Modern Wireless Technology

Matthias Kappeler

Sommerakademie in Leysin, August 2016

Abstract

In the following I will introduce different wireless communication technologies and discuss them in terms of energy consumption and security. Before that I will illustrate different kinds of networks and what kind of limitations there are when transmitting wirelessly.
The technologies I will introduce are: Communication Satellites, The Mobile Phone System, Wireless Lan, Bluetooth, RFID and ZigBee.

Contents

1 Introduction

Whether you want to check your email, brows the web, talk to your friends, or lots of other activities - One thing they have in common. You just don't want to be limited to your home computer to do it.

In the past decade our hunger for mobile data has gone through the roof. As a result we now expect to be able to access the internet wherever we are, whatever we do and wherever we go. Today we still have to be a little proactive to find connectivity but in the future, and there is no doubt, we will have ubiquitous connectivity and access to the Internet will be omnipresent.

The cause for this transformation in information technology is of course the establishment of wireless networks. Practically the only difference between any network and a wireless network is that there is no such thing as a cable necessary to connect the device with the network. Of course there is not that one and only wireless network. There are several widespread wireless technologies in use: WiFi, Bluetooth, ZigBee, NFC, LTE, HSPA, earlier 3G standards, satellite services and a lot more. Each technology has its advantages and disadvantages and is optimised for a specific task and context. Because of this diversity you can not make generalisations about the performance of wireless networks. However, because of standardisation and evolving technologies they now mostly have common principles and are subject to common performance criteria and constrains.

Even though the way of data delivery via radio communication is different in each technology the outcome as experienced by the user within is, or should be, all the same - same performance, same results. And this is where we are heading.

As everything around us is getting connected and we are talking about the Internet of Things (IoT) two major questions arise. Where do we get the power from or how do we get them so power efficient that we can afford to really connect all the devices within our homes and the second question: Are these wireless technologies secure?

In this paper I try to outline the common wireless technologies and also try to answer these two big questions about each of them.

2 Different Types of Wireless Networks

Each technology is usually designed for a specific purpose. This includes features like the range of the wireless network and what application it has. Of course this table is not complete and it is

Type	Range	Applications	Standards
Personal area network (PAN)	Within reach of a person	Cable replacement for peripherals	Bluetooth, ZigBee, NFC
Local area network (LAN)	Within a building or campus	Wireless extension of wired network	IEEE 802.11 (WiFi)
Metropolitan area network (MAN)	Within a city	Wireless inter-network connectivity	IEEE 802.15 (WiMAX)
Wide area network (WAN)	Worldwide	Wireless network access	Cellular (UMTS, LTE, etc.)

Figure 1: Types of wireless networks

not really possible to draw a clear line between these technologies because for example Bluetooth started out as cable replacement but evolved and acquired more capabilities, reach, and throughput. WiMAX was first designed as a fixed wireless solution but with time acquired additional mobility capabilities, making it a good alternative to cellular technologies.
There are way more criteria that determine the characteristics of each type of network than the ones shown in the table. Such criteria can be: the power source, battery life, data rates and lots more.
One thing they all have in common. They use the electromagnetic spectrum to transfer data.

3 Electromagnetic Spectrum

Sometimes they are called radio waves but the proper term is electromagnetic radiation. The electromagnetic spectrum contains all kinds of wavelengths (frequency) and depending on the frequency you can use it for a special purpose. The electromagnetic spectrum is a natural constant so you can not just add some more frequencies. This is why there are strict regulations and licenses for the use of a frequency. As you can see in figure 2 not the whole spectrum is used to transfer data. Only the low frequencies are used for this purpose. If you look further to the right of the spectrum you can see the visible light and after that there are waves which harm the human body

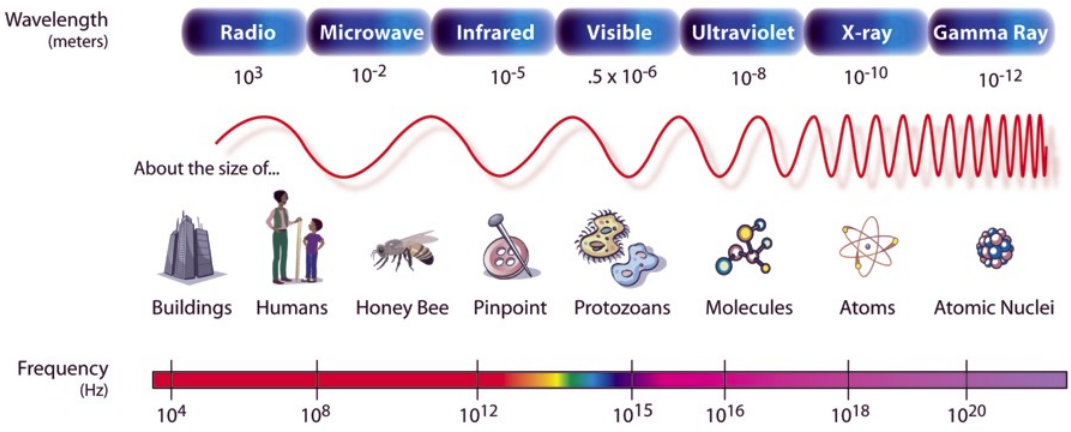


Figure 2: The electromagnetic Spectrum

like Ultraviolet Rays, X-rays or Gamma Rays. That part of the spectrum is also useful for certain applications but not in wireless technologies.
If we zoom in a little to see how the spectrum which is used for data transmission is divided into the certain kind of fields it starts to look a little complicated. And this is just a little part of the

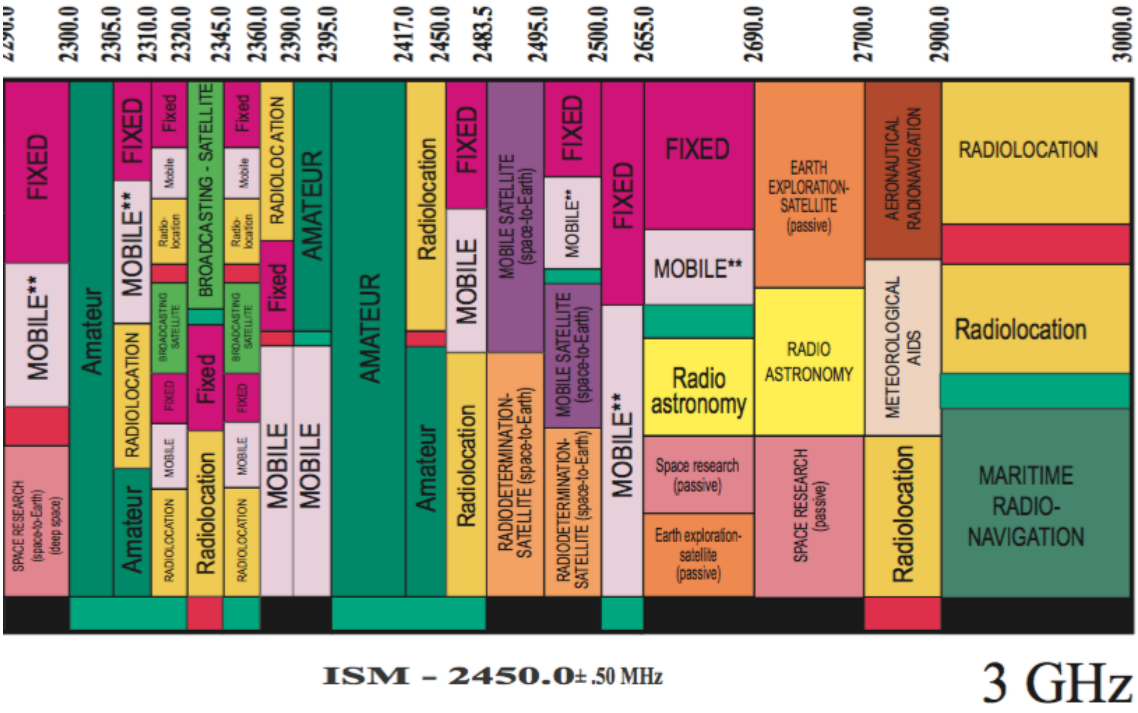


Figure 3: The electromagnetic Spectrum

spectrum. This part of the spectrum is called the ISM-Band. This stands for Industrial, Scientific and Medical and therefore it is unlicensed and so everybody can set up a WiFi within this spectrum (and some other frequencies) at home. Since the spectrum is such a scarce source, organisations like the FCC in the US regulate the distribution of the frequencies. Sometimes a block of the spectrum

gets offered in an auction and this is how private telecommunication provider can get their share of the spectrum. Usual prices which are gained at such an auction are in the billions.

3.1 Limitation

Each wireless technology has its limitations but all communication methods have a maximum channel capacity. Claude E. Shannon put this limitation in a mathematical term and gave us a model to calculate the maximum information rate (channel capacity).

$$C = BW \cdot log_2(1 + \frac{S}{N}) \tag{1}$$

- C is the channel capacity and is measured in bits per second.
- BW is the available bandwidth, and is measured in Hertz.
- S is signal and N is noise, and they are measured in Watts.

This shows us that if you double the available bandwidth you can also double the transferred data per second. This is why everybody is talking about broadband because with a broader band you can send and receive more data.

The second big limitation is the signal power between the transmitter and the receiver. This is also called the signal-power-to-noise-power ration, S/N-ration. It is a measure that compares the level of desired signal to the background noise and interference. The more noise there is, the stronger the signal has to be.
Just imagine the microwave oven operating at 2.5 Ghz fighting your WiFi and creating interference which harm your WiFi signal. Another source of interference could be your neighbours WiFi.
In the ideal case, you would be the one and only user within a certain frequency range, with no other background noise or interference. As you can imagine, this is just a theoretical condition.

4 Communication Satellites

Probably one of the oldest wireless technologies which are still used all around the world but there is no such thing as the one satellite technology. There are three major groups of Satellites each used for different purposes. These three are called: GEO, MEO and LEO.

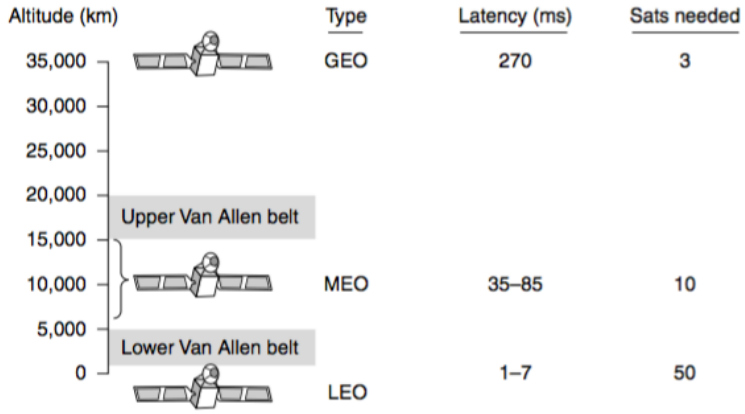


Figure 4: Communication satellites and some of their properties, including altitude above the earth, round-trip delay time, and number of satellites needed for global coverage.

4.1 GEO

Geostationary Satellites as the name already reveals stay at the same place. They are quite large, weigh over 5000 kg and consume sever kilowatts of electric power produced by the solar panels. A satellite like this can operate 10 years and after that its fuel for the "station keeping" is empty and it eventually drifts off and burns in the earths atmosphere.

These satellites are at a hight of 35000km and there are just 3 satellites needed to cover the whole earth. With current technology, it is unwise to have geostationary satellites spaced much closer than 2 degrees in the 360-degree equatorial plane, to avoid interference. So am maximum of 180 Satellites can be in the sky at once. However, each transponder can use multiple frequencies to increase the available bandwidth.

This technology is used for broadcast satellite television for one-way transmission. Because they are quite fare away from earth there is a delay in the signal. A typical value is 270 msec. Compared with a fiber optic link which has a delay of 5μsec/km this is quite much.

What makes them really attractive for Television Broadcasting is that it does not matter if you send the signal to just one device or several million within the satellites beam. The costs stay the same. Regarding privacy satellites are a quite disaster. Everybody can hear everything. Encryption is essential when security is required (for example military use).

4.2 MEO

Far below the GEO we find the MEO (Medium-Earth-Orbit) satellites. These take about 6 hours to circle the earth. Since they are moving they have to be tracked. Because they are lower than the GEO they have a smaller footprint on the ground and require less powerful transmitters. Currently they are used for navigation rather than telecommunication. One example for this is the GPS (Global Positioning System) which consists of 30 Satellites orbiting at about 20,200 km altitude. The latency in this height is between 35-85ms. Depending on the altitude.

4.3 LEO

This third category are the lowest satellites. Therefore they are quite fast. This results in a large number of satellites needed for global coverage. Advantages are the short delay and the low launch costs. In 1990 Motorola started to send 66 satellites in orbit but the commercial success was not possible. This was due the lack of demand for satellite phones. It got sold to an investor and are now used for paging, navigation, data and voice. Especially for companies which operate in areas where no other communication service is available (for example oil exploration) use this kind of service.The latency in the hight between 200 and 2000 km where these satellites orbit is between 1 and 7 ms.

4.4 Energy consumption

The Satellites do need a lot of Energy but they harvest all of the needed energy via their solar panels. The receivers which are stationed on earth are usually kept quite simple because they only have a downstream link and no upstream. For uploading far more energy would be necessary.

4.5 Security

Because satellites reach thousands of square kilometre it is hard to avoid someone else not getting the information which is transmitted via the satellite. Therefore a good encryption is needed especially for military use. In case of television broadcasting it does not have to be encrypted because there are no privacy concerns.

5 The Mobile Phone System

Since the first mobile phone system was available a lot has happened. From the push-to-talk systems to LTE was a long way.
There are two major organisations which set the standards. They are called 3GPP and 3GPP2. Since the 3GPP is the one setting standards for Europe we focus on that one.

5.1 1G

The first generation (1G) was analog and just used to transfer voice calls. The technique where an area gets divided into small cells (that is where the name cellphone comes from) is still common practice in later technologies. With this devision into small cells one frequency can be used in multiple cells which allows more bandwidth within one cell.

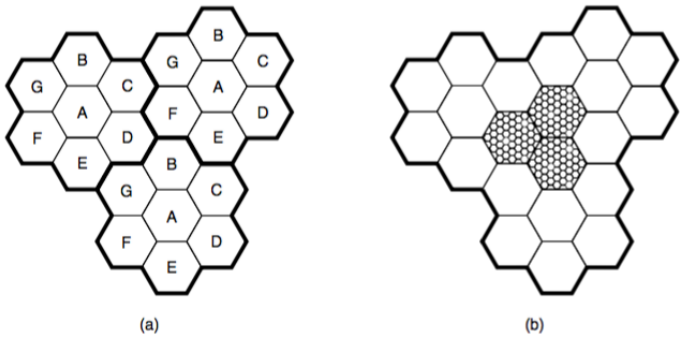


Figure 5: a) Frequencies are not reused in adjacent cells. b) To add more users, smaller cells can be used.

This means that the cells in a metropolitan area are smaller than somewhere in the outback. If you leave a cell the antenna notices that the signal gets weaker and your phone is looking for a closer antenna. The switching in between two cells can either be a soft handoff (no signal loss) or a hard handoff where the old station drops the signal before the new one is acquired.

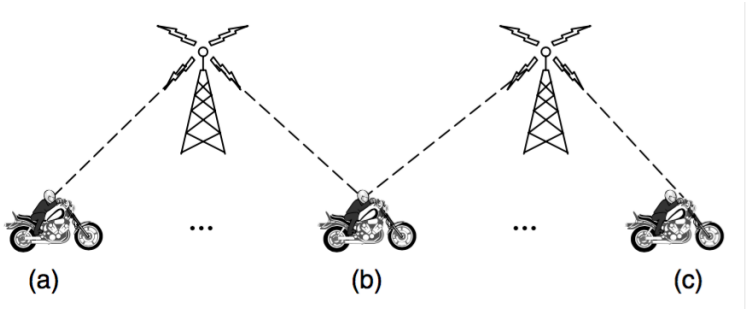


Figure 6: The handoff in the mobile phone system

5.2 2G

The second generation introduced digital signaling. It was baed on the GSM (Global System for Mobile Communication) and was able to transfer peak data rates of 9.6Kbit/s. When GPRS was introduced you could reach up to 172 Kbit/s. A few years later these networks were enhanced by

Generation	Organization	Release
2G	3GPP	GSM
	3GPP2	IS-95 (cdmaOne)
2.5G, 2.75G	3GPP	GPRS, EDGE (EGPRS)
	3GPP2	CDMA2000

Figure 7: Cellular network 2G standards

EDGE(Enhanced Data rates for GSM Evolution) and so 384 Kbit/s were possible. This technology launched in the U.S. in 2003.

5.3 3G

3G	3GPP	UMTS
	3GPP2	CDMA 2000 1x EV-DO Release 0
3.5G, 3.75G, 3.9G	3GPP	HSPA, HSPA+, LTE
	3GPP2	EV-DO Revision A, EV-DO Revision B, EV-DO Advanced

Figure 8: Cellular network 3G standards

With 3G more and more the data rates increased. You might wonder but LTE is not 4G. It is 3.9G. It is a transitional standard.

5.4 4G

4G	3GPP	LTE-Advanced, HSPA+ Revision 11+

Figure 9: Cellular network 4G standards

4G requirements are really hard to obtain. Some examples for the requirements are the following:

- Interoperable with previous wireless standards (3G and 2G)
- 100 Mbit/s data rate for mobile clients and Gbit/s when stationary
- Dynamic allocation and sharing of network resources between users

The actual list is much, much longer and as you might realise now is your 4G mobile contract not really 4G. LTE does not meet these criteria and is therefore just 3.9G, even though it lays much of the necessary groundwork to meet the 4G requirements. LTE-Advanced is designed to meet these standards.
The providers use the 4G label as a marketing coup and sell contacts as 4G which are just quite close to 4G but not there, yet.
LTE-Advanced will be deployed but how the real 4G will be marketed is not clear, yet.
As the name already says LTE (Long Term Evolution) is definitely the long-term evolution plan for virtually all future mobile networks. A few carriers have already begun to invest into LTE infrastructure but current industry estimates show that this migration will indeed be a long-term one. In the meantime, HSPA+ is set to take the center stage.
HSPA+ has one huge advantage over LTE. It is way cheaper for the carriers. With HSPA+ they can use their existing infrastructure and do not have to develop new radio networks which are needed for LTE. HSPA+ meets many of the 4G criteria but of course not all. So the answer to the question why HSPA+ is still developed is that it is way cheaper than LTE. The biggest share is the one of

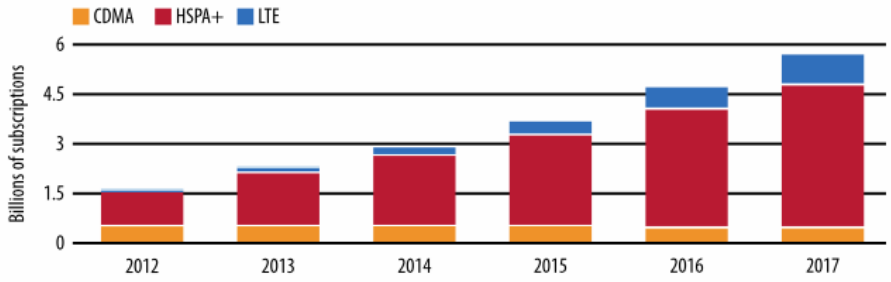


Figure 10: Forecast of the mobile broadband growth in America

HSPA+. It is leading worldwide 4G adoption and estimates are that it will be the dominant mobile wireless technology of the current decade. In 2016 the number of LTE subscriptions outnumbered the HSPA+ subscribers (in America) but they probably do not perform better than their HSPA+ counterpart.

	HSPA+	LTE	LTE-Advanced
Peak downlink speed (Mbit/s)	168	300	3,000
Peak uplink speed (Mbit/s)	22	75	1,500
Maximum MIMO streams	2	4	8
Idle to connected latency (ms)	< 100	< 100	< 50
Dormant to active latency (ms)	< 50	< 50	< 10
User-plane one-way latency (ms)	< 10	< 5	< 5

Figure 11: HSPA+, LTE and LTE-Advanced comparison

5.5 Energy consumption

You can say that the more data is transferred the more energy is consumed. For example a LTE-capable device must have multiple radios for mandatory MIMO (multiple input multiple output) support. However, each device will also need separate radio interfaces for earlier 3G and 2G networks. If you are counting, that translates to three or four radios in every handset! For higher data rates with LTE, you will need 4x MIMO, which brings the total to five or six radios. This is why it is so energy consuming.

5.6 Security

Since every handset has the so called SIM-card (Subscriber Identity Module) which is protected via password a certain kind of security is given.
But there are also ways of infiltrating the handheld device. For example viruses can be spread via MMS. Since MMS is not that common anymore this abandoned that threat almost completely. Probably the highest risk lays within the lower 2G network. 4G and 3G networks are quite save but as soon as a cellphone connects to the 2G network it is vulnerable. A person could try now to take down the 4G and 3G service within the area (DDoS Attack) his victim is in and as soon as the phone connects to 2G one can see what kind of data is transmitted or received by the phone.

6 Wireless Lans

WiFi operates in the unlicensed spectrum and is therefore trivial to deploy by anyone, anywhere. Nowadays almost every electronic divide is WiFi enabled.
At first some facts about WiFi:

- WiFi provides no bandwidth or latency guarantees or assignment to its users.
- WiFi provides variable bandwidth based on signal-to-noise in its environment.
- WiFi transmit power is limited to 200 mW, and likely less in your region.
- WiFi has a limited amount of spectrum in 2.4 GHz and the newer 5 GHz bands.
- WiFi access points overlap in their channel assignment by design.
- WiFi access points and peers compete for access to the same radio channel.

Does not that sound as if WiFi is just limited in everything and as if its almost worthless? Well we all know (and probably love) the real power of WiFi. Nobody (at this point) would prefer his mobile data plan on his phone over his WiFi at home. But yes a Wifi's life is not easy. It always has to fight other WiFi's, it even has to deal with multiple people wanting maximum data at the same time and so on.

But the WiFi we know today has not always been this way. Since 1999 there were several new standards and protocols for more and more data rate per stream.

802.11 protocol	Release	Freq (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)	Max MIMO streams
b	Sep 1999	2.4	20	1, 2, 5.5, 11	1
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1
n	Oct 2009	2.4	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4
n	Oct 2009	5	40	15, 30, 45, 60, 90, 120, 135, 150	4
ac	~2014	5	20, 40, 80, 160	up to 866.7	8

Figure 12: WiFi release history and roadmap

Today the "b" and "g" standards are the most widely deployed and supported. The future is broadband WiFi. The "n" and "ac" standards use twice the size of bandwidth used by previous technologies and therefore can transfer much more data than older standards. The new technologies also use several radios which allows multiple streams parallel. This is called multiple-input and multiple-output (MIMO). These new features enable gigabit-plus throughput (in ideal condition) with the "ac" standard.
Since there is no WiFi which has guaranteed data transmission there are ways to adapt to variable bandwidth. One way is Adaptive Bitrate Streaming. With this technique the download speed is monitored and the video quality adapts to the available downstream.

Container	Video resolution	Encoding	Video bitrate (Mbit/s)
mp4	360p	H.264	**0.5**
mp4	480p	H.264	**1–1.5**
mp4	720p	H.264	**2–2.9**
mp4	1080p	H.264	**3–4.3**

Figure 13: Sample YouTube video bitrates for H.264 video codec

6.1 WiFi Protocol

The WiFi protocol consists of three different layers. The physical layer determines what kind of

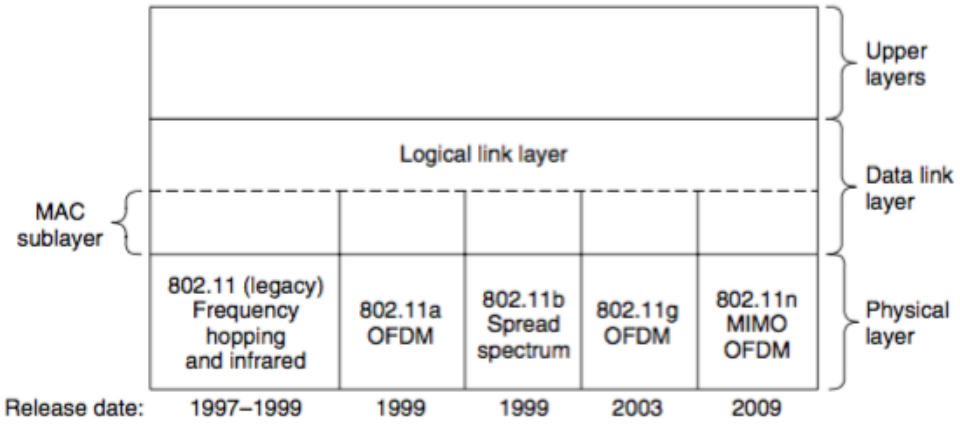


Figure 14: Protocol stack

WiFi standard is used. The data link layer consists of the MAC sublayer and the logical link layer. In the upper layer the IP address for example finds its place.
When data is transmitted wireless it is sent in packages. A package in the WiFi protocol looks as shown in Figure 15. The first thing in the package is the frame control. This part is split up into

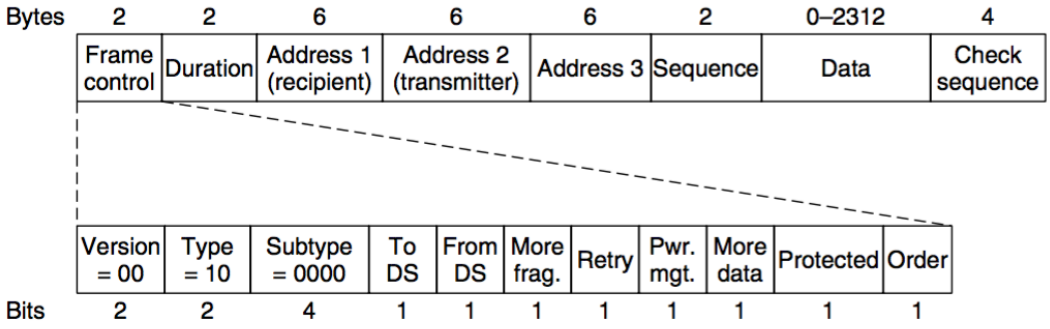


Figure 15: WIFI Package

eleven parts. The fist one is called version and with type and subtype they determine what kind of WiFi technology/hardware is used and what kind of package is send. Different types of packages are data, control, and management packages.
To or from DS bits determine whether the package is going to or coming from the network connected to the access points. The more fragments part determines if there are more fragments to come. The retry bit tells the system if the package collided in an earlier transmission approach. The power management tells if the receiver can go into sleep mode after receiving the package. The more data bit determines whether more data is following. Protected tells if the package is encrypted and order tells the recipient if the order in which the packages are sent matters. This was just the

frame control.
Duration tells how much time the transmission will take. Address 1 to 3 consist of the MAC address of the receiver and the transmitter. The sequence field numbers frames so packages which are sent twice can be detected. Data is the biggest part and as the name already says it is the part where the data is in. In this part also the upper layers like the IP address find their place. The check sequence is there for the so called CRC (Cyclic Redundancy Checks) which is a error-detecting code but i will not go into detail with that.
In normal ethernet transmission there is a technology called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to detect whether a package collided on the way. Since there is no clear path in a wireless transmission, collisions have to be avoided before they occur. This is why in WiFi the CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is used. It avoids collisions. To do so the sending device checks whether the channel it wants to use is idle or not. If it is not idle it backs off for a random time and tries again. If there is still a collision the system has certain

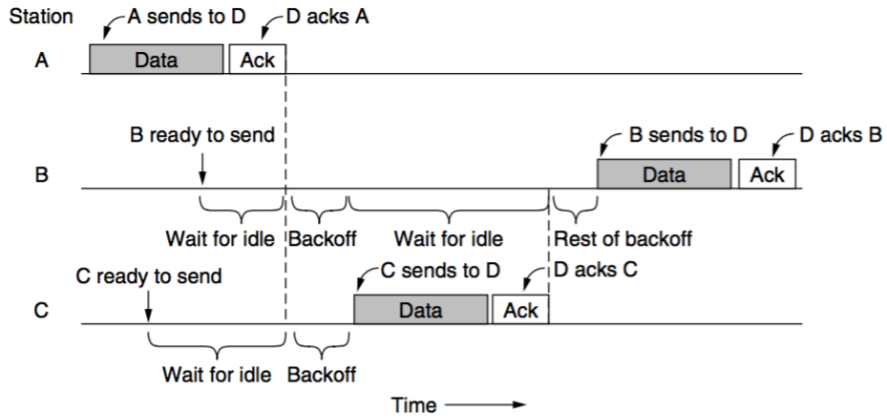


Figure 16: WIFI Collision avoidance / Backoff time

times to back off. The back off time is determined by the priority and some other factors which I will not illustrate further.

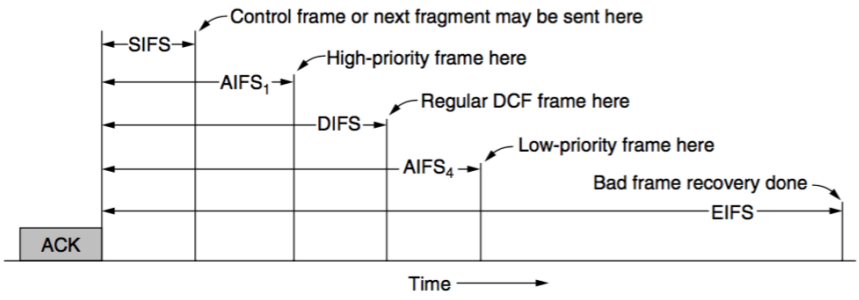


Figure 17: WIFI Backoff

6.2 Energy consumption

WiFi is quite energy consuming. Since the newer technologies use the MIMO technologies multiple radios have to be powered in one device. The router for example is not the problem because it is usually directly plugged in somewhere in the house and does not have to be mobile. The handhelds though have to be driven by lithium-ion accumulators or have to be plugged in as well. But since mobility is what we expect from a WiFi network the mandatory lithium-ion battery is the way to go.
This is the reason why this technology is not that likely to be used in machine to machine (m2m) communication because it is just too energy consuming and since smart home devices just transmit small junks of data the bandwidth of WiFi is not needed.

6.3 Security

There are different ways to make sure a WiFi network is secure. Different encryption standards have been deployed and the most common nowadays are probably WPA/WPA2. WEP has lost importance due to a lack of security. WPA and WPA2 are still considered secure and can be used without fear.
One big security concern are public WiFis. If there is no password needed all the data is transmitted without any encryption and with the right equipment all the data which is received or transmitted can be read out.
Another threat is that a lot of people do not delete old WiFi networks they connected to. Lets say someone connected to a WiFi network in his favourite fastfood restaurant and the phone always automatically connects to it. Now a second person can set up a network just like the one in the restaurant and because the phone automatically connects to this network there is no validation needed. This kind of attack is calls the evil twin attack.

7 Bluetooth

There are different versions of Bluetooth but the Bluetooth v4 is the standard at the moment. Bluetooth v5 has been introduced in early 2016 but is not deployed yet. The speed of Bluetooth v4 is 25 Mbit/s and the range is 200 feet which is the equivalent of 61 metre. Version 5 doubled the speed and quadrupled the range. This shows that a lot is changing in this technology and Bluetooth which has a bad range and low data rates belong to the past. In terms of range and data rates it becomes more and more like WiFi. One significant difference to WiFi is that there are preset profiles in the Bluetooth protocol so you can not just use it for whatever you like but the kind of profile has to be implemented in the first time. Examples for profiles are: Audio, Printer, Headset, Keyboard and some more. There are a total of 25 Profiles. This is why Bluetooth is usually used as a cable replacement for peripherals and not for multi purpose data transmission.
Another unique thing about Bluetooth is that it can only connect to a maximum of 8 devices.

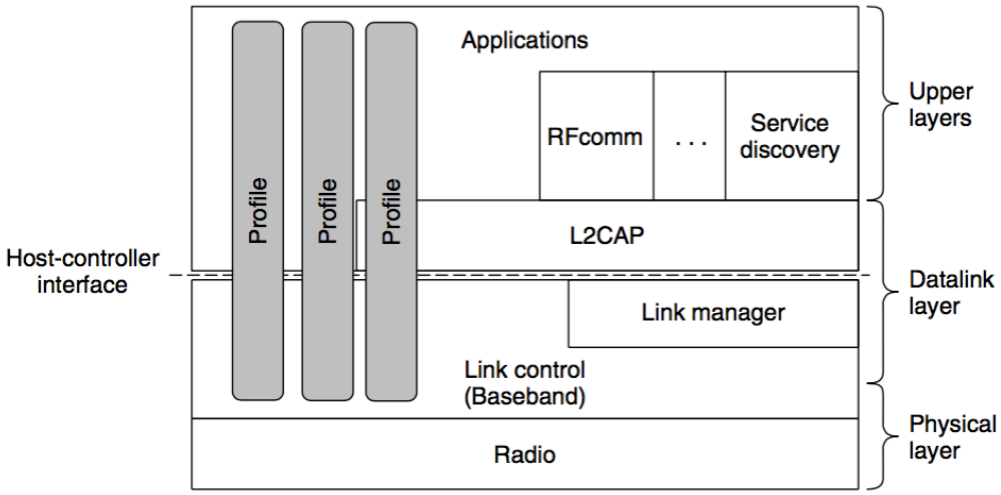


Figure 18: Bluetooth protocol stack with the preset profiles (25)

These 8 devices are called slaves because these are fairly dumb and are controlled by one master. If you want to connect more than eight devices you have to use a bridge slave. This way of setting up the network has the advantage that the slaves are quite cheap (around 5$) and therefore can be deployed quite fast.

One disadvantage with the newer version of Bluetooth (4 and higher) is that it is not compatible

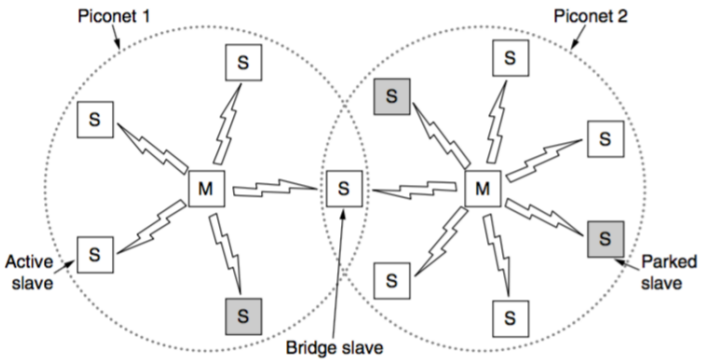


Figure 19: Bluetooth network

with the lower versions. This means that if devices which do not have the same standard need an intermediate. This intermediate is usually the master and therefore it has to be compatible with both standards.

7.1 Energy consumption

Bluetooth and especially the newer version like BTLE are fairly energy efficient. This is why this kind of technology is one of the most likely to be used in smart home devices. Batteries can last

from a couple of days up to a year with the BTLE technology.

7.2 Security

Bluejacking, bluesnarfing, bluebugging... These are names for different ways of attacking a Bluetooth device. It is quite easy to obtain the control over a device which enabled Bluetooth and therefore it is quite unsecure. There are different ways to make it a little more secure but these all are based on the awareness of the user.

- Enable Bluetooth only when required
- Enable Bluetooth discovery only when necessary, and disable discovery when finished
- Do not enter link keys or PINs when unexpectedly promoted to do so
- Remove paired devices when not in use
- Regularly update firmware in Bluetooth-enabled devices

8 RFID

Probably everybody has some RFID chips but most people do not notice that these can actually be part of a computer network. An RFID (Radio Frequency IDentification) tag looks like a postage stamp-sized sticker that can be affixed to (or embedded in) an object so that it can be tracked. The object can be anything for example a cow, passport, book, and so on.

The tag consists of a microchip with a unique identifier and an antenna that receives radio

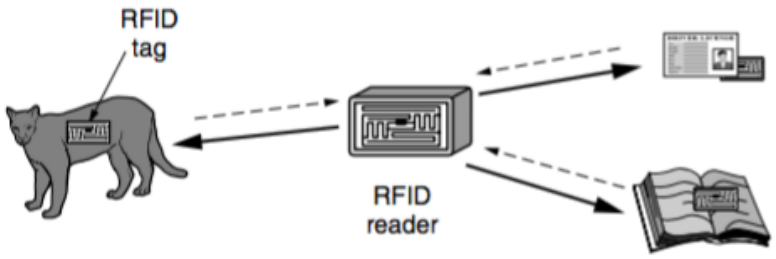


Figure 20: RFID used to network everyday objects.

transmission. Most RFID tags have neither an electric plug nor a battery. Instead all the energy needed is supplied by the RFID reader in form of radio waves. This technology is called passive RFID but there are also active RFID tags in which there is a power source on the tag.
There are three major categories of RFID technologies. Each designed for a special purpose.

8.1 UHF RFID

UHF stands for Ultra-High Frequency. This technology allows the communication of readers and tags at a distance of several meters. When the reader sends out its signal the tag changes the way the radio-waves are reflected and the reader can pick up there reflections.This way of communicating is called backscatter. It is used on shopping pallets and some drivers licenses. The frequency for this is the 902-928 MHz band in the United States.

8.2 HF RFID

This HF (High Frequency) RFID operates at 13.56 MHz and is usually used in passports, credit cards and noncontact payment systems. It has a quite short range of a meter or less and this is because it uses induction rather than backscatter to communicate.

8.3 LF RFID

The LF (Low Frequency) RFID was developed before the others and is used for animal tracking. Cats for example usually get this kind of chip.

8.4 Energy consumption

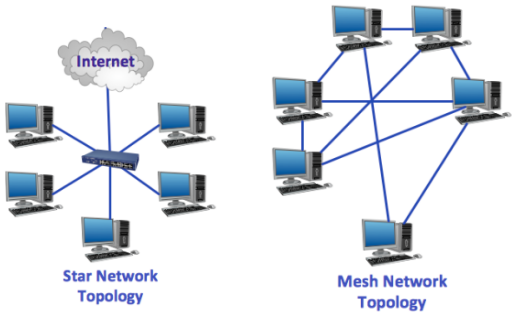
Since an RFID tag usually does not have any computing power and all the energy it needs is supplied by the reader it is really convenient to be part of sensor networks.
If computing power is necessary to encrypt the data on the tag a battery is needed. As battery capacities reach new heights this should not be a problem in the future.

8.5 Security

To encrypt something computing power is needed. Since a RFID tag does not have any computing power it can not encrypt the data transmitted and this is a huge disadvantage.
RFID tags started as identification chips but now are rapidly turning into tiny computers. For example, many tags now have small memory that can be updated and later queried, so that information about what has happened to the tagged object can be stored with it. Rieback et al. (2006) demonstrated that this means that all of the usual problems of computer malware apply, only now your cat or your passport might be used to spread an RFID virus. There are different type of approaches to solve the security issue with RFID. They reach from a password to self destroying tags which initiate a short circuit if there is an unauthorised RFID reader reading out the tag. These security mechanisms are not common today and therefore a lot research has to be done before this technology can be used without any concernes in terms of security.

9 ZigBee

ZigBee is based on the IEEE 802.15.4 standard which specifies the physical layer and media access control for low rate wireless personal area networks. This makes this technology really convenient for machine to machine communication. Machines do not need a lot of bandwidth when communicating with each other.
The special character of ZigBee is its network topology. A normal WiFi network is set up like a star. There is the router in the middle and each device connects to it. In ZigBee each device is linked to each other and this improves the stability in case of the failure of one node. This kind of network topology is called a mesh network.



As mentioned before ZigBee is based on the IEE 802.15.4 standard and this is also relevant in the protocol stack. The upper layers are determined by the ZigBee Alliance which specify the standards for this technology. ZigBee can be used to monitor different kind of parameters around the house

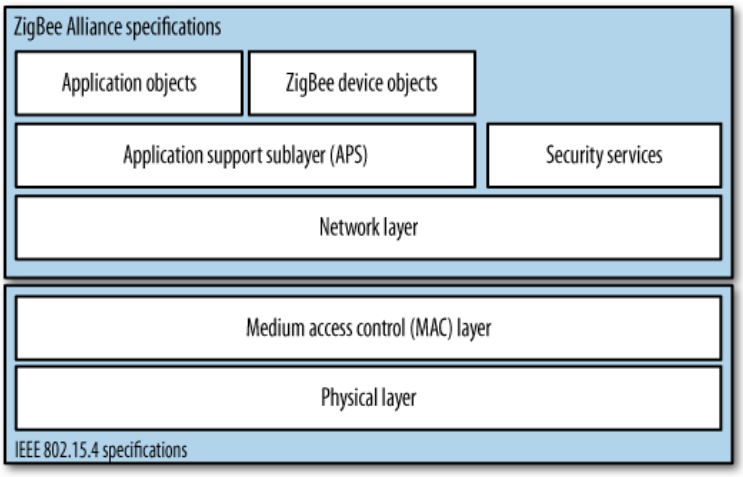


Figure 21: ZigBee protocol stack

or even within a city. So it could count the cars passing one specific street and maybe redirect other cars so no traffic jam occurs. This and a whole lot more can be realised with ZigBee. And because its stability which is provided by its network topology it is even suitable for critical applications.
One disadvantage of this kind of network is that with more and more nods the overhead of the network grows and more power has to be used to connect the nods to each other.

Looking at all the other technologies one must say that ZigBee is probably the most promising technology for wireless sensor networks.

9.1 Energy consumption

In terms on energy consumption ZigBee is really efficient. Since it is especially made for sensor networks and therefore for m2m communication just a small battery is needed to run a node for a long time. If the sensor network is not too big and the overhead is not that large the system is really efficient. As the number of linked nods increases the efficiency goes down.

9.2 Security

ZigBee relies on a extended version of CCM* in terms of encryption. As encryptionalgorithem AES-128 is used and this is considered secure. Nevertheless the protocols which are in use have unsecure parts.
ZigBee is still quite secure though and because of its reliability and security it even can be used in more critical applications.

10 Comparison

Now I compare the energy consumption of the most relevant wireless technologies which are suitable for smart home devices.
As you might already figured out in the more detailed description of each technology there are technologies which suit the needs for a connected home better than others.

10.1 Energy Consumption

In terms of energy consumption there are big differences in the different technologies. Starting with WiFi which needs Li-Ion batteries down to RFID which does not even need a battery.
each technology has its benefits.

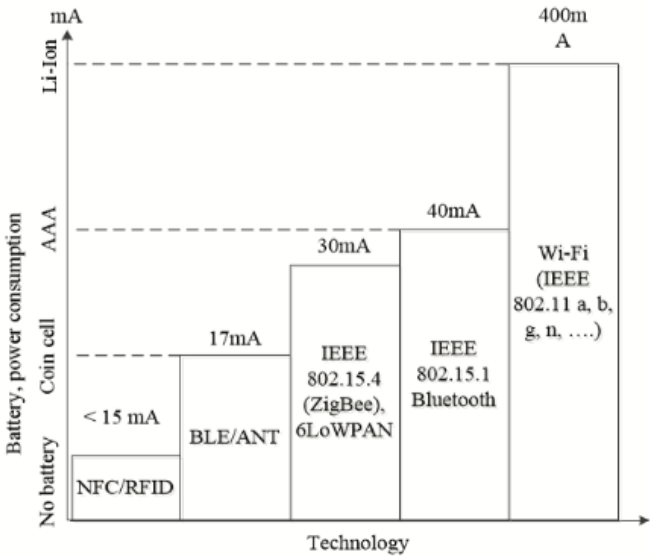


Figure 22: The types of power supplies for using access technologies in WSN (Wireless Sensor Networks)

10.2 Bandwidth

Bandwidth is really important for consumers. Machines do not really care about the bandwidth. Of course there are some applications where even machines do need to transfer a lot of data but in normal smart home devices this is not the case. In figure 23 you can see that WiFi has the broadest bandwidth and NFC/RFID has the narrowest. If you compare this scheme with the previous one about energy consumption one can see that a broader bandwidth comes along with a higher energy consumption. This is why WiFi is good for video streaming and other end user applications where power supply is no big problem but for the internet of things it will not be the technology to connect our devices.

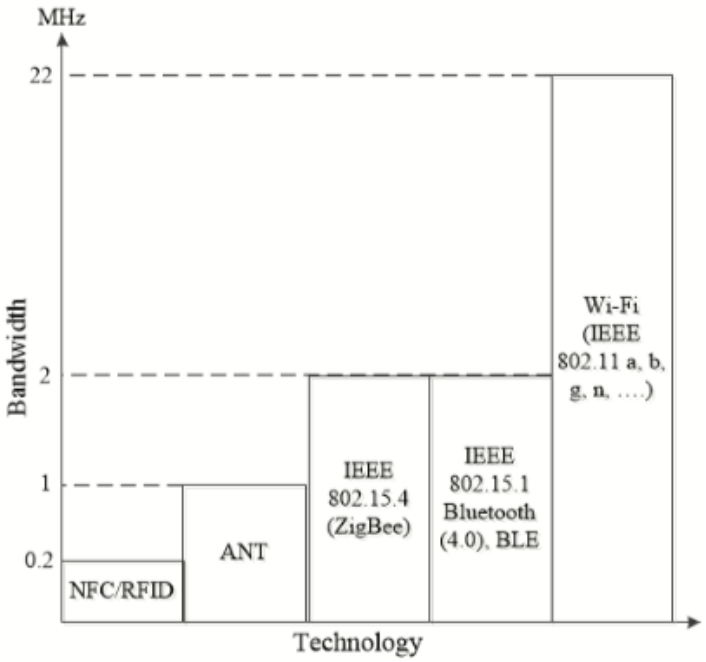


Figure 23: The maximum available bandwidth of technologies used in WSN (Wireless Sensor Networks)

11 Sources

- High Performance Browser Networking - by ILYA GRIGORIK `https://hpbn.co` (30.09.16 19:04)
- Overview of wireless technologies for organizing sensor networks - Artem Proskochylo, Andrey Vorobyov and Michail Zriakhov `http://ieeexplore.ieee.org/document/7357263/` (30.09.16 19:06)
- A Study of Efficient Power Consumption Wireless Communication Techniques/ Modules for Internet of Things (IoT) Applications - Mahmoud Shuker Mahmoud, Auday A. H. Mohamad `http://file.scirp.org/pdf/AIT_2016042217163795.pdf`(30.09.16 19:08)
- Computer Networks 5th Edition - Tanenbaum and Wetherall

- `http://mynasadata.larc.nasa.gov/images/EM_Spectrum3-new.jpg` (30.09.16 19:00)
- `https://commons.wikimedia.org/wiki/File%3AEM_Spectrum_Properties_edit.svg` (30.09.16 19:00)
- `https://www.safaribooksonline.com/library/view/building-wireless-sensor/780596807757/httpatomoreillycomsourceoreillyimages741225.png` (30.09.16 19:03)