Universiteit Utrecht

The Internet of Things

How the world will be connected in 2025

Author: Steven Hendriks | 3238768
s.hendriks2@students.uu.nl

Supervisor: Dr.Ir. Alexander Peine

Master thesis
Innovation Sciences
Utrecht University

August 2016

Abstract

The Internet of Things (IoT) is a rapidly growing emerging topic of technical, social, and economic significance. Objects are being combined with internet connectivity and powerful data analytic capabilities that promise to transform the way we work and live. At the same time, however, the Internet of Things raises significant challenges that could stand in the way of realizing its potential benefits. One of them is standardization, due to the numerous different technologies that have to work together in an IoT system. In a fully interoperable environment, any IoT device would be able to connect to any other device, regardless of manufacturer or technology. In practice, interoperability is more complex. Open standards can facilitate interoperability, but yet it is poorly understood which strategies need to be executed in order to create standards that allow a degree of functional openness. This research therefore explores which innovation strategies have been applied by actors in the field with respect to open standardization and which implications it has for innovation. By using a theoretical framework that combines elements from complex technical system, dominant design theory, standardization theory and lead users, an exploratory study has been carried out. More than 150 documents have been analyzed by means of qualitative data analysis and coding. The results show that several standards dominate the market at the moment and that standardization is mainly driven through proprietary approaches by companies, leading to a fragmented IoT field in which devices are just party interoperable with each other. It becomes more recognized by actors in the field that IoT only succeeds if devices are fully interoperable. Creating middleware that allows connecting devices operating on different technologies, learning from users and open source platforms are examples of strategies that enable full interoperability. The open nature of IoT leads to the creation of dominant configurations, in which its components can rearrange depending on the context. This has implications for innovation. Since IoT is not a consolidated industry in which a dominant design guides incremental innovation, innovation stems from linking components together by focusing on inter-industry collaboration and user involvement instead. This will stimulate the further development and deployment of IoT.

Table of contents

1 Introduction

1.1. Problem area

‘In 2003, there were 6.3 billion people living on the planet with 500 million devices connected to the Internet’ (Fell, 2014; p.10). This will become 7.6 billion people on the planet and 25-50 billion devices connected to the Internet by 2020 (Fell, 2014; European Parliament [EP], 2015; IERC, 2015). Although the final number of devices may not be clear yet, it is for sure that this rapidly emerging ‘Internet of Things’ (IoT) will have a profound impact on our society (Fell, 2014; Zanella et al., 2014; EP, 2015).

‘Internet of Things (IoT) is a recent communication paradigm that envisions a near future, in which the objects of everyday life will be equipped with microcontrollers, transceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, becoming an integral part of the Internet’ (Zanella et al., 2014; p.22). Hence, it can be seen as a distributed network of physical objects that can act on their environment and can communicate with other machines or computers (EP, 2015). According to the European Commission, ‘Internet of Things (IoT) represents the next step towards the digitisation of our society and economy, where objects and people are interconnected through communication networks and report about their status and/or the surrounding environment’ (European Commission [EC], 2015). The future Internet will embody a large number of objects that provide information and services to the final users through standard communication protocols and unique addressing schemes (see figure 1) (International Telecommunication Unit [ITU], 2005; Atzori et al., 2014; EC, 2015).

Fig. 1. Schematic illustration of IoT (EC, 2015)

In the IoT everything becomes virtual: each person and thing has a locatable, readable and addressable counterpart in the Internet (Atzori et al., 2014; Fell, 2014). IoT enables easy access and interaction with a wide variety of devices, such as home appliances, surveillance cameras, monitoring, sensors, actuators, displays, vehicles, and so on (Fell, 2014; Zanella et al., 2014). This enables the provision of new services to citizens, companies, and public administrations. Hence, it will have a high impact on several aspects of every-day life and behavior of potential users (ITU, 2005; Zanella et al., 2014). For a private user, the most obvious effects of the IoT will be visible in both working and domestic fields (Bellavista et al., 2010; Bandyopadhyay & Sen, 2011). Smart homes and offices, e-health and assisted living are only a few examples of possible application scenarios in which the new paradigm will play a leading role in the near future (Bellavista et al., 2010; Bandyopadhyay & Sen, 2011; Zanella et al., 2014). One example is the Nest Thermostat (see figure 2). Recently acquired by Google, Nest is a home device company that is responsible for the Nest Learning Thermostat (Fell, 2014). Most people leave the house at one temperature and forget to change it. So the Nest Thermostat learns ones schedule, programs itself and can be controlled from a phone, tablet or PC. If one teaches it well it is claimed that the Nest thermostat can lower the heating and cooling bills by up to 20% (Fell, 2014).

Fig. 2. Illustration of the Nest thermostat (Fell, 2014)

However, such a heterogeneous field of application makes building a general architecture for IoT a complex task, due to IoT's complexity and novelty (Zanella et al., 2014). This difficulty has led to a large amount of different and, sometimes, incompatible proposals for the practical realization of IoT systems (Fell, 2014; Zanella et al., 2014). Furthermore, the adoption of the IoT paradigm is also hampered by the lack of a clear and widely accepted business model that can attract investments to promote the deployment of these technologies (Laya et al., 2013; Zanella et al., 2014). Hence, many challenging issues still need to be addressed, both technologically as socially. In March 2015 the European Commission therefore initiated the creation of the Alliance for Internet of Things Innovation (AIOTI) (EU, 2016). This alliance flags the intention of the European Commission to work closely with all stakeholders and actors of the Internet of Things (EU, 2016). The main question is how to achieve full interoperability between interconnected devices and provide them with a degree of 'smartness', but guaranteeing trust, security, and privacy of the users and their data at the same time (Atzori et al., 2010; Bandyopadhyay & Sen, 2011). IoT can only be realized by useful deployment of hardware, software and applications around each domain of technology (Bandyopadhyay & Sen, 2011; IERC, 2015). Examples of these key technologies are identification technology, IoT architecture technology, communication technology, network technology, data and signal processing technology, power and energy storage technology, security and privacy technologies (Bandyopadhyay & Sen, 2011; Bellavista et al., 2010; Zanella et al., 2014). Thus, IoT is a complex structure of hardware, sensors, applications and devices that need to be able to communicate with each other in different ways. This requires shared standards to exchange data across different organizations (ITU, 2005; Bellavista et al., 2010; IERC, 2015). If devices from different manufacturers do not use the same standards, interoperability will be more difficult, requiring extra gateways to translate from one standard to another (EP, 2015; IERC, 2015). 'Standards enable innovation, and are key for interoperability, may improve safety and security, are drivers for emergence of new markets, facilitate introduction of technologies (such as IoT), enhance competition and can help to „de-verticalize“ industry by sharing and inter-operation of tools and technology, reducing the development and deployment costs for IoT applications' (IERC, 2015; p.11). Hence, standards are important in creating markets for new technologies and prevent consumers of being locked into one family of products (ITU, 2005; EP, 2015). As to IoT, standards should address common requirements from a wide range of industry sectors as well as the needs of the environment, society and individual citizens (Bandyopadhyay & Sen, 2011; Fell, 2014). The central issue is how standardization can be realized in order to create a 'shared language', without losing the openness for the numerous heterogeneous applications. Hence, the realization these standards will most likely be based on open standards, rather than proprietary technologies (ITU, 2005; IERC, 2015). Open standards facilitate interoperability of devices and functions from different heterogeneous sources. Open standards are 'standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. They facilitate interoperability and data exchange among different products or services and are intended for widespread adoption' (ITU, 2005). Exploring open standardization within the field of IoT thus forms the basis for this research.

1.2. Research question

In the light of IoT, standards need to be flexible enough to integrate new components and possibly abandon old components. Ideally, users should be able to do this by themselves in order to enable them to configure their own system with the devices they prefer. This research therefore aims to explore how (open) standardization has been approached by actors in the field, in order to provide insights about which strategies are useful to employ and which strategies are not. The research aim is accomplished through an analysis of the main technological standards that have been realized in the last fifteen years, together with the innovation strategies have been used by actors in the field to deal with open standardization. This results in the following research question:

Which strategies have been used in order to create open standards with respect to IoT and how does this affect standardization of IoT nowadays?

1.3. Relevance

Theoretically this research contributes to the understanding of the evolution of complex technical systems, such as IoT. As to IoT, no dominant design exists on a system level. After all, the system has to retain a certain degree of openness so it remains suitable for a wide range of applications within different industry sectors. Hence, the IoT technology has to evolve based on open standards. In other words, innovation thrives on open standards that facilitate interoperability while retaining a degree of functional openness (Peine, 2009, pp. 406). This requires both a certain degree of looseness as a certain degree of rigidness of the system. This area is poorly understood nowadays (Peine, 2008; Peine, 2009; Atzori et al., 2010; Fell, 2014; EP, 2015). Therefore, this research tries to fill this gap by providing insights in how this issue has been addressed in the past and which lessons should be learned from that. For example, how can incremental innovation take place without the presence of a dominant design? Which implications have open standards for product and process innovation? What kind of dominant design can exist together with open standards? Which innovation strategy should a company ideally implement in order to manage innovation based upon open standardization?

This research finds its societal relevance in providing insights for many different players in the field of IoT. Understanding the nature of IoT is a key element towards devising adequate policy measures for its creation and diffusion. Because no 'traditional' dominant design emerges, policy makers need to make choices based on open standards. This research provides insights in these open standards and thus serves as a guideline for policy makers in the field of IoT. There are several major challenges that impact a broad implementation of IoT. First, as mentioned earlier, IoT is a complex structure of hardware, sensors, applications and devices that need to be able to communicate between different geographical locations. Second, ownership of data is and probably will remain a difficult topic for years, but it is probably shifting to having access to the data and being able to use it for analysis. Moreover, mixing the digital and the physical world will require high security standards in order to prevent accidents (Atzori et al., 2010; Fell, 2014). Furthermore, standards can provide cost efficient realizations of solutions (IERC, 2015). Global standards are needed to achieve economy of scale and interworking. In order to deal with these challenges, a comprehensive understanding of how IoT develops and what elements help to set standards will be very useful. This research will contribute to this understanding.

1.4. Outline

The next chapter will present the theoretical framework that has been used in order to answer the research question, which served as 'sensitizing' framework during the research. Subsequently the research methodology that has been applied will be presented, followed by an analysis of the standards that have been realized and the innovations strategies with respect to open standardization that have been applied in the last fifteen years. Thereafter, an answer to the research question will be given in the conclusion, followed by a discussion about the theoretical and methodological implications of this research.

2 Theoretical framework

The theoretical framework in this research consists of different strands of literature. Notions of complex technical systems, dominant design theory, standardization and lead users will together form the theoretical perspective that has been used in order to answer the research question. Concepts from this 'framework' have been used as sensitizing concepts throughout this research. The different notions will be elucidated below.

2.1. Complex technical systems

In innovation literature, the market and the technological context influence the implementation of an effective innovation strategy (Tidd & Bessant, 2009). In cases where the market and technology are both new and consequently poorly understood, like with IoT, the product or system is classified as 'complex' (Tidd & Bessant, 2009). Complex technical systems are technologies that are defined by a set of components and an architecture that specifies how to arrange these components into a system (Henderson & Clark, 1990). Complex products typically consist of a number of components or subsystems. Depending on how open the standards are for interfaces between the various components, products may be offered as bundled systems, or as subsystems or components (Tidd & Bessant, 2009). For bundled or closed systems, customers evaluate purchases at the system level, rather than the component level (Tidd & Bessant, 2009). E.g., a manufacturer can offer the customer a complete IoT application, consisting of several interoperable components. This can offer the customer an enhanced performance due to the presence of optimized components using proprietary interfaces (Tidd & Bessant, 2009). However, such a bundled system does not allow the customer to adjust the system to their own needs. To enable the customer to configure its own system, open complex technical systems are required. Open systems display a greater degree of looseness than closed systems, and become systems only in the light of local contingencies (Peine, 2008). In open technical systems, only a range of components is defined. The selection of the exact set of components to be included as well as the plan how to arrange these components is dependent on the context in which a particular system operates. This specific arrangement can be denoted as a configuration. In other words, the system does not define clear choices in the first place (Peine, 2009). Configurations bring together technical components, software, standards, services and user practices in more or less unique ways, and they are thus dependent on specific contexts of applications. Components comprise established technologies with corresponding standards at the component level. However, at the architectural level this needs to be integrated in an interoperable system. As to understanding these systems, two types of knowledge can be distinguished: component knowledge (regarding form and functions of the subsystems) and architectural knowledge (regarding form and function of the entire system). 'For open technical systems, the knowledge bases for the component knowledge are stable, while the architectural knowledge has to be specified for each system separately' (Peine, 2008; p.509). Understanding the dynamics of systems, therefore, makes it necessary to take into account two levels of dynamism: changes in component knowledge and changes in architectural knowledge (Peine, 2009).

2.2. Dominant design

Innovation opportunities change over time and can be described through three phases of the innovation life cycle. In new industries a lot of players experiment around new product and service concepts (Utterback, 1996; Tidd & Bessant, 2009). In the situation where new technologies and/or markets emerge, the so-called 'fluid phase', there is high uncertainty about the target (what will the new configuration be and who will want it?) and how to create this target in a technical way (Utterback, 1996; Tidd & Bessant, 2009). No one knows what the 'right' configuration will be, so there is a lot of experimenting of many players. Gradually these experiments converge to what is called a dominant design, i.e. a representation of 'the rules of the game' (Utterback, 1996; Tidd & Bessant, 2009). The phase towards the realization of a dominant design is called the 'transitional phase'. Once this is accomplished, problem solving travels down the design hierarchy (Utterback, 1996; Peine, 2009). When a dominant design has emerged, the so-called 'specific phase' starts which drastically changes the basis of competition (Utterback, 1996). Although many players are eliminated from further participation in the industry with the appearance of the dominant design (an industry shake-out), some new players enter the market that are trying to gain market share with imitations of the dominant design. Nevertheless, eventually the total number of firms declines until it reaches a point of stability (Suárez & Utterback, 1993). Hence, the industry now changes from one characterized by many firms and many unique designs to one of few firms with similar product designs (Utterback, 1996). This enables benchmarking, since more firms are working on similar products. Moreover, consumer preferences are better known at this point. Hence, more information is available to the industry's players. Since product standards are now established, effective competition shifts to incremental product performance along technological trajectories and process innovation (i.e. price), instead of radical product innovation (Suárez & Utterback, 1993; Utterback, 1996). Firms that are unable to make this transition are unable to compete effectively and very often fail (Suárez & Utterback, 1993; Utterback, 1996).

However, open complex systems do not lend themselves for a 'traditional' dominant design, since the components need to be able to rearrange in order to create different configurations. Hence, no 'one-fits-all' dominant design can be established and other forms of standardization have to be found in order to create interoperability among components. The following section illustrates different forms of standardization.

2.3. Technological standardization

'Technical standards are established norms or requirements applied to technical systems' (Shin et al., 2015, p.152). 'A standard can be defined broadly as the consensus of different agents to do certain key activities according to agreed-upon rules, and a technology standard can be viewed as 'a set of specifications to which all elements of products, processes, formats, or procedures under its jurisdiction must conform' (Narayanan & Chen, 2012, p.1376). In this context, there are differences between the supply and the demand side. On the supply side, a technology standard represents the synthesis of proven concepts on the design logics to organize the hierarchy and functional parameters for a particular type of product. On the demand side, a technology standard reflects the desire of consumers for agreement on a uniform technological format (Baron et al., 2014). Hence, a technology standard represents the collective choice resulting from a balance between utility to consumers, technical possibilities and the cost structure of manufacturers on the one hand, and constraints of political, social, and economic institutions on the other (Narayanan & Chen, 2012; Shin et al., 2015). Research from supply-side standardization generally considers how a technology in the market is established as a standard (Shin et al., 2015). Some technologies are chosen as de facto standards as a result of firms' continuous efforts and investment in R&D activities and innovation. A de facto standard is a product on the market that is adopted by so many consumers that it is practically recognized as a standard (Axelrod, 1995; Shin et al., 2015). Led by a specific organization, some technologies are developed from the beginning of research planning, resulting in a de jure standard. A de jure standard is a standard developed or established by a standard-setting organization (SSO) (Axelrod, 1995; Baron et al., 2014; Shin et al., 2015). Against this background, it has become frequent that some companies contributing to the standard form an alliance in order to supplement the formal standard setting process (Baron et al., 2014). In such case, a number of firms collectively establish an organization in the form of a consortium and produce optimal technology standards through their own standard-setting process (Shin et al., 2015).

2.4. Lead users

As mentioned before, open complex system do not have a stable system identity (Henderson & Clark, 1990; Peine, 2009). Local practical knowledge is consequently the most important for the design of specific systems in order to create a configuration that meets the needs of users (Peine, 2009). After all, the generic knowledge is dispersed over different industrial sectors. Configurations are derived from several knowledge bases that make up the total generic technology knowledge. Hence, IoT is heterogeneous in terms of the generic technology knowledge it comprises. The implementation of an

IoT system therefore requires the integration of different bases of generic technology knowledge and local practical knowledge (Henderson & Clark, 1990; Peine, 2009). Local practical knowledge comprises everyday social practices and routines (Peine, 2009). When designing IoT, this knowledge has to be taken into account in order to attract potential users. Each system has to be technically feasible and it has to provide a meaningful application, which depends on the capability to actually derive such knowledge and the degree of openness that can be realized within the range of technological solutions (Henderson & Clark, 1990; Peine, 2009). Hence, misconceiving IoT as integrated systems will lead to standardized technological solutions which cannot provide the degree of adaptability that is required for the successful implementation of IoT.

Lead users are critical to this development and adoption of IoT, since they can provide the local practical knowledge as described above. Lead users are users that demand new requirements ahead of the general market of other users (Von Hippel, 1986; Tidd & Bessant, 2009). They can help to co-develop innovations, and are often early adopters of such innovations. Lead users can recognize requirements early, expect high levels of benefits and develop their own applications (Von Hippel, 1986; Tidd & Bessant, 2009). Hence, a producer of a complex product should identify potential lead users to contribute to the development and adoption of the innovation. Furthermore, lead users provide insights to the diffusion of innovations (Von Hippel, 1986; Tidd & Bessant, 2009).

2.5. Summary

IoT comprises a lot of different technologies/components that have to work together. Since these components need to be able to rearrange in order to create specific configurations, no one-fits-all dominant design can be realized. An IoT system does not need to be considered as an integrated system, because it is consists of components (stemming from other industries) that need to be linked together, depending on the context. Thus, the system needs to retain a certain degree of functional openness, so that users can adjust the system to their individual needs. Here (open) standardization comes into play. In order to enable innovation, open standardization is necessary to facilitate interoperability among different components of IoT. Standards are established norms or requirements applied to technical systems and can be established in multiple ways. Lead users are an important source of knowledge that can provide insights in user needs and how the technology is applied in different contexts. Learning about this helps to further develop and deploy IoT systems.

3 Methodology

3.1. Research design

This research has an exploratory character, since IoT is a relatively new and complex field and standardization is still evolving. An exploratory research is useful since it provides the researcher with detailed insights that can contribute to theory. As mentioned before, the theoretical framework had a sensitive function during this exploration. It is not preferable to express the findings of this study in just numerical values, since those would not provide a rich understanding (the why and how). Therefore, the study followed a qualitative strategy. A case study had been executed, because a case study enables the researcher to gain a rich understanding of the context of the research and the processes being enacted (Saunders, et al., 2009). Nine wireless technologies that enable IoT have been selected as cases within this research. They were selected by theoretical sampling in order to gain as much information as possible. I.e. based on the data that were available, a selection of cases has been made of which was expected that these cases yield the most comprehensive information in order to answer the research question. For these cases it has been analyzed which actors influence the standard-setting process of the technology and in which way. Consequently, this research provides insights in how actors in the field dealt with open standardization of IoT, by mapping the main standards have been realized and which strategies have been applied with respect to open standards.

3.2. Data collection

Multiple sources of (secondary) data have been used in order to apply triangulation (Bryman, 2008; Saunders, et al., 2009). That is, by using multiple sources of evidence, the probability that data are based on coincidence diminishes, because the data are more likely to be valid if multiple different data sources support these data (Bryman, 2008; Saunders, et al., 2009). Within this research, the different data sources are (I) research reports obtained from public sources, (II) news articles obtained from public sources and (III) scientific articles, obtained from the scientific databases Scopus and Google Scholar. Especially grey literature had been used since it is numerous and enabled access to historical data. It was planned to interview some respondents of corporations that have dealt with standardization issues with respect to IoT, in order to gather detailed information on a company level about the standardization strategies that had been executed. Unfortunately interview requests to companies were rejected or ignored, probably due to secrecy reasons. So interviews are no part of the sources of data. The time frame that had been applied is 2000-2016, since the concept of IoT was created around 1999 and gained publicity in the years after (Fell, 2014). Hence, it was expected that the time frame 2000-2016 yields the most valuable information. An initial exploration of the field of IoT technologies indicated that IoT has a lot of overlap with concepts as ‘home automation’ and ‘smart homes’. What previously has been called ‘smart homes’ or ‘home automation’, is nowadays called ‘Internet of Things’. In order to only involve data that comprise technologies and standards that are in line with the new paradigm of IoT, only the terms ‘IoT’ or ‘Internet of Things’ have been used in search queries used to denote the field. Hereby it has been assumed that information linked to smart homes and home automation also appeared when using the alternative term ‘Internet of Things’ to denote the field.

The followings questions were kept in mind during data collection: Who are important players in the field? Which standardization attempts were made in the past and why do they have (not) succeeded? Which lessons can be learned from that and by whom? Which innovation strategies underlie the design of IoT and how do they take the complex nature of the corresponding technology into account? Which activities are undertaken in order to establish standards? And how are these standards conceived by important players in the field? And more important, what are the opportunities to standardize IoT nowadays?

To demarcate the research, only data from the US and Europe were taken into account because it appeared that the most leading standard-setting organizations and corresponding standards are US or Europe-based. Standards were searched for by using terms like ‘IoT standards’, ‘IoT standardization overview’ and ‘IoT standards and protocols’. This yielded many results, especially articles from bloggers or online magazines. Since there are many players in the field of IoT, only (articles about what appeared to be) the main players (i.e. the actors of which the most articles were written about) were taken into account in this research. Consequently, further detailed information about a standard was found by using the name of the standard plus a term that denotes the subject of which more information was needed, e.g. ‘IEEE 802.4.15 history’. Another criterion that has been applied in mapping the main standards was the ability for a standard/technology to connect to the internet, since that is what IoT is about.

As to searching for strategies that have been applied with respect to standardization, the search query ‘Internet of Things’ and ‘standardization strategy’, for example, yielded no useful results, since results were about possible strategies for companies to implement IoT and obviously not about standardization strategies that have been applied by players in the field. Hence, the term ‘strategy’ was obviously not very useful to use. Therefore, other search queries had to be used in order to yield results from which innovation strategies could be derived. Examples of search terms, based on the theoretical framework, that had been used in order to yield results with respect to strategies are ‘alliances’, ‘collaboration’, ‘user involvement, ‘standard-setting organization’, ‘industry agreement’ and ‘sources of knowledge’. Consequently, more detailed information was searched for by using search queries that lead to more delimited information, e.g. which specific companies are part of a certain degree of membership within an alliance.

In this research theoretical sampling had been applied. This means that first some data had been collected and consequently analyzed to form initial concepts, e.g. 'leadership' or 'building coalitions'. Thereafter, new data had been collected to refine those concepts. The processes of data collection and data analysis are thus interrelated and not two separate processes. Moreover, theoretical saturation, i.e. the point where new data do not add to theory anymore, had been applied. Although theoretical saturation might not actually have been reached in this research due to the numerous amounts of articles available concerning IoT, the documents that had been analyzed were useful in the verification of concepts. An overview of these documents can be found in appendix 1, in which A stands for Article and R for Report.

3.3. Data analysis

Data analysis was conducted through qualitative data analysis by means of coding, i.e. the process whereby data are broken into parts which are given names (Bryman, 2008). The first step in the process of analyzing data consisted of searching on the internet for articles, based on the search queries as mentioned in the previous paragraph. Also, memos were made, i.e. analytical writings that contain a brief description of the article or document. These memos helped to move through the raw data. The memos mainly focused on possible links between the realization between different standards, since this might indicate a possible (shared) strategy by companies that maintain the standard. Articles and documents that seemed relevant for the research were imported in the coding program NVivo 11. Then open coding had been conducted, i.e. labels (concepts) were assigned to text fragments. In this research text fragments comprised several lines of text. See appendix 8.4 for a coding example. Notes were made when ideas arose whilst coding (e.g. about possible links between concepts assigned). Concepts of the theoretical framework served as 'sensitizing concepts', i.e. concepts that act as a guide in an investigation, so that it points in a general way to what is relevant or important (Bryman, 2008). The usage of these sensitizing concepts gave the coding process guidance. For example, the fragment '*In 1998, for instance, Ericsson, IBM, Nokia, Toshiba and Intel created the Bluetooth special interest group (Bluetooth SIG)*' (R1) is relevant since it provides information about the members that constituted a certain alliance. Knowing the members of an alliance is essential in order to know what the interests of the alliance are. These interests are consequently determining a certain vision/mission with a corresponding standardization strategy. Another example is the following fragment: '*Usually, such standards are open and non-proprietary, so developers of the standard agree to reveal intellectual property regarding the standard on a non-*

discriminatory, royalty-free or reasonable royalty basis to all interested parties' (A33). This is relevant since it provides information about the accessibility and thus the degree of openness of a certain standard. When the open coding had been finished, the concepts were organized and grouped around certain topics to create overview. For example, 'alliance', 'membership' and 'license agreement' are forms of 'collaboration'. And 'easy to use', 'technology sharing' and 'control' were grouped into 'user needs'. Then so-called axial codes (i.e. the strategies that have been applied in the field) were designed, which are of a higher level of abstraction. During axial coding, connections were made between the initial concepts by linking them to contexts, consequences or causes (Bryman, 2008). Concepts that could not be linked to other concepts or seemed to be irrelevant in the light of the theoretical framework are withdrawn from further analysis. This resulted in categories that comprise relationships between the initial concepts and the conditions that gave rise to them, based on the notion of the theoretical framework. For example, because the field of IoT consists of different established technologies, companies try to develop a 'value proposition for users' through 'marketing' and 'rebranding' in order to 'enable IoT' since the 'awareness of the concept of IoT increased' nowadays. Another example: 'learn from users' requires 'user involvement' by means of 'open source' projects and therefore 'publish specifications'. This allows manufactures to gain insights about 'user needs' and how they 'use a certain technology'. A short overview can be found in table 1 below.[1] These strategies have been interwoven through the results section, organized around examples of standards and projects from the field.

Strategy	**Concepts**	
Proprietary approaches	Alliance formation Membership Certification program	Market share Reduce risk License agreement
Create middleware	Technological improvements Open source Network effect Building bridges	Interoperability Building blocks Core specification Semi open standards
Learn from users	Open source User knowledge User needs	Use of technology User involvement Publish specifications
Create value proposition for users	Enabler of IoT Rebranding	Increasing awareness IoT Marketing

Table 1. Concepts standardization strategies

[1] For a complete overview of how concepts are constituted, the NVivo file can be obtained via s.hendriks2@students.uu.nl

4 Internet of Things: standards and strategies

This section will present the main enabling IoT technologies that have been established in the last fifteen years. Each paragraph contains a (technical) description about the corresponding standard and an analysis of the innovation strategy that has been applied with respect to (open) standardization. Before the technologies will be discussed, first some background information is given in paragraph 4.1. The section concludes with a paragraph about open source projects and some concluding remarks. For some background information about the (technological) architecture of IoT, see appendix 8.1 and 8.2.

4.1. IEEE 802

It all began in 1985 after the United States Federal Communications Commission opened up the wireless frequencies 900Mhz, 2.4Ghz, and 5.8Ghz to be used without a license (A107). These radio bands were already used by household appliances such as microwaves, but were assumed to have no practical application in communications. Later, WLAN (Wireless Local Area Network) technology emerged, but the technology was proprietary, so wireless devices from one manufacturer would not work with technology from another (A108, A109). However, in 1988, the NCR Corporation wanted a WLAN standard for use in their wireless cash registers and asked the Institute of Electrical and Electronic Engineers (IEEE) for assistance. The IEEE set up a working group and called it IEEE 802. IEEE 802 refers to a group of IEEE standards dealing with local area networks (LANs) (A20, A36, A109). The services and protocols specified in IEEE 802 map to the lower two layers (physical and data link) of the seven-layer OSI networking reference model (see appendix 8.2) (A20, A36, A107). From here, several standards have been created that now form the basis of many local area networks. This gave rise in 1997 to standard IEEE 802.11, which refers to a family of specifications developed for wireless local area networks (WLAN) (A107, A108). Another example is IEEE 802.15, which refers to the working group which specifies wireless personal area network (WPAN) standards (A36). Within this working group, several task groups exist. Each task groups deals with a certain subject of study from which a standard can be derived. For example, the IEEE 802.15.1 project has derived a Wireless Personal Area Network (WPAN) standard based on Bluetooth, IEEE 802.15.3 a standard concerning high-rate WPANs and IEEE 802.15.4 deals with low-rate WPANs. This last standard forms the basis of several protocols within the field of IoT (A20, A107). The IEEE is now one of the leading standard-setting organizations in the world and consists mainly of engineers.

4.2. Wi-Fi

4.2.1. What is Wi-Fi and how can it be used?

Based on a star-shaped topology (see appendix 8.2), Wi-Fi networks use the access point (AP) as their Internet gateway. Wi-Fi is based on the IEEE 802.11 standard and was designed as a wireless replacement for the widely used, cable-based IEEE 802.3 Ethernet standard (A56, A107). Currently, the IEEE 802.11 standard is used in homes and many businesses, which offers serious throughput in the range of hundreds of megabit per second. This capacity is fine for file transfers, but may be too power-consuming for many IoT applications. Moreover, the high power consumption required for achieving high data rates and good coverage in buildings makes Wi-Fi not often suitable for battery-operated devices. Although the Wi-Fi technology mainly defines the data link layer of a LAN, it is also integrated into the TCP/IP stack. Using Wi-Fi therefore implies that TCP/IP is used for Internet connectivity. '*Until recently, it was quite expensive to provide Wi-Fi connectivity to devices with low processing performance (e.g. thermostats or household appliances) due to the size and complexity of the Wi-Fi and TCP/IP software. However, new devices and modules often include the Wi-Fi and TCP/IP software*' (A56).

A WLAN is usually password protected, but may be open, which allows any user within its range to connect his device to the WLAN network. Wi-Fi provides service in private homes, businesses, as well as in public spaces at Wi-Fi hotspots set up either free-of-charge or commercially. Some organizations and businesses, such as airports, hotels, and restaurants, often provide free-use hotspots to attract customers. Its range lies between 30-100 meters (A56, A107, A109).

4.2.2. How does the technology deal with standardization?

Initially, the 802.11 standard was capable of transmitting data at a speed of only two megabits per second. In 1999, a faster version called 802.11a was released, with a speed of fifty-four megabits per second, but with limited range and high production cost (A108, A109). Later in that year, 802.11b was released, which reduced production costs and improved the range. The sudden popularity of wireless networking led to an increase of new 802.11b hardware on the market. However, there was no way to ensure compatibility between devices from different manufacturers. In 1999, a group of six companies came together to create the Wireless Ethernet Compatibility Alliance (WECA), an organization that aimed to test Wi-Fi equipment for compatibility (A26). These companies were 3Com, Aironet (acquired by Cisco), Harris Semiconductor (now Intersil), Lucent (now Alcatel-Lucent), Nokia and Symbol Technologies (now Motorola) (A26, A110). In 2002, they coined the term Wi-Fi and renamed themselves Wi-Fi Alliance (A109). Over the years, in particular due to Apple's inclusion of it into their products, Wi-Fi gradually became a widespread technology (A110). '*Wi-Fi adoption continues to grow, and the common vision of connecting everyone and everything, everywhere continues to inform the collaboration of our members. Today about 600 Wi-Fi Alliance member companies from dozens of countries take part in our highly-effective organization, driving new technologies and applications and certifying thousands of Wi-Fi products each year*' (A26). Companies can become Implementer, Affiliate or Contributor member. A company needs to pay an annual fee of USD $5000 to become Implementer or Affiliate member and USD $15000 to become a Contributor member. Contributor members may contribute to the development of the certification programs and enabling technologies (A118).

Several amendments have been created by the IEEE since the creation of 802.11, denoted by an extra letter (e.g. 802.11ac). These amendments provide the basis for wireless network products using the Wi-Fi brand (A26, A109, A110, A111, A124). Each amendment is officially revoked when it is incorporated in the latest version of the standard. However, the corporate world tends to market to the revisions because they concisely denote capabilities of their products (A111). As a result, in the market place, each revision tends to become its own standard (A111). This is a good example of a standard that has been created in a 'de jure' way and refined by an alliance of different companies. In this way these companies can supplement the formal standard-setting process by producing technology standards through their own standard-setting process.

Nowadays the term "Wi-Fi" is used in general English as a synonym for "WLAN" since most modern WLANs are based on these standards (A108, A109). This indicates how well-known Wi-Fi is. However, Wi-Fi is a trademark of the Wi-Fi Alliance and can only be used on products that have successfully completed the Wi-Fi Alliance certification test (i.e. compatibility, conformance and performance). For users it is an assurance that a certain product has been tested in numerous configurations and with a diverse sampling of other devices to ensure compatibility with other Wi-Fi certified equipment (A26, A112).

This certification program is an instrument for the Wi-Fi Alliance to influence the standard-setting process. The need for interoperability has increased as Wi-Fi is now embedded not only in access points, wireless routers and laptops, but also phones, PDAs, printers and other consumer electronics devices (A108, A112). The certification program has been built around on three elements: interoperability, backward compatibility and innovation (A112). First, interoperability means that products from different equipment vendors can interoperate in a wide variety of configurations. Second, backward compatibility means that new products can work with existing gear. Third, innovation is supported through the introduction of new certification programs as the latest technology and specifications come into the marketplace (A112). After all, the introduction of new applications and devices is continuously expanding the concept of interoperability and raising performance requirements. The increasing importance of these applications has led not only to the introduction of new certification programs, but also to an increased emphasis on conformance and performance testing. The certification programs evolve to meet and anticipate market requirements and technology advances. An example is the realization of Wi-Fi Direct, a Wi-Fi standard enabling devices to easily connect with each other without requiring a wireless access point, even if they are from different manufacturers (A116). A side benefit of Wi-Fi Direct is that it can operate at higher speeds and greater distances than Bluetooth, though Bluetooth typically uses far less power (A106, A115, A116). Furthermore, the Wi-Fi Alliance has launched Miracast in 2012, a standard based on Wi-Fi Direct for wireless connections from devices (such as laptops, tablets, or smartphones) to displays (such as TVs or monitors). Miracast devices negotiate settings for each connection, which simplifies the process for the users and can be described as a 'wireless HDMI cable' (A113, A114). The Miracast standard also has optional components, however the use of optional components in standards sometimes causes issues if one vendor supports the optional components and another does not.

As mentioned before, Wi-Fi is relatively power-consuming which makes it not that suitable for battery-operated IoT applications. To tackle this problem, the Wi-Fi Alliance recently announced Wi-Fi HaLow. '*Wi-Fi HaLow operates in frequency bands below one gigahertz, offering longer range, lower power connectivity to Wi-Fi CERTIFIED™ products. Wi-Fi HaLow will enable a variety of new power-efficient use cases in the Smart Home, connected car, and digital healthcare, as well as industrial, retail, agriculture, and Smart City environments*' (A125). The Alliance claims that Wi-Fi HaLow will broadly adopt Wi-Fi protocols and deliver many of the benefits that consumers have come to expect from Wi-Fi today, including multi-vendor interoperability (A125).

4.2.3. What can be learned from this?

Wi-Fi is an open standard in the sense that it is freely available for the general public, at home or even at public places like cafés, stations and airports through 'hotspots'. Its range allows use for IoT applications, but it is still relatively power-consuming. Wi-Fi is not an open standard with respect to its development, i.e. not an open source standard. In order to qualify for obtaining Wi-Fi certification for products, a company must become a member of the Wi-Fi Alliance and pay an annual fee for this membership. This Alliance promotes Wi-Fi certification worldwide by encouraging manufacturers to follow standardized 802.11 processes. This ensures that Wi-Fi certified products are interoperable with other Wi-Fi certified products. A changing market, changing user needs and technology advances force the Alliance to offer new standards that enable users to connect more different devices to each other (including devices from different manufacturers). Hence, the Alliance stimulates incremental innovation by creating standards that provide new functionalities to users, as additional 'building blocks' to the basic technology/main standard. This stimulates the network effect of Wi-Fi: if more users can use Wi-Fi for fulfilling their needs, the more value Wi-Fi has for each user (since it can connect to more potential devices). Consequently, more companies want to become member of the Alliance and produce Wi-Fi certified products.

4.3. Bluetooth

4.3.1. What is Bluetooth and how can it be used?

Bluetooth technology was invented by Ericsson in 1994 as a standard for wireless communication between phones and computers. Bluetooth is an open wireless technology standard for exchanging data over short distances among disparate devices and for building personal area networks (PANs) (A56, A123). Bluetooth has an average range of approximately 10 meters. Bluetooth exists in many products and the technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations (A56, A146). A personal computer that does not have embedded Bluetooth can use a Bluetooth adapter that enables the PC to communicate with Bluetooth devices, which makes the technology potential accessible to all users. Bluetooth is a PAN (Personal Area Network) technology and supports data rates up to 2Mbps. Bluetooth is primarily used in a point-to-point or in a star network topology. '*The main use case that made Bluetooth popular initially was hands-free phone calls with headsets and car kits. Thereafter, as mobile phones became more capable, more use cases like high-fidelity music streaming and data-driven cases such as health and fitness accessories evolved*' (R6).

Bluetooth Low-Energy (BLE) (also called Bluetooth Smart), published in 2006, was designed to offer significantly reduced power consumption. '*The power-efficiency of Bluetooth with low energy functionality makes it perfect for devices that run for long periods on power sources such as coin cell batteries or energy-harvesting devices. The smart part is the native support for Bluetooth technology on every major operating system, for easy mobile application development and connectivity for cloud computing and the social economy*' (A67). However, BLE is not really designed for file transfer and is more suitable for small chunks of data. Given its widespread integration in many mobile devices, BLE has certainly a major advantage certainly in a more personal device context. Importantly, version 4.2 allows Bluetooth Smart sensors to access the internet directly via 6LoWPAN connectivity (see 4.5), which makes it possible to use existing IP infrastructure to manage Bluetooth Smart devices.

'*Bluetooth low energy also introduced proximity capabilities that opened the door to location-based services like beaconing and geo-fencing applications'* (R6).

4.3.2. How does the technology deal with standardization?

Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 30,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics (A119, A120, A123). The Bluetooth SIG oversees development of the specification, manages the qualification program, and protects the trademarks (A148). The SIG does not make, manufacture or sell Bluetooth enabled products. Only when a product meets the standards of Bluetooth SIG, a manufacturer may market the product as a Bluetooth device. Bluetooth trademarks are licensed out by the SIG for use to companies that are incorporating Bluetooth wireless technology into their products. To become a licensee, a company must become a member of the Bluetooth SIG (after paying all membership, declaration, enforcement and other fees set by Bluetooth SIG) (A119). The membership is only open to companies, not to individuals. There are three possible memberships: Adopter (lowest degree), Associate and Promoter (highest degree). The SIG also manages the Bluetooth SIG Qualification program, a certification process required for any product using Bluetooth wireless technology and a pre-condition of the intellectual property license for Bluetooth technology (A60, A150).

The SIG members participate in so-called Study Groups, Expert Groups, Working Groups along with committees (A120). The Working Groups are responsible for developing new and enhanced Bluetooth specifications. They are only accessible for a selected group of members. The Expert Groups act as advisors to working groups while providing expertise and guidance. Lastly, the Study Groups develop guidance documentation to enable new usage models which may lead to development of new specifications (A120, A121). The influence of a member on the standardization process thus depends on its membership. Currently there are 7 companies that have been entitled as 'Promoter': Lenovo, Nokia, Intel, Apple, Ericsson, Toshiba and Microsoft (A122). Each Promoter member has one seat (and one vote) on the Board of Directors. When a new idea for a new profile or specification arises by one of the members, the Board of Directors has to approve the idea and assigns it to a study group (A148). Hence, the Promoter members have considerable influence on the strategic and technological directions of Bluetooth.

'One of the primary purposes of the Bluetooth SIG is to help members ensure that all products are properly qualified and comply with the Bluetooth license agreements. This promotes product interoperability and reinforces the strength of the Bluetooth brand to the benefit of all SIG members.

Using an online tool, members qualify and declare their product's compliance to the requirements and conditions of the membership agreements' (A122).

Nowadays, there are several 'kinds' (different amendments to the core specification) of Bluetooth, of which the specifications can be found online on the website of Bluetooth. The most common today are Bluetooth BR/EDR (basic rate/enhanced data rate; version 2.0/2.1) and Bluetooth LE (low energy functionality; version 4.0/4.1/4.2) (A123). Bluetooth EDR establishes a relatively short-range, continuous wireless connection, which makes it ideal for use cases such as streaming audio. Bluetooth LE is suited for bursts of long-range radio connection, making it suitable for Internet of Things (IoT) applications that do not require continuous connection, but depend on long battery life (A126). Nowadays, Bluetooth's strategy is more focused on IoT. In February 2016, the Bluetooth SIG introduced a new architecture including tools (the Bluetooth Internet Gateway Smart Starter Kit) that enables developers to quickly create Internet gateways for Bluetooth products (A129). In this way data can be transferred between Bluetooth sensors and the cloud. This enables one to monitor and control fixed Bluetooth sensors from a remote location, such as turning off the lights while on vacation or unlocking the front door for a friend. The toolkit can be downloaded from Bluetooth's website and is thus publicly accessible. Bluetooth claims that they heard this demand for gateway functionality from consumers, and not only from their members (A129). Moreover, Bluetooth changed its branding by altering the color of their logo, phasing out the Bluetooth Smart and Bluetooth Smart Ready logos, and changing the use of their tagline (A149). Additionally, Bluetooth announced Bluetooth 5 in June 2016, which will include 'significantly increased range, speed, and broadcast messaging capacity' (A133). "*Extending range will deliver robust, reliable Internet of Things (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. These Bluetooth advancements open up more possibilities and enable SIG companies – now at an all-time high of 30,000 member companies – to build an accessible, interoperable IoT."* (A133). This version will be available at the beginning of 2017.

4.3.3. What can be learned from this?

Bluetooth can wirelessly connect disparate devices together. The Bluetooth SIG maintains the standard. For companies Bluetooth is not freely available, they need to pay an administrative fee to use the brand and license the technology. A huge number of companies have joined the SIG which means that numerous devices can be connected with each other through Bluetooth. This obviously makes it a very accessible technology to use for users. However, one could question whether or not

Bluetooth will actually be suitable for IoT applications, since it initially was mainly designed and used for point-to-point communication. Hence, it did not provide network connectivity among devices through the internet, which is exactly what IoT is about. Probably Bluetooth noticed the same, because since the launch of version 4.2, Bluetooth Smart sensors are able access the internet directly, via a 6LoWPAN connection. However, this is not the easiest route for users that want to connect their devices to the cloud. Probably that is why Bluetooth introduced recently the tool kit that enables users to create their own internet gateways for their devices. Hence, a shift takes place from not only offering open standards, but also offering open source technologies. Bluetooth wants to incorporate internet access in their product portfolio. Lastly, and in line with this, Bluetooth 'rebranded' itself as the enabler of IoT networks by explicitly linking its new version Bluetooth 5 to IoT, together with changes in their logo and tagline. Apparently Bluetooth noticed that competition becomes stronger, which forced them to change their innovation strategy into one that is more focused on IoT solutions for consumers.

4.4. ZigBee

4.4.1. What is ZigBee and how can it be used?

Conceived as a mesh network (see appendix 8.2), ZigBee is a specification based on IEEE 802.15.4 that can reach a data throughput of up to 250kbps (although data rates tend to be much lower in practical applications) (A132, A133). The name ZigBee has been derived from the fact that it is a mesh network: '*ZigBee technology is interestingly named after the Waggle Dance that bees do when coming back from a field flight, to communicate to others in their hive the distance, direction and type of food they found'* (R6). The standard defines the protocol layers above the 802.15.4 data link layer and provides several application profiles.

ZigBee can be used in multiple applications, but it is has been mostly applied in smart energy, home automation and in lighting control applications within a +100-meter range (A86, A132). Although an IP specification (i.e. the method or protocol by which data is sent from one computer to another on the Internet) exists for the ZigBee standard, it is detached from the common profiles of the main application areas and has not reached widespread adoption yet. ZigBee networks require an application-level gateway for cloud connectivity. The gateway participates as one of the nodes in the ZigBee network and in parallel runs a TCP/IP stack and application over Ethernet or Wi-Fi to connect the ZigBee network to the Internet. '*Implemented as a node, the gateway is part of the ZigBee network while it simultaneously executes the TCP/IP stack via Ethernet or Wi-Fi*' (A56).

4.4.2. How does the technology deal with standardization?

ZigBee is based on the IEEE 802.15.4 standard, comparable to Wi-Fi and IEEE 802.11 (A86). The ZigBee standard is maintained by the ZigBee Alliance (A132, A134, A135). Its structure is comparable to that of Bluetooth. The Alliance has about 400 members, and only companies can become member. The Alliance is organized by committees, work groups, study groups, task forces and special interest groups and runs certification programs ensuring interoperability between ZigBee devices (A132, A134, A135). The Alliance has three levels of (paid) membership: Adopter, Participant and Promoter. Adopter members ($4000 USD/year) have access to final specifications and documents, may use of the ZigBee Member logo and can participate in interoperability events. Participant members have full participation in all Alliance committees, work/task groups and member meetings and earn voting rights in work groups. Lastly, a Promoter membership ($55000 USD/year) offers automatic voting rights in all work groups, final approval rights on all standards and a seat on the Alliance Board of Directors (A132, A134, A135). Examples of Promoter members are Philips, Texas Instruments, Schneider Electric and Comcast. Membership in the ZigBee Alliance is required if an organization uses the ZigBee brand (name, logos, interoperability icons). It is also required to request ZigBee Certified status for products or to participate in the development of Alliance standards and specifications. For users, no membership is required; ZigBee is an open standard and thus can be used freely by the generic public (only for non-commercial purposes). The specifications can be found online on the website of ZigBee (A86, A133). Like Wi-Fi, also ZigBee has a certification program to ensure that ZigBee-products function as expected and that products from different manufacturers interoperate with each other. The certification of products is also a critical part of the Alliance's standards development process (A130, A133).

Today, the ZigBee Alliance offers three specifications that serve as the base networking system to facilitate its interoperable market standards (A133). First, ZigBee PRO is designed to provide the foundation for Internet of Things. It is optimized for low power consumption and to support large networks with thousands of devices. Second, ZigBee RF4CE was designed for two-way device-to-device control applications that do not require the full-featured mesh networking capabilities offered by the ZigBee specification. Third, ZigBee IP is the first open standard for an IPv6-based full wireless mesh networking solution. It provides seamless Internet connections to control low-power, low-cost devices (A133). In 2014, ZigBee announced ZigBee 3.0, which is a merger from different existing standards into one, in order to simplify to choice for developers when creating IoT applications (A132, A144). In 2015, ZigBee and Thread announced to collaborate in order to create an end-to-end solution for IP-based IoT networks. *"The ZigBee Alliance will incorporate support for the Thread Group's networking layer with the comprehensive ZigBee Applications Layer, which now consolidates* *all previous market-specific ZigBee device profiles into a single, unified library. The goal is to release a complete solution, including an end-to-end certification program, during the third quarter of 2016 that meets the market's desire for IP-based low-power radio frequency communications in the Smart Home and other IoT markets."* (A145).

4.4.3. What can be learned from this?

ZigBee offers open standards in low-power, low data-rate wireless networks. Its range is comparable to that of Wi-Fi which makes it a suitable technology for creating IoT applications at home. The ZigBee Alliance maintains the standard by developing specifications based on IEEE 802.15.4. Companies have to become member of the Alliance in order to produce ZigBee products and/or influence the standardization process. The specifications are available for the generic public, i.e. the standards are open for users. The Alliance is shifting resources from specification development to application standard development. The major work on the ZigBee specification is considered complete. No additional updates to the ZigBee Specification are anticipated or scheduled. ZigBee's strategy is nowadays getting more focused on IoT solutions for users, by merging their own specifications on the one hand, and collaborating with Thread to increase the number of potential IoT solutions on the other hand. This might be a sign that ZigBee is not sure about its market position when it would continue solely.

4.5. 6LoWPAN

4.5.1. What is 6LoWPAN and how can it be used?

6LoWPAN is an open standard defined in RFC6282 by the Internet Engineering Task Force (IETF) (A39, R8). 6LoWPAN is an acronym that combines the latest version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN). Rather than being an IoT application protocols technology like Bluetooth or ZigBee, 6LowPAN is a (mesh) network protocol that only defines an efficient adaptation layer between the 802.15.4 link layer and a TCP/IP stack. '*6LoWPAN is intended for devices featuring very low power consumption and limited processing performance. It is meant to provide IoT connectivity even for very small devices*' (A11). 6LoWPAN aims to apply IP to the smallest, lowest-power and most limited processing power device. A key attribute is the IPv6 (Internet Protocol version 6) stack, which has been a very important introduction in recent years to enable the IoT. IPv6 (the most recent version of the Internet Protocol) is the successor to IPv4 and offers approximately 5 x 1028 addresses for every person in the world. This allows any embedded object in the world to have its own unique IP address, which consequently enables the devices to be connected to the Internet (A11, A39, R8).

4.5.2. How does the technology deal with standardization?

Currently, there is no industry standard for the entire protocol stack, nor a standard organization exists to run certification programs for a 6LoWPAN solution (A11, A39, R6, R8). Manufacturers can develop solutions that are not interoperable at the network layer, because of the multiple optional modes available in the data link layer. '*However, 6LoWPAN devices residing in different networks can communicate via the Internet as long as they use the same Internet application protocol*' (A56). 6LoWPAN applications are, just like Wi-Fi applications, able to access the internet directly, since the gateway is an IP-layer gateway and not an application-layer gateway. Since most of the deployed Internet today is still using IPv4, a 6LoWPAN gateway includes an IPv6-to-IPv4 conversion protocol (R8).

4.5.3. What can be learned from this?

6LoWPAN simplifies the use of IoT applications. Before 6LoWPAN, a complex application layer gateway was needed to make devices such as ZigBee, Bluetooth and proprietary systems connect to the Internet. 6LoWPAN solves this dilemma by introducing an adaptation layer between the IP stack's link and network layers. Its characteristics make the technology suitable for being applied to home automation with sensors and actuators, street light monitoring and control, and residential lighting.

4.6. Z-Wave

4.6.1. What is Z-Wave and how can it be used?

Z-Wave is a low-power radio-frequence communications technology that is primarily designed for home automation. '*The Z-Wave protocol is an interoperable, wireless, RF-based communications technology designed specifically for control, monitoring and status reading applications in residential and light commercial environments*' (A44). Z-Wave supports full mesh networks without the need for a coordinator node and is very scalable, enabling control of up to 232 devices. It is oriented to the residential control and automation market and is intended to provide a simple and reliable method to wirelessly control lighting, security systems, automated window treatments, swimming pool and spa controls, and garage and home access controls (A43, A76).

4.6.2. How does the technology deal with standardization?

Z-Wave is owned by Sigma Designs, which acquired Z-Wave in 2008 from the Danish start-up Zen-Sys. Established in 2005, the Z-Wave Alliance is comprised of industry leaders throughout the globe and aims to foster the development of Z-Wave as key enabling technology for 'smart' home and business applications (A135, A139). '*The Alliance encourages other leading home control manufacturers and service providers to join our dedication to wireless interoperability, and to develop and deploy products that utilize interoperable Z-Wave technology. Our vision is one of a common standard that allows simple wireless control for almost any residential or light commercial product or application'* (A48). Comparable to the technologies mentioned before, there exist different degrees of membership within the alliance: Full, Affiliate or Principal, of which only the 'Principal' members can join the Board of Directors. Currently, these Principal members are ADT, FAKRO, Ingersoll Rand, Jasco, LG U+, Nortek Security & Control, Sigma Designs and SmartThings (A135, A139). In total the alliance consists of 375 companies (A135). The alliance claims to deliver products and services to market that are interoperable, regardless of brand or vendor. To assure this interoperability, each Z-Wave product must pass a stringent conformance test to assure that it meets the Z-Wave standard for complete compliance with all other devices, including backward-compatibility between different versions. '*The key to Z-Wave's adoption by the vast majority of the security industry's lifestyle solutions is its large ecosystem of certified interoperable products. Z-Wave has over 1500 products from over 375 different manufacturers, with all of them interoperable and backward-compatible with each other. No other technology comes close to this kind of extensive ecosystem*' (A139).

Some of the vendors of the Z-Wave Alliance have embraced the open source and hobbyist communities by offering open sources codes that can be used by users to create their own products (A74, A139). An example of this is OpenZWave project, which has to goal '*to create free software library that interfaces with selected Z-Wave PC controllers, allowing anyone to create applications that manipulate and respond to devices on a Z-Wave network, without requiring in-depth knowledge of the Z-Wave protocol*.' (A140).

4.6.3. What can be learned from this?

From the beginning Z-Wave consistently positioned its technology as the enabler for home automation applications, which makes it nowadays a strong brand for consumers that want to command and control their homes. Z-wave designed its network size, bandwidth, efficiency and low power consumption to this end. The standard is maintained by the Z-Wave Alliance, which consists of approximately 375 companies that need to become member of the alliance in order to produce Z-Wave products. The alliance makes sure that products and services will work together with all certified Z-Wave products. Although not provided by the Z-Wave Alliance itself, some manufacturers of Z-Wave products offered open sources codes to the generic public, to enable them to make their own Z-Wave products. This stimulates the use of Z-Wave by allowing users to create their own customized network of applications. Because Z-Wave is mainly designed for home automation (which is just a part of IoT), it may not be suitable for other purposes, like health care or transportation.

4.7. AllJoyn

4.7.1. What is AllJoyn and how can it be used?

AllJoyn is an open source project that provides a programmable software framework that enables developers to create interoperable products that can interact directly with other AllJoyn-enabled products, regardless of operating system, platform, device type, transport layer or brand (A63, A142). '*AllJoyn is an open source software framework that makes it easy for devices and apps to discover and communicate with each other. Developers can write applications for interoperability regardless of transport layer, manufacturer, and without the need for Internet access. The software has been and will continue to be openly available for developers to download, and runs on popular platforms such as Linux and Linux-based Android, iOS, and Windows, including many other lightweight real-time operating systems'* (A62). It consists of an open source software toolkit and code base of service frameworks that enable functionalities as connection management, message routing and security (A63, A142). Users of the AllJoyn framework include developers, hardware manufacturers and consumers. The open source AllJoyn protocol was initially developed by Qualcomm and first presented at the 2011 Mobile World Congress in Barcelona. A few years later, in December 2013, Qualcomm passed the protocol to the Linux Foundation due to moderate successes. From there, the AllSeen Alliance was established with, among others, Cisco, Microsoft, LG, and HTC as members (A62, A63). Unfortunately, no information about the current scope (e.g. number of members of the Alliance and the number of products that use AllJoyn) is publicly available.

4.7.2. How does the technology deal with standardization?

AllJoyn is different from the technologies mentioned before in the sense that is fully open source; anyone can use AllJoyn without being obliged to become member of the alliance (A63). Companies can join by filling out a membership application and agreement. They can choose between a Premier membership (which costs $300,000 in the first year and $250,000 thereafter) or a Community Members (costs ranges between $5,000 and $50,000) (A64, A142). The AllSeen Alliance does not develop standards in the traditional way. '*The Alliance seeks to advance and promote a de facto standard through reuse of a common codebase developed in an open source project*' (A64, A142). The Alliance is governed by its members through participation on a Board (responsible for organization strategy, marketing and direction) and a Technical Steering Committee (responsible for technical decisions). Membership in the project is open to all with multiple levels of participation. Through an open source platform, anyone can contribute and can use the code (although implementation in commercial products requires an Internet Systems Consortium license) (A62, A64, A142). The AllJoyn protocol can be used directly in combination with physical layers that provide an IP stack, like Wi-Fi, Wi-Fi-Direct and Ethernet. For other transports, such as Bluetooth LE, 6LowPan, ZigBee or Z–Wave, support can be added easily (A62, A64, A142). Obviously, the Alliance encourages contributions in this area from the community in order to extend AllSeen's capabilities (A142). Moreover, the so-called AllJoyn Gateway Agent will enable the bridging of connections between devices that are on different transports (e.g. Bluetooth with Wi-Fi).

4.7.3. What can be learned from this?

Of all technologies discussed before, AllJoyn is the 'most open' standard, since the standard is freely available to the generic public and fully open source as well. Users have numerous possibilities to create their own customized IoT network, even if devices run on different technologies. There only might be practical limitations on how many devices can join and participate in a network. For example, for proximity-based networks such as Wi-Fi, the range of the technology may impose a limitation. AllJoyn makes use of the knowledge of (lead) users, by allowing them to contribute to the platform online. These users provide insights about user needs which in turn can be incorporated by products produced by companies of the alliance. Consequently these products will be adopted by users since they match with their needs. This rapid iteration leads to a form of collaborative development that stimulates technology adoption and evolution. However, since no exact numbers are available with respect to the scope of AllJoyn, it cannot be determined for sure if the use of AllJoyn leads to products that meet user needs in a better way in practice. Moreover, not all users may be capable or willing to create their own software/product.

4.8. Thread

4.8.1. What is Thread and how can it be used?

Another relatively new networking protocol aimed at the home automation environment is Thread. It is an IPv6 protocol based on various standards like IEEE 802.15.4 (standard for low-rate WPANs) and 6LowPAN and supports a mesh network using IEEE 802.15.4 radio transceivers (A52, A144). It supports 250 devices, including direct Internet and cloud access for every device since it is IP addressable. '*Thread is a networking protocol with security and low-power features that make it better for connecting household devices than other technologies such as Wifi, NFC, Bluetooth or ZigBee*' (A73).

4.8.2. How does the technology deal with standardization?

It was launched by the Thread Group in 2014 and the protocol is royalty-free (A52, A144). However, a paid membership is required for access to specifications. Companies can become Affiliate, Contributor or Sponsor member, from which Sponsor members have to most benefits and influence on the Group (e.g. a seat in the board of directors). Contributor and Sponsor Thread Group members can contribute to the development of the specification and the certification program through participation in the committees and working groups (A144). The Thread Group is the result of collaboration between Google's Nest Labs and the companies Samsung, ARM Holdings, NXP, Silicon Labs, Qualcomm and Yale, among others. By using a combination of open standards and low-power wireless signals, Thread aims to address several challenges for IoT applications (A52, A56, A144). They are focused on making an impact in the market, rather than serving as a standards body that tries to solve all issues for all industries. '*Most of today's technologies rely on a single device to communicate with products around the home. So if that device fails, the whole network goes down. Today's technologies can also be difficult and confusing to set up. And since many devices around the home need to stay connected 24/7, they end up draining battery life quickly. That's why we designed Thread. We wanted to build a technology that uses and combines the best of what's out there and create a networking protocol that can help the Internet of Things realize its potential for years to come*' (A69). As mentioned earlier, in 2015 Thread announced it is going to collaborate with ZigBee. '*The ZigBee Alliance, a non-profit association of companies creating open, global standards that define the Internet of Things (IoT) for use in consumer, commercial and industrial applications, today announced it is working with the Thread Group on an end-to-end solution for IP-based IoT networks. The solution will become part of the ZigBee Alliance's comprehensive set of product development specifications, technologies, and branding and certification programs*' (A93). Both Thread and ZigBee are based on the IEEE 802.15.4 standard (A52, A56). Comparable to Z-Wave, Nest released the OpenThread open-source implementation of the Thread networking protocol. Developers who chose to use OpenThread in products must join the Thread Group in order to gain the Intellectual Property (IP) rights in order to market them as Thread-certified (A144).

4.8.3. What can be learned from this?

The most existing wireless networking approaches were introduced long before the IoT gained popularity like nowadays. Thread takes existing technologies and uses the best parts of each to provide a better (i.e. no single point of failure, simple connectivity and low power) way to connect products in the home. For consumers it means that they can connect Thread devices to each other and to the cloud for easy control and access from anywhere. However, Thread-certified products are not available for purchase yet. Thread want to strengthen its position by collaborating with ZigBee (a strong brand with respect to home automation applications) on the one hand and offering an open source platform on the other hand to create user involvement in the further design and development of Thread.

4.9. NFC

4.9.1. What is NFC and how can it be used?

Evolved from radio frequency identification (RFID), NFC (Near Field Communication) is a set of communication protocols that enables a two-way interaction between electronic devices. In close proximity, wireless data can be transferred by detecting and enabling technology, without the need for an internet connection. NFC is especially applicable for smartphones, for example to perform contactless payment transactions and to connect electronic devices. When one of the connected devices has Internet connectivity, the other can exchange data with online services. '*Evolved from radio frequency identification (RFID) tech, an NFC chip operates as one part of a wireless link. Once it's activated by another chip, small amounts of data between the two devices can be transferred when held a few centimeters from each other'* (A97). No pairing code is necessary to link up and it is much more power-efficient than other wireless communication types, because it uses chips that run on very low amounts of power.

4.9.2. How does the technology deal with standardization?

NFC standards cover communications protocols and data exchange formats and are based on existing radio-frequency identification (RFID) standards, such as the ISO/IEC 18092 and ISO/IEC 14443 standards (A128, A131). ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) both publish international standards. NFC is empowered by the NFC Forum, which has been established in 2004 by Nokia, NXP and Sony. The NFC Forum develops specifications and test mechanisms in order to enable interoperable and safe NFC-based worldwide (A128, A131). Comparable to technologies discussed before, companies can become member of the NFC Forum trough a paid membership with varying benefits and influence (A128). Currently the Forum has approximately 200 members, with Nokia, NXP, Sony, Google, Apple, Intel and Visa being part of the board of directors, among others (A128). The NFC specifications are accessible for members only. For non-member, the specifications are available for purchase after completing a license agreement. The NFC Forum has created a special IoT working group to encourage broad adoption of the NFC technology by working with key players in the IoT industry (A131).

4.9.3. What can be learned from this?

NFC is not considered as a specific technology designed for IoT applications yet. It was designed for other purposes, but can be used additionally for IoT applications now IoT is becoming more and more well-known. For consumers, NFC is comparable to Bluetooth with respect to some of its functionalities. NFC and Bluetooth are both short-range communication technologies available on mobile phones. NFC operates at slower speeds than Bluetooth, but consumes far less power and does not require pairing. NFC has a shorter range, which reduces the likelihood of unwanted interception. When two devices are equipped with a NFC tag, NFC enables users to simply add or remove devices to the internet gateway of their smart home network, by transferring the configuration information of the network to the device when they are held close to each other. The mobile device then configures itself to the network and instantly connects. This saves the user manual network selections and typing passwords. Hence, NFC will be of use as additional feature to a wireless protocol that allows internet connectivity, like Wi-Fi or Bluetooth.

4.10. LoRaWAN

4.10.1. What is LoRaWAN and how can it be used?

Only one year old, LoRaWAN is a Low Power Wide Area Network (LPWAN) specification intended for wireless battery operated devices (A16, A56). Its network architecture is a typical star topology in which the gateways transfer messages between end-devices and a central network server. Gateways are connected to the network server via standard IP connections. '*Communication between end-devices and gateways is spread out on different frequency channels and data rates. The selection of the data rate is a trade-off between communication range and message duration. Due to the spread spectrum technology, communications with different data rates do not interfere with each other and create a set of "virtual" channels increasing the capacity of the gateway'* (A17). LoRaWAN data rates range from 0.3 kbps to 50 kbps. The LoRaWAN technology is ideal to target battery operated sensors and low power applications. LoRaWan has a significant range; a gateway deployed on a building or tower can connect to sensors more than 10 miles away or to sensors meters under water (A137, A138).

4.10.2. How does the technology deal with standardization?

LoRaWAN was presented in 2015 by the LoRa Alliance, which aims to standardize IoT. Members of the alliance include technology leaders such as IBM, ZTE, Bouygues and Semtech. Companies can join the alliance through a paid membership. The LoRa Alliance offers four levels of membership, which vary by privileges and participation level. '*The primary goal of the LoRa Alliance is to standardize*

LPWAN and through standardization enable large scale volume IoT deployments. The LoRaWAN™ ecosystem will enable product availability, the LoRaWAN™ Certification Program will ensure interoperability and both are due to our members collaborating together on the LoRaWAN™ standard' (A18). The The LoRaWAN R1.0 specification can be downloaded freely from the website of the Alliance. Hence, the technology is an open source protocol (A137, A138).

4.10.3. What can be learned from this?

Despite the numerous technologies that are already on the market which can be used for IoT applications, it apparently is still attractive for companies to launch a new technology and collaborate in the form of an alliance. Because IoT is still developing, also new technologies are developed that have improved features compared to the technologies already available. Moreover, relatively new technologies in the field of IoT, like LoRaWAN, are branded as being 'the enabler of IoT' more than the older technologies, since the concept IoT gains nowadays more publicity and awareness.

4.11. Open source projects

Besides the standards offered by the industry, open source platforms exist which help users to create their own customized application, based on the different devices they would like to have connected. AllJoyn already integrates these open source projects in their business model. An important note to make is that consumer adoption of IoT is not as far as the adoption by the industry. '*One contributing factor to this lag in the consumer market is that most consumers don't know the Internet of Things (IoT) exists'* (A52). However, some projects already have started. Some examples of these projects are mentioned below.

4.11.1 Kaa

Kaa is a multi-purpose middleware (the session, presentation and application layer from the OSI model) platform for building complete end-to-end IoT solutions, connected applications, and smart products. The Kaa platform provides an open toolkit with features for the IoT product development and thus reduces associated cost, risks, and time-to-market. Kaa offers a set IoT features that can be easily plugged in and used to implement a large majority of the IoT use cases. The software developments kits of Kaa are capable of being integrated with virtually any type of connected device or microchip. '*The Kaa server provides all the back-end functionality needed to operate even large-scale and mission-critical IoT solutions. It handles all the communication across connected objects, including data consistency and security, device interoperability, and failure-proof connectivity'* (A103). The Kaa server features interfaces for integration with data management and analytics systems, as well as with product-specific services. It enables the user to expand and customize the product to meet specific desired requirements.

4.11.2. OpenRemote

OpenRemote is an open source project, started back in 2009, with the ambition to overcome the challenges of integration between many different protocols and solutions available for home automation, and offer visualization tools. '*The challenge has only become bigger and expanded beyond home automation into several other application domains, ranging from building integration, to healthcare, hospitality, entertainment, and public spaces'* (A102). The OpenRemote Professional Designer consists of three software elements, the online Designer, the Controller, and the Apps or Panels. In the Designer the user can configure the system of devices and internet services. The Controller is the brain of the system and connects all the different devices and services. It also runs the automation scripts one has designed. Via de Apps the user can see the status of the devices or services as well as control the buttons, switches, sliders, or color pickers.

4.11.3. Arduino

Arduino is an open-source prototyping platform based on 'easy-to-use' hardware and software. Arduino boards are able to read inputs (light on a sensor, a finger on a button, or a Twitter message), turn it into an output and thereby activating a motor, turning on an LED or publishing something online. The user can tell the board what to do by sending a set of instructions to the microcontroller on the board. Over the years Arduino has been the brain of thousands of projects, from everyday objects to complex scientific instruments. *A worldwide community of makers - students, hobbyists, artists, programmers, and professionals - has gathered around this open-source platform, their contributions have added up to an incredible amount of accessible knowledge that can be of great help to novices and experts alike'* (A100).

4.11.4. Kinoma

KinomaJS is an open source runtime environment optimized for delivering applications on a wide range of IoT and consumer electronics products. With KinomaJS, developers can build embedded device applications using JavaScript. The platform is open source, so developers can customize Kinoma software across their product ecosystem, use preferred hardware components and cloud services, and do more with the products they create. '*The Kinoma open platform can accelerate the development of a broad range of IoT applications, including industrial, medical, smart objects and smart devices'* (A98).

4.11.5. Eclipse IoT Project

The Eclipse Project was originally created by IBM in November 2001 and supported by a consortium of software vendors. The Eclipse Foundation was created in January 2004 as an independent not-for-profit corporation. The independent not-for-profit corporation was created to allow a vendor neutral and open, transparent community to be established around Eclipse. *The Eclipse Foundation has been established to serve the Eclipse open source projects and the Eclipse community. As an independent not-for-profit corporation, the Foundation and the Eclipse governance model ensures no single entity is able to control the strategy, policies or operations of the Eclipse community'* (A102). Today, the Eclipse community consists of individuals and organizations from a cross section of the software industry.

4.12. Concluding remarks

The technologies and their standards that have been developed in the last fifteen years serve different purposes. Because each standard creates different features, it depends on the context which technology suits a certain purpose the best. For example, Wi-Fi can be used for home control, but requires too much energy for battery-powered devices, and might be subject to unreliability through traffic jams in homes with multiple Wi-Fi devices. But it is optimized for high bandwidth and high-power data transmission using a server-client topology. Bluetooth is optimized for short-range, high-bandwidth, one-to-few topology, but it does not really have the range or network size for home control. Battery-operated Z-Wave devices can last for years, but are mainly focused on home automation. Near Field Communication (NFC) is optimized for very short range and does not make use of internet directly, but is very power consuming. Moreover, some standards define different layers of the OSI model (see appendix 8.1.), which means that some technologies can complement each other in building an IoT network.

Standardization mainly allows the use of devices from other manufacturers, but does not incorporate devices that run on other technologies. However, relatively new technologies like 6LoWaPAN, AllJoyn and LoRaWAN, try to change this by publishing their specification in order to allow developers and users to connect their devices, even if they run on different technologies. The key objective in this strategy is to offer users value propositions by providing solutions to connecting different kinds of devices to the internet.

The established technologies, like Wi-Fi or Bluetooth, mainly focus on proprietary approaches in order to increase market share and deal with competition. Although this approach has added value for manufacturers, it does not have an added value for users per se. It is understandable why companies do so though. After all, most of established technologies have been created in their own industry before IoT arose. In these industries, they are part of a core business to the companies that created them. IoT combines these different technologies into a new paradigm, but that does not mean automatically that companies will stop their core business in the industry they originally operate. However, since the concept IoT becomes more well-known, the alliances that develop these technologies seem to recognize the importance of IoT solutions for users, despite that the technology they produce had originally been developed for other purposes. Hence, the focus shifts to creating a value proposition to users by, for example, offering bridging devices or technologies that allow connecting devices that run on different networks or protocols. These pieces of software that can mediate between applications running on different technologies are called middleware. Middleware thus increases interoperability among devices. Moreover, the growing awareness of IoT has led to the realization that learning from users becomes an important factor for the development and diffusion of IoT. Hence, a shift takes place to offering open source platforms that provide users a package of technologies that allow them to build their own IoT network.

5 Conclusion

This research started with the question which strategies have been used in order to create open standards with respect to IoT and how this affects standardization of IoT nowadays. Now an answer to this question can be given. Hereby a distinction can be made between established technologies that were already on the market before IoT became well-known, and technologies that have recently been developed specifically for the purpose of IoT. Most technologies that enable IoT already existed before the concept IoT really became popular. These technologies itself were already standardized in the industry they were created. Since the concept of IoT gains more publicity nowadays, these enabling technologies are altered and rebranded in an attempt to offer value propositions to users according to the new paradigm of IoT in which everything should work together. Ironically, the main strategy that has been used in these cases leads to fragmentation within the IoT field. Standardization of established technologies that enable IoT is characterized by proprietary approaches based on international standards, like standards established by the IEEE. Taking such a standard as a starting point, alliance formation takes place by a number of companies in order to further develop the technology. Forming an alliance reduces the risk individual companies have with respect to technological development or market entry. Moreover, it reduces time and costs to develop and commercialize new products. Lastly, it stimulates shared learning and knowledge exchange. The alliances have dealt with open standardization through the realization of new standardization specifications, as amendments to the core specification of the technology. These amendments or revisions are treated as standards by the corporate world, in order to denote new functionalities concisely and thereby creating value propositions for users. The core specification of an established technology might originally be developed for other purposes than IoT per se. Additional amendments try to redirect this towards IoT applications. For example, technological progress and changing markets lead to a new version of the technology that is more power-consuming or more interoperable with other devices, even if those devices are from different manufacturers. By means of certification programs the alliance can determine whether or not a manufacturer is allowed to add a certain product to the portfolio of the alliance. The establishment of several alliances with each its own proprietary approach, has given the field of IoT different 'silos' of devices that are mainly interoperable with only those devices and technologies within the same brand product line. Alliance formation offers companies added values, but does not offer consumers added values in the light of IoT per se. After all, IoT does not work unless the 'everything' works together: products from different companies that also might run on different technologies will need to communicate with each other. Consequently, it seems to be more and more recognized by the actors in the field that true interoperability is the key. Standardization therefore slowly incorporates features that allow a device to connect with a device from another manufacturer or a device that runs on another technology (i.e. middleware that serve as 'bridging units'). Manufacturers carefully enable users more to create an ecosystem (i.e. combining different technologies/devices) of interoperable devices instead of keeping users locked in to a certain product line (i.e. products from the same manufacturer based on one technology). Eventually this will create a network effect for manufacturers that stimulates further adoption.

Technologies that have recently been developed specifically for the purpose of IoT, deal with open standardization in a slightly different way. Although controlled by an alliance of multiple companies too, a shift takes place to open source standardization. Open source software and inter-industry collaboration have continually gained popularity. Open source projects provide the technological building blocks, i.e. middleware, that developers can use to create the interoperable devices that make up their own customized ecosystem of devices. Hence, the last few years numerous open source projects have arisen that enable users to create their own customized IoT network. Some of the alliances mentioned above have integrated such an open source project in their business model. These alliances thus have a dual strategy with respect to open standardization: create series of specifications determined by their members on one hand, and allow users to compose their own technologies and devices on the other hand. These open source platforms enable user involvement. Consequently, user involvement allows manufacturers to learn from them: what do users want and how do they apply their technology? Since IoT is still diffusing, only selections of (lead) users are currently experimenting with IoT. It is recommended that the industry treats users more as co-developers in the development and deployment of IoT. Especially when IoT further develops and gains more awareness among the generic public, this will be essential in order to stimulate adoption. This will also provide the industry with the exact needs of the users, something which would otherwise be more difficult to know. This same dynamic will likely be played out to varying extents in other areas, i.e. more focused platforms and ecosystems will emerge that are specific to an industry or specific solution. Thus, innovation stems not only from manufacturers anymore, but also from users. Coordination and knowledge exchange among users, technological solutions and their builders is a key factor. Future standardization strategies need to focus on open source and inter-industry collaboration in order to effectively connect (established) technologies for the purpose of IoT. Only then all the 'things' can really work together.

6 Discussion

6.1. Theoretical implications

A dominant design does not emerge in open complex technical systems like IoT. Instead, a dominant configuration emerges that influences further technological innovation. A dominant configuration defines how to arrange components for a specific IoT purpose, leading to a certain architecture. Unlike a dominant design, a dominant configuration can be exchanged for another in a relatively short period of time, depending on its context. Thus, a dominant configuration has a temporary character. More dominant configurations can exist next to each other in the IoT field, i.e. the field could comprise several systems. Before a dominant configuration emerges, innovation is initially based on frequent major product changes created by industry pioneers and product users. Competition is based on functional product performance and fitness for use. There are many competitors, but because they mostly unite themselves in alliances, the number of 'competing units' is limited.

The openness of IoT, in which components need to be able to rearrange, impedes stabilization towards the specific phase of the innovation life cycle. Consequently, the realization of mass markets is insecure. Hence, the innovation life cycle in classic dominant design theory does not apply here. Components stem from different industries and have been created according to the purposes and market conditions set by that industry. These different conditions are mixed together when taking all components together for the purpose of IoT. Thus, IoT cannot be seen as a comprehensive industry, but rather needs to be considered as a field that cuts through different industries in which components exist that have different backgrounds with respect to their creation and development. These different backgrounds need to be maintained due to the openness of IoT. This implies that consolidation of the IoT field is not possible. Consequently, the same technology of a manufacturer can be part of multiple dominant configurations. After all, when manufactures offer consumers the technological building blocks by means of open (source) standards, these building blocks or components can be used in different ways. The required arrangement (i.e. the architecture) of these components depends on the context in which the components are situated. This has major implications for innovation, since incremental innovation along the rules of a dominant design within one comprehensive industry is not possible. Instead, innovation stems from coordinating the existence of different components within the field and obtaining architectural knowledge from users. Innovation is about the linking of components to each other, through inter-industry collaboration, knowledge exchange and open source platforms. Further research should determine how this should be organized exactly. Another suggestion for further research is how manufacturers could incorporate architectural knowledge from users in a sustainable way.

Incremental innovation is possible at the component level though. Economies of scale and incremental product changes lead to cumulative improvements in productivity and quality (e.g. more power-consuming or extensive interoperability) of components. Product innovation is increasingly about differentiation through customization to meet the needs of particular users.

This context is mainly determined by user needs, i.e. the users possess specific knowledge that provides a manufacturer insight in what users want and expect. In other words, users can provide manufacturers knowledge about the desired architecture. Hence, open source project not only enable users to create their own customized IoT system, but also help manufacturers to gather architectural knowledge and learn from the field. Innovation strategies should thus allow learning from users. Further research should determine which forms of user involvement yield the most valuable information.

6.2. Practical implications

Policy makers have to keep in mind that IoT is a relatively new paradigm, although the field and the technologies that enable IoT might exist for a longer time already. Because of the new paradigm, the concept might not yet be diffused to all possible users. Currently the open source projects are mainly executed by lead users. Lead users are defined as members of a user population who anticipate obtaining relatively high benefits from obtaining a solution to their needs. Therefore, lead users may innovate and are at the leading edge of important trends in a marketplace under study. Hence, they are currently experiencing needs that will later be experienced by many users in that same marketplace (von Hippel, 1986). At first, the factors influencing the lead users’ use of IoT can be different from ordinary consumers, but as indicated by von Hippel (1986), lead users’ needs will later be experienced by other users in the marketplace too. Hence, it can be expected that the factors influencing the consumer use of other users are similar as well in the end. A repetition of this research after IoT has further been developed, and thereby has reached the awareness of the ordinary consumer, will reveal whether the factors influencing consumer use are indeed similar to those of lead users now.

Moreover, because of the openness of IoT, policy makers need to lead on to non-proprietary approaches in order to facilitate true interoperability. They should develop a business model in which both users as manufacturers can benefit from of a field consisting of fully interoperable devices, regardless the wireless technology a device runs on (e.g. creating network effects for manufacturers and simplified IoT solutions for users at the same time). This will defragment the standardization landscape of IoT and stimulate the development and deployment of technological products that are fully interoperable with each other. Not acknowledging the configurational open nature of IoT will lead to failed standardization attempts.

6.3. Limitations

Although this research has been set up with great care, it does have some limitations. This research has used a qualitative approach in order to answer the research question. This seemed to be an appropriate way since it resulted in a deeper understanding of the standardization strategies concerning the Internet of Things. Scientific articles and documents were analyzed. Unfortunately, these data often presented only a part of the whole strategy since they are mostly secondary data. Thus, strategies have been derived from secondary data. The detailed innovation strategies that have been set up internally within corporations were not visible in this way, nor the reasons according to them why certain strategies did or did not succeed. To fully understand how corporations deal with the standardization issues internally, which connections between companies exist and what their exact plans are, one needs to be in connection with the companies directly. Unfortunately interview requests were rejected so this information (if given in an interview anyway), is not part of the data. However, by analyzing articles and documents (grey literature), a lot of historical information had been obtained. This enabled theoretical sampling to be applied, which helped to refine the concepts and increases the validity of this research. That is, the results are grounded in a broad field of data.

Cases were selected based on theoretical sampling. Because of the overlap IoT has with home automation, it is possible that potential useful cases have not been taken into account, because they might be linked to the term 'home automation' instead of 'IoT'. However, as mentioned in the methodology, it is expected that relevant cases also appeared when using 'IoT' to denote the field, since home automation is a part of what nowadays is called IoT.

In this research theoretical sampling was used in order to collect and analyze the data, i.e. data were collected on basis of constant comparison of the concepts in order to identify interesting aspects regarding the research question. This makes that the analyzed data is not necessarily representative for the whole IoT field. Hence, this research aims to generalize results to theory rather than providing full evidence or truth statements.

7 Bibliography

Atzori, L., Iera, A. and Morabito, G. (2010). The internet of things: A survey. *Computer Network*, vol. 54 (15), pp. 2787–2805.

Axelrod, R. M., Mitchel, W., Bennet, R. E., & Bruderer, E. (1995). Coalition formation in standard-setting alliances. *Management Science* (41), pp. 1493-1508.

Baron, J., Ménière, Y. & Pohlmann, T. (2014). Standards, consortia, and innovation. *International Journal of Industrial Organization*, vol.36, pp. 22-35.

Beal, V. (2015). The 7 layers of the OSI model. Retrieved at 26 March 2016 from http://www.webopedia.com/quick_ref/OSI_Layers.asp

Bellavista, P., Cardone, G., Corradi, A. and Foschini, L. (2013). Convergence of MANET and WSN in IoT urban scenarios, *IEEE Sensors Journal*, vol. 13 (10), pp. 3558–3567.

Bandyopadhyay, D. and Sen, J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communication*, vol. 58 (1), pp. 49-69.

Bryman, A. (2008). *Social Research Methods*, Oxford University Press, London.

European Commission (2015). The Internet of Things. Retrieved at 7 November 2015 from http://ec.europa.eu/digital-agenda/en/internet-things#Article

European Commission (2016). The Alliance for Internet of Things Innovation (AIOTI). Retrieved at 9 December 2015 from https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti

European Parliament (2015). The Internet of Things - Opportunities and challenges. Retrieved at 14 November 2015 from http://www.europarl.europa.eu/RegData/etudes/ BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

Fell, Mark (2014). Roadmap for the Emerging Internet of Things - Its Impact, Architecture and Future Governance. Carré & Strauss, United Kingdom. Retrieved at 11 October 2015 from http://sweden.nlembassy.org/binaries/content/assets/postenweb/z/zweden/netherlands-embassy-in-stockholm/iot_roadmap_final_draft_0309145.pdf

Henderson, R. and Clark, K.B. (1990). Architectural innovation: the reconfiguration of existing product technologies and failures of established firms. *Administrative Science Quarterly*, vol.35 (1), pp. 9–30.

IERC (2015). Internet of Things – Position Paper On Standardization for IoT technologies. Retrieved at 23 November 2015 from http://www.internet-of-thingsresearch.eu/pdf/IERC_Position_Paper_IoT_Standardization_Final.pdf

International Telecommunication Union (2005). The Internet of Things. Retrieved at 23 November 2015 from https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

Laya, A., Bratu, V.I. and Markendahl, J. (2013). Who is investing in machine to machine communications*? Proc. 24th Eur. Reg. ITS Conf., Florence, Italy*, pp. 20–23.

Murmann, J.P and Frenken, K. (2006). Toward a systematic framework for research on dominant designs, technological innovations, and industrial change*, Research Policy,* vol.35 (7), pp. 925–952.

Narayanan, V.K. and Chen, T. (2012). Research on technology standards: Accomplishment and challenges. *Research Policy*, vol.41 (8), pp. 1375-1406.

Peine, A. (2008). Technological paradigms and complex technical systems – the case of Smart Homes, *Research Policy*, vol. 37, pp. 508-529.

Peine, A. (2009). Understanding the dynamics of technological configurations: A conceptual framework and the case of Smart Homes. *Technological Forecasting & Social Change*, vol.76, pp. 396–409.

Reiter, G. (2014). Wireless connectivity for the Internet of Things. Retrieved at 3 February 2016 from http://www.ti.com.cn/cn/lit/wp/swry010/swry010.pdf

Saunders, M., Lewis, P. & Thornhill, A. (2009). *Research methods for business students*. Pearson Eduction.

Scott, W.R. (1995). *Institutions and organizations*. Sage Publications, London/New Delhi.

Shin, D-H., Kim, H. & Hwang, J. (2015). Standardization revisited: A critical literature review on standards and innovation, *Computer Standards & Interfaces*, vol. 35, pp. 152-157.

Tidd, J., Bessant, J.R. & Pavitt K. (2009). *Managing innovation: integrating Technological, Market and Organizational Change*. Chichester: Wiley

Utterback, J. M. (1996). *Mastering the dynamics of innovation*. Boston, Machachusetts: Harvard Business School Press.

Utterback, J.M., Suárez, F.F. (1993), Innovation, competition and industry structure, *Research Policy*, vol. 22, pp. 1-21.

Von Hippel, E. (1986) Lead users: a source of novel product concepts. *Management Science*, 32(7), pp. 791-806.

Yin, R. K. (2003). *Case Study Research, Design and Methods*, 3rd ed. Newbury Park: Sage Publications, pp.19-39, 97-107.

Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, vol 1 (1), pp. 22-32.

8 Appendix

8.1. Architecture of IoT

Communication systems utilize a set of rules and standards to format data and control data exchange (Reiter, 2014). The most common model in data communication systems is the Open Systems Interconnection (OSI) model, which breaks the communication into functional layers allowing easier implementation of scalable and interoperable networks. Within this research, the OSI model will be used to shape the architecture of IoT. The OSI model is not tangible, but helps to better understand complex interactions. The OSI model has 7 layers (together also called a 'stack'), which will be elucidated below (see also figure 3).

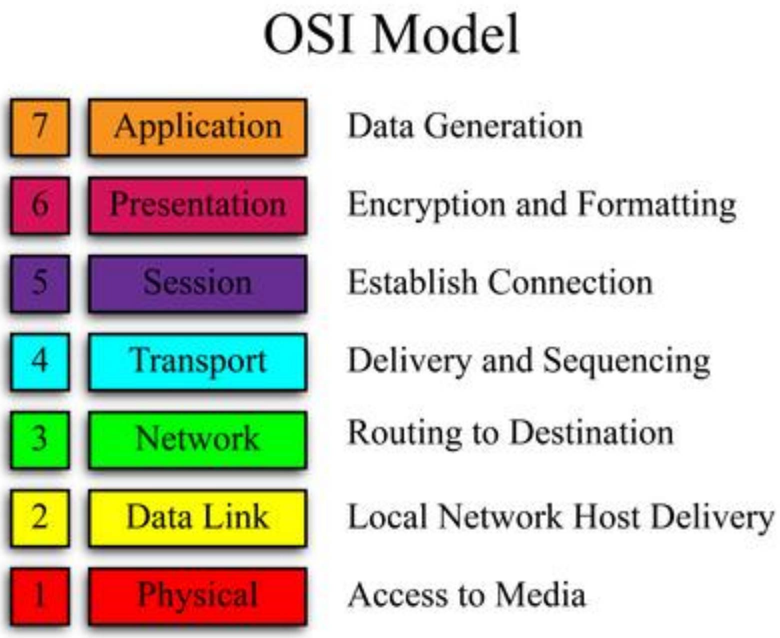

Fig. 3. Illustration of the OSI model (Beal, 2015)

1. **Physical layer**: conveys the bit stream (electrical impulse, light or radio signal) through the network at the electrical and mechanical level. This hardware layer consists of sensor networks, embedded systems, radio-frequency identification (RFID) tags and readers or other soft sensors in different forms. These entities are the primary data sensors deployed in the field (Atzori et al., 2010; Bandyopadhyay & Sen, 2011).
2. **Data link layer**: encodes and decodes data packets into bits. In this layer, the appropriate physical protocol is assigned to the data. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to

transmit it. The LLC layer controls frame synchronization, flow control and error checking (Beal, 2015).

3. **Network layer:** provides switching and routing technologies for transmitting data from node to node. IP (Internet Protocol) is the network layer protocol of the Internet, providing an IP address to devices and carrying IP packets from one device to another (Reiter, 2014; Beal, 2015).
4. **Transport layer:** his layer maintains flow control of data and provides for error checking and recovery of data between the devices. TCP (or Transmission Control Protocol) is the predominant transport protocol in the Internet (Reiter, 2014).
5. **Session layer**: establishes, manages and terminates connections between applications (Beal, 2015).
6. **Presentation layer**: has a converting function, by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. Moreover, this layer formats and encrypts data to be sent across a network (Beal, 2015).
7. **Application layer**: supports application and end-user processes (Bandyopadhyay & Sen, 2011; Beal, 2015). A popular application layer protocol in the TCP/IP stack is HTTP (or Hypertext Transfer Protocol) which was created to transfer web content over the Internet (Reiter, 2014).

8.2. Topologies of wireless networks

Wireless networks can be categorized by their topology, i.e. the way nodes in the network are arranged and connected to each other. The two most fundamental network topologies are star topologies and mesh topologies (see figure 4).

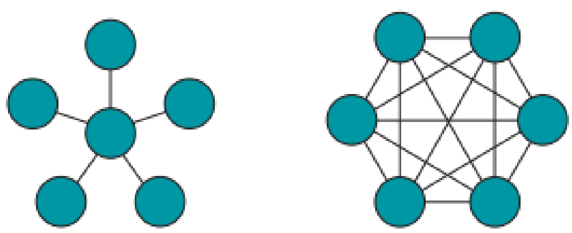

Fig. 4. A star topology (left) and a mesh topology (right) (Reiter, 2014)

In a star topology, all nodes are connected to a central node which usually provides the Internet connection as well. A popular example of a star topology is a WiFi network, where the center node is called an access point (AP) and the other nodes are called stations. In a mesh network, every node can connect to multiple other nodes. One or more nodes in the network serve as an Internet gateway. In this model, each node in the network is connected to every other node. However, mesh networks are more complex to design and forwarding messages can take much longer than in a star network. The benefit of a mesh topology is that it can extend the range of the network through multiple nodes, without increasing the power of the transmitters. They are also more reliable because there a more than one path to relay a message through the network. Mesh networks can potentially consist of thousands of nodes.

8.3. Data references

(A1) Ashton, K. (2009). That 'Internet of Things' Thing. Retrieved from http://www.rfidjournal.com/articles/view?4986

(A2) Hanlon, M. (2004). LG Internet Refridgerator. Retrieved from http://www.gizmag.com/go/1132/

(A3) Planetary Skin Institute (2016). About us. Retrieved from http://www.planetaryskin.org/about-us

(A4) Internet Society (n.d.) IPv6 is the new normal. Retrieved from http://www.worldipv6launch.org/

(A5) Ma, M. (2014). No-power Wi-Fi connectivity could fuel Internet of Things reality. Retrieved from http://www.washington.edu/news/2014/08/04/no-power-wi-fi-connectivity-could-fuel-internet-of-things-reality/

(A6) Ryall, J. (2014).Google Admits Secretly Testing a Drone Delivery System. Retrieved from http://mashable.com/2014/08/28/google-project-wing-drone-delivery-australia/#z6GI7SLuP8qj

(A7) Efrati, A. and Nellis, S. (2015). Google Developing 'Brillo' Software for Internet of Things. Retrieved from https://www.theinformation.com/Google-Developing-Brillo-Software-for-Internet-of-Things

(A8) Want, R., Hopper, A., Falcao, V. and Gibbons, J. (n.d.). The Active Badge Location System. Retrieved from http://alumni.media.mit.edu/~dmerrill/badge/Want92_ActiveBadge.pdf

(A9) Cisco (2015). Cisco Visual Networking Index: Forecast and Methodology, 2014-2019 White Paper. Retrieved from http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html

(A10) ITU (2014). Internet of Things – Trends and Challenges in Standardization. Retrieved from http://www.itu.int/en/ITU-T/Workshops-and-Seminars/iot/201402/Pages/default.aspx

(A11) RS Components (n.d.). 11 Internet of Things (IoT) Protocols You Need to Know About.

Retrieved from http://www.rs-online.com/designspark/electronics/knowledge-item/eleven-internet-of-things-iot-protocols-you-need-to-know-about

(A12) Matternet ONE (n.d.). Our product. Retrieved from https://mttr.net/

(A13) Lawson, S. (2014). Samsung, ARM, and Nest launch Thread, a low-power network for the smart home. Retrieved from http://www.pcworld.com/article/2454120/samsung-arm-and-nest-launch-thread-group-to-tie-home-iot-devices-together.html

(A14) GSMA (2015). GSMA Welcomes mobile industry agreement on technology standards for global low power wide area market. Retrieved from http://www.gsma.com/newsroom/press-release/gsma-welcomes-mobile-industry-agreement-on-technology-standards/

(A15) Sword, A. (2015). Mobile industry agrees IoT standards for M2M and wearables. Retrieved from http://www.cbronline.com/news/internet-of-things/m2m/mobile-industry-agrees-iot-standards-for-m2m-and-wearables-4756534

(A16) Yu, S. (2015). Industrial Internet Consortium and IEEE Standards Association Collaborating Toward Comprehensive Framework for Interoperable Internet of Things (IoT). Retrieved from https://standards.ieee.org/news/2015/iic_liaison.html

(A17) LoRa Alliance (2016). LoRa Technology. Retrieved from https://www.lora-alliance.org/What-Is-LoRa/Technology

(A18) LoRa Alliance (2016. LoRa FAQ. Retrieved from https://www.lora-alliance.org/The-Alliance/FAQ

(A19) Weinschenk, C. (2015). The who's who of Internet of Things standards bodies. Retrieved from http://boundless.aerohive.com/experts/The-Whos-Who-of-Internet-of-Things-Standards-Bodies.html

(A20) IEEE (2016). Internet of Things Related Standards. Retrieved from http://standards.ieee.org/innovate/iot/stds.html

(A21) Murphy, M. (2015). Cisco spearheads yet another IoT standards group leaving Google, Samsung, SAP, IBM and Intel at odds with each other. Retrieved from http://www.techworld.com/networking/cisco-spearheads-yet-another-iot-standards-group-leaving-google-samsung-sap-ibm-intel-at-odds-with-each-other-3618838/

(A22) Duffy, J. (2015). Cisco leading another IoT standards group. Retrieved from http://www.networkworld.com/article/2944510/internet-of-things/cisco-leading-another-iot-standards-group.html

(A23) Lawson, S. (2014). Why Internet of Things 'standards' got more confusing in 2014. Retrieved from http://www.pcworld.com/article/2863572/iot-groups-are-like-an-orchestra-tuning-up-the-music-starts-in-2016.html

(A24) Vizard, M. (2015). Internet of Things Standards Bodies Merge. Retrieved from http://www.itbusinessedge.com/blogs/it-unmasked/internet-of-things-standards-bodies-merge.html

(A25) Hughes, T. (2016). A world with more IoT standards bodies than IoT standards. Retrieved from http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/A-world-with-more-IoT-standards-bodies-than-IoT-standards

(A26) WiFi Alliance (n.d.). Who We Are. Retrieved from http://www.wi-fi.org/who-we-are

(A27) Postscapes (2013). Key Internet of Things Players: Large. Retrieved from http://postscapes.com/internet-of-things-key-players-large-companies

(A28) Wanpeng, F. and Yu, L. (2010). Opportunities, Challenges and Practices of the Internet of Things. Retrieved from http://wwwen.zte.com.cn/endata/magazine/ztetechnologies/2010/no5/articles/201005/t20100510_184418.html

(A29) Lavars, N. (2013). Tech giants form AllSeen Alliance to fast track "Internet of Everything". Retrieved from http://www.gizmag.com/allseen-alliance-internet-of-everything/30091/

(A30) JLL (n.d.). IntelliCommand. Retrieved from http://www.us.jll.com/united-states/en-us/intellicommand

(A31) Z-Wave Alliance (2005). Z-Wave Labs Applications Open In First Ever Global Z-Wave IoT Competition. Retrieved from http://z-wavealliance.org/z-wave-labs-applications-open-in-first-ever-global-z-wave-iot-competition/

(A32) GreenPeak (2007). Compliant to Industry Standards. Retrieved from http://www.greenpeak.com/Technology/Standards.html

(A33) Darianian, M. (2008). Smart Home Mobile RFID-Based Internet-of-Things Systems and Services. Retrieved from http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4736933&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4736933

(A34) Kranenburg, R. van (2008). The Internet of Things. Retrieved from http://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf

(A35) Banafa, A. (2013). The Internet of Things (IoT): 8 Myths and Facts. Retrieved from https://datafloq.com/read/internet-of-things-iot-myths-and-facts/1042

(A36) IEEE (n.d.). IEEE Mission & Vision. Retrieved from https://www.ieee.org/about/vision_mission.html

(A37) IEEE802.15 (2004). IEEE 802.15 WPAN Task Group 1 (TG1). Retrieved from http://www.ieee802.org/15/pub/TG1.html

(A38) WiFi Alliance (2009). Board of Directors. Retrieved from http://web.archive.org/web/20090917083253/http://www.wi-fi.org/board_of_directors.php

(A39) Neagle, C. (2014). A guide to the confusing Internet of Things standards world. Retrieved from http://www.networkworld.com/article/2456421/internet-of-things/a-guide-to-the-confusing-internet-of-things-standards-world.html

(A40) Randewich, N. (2014). Google's Nest launches network technology for connected home. Retrieved from http://www.reuters.com/article/us-google-nest-idUSKBN0FK0JX20140715

(A41) Fried, I. (2014). Google, Freescale Backing Yet Another Internet-of-Things Standard Effort. Retrieved from http://recode.net/2014/07/15/google-freescale-backing-yet-another-internet-of-things-standard-effort/

(A42) Walters, M. (2016). ZigBee Alliance Liaisons with Thread Group on IoT Solution. Retrieved from http://www.zigbee.org/zigbee-alliance-creating-end-to-end-iot-product-development-solution-that-brings/

(A43) Lawson, S. (2015). AllJoyn IoT platform reaches out to the Internet for remote control. Retrieved from http://www.pcworld.com/article/2866252/alljoyn-iot-platform-reaches-out-to-the-internet-for-remote-control.html

(A44) Z-Wave Alliance (n.d.). About Z-Wave Technology. Retrieved from http://z-wavealliance.org/about_z-wave_technology/

(A45) IERC (2010). About IERC. Retrieved from http://www.internet-of-things-research.eu/

(A46) Farnham, K. (2015). Cellular Technologies Enabling the Internet of Things. Retrieved from http://www.infoq.com/news/2015/12/cellular-enabling-iot

(A47) Deutscher, M. (2013). Internet of Things review: Cisco's new IoT + Google Glass accessories. Retrieved from http://siliconangle.com/blog/2013/11/01/internet-of-things-review-ciscos-new-iot-google-glass-accessories/

(A48) Z-Wave Alliance (n.d.). Z-Wave Alliance Vision And Mission. Retrieved from http://z-wavealliance.org/alliance_vision_and_mission/

(A49) Savitz E. (2012). How The Internet Of Things Will Change Almost Everything. Retrieved from http://www.forbes.com/sites/ciocentral/2012/12/17/how-the-internet-of-things-will-change-almost-everything/#34e6feb056d7

(A50) Barak, S. (2012). Internet of Things accelerator launched. Retrieved from http://www.eetimes.com/document.asp?doc_id=1262722

(A51) Internet.org (n.d.). Our Mission. Retrieved from https://info.internet.org/en/mission/

(A52) Neagle, C. (2014). What to expect of Internet of Things in 2014. Retrieved from http://www.networkworld.com/article/2172913/lan-wan/what-to-expect-of-internet-of-things-in-2014.html

(A53) Gorman, M. (2014). The Internet of Things isn't safe: thousands of smart gadgets hacked to send spam and phishing emails. Retrieved from http://www.engadget.com/2014/01/17/internet-of-things-hacked-malicious-email-phishing/

(A54) Smith, J. (2014). Data Centers and the Internet of Things to Come. Retrieved from http://www.wired.com/insights/2014/03/data-centers-internet-things-come/

(A55) Couts, A. (2012). Google debuts Project Glass: Augmented reality glasses, exactly as you want them to be. Retrieved from http://www.digitaltrends.com/cool-tech/google-debuts-project-glass-augmented-reality-glasses-exactly-as-you-want-them-to-be/

(A56) Peake, G. (2015). Wireless IoT connectivity: which standards can be used? Retrieved from http://www.newelectronics.co.uk/electronics-technology/wireless-iot-connectivity-which-standards-can-be-used/74705/

(A57) European Commission (2011). Europeans making smart device communication even easier. Retrieved from http://www.ecnmag.com/news/2011/04/europeans-making-smart-device-communication-even-easier

(A58) Carter, B. (2011). 5 predictions for smarter buildings in 2012. Retrieved from http://www.zdnet.com/article/5-predictions-for-smarter-buildings-in-2012/

(A59) Malik, O. (2010). Why Internet of Things Will Change Mobile Networks. Retrieved from https://gigaom.com/2010/12/30/why-internet-of-things-will-change-mobile-networks/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+OmMalik+(GigaOM:+Tech

(A60) Sony (2002). Philips and Sony announce strategic cooperation to define next generation near field radio-frequency communications. Retrieved from http://www.sony.net/SonyInfo/News/Press_Archive/200209/02-0905E/

(A61) Shine, J. (2013). The Internet of things. Retrieved from http://www.livemint.com/Leisure/RNrcXvkTdvngAqZ7DhTFLO/The-Internet-of-things.html

(A62) Allseen Alliance (n.d.). AllJoyn® Framework. Retrieved from https://allseenalliance.org/framework

(A63) Allseen Alliance (n.d.). Documentation. Retrieved from https://allseenalliance.org/framework/documentation

(A64) Allseen Alliance (n.d.). Frequently Asked Questions. Retrieved from https://allseenalliance.org/alliance/faq#n120

(A65) Rooney, J.P. (2013). Make way for the internet of things. Retrieved from http://www.theguardian.com/media-network/media-network-blog/2013/feb/05/standards-essential-patents-internet-things

(A66) AllSeen Alliance (2013). Technology Leaders Establish the AllSeen Alliance to Advance the 'Internet of Everything'. Retrieved from https://allseenalliance.org/announcement/technology-leaders-establish-allseen-alliance-advance-internet-everything

(A67) Ramon, S. (2014). Introducing Thread: A New Wireless Networking Protocol for the Home. Retrieved from http://news.silabs.com/press-release/introducing-thread-new-wireless-networking-protocol-home

(A68) Thread (n.d.). Why we made Thread. Retrieved from http://www.threadgroup.org/About

(A69) Thread (2014). Introduction. Retrieved from http://threadgroup.org/portals/0/documents/thread_introduction_website_7-15-14.pdf

(A70) Bluetooth (n.d.). Member directory. Retrieved from https://www.bluetooth.com/membership-working-groups/member-directory

(A71) McKendrick, J. (2013). Work begins to standardize 'internet-of-things' protocol. Retrieved from http://www.zdnet.com/article/work-begins-to-standardize-internet-of-things-protocol/

(A72) Rowe, K. (2014). Internet of Things requirements and protocols. Retrieved from http://embedded-computing.com/articles/internet-things-requirements-protocols/

(A73) Randewich, N. (2014). Google's Nest launches network technology for connected home. Retrieved from http://www.reuters.com/article/us-google-nest-idUSKBN0FK0JX20140715

(A74) Xavier, J. (2014). Internet of things begins at home. Retrieved from http://upstart.bizjournals.com/news/technology/2014/04/23/internet-of-things-begins-at-home.html?page=all

(A75) Rath, J. (2014). Texas Instruments Launches Internet of Things Ecosystem. Retrieved from http://www.datacenterknowledge.com/archives/2014/04/16/texas-instruments-launches-internet-of-things-ecosystem/

(A76) Bluetooth (n.d.). Low Energy. Retrieved from https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy

(A77) Staff, G. (2014). Middleware integrates systems across cloud, Internet of Things. Retrieved from https://gcn.com/articles/2014/04/17/red-hat-enterprise-middleware.aspx

(A78) Banks, M. (2015). The 360 degree view of the Internet of Things. Retrieved from http://diginomica.com/2015/03/19/360-degree-view-internet-things/

(A79) Lohr, S. (2011).The internet gets physical. Retrieved from http://www.nytimes.com/2011/12/18/sunday-review/the-internet-gets-physical.html?_r=2

(A80) Higginbotham, S. (2011). Behind the sensor web lies a cloud. Retrieved from https://gigaom.com/2011/11/26/behind-the-sensor-web-lies-a-cloud/

(A81) Vizard, M. (2012). Unifying a Fragmented "Internet of Things". Retrieved from http://www.programmableweb.com/news/unifying-fragmented-internet-things/2012/10/09

(A82) Iot-Inc. (n.d.) A Symbiotic Partnership between Standards Bodies and Consortia. Retrieved from http://www.iot-inc.com/internet-of-things-standards-bodies-consortia-podcast/

(A83) ITU (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

(A84) Colin Johnson, R. (2012). The intangible assets of the Internet of Things. Retrieved from http://www.eetimes.com/document.asp?doc_id=1261556

(A85) Sharwood, S. (2013). Oracle reveals strategy for internet of things. Retrieved from http://www.theregister.co.uk/2013/04/08/oracle_internet_of_things_strategy/

(A86) ZigBee Alliance (n.d.). The ZigBee Alliance creates IoT standards that help Control Your World. Retrieved from http://www.zigbee.org/zigbeealliance/

(A87) Pretz, K. (2013). The Next Evolution of the Internet. Retrieved from http://theinstitute.ieee.org/technology-focus/technology-topic/the-next-evolution-of-the-internet

(A88) ZigBee Alliance (n.d.). Open standards development. Retrieved from http://www.zigbee.org/zigbeealliance/developing-standards/

(A89) NXP (n.d.). Thread Networking Protocol. Retrieved from http://www.nxp.com/pages/thread-networking-protocol:THREAD-NETWORKING-PROTOCOL

(A90) OMG (n.d.) OMG And The IIoT. Retrieved from http://www.omg.org/hot-topics/iot-standards.htm

(A91) Postscapes (n.d.). Thread Group's protocol is ready to tie connected products together. Retrieved from http://postscapes.com/thread-groups-protocol-is-ready-to-tie-connected-products-together

(A92) Murphy, C. (2012). Internet Of Things: Coming To Pool Near You? Retrieved from http://www.informationweek.com/it-leadership/internet-of-things-coming-to-pool-near-you/d/d-id/1107883

(A93) Zigbee Alliance (2016). ZigBee Alliance Creating End-to-End IoT Product Development Solution that Brings Its Industry-Leading Applications Library to Thread Group's IP Network Protocol. Retrieved from http://www.zigbee.org/zigbee-alliance-creating-end-to-end-iot-product-development-solution-that-brings/

(A94) Arduino (n.d.). Getting Started with Arduino. Retrieved from http://www.arduino.cc/en/Guide/HomePage

(A95) NFC Forum (n.d.). What is NFC? Retrieved from http://nfc-forum.org/

(A96) San Ramon, C. (2015). LoRaWAN R1.0 Open Standard Released for the IoT. Retrieved from http://www.businesswire.com/news/home/20150616006550/en/LoRaWAN-R1.0-Open-Standard-Released-IoT

(A97) Faulkner, C. (2015). What is NFC? Everything you need to know. Retrieved from http://www.techradar.com/news/phone-and-communications/what-is-nfc-and-why-is-it-in-your-phone-948410

(A98) Yoshida, J. (2015). Unleash The Power of JavaScript For IoT. Retrieved from http://www.eetimes.com/document.asp?doc_id=1325891

(A99) Vanderkay, J. (2004). Nokia, Philips And Sony Establish The Near Field Communication (NFC) Forum. Retrieved from http://nfc-forum.org/newsroom/nokia-philips-and-sony-establish-the-near-field-communication-nfc-forum/

(A100) Arduino (n.d.). What is Arduino? Retrieved from http://www.arduino.cc/en/Guide/Introduction

(A101) Harvey, C. (2014). 35 Open Source Tools for the Internet of Things. Retrieved from http://www.datamation.com/open-source/35-open-source-tools-for-the-internet-of-things-3.html

(A102) OpenRemote (n.d.). Functions & Features. Retrieved from http://www.openremote.com/functions-features/

(A103) KAA (n.d.) Kaa IoT Platform overview. Retrieved from http://www.kaaproject.org/overview/

(A104) Eclipse (n.d.). About the Eclipse Foundation. Retrieved from https://eclipse.org/org/#Unique

(A105) Eclipse (n.d.). About Us. Retrieved from http://iot.eclipse.org/working-group/

(A106) Kinoma (n.d.). Marvell Open Sources KinomaJS to Accelerate Growth of the Internet of Things Industry. Retrieved from http://kinoma.com/media/2015/opensource/

(A107) Flashrouters (n.d.). What is Wi-Fi? (ROUTER FAQ). Retrieved via http://www.flashrouters.com/blog/2015/08/07/what-is-wi-fi-router-wireless-router-faq/

(A108) Morlat, C. (2015). The History of Wi-Fi. Retrieved from http://www.ucopia.com/en/news/history-of-wifi/

(A109) The Economist (2004). A brief history of Wi-Fi. Retrieved from http://www.economist.com/node/2724397

(A110) Wi-Fi Alliance (n.d.) Organization.Retrieved from http://web.archive.org/web/20090903004711/http://www.wi-fi.org/organization.php

(A111) Stobing, C. (2016). What Does WiFi Stand For and How Does Wifi Work? Retrieved from http://www.gadgetreview.com/what-is-wifi-what-does-wifi-stand-for-how-does-it-work

(A112) Wi-Fi Alliance (2006). Wi-Fi Certified makes it Wi-Fi. Retrieved from http://www.senzafiliconsulting.com/downloads/Wi-Fi_Certified_Makes_it_Wi-Fi.pdf

(A113) Wagner, K. (2012). What is Mircast? Retrieved from http://gizmodo.com/5944578/what-is-miracast

(A114) Wi-Fi Alliance (2012). Wi-Fi Alliance® to Launch Wi-Fi CERTIFIED Miracast™ to Deliver Display Applications.Retrieved from https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-to-launch-wi-fi-certified-miracast-to-deliver-display

(A115) Griffith, E. (2009). New 'Wi-Fi Direct' Spec Revamps Device Networks. Retrieved from http://www.pcmag.com/article2/0,2817,2354201,00.asp

(A116) Foresman, C. (2009). Wi-Fi Direct protocol to ease peer-to-peer WiFi connections. Retrieved from http://arstechnica.com/gadgets/2009/10/wi-fi-direct-protocol-to-ease-peer-to-peer-wifi-connections/

(A117) Belanger, P. (2007). Retrieved from https://web.archive.org/web/20151108080354/http://www.wifiplanet.com/tutorials/article.php/3680781

(A118) Wi-Fi Alliance (n.d.). Become a member. Retrieved of http://www.wi-fi.org/become-a-member

(A119) Bluetooth (n.d.). Applying for membership in the Bluetooth SIG. Retrieved from https://www.bluetooth.com/membership-working-groups/why-how-to-become-a-member

(A120) Bluetooth (n.d.). Working groups and committees. Retrieved from https://www.bluetooth.com/membership-working-groups/working-groups/working-groups-committees

(A121) Bluetooth (n.d.). Membership types/levels. Retrieved from https://www.bluetooth.com/membership-working-groups/membership-types-levels

(A122) Bluetooth (n.d.). Qualification & lising. Retrieved from https://www.bluetooth.com/develop-with-bluetooth/qualification-listing

(A123) Bluetooth (n.d.). Bluetooth. Retrieved from https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth

(A124) Wi-Fi Alliance (n.d.). 15 years of Wi-Fi. Retrieved from http://www.wi-fi.org/discover-wi-fi/15-years-of-wi-fi

(A125) Wi-Fi Alliance (n.d.). Wi-Fi HaLow. Retrieved from http://www.wi-fi.org/discover-wi-fi/wi-fi-halow

(A126) Bluetooth (n.d.). Bluetooth core specification. Retrieved from https://www.bluetooth.com/specifications/bluetooth-core-specification

(A127) NFC Forum (n.d.). NFC Forum Technical Specifications. Retrieved from http://members.nfc-forum.org/specs/spec_list/

(A128) NFC Forum (n.d.). Officers & Board of Directors. Retrieved from http://nfc-forum.org/about-us/the-nfc-forum/officers-board-of-directors/

(A129) Bluetooth (2016). Bluetooth sig announces architecture to connect billions of devices to the iot. Retrieved from https://www.bluetooth.com/news/pressreleases/2016/02/10/bluetooth-sig-announces-architecture-to-connect-billions-of-devices-to-the-iot

(A130) ZigBee Alliance (2014). ZigBee 3.0 Creates Single Open, Global Wireless Standard for Devices. Retrieved from http://www.zigbee.org/zigbee-3-0-creates-single-open-global-wireless-standard-for-devices/

(A131) NFC Forum (n.d.). About the Internet of Things (IoT) SIG. Retrieved from http://nfc-forum.org/internet-of-things-sig/

(A132) ZigBee Alliance (n.d.). Join the ZigBee Alliance and shape the future of the Internet of Things. Retrieved from http://www.zigbee.org/zigbeealliance/join/

(A133) ZigBee Alliance (n.d.). Low-power, low-cost, low-complexity networking for the Internet of Things. Retrieved from http://www.zigbee.org/zigbee-for-developers/network-specifications/

(A134) ZigBee Alliance (n.d.). ZigBee PRO with Green Power. Retrieved from http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeepro/

(A135) Z-Wave Alliance (n.d.). Member Companies of the Z-Wave Alliance. Retrieved from http://z-wavealliance.org/z-wave_alliance_member_companies/

(A136) NFC Forum (n.d.). Simplifying IoT: Connecting, Commissioning, and Controlling with Near Field Communication (NFC). Retrieved from http://nfc-forum.org/wpcontent/uploads/2016/06/NFC_Forum_IoT_White_Paper_-v05.pdf

(A137) LoRa Alliance (n.d.). The LoRa® Alliance Launches The LoRaWAN™ Certification Program End Device Interoperability To Enable Global Scalability For The IoT. Retrieved from https://www.lora-alliance.org/kbdetail/Contenttype/ArticleDet/moduleId/583/Aid/50/PR/PR

(A138) LoRa Alliance (n.d.). LoRaWAN R1.0 Open Standard Released For The IoT. Retrieved from https://www.lora-alliance.org/kbdetail/Contenttype/ArticleDet/moduleId/583/Aid/23/PR/PR

(A139) Z-Wave Alliance (n.d.). Smart Security With Z-Wave. Retrieved from http://z-wavealliance.org/smart_security_with_z-wave/

(A140) OpenZwave (n.d.). Introduction. Retrieved from http://www.openzwave.com/

(A141) Telegesis (n.d.). ZigBee 3.0. Retrieved from http://www.telegesis.com/about-us/zigbee-3-0-creates-single-open-global-wireless-standard-for-devices/

(A142) AllSeen Alliance (n.d.). Frequently Asked Questions. Retrieved from https://allseenalliance.org/alliance/faq#n120

(A143) Bluetooth (n.d.). Bluetooth® 5 quadruples range, doubles speed, increases data broadcasting capacity by 800%. Retrieved from https://www.bluetooth.com/news/pressreleases/2016/06/16/-bluetooth5-quadruples-rangedoubles-speedincreases-data-broadcasting-capacity-by-800

(A144) Thread (n.d.). Our Members. Retrieved from http://threadgroup.org/About#OurMembers

(A145) ZigBee Alliance (2016). ZigBee Alliance Creating End-to-End IoT Product Development Solution that Brings Its Industry-Leading Applications Library to Thread Group's IP Network Protocol. Retrieved from http://www.zigbee.org/zigbee-alliance-creating-end-to-end-iot-product-development-solution-that-brings/

(A146) AB&R (2013). Understanding Bluetooth Technology. Retrieved from http://blog.abrfid.com/understanding-bluetooth-technology/

(A147) Bluetooth (n.d.). Bluetooth technology basics. Retrieved from https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics

(A148) Bluetooth (n.d.). Specification development process. Retrieved from https://www.bluetooth.com/membership-working-groups/working-groups/specification-development-process

(A149) Bluetooth (n.d.). Brand best practices & guidelines. Retrieved from https://www.bluetooth.com/marketing-branding/brand-best-practices-guidelines

(A150) Bluetooth (n.d.). Market your Bluetooth product. Retrieved from https://www.bluetooth.com/marketing-branding/market-your-bluetooth-product

(R1) International Telecommunication Union (2005). The Internet of Things. Retrieved from https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

(R2) Jakobs, K. (n.d.). Standardising the Internet of Things – What the Experts Think. Retrieved from https://www.comsys.rwth-aachen.de/fileadmin/papers/2011/2011-kai-JITSR.pdf

(R3) IERC (2015). Internet of Things – Position Paper On Standardization for IoT technologies. Retrieved from http://www.internet-of-thingsresearch.eu/pdf/IERC_Position_Paper_IoT_Standardization_Final.pdf

(R4) Rose, K., Eldridge S. and Chapin, L. (2015). The Internet of Things: An Overview. Retrieved from http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf

(R5) European Parliament (2015). The Internet of Things: Opportunities and challenges. Retrieved from http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

(R6) Reiter, G. (2014). Wireless connectivity for the Internet of Things. Retrieved from http://www.ti.com.cn/cn/lit/wp/swry010/swry010.pdf

(R7) World Economic Forum (2015). Industrial Internet of Things: Unleashing the Potential of Connected Products and Services. Retrieved from http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

(R8) Olsson, J. (2014). 6LoWPAN demystified. Retrieved from http://www.ti.com.cn/cn/lit/wp/swry013/swry013.pdf

8.4. Coding examples

Text fragment	**Code**
The point of IoT is the data points it collects and the things it can control. The more of those that come into play, the more useful it will be.	Network effect
Smart buildings can help people translate the mass amounts of data that our buildings generate, which in turn helps us more accurately understand (and mend) our energy use.	Assistance to people
The problem is, people have limited time, attention and accuracy—all of which means they are not very good at capturing data about things in the real world.	Shortcomings humans
Not all those vital data points are gettable today, and we'll spend a lot of time in the coming year looking at the limits of the Internet of things, where the shortcomings are and what emerging technology is needed to drive this trend. But it's time to have the discussions about what data is needed and what might be possible.	Needs
The biggest threat to home IoT today is the very complexity that all the current and emerging devices present to consumers, said Lee Ratliff, a low-power wireless analyst at research firm IHS Technology.	Complexity to users
The LPWA network is designed to allow long-range communications at a low data rate, from devices that require long battery life and need to be able to operator unattended for long periods of time.	Battery saving