Universiteit Leiden

ICT in Business and the Public Sector

Towards a framework for IoT mesh analysis

Name: Ashwini Gopal
Student-no: s1525670

Date: 22/01/2020

1st supervisor: Dr. G. Ramackers

2nd supervisor: Dr. W. Heijstek

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)

Leiden University

Niels Bohrweg 1

2333 CA Leiden

The Netherlands

Acknowledgements

First and foremost, the support, feedback and continuous guidance of my first supervisor, professor Dr. G. Ramackers has been essential to this research project. Without his patience and advice, the outcome of this research would not be as it stands.

I would also like to thank my second supervisor, professor Dr. W. Heijstek for his feedback on this project.

Lastly, I would also like to extend my appreciation to Capgemini and its employees, most importantly Peter Paul Tonen. They provided the primary source of information throughout this research. Peter Paul Tonen has personally provided me with individual guidance and advice whenever necessary.

Structured abstract

Objective: the primary goal of this research is to develop a rigorous framework for the qualitative analysis of essential characteristics of IoT system architectures. This framework can be used in the development of IoT systems, specifically in the requirements phase, and for the analysis of their performance. The framework includes a clustering and dependency analysis of these characteristics. It has been constructed based on literature study and qualitative research; and tested and refined in the context of a case study in an industrial setting. In addition, an initial effort has been made to describe an analytical descriptive model for IoT architectures, and potential qualitative analysis techniques for the evaluation of several computational properties of such networks, such as latency, cost and power consumption.

Methods: core IoT characteristics were identified using literature study and further expanded upon with expert interviews. Interviewees are business and/ or (IoT-)networking professionals working at one of the largest IT-Business consultancy firms.

Results: 16 IoT characteristics (CSF) have been identified throughout the research project. Based on these characteristics, a qualitative analysis has been done on Capgemini's SmartOffice project. Furthermore, a graph theory-based network description of IoT systems is given, usable for network analysis. The relevance of the identified characteristics is linked to the network description, characteristics are defined as attributes of network elements (nodes, connections or the full system). Lastly, first steps are made towards the use of the framework as tool towards quantitative analysis.

Discussion: research is always affected internal and external forces. These affect the results and findings. These acting forces and their influence are discussed in this chapter. Most prominently, the collaboration with Capgemini for the creation of this research has had its effect on the project.

Conclusion: the research paper is concluded with a summary and discussion of the most important findings. Furthermore, future research recommendations are suggested as to how other researchers can expand on the findings in this paper.

List of terms

Internet of Things: the Internet of Things describes an interconnected network of sensors, actuators, or general information sensing equipment, which on a continuous basis generate, aggregate, communicate and analyze data for the advancement of processes.

Core characteristic: describes an attribute or characteristic feature of IoT mesh networks. It can be argued that the so-called core characteristics exert large influence on the operational behavior of an IoT network.

Star topology: a framework in which IoT sensory nodes are directly and solely connected to a gateway. Information is exchanged in a single direction, from sensory node to gateway.

Fully connected mesh: a mesh network describes a network topology in which sensory nodes are interconnected instead of directly connected to gateways. Data is routed to gateways through nodes in the mesh networking using multi-hop routing.

Dynamic/ partially connected mesh: dynamic mesh describes a specific type of mesh network. One in which sensory nodes do not necessarily provide data relay functionality. Sensory nodes can be either data relaying, or not.

LoRa: short for *"Long Rang"*, is a long-range wireless communication protocol. LoRa based IoT solutions are characterized as being long-range operated and low in power consumption.

IEEE 802.15.4: describes a technical standard for LR-WPANs, maintained by the IEEE 802.15 group. The standard forms a basis for several wireless communication technologies, among the one discussed in this paper; Zigbee.

Multi-hop: a data communication method used to forward and share information in mesh systems. Information is shared by routing data between nodes (and gateways). The sharing of data between nodes is called a "hop". Multi-hop describes a network where data is routed and shared using node hops.

Abbreviations

IoT: Internet of Things

NFC: Near Field Communication

RFID: Remote Frequency Identification

RF: Remote Frequency

IEEE: Institute of Electrical and Electronics Engineers

GDPR: General Data Protection Regulation

WMS: Wireless Mesh Solution

CRES: Capgemini Real Estate Services

MoSCoW: Acronym for a prioritization technique; must have, should have, could have, won't have.

CSF: Critical Success Factors

List of tables

List of figures

Table of content

1. Research Objectives and Breakdown

This introductory chapter of the thesis will introduce the research area and give a breakdown of what will be discussed in this paper. Besides this, research ethics are also discussed in this chapter. First, the background and relevance of the research subject will be discussed. Afterwards the aim and scope of the project will be discussed. Lastly, a small description of the following chapters is given.

1.1 Research background

The Internet of Things (IoT) has seen wide adoption over the last decade (Baker, Xiang, & Atkinson, 2017). Implementations of various forms of IoT enabled technology can be found in both business and governmental, and home environments. Business and governmental applications can range from office space monitoring and asset tracking, to continuous supply chain monitoring (Turcu & Turcu, 2013). At home applications often come in the form of home automatization or smart home applications, here IoT applications are more limited in. Continuous data collection on the scale provided by the Internet of Things is something that did previously not exist. Data provided from IoT applications offer improved insights to various business operations which in turn can result in improved e.g. operational efficiencies, reduction of financial expenses and improved waste management.

Internet of Things is a umbrella term which describes the concept of a variety of *things* such as sensors, actuators, mobile phones, RFID tags and other information sensing equipment, which are able to interact with one another through internet gateways to accomplish common goals (Atzori, Iera, & Morabito, 2010). By having continuous internet connectivity, IoT enabled devices allow convenient monitoring, identification, and collection of data (YE, Zhu, Wang, Malekian, & Qiao-min, 2014). If correctly aggregated and analyzed, this sensory data can provide useful insights as previously described (Uckelmann, Harrison, & Michahelles, 2011).

Current implementations frameworks often utilized for the realization of IoT projects revolve around the *star topology*. This topology describes a framework in which IoT enabled sensory nodes are directly connected to a gateway. An IoT gateway serves as a control point for IoT enabled controllers, sensors and other information sensing equipment. The gateway provides a place to temporarily store and processes sensory information before this is stored locally or on the cloud. Every sensory node in this network has a single point of connection, this to the gateway. This design framework is relatively straight forward to implement and manage as al collected data is directly forwarded, analyzed and aggregated at a predetermined point of control. This implementation framework, however, comes with several drawbacks. A single connection from sensory node to gateway results in a framework with a single point of failure. Secondly, each gateway can physically connect to a limited number of sensory nodes, besides this a gateway's can only operate in a fixed operating area. This creates the second flaw; this framework has limited scalability. Besides these points, this topology, offers limited support for core IoT characteristics. Attributes such as scalability, interoperability, and fault tolerance have found little support in a star topology implementation.

This IoT implementation framework leaves a lot to be desired. An alternative framework for the realization of IoT projects, *the mesh network*, addresses different characteristics compared to the star topology. This framework offers increased support for characteristics such as scalability, interoperability and fault tolerance, however, this at the cost of other attributes. This proposed research project will analyze the potential of mesh networks according to a set of key IoT characteristics. More in-depth information of how this project will be constructed can be found in the next sections.

1.2 Research objective

The primary goal of this research paper is to develop a rigorous framework for the qualitative analysis IoT mesh networks using essential characteristics. Characteristics will be identified using primary and secondary research methodologies. The framework will be a tool which can be used during the development phase of IoT project as a type of checklist, or, as an analysis tool for readily established networks.

1.3 Research question

In the duration of this research project a framework for IoT mesh analysis will be created. Its purpose being the simplification of development and analysis of mesh networks both before and after network deployment. The goal of this framework is furthermore to stimulate and simplify the use of mesh as IoT network solution for businesses and consultancy firms. Based on this, the following research question is created to guide the project:

How can a framework for IoT mesh network analysis be created based on CSF in order to simplify development and use of mesh systems?

1.4 Methodology

Data collection will be conducted using primary and secondary qualitative data collection methods. The objective of this research is to gain a deeper understanding of mesh networks for IoT applications, define core IoT characteristics, and analyze real-word applications. Qualitative data collection will allow me to acquire extensive knowledge in the above specified areas. Based on this, the following qualitative data collection methods have been decided upon:

1. **Literature review**: since a literature review is an integral part of every research project, this is not necessarily considered to be a research method. Literature review will be conducted to gain an understanding of the research area, previous work, relevance of the research subject, and will serve as basis for research to be conducted

in this research paper. The initial set of core characteristics will be identified by literature study.

2. **Expert interview**: interviews will be conducted with IoT network architects and consultant. The key of these interviews will be to identify among other things key IoT characteristics, consideration when designing a mesh solution, difficulties experienced with implementations, customer expectations/ requirements, current network analysis methods, and frameworks utilized.

   The interviews will be semi-structured. Consisting of a set of pre-determined questions, whilst also allowing room to deviate. This interview method allows me to acquire in-depth knowledge, experiences and opinions required from the participating interviewees. Besides this, a semi-structured interview leaves room to explorer other related research areas.

3. **Case study**: the list of characteristics identified during research will be used to analyze a large IoT undertaking. This case study example is part of a development at Capgemini. For each characteristic, if relevant, its relation to the project will be discussed.

In-depth specifications of these research methodologies are discussed in the chapter *"Research Design"*.

1.4.1 Ethical considerations

This project will be conducted under the guidance of Capgemini's Applied Innovation Exchange; besides this, expert interview participants and case study subjects will come from the Capgemini Group. Ethical considerations must be taken into account to protect the Capgemini Group and its employees.

When approaching individuals for any research related purpose, the following considerations will be taken into account (Bryman & Bell, 2007):

- Participation in the research project, or part thereof, is strictly voluntary. Participants shall not be forced, guilted or misled to participate in this research project, or disclose confidential information.
- Confidentiality of information and anonymity of individuals will be respected and preserved if requested.
- If an interview is to be recorded or documented otherwise, consent will be a prerequisite.
- All communication regarding the research project will be done with full transparency.

- If requested, a participant can withdraw his or her invitation at any time, no questions asked. If a participant would like to withdraw during an interview, same rule applies.

1.5 Thesis outline

This paper is divided into eight chapters, each with multiple sections and sub-sections. This first chapter serves as an introduction to the project, it describes the research background, research question and purpose of the research project.

Chapter 2 covers the research's theoretical foundation. This chapter introduces IoT concepts, definitions, and covers the initial list of core characteristics derived from literature review.

Chapter 3 describes the research methodologies. This chapter describes how research is conducted, which methods are used, why these are decided upon in particular, and how data will be analyzed.

Chapter 4 discusses Capgemini's newest and largest IoT undertaking, its *SmartOffice* project. The project details and outline are described and an analysis according to the identified characteristics is made.

Chapter 5 describes the interviews and interview analysis.

Chapter 6 describes the process and decisions made during the creation of a network description and describes the first steps towards a quantitative framework.

Chapter 7 discusses the choices made during the research project and their respective effects on the findings.

Chapter 8 concludes the research paper, giving a short summation of the findings.

2. Literature study

A literature study has been conducted to get an initial understanding of the background, concepts, history, uses, definition, and the key architectural elements and characteristics of an IoT network. Mesh is an umbrella term, describing a set of technologies in which nodes directly communicate information. With an understanding of the critical networking concepts, a further exploration of the types of mesh networks can be given.

2.1 Concept

First coined in 1999 by a member of the development team of Radio Frequency Identification (RFID), the term Internet of Things has recently become increasingly popular as a result of the rapid growth of mobile devices, sensors, and generally internet connected *things*. The concept of the Internet of Things revolves around the idea of a variety of internet connected objects such as RFID-tags, sensors, actuators, cameras, mobile phones etc. which interact with one another to achieve common goals, becoming an integral part of the internet. This group of internet-connected devices (forward on referred to as *"sensory nodes"*) can be embedded seamlessly in the environment around us.

Currently various smart devices are already connected to the internet. These can be things such as smartphones, home appliances and computers. However, enabling a wide variety of devices, which would previously not be internet connect, to be connected to the internet makes IoT unique and interesting. Connected devices can come in all shapes and sizes, toys, medical equipment, vehicles, home appliances, wearables, people, and building are a few examples of what this technology enables. The resulting networks will continuously amass information. Information which needs to be aggregated, analyzed and stored (Gubbi, Buyya, Marusic, & Palaniswamia, 2013). The Internet of Things will foster new developments as a result of this newly generated data. New services, or improvements to services based on data results can be provided to, among others, companies, citizens, and governmental institutions.

For successful deployment of IoT, it must work seamlessly with existing networks such as 4G, Bluetooth, and Wi-Fi. However, IoT applications must also provide support for objects usually not connected to the internet. IoT benefits can be found in the connectivity of everyday existing objects, beyond smartphones and readily connected devices (Draves, Padhye, & Zill, 2004). Benefits of IoT can be found in market segments such businesses, personal/ individual use, and healthcare.

From a business perspective, these benefits can be found in fields such as operations, automations, industrial manufacturing, logistics and supply chain management (Hunke, et al., 2017). With proper implementation in business environments, IoT could result in financial gains, decrease in expenses, increased organizational productivity, and customer experience and product improvement.

In the personal sphere, applications can be found in segments such as smart homes, home automation, smart vehicles, and wearables. These applications offer less benefits as a result of data collection but offer benefit in the form of convenience, ease of use and monitoring and/ or surveillance tool (Strengers & Nicholls, 2017).

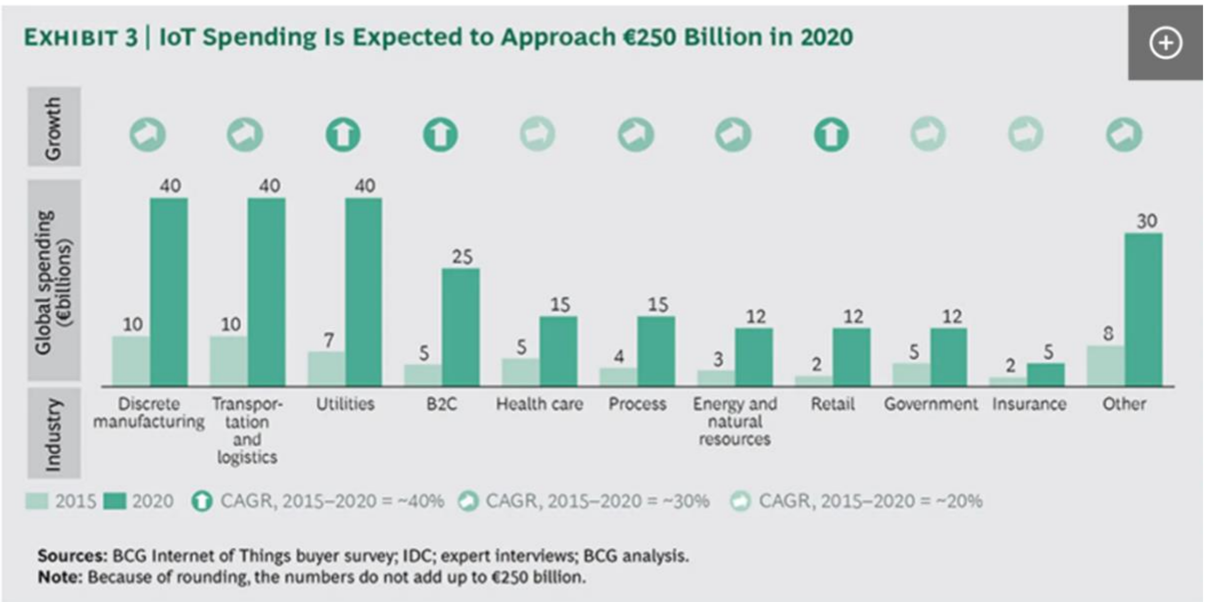

Figure 1: IoT in industries (Hunke, et al., 2017)

The healthcare sector, lastly, is a highly complex environment. The aging population is but one of many factors exerting pressure in this field. The demand for physical resources and knowledge is extremely high. IoT can offers solutions to alleviate the pressure in this industry (Baker, Xiang, & Atkinson, 2017). Applications in this field currently focus on continuous health care monitoring and remote monitoring. Patients can be actively monitored at home, reducing strain on the limited resources available in hospitals.

These are just several examples of fields which are innovated by the Internet of Things applications.

2.2 Definitions

Since this research will discuss IoT concepts in depth, it is necessary to have a common definition of this term to be used in this paper. However, a single unique unified definition of the Internet of Things does not exist. There are many groups of expert individuals and corporate organizations who have defined the term (Madakam, Ramaswamy, & Tripathi, 2015).

(Internet Society, 2015) defines the Internet of Things as a construct in which otherwise traditional objects and sensors are network connected and able to generate, communicate and analyze data with minimal (or without) human intervention.

(Xu, He, & Li, 2014), Xu being a senior member of the Institute of Electrical and Electronics Engineers (IEEE), an organization whose mission it is to advance technology for the benefit of humanity, has defined IoT as: a global network with self-configuring capabilities based on standard communication protocols, where *things* have identities, physical attributes, and are integrated into an information framework.

These definitions offered by different researchers clearly shows overlap in the general sense of what IoT encompasses. However, the level of detail used in each definition differs. This is most often the case when defining IoT. In order to have a general definition throughout this paper, a definition will be created which encompasses the most important characteristics of this technology. Since IoT in this paper solely looks at applications which could provide business value, the proposed definition will reflect this:

The Internet of Things describes an interconnected network of sensors, actuators, or general information sensing equipment, which on a continuous basis generate, aggregate, communicate and analyze data for the advancement of processes.

2.3 Core system characteristics

This section defined the initial core characteristics as derived from literature review. This serves a starting point towards defining the scope of characteristics to be used during this project. It is important to note that not all characteristics on this list might be included in the final model. Besides, characteristics not on this list could be in the final model, these have a basis in the knowledge extracted during research execution.

As previously mentioned, in literature, a lot of IoT architectures have been developed and suggested. However, each of the proposed architectures comes with drawbacks in one or more of the essential IoT characteristics. Support for the essential characteristics required for project success are often insufficient. In order to properly analyze properties of Internet of Things networks, an understanding of these characteristics, and formal definitions is needed.

IoT characteristics have been defined by (Abdmeziem, Tandjaoui, & Romdhani, 2016). Besides these defined characteristics, the list below, also describes architectural and functional requirements of an IoT network. This list is relevant for all IoT implementation types.

1. **Distributivity**: an IoT application will most likely be a distributed network, consisting of various sensors collecting a multitude of different data points, and type of data points. Not only can data be gathered in a distributed manner, but processing of collected data could also be performed by distributed systems.

2. **Interoperability and interconnectivity**: information sensing equipment come in a variety of forms; these sensory nodes collect different types of information, are created by different manufacturers, and are often designed to use different communication and data exchange protocols. Sensory nodes in an IoT network must be able to communicate with a gateway, and in some cases be able to communicate with one another.

3. **Scalability**: scalability of an IoT network describes its capability to adapt to a changing environment and meet the changing needs in the future (Gupta, Christie, & Manjula, 2017). A scalable system allows us to better address problems and needs as they arise; and makes effective use of its system resources. This characteristic is especially important in operating environments containing a continuous changing number of sensory nodes.

4. **Safety and security**: security plays a critical role in the development of any IoT application. Different methods can be used to secure a network: security by design, control network access and routing updates are among a few. Security is required to guarantee the integrity of a system.

5. **Latency**: in IoT networks, latency describes the time between data collection by the sensory node and data aggregation, processing, and storage by the gateway. Applications such as real time monitoring systems require a network which supports low-latency communication. If latency is not a deciding factor for a network, solutions which include cloud computing for example could be an attractive paradigm (Want, Schilit, & Jenson, 2015). Latency is a core element in the design of a network, this cannot (or hardly) be changed afterwards.

6. **Throughput**: throughput describes the maximum rate data can be shared, analyzed or stored in a or across a network. In an IoT network, data packages are continuously shared between sensory nodes and a gateway. In the context of IoT networks, we will refer to throughput with the maximum amount of data packages (size-wise) which can be shared across sensory nodes, and between sensory nodes and a gateway.

7. **Number of hops**: the number of *"hops"* (changes in sensory relay node) a data package must make between interconnected sensory nodes before reaching its destination, often a gateway. The number of hops in any given system is depending on the level of interconnectivity, number of data relaying nodes in the network, and data routing protocol used (Draves, Padhye, & Zill, 2004).

8. **Fault tolerance/ robustness**: IoT enabled sensors are susceptible to attacks and misuse. These irregularities will affect the operation of the individual sensor in a network, and the network as a whole. Fault tolerance is a measurement of a system's rigidity in the event of (partial) system failure.

   (Roman, Najera, & Lopez) have described a three-step process to increase fault tolerance in Internet of Things applications. The fault tolerance metric will be a measurement based on successful application of the specified three-step process;

1. **Security by design**: protocols, mechanisms and software implementation should be designed and implemented in a secure manner. Emphasizing software implementation, since it might not be possible to deploy software updates to thousands of devices.
2. **Continuous monitoring**: a monitoring mechanism should be in place which can detect and respond to abnormal situations. This system should operate network-wide.
3. **Sensor level protection**: sensory nodes should be able to defend themselves in the event of network failure or external attacks. If a node should also be able to degrade its service to the network in the event it is compromised.

9. **Range**: the area of operation of an IoT network is dependent on the network's purpose and capabilities. In a small operating area, sensory nodes can more easily communicate with a gateway (without the need of intermediaries). If sensory nodes are spread out, data relays might be necessary. In a mesh network, range can also refer to the area of communication between sensory nodes (with data relay capabilities).

10. **Power consumption**: dependent on the implementation and purpose of a proposed IoT network, power consumption can differ. Importance is often put on the use of low power wireless networks such as Zigbee, low power Wi-Fi, and LPWA (Mahmoud & Mohamad, 2016). Especially for networks which utilize fully wireless sensory nodes, battery power consumption plays a vital role. Systems in which sensory nodes are continuously powered, power consumption is of lesser importance.

11. **Cost**: the estimated sum of money required to create and maintain an IoT implementation. Costs include hardware, software, infrastructure, architectural design, and certifications: (Klubnikin, 2016)

    - **Hardware**: can consist of analysis and optimization based on functional requirements of the system. Modelling, prototyping and production of custom physical equipment. Cost of hardware is highly dependent on the purpose and complexity of the IoT network.

    - **Infrastructure**: infrastructural requirements such as a scalable and low-latency Wi-Fi network. If required middleware, a software functionality connecting sensory nodes which usually communicate using different communication protocols. Almost all IoT networks also utilize some form of data storage, this can be either a local datacenter, or a cloud solution.

- **Application and software**: software purchase or development costs inquired, required for the day-to-day operations of the IoT network. Applications allow end users to operate, communicate, and monitor the operations of the IoT network. Costs of software and application is highly dependent on the purpose and complexity of the IoT network.

12. **Communication protocols**: protocols describe the method information in an IoT network is exchanged. Different sensory nodes on a network use a different set of protocols and standards. Low power, close range communication protocols often used are NFC and RFID. For medium range, Bluetooth, Wi-Fi and RF methods such as Zigbee are often utilized (Sethi & Sarangi, 2017). Even though different communication protocols are utilized, communication between sensory nodes and gateways is necessary.

13. **Routing algorithm**: the routing algorithm manages how data is routed and communicated throughput the mesh network. Routing algorithms can differ in the purpose they serve for a network: optimal path creation, shortest path, longest path, path with least number of hops, etc. Several routing algorithms exist which can be used to create paths in a mesh network: Dijkstra's shortest path algorithm, Bellman – Ford algorithm, Floyd – Warshall algorithm, and the A* search algorithms are but a few that exist.

14. GDPR compliance: short for General Data Protection Regulation, is a set of regulations aimed at data and privacy protection for EU citizens. The GDPR gives individuals control over their personal data. All organizations using some form of personal or identifiable information must comply with GDPR regulations. For certain use cases, IoT networks must comply with these regulations. Personal data aggregated from IoT services such as smart homes and asset tracking must be treated in accordance with GDPR regulations. Individuals holds, among other rights, the right to access their personal data, view how it's process, request removal of data and deny access to processing of data (GDPR EU, 2019).

If GDPR regulations are violated, the organization might be susceptible to fines. Depending on the infringement, fines can be; a fine up to 10 million USD or 2% of the organization's revenue for less severe infringements, or a fine up to 20 million USD or 4% of the organization's revenue for more serious infringements. It is fair to conclude that GDPR compliance is of high importance for networks operational in the EU.

14. **Retrofit**: the ability of a network to be implemented in a readily established environment. Can a network be easily implemented alongside what already exists, or

do significant changes have to be made to support the IoT network? (interview H. Scholten)

15. **Technology qualification**: has a technology been around long enough to be developed upon? Has enough research gone into the technology? Are there other projects and/ or industries which have successfully deployed this technology? Maturity is a general estimation whether the technology has been explored and developed enough to be practical (H. Scholten).

This list of 16 characteristics describe the architectural, design and technological features of an IoT network implementation. When one of these characteristics is mentioned throughout this paper, its use refers to the description/ definition in this chapter.

2.4 Architecture

Besides the previously described characteristics, an IoT implementation is also highly dependent on its architectural makeup. An architecture describes the technical build of an IoT implementation. An IoT architecture can be divided into different layers. Like definition of the term IoT, there is no single architectural definition for the Internet of Things. Different researchers have proposed different architectures. Depending on the source material, the number of layers in an architecture can differ. However, the functions required to implement an IoT solution are all present in most architectural descriptions. In this study we will use the 3-layered architectural description given by (Patel & Patel, 2016) and (Sethi & Sarangi, 2017) to describe the architecture of the to be discussed frameworks.

(1) **Device/ perception layer**: the perception layer consists of physical information sensing equipment. These sensory nodes serve as a connection point between the physical and digital world. Real-time environmental information is collected in the perception layer.

(2) **Network/ management service layer**: the network layer connects sensory nodes, network devices, storage mediums, and other smart objects. Besides this, this layer also monitors, processes and analyzes data collected by the perception layer. Functionalities such as data privatization/ anonymization, data integration, and data synchronization can also be found in this layer. These functions ensure that only relevant data is provided to applications.

(3) **Application layer**: the application layer covers the real-world applications provided by the implementation of an IoT solution. Applications can be found in smart homes, smart cities, supply chain management, process monitoring, and healthcare.

An architecture should provide a design which is scalable, dynamic and secure.

2.5 Mesh implementations

Several implementation frameworks for mesh networks exist. Discussing all of these would be impossible, therefore I have selected mesh solutions to discuss based on their relevance in the market, and differences in protocols among them. Based on the performed literature review into the background, characteristics and architecture of this technology, these example networks should help illustrate how theory relates to real-world network implementations.

2.5.1 Zigbee

Zigbee is a RF based communication protocol based on the IEEE 802.15.4 standard (Soliman, Abiodun, Hamouda, Zhou, & Lung, 2013). IEEE 802.15.4 defines standards for low rate, low power consumption devices which operate in a small operating space (usually smaller than 10m) (Lee, Su, & Shen, 2007). Zigbee provides a self-controlled network with reliable mesh networking and low power consumption. Three types of unique devices can be identified in a Zigbee network (Muthu Ramya, Shanmugaraj, & Prabakaran, 2011):

(1) **Zigbee coordinator**: a single coordinator is present in all Zigbee networks, it forms the starting point of the network. The coordinator is responsible for controlling and managing nodes in the system and dataflow between nodes. Communication between nodes in also controlled by the coordinator.

(2) **Zigbee router**: a router performs exactly the operation its name suggests; it routes data from other devices in Zigbee system. A router can receive and send messages from other nodes, this is done through multi-hops. The router itself does not generate new data or modify incoming data. An existing network's range may be expanded using routers.

(3) **Zigbee end device**: end devices are data collecting nodes in the Zigbee network. These devices can be low energy using, battery powered devices. Communication with these devices is performed through routers or coordinators. End devices can not directly communicate amongst themselves, or relay data from other end devices. Depending on the end device functionality, it does not have to stay operational at all times. The coordinator and router, however, perform their respective functionality continuously.

A Zigbee network consists of a single Zigbee coordinator and several Zigbee routers and end devices. The Zigbee controller is responsible for controlling and managing nodes in the system and dataflow between nodes. Communication in a Zigbee system is controlled by the Zigbee controller. The following characteristics, as part of the constructed list, are defining for Zigbee systems:

- Scalability: a Zigbee uses mesh, mesh is inherently characterized as a scalable architecture.
- Self-healing: not part of the list of characteristics, this characteristic is unique to Zigbee mesh systems. It is defining of Zigbee systems therefor included in this list.
- Retrofit (ease of deployment): Zigbee systems can easily be deployed in existing infrastructures and locations.
- Power consumption: end nodes are characterized with a *very* long battery life.
- Safety and security: Zigbee's underlying infrastructure accommodates safe and secure operation.

- Cost (low cost): hardware, deployment and maintenance cost of Zigbee systems are lower compared to alternatives.

These are just a few examples of why Zigbee systems are often used to implement a mesh system for IoT.

2.5.2 Wi-Fi Mesh networking

Wi-Fi based on Wireless LAN, further referred to as Wireless Mesh Solutions (WMS) is another desirable implementation of mesh networking for IoT applications. WMS offers significantly greater support for high data rates relative to other mesh solutions (> 50 Mbps for IEEE 802.11a, g). WMS often consist of a combination of stationary and/ or mobile nodes. A system has one or more gateways, each can be connected to multiple relay nodes. The gateways serve as points of control, connecting the network to other systems. Whereas the relay nodes expand a network's coverage (Sichitiu, 2019).

Like Zigbee, data is communicated throughout the network using multi-hops.

WMS are often utilized for wide-scale implementation of broadband internet access. In this field, WMS offers considerable advantages:

- **Cost** (relatively small up-front cost): a WMS is usable right when it is deployed, with or without other nodes in the system. This bare-bone WMS, however, provides all the functionality of the system. Therefore, a simple system can easily be implemented and expanded upon to serve the needs of customers.

- **Scalability**: as with other mesh solutions, scalability is a key characteristic for these implementations. WMSs offer great support for scalability, in part due to multi-hop routing. Besides this, WMS makes use of robust communication protocols. Physical obstructions such as walls, trees, and buildings do not significantly impact a node's coverage.

- **Robustness** (reliability): mesh networks if correctly designed, eliminate the single point of failure problem. This can often be a critical problem of other implementation topologies. With a responsive routing algorithm, the WMS mesh network is able to adapt and re-route data in the case of node failure. In multi-gateway systems, the network is also able to re-route data from nodes to alternative operational gateways.

3. Research Design

With an understanding of the current operating environment of IoT mesh networks, and a list of initial core characteristics, new research can be conducted. This chapter will present an extensive description of which research methods will be used in this research project and will discuss how research will be performed. The next chapter will analyze and discuss the results.

3.1 Methodologies

With an understanding of the research area, the definition of mesh systems, and a list of characteristics research can be conducted. The list of core characteristics defined during literature review serves as the core for the research to be discussed in this chapter.

For each research method, the process and train of thought will be discussed in-depth in the next sections.

3.2 Preliminary research

Preliminary research was conducted in the form of a literature study. As mentioned previously, the literature study was conducted to get an understanding of the research area, previous research, and to define a set of term and characteristics to be used as a basis for the project. In order to perform a proper literature study, *The General Procedure for Conducting Literature Reviews* as defined by (Templier & Paré, 2015) has been executed:

1. **Formulating the problem**: justify the need of the literature review (formulate the problem) and define objectives for the review.
2. **Searching the literature**: identify relevant studies, papers, articles, and other information sources.
3. **Screening for inclusion**: screen previously identified information sources either select or reject these sources based on their relevance to the study.
4. **Assessing quality**: access the quality of research conducted in each information source. Determine whether the methodology was properly defined, executed and analyzed. Based on this, again either select or reject sources.
5. **Extracting data**: extract relevant data from each information source for the literature study.
6. **Analyzing and synthesizing data**: extract, aggregate, compare and analyze results from all information sources in a meaningful way in order to contribute to existing knowledge.

Besides using elements from (Templier & Paré, 2015), elements described by (Webster & Watson, 2002) have also been used during research. Like the framework described above, (Webster & Watson, 2002) have defined methods to properly conduct a literature review. These two methods complement each other, (Webster & Watson, 2002) discusses a relevant considerations to be made when conducting a literature review, not present in the previous framework.

- **Tone**: conduct an informative literature review. Respect others work, however, always be critical towards papers, reports, journals and other information sources. One cannot blindly cite others' work.

Information sources used in the literature review were gathered from a number of sources: general web searches, Google Scholar, and the University Library. Identification of potential papers was done through keyword searches: *Internet of Things mesh description, mesh networks, general mesh, IoT Architecture, etc.* This identification method yielded many search results. Articles were selected based on date of publication (articles published recently most likely contain more relevant and up to data information), number of citations, and order of suggestion by the search engine. Further selection and rejection of information sources was done by reading the abstract and conclusion, scanning the paper, and finally reading (relevant parts of) the paper.

3.3 Primary research

With a solid basis in preliminary research, the next logical step is the design of the research method. Data collection will be conducted using primary and secondary qualitative data collection methods. The objective of this research is to gain a deeper understanding of mesh networks for IoT applications, define core IoT characteristics, analyze these through a real-word application and create a framework for analysis. Qualitative data collection will allow me to acquire extensive knowledge the above specified areas.

Two qualitative collection methods are deployed during this project: interviews and case study. Both are discussed in detail in the next sections.

3.4 Expert interviews

The objective of the primary research method used is to refine the list of IoT core characteristics, identify new insights on IoT, more specifically mesh networks and mesh implementations, and acquire a use case example of a mesh network implementations. Based on these objectives, expert interviews would yield the best results. Interviews allow for qualitative data collection, a method where in-depth knowledge can be extracted from each participant. Besides this, interviews also allow participants to share their stories, experiences and feelings on different subject. The results produced by proper execution of this method fit perfectly with the objectives of the primary research. Other data collection methods such as questionnaires, focus groups, and observation, would produce results that would offer a lesser objective – solution fit.

The aim of the interviews can be divided into two parts, first the refinement and identification of core characteristics and identification of use case examples, second, the identification of the unknown. Based on these two objectives of the interview, a semi-structured method would work best.

The semi-structured interview topology is a middle ground between the structured interview and open interview. Similar to structured interviews, a semi-structured interview has a set of predefined questions which need to be answered/ addressed. Besides this list of question, the semi-structured nature of the interview allows for deviations in order to explorer interesting ideas and topics.

3.4.1 Participant selection

Two predetermined types of results need to be acquired from the interviews. First, refinement and further identification of characteristics, second the identification of use cases of IoT mesh networks. Therefore, interview participants must have extensive knowledge in at least one of the specified areas. All interview participants are professional experts in the field of Business, Innovation, and/ or IoT. Since this thesis is written as part of an internship at Capgemini, the researcher has access to experts with extensive knowledge on these subjects within the organization. The potential interviewees are therefore part of the Capgemini Group.

The list of core characteristics defined by literature review can be divided in two parts, characteristics relevant to the end user, and characteristics relevant to a system architect or developer. Characteristics such as latency and throughput are important for an end user, the number of hops a data package size is not. These characteristics, however, are important when designing an architecture. In order to correctly identify the relevant core characteristics to use for this research project, it is important to conduct interviews with both network architects/ developers and end users, or requirements analyst.

Table 1 contains a list of participants interviewed, their occupation at the time of interview, and subject they are interviewed on. The list of participants consists of both experts on the developer side, those who design and develop an implementation, and expert analysists who specify client requirements. This results in a mix of different perspectives which allows a clear understanding of which characteristics are of importance and to whom.

ID	Name	Years of experience	Occupation/ expertise	Scope
1.	Hans Scholten	23+ years	Group VP	Client
2.	Marco van der Pal	20+ years	Managing consultant	Developer
3.	Andres Smithuis	4+ years	Senior Embedded Software Engineer	Developer

Table 1: Interview participants

Initial interview participants were suggested by the director of Capgemini's Applied Innovation Exchange. Besides these initial participants, other participants were selected based on recommendations of interviewees or background reviews of Capgemini employees in relevant positions. All participants were contacted first by email, the format of the mail send can be found in *Appendix A – Interview email*. This email describes my background, the research project, purpose of research, what I need from each participant, and length of the interview (roughly one hour). Each mail ends with a request for action of the participant:

- If the participant is not able to participate, or would not like to participate in the interview, a confirmation of this is requested by response on the initial email.
- If the participant can participate in the interview, a confirmation of this is requested. The participant is also able to specify the date and time of the interview in this case.
- If any part of the email was unclear, the participant can request to inquire more information on this.

A possible participant is given a full week (7 days) to respond to the email. If no response is received after this period, a second reminder mail will be sent to the participant. This mail will clearly indicate that it is a reminder. The request for action will also be stated at the start of the mail, in addition to the end. If no response is received after the reminder email, no further requests will be sent. At this point, the assumption will be made that the potential participant is not able/ does not want to participate in the interview.

If a participant decides to participate in the interview, a date on which both parties are available is set. With this rule, a participant was given the choice to pick a date and time of his/ her choosing. If a time period has been decided upon, the participant will be sent a reminder a day in advance to the interview. If at this point, the participant is no longer available, the interview will be rescheduled, or cancelled.

3.4.2 Interview structure

The semi-structured nature of the interviews allows the researcher to be very flexible the manner the interviews are started and conducted. Depending on the expertise and background of the interviewee, the introduction can differ slightly. In general, the introduction will cover a short description of my educational background, the research concepts, reason for research, and previous findings relevant to the interview. The introduction introduces the basis on which the interview will be based on, a good introduction is therefore essential to conduct a proper interview. Once all concepts are introduced, the interview will naturally follow.

Depending on the background of the interviewee, the questions asked might differ slightly. When interviewing a requirements analyst for example, technical questions are not part of his/ her expertise and can therefore be considered unnecessary for the interview. This section covers only the essential questions which are discussed during an interview. Introduction, names, years of experience and other "*general questions*" are not included in this section, since it is assumed that it is common understanding that these will be inquired about.

The interviews will cover, but not be limited to the following questions, or variations thereof:

1. What is your professional background; what is the current position you hold at Capgemini?
2. How experienced are you with the Internet of Things?
3. How often have you worked on IoT projects that use some form of mesh, or looked at mesh as a possible solution?
4. Are there any characteristics you would leave out? Or are there any characteristics that you would like to add to this list?
5. From a client perspective, what characteristics would be most important? Or how does importance on these characteristics differ depending on the use-case?
6. How would you define a successful mesh solution (either as client or developer)?
7. What is in your opinion the difference between a good/ successful and a less successful mesh implementation? Why is that?

Since the interview will be semi-structured, questions will follow from answers given by the interviewee. The list of questions above serves as a guideline of what will be discussed in the interview. The full set of questions created can be found in *Appendix B – Interview questions.*

3.4.3 Analysis

Since the interviews will be semi-structured, there will be a baseline of questions asked to all interviewees. This creates a set of themes which will be present in all interviews. New insights could be extracted by analyzing the different views across these themes and interviewees. In order to achieve this, a qualitative analysis method capable of finding pattern across all interviews is required.

Phase		Tasks/ process	Result
1.	Familiarize with data	Transcribe interview (if necessary), read and re-read data, noting down initial ideas.	Initial notes and coding concepts
2.	Initial coding	Coding interesting features based on where they appear and what they describe, data collating.	Comprehensive code
3.	Searching for themes	Collating codes into potential themes, gathering other relevant pieces of data for each theme.	List of themes based on collated codes
4.	Reviewing themes	Check how identified themes fit with theoretical perspective and codes. If there are gaps in the themes, go back to the previous phases.	Understanding of how themes are related, and the story they tell
5.	Defining and naming themes	Define and name each theme, clearly specify what makes each theme interesting and relevant.	Analysis of relevant themes
6.	Reporting	Selection of extract examples from data, relating them back to literature. Producing a scholarly report.	Description of data

Table 2: Thematic analysis phases

Based on these criteria, the *Thematic analysis* method as described by (Braun & Clarke, 2006) works best for this research. Thematic analysis describes an analysis process consisting of six consecutive phases in which codes and themes across the dataset are identified and analyzed. These phases, however, are not followed in a linear fashion. Instead, a recursive process is needed, one in which you move between the phases.

Table 2 describes the six phases of the thematic analysis method. Each phase further refines a set of codes, until (in step three) themes are formed by collating codes. These themes present patterns in the dataset. Not all phases of this analysis method will be explicitly stated when discussing interview results. The process was, however, executed to produce the results discussed in the chapter *Results*.

In order to start working with the interview results, they must first be processed. The goal of this process is to create a cleaner dataset to be used for thematic analysis. With consent of the interview participant, the interview will be recorded. This allows focus to be put on conducting the interview and engaging with the interviewee. If this option is not on the table, notes will be taken during the interview. The recording of the interview will be transcribed in parts. Since the interviews will be semi-structured, there will be deviations from the predetermined set of question. These deviations, however, will not all be relevant to the scope of this research project. Unnecessary information must be removed from the dataset to reduce the chances of making mistakes when coding and identifying themes.

The deviations in the semi-structured interview can result in a situation in which predetermined questions are answered in the natural flow of the interview. In this case, explicitly asking the question would result in a similar answer is therefore redundant. During the execution of the Thematic Analysis, if necessary, these deviations will be properly identified and coded.

3.5 Case study

The expert interviews will allow a refinement of the characteristics identified in during the literature study. Furthermore, new characteristics can also be identified during this stage of research.

During the interviews, the second goal is to find one or more real-world use cases to use for the qualitative analysis using the identified characteristics. The goal of the use case is the validation of the model in a representative setting. The interviews will be used as a gateway to find a case study project at Capgemini which can be used in this research project.

4. International IoT example: SmartOffice

A Capgemini Smart Building development

The SmartOffice project is Capgemini's current undertaking to more efficiently optimize office space, see *Figure 2*. Its client, Capgemini's Corporate Real Estate Services (CRES), wants to monitor over 1.6 million square meters of building space and measure workspace usage. Spaces in over 400 offices, in over 40 countries, with over 15.000 meeting rooms, and over 200.000 employees.

4.1 Use cases

4.1.1 End-user perspective

From an end user perspective, the SmartOffice project presents an intuitive user interface in the form of a mobile application which can be used to view and book flex office spaces and meeting rooms. Its most important functionality; Capgemini employees can view all available office and flex workspaces and manage them through the mobile application.

Four main functionalities of the mobile application can currently be distinguished;

1. **Reserve and manage meeting rooms**
   The application's primary function is its ability to allow employees to easily reserve and manage meeting rooms throughput an office location. Rooms can be sorted by floor, room size, and availability. At any given time, any employee can view a floor map of the office. Available meeting rooms are be marked with a green indicator, occupied meeting rooms are marked with a red indicator, if a meeting room has been reserved but is currently not in use, the space is marked yellow.

   For every meeting room, once selected, its availability is shown to the user. The application allows meeting rooms to be booked months in advance; the time period must be specified, and meeting room bookings are always name bound. Booked meeting rooms must be occupied at most after ten minutes after starting time. If the meeting room has not been occupied in the ten-minute timespan, the booking will be automatically cancelled, and the room will be available for others to use.

   A meeting room will only change state from available (green) to reserved (red) once it is in use for at least ten minutes continuously. This is implemented to prevent accidental use/ entry of a meeting room as being "in use".

2. **View flex space occupation**
   Future plans for the SmartOffice application include the active monitoring of flex workspaces throughput an office location. Rather than having to look around to find an available workspace, an employee will be able to view occupation through the application and find a workspace more easily. Unlike meeting rooms, flex workspaces

do not have to be reserved. A proximity and motion sensor monitor whether a spot is in use. Available flex workspaces will be shown with a green indicator, those in use with a red indicator.

3. **View information based on office location**
   The application shows a selection of relevant information based on the office a user is located in. This information can vary depending on the location, but often includes the following; public transport arrival and departure times, stores and restaurants near the office, in-office restaurant menu, and news. This is simply an overview of what can be included in this section of the application, the list changes based on location.

4. **View events**
   Capgemini organizes many weekly and monthly events, workshops and talks. These events are organized and can be found under the "Events" section in the mobile application. In its current state, the application does not allow users to join events (for those events which require registration), only to view event details.

4.1.2 Client perspective

From the client's perspective, Capgemini's Real Estate Services, the insights extracted from the SmartOffice project are of different use. Besides creating a more efficient employee experience, the SmartOffice project also provides insight in how offices can be more efficiently optimized.

Figure 2: SmartOffice - an introduction

1. **Office space optimization**
   With current operations it is often unclear for CRES which office spaces are utilized or underutilized, and the reasoning behind this. To exemplify, reservations are still made by writing a name and time on a piece of paper and sticking that on the door of an office space. This is obviously unmanageable for CRES.

   With a single central system used to make reservation, which can be used by all employees, this information becomes widespread and easy to manage. Both employees can more easily view and manage reservation, and CRES can use this insight to better manage office facilities.

With active monitoring and analysis using SmartOffice's data, spaces which are underutilized can be identified – be that because of an unfavorable location, limited seating or another reason completely. These spaces can be improved upon to optimize all available spaces. Secondary, with proper monitoring, no-shows in meeting rooms can be significantly reduced, again optimizing available spaces.

2. **Flex space optimization**
   Like office space optimization, once flex spaces will be monitored, a similar analysis can be made. Underutilized flex spaces can be identified and improved upon; departments which might require more space could be repositioned in the office. Besides this, flex spaces which are almost consistently busy can be identified and changes can be made accordingly to dissipate workers and rightsize office space.

3. **Improve work environment**
   Besides monitoring spaces, sensors will also collect on CO2, noise, light, humidity and temperature.

4.2 Analysis by characteristics

16 characteristics have been identified during literature study and interviews. These characteristics are deemed of *"importance"* for IoT network design. The SmartOffice project is a large-scale IoT undertaking. Most of the aforementioned characteristics therefore impact the project in some way, shape, or form. An analysis of the SmartOffice project can be made using these characteristics. For each characteristic, its relevance to the project will be discussed. For those characteristics which do not affect the project, N/A – not applicable – will be displayed.

	Characteristic	**SmartOffice relevance**
1.	Distributivity	In its current application a single type of sensor motion sensor is used for meeting space monitoring. Flex spaces will deploy a simpler type proximity/ motion sensor. Two types of sensors, deployed office wide.
2.	Interoperability and connectivity	Not applicable for the SmartOffice project; the project does not deploy different types of nodes and/ or requires support of multiple communication types. Connectivity of nodes is achieved by implementation of LoRa broadcast – receiver systems.
3.	Scalability	Limited; highly depends on the number of gateways. In its current form, the system does not require a scalable design. The SmartOffice network will be deployed in a fixed environment. Scalability is therefore limited.

4.	Safety and security	Not of significant importance, the network only mostly communicates *"movement updates"*. This information is only of significance to CRES and Capgemini employees. If this information were to be compromised, it would result in next to no harm. Second, due to the choice of architecture, nodes communicate by broadcasting messages. Gateways pick up *all* messages on the correct frequency. Messages part of the network are identified by an identification string part of the broadcast. Theoretically, external devices with the correct identifier string could tamper with the network reading and results by broadcasting inaccurate information.
5.	Latency	Relevant, however, not of high importance. Latency does not critically affect the networks operation/ purpose and is therefore not seen as a critical consideration.
6.	Throughput	Throughput in the network is at the maximum capability the system supports. Nodes directly communicate with one or more gateway by broadcasting their message over a LoRa supported frequency. Gateways in proximity receive and process node broadcasts. Since communication is direct, throughput is not negatively affected in the network. Besides this, messages size is minimal as only critical information is communicated, this therefore does not exceed the gateways throughput capacity when communicating with multiple nodes simultaneously.
7.	Number of hops (NoH)	In its current form, the LoRa sensors do not communicate information among themselves. All communication is between sensor and gateway. If a network consists of multiple gateways, information is shared among them. The system can be described as a type of mesh between star systems. With current plans, at most 4 gateways will be required for the largest Capgemini locations. NoH will therefore not exceed 4. Sensor level mesh support is currently a work in progress, once rolled out, the SmartOffice project will adopt these sensors for future locations.
8.	Fault tolerance/ robustness	The network communicates information using a broadcast - receiver type setup. Nodes broadcast information and one or more gateways should receive and process the message. In such a network, all LoRa messages on the correct frequency will be received by the gateway. Each node part of the network, however, broadcasts its message with an identifier string. If the string is correctly identified by the gateway only the node's information is processed by the network. Falsified broadcasts would therefore be required to mimic this string. The effort required to do so outweigh the benefits.
9.	Range	With the current LoRa implementation, an office location – depending on its size – can be covered in 2 to 4 gateways. For the implementation of SmartOffice at

		Capgemini Utrecht for example, 3 gateways have been used, each on one side of the building. In this configuration all deployed sensors are in reach of at least one gateway.
10.	Power consumption	Gateways are connected to mains power, nodes are battery powered. The nodes are proprietary made and have a special deep-sleep function which allow the nodes to stay operational for 5+ years before needing battery replacements.
11.	Cost	Various costs factors can be identified across the lifetime of a project/ network. The physical network consists of nodes and gateways, their cost is a summation of the number of times a node or gateway is used in the network times the price per element. Development is another cost which is often harder to estimate, nevertheless, an estimation must be made. This cost can be calculated in several ways, ***Table 8*** discusses a general approach for development cost calculation. Next, other costs like power consumption and maintenance must also be accounted for.
12.	Communication protocols	LoRa - chosen based on the network requirements; unlicensed, low cost, low power consumption, long range. This protocol fulfils and achieves what is required from the network and service.
13.	Routing algorithm	Communication between nodes and gateway is direct, this is achieved using a broadcast - receiver type system. All gateways in the network are directly connected. Information can be shared among them, there exists a hybrid mesh type communication between gateways.
14.	GDPR Compliance	Since various Capgemini offices are located within the EU, the network should comply with EU regulations, specifically the General Data Protection Regulation (GDPR). Outside of the EU, data compliance is bound to local jurisdictions.
15.	Retrofit	The networks are to be implemented in readily established Capgemini facilities. Preferability, the technology used should be minimally intrusive. For Capgemini, this meant restricting the number of gateways (since these demand the most physical change to the existing infrastructure) and maximizing the number of nodes. LoRa inherently fits these needs.
16.	Technology qualification	LoRa as a technology has been around for several years. The technology has been thoroughly developed upon and is currently still being improved. Besides this, LoRa has been successfully deployed as underlying technology for large international projects. It is therefore safe to say the technology is proven to be competent.

Table 3: 16 characteristic analysis SmartOffice

4.3 Functional requirements

SmartOffice in an undertaking to modernize all Capgemini offices worldwide. In order to guarantee project success, Capgemini has constructed a list of challenges to overcome for the ideal solution;

- **Easy installation**: sensors must be easily installable, a plug and play nature.
- **Low maintenance**: once in place, the network requires minimum effort to maintain. Batteries powering the sensory nodes should last at a minimum 7 years.
- **Minimum infrastructure**: physical infrastructure should be kept to a minimum. Use the minimum number of gateways, and/ or long-range communicating systems.
- **Retrofitting**: as the network is to be deployed in existing building/ alongside existing networks, the chosen network must support this.
- **Global scalability**: to be deployed globally, the system should allow global operation in a single manner.
- **Secure**: security is an integral part in the design and development in the network. After deployment, the network must be easily updateable to combat security concerns.
- **GDPR compliant**: since various Capgemini offices are located within the EU, the network should comply with EU regulations, specifically the General Data Protection Regulation (GDPR).
- **Data efficient**: data must be efficiently collected; double entries are to be removed and entries are to be stored in databases.

These eight challenges are the network's functional requirements. These requirements had to be met during project inception and planning. These factors also critically influence the choice of architecture used.

The final system is to be compromised of three distinct layers, **sensors** – **middleware** – **application**. Each of these layers manipulates and relays information to the next layer in the chain. The physical sensors are bound by various software and hardware requirements, they must offer the following functionalities:

- Be able to accurately sense human occupancy.
- Only broadcast status change messages (the sensor must only communicate messages once it detects a status change in its sensing range). Nodes do not need to be in constant communication with the gateway.
- Have a long battery life span, with a minimum of at least 7 years.
- Low maintenance (next to no human intervention required). If an error were to occur, the sensor (and/ or network) should be able to detect and resolve it.
- Simple installation, plug-and-play with app-assisted installation (sensors can be easily installed and allocated to a room in the application/ network).

Middleware should offer functions of sensor network management, asset management, configuration management (sensor and gateway configuration updates), and sensor data decoding.

4.4 Network design

Based on the aforementioned challenges and network requirements, an analysis of potential radio communication protocols had been made. The network choice is critical as it affects all parts of the system.

The graph in *Figure 3* compares various radio communication protocols based on their data rate (maximum speed at which data can be communicated) and range (operating area). The figure only compares the communication technology and what it has to offer, not a specific implementation of a communication protocol.

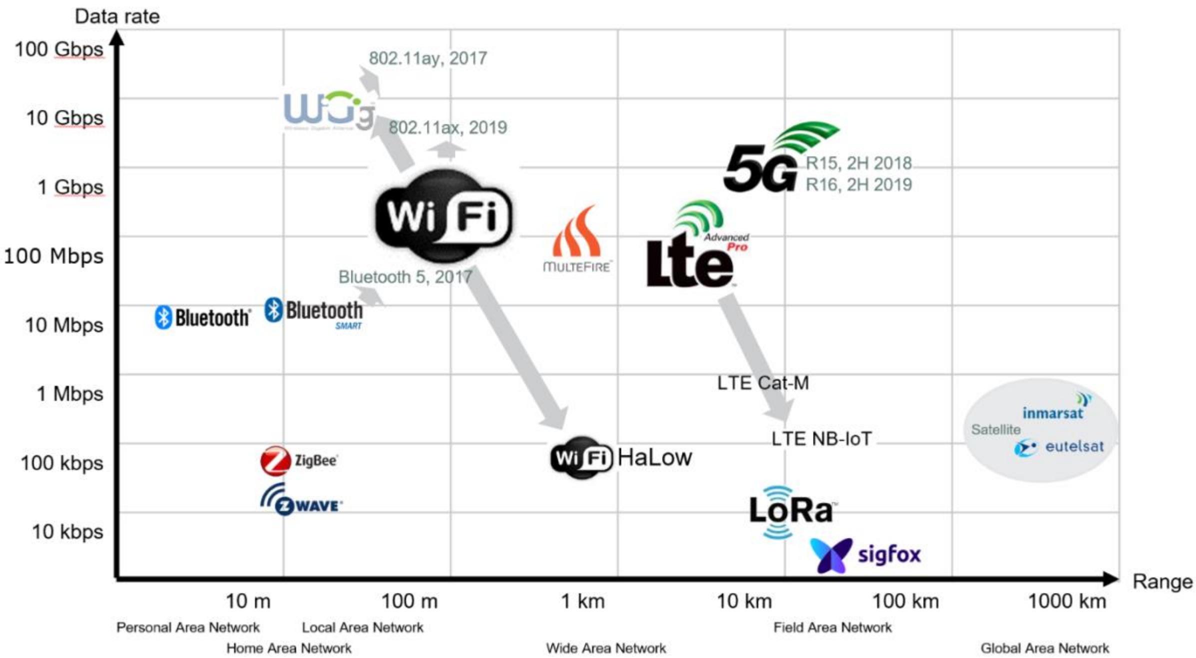

Figure 3: IoT communication protocols

The decision on a communication protocol has been made by comparing the protocol's fit with the following characteristics:

- **Licensed/ Unlicensed**: is a license required to use the communication protocol? LTE and 5G for example require mobile connectivity, these are periodically incurred costs which can be categorized as licensed.

- **Low cost**: costs incurred to deploy a network with a given protocol. General summation of hardware and software costs associated with a protocol.

- **Low power**: cost of power to broadcast communication signals for a protocol. Lower is better, a requirement of 7 years on batteries is set for sensory nodes.

- **Long range**: area of communication between sensory nodes among each other, and sensory nodes and gateway. Longer range desired, this results in the need for fewer gateways, resulting in lower costs.

Based on these four characteristics, a description of the communication protocols can be made. The graph-overlay in *Figure 4* displays the application of the characteristics to the protocols. This figure compares the communication protocols with regards to each characteristic and whether the protocols satisfy the characteristical needs.

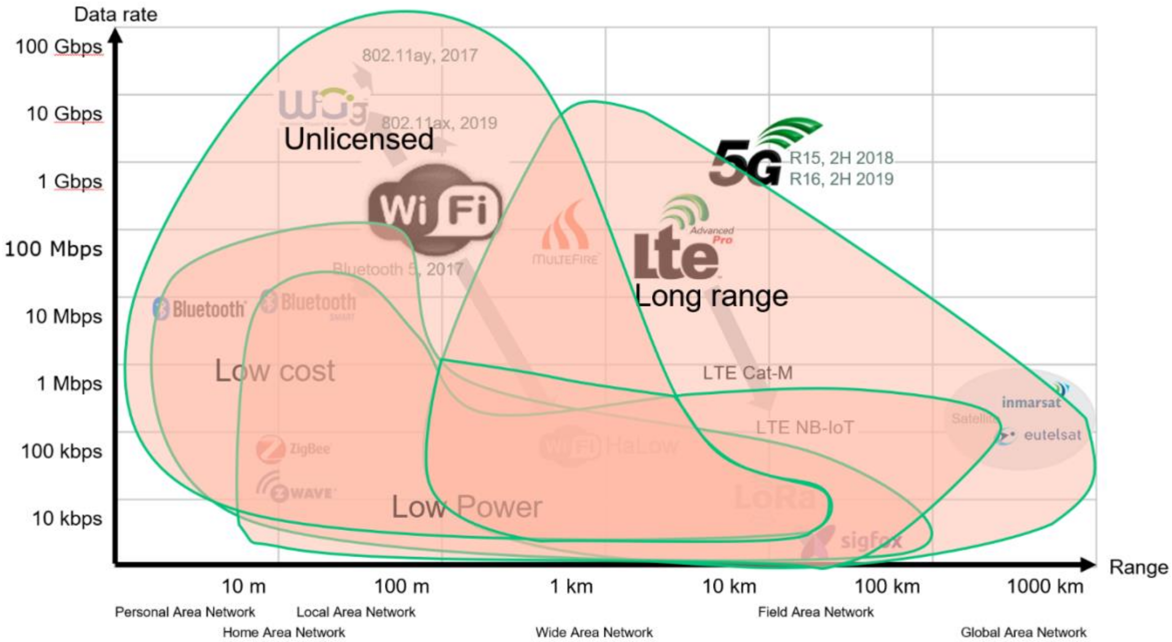

Figure 4: IoT protocols with categorical overlays

Four overlapping projections of the characteristics are drawn in *Figure 4*. We can derive two communication protocols which satisfy the need of all four characteristics. These are LoRa and WiFi Halow. Out of the bunch, these two protocols are the once which satisfy all characteristical needs and can therefore be considered for use.

WiFi Halow is a relatively new technology which has yet to see major development. Besides this, a limited number of physical technologies exists supporting the WiFi Halow protocol. LoRa on the other hand has already found many successes in the industry. 2015 marked the creation of the LoRa Alliance; a non-profit collaboration to ensure interoperability of LoRaWAN products and technologies. IBM, KPN, Cisco, and MicroChip among others are members of this alliance. Besides this, LoRa networks are used in projects worldwide; cotton farming, utility metering and smart fire alarms (LoRa Alliance, 2019).

It is clear that LoRa has the upper hand over WiFi Halow. The technology has proven industrial examples. Therefore, out of these two contenders, LoRa has been decided upon to further develop the SmartOffice project. For this undertaking, the LoRa communication protocol is positively characterized by the following attributes:

- Long range: outdoor up to 15 kilometers, **indoor up to 500 meters.**
- Low power: sensors can last months to **years on a battery**.

- Low cost: as low as **€20,- per node**, very low operating expenses.
- Low throughput: 250 bps – 50 kbps (up to 50 kB per hour).
- Open ISM band: **ability to build a private network**.
- Safety and security: 128 bit end-to-end encryption.

4.4.1 LoRa network implementation

LoRa is a license free long-range protocol used for the deployment of the SmartOffice project. The technology is characterized by its ability to operate nodes over a long range (as discussed in *Figure 4*), low power consumption, and its license free ISM band which allows individuals and corporates to build private networks. LoRa is a collective name for a number of technologies which build upon another, its most used form is LoRaWAN. Most implementations of LoRaWAN operate in the form of a star topology. Nodes communicate directly and solely with a gateway (Bor, Vidler, & Roedig, 2016).

In the SmartOffice project, the above described communication form is used for each gateway. Specifically, direct node – gateway communication in implemented using a broadcast – receiver method. With the SmartOffice project, however, several gateways are deployed at a Capgemini location to facilitate the communication of all nodes. In this arrangement, gateways are connected to one another in a mesh like configuration.

Gateways must communicate with one another to prevent errors such as duplicate data collections. The nature of the implementation allows multiple gateways to receive the broadcast of a single node. If not properly recognized and processes, this duplicate information could skew data.

4.4.2 LoRa and full mesh

Retrofit played an extremely important role in the decision to use LoRa for the deployment of the SmartOffice project. Compared to the alternative implementation methods, LoRa in its current form provides an implementation which benefits retrofitting the most. It is, however, not as user friendly and non-intrusive as is desired by CRES. As of writing, the LoRa team is working on development of node level mesh support. Currently mesh can be implemented, however, this would be a third-party implementation which often goes at the cost of LoRa's key characteristics. Having inherent mesh capabilities would reduce the adverse effects on these characteristics.

Mesh enabled nodes would allow deployment of the SmartOffice IoT network with a single gateway. Gateways have been identified as the most intrusive network element to deploy. Reducing the number of gateways would significantly increase the projects retrofit deployment. Furthermore, the ease at which the system can be installed would increase. This is another functional requirement of the project.

Once node level mesh functionality is publicly released, the Capgemini development team have already shown interest to move the project and further deployments of the SmartOffice network towards mesh.

4.5 Application layer

The application layer presents the different interfaces used to by end-users. Most – if not all – interaction with the SmartOffice system happens through an application interface. This layer can be divided into two part; a management application – *the control dashboard* – and an end-user mobile application.

4.5.1 Control dashboard

The control dashboard provides CRES with all relevant monitoring and maintenance tools for them to optimize Capgemini's facilities. All operational nodes and gateways can be managed, monitored and debugged through this dashboard. Besides this, in-depth analytics can be compiled (e.g. a table or graph of CO2 build-up throughout the building).

4.5.2 Mobile application

The mobile application serves two purposes. From an end-user standpoint (e.g. employee), the SmartOffice provides the user with four main functions; reserve and manage meeting rooms, view flex space occupation, view information on the current location and view interesting ongoing and upcoming events. These functionalities are thoroughly explained in this chapter's introduction.

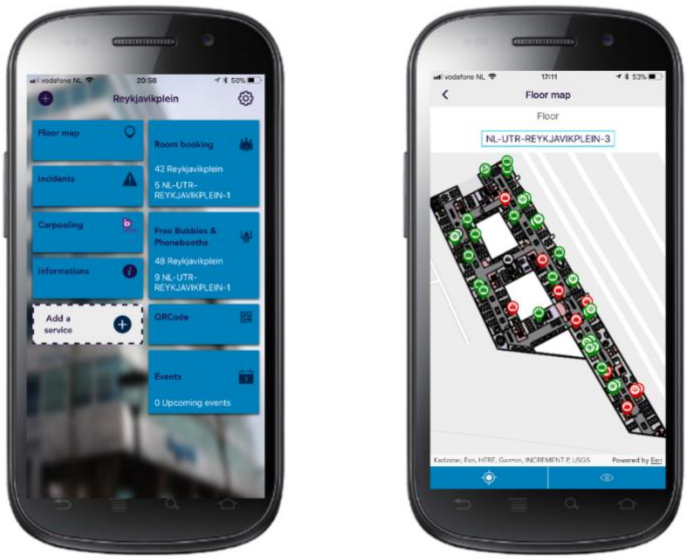

Figure 5: Mobile application (end user)

The mobile application serves a second purpose, it provides management and developers the ability to easily install and register nodes/ sensors to the network. Each sensor is outfitted with a QR-code, these codes are used to register the physical sensor to the network and assign each sensor its location on the building's floor map. This plug-and-play registration method allows locations to be quickly outfitted with the SmartOffice solution.

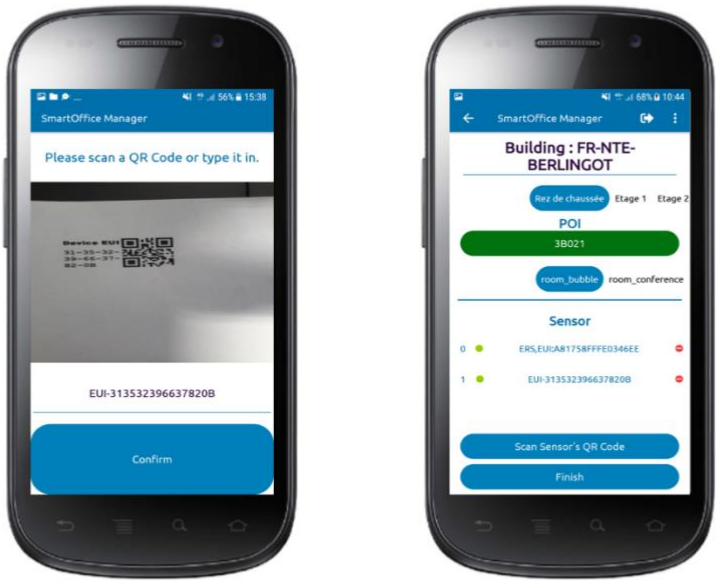

Figure 6: Mobile application (developer)

5. Interview breakdown

The interview and case study methodologies have been discussed in-depth in the previous chapter. This chapter will discuss the results of the performed research. Besides this, the set of core characteristics will be refined in this chapter for further use throughout this research paper.

5.1 Interview results

Not all questions are relevant for all interviewees. Depending on the background and experience of each interviewee, a subset of the questions is used. Interviewees with more technical background such as software developer or network architect will be asked question answerable from a developer's perspective. Interviewees who perform function in which they work closely with the client, e.g. requirement analyst, will be asked a subset of questions focused on the client-side of IoT mesh.

Since the interviews are conducted in a semi-structured fashion, the interview allows the interviewee and interviewer to deviate from the predetermined set of questions. Often, these deviations result in questions part of the list being answered naturally. The question itself would therefore not be asked explicitly, however, an answer could be deduced from the natural flow of the conversation.

This analysis will not discuss the answer of each question independently. Questions can be grouped (themes) to form answers which are more relevant to the scope of this research. This is what will be discussed in this analysis. As clarification, client related questions (Q12, Q13, and Q14) for example can be grouped and used to form an insight rather than be individually discussed in the analysis.

Working professional background, working experience, daily tasks:

"I am responsible for all staff support services for Capgemini Utrecht; HR, legal, marketing, the building… currently I'm also the head of a global smart office project at Capgemini where we actively monitor the use of flex-spaces and offices. In essence, sensors are used to monitor whether a working space is in use. This information is then displayed on a mobile app, accessible to all Capgemini employees."

[H. Scholten]

My background resides in networking and communication protocols, I have worked a lot with computer networking and everything around it. […] in general, my background is very technical, with a general setting in data communication. Currently I am working on the smart office project at Capgemini. My experience with IoT is roughly two years, with networking in general I have 20+ years of experience.

[M. van der Pal]

I mostly write the software which runs on the sensors. Embedded software development/ engineering. As part of this job I work closely with our hardware supplier to ensure the hardware fits well with the solution we are looking for, this is an external developer. The software which runs on these sensors are written by me.

Officially I am a coder on the team, however, I do a lot more besides this on the project/ within the team. […] I have designed the casing for the sensor module. I perform tasks in the backoffice, I've helped with the roll-out in this building (Capgemini Utrecht). […] in a couple of weeks, I will be going to Vienna soon to work on the deployment over there.

I started working as part of the OfficeSense team somewhere in March of last year. Currently I'm employed at Sogeti, so I am hired to work for Capgemini/ this project.

At Sogeti I am employed for almost three years now. I have studied electrical engineering, this ties in well with the combination of hardware and software I currently work on within this project.

Before this I work at Cube on Eneco's smart thermostat Toon. [..] there my project focused on revising the networks communication method. Communication occurs over the cloud instead of by VPN as it previously did. As part of this project, I again programmed on the chip-level to build the necessary code to support this new communication method.

[A. Smithuis]

What do IoT oriented projects at Capgemini look like? Other relevant networking experience?

An IoT solution consists of three segments; sensors, middleware and an information/ results layer, this can be seen as a "standardized" IoT solution. These three segments can be found in any IoT solution. Depending on the system […] we have different standardized frameworks which we use. If a mesh is the preferred solution for a problem, we might for example have to change the sensor types, the number of sensors or the information layer from the standardized model to fit this specific problem. However, the flow of data, and the existence of these segments remains the same. […] we fill in what we need depending on the problem.

[H. Scholten]

We have experimented with different technologies at Capgemini, one of them which uses mesh is Yanzi. Yanzi is based on IEEE's 802.15.4 networking standard. […] the technology offered by Yanzi uses a combination of gateways, sensory nodes, and intermediary data routing sensory nodes (these are both sender and receiver of information). We tested a couple of Yanzi sensors, […] whilst the technology they use is amazing, their solution based on that technology was not, […] from the roughly 150 sensors which we deployed; we couldn't get a *third operational. After trying with a new batch of sensors, we still couldn't get the majority of sensors up and running.*

Besides this, we had no way of monitoring the network. There was no troubleshooting functionality, we could not monitor simple things like see whether the network was performing its intended functionality or monitor whether all generated data is being collected. […] Yanzi did not provide any monitoring or troubleshooting functionality. This would be a non-functional requirement, however, for the daily operations of the network, this aspect is essential.

End users do not often think of this beforehand, until a network starts showing issues. Once this happens, monitoring tools should be in place.

[M. van der Pal]

[…] solutions at Capgemini are almost all custom-made, this ensures a good problem-solution fit. No two solutions (or problems for that matter) are the same. There is no real "template" which is used to develop a solution. For example, […] when looking at the hardware part of generic solutions, there are solutions which offer a device with multiple sensors. These devices can be used in various situations with different client problems. However, this solution will never be as efficient as a custom-made sensor, made specifically for a client's unique problem. When looking for the best solution, there is not one size fits all.

[…] the plan of action could be a good example of a general template. There is a certain order of steps followed to come to a solution. Depending on the client and problem, steps are added, extended or removed from the plan of action until a solution is created.

[A. Smithuis]

How experienced are clients with IoT, is it often the case that IoT is a desired solution, or that a problem suggests an IoT solution/ does a client care for the type of solution?

Clients often have a problem […] with an IT component. Depending on the problem, we start looking for possible viable solutions. Sometimes IoT is an obvious solution, […] were currently working on a project with the NS. They want to provide an app which displays seat availability. For such a project IoT is the perfect problem – solution fit. In general, a client does not come looking for an IoT solution, rather an IoT solution is suggested as a best fit to the client's problem.

[H. Scholten]

[…] the implementation of the technology does not (in most cases) concern the client. If a solution is using a star, mesh, or ring topology does not matter to clients, this as long as the solution satisfies the need.

[M. van der Pal]

Feedback on the list; do you think this list of characteristics is relevant for IoT projects or more specifically for mesh projects?

"… I think you did a pretty good job with the list, it most of these characteristics are relevant for IoT. Characteristics such as cost, and power consumption are obviously more valuable to a client. Other characteristics such as latency, throughput, number of hops are relevant for an architect."

[H. Scholten]

Your list contains mostly characteristics aimed at technical requirements. If were talking about requirements, these can be divided into functional and non-functional requirements. […] what's missing from your model characteristics aimed at management capabilities, everything that's about maintaining a mesh network. Your project currently looks at the technical aspect of mesh, how should a network perform. That, however, says nothing about how such a technology is used in practice and how it's used, this once a product has been handed over to a client.

Let's say you spend two years working on a project […] and after three months it turns out the technology used is outdated. The management tools used for technology might no longer be supported, or there might be somethings else taking the market by storm. So, even if the technical part of the project is up to par, but the supporting elements are lacking, no-one would be interested.

[M. van der Pal]

Scalability: important from a developer's perspective. If your solution is not scalable, its uses are significantly limited. This characteristic is especially important for the OfficeSense project. […] we aim to deploy hundreds of meeting room sensors, and thousands of flex space sensors. It is obvious that the solution must therefore be scalable.

Maintenance: again, from the perspective of the OfficeSense project […] maintenance played an important role. Once a sensor is deployed it should be able to manage itself. In the case of errors, the sensor should have the functionality to correct itself and reconnect with the network. Maintenance must be kept at a minimum; however, the system must be efficiently monitored to plan for maintenance.

GDPR: in becoming increasingly important […] this overlaps somewhat with privacy and security.

Privacy: we previously ran tests with Yaanzi sensors, […] what we noticed from these test runs was that people tended to cover up the sensors. This most likely because the sensors looked a lot like cameras. People tend not to like to be watched or be given the feeling that they are being watched.

Security: for this project, security did not play a critical role. If someone were to hack a sensor, the worst they could do is mis-display information. Make an empty room display as booked.

[…] the risks in this application are minimal. If we were to design a solution for another client however, security would be of higher concern. […] this especially if sensors for example operate on a common network. The impact of a compromised sensor could be significantly higher.

Distributivity: the OfficeSense network should be easily deployed. One such requirement was that an "average" non-tech savvy employee should have the know how to deploy the physical sensors and assign them their proper location.

[A. Smithuis]

Are there any characteristics you would leave your, or are there characteristics that should be part of this list?

Retrofit*; how difficult is it to implement IoT network in an established environment. Can a network be easily implemented alongside what already exists, or do significant changes have to be made to support the IoT network?*

GDPR*; as an extension to the security and privacy characteristic. Since we are operating most of our projects in the Netherlands, GDPR (or AVG) compliance is a pre.*

[H. Scholten]

[…] these might not necessarily be characteristics that should be present in your model, however, I would consider these characteristics important to acknowledge when designing an IoT solution.

Security*; you have already touched on this in part on your characteristic "Safety and Security". […] mesh networking is characterized by a large number of sensors. These sensors are network connected. Security plays an important role in mesh networking, not only to fend off outside forces, but also to ensure integral network safety. I would redefine this characteristic as "Security" to not underestimate its importance.*

Frequency band (ISM band)*; what radio frequency is used by the chosen communication protocol. Does a technology use a proprietary or common communication protocol? Certain protocols are licensed (e.g. 5G and LTE), others are freely available.*

Technological maturity*; has a technology been around long enough to be developed upon? Has enough research gone into the technology? Are there other projects and/ or industries which have successfully deployed this technology? Maturity is a general estimation whether the technology has been explored and developed enough to be practical.*

Rate of technological adoption*; at what has the industry adopted to a particular technology? Think of what percentage of the market is using this technology, and which industries.*

[M. van der Pal]

How would you define successful IoT (mesh) solution?

Success can be differently defined depending on the person you are asking, […] I will define success for our smart office project. In this building we currently have 200 sensors in office spaces, and we are currently adding another 1500 sensors for flex-spaces. […] requirements for the network are that each sensor should last at least 5 years, have a low number of gateways, and be operational in a large area (20+ m), low cost/ performance. With these requirements in mind we have evaluated several network topologies. We eventually settled for LoRa, it has a large operating area, this means we would only need 2 gateways to operate all sensors in this building (Utrecht). Besides this, LoRa sensors are equipped with a deep sleep functionality, allowing each sensor to operate for roughly 5 years. […] success in this case can be defined as conformity to the functional requirements. If we were to use a different type of network, let's say one which supports mesh, it would be required to perform at least as well as a non-mesh network.

[H. Scholten]

[…] from a consultant's perspective, our greatest asset for successful customer delivery would be our multi-disciplinary team. When designing a solution, the focus should not only be on the technical aspect but should also focus on the business solution the client is in need for. Try to tick off as many problems as you can with your proposed solution. Technical, functional and non-functional.

[M. van der Pal]

[…] when a client states their requirement, we always as the "why" questions. In order to create a solution, we must first fully understand the underlying problem. These "why" question allow us to look at the problem at a deeper level instead of at a surface level as often described by clients.

Clients come to us with a problem they cannot solve themselves. The solution is for us to suggest, develop and deliver. There is no standard model that fits every problem, solutions are almost all custom made. […] a solution should fulfill client needs and expectations.

[A. Smithuis]

What would you consider to be the advantages of mesh?

Mesh is more easily deployed compared to other network topologies. You would only need a single (or small number) for gateways, all information generated by the network could be routed to this gateway my hops through the mesh network.

Cost efficient, since a mesh network is often characterized by a small number of gateways and a large number of sensors. The costs of such a system would be lower compared to other network topologies. Sensors in themselves are much cheaper than if the alternative would be *having a larger number of gateways. Besides this, a gateway requires much more physical setup […] in our case this would mean breaking open the walls/ roof to create the necessary infrastructure.*

[H. Scholten]

Mesh's strength lies in its networks ability to communicate information between nodes, instead of solely between node and gateway. […] depending on the use-case, this ability can have various benefits. If a use-case requires you to use the fewest amounts of gateways (or maybe a single gateway) possible, this could affect the operating area of your network. A star network would be limited by the range nodes and gateways can communicate. Mesh on the other hand can propagate information from one node to the next in order for information to reach the gateway. In such a mesh network solution, range would not be as significantly affected.

[M. van der Pal]

[…] mesh obviously has its advantages, these advantages however are highly dependent on the use-case. […] a network topology should fulfill the needs of a possible solution. Just to name a few advantages/ disadvantages of mesh over other topologies:

Reliability; you can more easily ensure data reaches its destination in a mesh network. If needed, data can be routed differently, or be re-routed.

Network monitoring; the network can correct itself in case of malfunctions. If a node were to drop, information usually routed through that node could be re-routed through other nodes to ensure information reaches its destination (increased network integrity). Mesh networks often regulate themselves to actively provide this functionality/

[A. Smithuis]

What would you consider to be the disadvantage of mesh over other network topologies?

What does the power consumption look like? How many messages are generated and communicated in a mesh network? There should be a tradeoff between the efficiency of the network and its power consumption. If mesh sensors are battery powered, how do hops affect the sensors battery life? We obviously would not want to replace sensory batteries monthly.

How reliable is a mesh network? How do we ensure that every message generated by all sensors are collected? This process of routing all data packages is probably more complex compared to other networks where each sensor directly communicates with a gateway.

[H. Scholten]

With mesh you are mostly looking for a mobile solution to solve a mobile problem. […] the use of a technology is dependent on its use-case. Inherently, a technology does not have real *advantages or disadvantages […] this is however decided by its use-case. Any topology would have disadvantages if it were to be used to solve a problem it is not designed for.*

[M. van der Pal]

Costs; mesh networks are almost always more costly compared to (possible) alternative solutions. Operating a mesh network is energy costly, battery powered solutions are realistically not viable as a long-term low maintenance solution. […] another cost is pricing, mesh technology and mesh enabled hardware are paired with higher costs compared to non-mesh sensors and technologies.

[A. Smithuis]

How would you rank the identified key IoT characteristics from most to least important?

Depending on the use-case, different characteristics will be important. For one, latency might me the most important consideration. For another use-case, the most important characteristic could be throughput. Not all characteristics can always be combined in a single project. You cannot have low latency, high throughput and low costs. You have to choose two, and sacrifice the other in some way, shape or form. If you would like all three in this case, some other part of the project will be affected. There is always a sacrifice to be made. A ranking of characteristics therefore depends on the use-case, there is no one-fits-all ranking.

[M. van der Pal]

Measurable characteristics

[…] we don't measure characteristics such as latency or throughput for this project, this information is not critical for the operation of the network and our specific purpose of the network. […] a different project for another client may require us to collect this data, this is not the case for what we're currently working on.

[M. van der Pal]

[…] all communication in this network is device driven. We cannot remotely send requests to a sensor, if these are not broadcasting a message or tracking movement, the sensors are in continuous deep sleep. […] when a message is broadcast, the sensor opens a two second "communication window". During this time, messages can be received from gateways. […] during testing, on multiple occasions, we have found that this two second timeframe did not satisfice. Network latency resulted in 2+ second feedback loops between message received and feedback communicated.

[…] we monitor several statistics which give us an indication of network health. These measurements indicate whether the network operates efficiently or not. […] latency and throughput for example are ones we do not track. […] characteristics such as latency are bound by the communication method decided. LoRa has upper and lower bounds for latency

within networks. […] based communication protocol a developer knows how the network is bound by certain specifications.

[A. Smithuis]

Semi-structured insights.

When designing a mesh network, sensors have different or multiple purposes. This multi-purpose characteristic requires additional monitoring, therefor the system becomes more complicated. Maintaining such a system requires the monitoring team to possess more know-how and knowledge. Besides this, deployment of mesh systems compared to alternatives is more complicated in practice. In general, when looking at the cost of mesh compared to alternatives, mesh is more expensive. Training of employees, development costs, maintenance cost, cost of operation, these are all higher when deploying mesh systems.

[M. van der Pal]

5.2 Interview analysis

Interesting correlations can be found across the interviews. Below are the most important findings from the conducted interviews. These are not necessarily technical specifications on IoT or mesh, but more so noticeable repetitions.

- Do not simply look at client problems at a surface level, aim to understand the root and underlying needs of the problem. These are the real needs that need to be met.

- A universal ranking of characteristics cannot be made. Different projects emphasize different characteristics. Rankings can be made for projects, these however, often do not hold across projects.

- Method of implementation does most often not concern clients, the business and operational benefits the implementation offers however, do.

- Controversial: *IoT is not IT, its business*. IoT finds its uses almost exclusively in business; supply chain management and asset tracking for example. This point is further explained on by stating that IoT as application of networking technology finds its niche in mostly business environments. Solely developers – highly technical – do often not possess the know-how to create successful IoT systems by themselves. A collaboration of technical and business experts is required, more so compared to other projects.

- Systems must work, to a certain extent, seamlessly with existing systems. Retrofit tech is therefore required. Unless a completely new undertaking is being developed upon, retrofitting is critical.

Interesting is the contrast between this client-side and the developer-side “ranking” of characteristics. The developer interviewees consistently stated throughput the interviews that it is *impossible* to rank the characteristics without a use-case. Importance of the characteristics is directly influenced by a use-case. Certain use-cases might require a high throughput, low latency network whilst the next might put emphasis on long range and scalability. The developer-side interviewees therefore deemed it impossible to create a standardized ranking of these characteristics.

From client-side, the raking is interpreted as characteristics which impose important functional requirements of the current project. Not so much a general ranking of importance across IoT projects.

6. A generalized framework for analysis

Throughout the interviews and literature study conducted in this research, 16 characteristics have been identified. These characteristics can be termed *Critical Success Factors (CSF)*. Based on the research conducted in this study, the identified characteristics are ones most important for IoT project success, specifically for projects deploying mesh networks. Literature study formed the basis on which these CSF have been identified. Interviewees suggested several characteristics based on their experience and perceived importance from a developer and client perspective.

The 16 CSF part of the framework have been successfully used as a qualitative descriptive model for an IoT project, as part of the deliverable for this research paper. In *Table 3* in *Chapter 4.2* the SmartOffice project is analyzed using the identified characteristics. Here, the impact and relevance of each characteristic is discussed in terms of how it affects the project. In this use case, the model is used posterior for the analysis on a readily operating IoT network.

The framework can, however, also be used a priori. During project development, the CSF can be used as a checklist for developers and project stakeholders to ensure the key IoT network elements are properly addressed. Furthermore, the CSF can be used as starting point during network design.

Just to recap, the 16 CSF are the following; distributivity, interoperability and connectivity, scalability, safety and security, latency, throughput, number of hops, range, power consumption, cost, communication protocols, message size, routing algorithm, GDPR compliance, retro fit, and finally technology qualification.

6.1 Network description

From a high-level perspective, an IoT network consists of sensory or relay nodes, one or more gateways and connections between them. This type of network can be described in terms of mathematical graph theory. Similar to IoT networks, graphs are built up of vertices and edges and depending on the type of graph a description of dataflow between vertices in the graph is given. When translating IoT networks to graph systems, nodes and gateways are vertices, and connections are edges.

In its basic form, a graph system can be described as followed:

$G = \langle V, E \rangle$	*A graph G consists of a set of vertices V and edges E*
$V = \{v_1, v_2, v_3, \ldots, v_n\}$	*V a set of Vertices*
$E = \{e_1, e_2, e_3, \ldots, e_n\}$	*E a set of directed Edges*
$\forall V = \#e \in E \geq 1$	*A vertex V has at least one edge*

A graph G consists of a set of vertices and edges. The set V consists of all vertices present in the graph. The set E contains all edges in the graph. An edge *(x, y)* describes an edge in which information flows from vertex *x* to vertex *y*. If information flow is bi-directional, both *(x, y)* and *(y, x)* must be elements of the set E.

The above describes a graph system in which all vertices and edges are equal. The system does not distinguish different types of edges or different types of vertices. In IoT networks however, different types of nodes can be distinguished. Since the operation of these nodes differs and affects network performance, it is important to define and translate these node types to be used in the graph system. Three node types can be identified:

- **Sensory**: nodes which sense outside information, these nodes can also relay information to other nodes is mesh systems or to gateways. IoT networks are often composed of multiple sensory nodes.
- **Relay**: nodes which do not sense, their only purpose is to relay information from sensing nodes to other points in the network. Relay nodes are not required in all IoT networks
- **Gateway**: the gateway serves as a point of data collection from sensory nodes. IoT networks must have at least one gateway.

IoT networks often contain either all three node types, or at least sensory and gateway. These different node types must be included in the basic graph description given above in order to give an accurate representation of IoT networks. One way to achieve this is by adding an attribute to the vertices in set V which describes the node type.

$V = \{v_1, v_2, v_3, \ldots, v_n\}$ *V a set of Vertices*

Vertex Type VT = $\{Sensory: v^S; Relay: v^R; Gateway: v^G\}$

$V = \{v^{VT}_1, v^{VT}_2, v^{VT}_3, \ldots, v^{VT}_n\}$ *V a set of Vertices adjusted with attribute VT*

The adjusted set of vertices V now contains an identifier VT for each vertex which describes its type. With this addition, the graph description is able more closely describe IoT networks. Besides different types of nodes, different communication types are also identifiable in IoT networks. Communication is present between nodes; so, node to node, between node and gateway, and between gateways; so, gateway to gateway. The 10 identified clusters could affect these three types of communications differently, it is therefore important to distinguish between them.

- Node to node (N2N)
- Node to gateway (N2G)
- Gateway to gateway (G2G)

Like with vertices, an attribute can be added to each edge in the set E which describes its type.

$E = \{e_1, e_2, e_3, \ldots, e_n\}$ *E a set of directed Edges*

Edge Type ET = $\{N2N: e^{NN}; N2G: e^{NG}; G2G: e^{GG}\}$

$E = \{e^{ET}_1, e^{ET}_2, e^{ET}_3, \ldots, e^{ET}_n\}$ E a set of directed Edges adjusted with attribute ET

The adjusted set of edges E now contains an identifier ET for each edge which describes its type. The denotation of the connection type would also be visible when looking at the start and end vertices (or nodes) in the graph. Stating them, however, creates a more easily readable description of a network's make up.

Lastly, a basic linear IoT network must have at least one sensory node, one gateway, and one connection between them, type: node to gateway. This setup describes the most basic IoT network containing one of each network element. This prerequisite should be added to the network description:

For a graph G it must hold that:

$v^S, v^G \in V \geq 1$ *There must be at least one sensory and gateway node*

$e^{NG} \in E \geq 1$ *There must be at least one Node – Gateway connection*

6.1.1 Definition of IoT network in graph theory

With an updated description of both edges and vertices to more accurately describe IoT networks in terms of graph systems, a description of IoT networks can be given:

$G = \langle V, E \rangle$ A graph G consists of a set of vertices V and edges E

Vertex Type VT = {Sensory: v^S; Relay: v^R; Gateway: v^G}

$V = \{v^{VT}_1, v^{VT}_2, v^{VT}_3, \ldots, v^{VT}_n\}$ V a set of Vertices adjusted with attribute VT

Edge Type ET = {N2N: e^{NN}; N2G: e^{NG}; G2G: e^{GG}}

$E = \{e^{ET}_1, e^{ET}_2, e^{ET}_3, \ldots, e^{ET}_n\}$ E a set of directed Edges adjusted with attribute ET

$\forall V = e^{ET} \in E \geq 1$ *A vertex V has at least one edge*

For a graph G it must hold that:

$v^S, v^G \in V \geq 1$ *There must be at least one sensory and gateway node*

$e^{NG} \in E \geq 1$ *There must be at least one Node – Gateway connection*

This description states that an IoT network consists of a set of nodes and connections. Nodes can be of the form sensory, relay or gateway. Connections can be of the form node to node, node to gateway, or gateway to gateway. For each node part of the system, it must hold that it has at least one connection. Furthermore, a network must have at least one gateway, one sensory node and one connection of type node to gateway. This describes the most basic linear IoT network containing one of each network element.

Using the graph description, the network in *Figure 7* has been created with the appropriate graph description. This illustrates the use of the graph description.

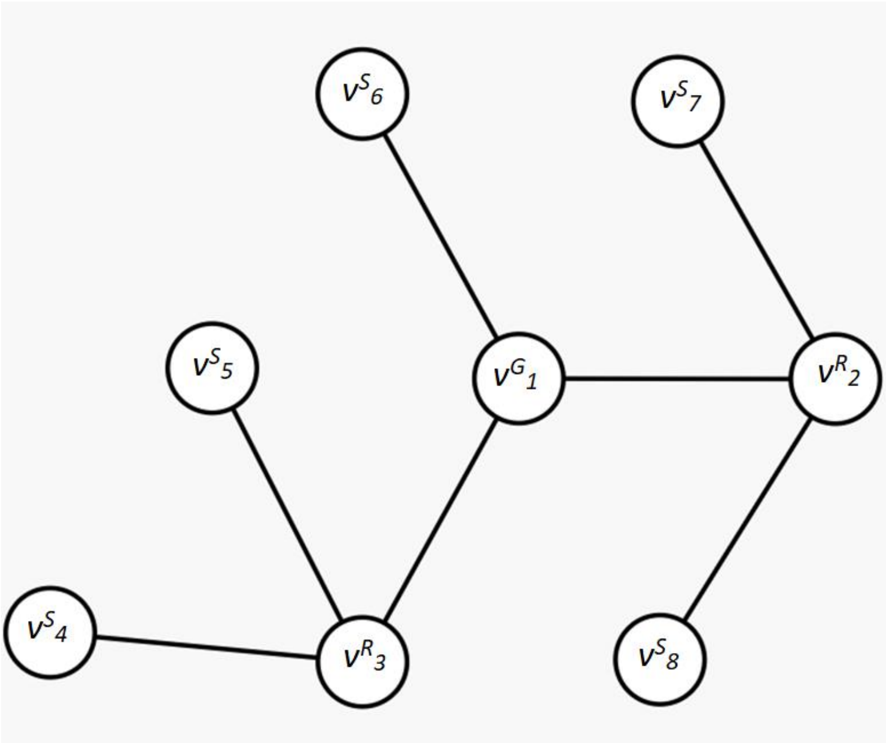

Figure 7: Simple IoT network design

$G = <V, E>$

$V = \{v^G{}_1, v^R{}_2, v^R{}_3, v^S{}_4, v^S{}_5, v^S{}_6, v^S{}_7, v^S{}_8\}$

$E = \{(v_1, v_2)^{NG}, (v_1, v_6)^{NG}, (v_1, v_3)^{NG}, (v_2, v_7)^{NN}, (v_2, v_8)^{NN}, (v_3, v_5)^{NN}, (v_3, v_4)^{NN}, (v_2, v_1)^{NG}, (v_6, v_1)^{NG}, (v_3, v_1)^{NG}, (v_7, v_2)^{NN}, (v_8, v_2)^{NN}, (v_5, v_3)^{NN}, (v_4, v_3)^{NN}\}$

Figure 7 describes an IoT network with five sensory nodes, two relay nodes, and one gateway. Communication in this network is bi-directional, this is also described in the graph description set of vertices.

6.2 Relation between CSF and network description

The 16 identified characteristics affect different parts of IoT networks. Using the graph description, three segments can be identified: nodes (vertices), connections (edges), and the full network (full graph). Not all characteristics affect all three segments. In order to further analyze IoT networks using the identified characteristics in relation with the graph description, the relation between each characteristic and the segments of a network is important to explorer. It is possible to assign each characteristic as attribute of nodes, connections, or the full network.

The *full network* segment can be described as one which affects all operations of the network; network wide. If a characteristic is part of this segment, the characteristic affects the system as a whole rather than either nodes or connections, it is an inherent design consideration. *Table 4* lists all 16 characteristics and which segment it affects. The sections below further explain the division.

Characteristic	Nodes	Conn.	Network
Distributivity	x		
Interoperability and connectivity	x		
Scalability			x
Safety and security			x
Latency			x*
Throughput			x*
Number of hops (NoH)		x*	
Fault tolerance/ robustness	x		
Range		x	
Power consumption			x
Cost			x
Communication protocols			x
Message size	x		
Routing algorithm		x	
GDPR Compliance			x
Retrofit	x		
Technology qualification			x

Table 4: Relation between characteristics and network elements

Node

The node describes all types of sensory, relay and gateway nodes present in the system. For the purpose of this section, sensory and relay nodes can be grouped, as these are similar in functionality compared to the gateway. The characteristics will influence sensory and relay nodes in mostly the same way, for gateways there is more difference.

In *Table 4*, five characteristics have been assigned to nodes. These are; distributivity, interoperability and connectivity, fault tolerance/ robustness, message size, and retrofit.

- **Distributivity**: in IoT networks, the distributed element is the sensor and gateway. Sensors are the network element collecting and/ or communicating information. Gateways are end points for this information. The physical reach of a system is (among other characteristics) defined by the distributivity of its nodes.
- **Interoperability** and connectivity: depending on the IoT network, different types of sensors can be deployed. E.g. humidity sensor, motion sensor, temperature sensor, CO_2 sensor, etc.
- **Fault tolerance/ robustness**: the nodes are the network elements most susceptible and accessible to attacks and misuse. By design, these nodes must therefore be secure enough to be able to fend off possible attacks. Furthermore, sensory nodes and gateways are the core elements when it comes to collecting and processing data in an

IoT network. It is of importance that data collected accurately represents the real word situation.

- **Message size**: sensory nodes are the sole element in an IoT network which senses the outside world to generate data. Communicated message sizes are often predefined, however, communicated by these nodes.
- **Retrofit**: describes the ability of a system to be installed in a readily established environment. Among the elements of an IoT network, the most intrusive is the node.

Connections

Connections cover all means of communication in an IoT network. In this research we have identified three communication types; node to node, node to gateway, and gateway to gateway. Small differences might be present across communication types (e.g. throughput between node to gateway connections is larger compared to node to node connections as more data is communicated over these connections), however, the characteristics which influence connections affects all communication types.

In *Table 4*, three characteristics have been assigned to connections. These are; number of hops*, range, and routing algorithm.

- **Number of hops***: specific to mesh systems, the number of node-hops a message makes before reaching its destination. Besides a general use of this characteristic, the number of hops can also be calculated for sub-nets or specific graph paths in an IoT network.
- **Range**: the area of communication between nodes in an IoT network. Nodes can be used to extend a network's reach.
- **Routing algorithm**: defines how communication is established, routed and managed throughout a network.

Full network

The full network segment covers elements which are inherent design considerations/ choices. The characteristics assigned to this segment are directly affected by the network's underlying architecture and implementation and influence all aspects of a network.

In *Table 4*, three characteristics have been assigned to the full network segment. These are; scalability, safety and security, latency*, throughput*, power consumption, cost, communication protocol, GDPR compliance, technology qualification.

Two characteristics have been appended with an asterisk, these are latency and throughput. Unlike the other characteristics part of this segment, latency and throughput are not only design considerations. These characteristics can also be used to define their respective element on sub-nets or graph paths in an IoT network.

- **Scalability**: the ability of a network architecture to adapt to a changing environment and changing needs.
- **Safety and security**: the implementation of network security is a consideration which must be made at a project's inception. Safety and security features can be realized in

various methods, security by design, control network access and routing updates are among a few. Its implementation is defining for the security of all network functions and elements.

- **Latency***: the calculation of latency is dependent of the use case. An upper and lower bound for latency, however, is predefined by the network's implementation and architecture.

  For use cases, latency can be calculated on specific graph paths or in sub-nets of a network. In this sense, latency describes the time between data collection by the sensory node and data aggregation, processing, and storage by the gateway or by another node in the network.
- **Throughput***: the calculation of throughput is dependent of the use case. An upper and lower bound for throughput, however, is predefined by the network's implementation and architecture.

  For use cases, throughput can be calculated on specific graph paths or in sub-nets of a network. Throughput describes the maximum rate data can be shared, analyzed or stored in a or across a network.
- **Power consumption**: all network elements are power consuming. Sensory and relay nodes, gateways, connections, these are power consuming elements. The design implementation of a network, however, is defining of the level of power consumption of these elements. Different node types for example can have vastly differ in their power consumption (e.g. battery powered nodes as opposed to nodes connected to the outlet).
- **Cost**: different types of costs can be distinguished; fixed, variable and maintenance. Network elements have a fixed cost associated with them, nodes and gateways are purchased at a price per unit. R&D and development costs are associated with creating the appropriate infrastructure required to deploy the network. There are costs for power consumption, licenses, certifications etc. Maintenance costs are made to keep the network operational once it is deployed. These costs have been thoroughly discussed in previous chapters.

  The method of implementation of an IoT network severely affects the costs contributing factors described. Depending on the implementation, these costs can vary.
- **Communication protocol**: specifically describes the method of communication part of design and development. Affects all elements part of the IoT network (e.g. LoRa, WiFi, ZigBee, etc.).
- **GDPR compliance**: development of the network and all elements thereof according to the GDPR.
- **Technology qualification**: verification whether the technology (usually a relative new technological development) meets the requirements of what is expected of the IoT system/ deliverables.

6.3 Clustering of characteristics

The identified CSF do not all describe unique or exclusive attributes, overlap can be found across several characteristics. To illustrate this, throughput for example is influenced by other characteristics, this being number of hops, range, communication protocol and routing algorithm, these characteristics influence the throughput characteristic and must be considered. Based on overlaps identified during literature study and the conducted interviews, a dependency graph can be constructed containing each characteristic and their dependencies (if applicable) to other characteristics.

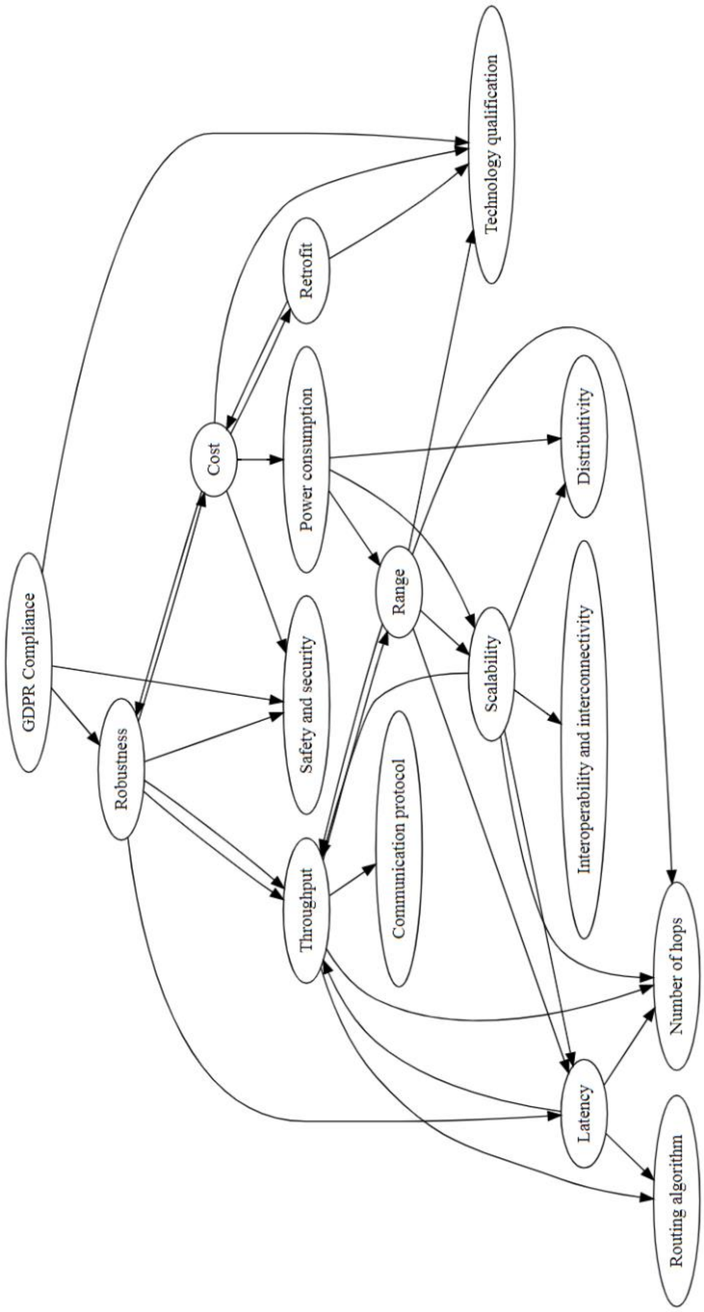

Figure 8: Dependency graph characteristics

Figure 8 displays the dependency graph containing all characteristics identified in this research paper. An arrow describes a dependency. E.g. X -> Y describes a dependency of characteristic X on characteristic Y. Dependencies are between the starting point of the arrow to the head. *Figure 8* contains all connections, in order to more easily use the information in this figure, dependencies can be clustered and grouped. *Table 4* is a translation of what is found in the dependency graph. Ten clusters can be identified in this figure. For each cluster, its dependencies are stated. For certain characteristics, other elements (not part of the list of characteristics) are deemed of importance and therefore included in *Table 4*.

Summation		
1.	**Throughput**	Number of Hops - Range - Communication protocol - Routing algorithm
2.	**Latency**	Throughput - Number of Hops - Routing algorithm
3.	**Cost**	*License - Standard or proprietary technology* - Retrofit - Power consumption - Technology qualification - Safety and security - Robustness
4.	**Range**	Throughput - Latency - Number of Hops - Technology qualification - Scalability
5.	**Power consumption**	Scalability - Distributivity - Range
6.	**Technology qualification**	*Technology maturity - Rate of adoption (not characteristics, however other aspects of importance)*
7.	**Scalability**	Interoperability and connectivity - Distributivity - Number of Hops - Throughput - Latency
8.	**Robustness**	*Overarching characteristic - Communication protocol -* Throughput - Latency - Cost - Safety and security
9.	**Retrofit**	Cost - Technology qualification
10.	**GDPR Compliance**	Safety and security - Technology qualification - Robustness

Table 5: List of clustered characteristics

The first column in *Table 4* represents the cluster (cluster name), the second column the characteristics they are dependent on. Ground for the dependencies identified are based in literature study and the conducted interviews. As previously explained, the second column does not only contain characteristics, but also other elements of importance required to properly describe a cluster. To illustrate this point; *Cost* is a rather arbitrary characteristic. Besides the other characteristics cost is dependent on, other elements also influence this characteristic. This research has specifically identified *License* and *standard or proprietary technology* as two cost affecting elements. These are therefore also included in the table, however not in the dependency graph. All additional elements part of *Table 4* can be found and are thoroughly discussed throughout various chapters of this research.

The analytical use in term of the CSF has previously been discussed. The clustered set sizes the number of characteristics down to a more usable number which can be used to create an initial analytical descriptive model for IoT architectures.

6.3.1 Initial analytical description of framework

The majority of the characteristical clusters are quantifiable. Depending on the characteristics, an analytical description can be given a priori or posteriori. CSF such as latency and cost can be calculated before the deployment of a network. Other CSF would need to be thoroughly tested in the field, once deployed, in order to be quantified. Robustness for example, becomes quantifiable once a network has failed a couple of times. The same holds true for the (negative)effects of not complying to GDPR regulations.

Using the clustered sets of CSF given in *Table 4*, an initial start can be mate towards the quantification of the clusters. To illustrate this use of the framework, an initial attempt is made towards the computation of *latency*, *cost* and *power consumption*.

Latency

Latency describes the timeframe required to transfer a data package from one point in a network to another designated point. In IoT networking, these transfers will most often describe data transfers from sensory nodes to gateway.

As latency can be defined in various ways, a common description to be used during model creation is required. In this model, latency defines the total experienced by a data package from start to finish (sensing node to gateway) on a given graph path. Latency is therefore a summation of the total latency experienced by the data package on its graph path, the timeframe used will be milliseconds.

How is latency affected?

- Larger data packages, measured in number of bytes, negatively impact latency. Increase in package size directly correlates in increased latency. This is an expected result, as it takes more time to transmit larger data packages (Silicon Labs, 2018).

- Latency increases as the network increases. Larger networks have more connections which in turn result in more transmission between nodes, increasing latency.

- Interfering communications on public protocols can tamper or negatively impact latency. In public spaces and dense office environments these effects will be more prominent.

When measuring latency, it is also essential to describe the percentage of packages received. Ensuring all packages reach their destination is essential. In mesh networks, this communication is more complex, therefore measuring the number of packages received is essential to ensure proper operation of the network. Furthermore, this measurement gives an estimation of a network's reliability and fault tolerance/ robustness.

Shortly summarized, latency is the transfer time of a data package divided by the rate of transfer or throughput;

Maximum latency = data package size in bits / throughput

This formula provides a general calculation of the term latency. For IoT networks, this formula needs to be extended in order to properly discuss latency. Furthermore, latency in IoT networks cannot be described using a single measurement. Depending on network load and usage, latency could be negatively affected. This can not directly be combated, it, however, needs to be described. Based on this, a *BestCase (BC)* and *WorstCase (WC)* scenario for latency should be calculated.

Latency is described based on data transfer between two points in the network graph. The start and end point between which latency needs to be calculated must be elements of set V; v_{start} and v_{end}. Here, V can be either the full network, or a sub-net. Furthermore, there must exist a directed graph path in E between nodes, element of set V, such that v_{start} and v_{end} are connected. This implies that there exists a path (at least one) such that data can be transferred from v_{start} to v_{end}. For each node, the maximum (BC) and minimum (WC) latency must be specified. This is inherently dependent on the network architecture and the load per node.

$G = \langle V, E \rangle$

$v_{start}, v_{end} \in V$

$\{(v_{start}, v_1), (v_1, v_2), (v_2, v_n), \ldots, (v_n, v_{end})\} \in E$

Latency BC = summation BC latency $\forall v \in e \in E$

Latency WC = summation WC latency $\forall v \in e \in E$

Latency is a summation of latency in BC/ WC of all nodes present in the graph path between v_{start} *and* v_{end}*.*

Depending on the routing algorithm used, ideal graph paths for routing data could differ between IoT networks. This mostly affects the *BesteCase* scenario for latency calculation. For shortest path calculations for example, Dijkstra's Shortest Path First Algorithm and the A* algorithm are often utilized. In IoT networks, however, the shortest path is not always the path with the lowest latency, it is dependent on various other elements. If for example, one of the above stated algorithms is used, the shortest path does equal lowest latency.

Cost

An accurate estimation of costs to be incurred is critical to increase the chance of success of IoT projects. Cost is a highly complex characteristic, it does not affect a network performance directly, but does so indirectly. Once in place, a networks performance is not (significantly) affected by the cost characteristic. When designing a networks structural makeup, costs play a critical role. Quality of nodes, algorithms, communication protocols etc. influence how the system will perform.

These cost-based considerations in turn affect characteristics such as throughput, latency, number of hops and range. Cost itself is a summation of expenses like research and development, hardware cost, testing, licenses, installation, maintenance, and standard or proprietary technology used.

(Evdokimov, et al., 2019) have thoroughly described the cost analysis for Internet of Things projects in their paper; *A cost estimation approach for IoT projects*. First, is important to recognize that there is no single method to estimate costs. Analyst teams using different cost estimation approaches will have vastly different approximations of this characteristic. It is therefore impossible to give an exact cost estimation for an IoT project.

Seven criteria are defined to provide an accurate forecasting of the total costs. These criteria can highly influence the cost estimation. *Table 8* discusses the criteria.

	Name	**Definition**
1	Requirements analysis	Accurately define project requirements and make sure they are correct.
2	Specification of work	Lists task to implement, i.e. according to MoSCoW. What tasks can be excluded to reduce costs without harming the project?
3	Effective documentation	Important when managing (large) projects, associated costs are often overlooked.
4	Qualified employees	Project participants should posses the skills and knowledge to solve problems and complete work tasks effectively.
5	Planning and writing specifications	Define all project restrictions, any additional work can increase project costs.
6	Regular project reviews	Agile project development allows developers to take measures for changing customer requirements. Change can also result in going over-budget or schedule delays.
7	Choice of technology	The wrong choice of a technology is the primary factor for cost overruns. Additional costs should be estimated for learning new technologies.

Table 6: Cost estimation (Evdokimov, et al., 2019)

In their paper, (Evdokimov, et al., 2019) have created a cost estimation formula based on fitting a regression formula using historical project data in combination with the Use Case Points method and PERT method (Program Evaluation and Review Technique) used in software development. IoT projects can be seen as complex software development undertakings. The following formula is described:

$$E = (O + 4M + P) / 6$$

O: the most optimistic scenario (best case); *P*: the most pessimistic scenario (worst case); *M*: the most probable scenario.

Besides the cost estimation of development, the cost characteristic is mostly a summation of all cost contributing factors. Physical hardware such as gateways and sensors often have fixed prices per unit. For this, a simple summation would suffice to calculate its cost. Licenses can be one-time fees, or periodical payments.

Costs can again be separated in up-front or development cost, and maintenance and operational costs. To expand on this, hardware will only have to be purchased once, therefor this is an up-front cost. License costs and services (e.g. cloud storage) are among costs which are incurred once a system is up and running, this will be present during a system’s lifetime.

In terms of costs of an IoT network's physical elements, costs can be described as a summation of fixed price per element multiplied by the number of elements, this for each type of element part of the IoT network. Alternatively, depending on the IoT network, a base cost can be defined, consisting of prerequisite hardware like gateway(s) and backend data storage. For each node or connection added to the base system, the costs are increased with a fixed amount per unit.

$G = <V, E>$

$V = \{v^{VT}_1, v^{VT}_2, v^{VT}_3, \ldots, v^{VT}_n\}$

$E = \{e^{ET}_1, e^{ET}_2, e^{ET}_3, \ldots, e^{ET}_n\}$

$Network\ cost = \forall v \in V, \forall e \in E: (\$e^{ET} \in E * \#e^{ET} \in E) + (\$v^{VT} \in V * \#v^{VT} \in V)$

This simple description states that for all nodes v^{VT} element of V and all edges e^{ET} element of E, the cost is calculate by multiplying the cost per unit by the number of times that element appears in the network. All costs are added to give the total cost of the physical network.

Rather than calculating the total cost of the network. The description can be segmented in order to give the cost per element type, the cost on a sub-net or the costs on a given graph path. In the latter use case, a start and endpoint need to be defined, cost is then calculated over the nodes and edges on a given path from start to end. Similarly, as is done with latency.

Power consumption

IoT networks are in continuous operation, in mesh systems, three different modes can be distinguished for the system's nodes; active sensing, routing, and sleep. Mesh nodes usually feature these three modes or a variation thereof.

Several active power consuming elements can be identified in mesh systems; the sensing and routing nodes, and the gateway(s).

With simple IoT systems, low power node solutions often run on limited energy sources like batteries. These nodes remain in a deep sleep mode in order to save energy. The node is only active when sensing or transmitting information. Mesh solutions on the other hand present a more complex node functionality, nodes actively receive, transmit and route data. Nevertheless, battery powered mesh solutions are not out of the ordinary.

As the number of transmissions a node makes increases, so does its energy consumption (Nagabhushan, Shiva Prakash, & Krinkin, 2012). Depending on the routing algorithm used, energy consumption across nodes can me normalized. Energy efficient algorithms route data through nodes with enough energy. These algorithms result in equal degradation of battery life across a majority of (battery powered) nodes.

Power consumption is a summation of the total power consumption of all energy consuming actors in the mesh system. The unit of measurement can differ depending on the use-case of the network. For example, for battery powered devices, a measurement can be given in the total number of battery replacements per year (or other time period) per device. This definition is more informative compared to a technical definition in kWh.

A traditional calculation of power consumption can be given for all operating devices based on each device's usage (time active) and wattage:

Calculate watts per day		
1.	Say a system deploys 3 gateways consuming 800 watt each for 12 hours a day. This comes to a total of 3*800*12 = 28.800 watt-hours per day.	3 * 800 watts * 12 hours = **28.800 watt-hours**

Convert watt-hours to kWh		
2.	Electricity is measured in kWh, not in watt-hours. A kWh consists of 1000 watt-hours. Therefore, a simple division by 1000 of the watt-hours will provide the kWh.	28.800 watt-hours / 1000 = **28.8 kWh per day**

Convert to usage per month (or payment period)		
3.	The single day usage has to be converted to the time frame of the payment period. Usually this is 30 days (one month).	28.8 kWh * 30 days = **864 kWh per month**

Calculate cost		
4.	Electricity cost is calculated and payed in kWh usage. In this example we can assume an average cost of €0,20 per kWh. Costs differ per provider; besides this, the price of kWh can differ depending on the time of day. For an accurate calculation these factors must be considered.	864 kWh * €0,20 per kWh = **€172,80 per month**

Table 7: Power consumption calculation

In the example in *Table 7*, power consumption is calculated per payment period in kWh. Cost has also been included in this table as this would be the next natural step and provides more information of the effect of the power consumption cluster.

The formulas used in *Table 7* can be re-written into a single formula:

$$kWh\ per\ device = \frac{wattage * time\ operational * payment\ period}{1000}$$

Wattage in *watts,* time operational in *hours*, and payment period in *days*.

Using this generally accepted description of power consumption for all elements in an IoT network, allows a network to be analyzed and compared. kWh is universally recognized for the calculation of power consumption for most energy consuming devices.

As previously discussed, three node types and three edges types can be identified in IoT networks. Nodes will undisputedly be the most power consuming elements in a network. Communications over edges will consume significantly less power, these should nevertheless be accounted for, as frequent data exchanges do add up over time.

Let's assume power consumption will be calculated in kWh for all elements in the network. The total power consumption of all physical network elements identified in the network description is a summation of the total kWh per unit multiplied by the number of times the element appears in the network. kWh is calculated according to the formula stated above.

$G = <V, E>$

$V = \{v^{VT}_1, v^{VT}_2, v^{VT}_3, \ldots, v^{VT}_n\}$

$E = \{e^{ET}_1, e^{ET}_2, e^{ET}_3, \ldots, e^{ET}_n\}$

$Network\ cost = \forall v \in V, \forall e \in E: (kWhe^{ET} \in E * \#e^{ET} \in E) + (kWhv^{VT} \in V * \#v^{VT} \in V)$

This description, however, is not complete. Unlike with the cost characteristic, power consumption differs and increasing depending on the usage of each node or connection in the IoT network. The number of activations per element must be taken into account. There will most likely be several nodes and connections whose traffic is larger compared to others. These elements will undoubtedly consume more power.

$G = <V, E>$

$V = \{v^{VT}_1, v^{VT}_2, v^{VT}_3, \ldots, v^{VT}_n\}$

$E = \{e^{ET}_1, e^{ET}_2, e^{ET}_3, \ldots, e^{ET}_n\}$

$Network\ cost = \forall v \in V, \forall e \in E: ((kWhe^{ET} \in E * \#e^{ET} \in E) * \#activations\_\ e^{ET}) + ((kWhv^{VT} \in V * \#v^{VT} \in V) * \#activation\_\ v^{VT})$

For this description to be insightful, the number of activations per network element must be accurately tracked. With this information, the load on an IoT network can be thoroughly analyzed in order to identify bottlenecks for example.

6.4 Implications of the framework

The aim of this research was to develop an (analytical) descriptive tool for IoT *mesh* analysis. The literature study and qualitative analysis conducted in this study have focused heavily on this. Mesh is but one implementation of IoT systems. This topic has been touched upon at the start of the thesis. Because of this, only part of the identified CSF are specific to mesh systems. Several characteristics are defining for most, not only mesh, IoT networks. Furthermore, depending on the wide definition of a characteristic, part of the description might no longer apply for non-mesh IoT networks. Distributivity is one example; both mesh and non-mesh systems can possess the distributivity characteristic. It, however, applied differently to the system based on its type. In mesh systems, distributivity is mostly defined in the network's inherent capability for nodes to communicate and parse information which in turn allows the network to be distributed over a large physical area. For non-mesh systems, distributivity is still relevant, however, often achieved to a lesser end and through other means.

Based on the findings in this research, a subset of the CSF can be used to analyze other types of non-mesh IoT networks. The subset of characteristics is highly dependent on the underlying architecture of the network and its use-case.

7. Discussion

Part of this research paper was conducted under guidance and with assistance of Capgemini's Applied Innovation Exchange and its employees. The interviewees are experienced employees working on networking related projects. Unfortunately, a limited number of interviews were conducted during the scope of this project as result of a limited number of available participants.

If a larger set of experts were to be interviews during the project, this would result in a more thorough analysis and a more insightful data set. Internal consistencies could for example be more easily identified if the number of interviewees were larger. Besides this, more unknown unknowns could have been found. This does not, however, diminish the usefulness of the interviews conducted during the thesis project and the data extracted from the interviews. The interviewees part of this research project are business professionals with deep knowledge and experience.

The project used in this paper; Capgemini's SmartOffice project, is one in-house developed by Capgemini for Capgemini. At the moment, it is the sole IoT project being developed and build by Capgemini's AIE, all resources are invested in this project. This is the reason the SmartOffice project is the only project referred to and used in this thesis. If other projects, ongoing or past, were available, it would allow the researcher to create a comparative analysis between the project in order to more thoroughly test and refine the framework. This, however, opens up the possibility for future study.

The collaboration with Capgemini obviously affects the thesis, this has been the most variable factor in this research. All resources used are Capgemini-related. If the project was conducted independently or with assistance of another corporation, results could have differed. The information provision was provided by industry experts, it is therefore safe to assume results would have only been marginally different. The examples, projects and list of characteristics (to some extent) would, however, have been different. This, since these elements are almost directly related to Capgemini in some form.

The list of 16 CSF is constructed based on a combination of literature study and interviews. The majority of characteristics have been identified during literature study, this initial list was expanded on and refined by expert interviews. Independent of the research method used, the list of characteristics constructed solely as result of literature study would have been the same.

Furthermore, the descriptive framework has displayed its use for the SmartOffice project use case. Stress testing the CSF over different projects and use cases in would allow the researcher to identify gaps or possible shortcomings.

8. Conclusions

8.1 Conclusion on results

This research project has resulted in a list of 16 CSF, characteristics find their base in literature study and qualitative research. Using the Capgemini SmartOffice project as use case, the 16 CSF have been used posteriori in order to analyze the project and its effects on the characteristics. Besides the posteriori approach used, the CSF can also be used a priori. During project development, the CSF can be used as a checklist for developers and project stakeholders to ensure the key IoT network elements are properly addressed. Furthermore, the CSF can be used as starting point during network design.

During framework development, a general network description notation is given. One which can be used to describe, compare and analyze IoT networks. The network description finds its base in graph theory; nodes and connections are represented as vertices and edges. In this description, three different node and connection types are identified and discussed. The network description is also directly linked to the 16 CSF, the characteristics are described as attributes of nodes, edges or the full network.

Lastly, the analytical capabilities of the CSF are discussed. The characteristics are clustered based on their dependencies on one another. The clustering of the characteristics allows for the creation of an analytical framework which is easier to use and more insightful. The final clustering consists of ten characteristical clusters. Several clusters are quantifiable a priori, out of the clusters which can be quantified, three have been chosen to further develop to display the analytical use of the clustered framework. The characteristics latency, cost and power consumption have been further explored. In its analytical description, the relation between the cluster and graph network description is given. For each of the three clusters, the calculation of its description is described using the graph network elements.

8.2 Recommendations for further study

The research conducted in this study has focused on the identification of 16 CSF for IoT *mesh* network development. Mesh is but one implementation of IoT networks. Because of this, only part of the identified CSF are specific to mesh systems. Several characteristics are defining for most, not only mesh, IoT networks. One recommendation for further study would be the expansion and further development of the framework and its characteristics in regard to other IoT network architectures and implementations. This would yield several CSF and frameworks specific to IoT network types.

Another recommendation would be the refinement of the framework using a comparative analysis of various IoT projects using the 16 characteristics as base for analysis. This would allow the researcher to identify gaps or shortcoming of the framework if present.

Lastly, an initial step has been made towards the development of the analytical description of the clustered characteristics. Further research could be done towards the analysis of the other characteristical clusters.

Alternatively, the network description and clustered framework could potentially be digitalized. A python-based tool could for example be useful for automated analysis of IoT networks.

Bibliography

Abdmeziem, M., Tandjaoui, D., & Romdhani, I. (2016). Architecting the Internet of Things: State of the Art. *Robots and Sensor Clouds*, 55 - 75.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Elsevier*. Retrieved from https://www.cs.mun.ca/courses/cs6908/IoT-Survey-Atzori-2010.pdf

Baker, S., Xiang, W., & Atkinson, I. (2017). Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access*. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8124196

Bor, M., Vidler, J., & Roedig, U. (2016). *LoRa for the Internet of Things.* Graz, Austria: International Conference on Embedded Wireless Systems and Networks . Retrieved from https://www.researchgate.net/profile/John_Vidler2/publication/297731094_LoRa_for_the_Internet_of_Things/links/56e1893e08ae4bb9771ba9e3/LoRa-for-the-Internet-of-Things.pdf

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 77 - 101. Retrieved from https://www.tandfonline.com/doi/pdf/10.1191/1478088706qp063oa

Bryman, A., & Bell, E. (2007). *Business Research Methods.* Oxford: Oxford University Press. Retrieved from https://www.researchgate.net/profile/Yousef_Shahwan4/post/What_is_the_best_and_the_most_recent_book_in_medical_research_methodology/attachment/59d6525179197b80779aa90f/AS%3A511717807321088%401499014441133/download/Social+Research+Methods.pdf

Draves, R., Padhye, j., & Zill, B. (2004). Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks. *Proceedings of the 10th annual international conference on Mobile computing and networking*, 114 -128. Retrieved from https://www.cs.montana.edu/courses/spring2009/541/Ref/Draves-MobiCom04.pdf

Evdokimov, I. V., Alalwan, A. R., Tsarev, R. Y., Yamskikh, T. N., Tsareva, O. A., & Pupkov, A. N. (2019, March). A cost estimation approach for IoT projects. *Journal of Physics: Conference Series*. Retrieved from https://www.researchgate.net/publication/331902254_A_cost_estimation_approach_for_IoT_projects

GDPR EU. (2019). *Complete guide to GDPR compliance*. Retrieved from GDPR.EU.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswamia, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future generation computer systems*, 1645 - 1660. Retrieved from https://arxiv.org/ftp/arxiv/papers/1207/1207.0203.pdf

Gumel, M., & Faruk, N. (2012). *WIRELESS MESH NETWORKS THROUGHPUT CAPACITY ANALYSIS.* Ilorin, Nigeria: NJTD. Retrieved from https://www.researchgate.net/publication/295403088_WIRELESS_MESH_NETWORKS_THROUGHPUT_CAPACITY_ANALYSIS

Gupta, A., Christie, R., & Manjula, R. (2017). Scalability in Internet of Things: Features, Techniques and Research Challenges. *International Journal of Computational Intelligence Research*, 1617 - 1627. Retrieved from https://www.ripublication.com/ijcir17/ijcirv13n7_06.pdf

Hunke, N., Yusuf, Z., Rüßmann, M., Schmieg, F., Bhatia, A., & Kalra, N. (2017). *Winning in IoT: It's All About the Business Processes.* BCG Henderson Institute. Retrieved from https://www.bcg.com/publications/2017/hardware-software-energy-environment-winning-in-iot-all-about-winning-processes.aspx

Internet Society. (2015). *The Internet of Things: An Overview*.

Klubnikin, A. (2016, 10 12). *Internet of Things: How Much Does it Cost to Build IoT Solution?* Retrieved from R-Style Lab: https://r-stylelab.com/company/blog/iot/internet-of-things-how-much-does-it-cost-to-build-iot-solution

Lee, J., Su, Y., & Shen, C. (2007). A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. *The 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON)*, 46 - 51. Retrieved from http://eee.guc.edu.eg/Announcements/Comparaitive_Wireless_Standards.pdf

LoRa Alliance. (2019). *Wi-Fi & LoRaWAN® Deployment Synergies.* Retrieved from https://lora-alliance.org/sites/default/files/2019-09/wi-fi_and_lorawanr_deployment_synergies_0.pdf

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature. *Journal of Computer and Communications*, 164 - 173. Retrieved from https://file.scirp.org/pdf/JCC_2015052516013923.pdf

Mahmoud, M., & Mohamad, A. (2016). A Study of Efficient Power Consumption Wireless Communication Techniques/ Modules for Internet of Things (IoT) Applications. *Advances in Internet of Things*, 19 -29. Retrieved from http://repository.embuni.ac.ke/bitstream/handle/123456789/825/IoT.pdf?sequence=3

MeshDynamics. (2003 -2005). *Performance Analysis of Three Competing Mesh Network Architectures*. Retrieved from MeshDynamics: https://www.meshdynamics.com/performance-analysis.html

Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Intenet of Things (IoT). *IEEE Internet Initiative*.

Muthu Ramya, C., Shanmugaraj, M., & Prabakaran, R. (2011). Study on Zigbee Technology. *Electronics Computer Technology (ICECT)*, 297 - 301. Retrieved from https://www.researchgate.net/publication/261497749_Study_on_ZigBee_technology

Nagabhushan, T. N., Shiva Prakash, S. P., & Krinkin, K. (2012). *Power-saving Routing Algorithms in Wireless Mesh Networks: a Survey.* Retrieved from https://www.researchgate.net/publication/235324694_Power-saving_Routing_Algorithms_inWireless_Mesh_Networks_a_Survey

Patel, K., & Patel, S. (2016). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. *IJESC*. Retrieved from http://ijesc.org/upload/8e9af2eca2e1119b895544fd60c3b857.Internet%20of%20Things-IOT%20Definition,%20Characteristics,%20Architecture,%20Enabling%20Technologies,%20Application%20&%20Future%20Challenges.pdf

Roman, R., Najera, P., & Lopez, J. (n.d.). *Securing the Internet of Things.* Malaga: University of Malaga, Spain. Retrieved from https://www.nics.uma.es/sites/default/files/papers/1633.pdf

Sethi, P., & Sarangi, S. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, 1 - 25. Retrieved from https://www.researchgate.net/publication/312957467_Internet_of_Things_Architectures_Protocols_and_Applications

Sichitiu, M. (2019). *Wireless mesh networking: oppotunities and challanges.* Retrieved from https://www.researchgate.net/publication/228525550_Wireless_mesh_networks_opportunities_and_challenges

Silicon Labs. (2018). *AN1138: Zigbee Mesh Network Performance.* Austin, TX. Retrieved from https://www.silabs.com/documents/login/application-notes/an1138-zigbee-mesh-network-performance.pdf

Soliman, M., Abiodun, T., Hamouda, T., Zhou, J., & Lung, C. (2013). Smart Home: Integrating Internet of Things with Web Services and Cloud Computing. *IEEE International Conference on Cloud Computing Technology and Science*, 317 - 320. Retrieved from https://cs.uwaterloo.ca/~brecht/courses/854-IoT-2016/readings/smart-home/smart-home-integrating-web-and-cloud-iccts-2013.pdf

Strengers, Y., & Nicholls, L. (2017, October). Convenience and energy consumption in the smart home of the future: Industry visions from Australia and beyond. *Energy Research & Social Science - Elsevier*, 86 - 93. Retrieved from https://www.sciencedirect.com/science/article/pii/S221462961730049X

Strixsystems. (2005). *Solving the Wireless Mesh Multi-Hop Dilemma.* Retrieved from http://www.strixsystems.com/products/datasheets/StrixWhitepaper_Multihop.pdf

Templier, M., & Paré, G. (2015). A Framework for Guiding and Evaluating Literature Reviews. *Communications of the Association for Information Systems*, 112 - 137. Retrieved from https://www.researchgate.net/publication/281465222_A_Framework_for_Guiding_and_Evaluating_Literature_Reviews

Tracy, P. (2016, 10 17). *Network topology guide for the internet of things*. Retrieved from RCRWirelessn: https://www.rcrwireless.com/20161017/big-data-analytics/network-topology-guide-tag31-tag99

Turcu, C., & Turcu, C. (2013). Internet of Things as Key Enabler for Sustainable Healthcare Delivery. *SciVerse ScienceDirect*, 251 - 256.

Uckelmann, D., Harrison, M., & Michahelles, F. (2011). *An Architectural Approach Towards the Future Internet of Things.* Springer-Verlag Berlin Heidelberg. Retrieved from https://s3.amazonaws.com/academia.edu.documents/35276741/An_Architectural_Approach_Towards_the_Future_Internet_of_Things.pdf?response-content-disposition=inline%3B%20filename%3DAn_Architectural_Approach_Towards_the_Fu.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&

Want, R., Schilit, B., & Jenson, S. (2015). *Enabling the Internet of Things.* IEEE Computer Society. Retrieved from http://www.roywant.com/cv/papers/pubs/2015-01%20(IEEE%20Computer)%20Enabling%20the%20Internet%20of%20Things.pdf

Webster, J., & Watson, R. (2002). Analyzing the past to prepare for the future: writing a literature review. *Management Information Systems Quarterly*. Retrieved from https://web.njit.edu/~egan/Writing_A_Literature_Review.pdf

Xu, L., He, W., & Li, S. (2014). Internet of Things in Industries: A Survey. *IEEE Transactions on Industrion Informatics*. Retrieved from https://www.researchgate.net/profile/Wu_He2/publication/270742269_Internet_of_Things_in_Industries_A_Survey/links/55fc355a08aec948c4b189f6/Internet-of-Things-in-Industries-A-Survey.pdf

YE, N., Zhu, Y., Wang, R., Malekian, R., & Qiao-min, L. (2014). An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things. *Applied Mathematics & Information Sciences*, 1 - 8. Retrieved from https://www.researchgate.net/profile/Reza_Malekian2/publication/258509303_An_Efficient_Authentication_and_Access_Control_Scheme_for_Perception_Layer_of_Internet_of_Things/links/0c96052866620bf70a000000.pdf

Appendices

Appendix A – Interview email

Interviews were held with native Dutch speaking individuals; therefore, mails send to potential interviewees were also in Dutch. Emails send to participants followed the following structure (with slight alterations depending on the participant):

Beste meneer/ mevrouw *[insert name]*,

Ik mail u op advies van mijn begeleider Peter Paul Tonen, mij is verteld dat uw expertise een bijdrage kan leveren aan het project waar ik op dit moment mee bezig ben, middels deze mail wil ik bekijken of de mogelijkheid bestaat om eens een uurtje met u in te plannen voor een interview (hier volgt zometeen iets meer over). Eerst even in het kort iets over mijzelf, mijn naam is Nieradj Gopal, ik ben een tweede jaars master ICT in Business student aan de Universiteit Leiden. Op dit moment ben ik bezig met mijn afstudeerscriptie waarbij ik onderzoek doet naar het gebruik van mesh netwerken voor het Internet of Things, dit onderzoek doe ik bij van het Applied Innovation Exchange.

Het doel van mijn onderzoek is het creeren van een model welk gebruikt kan worden om mesh implementaties te beoordelen en analyseren. Dit model kijkt naar een aantal karakteristieken welk vaak geassocieerd worden met IoT netwerken (denk hier bijvoorbeeld aan latency, throughput, data size, etc.). Uiteindelijk zou dit model een mesh implementatie of prototype moeten kunnen beoordelen en aangeven hoe de implementatie presteert, en of deze voldoet aan een zet van functionele eisen (bijvoorbeeld; voldoet deze aan een latency eis gezet door de client).

Tot zo ver heb ik enkel onderzoek gedaan naar deze aspecten vanuit beschikbare literatuur. Vaak is het echter zo dat literatuur en de werkelijkheid niet perfect op elkaar aansluiten. Dit is waar ik uw hulp nodig heb! Graag zou ik een keer met u een onder een kop koffie een interview willen houden om de lijst van karakteristieken welk ik gebruik om mesh netwerken te beoordelen te verfijnen of uitbreiden, gebaseerd op uw kennis en ervaring, en in het algemeen meer te weten willen komen hoe IoT georienteerde projecten eruit zien en verlopen binnen Capgemini. Ook zou ik graag enkele implementaties of projecten vanuit Capgemini willen gebruiken voor mijn onderzoek. Indien mogelijk zou ik ook dit graag met u bespreken.

In de bijlage vind u mijn project verzoek, deze geeft in het kort weer wat het doel is van het onderzoeksproject. Deze is niet noodzakelijk om door te lezen voor een eventueel interview en heb ik uitsluitend toegevoegd als extra informatie voorziening.

Graag hoor ik of u beschikbaar bent voor een interview. Indien u niet beschikbaar bent vind ik dit erg jammer, maar verzoek ik u dit mij ook te laten weten middels een reactie op deze mail. Als u nog eventuele vragen heeft, kunt u mij altijd telefonisch of via de mail bereiken. Helaas is mijn beschikbaarheid iets gelimiteerd, ik ben wekelijks de hele dag beschikbaar op enkel maandag, dinsdag en donderdag. Indien het voor u uitkomt hoor ik graag of u in de komende weken op een van deze dagen een gesprek met mij zou willen aangaan.

Bij voorbaat bedankt voor uw medewerking.

Nieradj Gopal
06-29767455
Nieradj.gopal@capgemini.com

Appendix B – Interview questions

The interviews will cover, but not be limited to the following questions, variations, or subsets thereof:

1. What is your educational and professional background?
2. What position do you currently hold at Capgemini?
3. What tasks do you perform in this function? Is this on a daily/ weekly basis?
4. How experienced are you with the Internet of Things? (Number of projects partaken, years of experience, etc.)
5. How often have you worked on IoT projects that use some form of mesh, or looked at mesh as a possible solution?
6. From a high-level perspective, what does the process of designing an IoT solution look like from inception to delivery?
7. For what types of problems do clients often seek IoT solutions? Or is it more often the case that an IoT solution is proposed for a given problem?
8. How would you define a mesh network for IoT?
9. Have you worked with mesh before (not necessarily in IoT but more so in general)?
10. If so, for what type of projects was mesh used as an implementation method?
11. *Direct feedback on the list:* do you thinks these characteristics are relevant for IoT projects, specifically mesh IoT projects? *Each characteristic is explained to the interviewee, to have a common understanding.*
12. Are there any characteristics you would leave out? Or are there any characteristics that you would like to add to this list?
13. From a client perspective, what characteristics would be most important? Or how does importance on these characteristics differ depending on the use-case?
14. How would you define a successful mesh solution (either as client or developer)?
15. From your experience, to what extend is the client concerned with a proposed implementation topology (e.g. mesh, start, ring)?
16. From your experience, how knowledgeable are clients with IoT? How does this affect the collaboration between the client and Capgemini?
17. What characteristics/ aspects of a project do you focus on to ensure a successful customer delivery?
18. What are alternative implementation methods to mesh?
19. What are the advantages of using mesh over other types of network topologies?
20. What are the disadvantages of using mesh over other types of network topologies?
21. What is in your opinion the difference between a good/ successful and a less successful mesh implementation? Why is that?
22. How are IoT implementations analyzed at Capgemini? How do developers ensure that suggested implementations meet client requirements?
23. Is there a preferred network topology which is often used, or does this depend on the on the problem/ use-case?

24. Can you create a ranking of the characteristics from defined list? Once from a client perspective, once from a developer's perspective.

The questions described provide a guideline of topics which need to be discussed during the interview