Communication Technologies for Smart Objects

Ubiquitous computing seminar FS2014
Student report

Dominik Kovacs
ETH Zurich
dkovacs@student.ethz.ch

ABSTRACT

Today the world is overwhelmed by a load of different wireless communication technologies. The concept of interconnecting the things around us into a network raises the question about which communication technologies to use for a specific domain. This paper gives an overview over common wireless communication technologies and how to use them to connect smart objects in different application domains. It summarizes the characteristics and requirements on the communication and finally compares the technologies to each other and classifies them. It comes to the conclusion that no single technology *dominates others*.

Keywords: Internet of Things, Smart Objects, Wireless Communication.

1. INTRODUCTION

The Internet of Things (IoT), a term that is constantly gaining in importance, is a vision of interconnecting the *things* (from now on referred as *smart objects*) around us in order to create smart environments. For example, having a smart garbage collection system in a city[1]. The garbage cans, equipped with sensors, would automatically send their capacities to a central garbage collection facility, where based on those fill levels the next garbage collection route will be generated. This does increase the efficiency and saves time, fuel and money.

From a general point of view all IoT applications can be modelled as follows. They consist of two main components:

- **Smart objects**, which are equipped with sensors and/or actuators, whose main task is to *sense* and/or *change* the environment.
- An **Aggregator**, which collects the data from the smart objects, processes and sends them either back to the smart objects or to a higher level network. The Aggregator can be in the near vicinity of its smart objects or be located on the other side of the Internet.

In order to connect these two components, a reliable **communication network** is needed which will be the focus of this paper. Said communication networks seem to be the bottleneck in developing IoT systems. This is hard to believe since numerous milestones necessary for the vision of IoT have already been achieved: Over the last couple of decades, computers have become smaller and smaller. Thanks to improved battery technology, they can be placed at almost every location and due to progression in radio technology they are able to communicate at an even higher bandwidth over an even larger distance than before. All this development fosters the vision of the Internet of Things. The reason said vision has not already been established, is mainly due to the lack of interoperability. Having one technology only would solve this problem.

This paper is organized as follows. Section 2 briefly summarizes the different types of communication. Section 3 gives a short introduction into wireless technology along with the additional difficulties that come with it. Section 4, the main focus of this paper, goes over the five main application domains and compares existing wireless technologies. Section 5 concludes this paper.

2. TYPES OF COMMUNICATION

Communication, which comes from the Latin word *commūnicāre* (*to share*), is a form of exchanging information. In the vision of IoT information is mainly exchanged between two machines. Using machines for sharing information, there are the following three main concepts with regard to the *start and end-point* of the communication:

- **Human-to-Human (H2H)** This is the most natural form of communication. For instance, a conversation on the spot, on the phone or in writing (messages, postcards). Regardless the use of a machine (e.g., a telephone or a postal sorting machine) this information starts and ends with a human being.
- **Human-to-Machine (H2M)** The machine replaces either the start or the end of the communication. For Example, the authorization of ATM machines, GPS systems, traffic lights or lie detectors.
- **Machine-to-Machine (M2M)** This type of communication does not involve any humans. The reason for communication is usually an event, generated by a sensor or a timer. For instance, the automatic download of an eBook from the server to the tablet, which consists of two subprocesses. In a first step the user establishes connection to the eBook webserver, authorizing the payment process (H2M). The eBook webserver then initiates a communication with the tablet, managing the download of the paid eBook (M2M) [2]. Another example for M2M would be vending machines informing the distribution terminal (a machine hence M2M) when a particular item is out of stock. The distribution terminal would inform the local delivery services on duty (M2H) for initiating the restock.

[1] BigBelly Solar: `http://bigbellysolar.com`, Accessed: 2014-05-20

IoT vs M2M

Recently there has been some confusion about the terms IoT and M2M. They would be used interchangeably although they actually mean two different concepts.

- **M2M** is about connecting different machines to each other, which has been existing for a couple of decades already. One of the first M2M application was the *Identify Friend or Foe (IFF)* during World War 2[2]. The term M2M become widely popular later on in time when telecommunication companies started to put SIM cards into their devices so that they could communicate to each other.
- **IoT** on the other hand is much more than just about connecting devices. It is a more abstract concept. It is a vision about using said M2M connectivity to create smart environments. Therefore M2M can be seen as a subset of IoT.

3. WIRELESS TECHNOLOGY

Smart objects cannot realistically be wired up to each other, it would be too expensive, too inconvenient, too immobile, sometimes even impossible. For all these reasons the wireless technology becomes vital; therefore this paper focuses on it.

Implementation Differences

Referring to the Open Systems Interconnection (OSI) [10] model, the main differences in terms of implementation between wireless and wired networks take place in the first two layers:

- The first layer, the physical layer (PHY), handles the communication of information by radio waves (instead of moving electrons through wires).
- The second layer, the data link layer (MAC), detects and possibly corrects errors in the transmission process. Especially in wireless communications, this layer becomes much more sophisticated since the transmission passes through a commonly shared medium (the air).

A Limited Resource

Wireless technologies transmit their information through radio waves. The radio wave spectrum, which is part of the electromagnetic spectrum, is ranged between 3 KHz and 300 GHz. A radio wave can be characterised by its frequency, amplitude and phase offset. The most severe problem that wireless communication has to cope with is **interference**. Two radio waves, with the same or nearly the same frequency, add up their amplitudes, which means an increase or a neutralisation (see Figure 1 on the right). An interference usually causes the alteration of the waves, which can lead to packet losses, a decrease of the strength of a signal or a considerable loss of the bandwidth. One way to prevent such interferences, is to multiplex the signals. The following four methods are commonly used in combination with wireless signals:

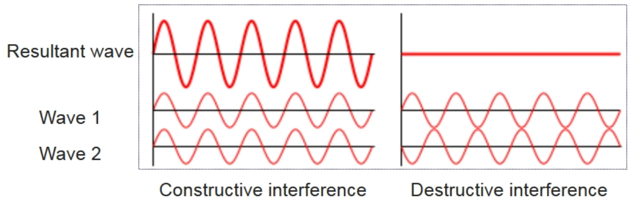

Figure 1: Superposition principle

- **Space-division multiplexing**: The easiest way to prevent interference, without altering the signals frequency, is to ensure that no radio wave is in the range of others. The range of radio waves depend on the transmission power.
- **Frequency multiplexing**: If such a space-division cannot be achieved and the radio waves are operating in the same environment, then they have to use different frequencies in order not to interfere with others.
- **Time division multiplexing**: If devices operate within the same network (where they all have the same *coordinator*) then the same frequency can be used by coordinating the transmissions into different time windows.
- **Code division multiplexing**: If devices do not operate within the same network then different *pseudorandom codes* can be used to encode information. This enables multiple users transmitting on the same frequencies.

Despite those promising-seeming multiplexing methods, it is still a huge challenge to allocate frequencies for certain tasks. Even though each country has its own regulation authority (in the US: the Federal Communications Commission (FCC), in Switzerland: the Bundesamt für Kommunikation (BAKOM)), there are globally regulated frequency bands, one of them is the **Industrial, scientific and medical (ISM) band** (see Table 1 on page 2). Those are frequencies that were originally reserved for industrial, scientific and medical purposes only, but were opened-up for the public. They are now free to use except in the near vicinity of industrial, scientific and medical buildings (such as hospitals). The most common ISM band is the 2.4 GHz band, on which a lot of commonly used mobile and household devices operate, such as smartphones (Wi-Fi or Bluetooth), microwaves and ovens.

Frequency Range		Availability
6.765 MHz	6.795 MHz	∗
13.553 MHz	13.567 MHz	Worldwide
26.957 MHz	27.283 MHz	Worldwide
40.660 MHz	40.700 MHz	Worldwide
433.050 MHz	434.790 MHz	Region 1 only and ∗
902.000 MHz	928.000 MHz	Region 2 only
2.400 GHz	**2.500 GHz**	**Worldwide**
5.725 GHz	5.875 GHz	Worldwide
24.000 GHz	24.250 GHz	Worldwide
61.000 GHz	61.500 GHz	∗
122.000 GHz	123.000 GHz	∗
244.000 GHz	246.000 GHz	∗

Table 1: ISM Bands (International Telecommunication Union. Page on definitions of ISM bands: `http://www.itu.int/ITU-R/terrestrial/faq/index.html#g013`, Accessed: 2014-05-20), (∗ Subject to local acceptance)

4. APPLICATION DOMAINS

Nowadays there is a plethora of wireless technologies (see Table 2 on page 8). One way to bring some order into chaos

[2] US Army Air Defense Digest, 1972 `http://ed-thelen.org/72digest1.html`, Accessed: 2014-05-20

is to arrange them based on their data rate and range (see Figure 7 on page 7). It would not make much sense to compare a long-range technology (such as LTE) with an ultra-short-range technology (such as NFC), because they are used in two completely different types of applications. Therefore the technologies are classified based on the application domains, that they are commonly used in, and will be discussed further in their specific domain.

Throughout the different application domains, the structure is organized as follows. First the application domain must be introduced. Then the typical characteristics of said domain are presented, followed by the implications on the communication requirements. Lastly, the different technologies fulfilling all those requirements are compared to each other.

4.1 Body Area Network

A Body Area Network (BAN) is a network consisting of smart objects, which are placed on or inside the human body communicating with an aggregator (e.g., a smartphone, see Figure 2 on the top right). The purpose of this network is to gather information about the human body for the sake of other services. For example, monitoring the heart rate and alerting the nearest hospital in case of a heart attack. BAN devices can be worn (wearables, such as smart glasses, smart watches, sensors on clothes or on the skin). The most common implant is the Smart Pacemaker which is an evolution of the traditional pacemaker delivering vital information (by a base station at home) to the nearest hospital[3].

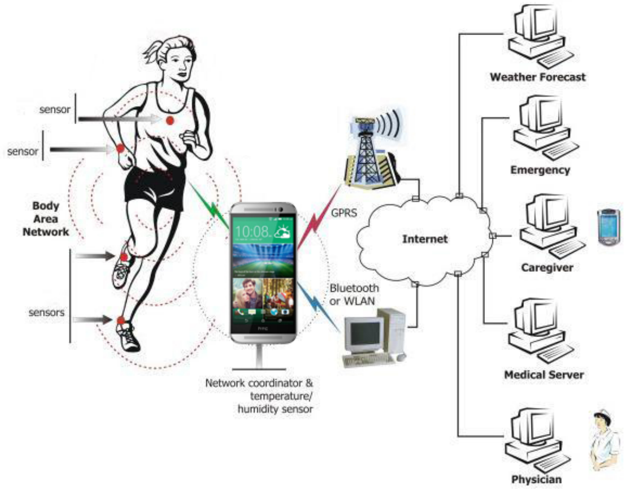

Figure 2: Body Area Network

Characteristics First of all, BAN devices usually have **low CPU power** because their prime task is to collect rather than to process information. Since a BAN operates around a human, which as a carrier of BAN devices is rather mobile than stationary, all those devices have to rely on **battery power**. As implants require small-sized batteries, BAN devices need to operate in a **low power**-mode in order to perform on any useful long-term application. Furthermore there usually is **no line of sight** between several BAN devices, because the human body and/or cloths are blocking the sight. Last but not least, the most important characteristic about BAN devices is that they **can be health critical**.

Communication Requirements As already stated, the communication needs to be **power efficient**. In order to provide a reliable communication, especially when running a health critical application, such as in a smart pacemaker, it needs to be **robust against** any kind of **interference**: [3][8]

- **Off-body interference** (see Figure 3 below) is the interference between devices of different BANs. It can be massively reduced by using communication technologies of limited ranges.
- **On-body interference** is the interference between devices of the same BAN. Since all smart objects of the same BAN use the same aggregator (coordinator), time division multiplexing can be used to prevent interference.

The last requirement is **interoperability**. Wearables are not to be bought from the same vendor, this would result in a **vendor lock-in**, which means being dependent on only one vendor. Buying further or replacing products from other vendors would simply not comply with the existing ones. If for example the vendor goes bankrupt and his application services cannot be purchased anymore, the continuance, the innovation of his products and their full functionalities will stop. Vendor lock-in means the total dictation of his prices and conditions which is especially critical with regard to privacy.

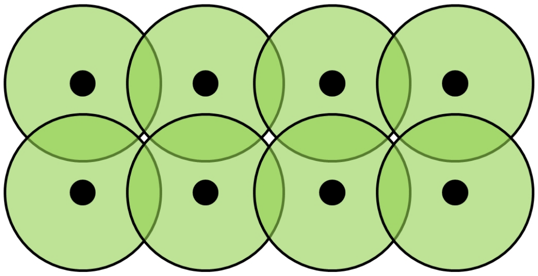

Figure 3: Off-body interference, the center of the circles stands for human carriers and the green circles mark the range of their BANs. Interception of circles mean interference.

Communication Technologies Due to the possible off-body interference and the lack of low-power communication, when using medium to long-range communication technologies, one is limited with the low-range sector. Technologies in that range are shown in Table 2 on page 8, Category 1.
Starting with implants, the most health-critical application in the BAN area, **Zarlink** is the best option. Despite being proprietary, it is the only technology especially developed for implants. Even though not fulfilling the interoperability requirement, and most likely causing a vendor lock-in, it is a special case because of the following reasons: First of all, it covers a very specific application area. Second, it is less likely to cause off-body interference due to operating in a lower and less crowded frequency area. Third, before im-

[3] Smart Pacemaker by Medtronic: http://healthbleep.magnify.net/video/Medtronic-leadless-pacemaker-wi, Accessed: 2014-05-20

planting anything, one is in intense dialog with a hospital. Nobody just goes to a local implant store, buys the implant, injects it and expects it to interoperate with the existing BAN. Last and most importantly, for health critical implants, it is vital to have a reliable (and possibly separate) connection to the hospital (through an extra aggregator), than being compatible with a smartphone as the main BAN aggregator.

Regarding wearables, there are a couple of technologies worth considering: [3][4][8]

- **Sensium** is a proprietary technology, which operates on a less crowded 868 MHz and 915 MHz ISM, offering a data rate up to 50 Kbit/s and a range of 5m. Due to its limited data rate it can only be used for low-bandwidth applications.
- **Bluetooth/BLE (Bluetooth Low Energy)**, one of the most established standards (IEEE 802.15.1), operates on the crowded 2.4 GHz ISM band, offering a data rate up to 1 Mbit/s and a range of 10m. Due to being supported by almost every smartphone in the market, it is predestined to be used with a smartphone-aggregator. Because of its high data rate it can support high-bandwidth applications. Its frequency hopping feature, unique in each piconet, can effectively withstand the chance of off-body interference.
- **Ultra Wideband (UWB)** is based on several standards but not very well established, it operates on higher and less crowded 3.1 - 10.6 GHz frequencies, offering a data rate of 110 Mbit/s (which is the highest among here) and a range of 10m. Even though it has a by far higher data rate than Bluetooth/BLE, it cannot be easily used in conjunction with nowadays smartphones, which is why it is not the prime choice when it comes to wearables.
- **ANT**, a proprietary technology, operates on the crowded 2.4 GHz ISM band, offering a data rate up to 1 Mbit/s and the widest range of all of 30m. Due to its operating frequency and range, it is likely to cause off-body interference. Apart from that, due to its high data rate, it is able to support high-bandwidth applications.

Even though Bluetooth/BLE seems to be the perfect ”candidate” for wearables right now, when it comes to implants, proprietary technologies still have to be given priority. It seems, at least for the BAN area, no technology can dominate them all.

4.2 Smart Home

Smart Home is the vision for the future. For a couple of years, the market has been flooded by the term *Home Automation*, which is all about remote controlling the home, such as pre-heating the oven on the way home or checking on the condition of the home from outside. Smart Home offers much more. The above-mentioned Home Automation heavily relies on a human factor interacting whereas the vision of Smart Home focuses on M2M communication managing the home itself. For instance, the gardening area where sensor plants monitor the moistness of the soil (and much more); it would initiate the sprinkler to turn on the water as soon as a certain threshold, in terms of the soil becoming to dry, has been reached (see Figure 4 above). Another example would be a smart fridge which automatically reports missing items to the grocery delivery service.

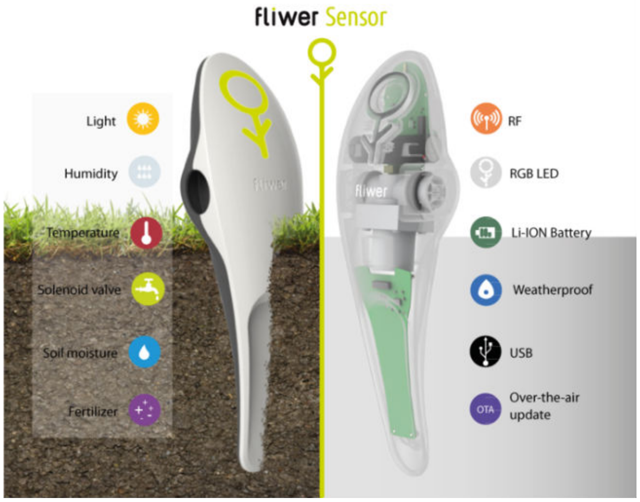

Figure 4: Example of Smart Gardening as part of Smart Home (Fliwer Sensor http://www.fliwer.com, Accessed: 2014-05-20)

Characteristics In contrast to BANs, Smart Homes are fairly **stationary** most of the time (except moving the home). Despite that most objects in a Smart Home could be wired up, most devices still rely on **battery power**, cost and ease-of-use. Since a Smart Home relies on a huge quantity of sensors, **the cost per device** becomes usually very **low**. For this reason numerous sensors for the whole garden can easily be afforded. Same as with BANs, there is **no line of sight** because of walls. There is also a huge **variety of applications** in and around the home.

Communication Requirements Having moved on from BAN to Smart Home, the scale increases. To cover an entire home, technologies with a **sufficient range** are needed. Having a huge variety of applications also requires the **bandwidth** to be **variable**. A multimedia streaming application, for instance, needs a bandwidth in the Mbits whereas a plant sensor informs the aggregator device that the soil has become dry; it only needs to flip one bit. In terms of **interoperability** the same argument can be given as with BANs. One wants to easily buy devices from different vendors and lets them flawlessly connect and communicate to each other.

Communication Technologies Due to the extended range, technologies with slightly longer ranges have to be considered. On the other side, technologies with an insufficient range such as Sensium, Bluetooth/BLE and UWB have to be omitted (again, see Table 2 on page 8, Category 2). Even though, **Z-wave**, a proprietary technology, having an astonishing range of 300m, cannot be included in the final comparison due to its chips being only available from one source, Sigma Designs[4], thus causing the already discussed vendor lock-in problem. Therefore 6 technologies remain for further comparisons: [8]

[4] L. Frenzel. What is the Difference Between ZigBee and Z-Wave? http://electronicdesign.com/communications/what-s-difference-between-zigbee-and-z-wave, Accessed: 2014-05-20

- **RuBee**, based on the IEEE 1902.1 standard, operating at a relative low 131 KHz frequency, offers a data rate of only 9.6 Kbit/s but has a range of 30m. Due to operating at 131 KHz, its radio signals are not attenuated by liquid or metal, therefore no line of sight is needed, which makes it ideal for harsh environments. Depending on the size and scope of a garden, it can be very dense, with loads of plants and bushes blocking the line of sight, which makes RuBee an ideal ”candidate” for Smart Gardening applications. Offering only 9.6 Kbit/s is quite insignificant, since one does not necessarily want to live-stream his plants and as already mentioned above, a single bit flip could be sufficient to turn on the sprinkler service.
- **Insteon**, is a proprietary technology, operating on the 902 - 924 MHz ISM band; it offers a data rate of 13 Kbit/s and a range of 45m. It was especially designed for home automation networking (such as light switches, thermostats and motion sensors).
- **Wi-Fi**, is so-called one of the most established standards (IEEE 802.11), operating on the crowded 2.4 GHz ISM band as well as on 5 GHz (IEEE 802.11a and IEEE 802.11n). It offers the highest bandwidth of up to 54 Mbit/s and has a range of 100m. Due to its high bandwidth and well established standard it is especially suited for multimedia-streaming.
- **ZigBee**, built on top of the IEEE 802.15.4 standard, operates on the crowded 2.4 GHz ISM band. It has a data rate of 250 Kbit/s, a range of 30m and supports a mesh topology, which makes it possible to cover larger areas. Therefore it is well suited for Smart Metering and Home Automation.
- **RFID (Radio-Frequency IDentification)**, a well established standard (ISO/IEC 1800-6), operates at 860 - 960 MHz, offering a data rate of 10 - 100 Kbit/s and a range of 1 - 100m depending on whether its working in active or passive mode. It is especially interesting in its passive mode, since it does not require a battery[5]. Therefore it is suitable for access control and identification.
- **DECT ULE**, the latest iteration of the DECT standard, well known from cordless phones, operates at 1.9 GHz, offering a data rate up to 1 Mbit/s and a range of 300m. It can be used for Smart Metering as well as for Home Automation.

Prime choices for certain specific areas as Smart Gardening, Multimedia-streaming and Access Control are available. But with regard to Smart Metering and Home Automation as much as for BAN, no dominating technology can be found.

4.3 Smart Factory (Industry 4.0[6])

The world is undergoing a Fourth Industrial Revolution. After the use of steam, electric and computer power the Internet of Things will finally bring an autonomic factory into reality.

Characteristics Another up-scale has been done in comparison to Smart Home. Smart objects in a Smart Factory need to be connected over **wider coverage** and to penetrate through **thicker and more walls**, which are more likely to be made of metal. Again there is **no line of sight** within such a huge building. However, since factories are managed by big companies, there is also a **larger financial budget**.

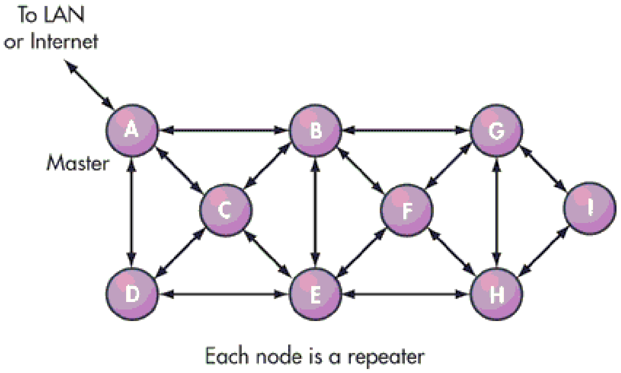

Figure 5: Mesh topology

Communication Requirements Due to the extended coverage, there are two ways of interconnecting all those smart object to each other: either by a **long range network** connecting all the sub-area networks or by a technology supporting **mesh topologies**. A mesh topology is characterised by nodes being connected to all of their neighbours, making it possible to compensate each single node failure by re-routing the traffic (see Figure 5 above).

Communication Technologies The technologies can be therefore grouped and prioritized with regard to their ranges as follows (again, see Table 2 on page 8, Category 3):

- Long range network
  - **RFID**: 1-100m
    Even though RFID is not meant to connect subnetworks together, it can still be used for access control and identification, especially for the factory environment (keeping track of items or people leaving/entering a part of the building)
  - **Wi-Fi**: 100m
    Due to the increased amount/width of walls, using Wi-Fi as a gateway for subnetworks might not be a good idea. It is better to use it in conjunction with wired solutions (one access point per room, as already been used in most public buildings).
  - **DECT ULE**: 300m
    Same argument as with Wi-Fi can be given here.
  - **Wireless M-Bus**: 1000m
    Based on the EN13757 standard, it operates at 868 MHz and offers a data rate up to 100 Kbit/s. Due to its huge range it is especially suited for connecting subnetworks.
  - **DASH7**: 2000m
    Based on the ISO/IEC 18000-7 standard, it operates on the 433.92 MHz ISM band and offers a data rate up to 200 Kbit/s. The same argument as with DASH7, regarding its range, can be given here.
- Mesh topology network
  - **Wireless HART**: 250m
    Based on the IEEE 802.15.4 standard (as ZigBee), it operates on the crowded 2.4 GHz ISM band and transmits

[5] RFID Journal. What is the difference between passive and active tags? http://www.rfidjournal.com/faq/show?68, Accessed: 2014-05-20

[6] Plattform Industrie 4.0: http://www.plattform-i40.de/, Accessed: 2014-05-20

data at 250 Kbit/s. It is very well suited as a base network covering the whole building due to its mesh topology support.

Several approaches have been presented and no technology seems to *dominate others*.

4.4 Smart Grid

Smart Grid is an application of connecting producers and consumers of energy power to each other [9] (see Figure 6 below).

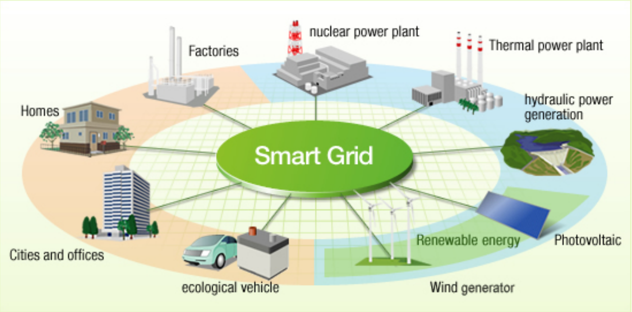

Figure 6: Smart Grid

Characteristics Smart Grid is a **stationary centralized two-way communication** tree. It has to **cover wide areas** and can cope with **hourly peaks**, especially when all households transmit their usage at the top of the hour [7].

Communication Requirements Depending on the structure and size of the tree-shaped network, **long range**-technologies have to be used. Since energy usage information has to be present fairly quickly (within a few ms) [7], the technology also needs to have a **short transfer latency**. It also has to be fairly **scalable**, since it is going to be a network that up to a millions households are going to use. Last but not least, it also has to be **interoperable**.

Communication Technologies In terms of connecting all those households together, one has to use a tree or cellular-shaped network. The denser the living areas, the smaller the cells or the range of the leaf-networks in the network-tree. ”Candidates” of those two categories are listed below (again, see Table 2 on page 8, Category 4):

- **Wireless M-Bus & DASH7** can be used as neighbour aggregators, where they collect the data from a whole neighbourhood and forward it to a higher-layer network
- **Cellular & WiMax**
  Cellular, a combination of all the cellular technologies from the former GSM up to the most recent LTE-Advanced, offers a long range up to 10km. WiMax, which is another technology, can cover even up to 50km. Both, on their most current iteration, offer large bandwidths. However, the coverage of those latest iterations is only limited to bigger cities. This makes it more suitable for older cellular technologies, such as EDGE, they also cover other areas and are needed for Smart Grid. SMS (GSM) is rather inappropriate due to its long latency of several seconds.

Both categories, wireless and cellular, can be useful. Again, there seems to be no *dominating* technology.

4.5 Logistics

According to the Oxford English Dictionary, logistics is *”the commercial activity of transporting goods to customers”*. Some specific IoT applications in logistics are: monitoring the condition and quality of shipment, localizing items within a harbour or warehouse, detecting storage incompatibilities (i.e. prevent storing light inflammable items near explosive materials) and general tracking of the fleet.

Characteristics Smart objects in Logistics can be highly **mobile**, which again forces them to be battery powered. While being transported, they usually enter **”Off-the-grid” environments**, areas where there is no cellular coverage (such as on the sea, or up in the air). There is also a **huge variety** of different smart objects in this domain.

Communication Requirements In terms of the requirements, almost the same can be said as with the Smart Grid: **long range** communications, which are **scalable** and **interoperable**.

Communication Technologies The whole transportation process of goods can be split into different sub processes, such as storing in warehouses, loading and unloading on a harbour and transporting by ship, plane or truck. For covering those subdomains, different technologies are preferred, which are listed below (again, see Table 2 on page 8, Category 5):

- **Wireless M-Bus & DASH7**
  Due to their large range they can be used in indoor environments, such as large harbours, warehouses or even on board of large ships (with a satellite dish as an aggregator, connecting the ship with the *rest of the world*)
- **Cellular**
  Despite SMS (GSM) being declared as not suitable for Smart Grid applications, it is very usable in Logistics applications because they do not rely on a low latency (e.g., sending the GPS coordinates of a truck to the base, which could accept delays of several seconds). Another advantage in using SMS instead of data packets, is its lower energy profile.
- **WiMax**
  Due to the low coverage of WiMax in less populated areas, it cannot be used for fleet tracking and when it comes to area aggregation, one is better suited with Wireless M-Bus or DASH7.
- **Satellite**
  Due to its range up to 600km, it is predestinated for ”Off-the-grid” environments.
- **Weightless**[7] is a new upcoming standard. It operates in the White Space spectrum. White spaces refer to frequencies that are allocated to a broadcasting service (primary network) but are not used locally and therefore can be used by secondary devices without interfering with the primary network [5]. It can offer a data rate up to 16 Mbit/s and cover a range of 5km. It can be highly dependent on the location in terms of white space availability but when there is any, it is very useful for low reception environments.

[7] Weightless: `http://www.weightless.org/`, Accessed: 2014-05-20

Due to the many sub areas in Logistics, there is no *dominating* technology.

4.6 Summary

The last five application domains have made something very clear. Due to different requirements within the domains, there is no single technology that can be used for all tasks. Despite having all those different requirements, one that showed up over and over again was interoperability.

5. CONCLUSION

Interoperability is very important for the Internet of Things. It enables devices from different vendors to connect to each other without any compatibility issues which is the foundation for a smart environment. Having one technology only would be a way to solve the interoperability problem. However, there is a **trade-off between reliability and interoperability**. Especially in the health section, it is far more important for health-critical devices to operate reliably, by all means with a proprietary technology like Zarlink, than to interconnect with other devices. In other areas, such as smart home, using different technologies instead of only one could reduce the overall energy consumption and cost. A smart plant for instance does not need to support a high bandwidth that supports multimedia-streaming and therefore has a much higher energy consumption than if it would stick with a low-power technology. Therefore also a **trade-off between economicalness and interoperability** needs to be made. Another reason why one cannot use one technology for all domains is a plain physical one: it is impossible to have a technology with a power consumption to be low enough to connect smart pacemakers on one side, and with a range to be long enough to connect them to a central city aggregator a couple of kilometres away. At least not with current radio wave technology. Based on all those factors it is therefore recommended to stick with different technologies and work on standardizing the application layer.

ACKNOWLEDGMENTS

The author would like to acknowledge the assistance, support and guidance of Matthias Kovatsch in preparing this report and the corresponding presentation.

REFERENCES

1. M. Allman, Enhancing TCP Over Satellite Channels using Standard Mechanisms (RFC2488), Jan 1999
2. E. Darmois, O. Elloumi. Introduction to M2M. In *M2M Communications: A Systems Approach, John Wiley & Sons, 2012*
3. S. Movassaghi, P. Arab, M. Abolhasan. Wireless Technologies for Body Area Networks: Characteristics and Challenges. In *Proceedings of the International Symposium on Communications and Information Technologies (ISCIT), pp.42-47, 2012*
4. M. Patel and J. Wang. Applications, Challenges and Prospective in Emerging Body Area Networking Technologies. In *IEEE Wireless Communications, pp.80-88, February 2010*
5. W. Webb. On Using White Space Spectrum. In *IEEE Communications Magazine, pp.145-151, August 2012*
6. W. Webb The Role of Networking Standards in Building the Internet of Things. In *Digiworld Economics Journal, no.87, pp.57-66, 2012*
7. G. Wu, S. Talwar, K. Johnsson, N. Himayat, K. D. Johnson. M2M: From Mobile to Embedded Internet. In *IEEE Communications Magazine, vol.49, no.4, pp.36-43, 2011*
8. Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, M. Guizani. Home M2M Networks: Architectures, Standards and QoS Improvement. In *IEEE Communications Magazine, pp.44-52, April 2011*
9. Y. Zhang, R. Yu, M. Nekovee, Y. Liu, S. Xie, S. Gjessing. Cognitive Machine-to-Machine Communications: Visions and Potentials for the Smart Grid. In *IEEE Network, vol.26, no.3, pp.6-13, May/June 2012*
10. H. Zimmermann. OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection. In *IEEE Transactions on Communications, vol.28, no.4, pp.425-432, Apr 1980*

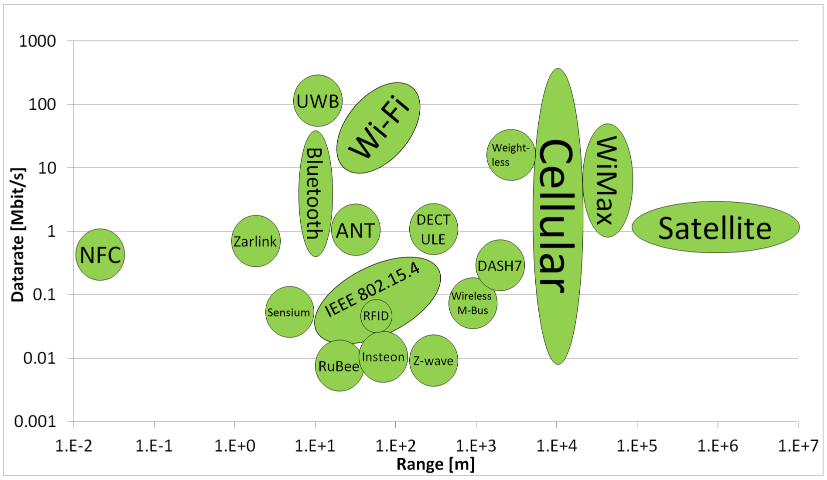

Figure 7: Datarate-Range Diagram, based on Table 2 on page 8

Cat	Technology	Standard	Frequency	Data Rate	Range	Application
1,2	NFC	ISO/IEC 18092:2013	13.56 MHz ISM	106, 212, 424 Kbit/s	up to 20cm	Identification
1	Zarlink	Proprietary	402 - 405 MHz, 433 - 434 MHz ISM	200 - 800 Kbit/s	2m	Implants
1	Sensium	Proprietary	868 MHz, 915 MHz ISM	50 Kbit/s	5m	Low Bandwidth Wearables
1	Bluetooth/BLE	IEEE 802.15.1	2.4 GHz ISM	1 Mbit/s	10m	High Bandwidth Wearables
1	Ultra Wideband	Several	3.1 - 10.6 GHz	110 Mbit/s	10m	Very High Bandwidth Wearables
1	ANT	Proprietary	2.4 GHz ISM	1 Mbit/s	30m	High Bandwidth Wearables
2	RuBee	IEEE 1902.1	131 KHz	9.6 Kbit/s	30m	Smart Gardening
2	Insteon	Proprietary	902 - 924 MHz ISM	13 Kbit/s	45m	Home Automation
2	Wi-Fi	IEEE 802.11n	2.4 GHz ISM, 5 GHz	54 Mbit/s	100m	Multimedia-Streaming
2	ZigBee	IEEE 802.15.4	2.4 GHz ISM	250 Kbit/s	30m	Smart Metering, Home Automation
2,3,5	RFID	ISO/IEC 1800-6	860 - 960 MHz	10 - 100 Kbit/s	1 - 100m	Access control, Identification
2	DECT ULE	DECT	1.9 GHz	1 Mbit/s	300m	Smart Metering, Home Automation
2	Z-wave	ITU-T G.9959	900 MHz ISM	9.6 Kbit/s	300m	Not usable due to Vendor lock-in
3	Wireless HART	IEEE 802.15.4	2.4 GHz ISM	250 Kbit/s	250m	Smart Factory
3,4,5	Wireless M-Bus	EN13757	868 MHz	100 Kbit/s	1km	Smart Building, Neighbourhood Aggregator
3,4,5	DASH7	ISO/IEC 18000-7	433.92 MHz ISM	200 Kbit/s	2km	Smart Building, Neighbourhood Aggregator
5	Weightless	Weightless SIG	White Space	16 Mbit/s	5km	Low Reception Environments
4,5	Cellular	Several	Several	up to 1 Gbit/s	10km	Logistics
4,5	WiMax	IEEE 802.16	Several	128 Mbit/s	50km	Wide Area Coverage
5	Satellite	Internet over Satellite	Several above 2 GHz	1 Mbit/s	600km	*Off-the-grid* Environments
Cat: Categories they are most used (1: BAN, 2: Smart Home, 3: Smart Factory, 4: Smart Grid, 5: Logistics)						

Table 2: Wireless Technologies Overview, sorted by range in ascending order [1][3][4]