bridge. A number of object specific protocols, such as CoAP and ZigBee, provides their own discovery mechanisms. For instance, CoAP objects are discovered via built-in CoAP discovery mechanisms. To that end, the need of additional discovery mechanisms is not required anymore, which reduces the complexity of the architecture. However, this notion is only valid for protocols that include these mechanisms. MQTT is such a standard that does not natively supports auto discovery. Therefore, additional components are required. Fortunately, many studies have provided certain mechanisms on top of MQTT to auto discover objects. We will adopt the approach of Happ and Wolisz that is introduced in Chapter 3 (Happ & Wolisz, 2017).

Their study provided an approach to auto discover MQTT objects through additional advertisement messages that not alters the core messaging format of the standard.

The auto discovery mechanism of our architectural approach is depicted in Figure 16. On the bottom of the figure, we have illustrated the most used IoT messaging protocols. On top of that, we have illustrated how these protocols propagate the existence of new objects. The protocol adapters in the Southbound Bridge are responsible for aggregating these messages and registering it in the object repository. These objects can then be requested via the device management in the IoT platform through the discovery service.

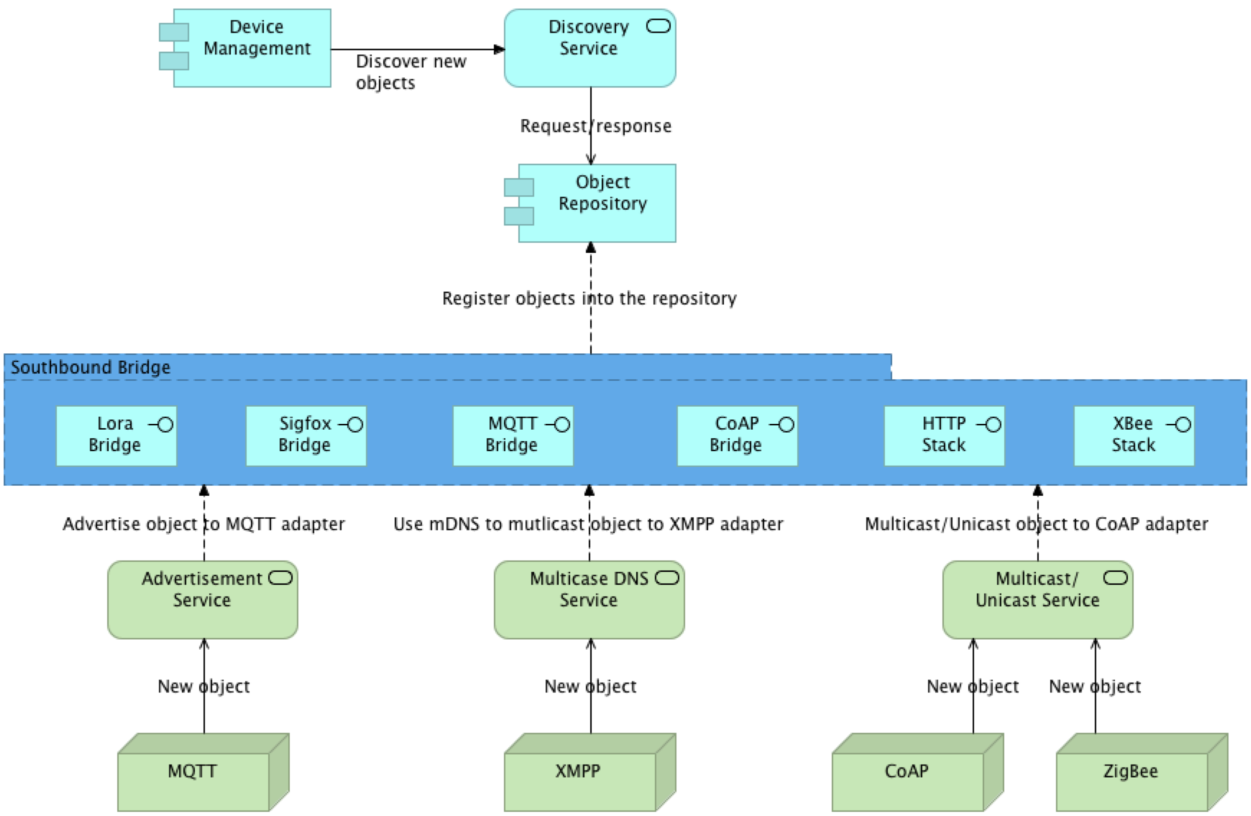

Figure 16. Auto Discovery approach

5.5 High Availability

Next to auto discovery, we have also identified high availability as an important feature. Therefore, we will incorporate high availability in our architectural approach as well. We have already defined which high availability approaches are suitable for IoT platforms, namely clustering and virtualization. In this approach, multiple servers act as one node through a hypervisor. Virtual machines are installed on top of the hypervisor and will serve as an application server to host the IoT platform and cloud gateway via the infrastructural service. It is highly recommended to place the cluster at separate locations. In case of outage on a location, due to electricity failures or natural disasters, the other location will continue providing infrastructural services to the IoT platform and cloud gateway.

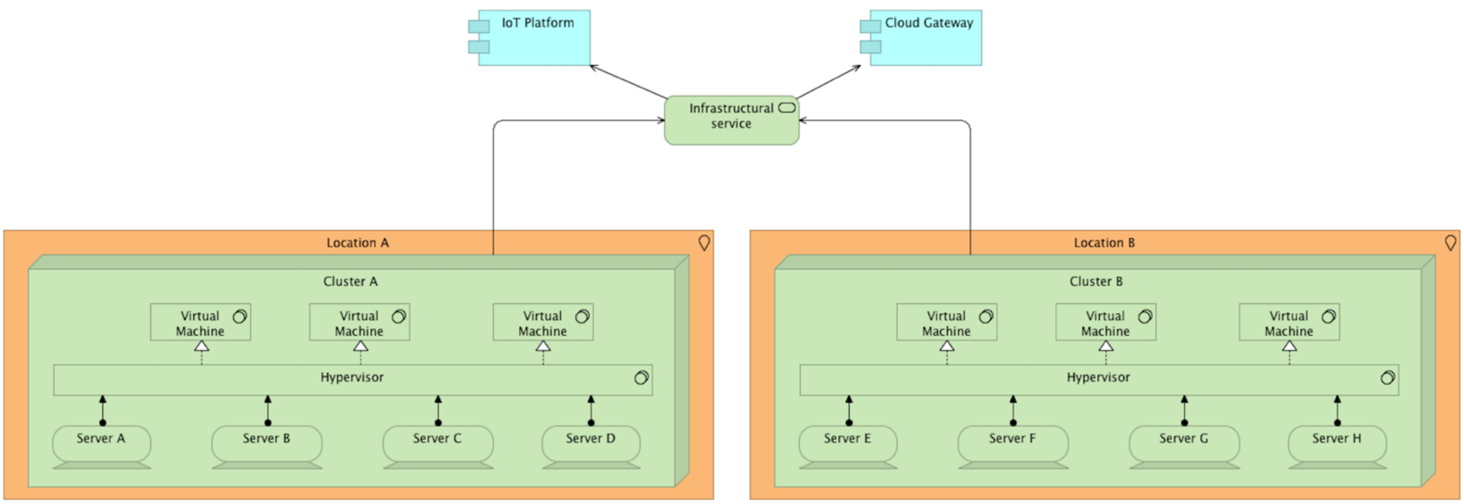

Figure 17. High Availability

5.6 Business layer

In this section, we will outline the most important part of the architectural approach, namely the business layer. Although it is not the most emphasized part of this study, we definitely have to take into account this layer as well. This layer describes how the underlying layers are creating value for the business processes of a Smart City.

In the application layer section, we have ended the model with the messaging service of the IoT platform. This service feeds the city applications with data of the objects. The city applications can be a traffic management application, crowd control application, and so on. The city applications can be built from scratch or on top of the IoT platform.

City applications provide services to the upper layers, such as the air pollution application that enables the air pollution services used by the environmental processes of the environmental city domain.

One important aspect that emerged in this model is depicted in the crowd control service. Due to the agnostic gateway layer, it is now possible to use data from one city domain in another city domain. The crowd control service is used in the traffic process, citizen management process and garbage process. Nowadays, it is often the case that these domains are operating separately with specific IoT solutions, which eventually results in a city of islands with their own set of data, knowledge and IoT infrastructure.

In addition to that, it is important to note that the solution we have provided is not the only answer to the smart city challenges. Our approach can be regarded as a bottom-up approach by providing scalability and interoperability to encounter the challenges. In other words, our architectural approach is a supporting factor to realize that specific need. It is a prerequisite that the city domains have to work together in order to achieve this. The architectural approach should be regarded as a means to realize the collaboration of city domains.

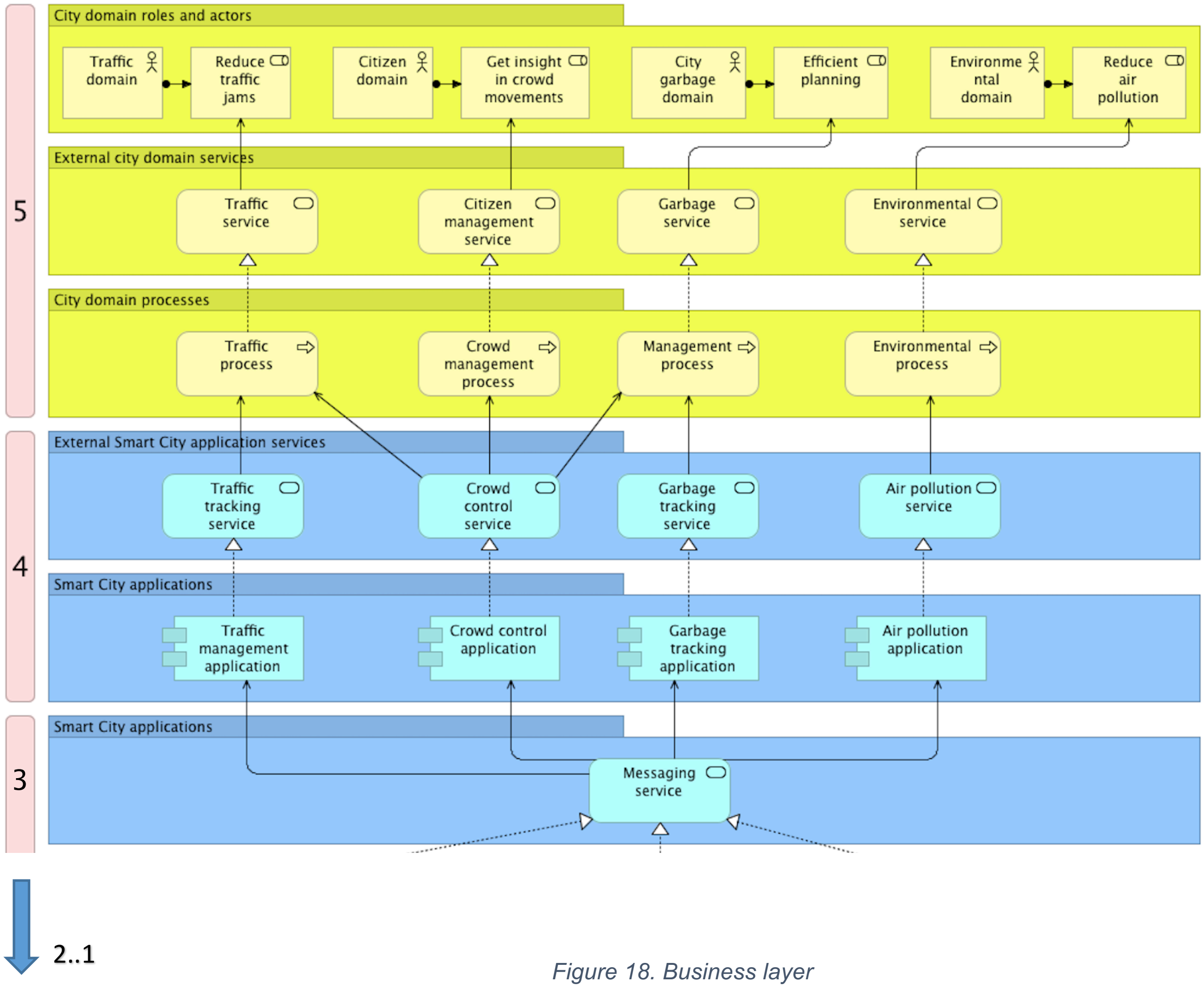

Figure 18. Business layer

5.7 Conclusion

The aim of this chapter was to answer the second part of the research question: "Are existing architectural approaches capable of satisfying the criteria and if not, how can a new architectural approach satisfy the criteria?" The focus of this chapter was to define a novel architectural approach that satisfies the constraints and fulfills the gap of the existing architectural approaches. The result of the previous chapter was that ClouT/BigClouT is the most potential IoT platform for a Smart City. However, there are a number of aspects that require attention, such as auto discovery and high availability. Furthermore, this approach also not included an IoT agent that can be implemented in the object itself. Only Cumulocity provides this feature, which is a suitable solution for objects that have sufficient computing and power capacity. Therefore, we have incorporated this feature in our architectural approach as well.

As a result, we introduced our novel architectural approach based on Archimate. We have described the technology, application and business layer. Moreover, we have explained how we will provide auto discovery and high availability. We argue that our architectural approach addresses the scalability and interoperability challenges IoT in a Smart City. The main reason for argument is as follows. First, our architectural approach supports the majority of IoT protocols and standards via the agnostic SensiNact gateway. Second, we provide auto discovery by making use of the native auto discovery mechanisms of the protocols and use additional components when auto discovery is not natively supported, such as MQTT. Next, our approach includes how high availability can be guaranteed and capacity can be adapted conform the magnitude of the context through clustering and virtualization. On top of that, the business layer reflects how the architectural approach allows Smart City domains to cooperate and adds value to Smart City activities. However, it is important to note that the Smart City domains must be willing to cooperate, which means that the governance of a city has to be established properly. The architectural approach should be regarded as a means to realize the collaboration of the city domains.

Chapter 6: Case Study & Expert Validation

The aim of this chapter is to answer the research question: "*Assuming the architectural approach can satisfy the criteria, can we evaluate it in form of a case study?*" We argue that the proposed architectural approach is suitable for the Volvo Ocean Race (VOR). First, the agnostic gateway allows the VOR to communicate with various data sources, which enables interoperability. Second, our approach enables scalability in terms of capacity and performance by virtualization and clustering techniques, which makes the approach suitable for small as well as large events. Next, we also validate our architectural approach trough an expert validation that allows us to verify the approach from different perspectives.

6.1 Introduction

In this chapter, we aim to answer the research question "*Assuming the architectural approach can satisfy the criteria, can we evaluate it in form of a case study?*" Since we proposed an architectural approach in the previous chapter that satisfies the criteria, we are able to evaluate it in a case study. To do so, we have selected the Volvo Ocean Race (VOR) as case study since we believe that it has the appropriate contextual setting that is similar to a Smart City. First, we will introduce the VOR case study by describing the IoT applications and coherent challenges. Second, we will model the platform used by the VOR based on our proposed architectural approach. In this way, we are able to evaluate whether our architectural approach is capable of addressing IoT challenges of the VOR.

6.2 Case study: Crowd Movement Volvo Ocean Race

The Volvo Ocean Race (VOR) is one of the largest sailing events in the world. A group of sailors is competing in a race of nine months throughout the world to cross the finish line. The race will finish in The Hague at the end of June 2018. The finish is a big event that attracts a great number of visitors. This makes the event a suitable case for a Smart City where also a large number of people are involved.

Students from the Leiden University have worked, together with The Hague Security Delta (HSD), on a number of ideas to organize this event as smooth as possible. The HSD is a security cluster that closely collaborates with organizations such as universities and governmental institutions to tackle challenges in the field of cyber security.

One of the promising ideas, that is emerged from the collaboration of the students and HSD, is to track the movement of a large number of people. This can be useful for big events and large cities to get insight how people are moving in certain areas. Based on the insight, cities and event organizations can, for instance, anticipate on disasters or formulate strategies to let the crowd flow as smooth as possible. The fundamental question regarding this study is how data of various data sources can be fed into the platform that is used by the organization of the Volvo Ocean Race event so that interoperability of the multiple IoT solutions, as well as, data sources can be guaranteed. There are a number of data sources within the city that collects data necessary to determine the movement of crowds. These sources can be regarded as city and police cameras, telecom base station of KPN, Wi-Fi access points and noise sensors. Therefore, we can argue that the infrastructural environmental of the platform can be regarded as heterogeneous. This makes it challenging to fed data sources uniformly into the platform since we have to deal with various connectivity protocols and messaging architectures, which makes interoperability a significant challenge. For this very reason, we have developed an architectural approach that addresses these challenges. Therefore, we will use this particular case to validate whether our proposed architectural approach is suitable for this contextual setting or not. To do this, we will start at the technology layer by describing the infrastructural components of the Cloud Event platform. Second, we will model the application layer by describing how various data sources are fed into the platform through the SensiNact gateway. Finally, we will model the business layer to show how business value is created. The architectural model of crowd movement function is depicted in Figure 19 on the next page.

Crowd Movement Model

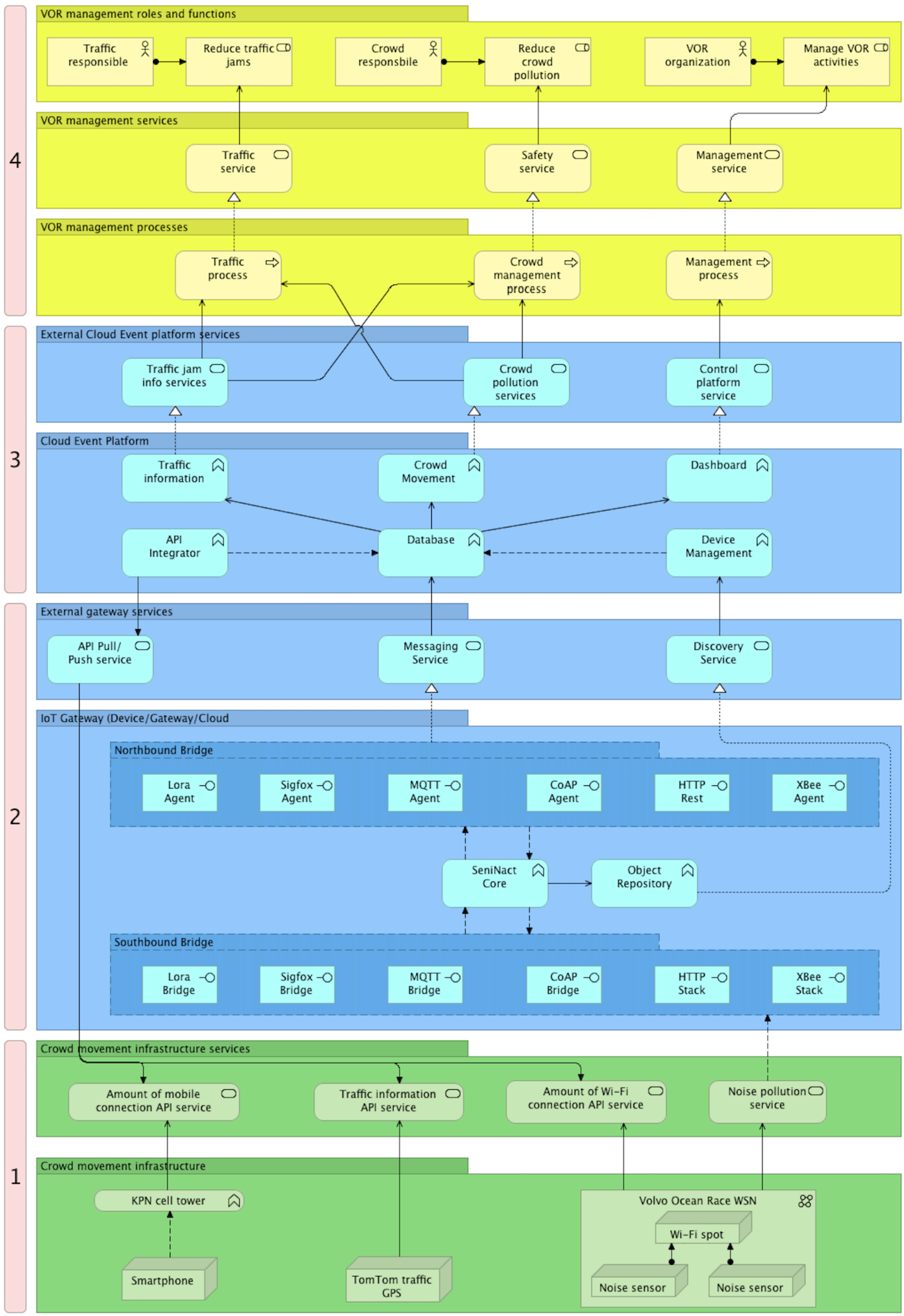

Figure 19. Crowd Movement architectural model

Technology layer

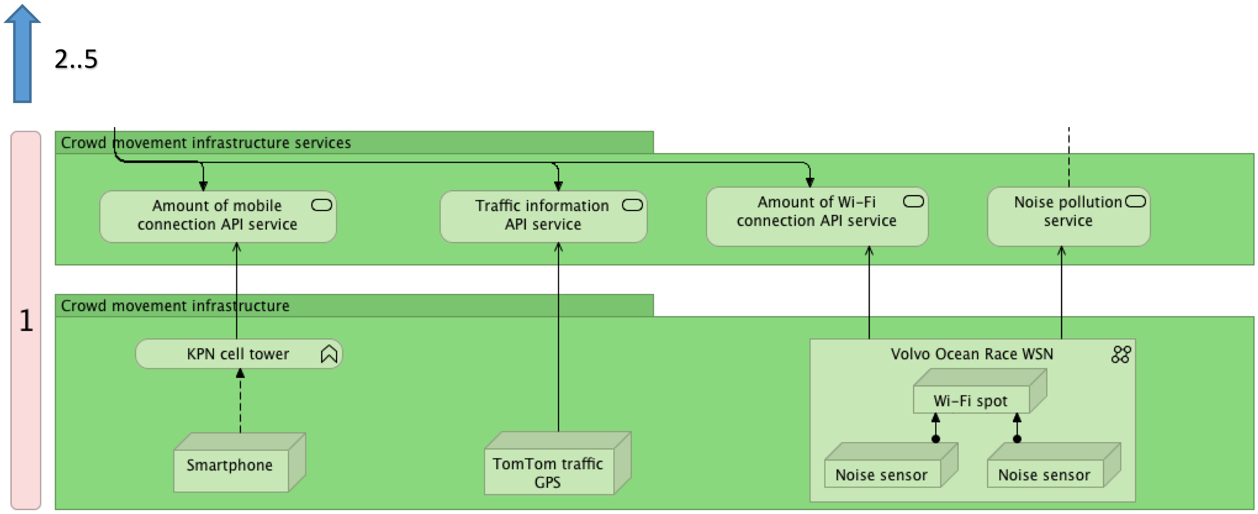

Figure 20. Crowd movement technology layer

As depicted in Figure 20, the crowd movement application is making use of various data sources. Most of the data sources are managed by third parties such as the KPN and TomTom, which offers data in form of API services. KPN offers API services that provide the number of connected smartphones to the KPN cell towers. This information is valuable to get insight where people are present. TomTom offers traffic information API's that are used to get insight of traffic towards the VOR. Next to that, the VOR and The Hague has implemented Wi-Fi access points to offers internet services to citizens and Volvo Ocean Race visitors. The number of connected smartphones to these access points is also used to get insight on where people are present. The VOR organization is thinking about placing noise sensors to get a more accurate indication of the number of people in certain areas. These sensors can be incorporated by the existing Wi-Fi access points, which then results in two services, namely the number of Wi-Fi connections and noise pollution.

Application layer

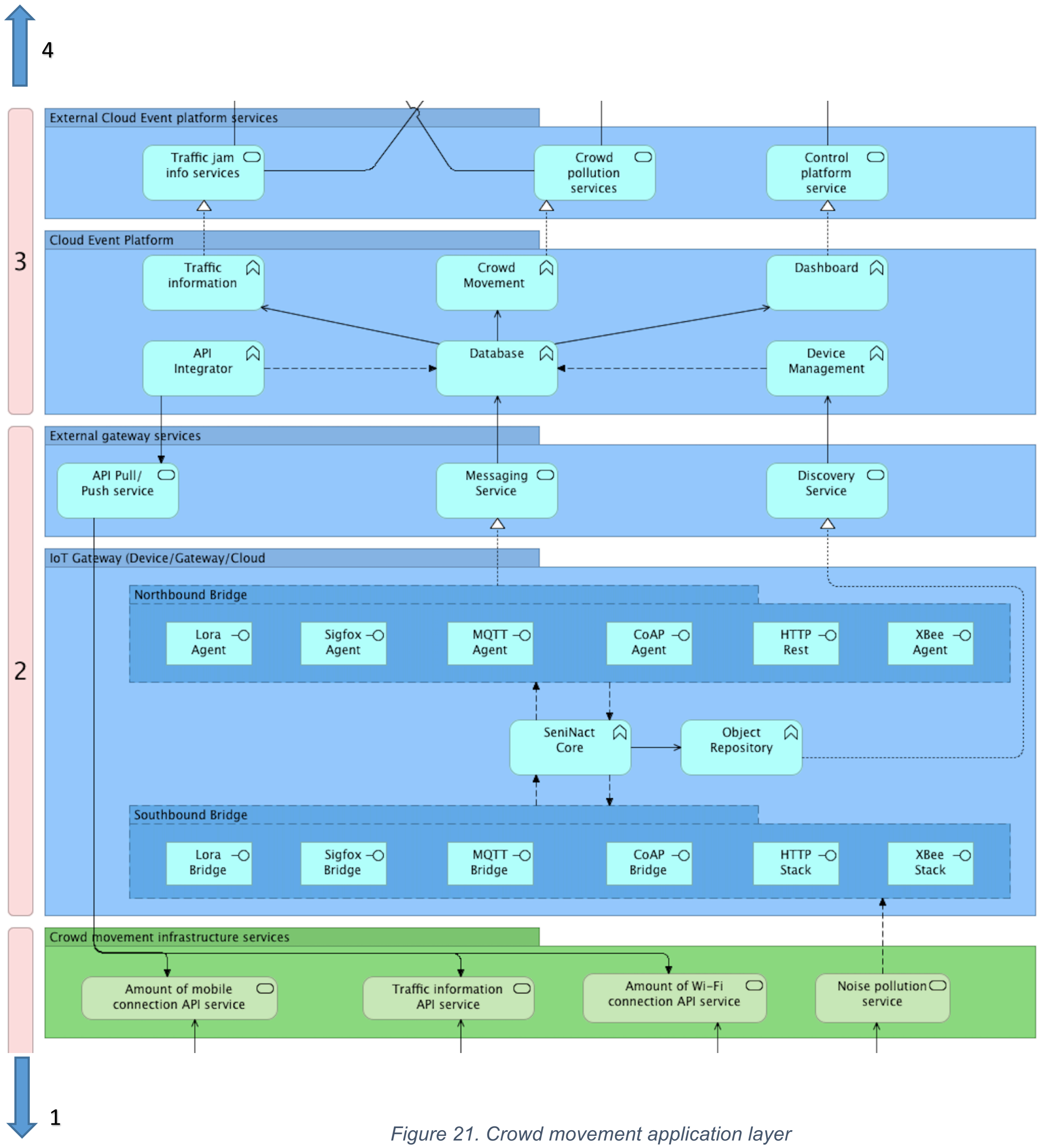

Figure 21. Crowd movement application layer

As ended in the previous section, the technology layer consists of data sources that provide services to the platform. These services are depicted on the green layer at the bottom of the model in Figure 21. All services, except noise pollution, are offered in the form of API's. It is not necessary for the API's to go through the gateway since no translating activities are required. The API services are directed to the API integrator of the platform via the API pull and push service. This service is in charge of retrieving (pull) or receiving data (push). The data of the API's are stored in the database which can then be used in the platform. The noise pollution service is offered by noise sensors that are connected via the Wi-Fi access points. In this case, the Wi-Fi acts as the SensiNact gateway to translate object specific protocols (Southbound bridge) into the language that is interpretable by the platform (Northbound bridge). The activities in the gateway are offered as a messaging service to the platform. As a result, the platform uses the messaging and API services for the crowd movement, dashboard and traffic information application.

The crowd movement application provides a simulation model to predict where crowd pollution can occur. The traffic information application offers visitors information regarding traffic jams, free parking spaces, and so on. The dashboard offers the VOR organization a centralized dashboard to manage certain tasks such as placing messages and creating alerts. The activities of the applications are provided as traffic jams info services, crowd pollution services and control platform services to the business processes.

Business Layer

We have ended the previous section with the application services that are provided by the Event Cloud platform. As we can see, we have defined three business processes. Namely, traffic process which aims to reduce traffic jams, crowd management process that aims to reduce crowd pollution and management processes to manage the organizational activities of the VOR. All these processes are carried out by teams that are responsible for a specific set of activities within the process. Since the heterogeneous data sources are uniformly fed into the platform, it is possible to offer services in multiple domains. For instance, the crowd pollution service can now be used for the traffic as well as the crowd management process. In this way, the team responsible for reducing traffic jams can also use noise sensor data and, similarly, the team responsible for reducing crowd pollution can use traffic data from TomTom's API to predict more accurately.

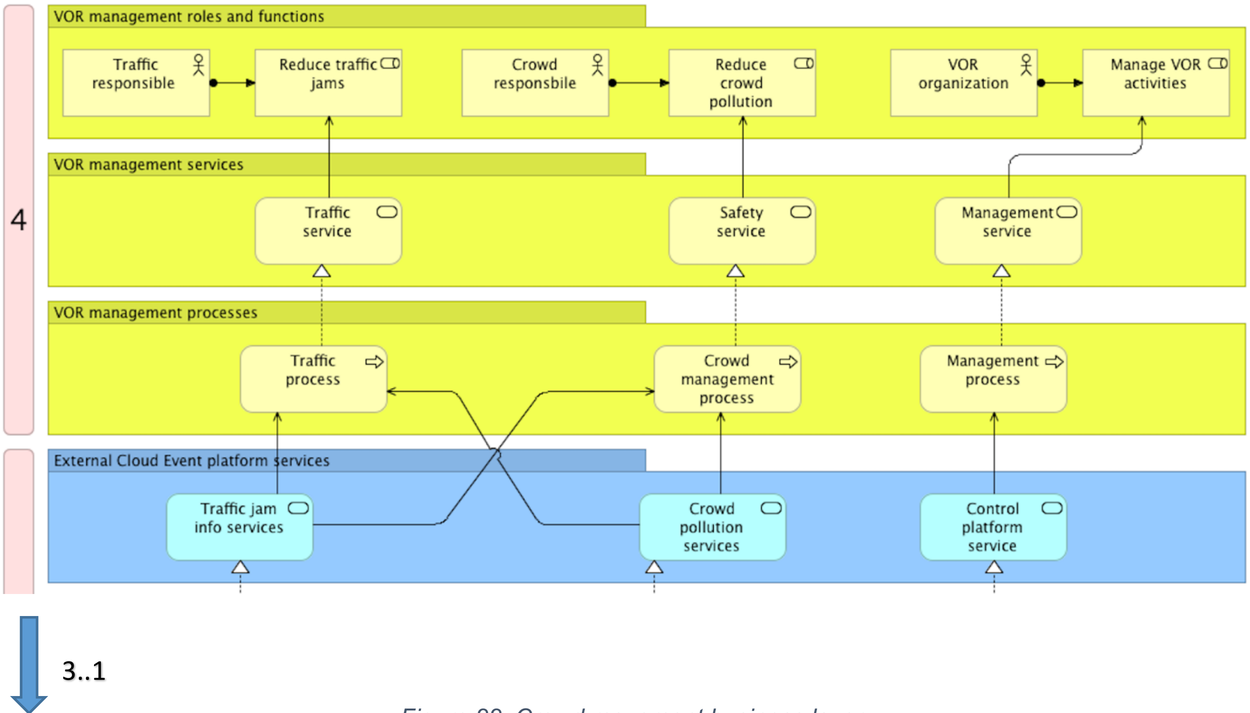

Figure 22. Crowd movement business layer

6.4 Improvements on the architectural approach

The case study of the VOR and the expert validation allows us to validate our novel architectural approach. To that end, a number of improvements have been emerged on the technical and application layer. In this section, we will go through the model and apply these improvements in the form of a new version. We will start with the technical layer followed by the application layer. At the end of this section, we will provide a new version of the model.

Technical layer 2.0

We have learned from the case study that many data sources of the VOR are deployed by third parties such as KPN, TomTom and 9292. The third parties offer data in form of API's to the VOR organization. Initially, third-party datasets were not a part of the architectural approach. Therefore, we have included the third-party datasets in the new version of the architectural approach. These datasets are offered via API services to the application layer, which is described in the next section. Based on the expert interview, we have included the core translation server that is responsible for translating the packages before it can be sent to the cloud. Moreover, we have replaced HTTP and XMPP protocol by binary and ASCII since these formats are often used on this layer. The new version is illustrated in figure 23.

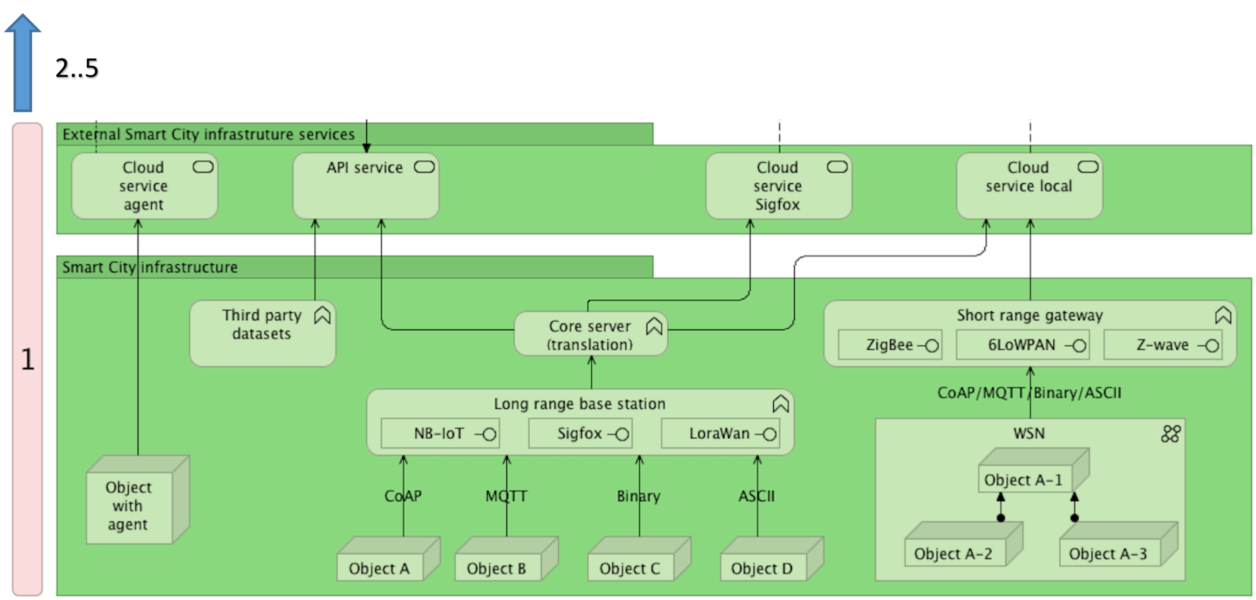

Figure 23. Technical layer 2.0

Application layer of the gateway 2.0

In the application layer of the gateway, we have included an API Pull/Push service that is directly linked to the third-party API service. In that way, third-party API's can be pulled/pushed to/from the IoT platform. It is not required that third-party API's are going through the gateway since no translating activities are required. Data from these services are in a format that is interpretable by the platform and can therefore directly fed into it. We also distinguished the northbound bridge in the actual bridges and agents. The bridges can be considered as the payload format that are used for the communication to the application. The new version of this layer is depicted in Figure 24 below.

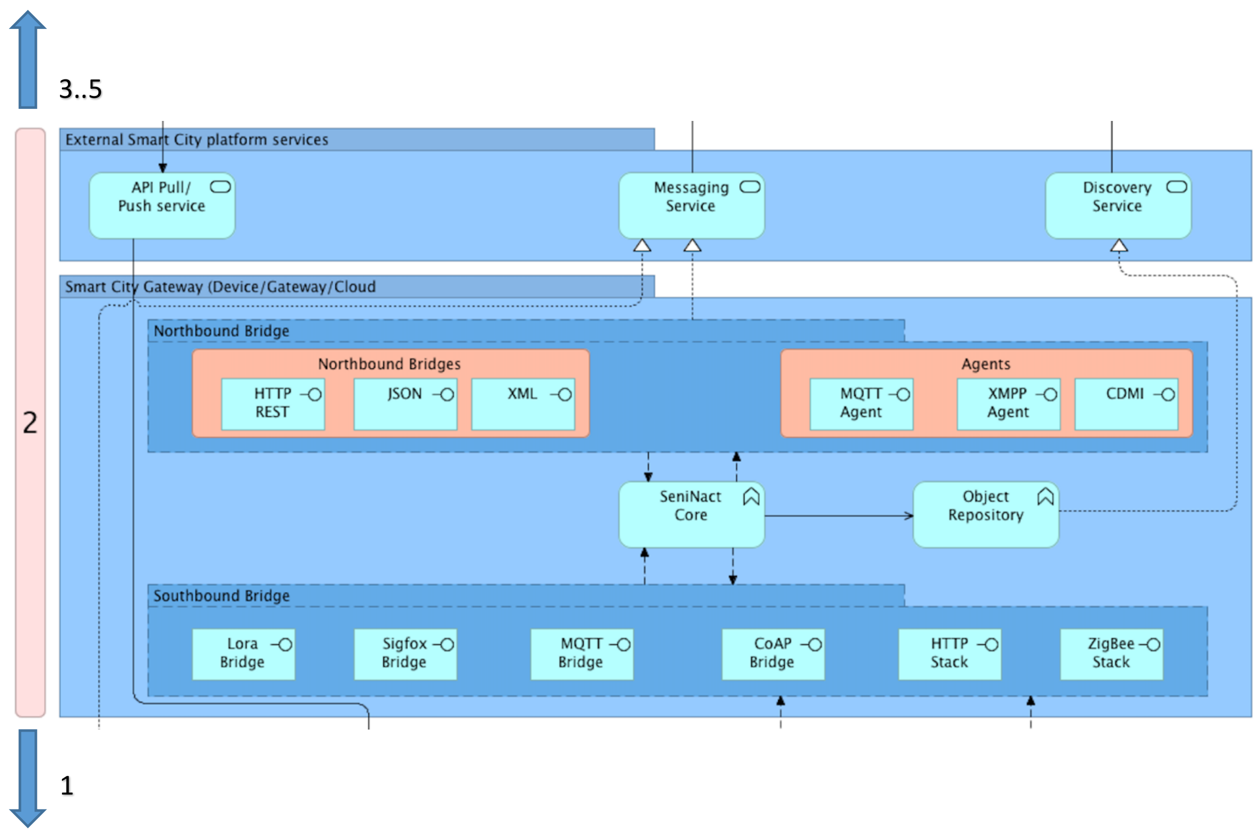

Figure 24. Application layer of the gateway 2.0

Application layer of the IoT platform 2.0

In the application layer of the IoT platform, we have included the API integrator that acts as a module that is in charge of pushing/pulling API's via the API service. Moreover, we have included a database that data retrieved from the API's, data from the gateway and data from the device management module. The database serves the A.I / machine learning, data analytics and data visualizations modules of the IoT platform. The new version of this layer is depicted in Figure 25 below.

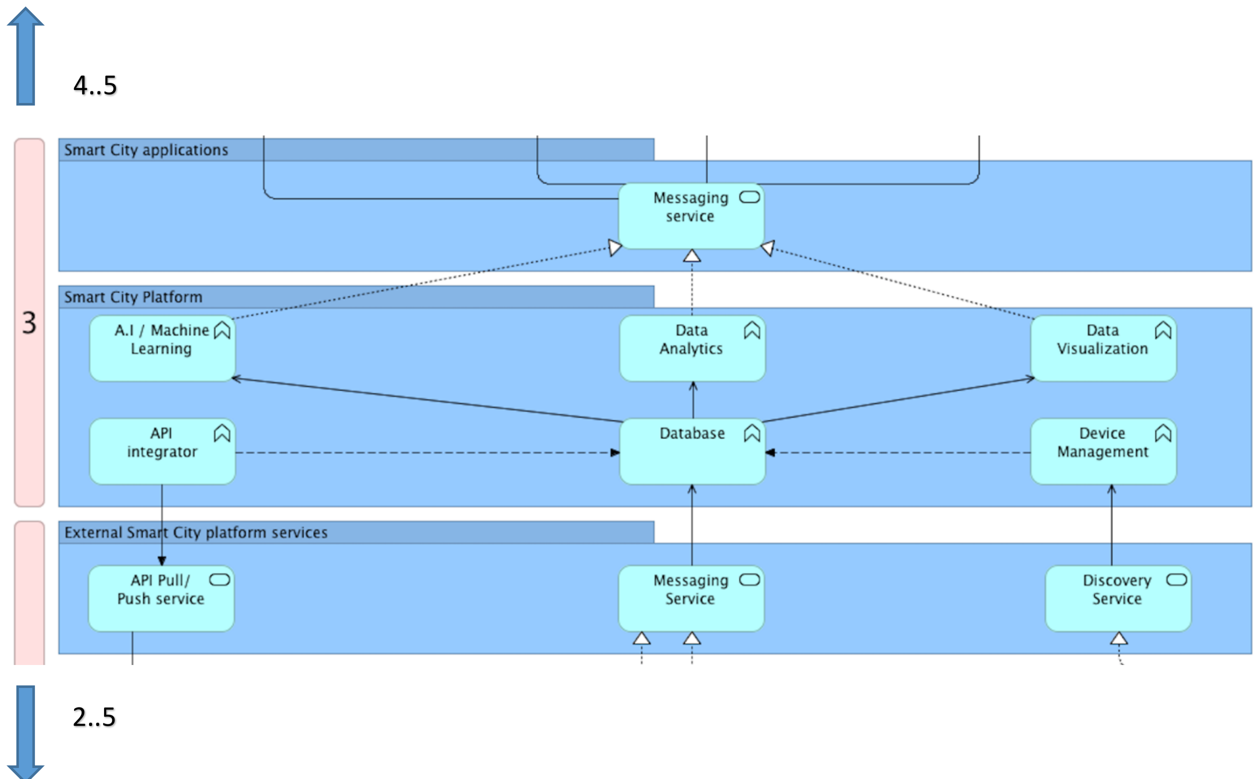

Figure 25. Application layer of the IoT platform 2.0

6.5 Architectural approach 2.0

Based on the new insights of the case study, we have revamped our architectural approach in a new version. Version 2.0 takes into account the third-party API's as well as a database to store the collected data. The new version is depicted in Figure 26 below.

Architectural approach 2.0

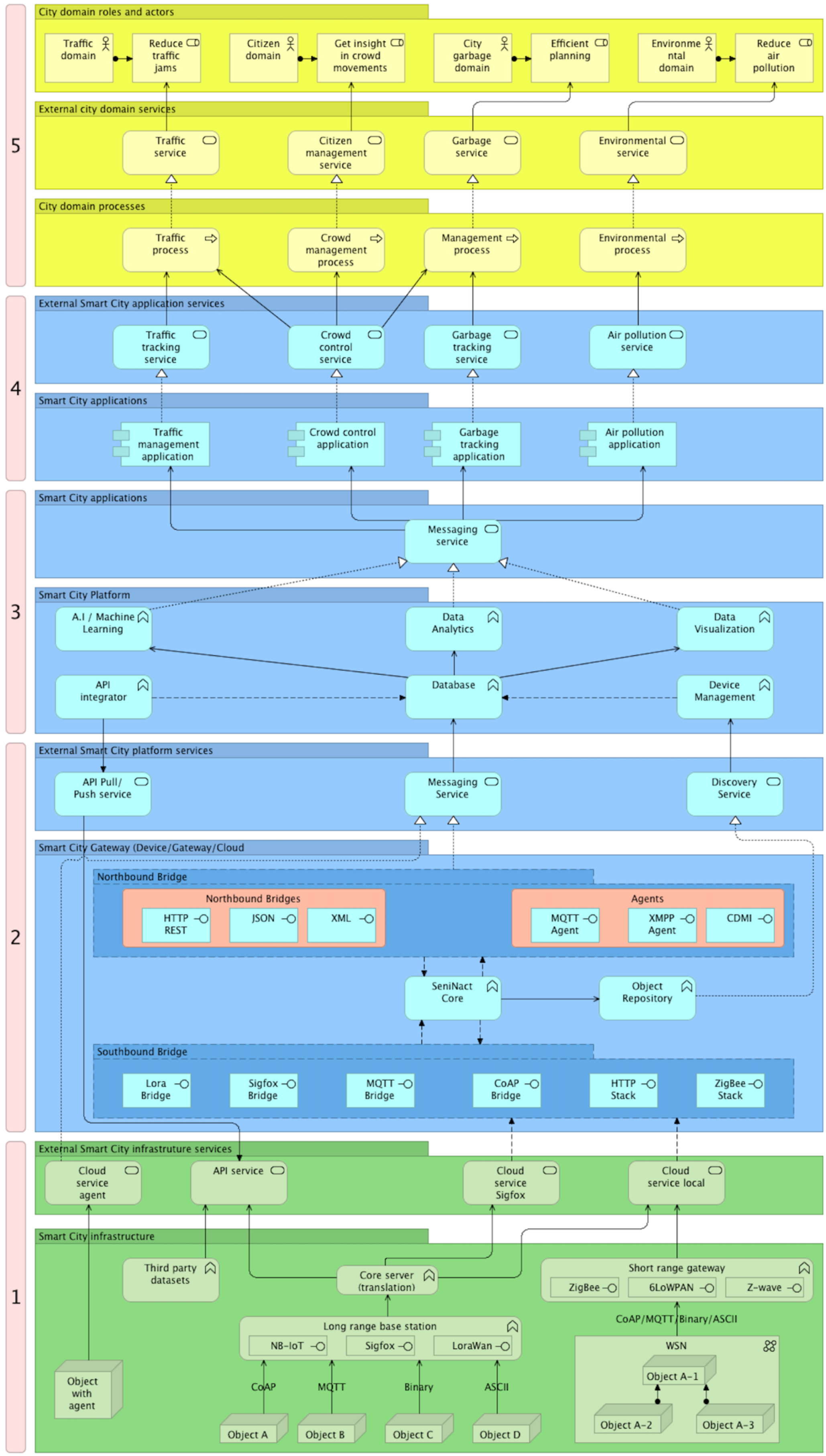

Figure 26. Architectural Approach 2.0

6.6 Conclusion

The case study shows that the new version of the architectural approach is suitable for the VOR. It exhibits the capability in addressing the interoperability and scalability challenges of events where a large number of people are present and many data sources are used. The SensiNact gateway allows the VOR organization to simply extend the range of data sources and sensors. There are no additional gateways and platforms required when the organization wants to make use of more data sources to, for instance, control lights of the events or track sailors nearby the coast by using LPWAN sensors. The SensiNact gateway handles the majority of standards and protocols used in the IoT era. This makes the proposed architectural approach interoperable as well as scalable. First, it is interoperable since it can handle various IoT standards and protocols. Second, it is scalable since it can be used for relatively small events, like the VOR, where only a handful IoT solutions are used and it can be simply extended to environments where a great number of IoT standards and protocols are being used. Moreover, our proposed architectural approach is also scalable in terms of performance and availability through virtualization and clustering techniques, which makes it suitable for both small and large events.

Next to the case study, we also validated our architectural approach through an expert validation that allowed us to verify the model from a different perspective. The outcome of this validation was that auto discovery is, security-wise, not realistic in public networks such as a Smart City. The communication of the auto discovery process goes through open ports that is, in theory, accessible by everyone on the internet. Therefore, it is not safe to implement auto discovery mechanisms in a Smart City. However, it might be applicable in private network environment behind a firewall, which can block unwanted visitors from the network. Moreover, we have incorporated the core server and payload format in the architectural approach since these components can be considered as key in an IoT architecture.

At the end of this chapter, we have provided an improved version of the architectural approach which includes the outcomes of the case study and expert validation.

Chapter 7: Conclusions

The aim of this chapter is to answer the main research question: "*To what extent can IoT challenges in Smart City be addressed by means of an architectural approach?*" The main conclusion is that our novel architectural approach allows a Smart City to implement IoT solutions in a scalable and interoperable manner. Our approach includes an agnostic gateway that effectuates interoperability of IoT. Next, we also provide an approach to auto discover objects, which minimizes the human intervention of managing objects. Lastly, we provide an approach that that guarantee scalability in terms of performance and availability through virtualization and clustering techniques.

7.1 Introduction

In this last chapter, we will fulfill the last part of this study with a final conclusion. This conclusion includes all research questions of this study and will answer the main research question: "*To what extent can IoT challenges in Smart City be addressed by means of an architectural approach?*" First, we will provide the main conclusion followed by a separate concise conclusion of each research question. In this way, we will be able to go throughout the research process to highlight the findings. Second, we will provide a section where we discuss the role of a data scientists and the application of cross-functional teams in a Smart City. At the end, we will provide four subjects for implication and suggestions for further research. These subjects are security, use cases in a Smart City, collaboration of city domains and validation of the SensiNact gateway

7.2 Main conclusion

The main research question of this study is "*To what extent can IoT challenges in Smart City be addressed by means of an architectural approach?*" We conclude that our novel architectural approach allows a Smart City to implement IoT solutions in a scalable and interoperable manner. We argue that our approach intervenes the silo IoT initiatives that mostly results in inefficiencies, less effective solutions and extra costs. Our approach includes an agnostic gateway that can handle various standards and protocols used in the IoT era. To that end, we are able to effectuate interoperability of IoT solutions that are implemented in Smart City domains. Next, we also provide an approach to auto discover objects, which is an important feature to realize scalability. This approach minimizes the human intervention of managing objects in a Smart City. Lastly, we provide an approach that guarantees scalability in terms of performance and availability, which is realized by virtualization and clustering techniques. These techniques allow us to increase or decrease the hardware capacity without affecting the daily operations. Moreover, in case of hardware failure, the nodes will continue delivering services since multiple hardware nodes are virtually acting as one single node which eliminates the single point of failure. At the end, we have validated our architectural approach through a case study and expert validation. This case study underlined that our architectural approach is applicable in the context where a) a large number of people are present and b) various IoT solutions, as well as, data sources are being used. This contextual setting is representative for a Smart City. The expert validation allowed us to verify our approach through a practical perspective. A number of essential factors such as auto discovery, core servers and payload formats are discussed and the outcomes are incorporated in a new version of the architectural approach, which made our architectural approach more robust.

Conclusion per research question

We will substantiate our conclusion by concisely underlining each research question. In this way, we are able to go throughout the research process and underline our main conclusion appropriately.

1. How is IoT involved in Smart City and what are the challenges?

Smart City is a concept that creates benefits for citizens such as well-being and environmental quality by means of innovative technology. One of the fundamental technologies is IoT, which allows a large variety of objects to connect to the worldwide internet. In that way, a city can control these objects and perform smart activities with it. However, there are some frictions in the concept of IoT and context of Smart City that resulted in various challenges. We have identified scalability and interoperability as an imperative challenge and will focus on this during the rest of the study. First, we have identified scalability as a challenge since a large group of people is moving from plural to urban areas. Moreover, this concept is applied in cities varying from thousand to hundreds of millions of citizens. Second, we have identified interoperability as a challenge since a city can be considered as a system of independent systems that have a common goal to transform the city into a Smart City. In order to make this transformation seamless and efficient, these domains have to cooperate and collaborate intensively. Otherwise, this transformation will be inefficient, costly and unlikely.

2. What criteria are required to address the IoT challenges in a Smart City?

As we have identified the challenges of IoT in a Smart City in the previous research question, the next step is to define the criteria that are required to address these challenges. The main conclusion is that there is no one-size-fits-all solution suited for all domains of a Smart City. Therefore, we have to embrace the standards and protocols that are used in the IoT era to gain interoperability in a Smart City. To do so, we have defined a set of constraints in which an architectural approach should comply to assure interoperability on this level. In addition to that, we also identified two main features, which are auto discovery and virtualization and clustering, which allows scalability and interoperability in a Smart City.

3. Are existing architectural approaches capable of satisfying the criteria and if not, can a new architectural approach satisfy the criteria?

The deliverable of the previous research question was a comparative framework, which is used as input to answer this research question. We have analyzed four architectural approaches and evaluated them based on the set of constraints. The main conclusion was the architectural approaches were not capable of satisfying all six constraints. None of the approaches include full auto discovery mechanisms and some of them were not capable of supporting a number important standards and protocols. Moreover, none of the architectural approaches, provides a uniform model that illustrates the building blocks in a comprehensible and coherent manner. We argue that a uniform model is an imperative mean to communicate the architectural approach as effective as possible to the public. At last, none of the architectural approaches shows how value is created in a Smart City. We argue that it the most important part to assure the stakeholders that the architectural approach is worth implementing it.

Therefore, we have proposed a novel architectural approach that a) satisfies all constraints, b) is based on a uniform modeling language and c) shows how value is created in a Smart City. We have selected Archimate since it an open enterprise architecture modeling language that is widely used in the architectural era. This modeling language also shows how certain technology solutions add value to the business. Our main conclusion is that our architectural approach addresses the interoperability and scalability constraints since we support the majority of IoT protocols and standards via the agnostic SensiNact gateway. Moreover, we provide auto discovery by making use of the native auto discovery mechanisms of the protocols and use additional components when auto discovery is not natively supported, such as MQTT. Lastly, our approach includes how high availability can be guaranteed and capacity can be adapted conform the magnitude of the context through clustering and virtualization techniques.

4. Assuming the architectural approach can satisfy the criteria, can we evaluate it in form of a case study?

In the previous research question, we argued that our proposed architectural approach satisfied all constraints. Therefore, we were able to evaluate our proposed architectural approach in a case study. We have performed this evaluation in the Volvo Ocean Race (VOR). The main conclusion is that our architectural approach is suitable for the VOR since we have shown that our approach is scalable as well as interoperable. First, it is interoperable since it can handle various IoT standards and protocols. Second, it is scalable since it can be used for relatively small events, like the VOR, where only a handful IoT solutions are used, and it can be simply extended to environments where a great number of IoT standards and protocols are being used. Moreover, we have also validated our model through an expert validation that allowed us to validate the approach from a practical perspective.

7.3 Implications and further research

In this section, we will describe the implications and suggestions for further research. First, we will start with security followed by use cases for Smart Cities, city domain collaboration and the validation of the SensiNact gateway. Moreover, we will provide a description how our study is related to the field of data science and cross-functional teams.

Security

Although security is excluded in our study, we argue that it should be one of the top priorities. Security is one of the main concern of IoT and in particular Smart Cities. A significant number of objects that are supporting daily activities are exposed to the world-wide internet. The abuse of these objects can have, therefore, tremendous impact in a city. For instance, the manipulation of deployed sensors in strategic areas in a city. In that case, people with bad intentions can have control in a city. In addition to that, the abuse of data is also possible. In worst case, data can be gathered to get insight in certain activities or track people.

Use cases for Smart City

In the course of the years, a significant number of standards and protocols have been introduced in the IoT era. Each set of standards and protocols have their own advantages in specific contextual settings. Therefore, one of the main conclusions of our study is to embrace the standards and protocols rather than exclude them. However, due to the large variety, we believe that is it not yet clear what set of standards and protocols creates the maximum value in certain contextual settings. To that end, more scientific studies are necessary to acquire certainty that the proper set of standards and protocols are implemented in a suitable context and thereby maximizing the value of IoT solutions.

Collaboration of city domains

The main deliverable of this study can be considered as a bottom-up approach to realize scalability and interoperability in a Smart City. It is important to note that the solution we have provided is not the only answer to the Smart City challenges. It is a prerequisite that the city domains have collaborate closely in order to achieve this. The architectural approach should be regarded as a mean to realize and encourage the collaboration. Hence, the governance body of a city is a crucial factor in the success of a Smart City.

Validation of the SensiNact gateway

One of the core components of our architectural approach is the agnostic SensiNact gateway that enables the interoperability of various standards and protocols. However, at this very moment, the gateway is going through the standardization process by the Eclipse community and is not yet available. Therefore, we were not able to validate the gateway on its capabilities. We argue that future research is required to thoroughly test the gateway prior to implementing it in a Smart City.

Auto Discovery security in Smart City

Auto discovery is currently not safe for Smart Cities. The communication of the auto discovery process is realized through an open port, which means in theory that everyone on the internet can access the objects. However, we have identified auto discovery as an important element of an architectural approach to enable scalability. Therefore, we argue that further research is necessary in the field of security and auto discovery mechanisms to enable scalability in Smart Cities.

Reference Architecture

Our proposed architectural approach can also be considered as a reference architecture for further research in the era of IoT. Scholars can use the model to have an overview of the crucial components of a scalable and interoperable IoT platform. Each component can be used for a deeper level of research. For instance, the SensiNact gateway is not released yet and considerable for further testing purposes or the research of secure auto discovery mechanisms in public areas.

Data Science

The deployed sensors in a city collect an enormous set of data that can be regarded as valuable input for data science purposes. Based on the collected data, especially from multiple city domains, new insight can be discovered which can be used to increase the life quality of citizens. However, due to the silo implementations of IoT solutions, the data cleansing process is getting more intensive and time-consuming. To that end, our architectural approach provides an agnostic gateway that is already performing some activities of the data cleansing process. The Southbound bridge is responsible for acquiring data from multiple data source and the Northbound bridge is in charge of providing the data in the preferred format. In this way, data from multiple sources can be provided by the gateway in a format that is interoperable by the data science tools. We can regard this as a plug-and-play approach where a data scientist does not have to be concerned about the technical environment of the data sources, and can only focus on his/her core competencies, namely deriving new insight and knowledge based on a large amount of data.

Cross functional teams

Our architectural approach encourages city domains to work in close collaboration. This is in line with the phenomenon of cross-functional teams, which praised by many scholars in this area. We describe this as a team of people, from various disciplines, that are closely working together in order to achieve a common goal. Cross-functional teams are the core of new project approaches such as Scrum. This project approach widely deployed in companies such as Spotify and Microsoft. The proponents of this approach argue that cross-functional teams tend to be more creative since they that have detailed data and knowledge of their domain. The combination of this provides teams new insight and stimulates the creativity process. Placing this in the context of the study, we believe that the collaboration of city domains in a Smart City will have a positive impact on the city in terms of innovation. This gives us extra stimulation the promote the architectural approach in a Smart City.

Summary and prioritization

In the sections above, we have provided a number of implications and arguments for further research. In this section, we prioritize the further research proposals in order to weight the gravity.

Priority	Further research proposal	Argument
1	Security	Security is the top priority for further research We must ensure that promising IoT solutions must always be secure so that it will not harm people.
2	Collaboration of city domains	We have listed this proposal as priority number two since the collaboration of city domains is a precondition for the success of our architectural approach.
3	Secure auto discovery	This proposal is listed as number three since auto discovery is an important element that addresses scalability challenges. However, due to security reasons, it is not safe to implement in a Smart City. Therefore, further research is required to implement a secure auto discovery mechanism in public environments to ensure scalability.
4	Validation of SensiNact gateway	The validation of the SensiNact gateway is listed as number four. This component is an important element to address interoperability challenges. However, due the novelty of this gateway, further research is required in form of validation.
5	Use cases for Smart City	The last proposal we have listed is the use cases for Smart City. Due to the large number of standards and protocols, it is not clear what set of standards and protocols creates the maximum value in certain contextual settings.

Table 10. Prioritzation of further reserach proposal

This section reveals that, in general, a great deal of research is required in the field of IoT and Smart City. This might be related by the novelty of these concepts. On that basis, our architectural approach is a good start to stimulate further research in this field. Our architectural approach provides the essential components of a scalable and interoperable IoT platform in a Smart City. To that end, scholars can zoom-in to get a deeper understanding on these matters.

References

Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melià-Seguí, J., & Watteyne, T. (2017). Understanding the Limits of LoRaWAN. *IEEE Communications Magazine*. Retrieved from https://arxiv.org/pdf/1607.08011.pdf

Aggarwal, N., Dai, Q., & Walden, E. A. (2012). Are open standards good business? https://doi.org/10.1007/s12525-011-0078-7

Anthopoulos, L. (2015). Defining Smart City Architecture for Sustainability. In *Electronic Government and Electronic Participation E. Tambouris et al.* Retrieved from http://eadic.teithessaly.gr/publications/12/paper 61.pdf

Anthopoulos, L., & Fitsilis, P. (2014). Exploring Architectural and Organizational Features in Smart Cities. In *16th International Conference on Advanced Communications Technology*. Retrieved from http://de.teilar.gr/publications/310/AnthopoulosICACT_Conf_paper_Final_v.1.pdf

Anthopoulos, L. G., Reddick, C. G., Rodríguez-Bolívar, M. P., Bolivar, M. P. R., Meijer, A. J., Chen, S.-C., Wu, C.-C., Eom, S.-J., Choi, N., Sung, W., Gil-Garcia, J. R., Zhang, J., Puron-Cid, G., Sayogo, D. S., Meijer, A. J., Gil-Garcia, J. R., Bolivar, M. P. R., Scholl, H. J., Scholl, M. C., & AlAwadhi, S. (2016). Smart City Research: Contextual Conditions, Governance Models, and Public Value Assessment. *Government Information Quarterly*, *55*(1), 255–277. https://doi.org/10.1177/0894439315618890

Antonic, A., Marjanovic, M., Skocir, P., & Zarko, I. P. (2015). Comparison of the CUPUS middleware and MQTT protocol for smart city services. *Proceedings of the 13th International Conference on Telecommunications, ConTEL 2015*. https://doi.org/10.1109/ConTEL.2015.7231225

Arenas, M., Corcho, O., Simperl, E., Strohmaier, M., D'Aquin, M., Srinivas, K., Groth, P., Dumontier, M., Heflin, J., Krishnaprasad, T., & Steffen, S. (2015). The Semantic Web. In *14th International Semantic Web Conference*. Springer. Retrieved from https://books.google.nl/books?id=OgO5CgAAQBAJ&pg=PA247&lpg=PA247&dq=registering+devices+openiot&source=bl&ots=mOdeuzpdA8&sig=grnJpvyy4I_l6hEAOTTLjZFmsQc&hl=en&sa=X&ved=0ahUKEwjtitHM3LDUAhWHbVAKHbnDAL4Q6AEIQTAF#v=onepage&q=registering devices openiot&f

B. Cohen. (2014). Methodology for 2014 Smart Cities Benchmarking. Retrieved March 2, 2017, from https://www.fastcoexist.com/3038818/the-smartest-cities-in-the-world-2015-methodology

BigClout. (2017). BigClouT - Big data meeting Cloud and IoT for empowering the citizen clout in smart cities. Retrieved June 7, 2017, from http://bigclout.eu/

Brian Ray. (2017). What is Narrowband IoT (NB-IoT)? - Explanation and 5 Business Benefits. Retrieved May 17, 2017, from https://iot-for-all.com/what-is-narrowband-iot-nb-iot/

BSI. (2014). *Mapping Smart City Standards*. London.

Central Policy Unit Hong. (2015). *Research Report on Smart City*. Retrieved from http://www.cpu.gov.hk/doc/en/research_reports/CPU research report - Smart City(en).pdf

Cirani, S., Davoli, L., Ferrari, G., Leone, R., Medagliani, P., Picone, M., & Veltri, L. (2014). A scalable and self-configuring architecture for service discovery in the internet of things. *IEEE Internet of Things Journal*, *1*(5), 508–521. https://doi.org/10.1109/JIOT.2014.2358296

ClouT. (2013a). *D1.3 – Final Requirements and Reference Architecture*.

ClouT. (2013b). *D2.3 – CIaaS specification and reference implementation*.

Cocchia, A. (2014). *Smart and Digital City: A Systematic Literature Review*. *International Journal of Distributed Sensor Networks* (Vol. 2014). https://doi.org/10.1155/2014/867593

Cumulocity. (2017). Cumulocity | Connect to innovate. Retrieved June 6, 2017, from http://cumulocity.com/

da Silva, W. M., Alvaro, A., Tomas, G. H. R. P., Afonso, R. a., Dias, K. L., & Garcia, V. C. (2013). Smart cities software architectures. *Proceedings of the 28th Annual ACM Symposium on Applied Computing - SAC '13*, 1722. https://doi.org/10.1145/2480362.2480688

Dameri, R. P. (2016). *Smart City Implementation*. Springer International Publishing AG. https://doi.org/10.1007/978-3-319-45766-6

Desai, P., Sheth, A., & Anantharam, P. (2015). Semantic Gateway as a Service architecture for IoT Interoperability. *IEEE Software*, *32*(2). https://doi.org/10.1109/MS.2015.51

Eclipse. (2017). SensiNact/Gateway Overview. Retrieved June 20, 2017, from https://wiki.eclipse.org/SensiNact/Gateway_Overview

Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). The Internet of Things : New Interoperability, Management and Security Challenges. *International Journal of Network Security & Its Applications*, *8*(2), 85–102. https://doi.org/10.5121/ijnsa.2016.8206

Endo, P. T., Rodrigues, M., Gonçalves, G. E., Kelner, J., Sadok, D. H., & Curescu, C. (2016). High availability in clouds: systematic review and research challenges. *Journal of Cloud Computing*. https://doi.org/10.1186/s13677-016-0066-8

Gartner. (2016). Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018. Retrieved May 17, 2017, from http://www.gartner.com/newsroom/id/3221818

Gartner. (2017). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Retrieved May 29, 2017, from http://www.gartner.com/newsroom/id/3598917

Gordon E. Moore. (1965). Cramming more components onto integrated circuits. *Electronics*, *38*(8).

GSMA. (2017). Narrow Band – Internet of Things (NB-IoT) | Internet of Things. Retrieved May 15, 2017, from http://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/

Happ, D., & Wolisz, A. (2017). Limitations of the Pub/Sub pattern for cloud based IoT and their implications. *2016 Cloudification of the Internet of Things, CIoT 2016*. https://doi.org/10.1109/CIOT.2016.7872916

Hussain, M. I. (2016). Internet of Things: challenges and research opportunities. *CSI Transactions on ICT*, *5*(1), 87–95. Retrieved from http://download.springer.com.ezproxy.leidenuniv.nl:2048/static/pdf/532/art%253A10.1007%252Fs40012-016-0136-6.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Farticle%2F10.1007%2Fs40012-016-0136-6&token2=exp=1491749800~acl=%2Fstatic%2Fpdf%2F532%2Fart%25253A1

IBM. (2017a). IBM Watson Internet of Things (IoT). Retrieved June 7, 2017, from https://www.ibm.com/internet-of-things/

IBM. (2017b). Introduction to MQTT. Retrieved May 21, 2017, from https://www.ibm.com/support/knowledgecenter/SS9D84_1.0.0/com.ibm.mm.tc.doc/tc00000_.htm

IBM Bluemix. (2017). Watson IoT Platform. Retrieved June 13, 2017, from https://console.ng.bluemix.net/docs/services/IoT/iotplatform_overview.html#about_iotplatform

IEC. (2014). *Orchestrating infrastructure for sustainable Smart Cities*. Retrieved from https://www.ceps.eu/system/files/iecWP-smartcities-LR-en.pdf

International Telecommunication Union. (2012). New ITU standards define the internet of things and provide the blueprints for its development. Retrieved from http://www.itu.int/ITU-T/newslog/New+ITU+Standards+Define+The+Internet+Of+Things+And+Provide+The+Blueprints+For+Its+Development.aspx

James Stansberry. (2015). MQTT and CoAP: Underlying Protocols for the IoT. Retrieved May 19, 2017, from http://www.electronicdesign.com/iot/mqtt-and-coap-underlying-protocols-iot

Kakarontzas, G., Anthopoulos, L., Chatzakou, D., & Vakali, A. (2014). A conceptual enterprise architecture framework for smart cities: A survey based approach. *11th International Conference on E-Business, ICE-B 2014 - Part of 11th International Joint Conference on E-Business and Telecommunications, ICETE 2014*, 47–54. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84910028379&partnerID=40&md5=a47489346e501d41f5dbf3bfbfa7a1e1

Karagiannis, V., Chatzimisios, P., Vazquez-Gallego, F., & Alonso-Zarate, J. (2015). A Survey on Application Layer Protocols for the Internet of Things. *Transaction on IoT and Cloud Computing*, *3*(1), 11–17. https://doi.org/10.5281/ZENODO.51613

Kefalakis, N., Petris, S., & Soldatos, J. (2013). *Core OpenIoT Middleware Platform* (Vol. 12). Retrieved from http://cordis.europa.eu/docs/projects/cnect/5/287305/080/deliverables/001-OpenIoTD431Draft.pdf

Kefalakis, N., Soldatos, J., Anagnostopoulos, A., & Dimitropoulos, P. (2015). A Visual Paradigm for IoT Solutions Development (pp. 26–45). Springer, Cham. https://doi.org/10.1007/978-3-319-16546-2_4

Kim, S. M., Choi, H. S., & Rhee, W. S. (2016). IoT home gateway for auto-configuration and management of MQTT devices. *2015 IEEE Conference on Wireless Sensors, ICWiSE 2015*, 12–17. https://doi.org/10.1109/ICWISE.2015.7380346

Le Vinh, T., Bouzefrane, S., Farinone, J.-M., Attar, A., & Kennedy, B. P. (2015). Middleware to Integrate Mobile Devices, Sensors and Cloud Computing. *The 6th International Conference on Ambient Systems*, *52*, 234–243. https://doi.org/10.1016/j.procs.2015.05.061

Li Qi, & Lin Shaofu. (2001). Research on digital city framework architecture. In *Research on digital city framework architecture* (Vol. 1, pp. 30–36). IEEE. https://doi.org/10.1109/ICII.2001.982715

Liu, M., Leppanen, T., Harjula, E., Ou, Z., Ylianttila, M., & Ojala, T. (2013). Distributed resource discovery in the machine-to-machine applications. *Proceedings - IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems, MASS 2013*, 411–412. https://doi.org/10.1109/MASS.2013.46

Lopez, P., Fernandez, D., Marin-Perez, R., Jara, A. J., & Gomez-Skarmeta, A. F. (2013). Scalable Oriented-Service Architecture for Heterogeneous and Ubiquitous IoT Domains. *Pervasive and Mobile Computing*, *0*, 1–23. Retrieved from https://arxiv.org/pdf/1311.4293.pdf

LoRa Alliance. (2017). LoRa FAQ. Retrieved May 13, 2017, from https://www.lora-alliance.org/The-Alliance/FAQ

Lyle, R. D., & Harrison, C. (2014). *Livable Cities of the Future: Proceedings of a Symposium Honoring the Legacy of George Bugliarell*. National Academies Press. Retrieved from https://www.nap.edu/read/18671/chapter/14

McKinsey & Company. (2015). The Internet of Things: Mapping the value beyond the hype. *McKinsey Global Institute*, (June), 144. https://doi.org/10.1007/978-3-319-05029-4_7

Medvedev, A., Zaslavsky, A., Khoruzhnikov, S., & Grudinin, V. (2015). Interoperability and Open-Source Solutions for the Internet of Things. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9001*(May 2016), 169–182. https://doi.org/10.1007/978-3-319-16546-2

Ojo, A., Dzhusupova, Z., & Curry, E. (2016). Exploring the nature of the smart cities research landscape. https://doi.org/10.1007/978-3-319-17620-8

OpenIoT. (2016). OpenIoT – Open Source cloud solution for the Internet of Things. Retrieved June 6, 2017, from http://www.openiot.eu/

Perera, C., Jayaraman, P. P., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context-aware dynamic discovery and configuration of “Things” in smart environments. *Studies in Computational Intelligence*, *546*(27), 215–241. https://doi.org/10.1007/978-3-319-05029-4_9

Peter Gutierrez. (2016). Is NB-IoT the LPWAN to rule them all? Retrieved May 17, 2017, from https://www.iothub.com.au/news/is-nb-iot-the-lpwan-to-rule-them-all-434240

Poudel, S. (2016). Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security. *Berkeley Technology Law Journal Annual Review*, *31*(2). https://doi.org/10.15779/Z38WW0V

R. Giffinger. (2007). *Smart Cities: Ranking of European medium-sized cities*. Retrieved from http://www.smart-cities.eu/download/smart_cities_final_report.pdf

Rahman, A. B. A. (2015). Comparison of Internet of Things (IoT) Data Link Protocols, 1–21. Retrieved from http://www.cse.wustl.edu/~jain/cse570-15/index.html

Raza, U., Kulkarni, P., & Sooriyabandara, M. (2017). Low Power Wide Area Networks: An Overview. *IEEE Communications Surveys & Tutorials*, *PP*(99). https://doi.org/10.1109/COMST.2017.2652320

Rémi Druilhe. (2016). IoT Open Platforms. Retrieved June 12, 2017, from http://open-platforms.eu/library/sensinact-aka-butler-smart-gateway/

Sadasivan, G., Brownlee, J., Claise, B., & Quittek, J. (2014). *The Constrained Application Protocol (CoAP)*. RFC Editor. Retrieved from https://tools.ietf.org/html/rfc7252

Salman, T. (2015). *Networking Protocols and Standards for Internet of Things*. Retrieved from http://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/index.html

Sanchez-Iborra, R., & Cano, M. D. (2016). State of the art in LP-WAN solutions for industrial IoT services. *Sensors (Switzerland)*, *16*(5). https://doi.org/10.3390/s16050708

Sanchez, L., Munoz, L., Galache, J. A., Sotres, P., Santana, J. R., Gutierrez, V., Ramdhany, R., Gluhak, A., Krco, S., Theodoridis, E., & Pfisterer, D. (2014). SmartSantander: IoT experimentation over a smart city testbed. *Computer Networks*. https://doi.org/10.1016/j.bjp.2013.12.020

Santana, E. F. Z., Chaves, A. P., Gerosa, M. A., Kon, F., & Milojicic, D. (2016). Software Platforms for Smart Cities: Concepts, Requirements, Challenges, and a Unified Reference Architecture. Retrieved from http://arxiv.org/abs/1609.08089

SIG. (2016). Bluetooth® 5 Quadruples Range, Doubles Speed, Increases Data Broadcasting Capacity by 800%. Retrieved May 2, 2017, from https://www.bluetooth.com/news/pressreleases/2016/06/16/-bluetooth5-quadruples-rangedoubles-speedincreases-data-broadcasting-capacity-by-800

Soldatos, J., Kefalakis, N., Hauswirth, M., Serrano, M., Calbimonte, J.-P., Riahi, M., Aberer, K., Jayaraman, P. P., Zaslavsky, A., Zarko, I. P., Skorin-Kapov, L., & Herzog, R. (2015). OpenIoT: Open Source Internet-of-Things in the Cloud. *Lecture Notes in Computer Science*, *10218*(March). https://doi.org/10.1007/978-3-319-56877-5

Statista. (2014). • Smartphone users worldwide 2014-2020. Retrieved February 2, 2017, from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Stuckenbruck, L. . (1979). The Matrix Organization. Retrieved July 6, 2017, from https://www.pmi.org/learning/library/matrix-organization-structure-reason-evolution-1837

Sutaria, R., & Govindachari, R. (2013). *Understanding The Internet Of Things*.

Thangavel, D., Ma, X., Valera, A., Tan, H. X., & Tan, C. K. Y. (2014). Performance evaluation of MQTT and CoAP via a common middleware. *IEEE ISSNIP 2014 - 2014 IEEE 9th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Conference Proceedings*, (April), 21–24.

https://doi.org/10.1109/ISSNIP.2014.6827678

Tobergte, D. R., & Curtis, S. (2013). Extensible Messaging and Presence Protocol (XMPP): Core. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

United Nation Framework Convention on Climate Change. (2016). Kyoto Protocol. Retrieved February 2, 2017, from http://unfccc.int/kyoto_protocol/items/2830.php

United Nations. (2014). World Urbanization Prospects 2014. *Demographic Research*, 32. https://doi.org/(ST/ESA/SER.A/366)

Van den Abeele, F., Hoebeke, J., Moerman, I., & Demeester, P. (2015). Integration of Heterogeneous Devices and Communication Models via the Cloud in the Constrained Internet of Things. *International Journal of Distributed Sensor Networks*, *2015*, 1–16. https://doi.org/10.1155/2015/683425

Vodafone. (2016). Enabling the Internet of Things with NB-IoT. Retrieved May 17, 2017, from http://www.vodafone.com/content/index/what/technology-blog/enabling-iot.html#

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, *1*(1), 22–32. https://doi.org/10.1109/JIOT.2014.2306328

Zanella, A., & Zorzi, M. (2016). Long-range communications in unlicensed bands : The rising stars in the IoT and Smart City scenarios, (October), 60–67.

Appendix

Appendix I – Deliverables

The table below shows the elaborated version of the deliverables of this study. The deliverables are described per research question.

Research question	Deliverable
How is IoT involved in Smart City and what are the challenges?	The first deliverable is a description of the literature review where the context of Smart City is analyzed, the involvement of IoT is described and the coherent challenges are identified. From these challenges, one or two challenges will be selected for further research.
What criteria are required to address the IoT challenges in a Smart City?	Framework that consist of required criteria. Such as what kind of API, open source or not, which architectural method and which type of protocol addresses the challenges? This framework will to compare the architectural approaches.
Are existing architectural approaches capable of satisfying the criteria and if not, how can a new architectural approach satisfy the criteria?	A list, in form of an Excel Sheet, will be provided where the architectural approaches are analyzed based on the framework. When the existing architectural approaches are not capable of satisfying the criteria, a new approach will be provided. This new approach will be described based on architectural modeling language such as Archimate. However, this is provisional and will be determined during the study.

Assuming the architectural approach can satisfy the criteria, can we evaluate it in form of a case study?	The last deliverable is an analysis of the case study where the architectural approach is validated in the context of Smart City. The analysis will describe whether the architectural approach is sufficient in addressing the challenges. Based on the result, the architectural approach may be adjusted and optimized.

Table 11. Deliverables

Appendix II – Definition analysis

This table is based on the definition analysis of Cocchia (Cocchia, 2014). The study provided a definition analysis of nine Smart City studies. In addition to that, we have identified four elements, which are depicted in Table 12, and analyzed which definition contains the elements. In that way, we were able to identify the most comprehensive definition.

	Definition	Reference
1	"A Smart City is a city well performing built on the 'smart' combination of endowments and activities of self-decisive, independent and aware citizens"	Giffinger (2011)
2	"A smart community is a community that has made a conscious effort to use information technology to transform life and work within its region in significant and fundamental rather than incremental ways"	California Institute (2001)
3	"A city to be smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infra-structure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance"	Caragliu et al. (2011)
4	"Smart city is defined by IBM as the use of information and communication technology to sense, analyze and integrate the key information of core systems in running cities"	IBM (2011)
5	"Smart City is the product of Digital City combined with the Internet of Things"	Su et al. (2011)
6	"Concept of a Smart City where citizens, objects, utilities, etc., connect in a seamless manner using ubiquitous technologies, so as to significantly enhance the living experience in 21st century urban environments"	Northstream (2010)

7	"A city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rails, subways, airports, seaports, communications, water, power, even major buildings, can better optimize its resources, plan its preventive maintenance activities, and monitor security aspects while maximizing services to its citizens"	Hall (2000)
8	"Smart City is a city in which it can combine technologies as diverse as water recycling, advanced energy grids and mobile communications in order to reduce environmental impact and to offer its citizens better lives"	Setis-Eu (2012)
9	"A smart city is a well-defined geographical area, in which high technologies such as ICT, logistic, energy production, and so on, cooperate to create benefits for citizens in terms of well-being, inclusion and participation, environmental quality, intelligent development; it is governed by a well-defined pool of subjects, able to state the rules and policy for the city government and development"	Dameri (2013)

Table 12. Smart City definition (Cocchia, 2014)

Citizens / Life quality	**Information Technology**	**Infrastructure**	**Environmental impact**
1,2,3,6,7,8,**9**	2,3,4,5,6,8,**9**	3,6,7,**9**	7,3,8,**9**

Table 13. Key terms of definitions

Appendix III – Overview of standards and protocols used in IoT

In this appendix, we will provide an elaborated overview of the standards and protocols used in IoT. The OSI model is used to plot the standards and protocols on the logical layers. First, the short-range protocols are described followed by network layer protocols and

Short range protocols

IEEE 802.15.4 is the most common standard used in this layer. In contrast to other standards, such as Wi-Fi, this standard emphasis the low cost and low power properties that makes it suitable for IoT devices. ***Zigbee*** and ***WirelessHART*** are popular protocols that are based on this standard. The former is mainly used in the home automation and healthcare.

IEEE 802.11ah is a recently developed extension of the well-known IEEE 802.11 wireless standard. The new version aims at providing a lightweight version of the IEEE 802.11 standard to meet the requirements of IoT devices.

Z-Wave is a company that operates mainly in the home automation market and have more than 1700 interoperable products worldwide. The company has developed their own wireless communication protocol that is aimed IoT solutions in home and office automation. Giving the contextual setting of this protocol, it differs significantly in terms of throughput and coverage rate compared to IEEE 802.11ah and IEEE 802.15.4.

Bluetooth is also known as a widely used short-range communication protocol in IoT. Bluetooth 5 is the newest version and is adapted to the needs of IoT. The newest version has significantly improved. The Bluetooth Special Interest Group (SIG) has described the improvement as follows: "*Bluetooth 5 will include significantly increased range, speed, and broadcast messaging capacity. Extending range will deliver robust, reliable IoT connections that make full-home and building and outdoor use cases a reality. Higher speeds will send data faster and optimize responsiveness. Increasing broadcast capacity will propel the next generation of "connectionless" services like beacons and location-relevant information and navigation."* (SIG, 2016).

Network layer protocols

The network layer is responsible for the routing of packages throughout the network. As described in the data link layer, IoT requires efficiency to ensure performance and availability, which is also valid for this layer. The most known and used protocol in this layer is the Internet Protocol version 6 (IPv6). This version of the protocol is, however, not compatible with the requirements of IoT. Packages of IPv6 are too long and do not fit in datalink frames that are purposely smaller (Salman, 2015). The IETF designed an alternative named 6LoWPAN. This protocol stands for IPv6 over Low Power Wireless Personal Area Networks. This is a widely used protocol in IoT that allows devices with limited processing capabilities to communicate to the internet.

Transport layer protocols

The layer is responsible for the reliable transport of packages of end-to-end nodes in a network. The protocols make use of mechanisms for error checking and data flow. The most well-known protocol in this layer is TCP and UDP. The former is known as reliable since it guarantees that all packages are received and that no data is lost or corrupted during the transportation. UDP is similar to TCP but the main difference is that it does not guarantee the transportation of all packages since the checking mechanisms are not used. Both TCP and UDP are used in the IoT era.

Standard	**ZigBee**	**Bluetooth LE**	**Z-Wave**	**NFC**	**HomePlug GP**	**Wi-Fi**
IEEE Spec	802.15.4	802.15.1	ITU-T	ISO 13157 etc.	IEEE 1901-2010	802.11a/b/g
Freq. Band	868/915 MHz; 2.4 GHz	2.4-2.5 GHz	908.42 MHz	13.56 MHz	1.8 MHz to 30 MHz	2.4 GHz; 5 GHz
Max Signal Rate	250 kb/s	305 kbps	40 kbit/s or 100 kbit/s	424 kbit/s	ROBO : 4 Mbps to 10 Mbps Adaptive Bit Loading : 20 Mbps to 200 Mbps	54 Mb/s
Nominal Range	10 m	~50 m	~30 m	~5 cm	~100m	100 m
Cryptography	AES block cipher (CTR,counterm ode)	AES Encryption	AES encryption	Not with RFID	AES Encryptio n	RC4 stream cipher (WEP), AES block cipher
Network Type	WPAN	WPAN	WPAN	P2P	WPAN	WPAN/P2P
Spreading	DSSS	FHSS	FHSS	GSMA	BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM, 1024 QAM	DSSS, CCK, OFDM
Modulation type	BPSK (+ ASK), O-QPSK	TDMA	GFSK/ISM	ASK	OFDM	BPSK, QPSK COFDM, CCK,MQAM
Coexistence mechanism	Dynamic freq. hopping	Adaptive freq. hopping	Adaptive freq. hopping	RFID	Dynamic freq. hopping	Dynamic freq. selection, transmit power control (802.1 1h)
Power Consumption	~ 40 mA	~ 12.5 mA	2.5 mA	~50 mA	0.5 W	~ 116 mA (@1.8 V)

Table 14. Comparison of short range data link protocols (Rahman, 2015)

	LoRaWAN	Sigfox	Weightless			Ingenu	Telensa	Dash7	IEEE 802.15.4k (DSSS)	IEEE P802.11ah	LTE-MTC
			-W	-N	-P						
Band	433/868/780/915 MHz	868/915 MHz	TV whitespace	Sub-GHz	Sub-GHz	2.4 GHz	Sub-GHz	Sub-GHz	Sub-GHz/2.4 GHz	Sub-GHz	Cellular
Max. data-rate	50 kbps	100 bps	10 Mbps	100 bps	100 kbps	19 kbps/MHz	346 Mbps	-	125 kbps	346 Mbps	200 kbps
Range (urban)	5 km	10 km	5 km	5 km	2 km	15 km	1 km	3 km	5 km	1 km	5 km
Packet-size	Max. 256 B	12 B	Min. 10 B	Max. 20 B	Min. 10 B	Max. 10 kB	Max. 65 kB.	-	Max 32 B	Max. 65 kB.	-
Downlink	Yes. Different plans	Yes (not sym.)	Yes (sym.)	No	Yes (sym.)	Yes (not sym.)	Yes (sym.)	Yes (sym.)	Yes (not sym.)	Yes (sym.)	Yes (sym.)
Topology	Star-of-stars	Star	Star	Star	Star	Star/Tree	Star/Tree	Star	Star	Star/Tree	Star
Roaming	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-	Yes	Yes
Security	Fully addressed	Partially addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	In development	-	Partially addressed	In development	In developme
Protocol ownership	Partially proprietary	Proprietary	Standard	Standard	Standard	Proprietary	Standard	Proprietary	Standard	Standard	Standard

Table 15. Comparison of long range data link protocols (Sanchez-Iborra & Cano, 2016)