Wireless standards for IoT

Interlab AIT September 2019 – Sebastian Büttrich

At the IT University of Copenhagen, Denmark

A little bit about us ...

PIT LAB

a **research and education lab** working with
Pervasive Computing and IoT, along full data lifecycles

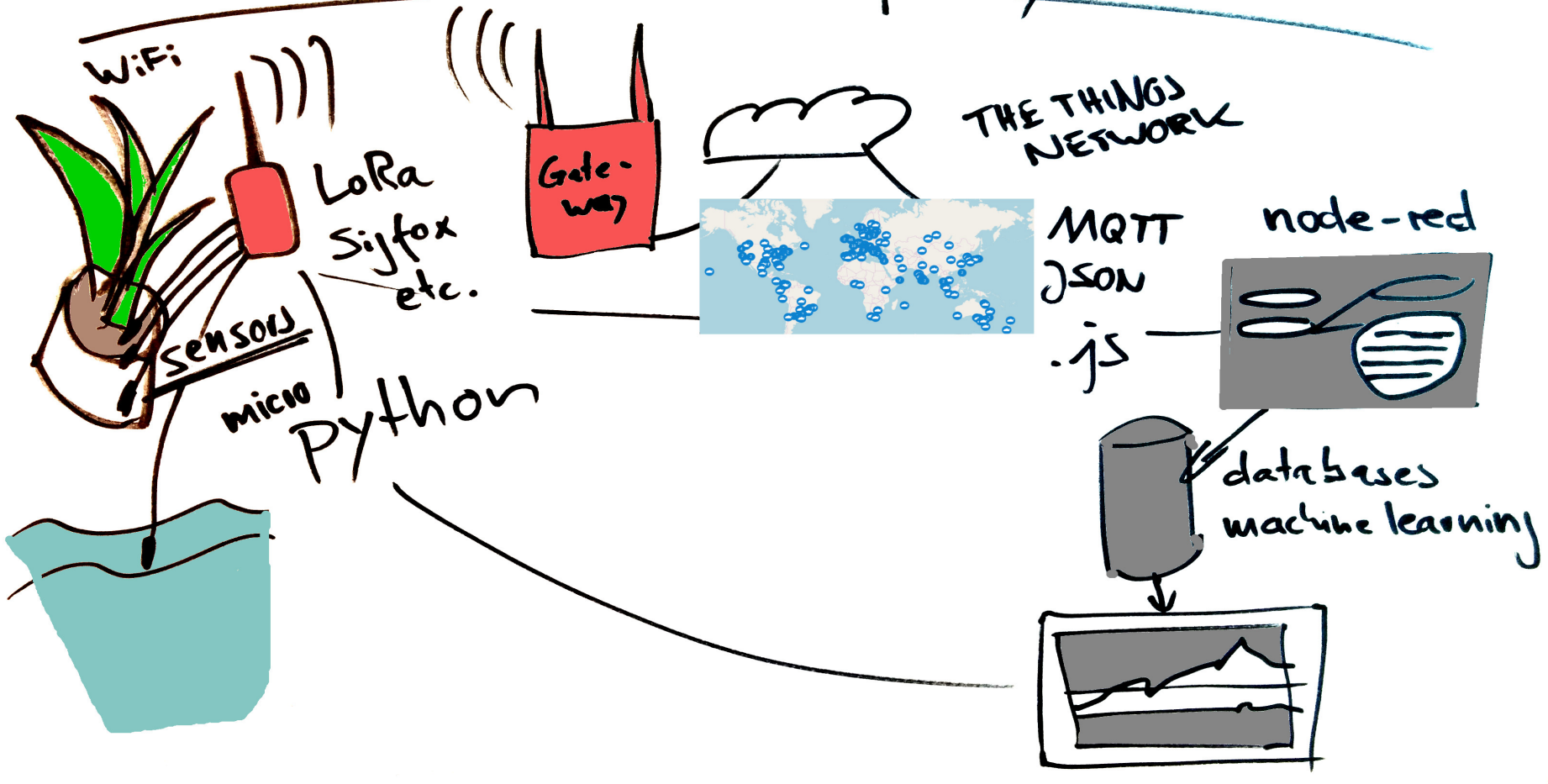
from instrumentation (sensors, actuators, embedded programming, energy) over transmission (networks, gateways) to back-end (storage, analytics).

We study the **socio-technical context and implications** of IoT systems.

Our method is experimental: We **build/evaluate** prototypes. We deploy demonstrators. We collect and curate **data sets**.

We focus on IoT systems **contributing to the UN 2030 Agenda**.

IoT data lifecycles




THE THINGS
NETWORK
COPENHAGEN
Vasbygade
Amager Fælled
Royal Golf Center
Course
Englandsvej
Copenhagen
SHUTTLEWORTH
FUNDED

Agenda: Networking, part 1

- Scope
- **Criteria for IoT Networks**
- Properties of the Physical Layer
- **Overview of relevant IoT Network Options in 2019**
- Link budgets, dBms, etc
- **LoRa & LoRaWAN**

A little introductory discussion

We call it the **Internet of Things** – why?

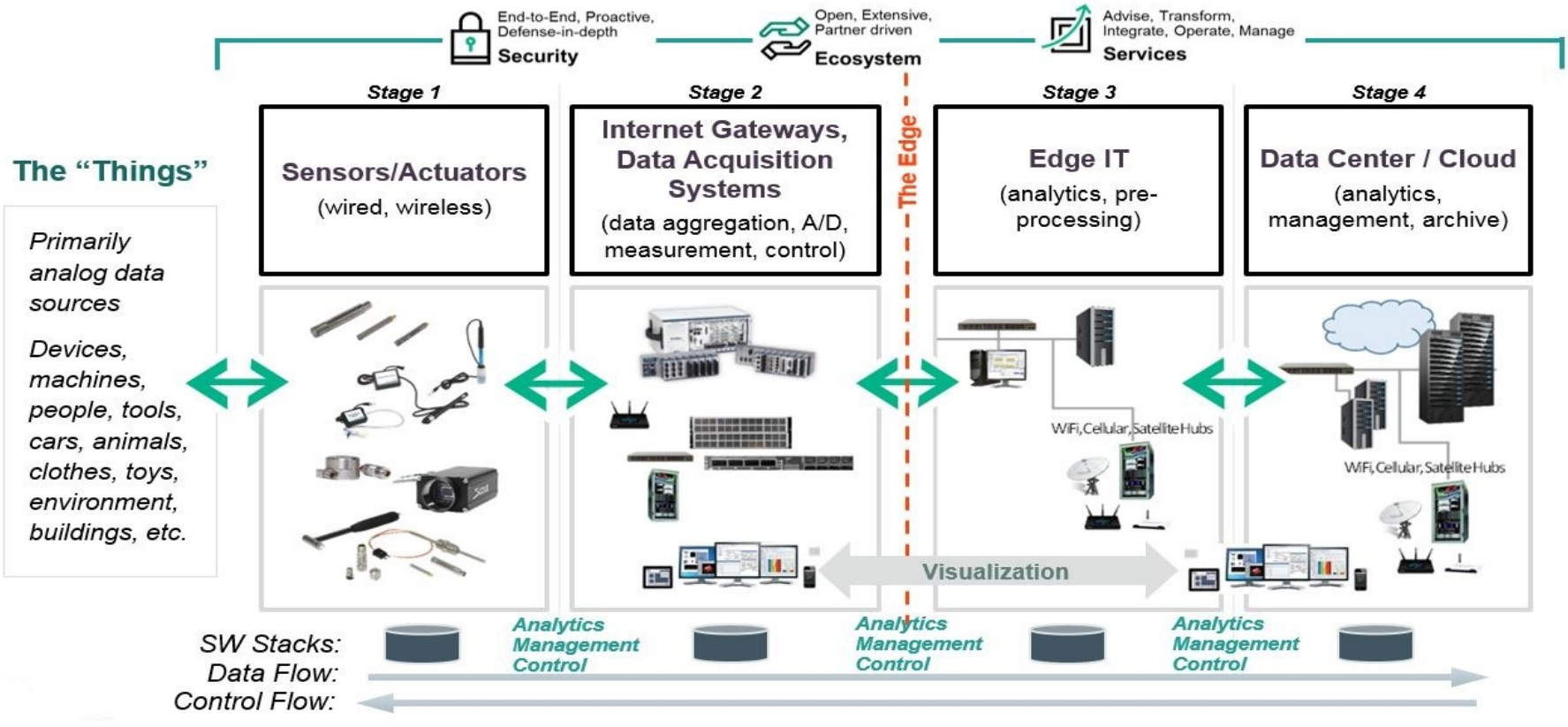
What about it is “Internet”, and in what way?

Terminology

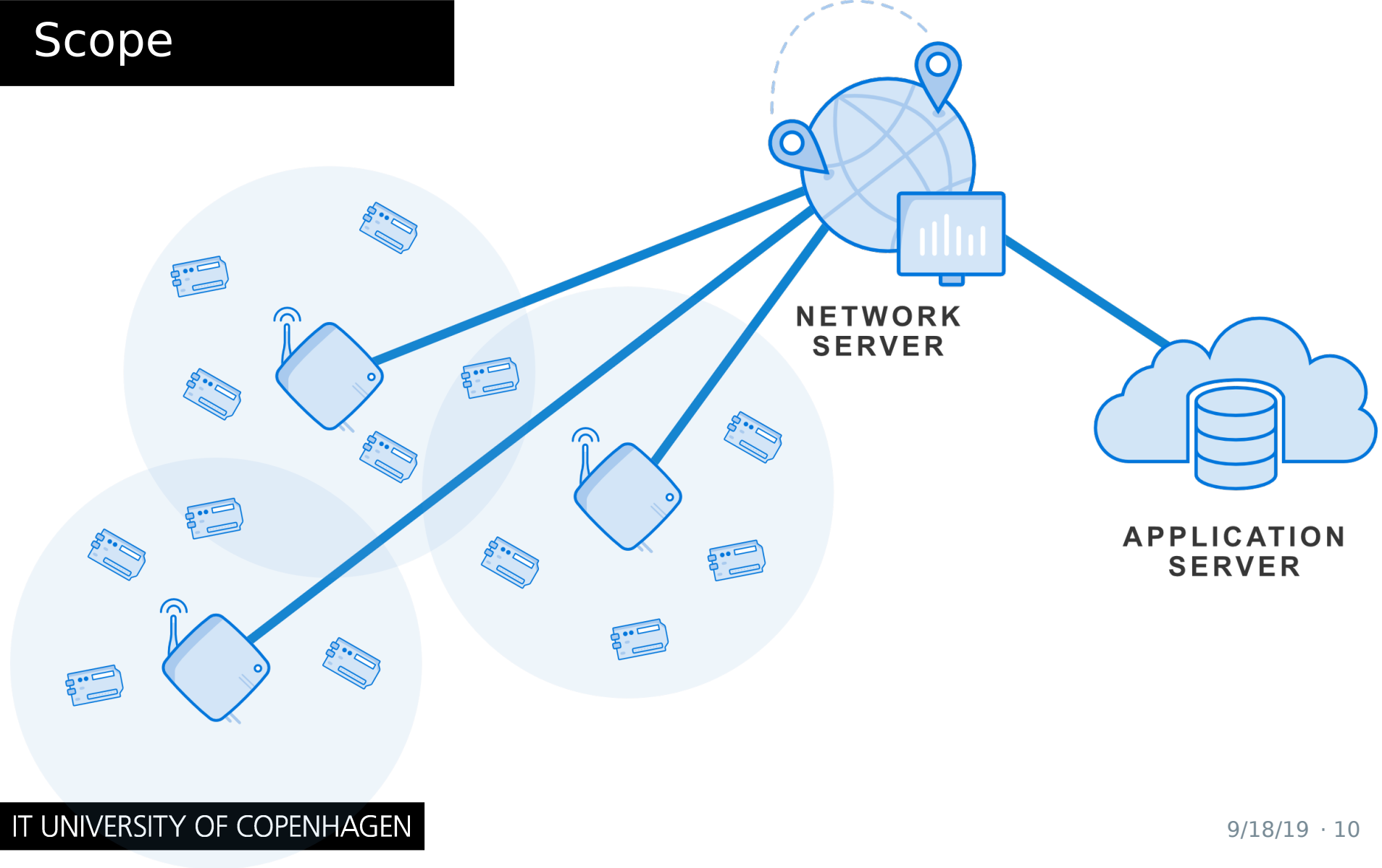
- **Sensor:** the part that creates the actual measurement
- **Sensor node** or **Device:**
  - the Sensor + a lot more:
  - MCU/CPU, network, storage, etc

Scope

The 4 Stage IoT Solutions Architecture

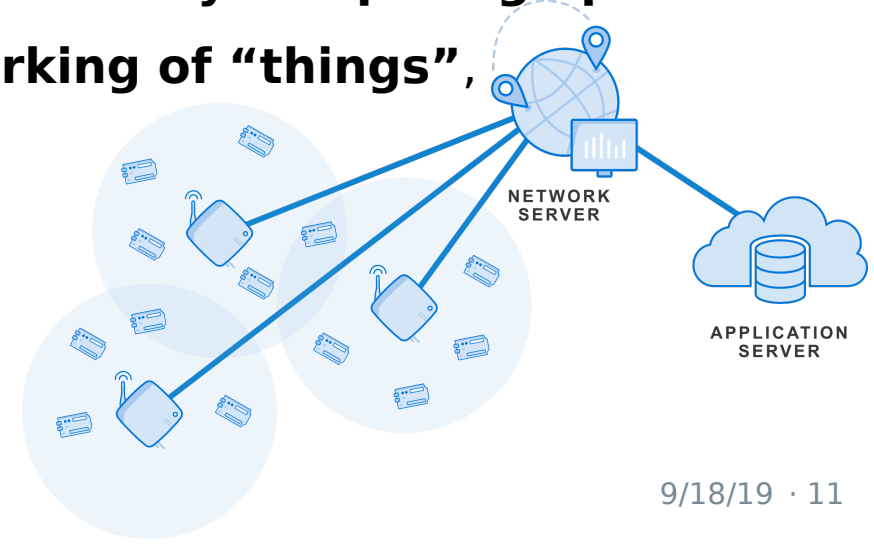


Scope



Scope

- Between the four (or more) stages/tiers in IoT systems: **networks**
- Connectivity in the **backend is mostly of conventional type** (internet infrastructure – **fiber, cables**, etc – tcp/ip, https, …)
- Connectivity on the first meters, for the actual “things” (from sensors, nodes, motes to gateways, APs, base stations) is still an **emerging landscape with many competing options**
- This lecture is mostly about **networking of “things”**, less about the backend.



Scope

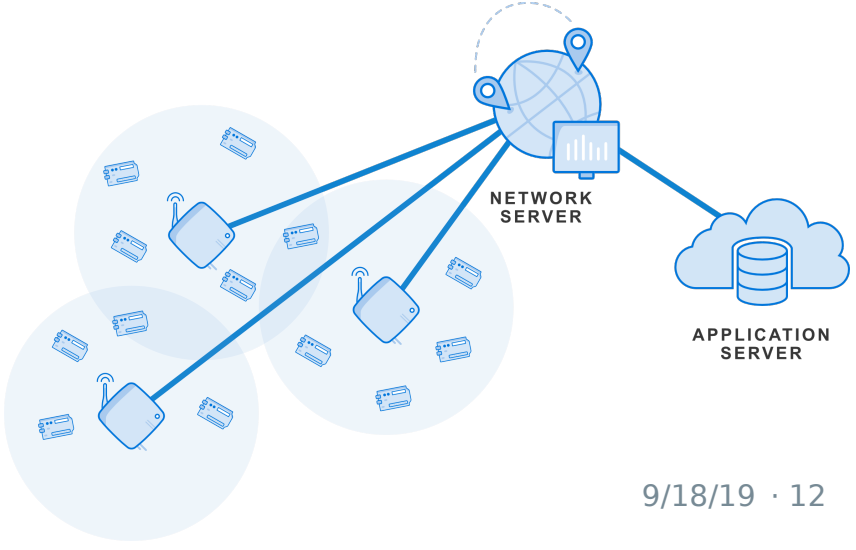
- **However – never forget:**

  No IoT,

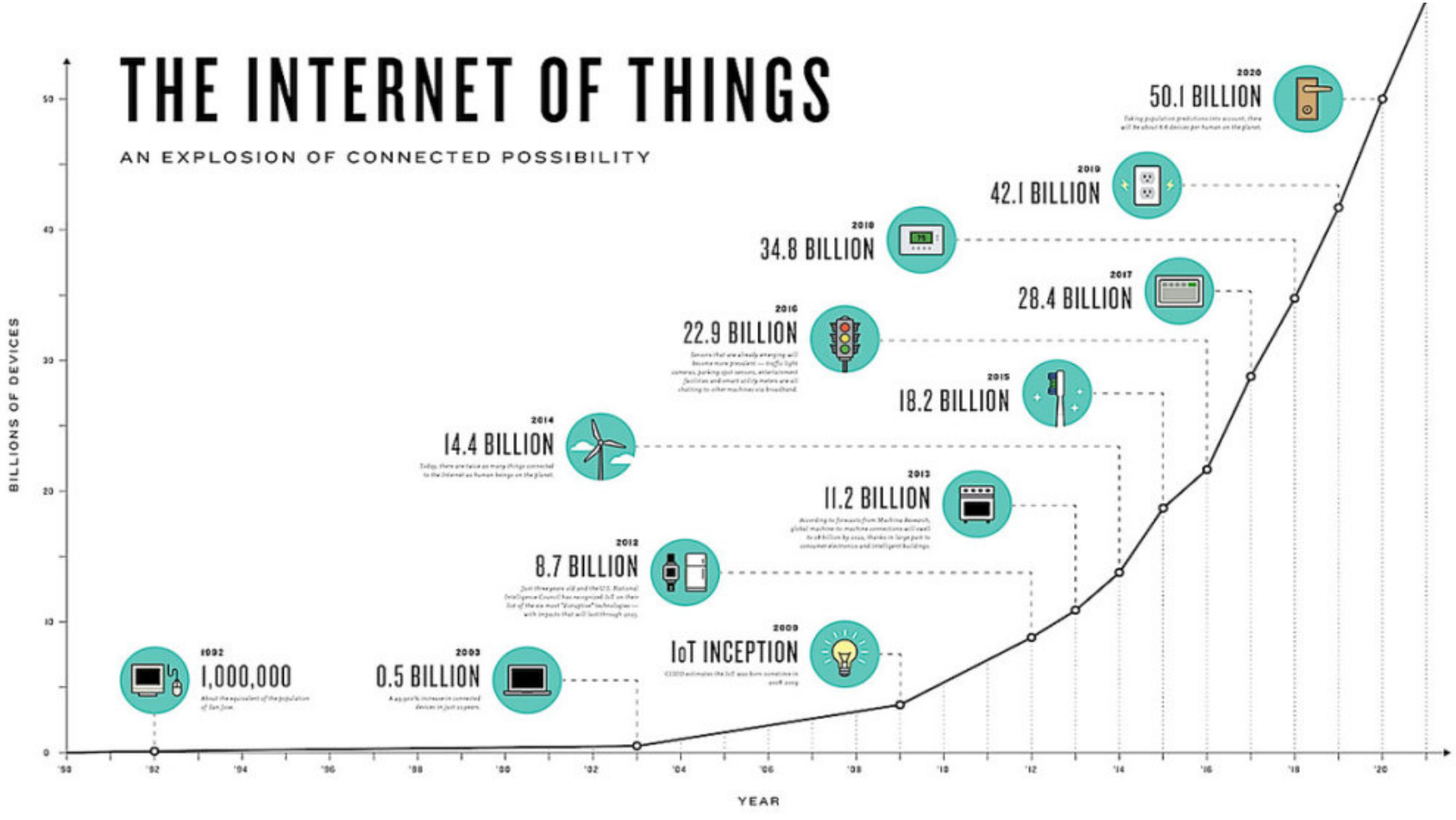
  no wireless or mobile networks

  can exist without a

  solid <u>wired</u> backbone

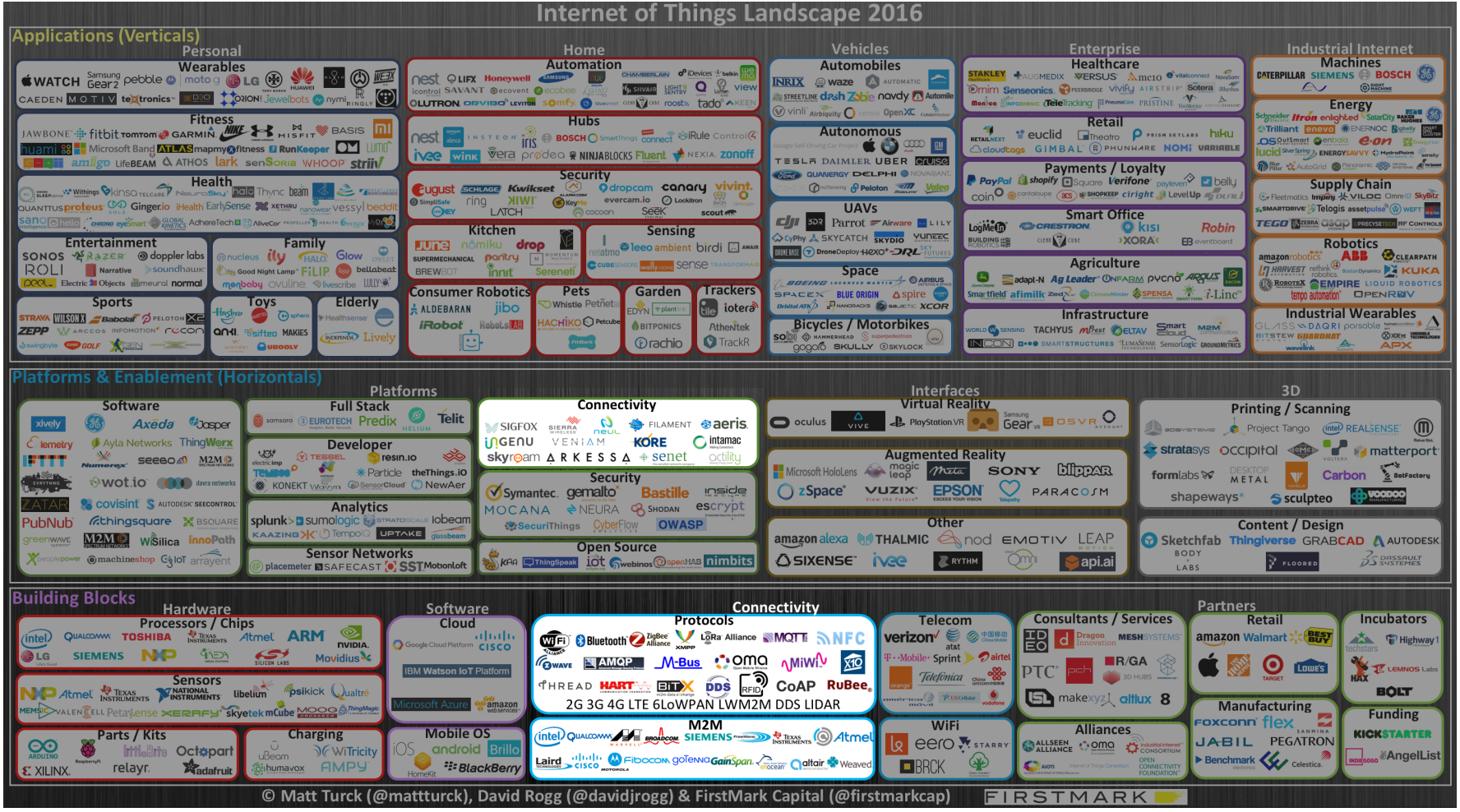


Number of things



Source:NCTA - https://www.ncta.com

Scope


Internet of Things Landscape 2016
Applications (Verticals)
Personal
Wearables
Fitness
Health
Entertainment
Family
Sports
Toys
Elderly
Home
Automation
Hubs
Security
Kitchen
Sensing
Consumer Robotics
Pets
Garden
Trackers
Vehicles
Automobiles
Autonomous
UAVs
Space
Bicycles / Motorbikes
Enterprise
Healthcare
Retail
Payments / Loyalty
Smart Office
Agriculture
Infrastructure
Industrial Internet
Machines
Energy
Supply Chain
Robotics
Industrial Wearables
Platforms & Enablement (Horizontals)
Platforms
Software
Full Stack
Developer
Analytics
Sensor Networks
Connectivity
Security
Open Source
Interfaces
Virtual Reality
Augmented Reality
Other
3D
Printing / Scanning
Content / Design
Building Blocks
Hardware
Processors / Chips
Sensors
Parts / Kits
Charging
Software
Cloud
Mobile OS
Connectivity
Protocols
2G 3G 4G LTE 6LoWPAN LWM2M DDS LIDAR
M2M
Telecom
WiFi
Consultants / Services
Alliances
Partners
Retail
Manufacturing
Incubators
Funding
© Matt Turck (@mattturck), David Rogg (@davidjrogg) & FirstMark Capital (@firstmarkcap)
FIRSTMARK

Classification of Sensor Nodes

We can look at sensor nodes by ...

- **Locality:** Stationary / moving
- **Power:** autonomous / semi-autonomous (depending on recharge, battery) / grid

These two largely determine our network options.

Scope

Options for networking things:

- Wires & cables & fiber
- *Conventional* human connectivity networks (WiFi, Bluetooth)
- Mobile (GSM/2G/3G, LTE/4G, 5G …)
- LPWAN (Low Power Wide Area Networks)
- Satellite (which can mean many things)

Criteria

In order to navigate the confusing landscape, we need a clear understanding of our **criteria** – how do we choose the right option (or one of them) for a given case?

The ideal IoT network	
reaches far and wide	(*reach, coverage)*
to send a lot (and fast!)	*(data rates, bandwidth, time)*
over a long time	*(power, autonomy)*
at little cost	*(business aspects)*
(in a legal manner)	

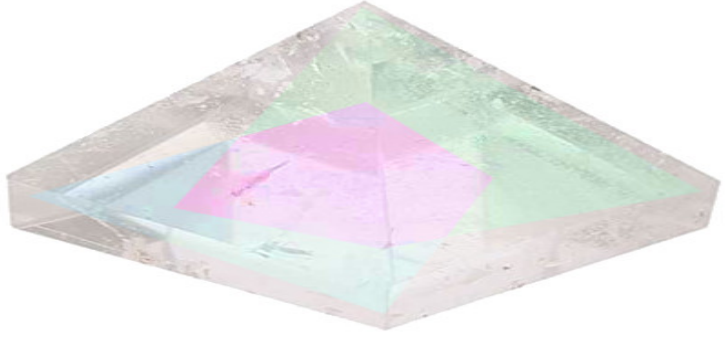
Criteria

In reality, we will not be able to have all of it, at the same time – luckily, we typically do not need all of it either.

It s a balance act – balancing trade-offs.

reach

data



power

cost

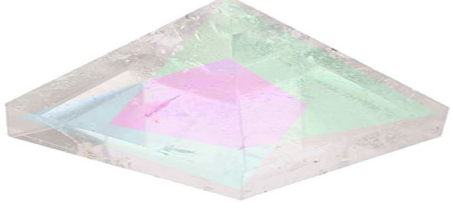
Criteria

IoT Networks often are characterized by

- very low data rate – **just a few bytes**
- low power – **long lifetime**
- **low cost** per node
- range/reach may vary
- time characteristics might vary

reach

data



power

cost

Criteria

reach

Distances

LOS (line of sight) / NLOS (non line of sight)

Coverage: local / regional / global?

One/many locations?

Mobility?

Roaming?

Criteria

bandwidth / data rates

packet sizes – how much do I need to send?

flexibility of packets – does size vary?

capacity/scale - how many nodes?

up/downlink – do I need to push updates etc to nodes?

time!

latency – synchronous vs. asynchronous

do I need my in data real-time? how much, how often?

Precision – esp. when doing

Geolocation over Time of Flight

Criteria

cost ($)

cost of hardware, networks, infrastructure, people, ..

business model – provider, self-driven, public, ...?

legalities/regulations – in all locations

Criteria - Power

Some comments on power

(The main power cost is transmission/networking

(no rule without exception though – need to verify!)

Processor: typically < 1 nJ per Instruction

Acquiring a digital data sample from a sensor: order of 1 nJ

Networking: Example: WiFi

100 mW (pure radio power, no periphery) gives you in the range of 10 Mb/s ==> 10 nJ/bit ==> 100 nJ / 10bit sample

Power uptake of radio chips is typically several times the radio output power

(scales quadratically with distance)

==> Sending the sample requires 100x more power than sampling it!

Cases

Some examples:

Discuss the Criteria for …

The SEA-HAZEMON nodes

Criteria - ....

Have we not forgotten something?

Yes.

The “S” in IoT stands for Security.

Criteria - Security

The “S” in IoT stands for Security.

Security deserves its own chapter.

While it is obviously one of our criteria,

it is very dangerous to choose a networking option based on security,

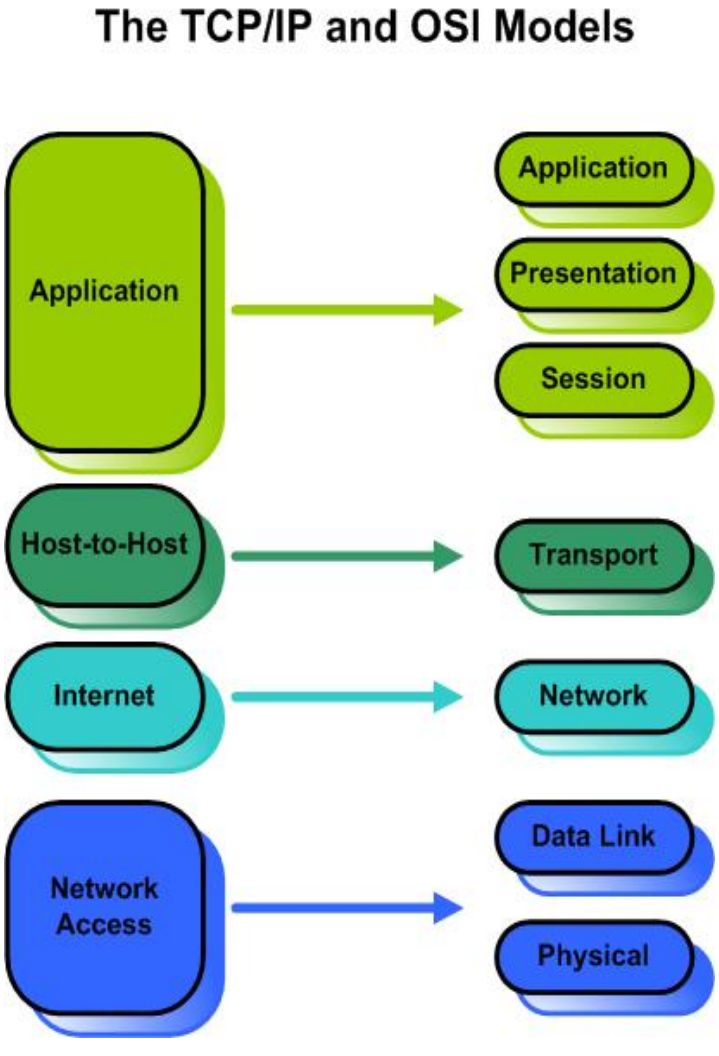
and then assume that the system is “secure”.

Vulnerabilities on the physical network layers are just some of many more.

Obviously, we will demand certain minimal security features on the networking level – device authentication, session encryption, etc

Some of these may be additional, not supplied by the networking platform as such.

Layer Models



Layer Models / Discussion

Examples for Discussion:

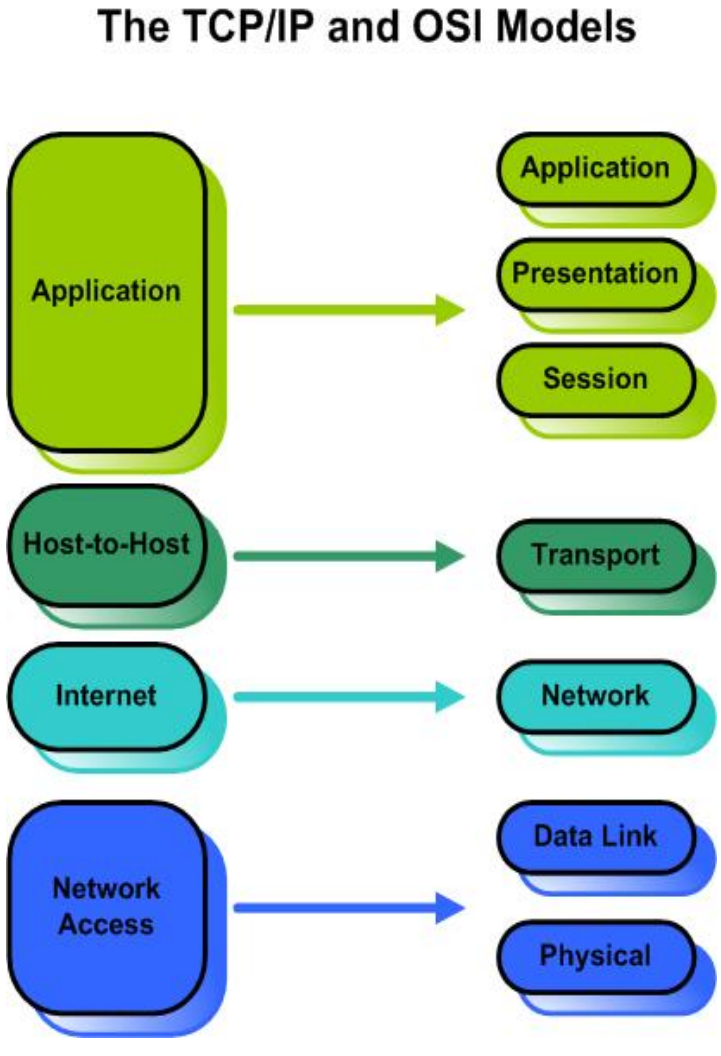
Where do these belong?

… a web browser?
… 923 MHz?
… a copper cable?
… Wi-Fi?

Can we do IP over Bluetooth?

Can we have MQTT without IP?

Can you do LoRa on 2.4 GHz?



Properties of the physical layer

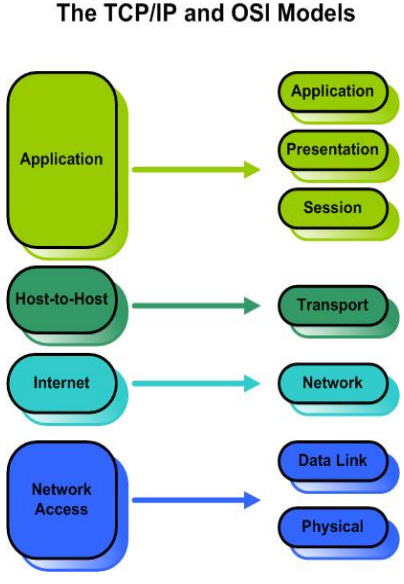
A quick view on the physical layer (Layer 1)

The first, raw physical layer (PHY) consists of

Copper, glass, electromagnetics, optics,
Waves, beams -

before any modulation (Layer 2, MAC)
or protocols of higher layers comes into effect.

https://en.wikipedia.org/wiki/Physical_layer



Properties of the physical layer

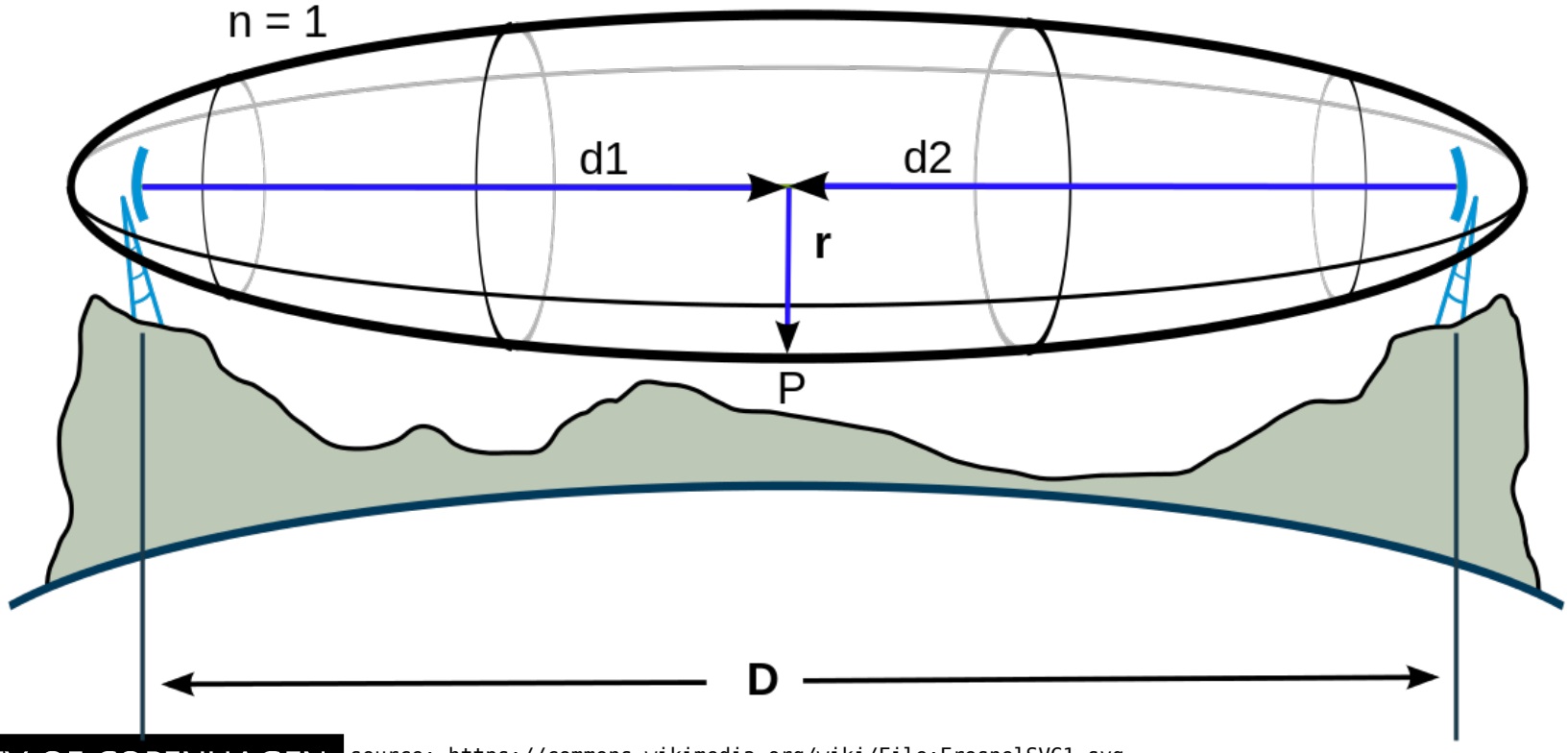
For all wireless (electromagnetic, radio) communications, some simplified rules:

Low frequency **Long wavelength**	**High frequency** **Short wavelength**
Better penetration ***Longer range***	***Easily blocked*** ***Shorter range***
Better NLOS capability	***Strictly LOS***
Less data *	***More data ****

**** because more bandwidth is available at higher frequencies***

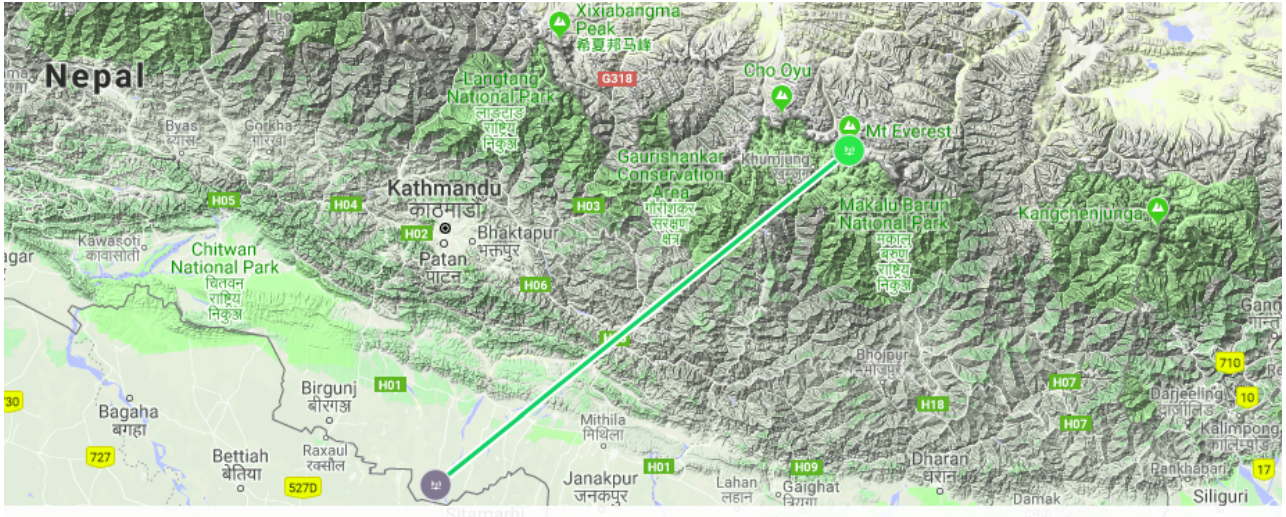
LOS vs NLOS

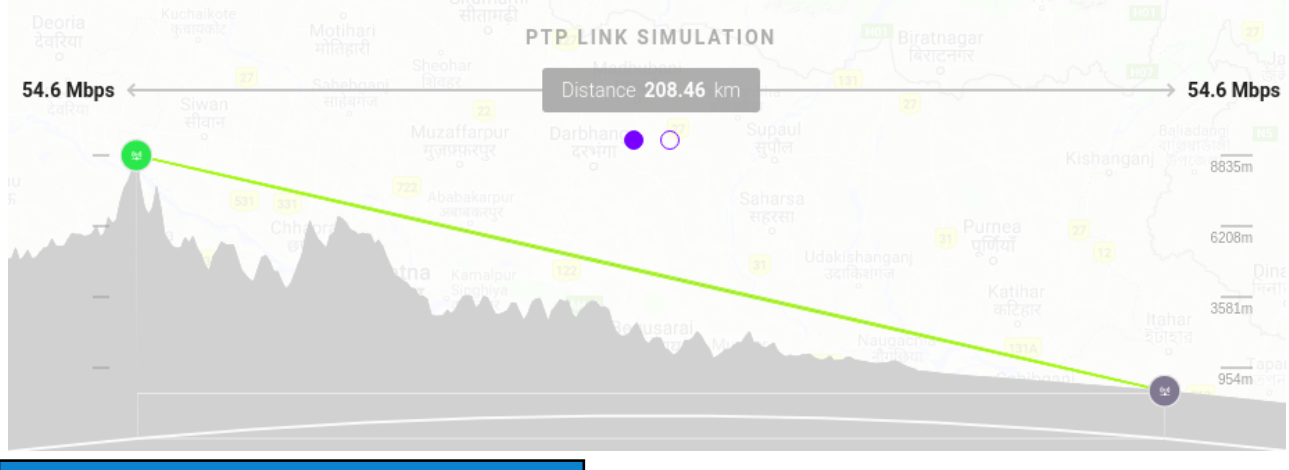
Line-of-sight (LOS), non-Line-of-sight (NLOS)
Fresnel zones



source: https://commons.wikimedia.org/wiki/File:FresnelSVG1.svg

The case for … mountains

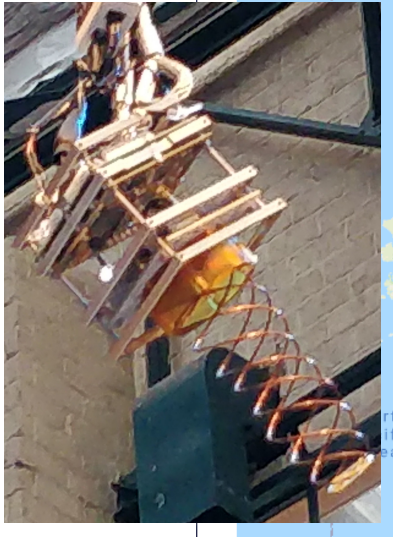




Mountain topologies help us get around **Earth Curvature**

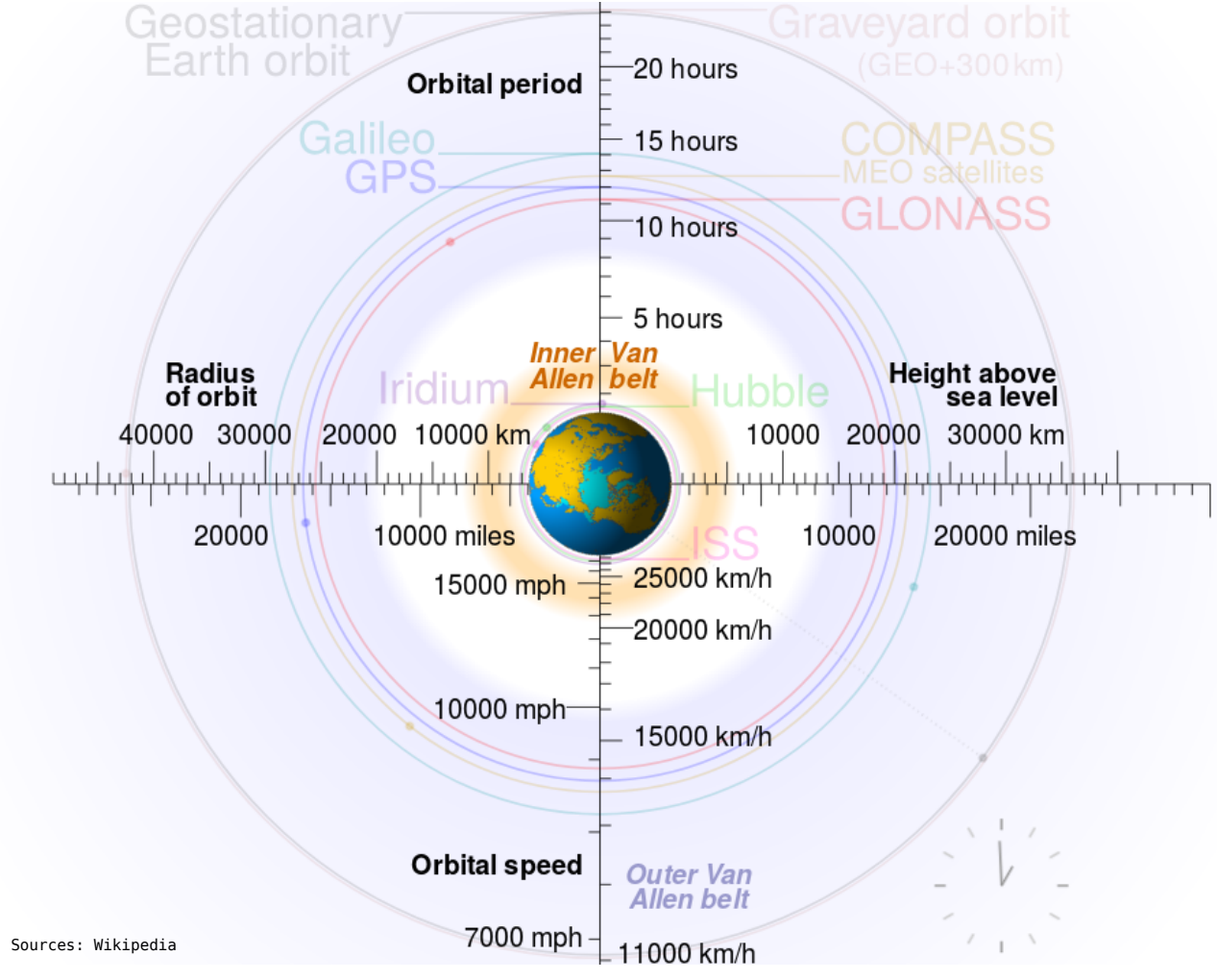
Link simulation for a Nepal project, 2019

The case for … satellites



Sources: lacuna.space, talia.net

Satellite orbits



Sources: Wikipedia

Bandwidth, throughput, data rates

The **Shannon–Hartley theorem** describes the **maximum rate** at which information can be transmitted over a communications **channel** of a specified **bandwidth** in the presence of **noise**.

Statement of the theorem [edit source]

The Shannon–Hartley theorem states the channel capacity C, meaning the theoretical tightest upper bound on the information rate of data that can be communicated at an arbitrarily low error rate using an average received signal power S through an analog communication channel subject to additive white Gaussian noise of power N:

$$C = B \log_2 \left(1 + \frac{S}{N}\right)$$

where

- C is the channel capacity in bits per second, a theoretical upper bound on the net bit rate (information rate, sometimes denoted I) excluding error-correction codes;
- B is the bandwidth of the channel in hertz (passband bandwidth in case of a bandpass signal);
- S is the average received signal power over the bandwidth (in case of a carrier-modulated passband transmission, often denoted C), measured in watts (or volts squared);
- N is the average power of the noise and interference over the bandwidth, measured in watts (or volts squared); and
- S/N is the signal-to-noise ratio (SNR) or the carrier-to-noise ratio (CNR) of the communication signal to the noise and interference at the receiver (expressed as a linear power ratio, not as logarithmic decibels).

source: https://en.wikipedia.org/wiki/Shannon%E2%80%93Hartley_theorem

The Essence of the Shannon-Hartley Theorem

Capacity ~ Bandwith x log(Signal-to-Noise)

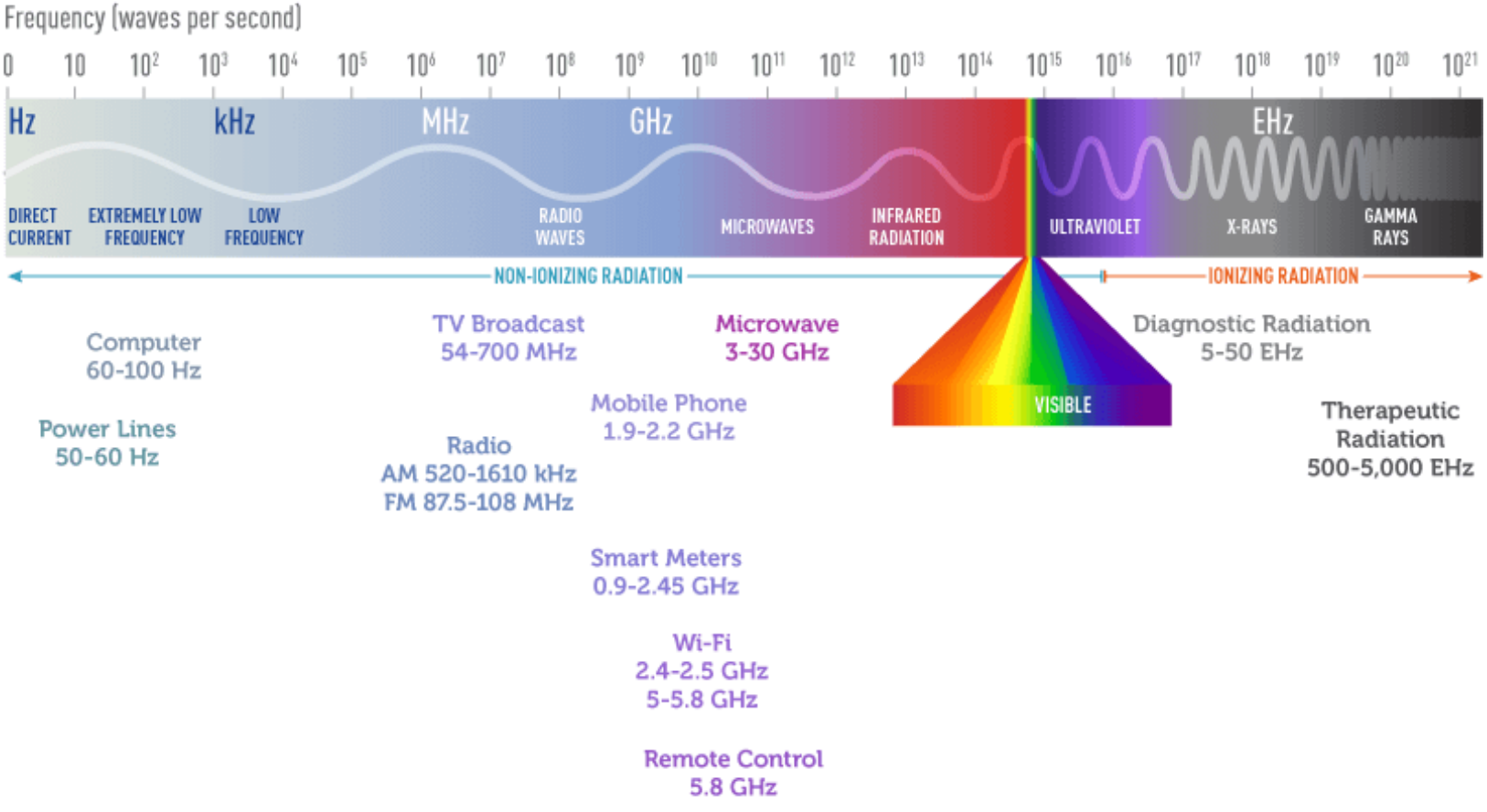
Capacity (Data Rate) does NOT directly depend on operating frequency,

however

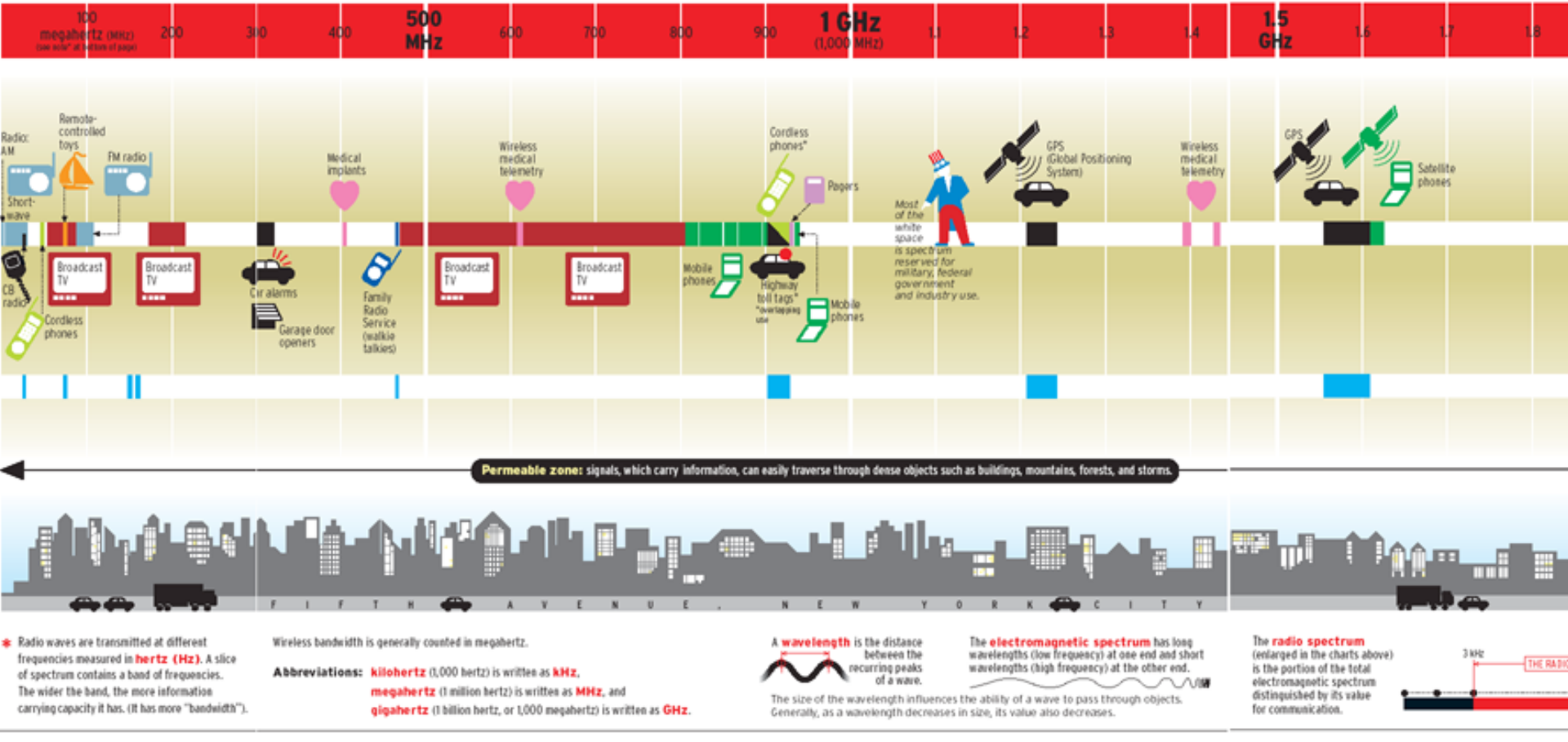
larger bandwidths are available at higher frequencies.

source: https://en.wikipedia.org/wiki/Shannon%E2%80%93Hartley_theorem

Frequency spectrum



Frequency spectrum



* Radio waves are transmitted at different frequencies measured in **hertz (Hz)**. A slice of spectrum contains a band of frequencies. The wider the band, the more information carrying capacity it has. (It has more "bandwidth").

Wireless bandwidth is generally counted in megahertz.

Abbreviations: **kilohertz** (1,000 hertz) is written as **kHz**, **megahertz** (1 million hertz) is written as **MHz**, and **gigahertz** (1 billion hertz, or 1,000 megahertz) is written as **GHz**.

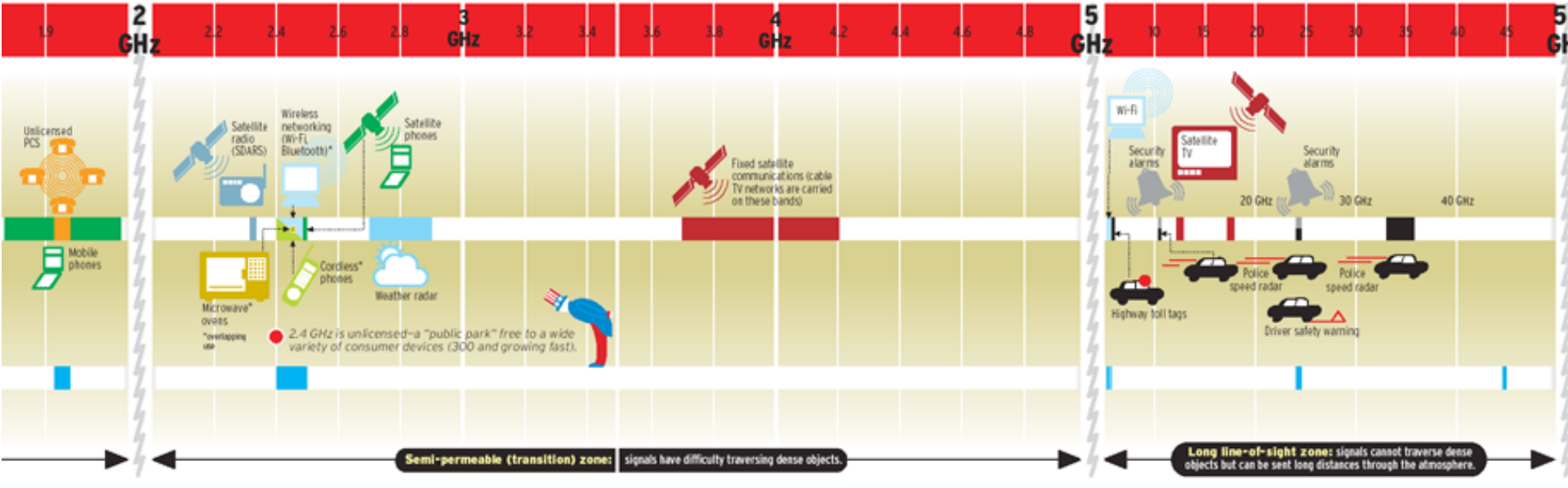
A **wavelength** is the distance between the recurring peaks of a wave.

The **electromagnetic spectrum** has long wavelengths (low frequency) at one end and short wavelengths (high frequency) at the other end.

The size of the wavelength influences the ability of a wave to pass through objects. Generally, as a wavelength decreases in size, its value also decreases.

The **radio spectrum** (enlarged in the charts above) is the portion of the total electromagnetic spectrum distinguished by its value for communication.

Frequency spectrum

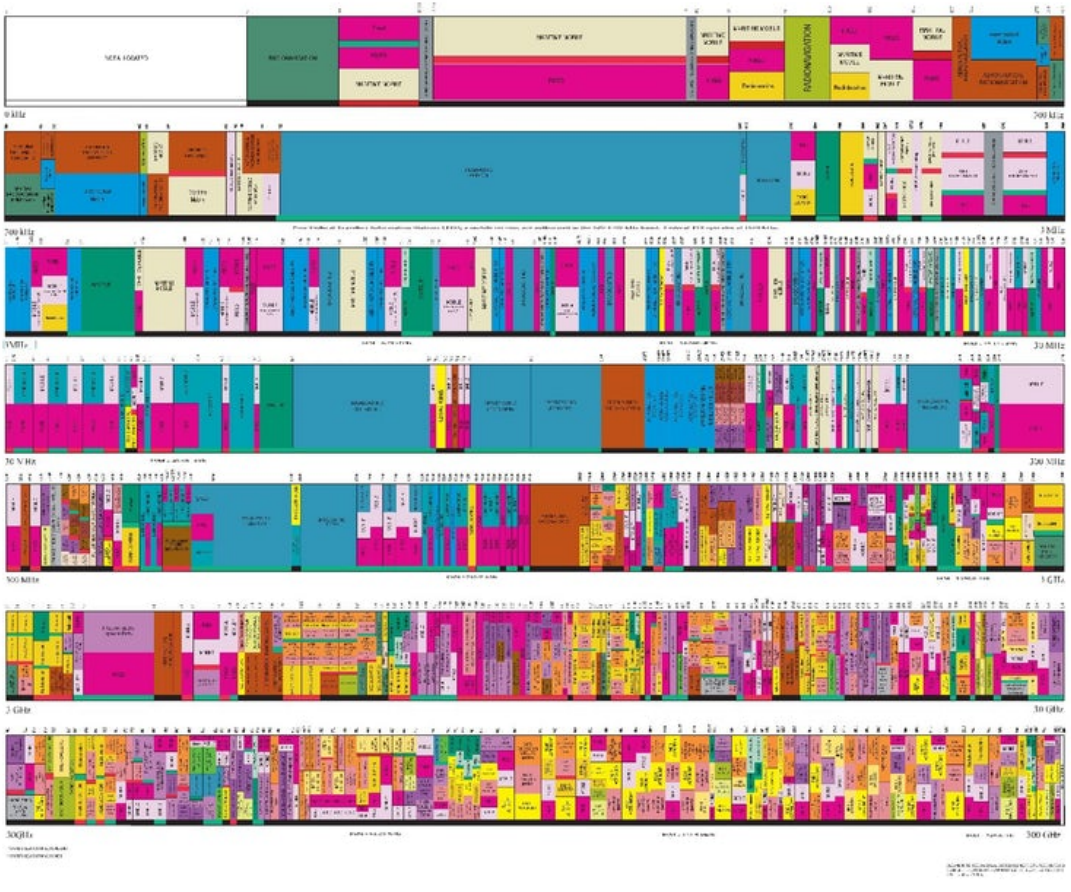


The amount of spectrum required for everyday communications

Today, most wireless communication is low fidelity audio. In the future, high fidelity video could require up to 5,000 times as much bandwidth.

"The basic problem is that demand for spectrum is outstripping the supply."
U.S. General Accounting Office Report, September 2002

Frequency allocation



source: DARPA, https://newatlas.com/darpa-radio-bandwidth-grand-challenge/

Frequencies relevant to us

- **ISM (Industrial Scientific Medical - license exempt) bands** at
  - 169 MHz – 170 cm - emerging ...
  - 433 MHz – 70 cm
  - 868 (EUR, Africa) / 915 (US) / 923-925 (AS2) MHz – 35 cm
  - 2.4 GHz – 802.11b/g – 12 cm
  - 5.x GHz – 802.11a – 5...6 cm
- Other (non-ISM) bands interesting to us
  - 470 – 790 MHz (TVWS)
  - 700-800-900 MHz (GSM)
  - All cellular (e.g. 1.8 – 2.7 GHz)
  - New 5G bands FR1 (<6 GHz, e.g. 3.5 GHz), FR2 (>26 GHz)
  - Other proprietary bands

Modulation & encoding

In electronics and telecommunications, **modulation is the process of varying one or more properties of a periodic waveform, called the carrier signal, with a modulating signal that typically contains information to be transmitted.** Most radio systems in the 20th century used frequency modulation (FM) or amplitude modulation (AM) to make the carrier carry the radio broadcast.

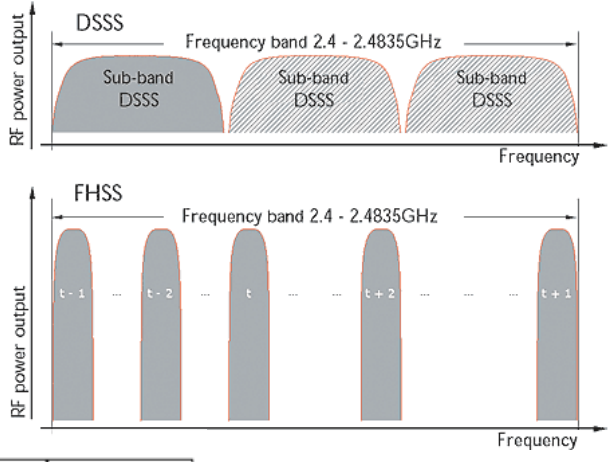
Modulation techniques include
Spread Spectrum (e.g. FHSS Frequency Hopping) used in Bluetooth,
direct-sequence spread spectrum (DSSS) used in 802.11b,
Orthogonal frequency-division multiplexing (OFDM) used in 802.11a/g/n/c,
Chirp spread spectrum (CSS) as used in LoRa.

These techniques are crucial for the **robustness against noise and utilization of spectrum.**

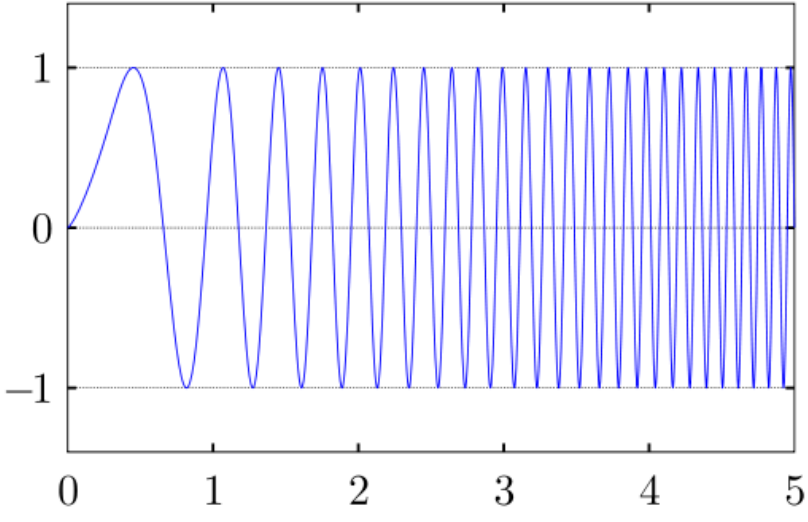
Read more here:
https://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum

Modulation & encoding

Spread Spectrum (e.g. **FHSS Frequency Hopping**) used in Bluetooth,
direct-sequence spread spectrum (DSSS) used in 802.11b,



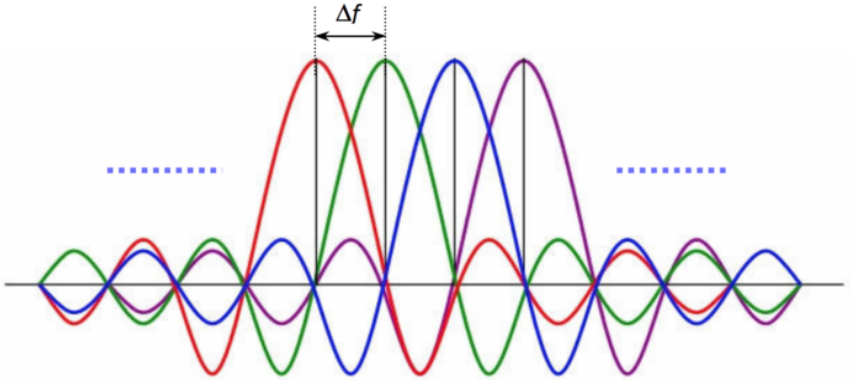
Chirp spread spectrum (CSS) as used in LoRa.



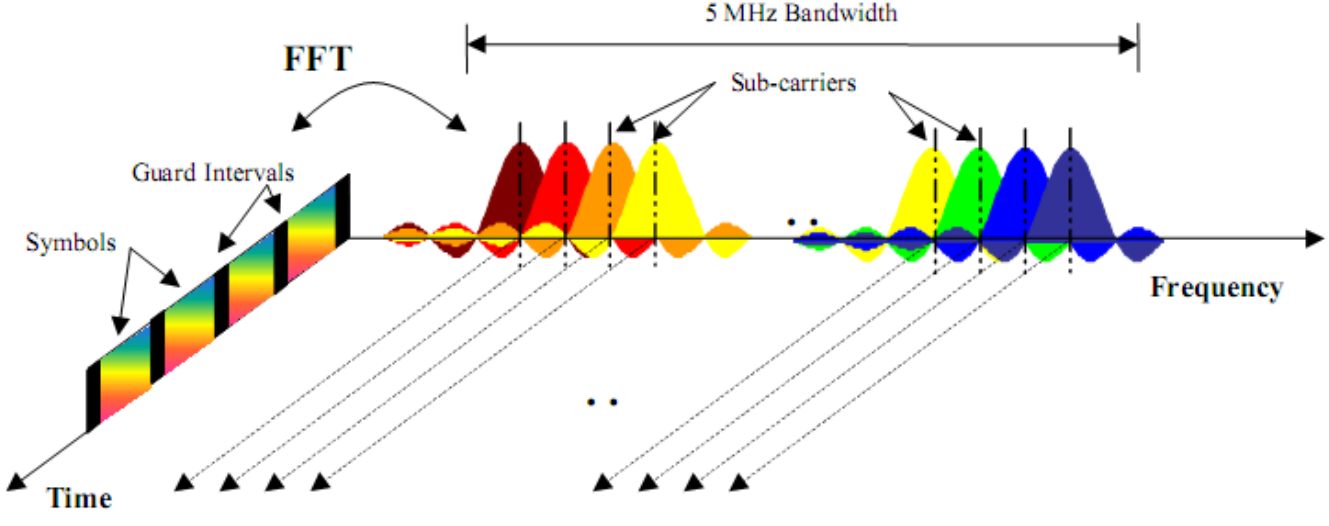
Source:
IEBMedia http://www.iebmedia.com/index.php?id=4466,
wikipedia

Modulation & encoding: OFDM

Idea: Overlapping carriers with a spacing such that neighbouring carriers' sidebands cancel each other out.
(Orthogonality)



Source:
IEBMedia http://www.iebmedia.com/ir
wikipedia



IoT Options – detailed comparisons

The main thing to look at when looking at the following comparison tables:

- where they come from, i.e. which **bias** you might find.

(also in these slides!)

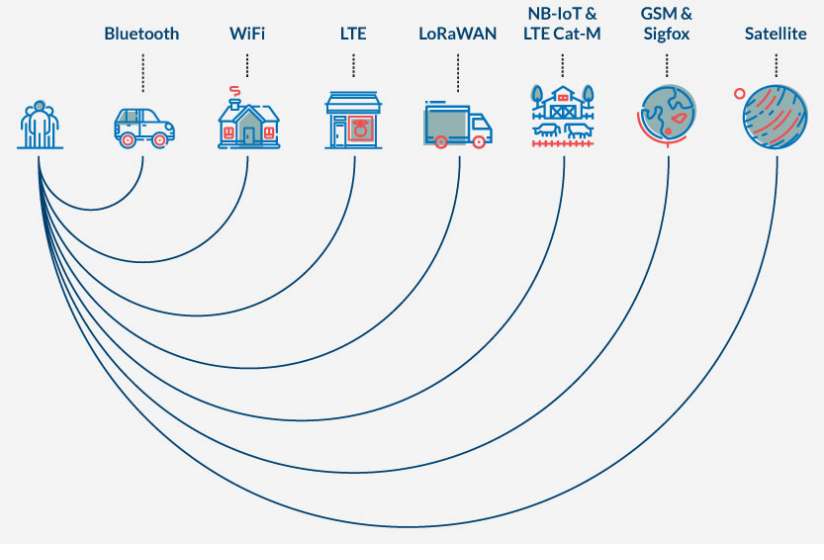
Even the most simple column in such overviews is almost impossible to fill with credible values -

e.g. what is the range/distance?

How far does LoRa go?

What about WiFi?

Sigfox?



IoT Options – rough overview

	Frequency	Modulation	Reach	Bandwidth	Data Rates	Power	Cost
LoRa	433, 868/915 MHz	Chirp SpreadS	10s of kms	125 kHz	Some 100 Bytes	low	Low (..)
Sigfox	868/915 MHz	UNB	10s of kms	100 Hz	Some Bytes	low	Low
LTE-_	1.8-2.7 GHz	OFDM	(km)	200 kHz	high	Mid	Mid
WiFi	2.4/5 Ghz	OFDM	100m .. 100 km	20/40 MHz/channel	high	high	Mid
Bluetooth	2.4 GHz	FHSS	10 m	1 MHz/channel	mid	mid	Low
RPMA	2.4 GHz	DSSS	10s of kms	80 MHz	(flexible)	low	Low (...)
Zigbee	433, 868/915 MHz	DSSS	100 m	MHz	bytes	Low	Low

IoT Options – detailed overviews

Comparison of Low-Power WAN Alternatives

Name of Standard	Weightless			SigFox	LoRaWAN	LTE-Cat M	IEEE P802.11ah (low power WiFi)	Dash7 Alliance Protocol 1.0	Ingenu RPMA	nWave
	-W	-N	-P							
Frequency Band	TV whitespace (400-800 MHz)	Sub-GHZ ISM	Sub-GHZ ISM	868 MHz/902 MHz ISM	433/868/780/915 MHz ISM	Cellular	License-exempt bands below 1 GHz, excluding the TV White Spaces	433, 868, 915 MHz ISM/SRD	2.4 GHz ISM	Sub-GHz ISM
Channel Width	5MHz	Ultra narrow band (200Hz)	12.5 kHz	Ultra narrow band	EU: 8x125kHz, US 64x125kHz/8x125kHz, Modulation: Chirp Spread Spectrum	1.4MHz	1/2/4/8/16 MHz	25 KHz or 200 KHz	1 MHz (40 channels available)	Ultra narrow band
Range	5km (urban)	3km (urban)	2km (urban)	30-50km (rural), 3-10km (urban), 1000km LoS	2-5k (urban), 15k (rural)	2.5- 5km	Up to 1Km (outdoor)	0 – 5 km	>500 km LoS	10km (urban), 20-30km (rural)
End Node Transmit Power	17 dBm	17 dBm	17 dBm	10µW to 100 mW	EU:<+14dBm, US:<+27dBm	100 mW	Dependent on Regional Regulations (from 1 mW to 1 W)	Depending on FCC/ETSI regulations	to 20 dBm	25-100 mW
Packet Size	10 byte min.	Up to 20 bytes	10 byte min.	12 bytes	Defined by User	~100 -~1000 bytes typical	Up to 7,991 Bytes (w/o Aggregation), up to 65,535 Bytes (with Aggregation)	256 bytes max / packet	Flexible (6 bytes to 10 kbytes)	12 byte header, 2-20 byte payload
Uplink Data Rate	1 kbps to 10 Mbps	100bps	200 bps to 100 kbps	100 bps to 140 messages/day	EU: 300 bps to 50 kbps, US:900-100kbps	~200kbps	150 Kbps ~ 346.666 Mbps	9.6 kb/s, 55.55 kbps or 166.667 kb/s	AP aggregates to 624 kbps per Sector (Assumes 8 channel Access Point)	100 bps
Downlink Data Rate	1 kbps to 10 Mbps	No downlink	200 bps to 100 kbps	Max 4 messages of 8 bytes/day	EU: 300 bps to 50 kbps, US:900-100kbps	~200kbps	150 Kbps ~ 346.666 Mbps	9.6 kb/s, 55.55 kbps or 166.667 kb/s	AP aggregates to 156 kbps per Sector (Assumes 8 channel Access Point)	--
Devices per Access Point	Unlimited	Unlimited	Unlimited	1M	Uplink:>1M, Downlink:<100k	20k+	8191	NA (connectionless communication)	Up to 384,000 per sector	1M
Topology	Star	Star	Star	Star	Star on Star	Star	Star, Tree	Node-to-node, Star, Tree	Typically Star. Tree supported with an RPMA extender	Star
End node roaming allowed	Yes	Yes	Yes	Yes	Yes	Yes	Allowed by other IEEE 802.11 amendments (e.g., IEEE 802.11r)	Yes	Yes	Yes
Governing Body	Weightless SIG			Sigfox	LoRa Alliance	3GPP	IEEE 802.11 working group	Dash7 Alliance	Ingenu (formerly OnRamp)	Weightless SIG
Status	Limited deployment awaiting spectrum availability	Deployment beginning	Standard in development. Scheduled release 4Q 2015	In deployment	Spec released June 2015, in deployment	Release 13 expected 2016	Targeting 2016 release	Released May 2015	In Deployment	In Deployment

Source: EDN.com - Copyright 2015 UBM Americas Rev. 9/15/15

Source: https://www.cnx-software.com/2015/09/21/comparison-table-of-low-power-wan-standards-for-industrial-applications/

IoT Options – detailed overviews

COMPARISON – main LPWAN technologies

Vertical M2M

Feature	LORAWAN	SIGFOX	LTE Cat 1	LTE M	NB - LTE
Modulation	SS chip	UNB / GFSK / BPSK	OFDMA	OFDMA	OFDMA
Rx Bandwith	500 – 125 KHz	100 Hz	20 MHz	20 – 1.4 MHz	200 KHz
Data Rate	290bps – 50Kbps	100 bit / sec 12 / 8 bytes Max	10 Mbit /sec	200 kbps – 1 Mbps	Average 20K bit / sec
Max. # Msgs/day	Unlimited	UL: 140 msgs / day	Unlimited	Unlimited	Unlimited
Max Outpu Power	20 dBm	20 dBm	23 – 46 dBm	23/30 dBm	20 dBm
Link Budget	154 dB	151 dB	130 dB+	146 dB	150 dB
Battery lifetime – 2000 mAh	105 months	90 months		18 months	
Power Efficiency	Very High	Very High	Low	Medium	Med high
Interference immunity	Very High	Low	Medium	Medium	Low
Coexistence	Yes	No	Yes	Yes	No
Security	Yes	No	Yes Oui	Yes	Yes
Mobility / localization	Yes	Limited mobility, No localization	Mobility	Mobility	Limited mobility, No localization

Source: LoRAWAN Alliance, 2015

www.vertical-m2m.com

Source: LoraWAN Alliance, 2015

IoT Options – views: license

Two categories of LPWA technologies

1. Free / Unlicensed bands

LoRa™ SIGFOX INGENU formerly ON-RampWireless

2. Proprietary / Licensed bands

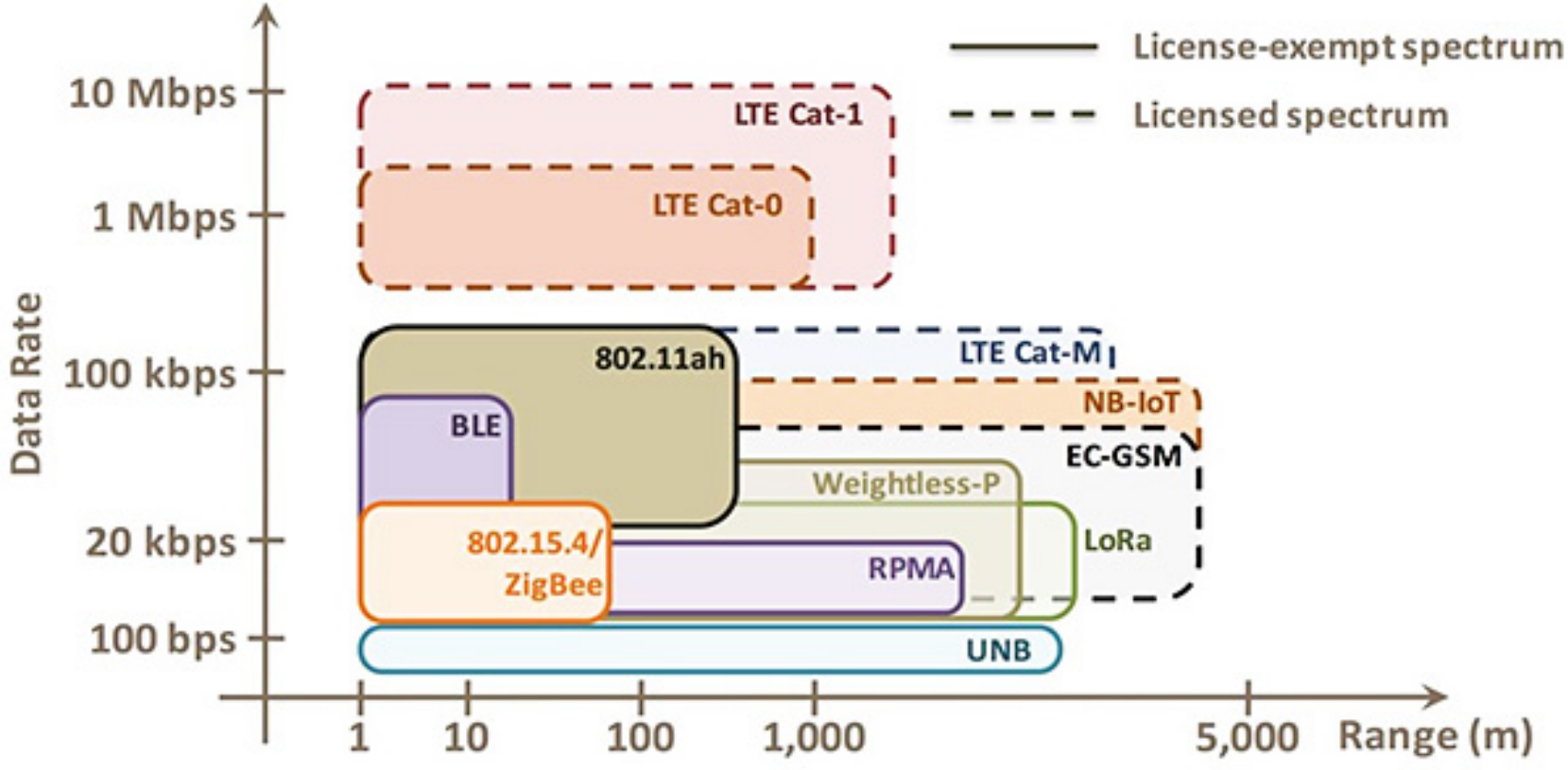
3GPP

1. **LTE-M** (aka LTE-MTC, Cat-M1)
2. **NB-IOT** (aka Cat-NB1)
3. **EC-GSM-IOT** (aka EC-GPRS)

SIERRA WIRELESS

Source: Sierra Wireless

IoT Options – views: range/license



IoT Options – comments on range

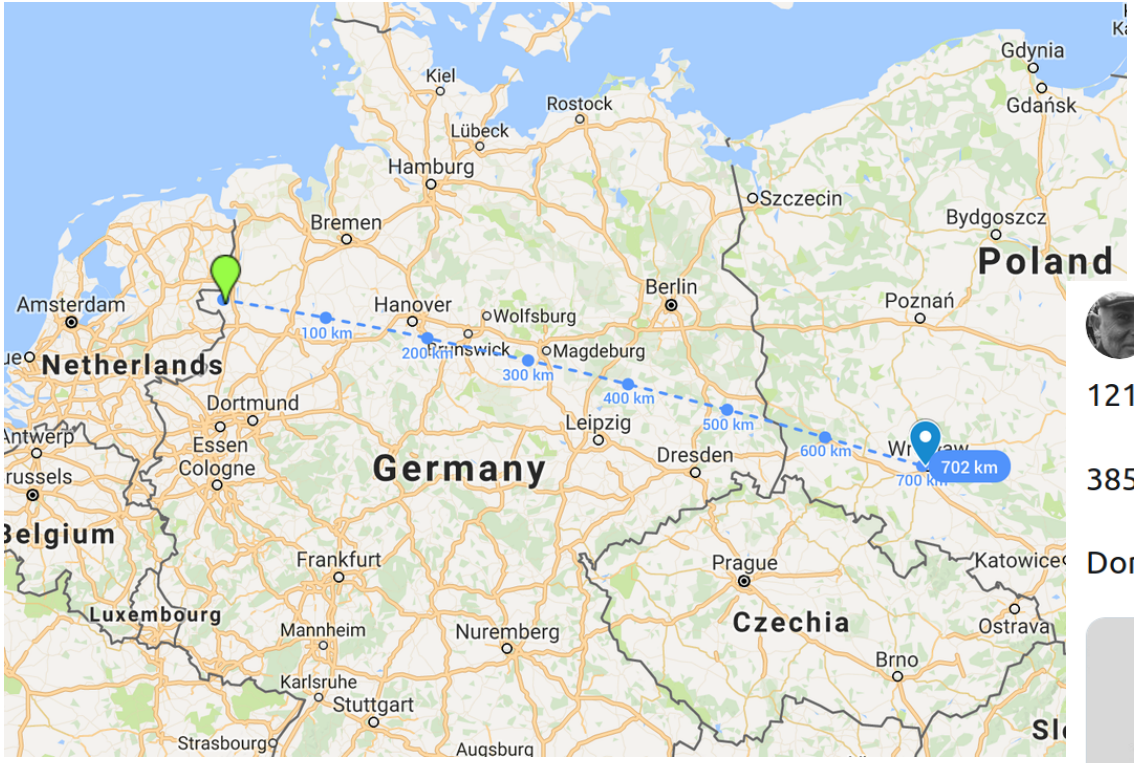
Range depends on who you ask …. some hints:

	Typical	**Record**	**Realistic, stable**
Bluetooth	some 10 m	?	10 m
Wi-Fi	100 m	378 km	100 km
LoRa	5-10 km	766/1200 km	100 km (...)

IoT Options – Wi-Fi World Record 382 km

Ermanno Pietrosemoli (ICTP, Eslared) and team

IoT Options – LoRa World Record(s)

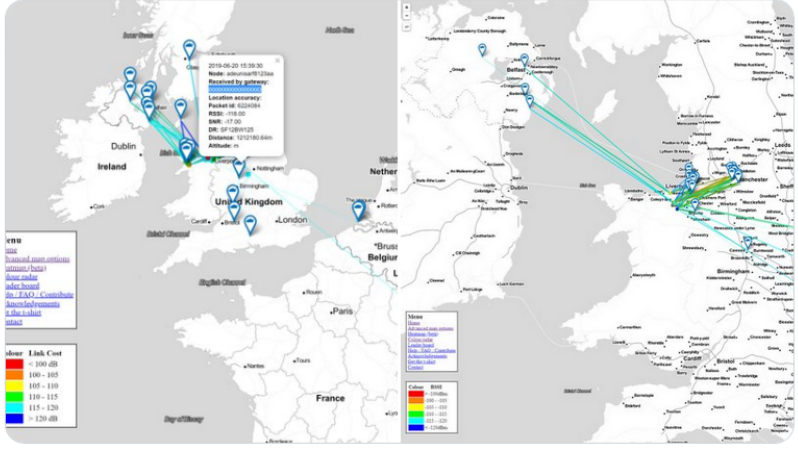


John Cassidy (M7DXO)
@JohnCassidyGB

1212km (SF12) from England to Italy.

385km (SF7) from Wales to England.

Done on @adeunisrf and @pycomIOT devices.



Terrestrial & with balloon

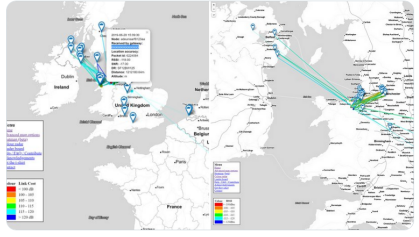
IoT Options – LoRa World Record(s)

John Cassidy (M7DXO)
@JohnCassidyGB

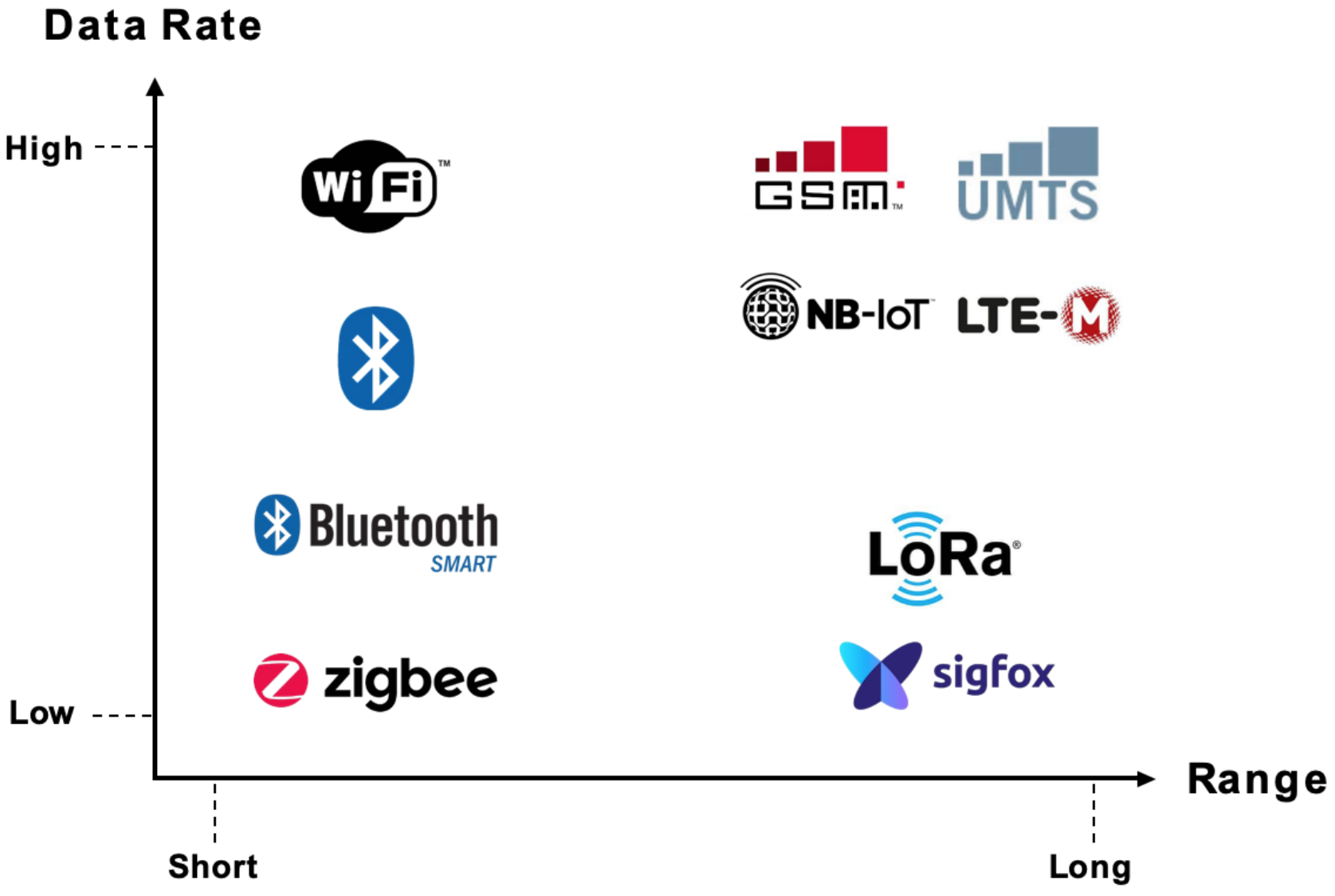
1212km (SF12) from England to Italy.

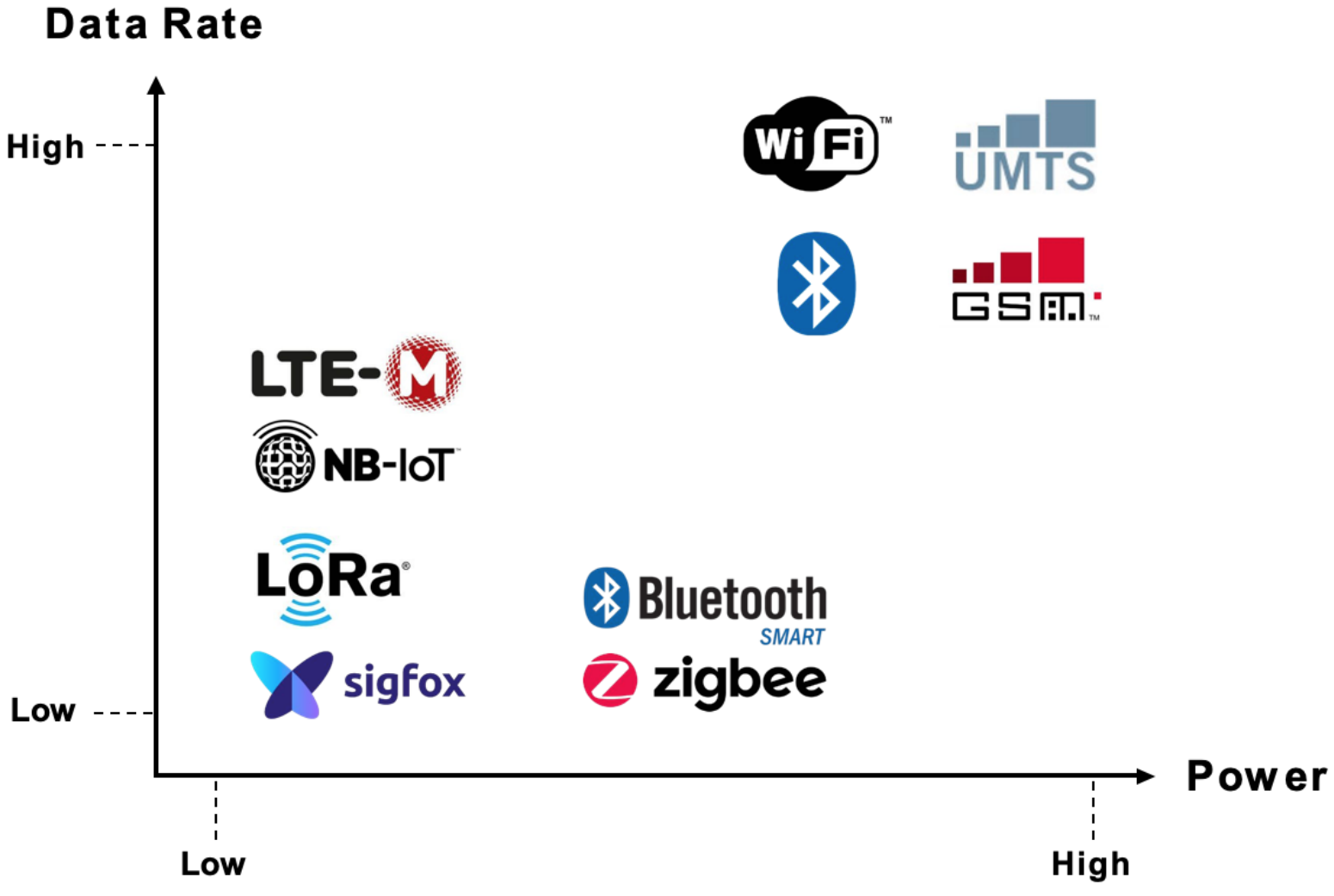
385km (SF7) from Wales to England.

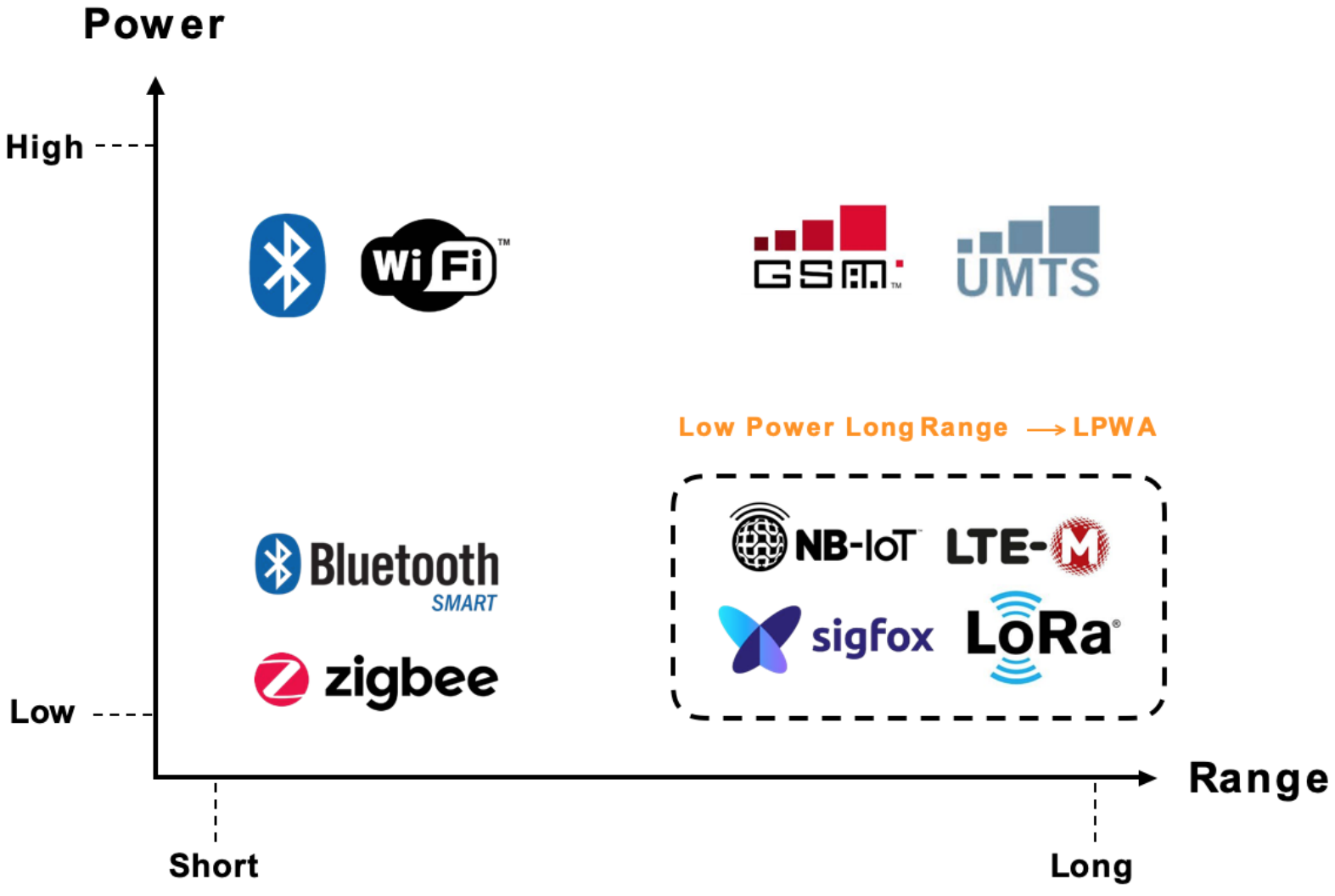
Done on @adeunisrf and @pycomIOT devices.



14 dBm / 25 mW! Pycom gear


Data Rate
High
Low
Short
Long
Range
Wi Fi
GSM
UMTS
NB-IoT
LTE-M
Bluetooth
SMART
LoRa
zigbee
sigfox


Data Rate
High
Low
Low
High
Power
Wi Fi
UMTS
GSM
LTE-M
NB-IoT
LoRa
sigfox
Bluetooth
SMART
zigbee


Power
High
Low
Short
Long
Range
Wi Fi
GSM
UMTS
Low Power Long Range → LPWA
NB-IoT
LTE-M
sigfox
LoRa
Bluetooth
SMART
zigbee

LPWAN & Cellular

LTE-M

NB-LTE

IEEE 802.11ah

EC-GSM

ZigBee3.0

Criteria

A quote by Nick Hunn - http://www.nickhunn.com/lora-vs-lte-m-vs-sigfox/

Sigfox – become a global Internet of Things operator

LoRa – provide a technology that lets other companies enable a global Internet of Things

LTE-M – evolve an existing technology to make more money for network operators

Criteria

A quote by Nick Hunn - http://www.nickhunn.com/lora-vs-lte-m-vs-sigfox/

There's a battle going on for the infrastructure technology that will support the Internet of Things. Currently the three most talked about contenders are Sigfox, LoRa and LTE-M. There are a lot of other alternatives and it's quite possible that none of LoRa, Sigfox nor LTE-M0 will win, but that's another story. If you search for LPWAN (Low Power Wireless Area Networks) you'll see that the battle for supremacy is a hot topic. It's largely because of the impending loss of the GPRS networks which power much of today's M2M business. As a result, almost every day you'll find another article debating their respective technical merits.

I'm going to argue that these comparisons miss the point. Which technology will win depends far more on the business model than on the underlying technology. The three technologies listed above are interesting to compare, as they exemplify three significantly different approaches to an IoT business, which can be broadly summed up as:

Sigfox – become a global Internet of Things operator

LoRa – provide a technology that lets other companies enable a global Internet of Things

LTE-M – evolve an existing technology to make more money for network operators

“LoRa – provide a technology that lets other companies enable a global Internet of Things”

LoRa PHY is a **proprietary**, chirp spread spectrum (CSS) radio modulation technology for LPWAN used by LoRaWAN, Haystack Technologies, and Symphony Link.

LoRaWAN is a media access control layer (MAC) protocol for managing communication between LPWAN gateways and end-node devices, maintained by the LoRa Alliance.

LoRaWAN defines the communication protocol and system architecture for the network while the LoRa physical layer enables the long-range communication link.

LoRa works on 169, 433 and 868/915 MHz ISM bands.

TheThingsNetwork is a “people’s IoT” project based on LoRa.

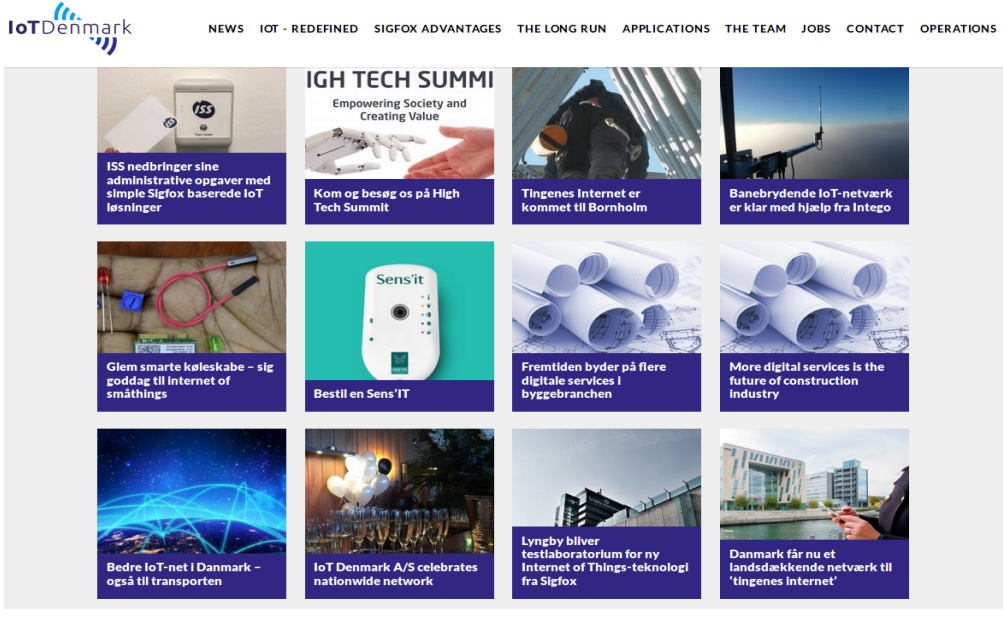
Commercial providers include **LORIOT.IO, Linklabs**

“Sigfox – become a global Internet of Things operator”

Like LoRa, Sigfox works on 433 and 868/915 MHz ISM bands.

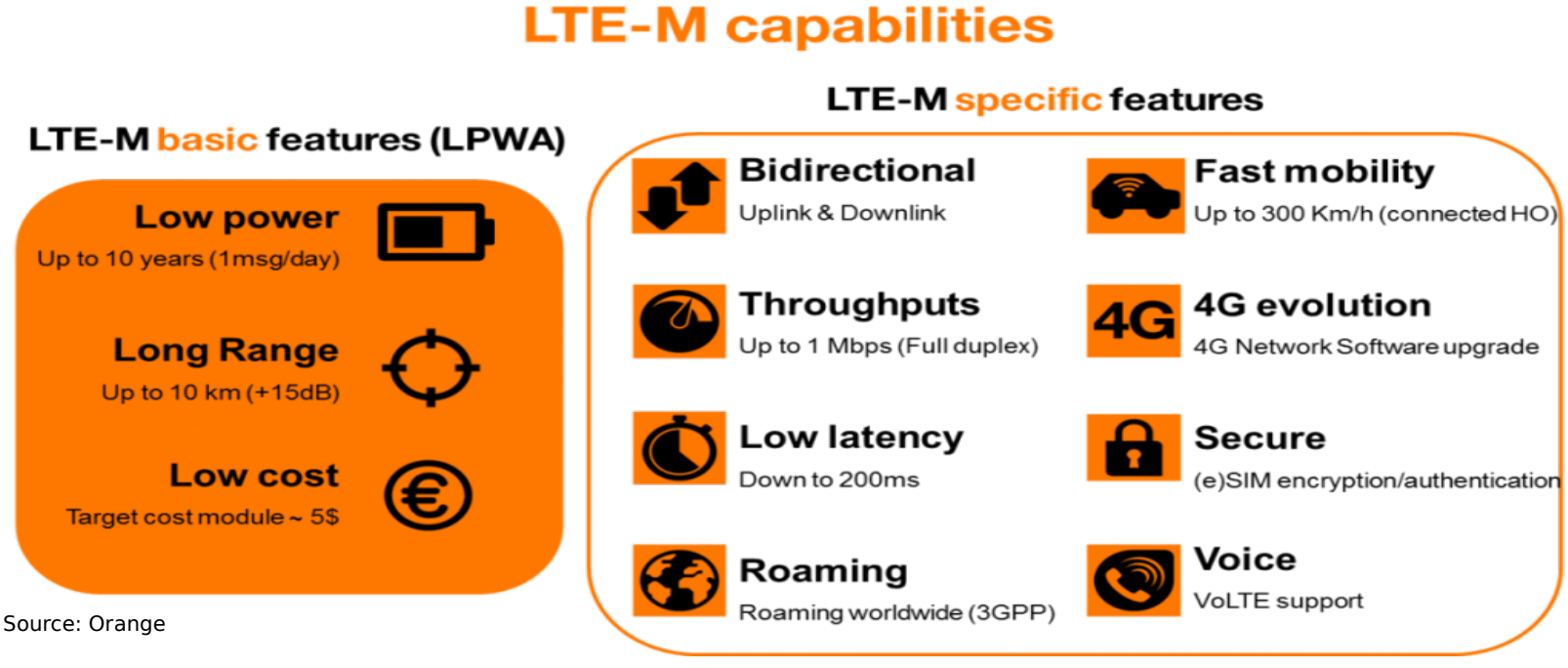
It uses UNB (Ultra narrow band) modulation technique.

A main difference lies in the business model: Sigfox is provided by an (exclusive) provider, just like mobile networks, on a subscriber basis.
In Denmark offered by http://iotdanmark.dk/



“LTE-M – evolve an existing technology to make more money for network operators”

Utilizing existing 5th generation mobile networks, seeking to enable those for IoT.



Source: Orange

802.15.4 is a Layer 1 & 2 standard, comparable to 802.11 for wireless

Zigbee is a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4-2003 standard for Low-Rate Wireless Personal Area Networks (LR-WPANs).
It specifies a.o. mesh routing, a slightly modified the AODV (Ad hoc On-Demand Distance Vector) standard (compare e.g. 802.11s)

6lowPAN = IPv6 over LoW Power wireless Area Networks. 6lowpan is the name of a working group in the internet area of the IETF. IPv6 packets over IEEE 802.15.4 based networks. RFC 4944/ RFC 4919.

Recap: Some basics in radio link calculation

Link budgets and dB

Link budget

is the calculation of losses and gains along a full signal path.

(Demonstrate by example)

Margin

Is the remaining signal left along the whole link

dB

Is the common unit used in radio link budgets

dB

- **Definition: $10 \times \text{Log}_{10} (P_1 / P_0)$**

- 3 dB = double power
  -3dB = half the power
  10 dB = one order of magnitude up = x 10
  -10 dB = one order of magnitude down = /10

- Calculating in dBs is easier :)

- Relative dBs
  - dBm = relative to 1 mW
  - dBi = relative to ideal isotropic antenna

dB

- **Definition: $10 \times \text{Log}_{10} (P_1 / P_0)$**

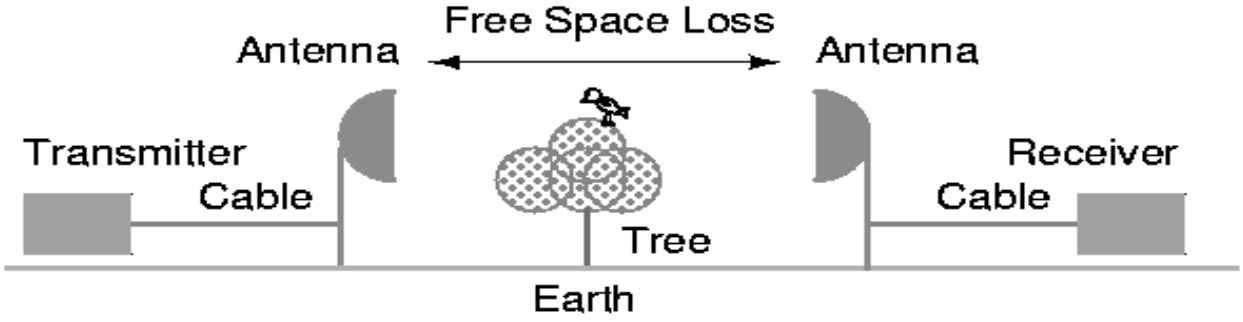
- 1 mW = 0 dBm
- 100 mW = 20 dBm
- 1 W = 30 dBm
- An omni antenna with 6 dBi gain
- A parabolic dish with 29dBi gain
- A cable (RG213) with 0.5 dB/m loss
- Maximum power of LoRa: 14 dBm = ….?
- WiFi?

Radio link

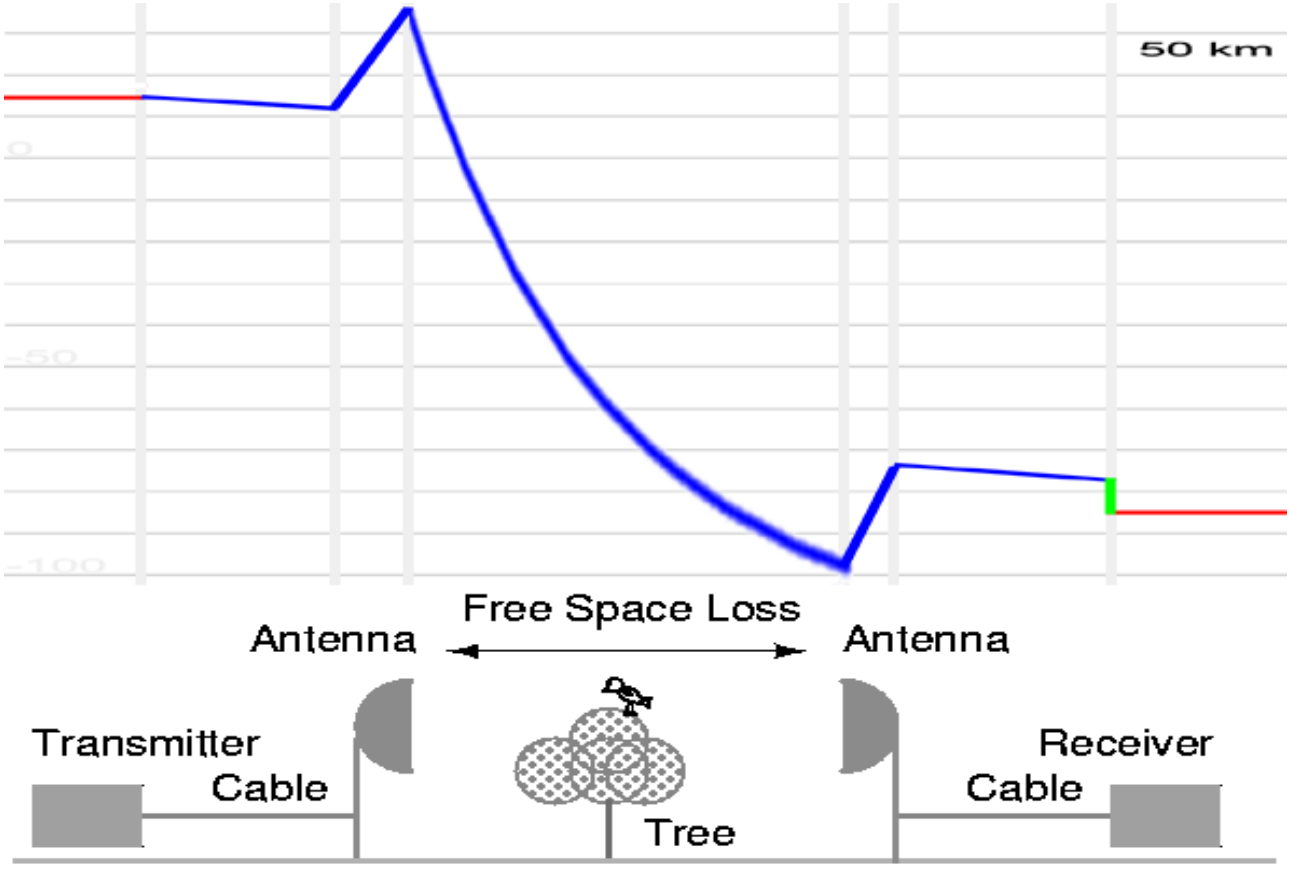
- **Effective transmit power:**
  transmit power [dBm]
  - (cable + connector) loss [dB]
  + amplifier gain [dB]
  + antenna gain [dBi]

- **Propagation loss [dB]:**
  Free space loss [dB]

- **Effective receiving sensibility:**
  antenna gain[dBi]
  + amplifier gain [dB]
  - cable loss [dB]
  - receiver sensitivity [dBm]



Link budget


50 km
Free Space Loss
Antenna
Antenna
Transmitter
Cable
Receiver
Cable
Tree

Take-Aways

- Criteria for networking options in IoT:
  Power, reach, bandwidth, cost,
  security, business aspects and more

- Properties of the physical layer: Frequency, bandwidth and their impact

- Basic terms: LPWA(N), LOS/NLOS, Modulation (Spread Spectrum)

- The most relevant options (in 2019) and their main characteristics:
  LPWANs: LoRa, Sigfox, NB-IoT,

  and others: Bluetooth, WiFi, Cellular (GSM, LTE-..), Satellite

LoRa / 1

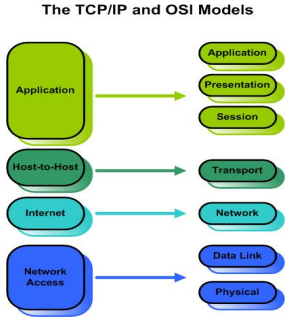
LoRa is a **proprietary Layer 1 standard** owned by Semtech

Chirp Spread Spectrum (CSS) with forward error coding and interleaving).

Bandwidth 125/250/500 kHz

Frequency in Europe: **ISM 433/868 Mhz**

Asia: often AS2 923-925 MHz



Data Rate up to 11 kbps

Focus is on **long range, power efficiency, robustness.**

https://www.semtech.com/lora/what-is-lora

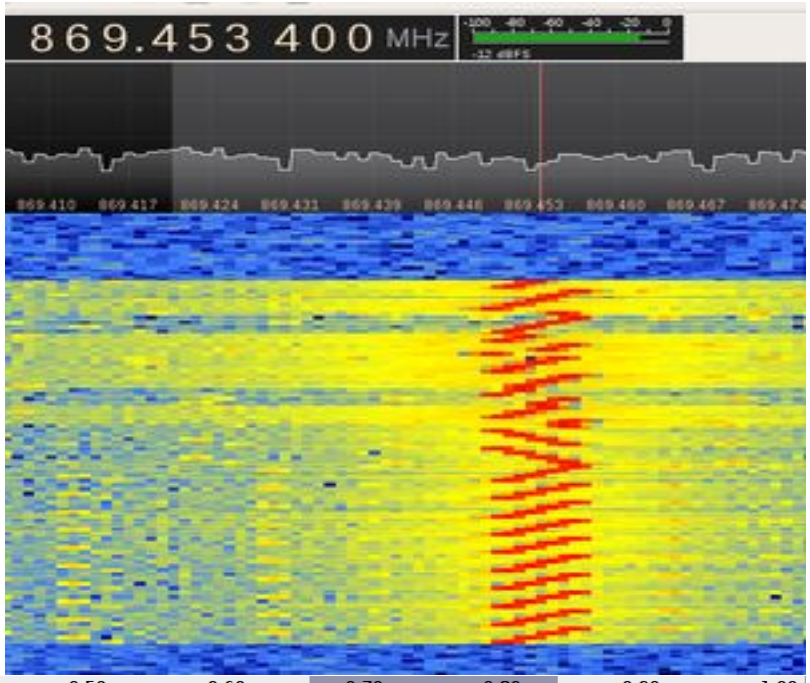
LoRa / 2 / CSS

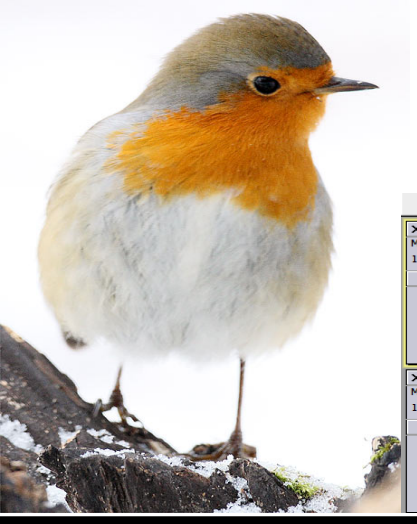
Chirp Spread Spectrum

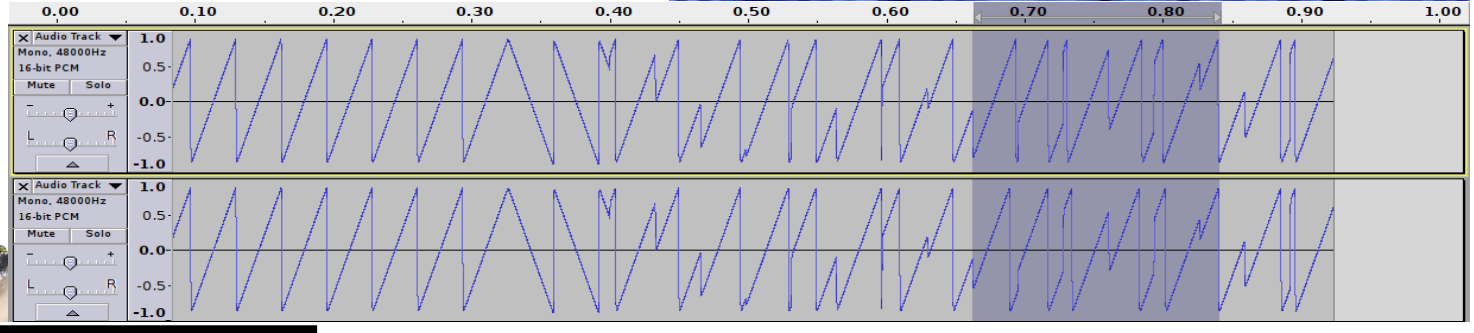
What is a chirp?

Source: https://revspace.nl/DecodingLora

Preamble (of variable length), here:
10 up, 2 down ->



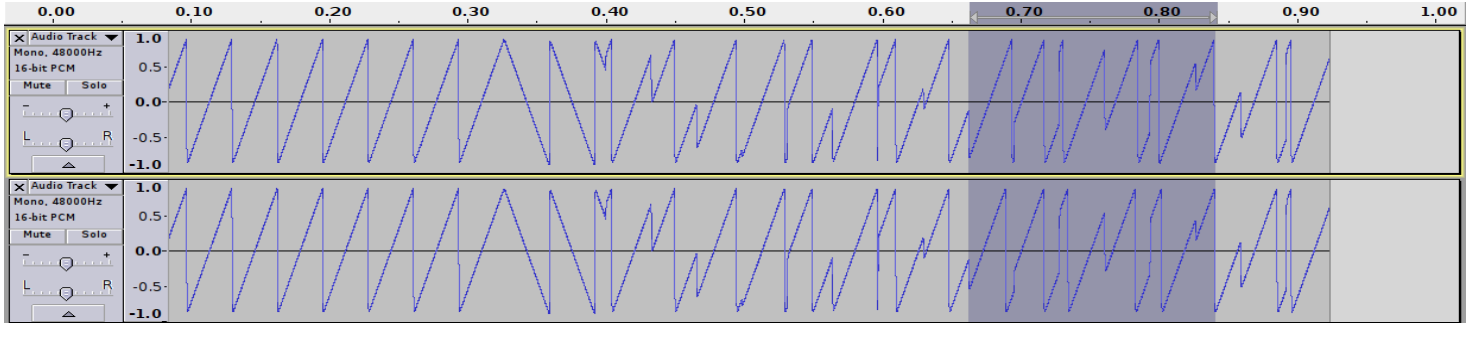




LoRa / 3 / CSS details

Modulation details, reverse engineering:

http://www.semtech.com/images/datasheet/an1200.22.pdf
https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN101.pdf
https://revspace.nl/DecodingLora#Modulation_basics
https://myriadrf.org/blog/lora-modem-limesdr/
https://static1.squarespace.com/static/54cecce7e4b054df1848b5f9/t/57489e6e07eaa0105215dc6c/1464376943218/Reversing-Lora-Knight.pdf



LoRa / 4 / SF & CR

Spreading Factor SF

$$\mathrm{SF} = \frac{\text{chip rate}}{\text{symbol rate}}$$

(think of it as “one bit is spread out over so and so many pulses”)

Control rate CR, determines depth of forward error coding
(Think of it as saying CCCAAAFFFEEE or CAFECAFECAFE instead of CAFE)

LoRa / 5 / Interleaving

“Mixing up the letters to gain robustness against *burst errors*”

```
Transmitted sentence:              ThisIsAnExampleOfInterleaving...
Error-free transmission:           TIEpfeaghsxlIrv.iAaenli.snmOten.
Received sentence, burst error:    TIEpfe______Irv.iAaenli.snmOten.
after deinterleaving:              T_isI_AnE_amp_eOfInterle_vin_...
```

LoRa / 6 / Data Rate

Data Rate depends on Bandwidth, CR, SF

$$R_b = SF * \frac{\left[\frac{4}{4+CR}\right]}{\left[\frac{2^{SF}}{BW}\right]} * 1000$$

SF = Spreading Factor (6,7,8,9,10,11,12)

CR = Code Rate (1,2,3,4)

BW = Bandwidth in KHz
(10.4,15.6,20.8,31.25,41.7,62.5,125,250,500)

Rb = Data rate or Bit Rate in bps

http://www.rfwireless-world.com/calculators/LoRa-Data-Rate-Calculator.html

LoRaWan / 1

- LoRaWan is an open LPWAN standard building on top of LoRa
- https://www.lora-alliance.org/

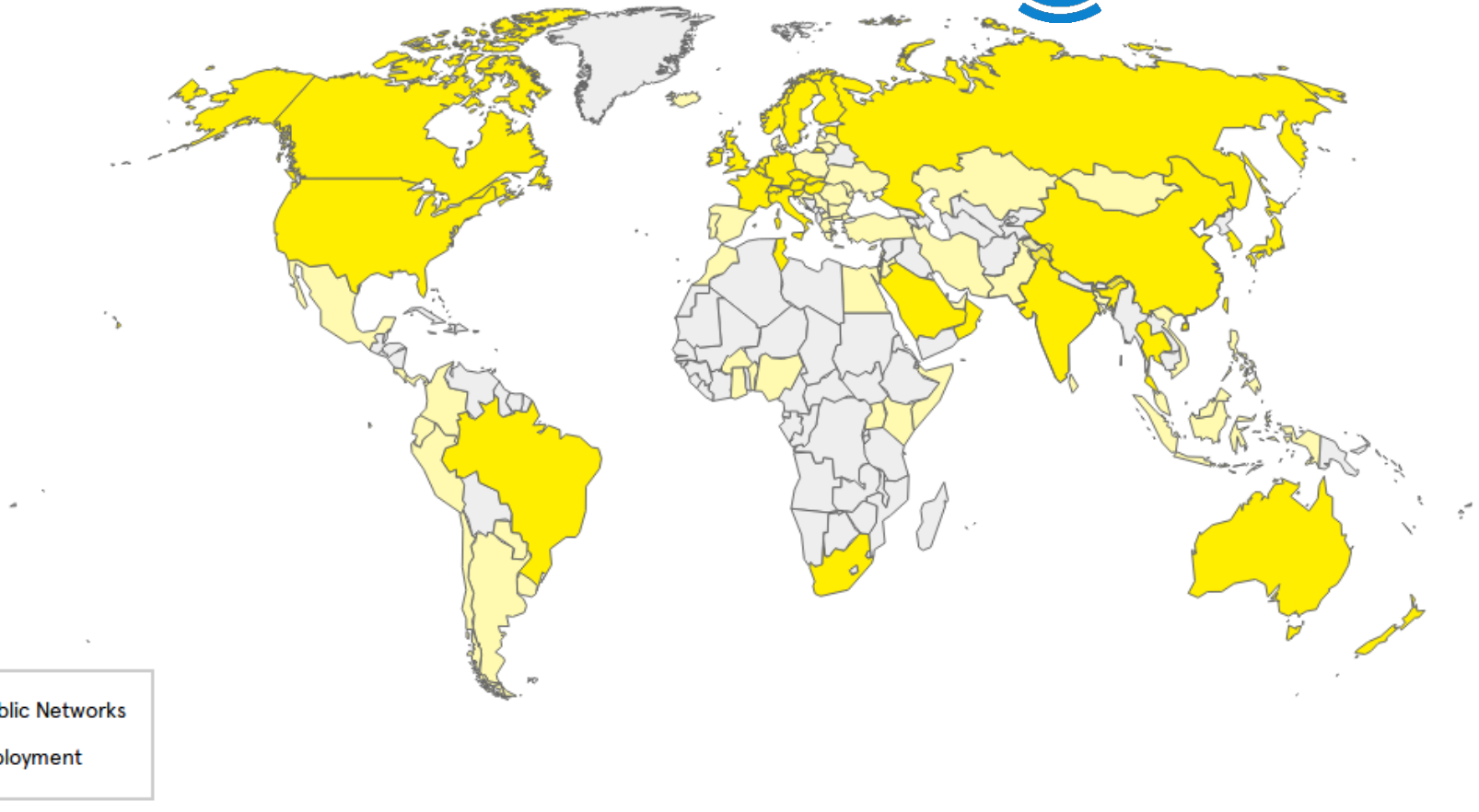
LoRaWan / 2

100
Network Operators

68
Alliance Member Operators

51
Countries operating in

100
Countries with LoRaWAN Deployments



LoRaWan / 3 / concerns

LoRaWAN™ addresses:

architecture
topology
entities
addressing
data rates
mobility
localization
security

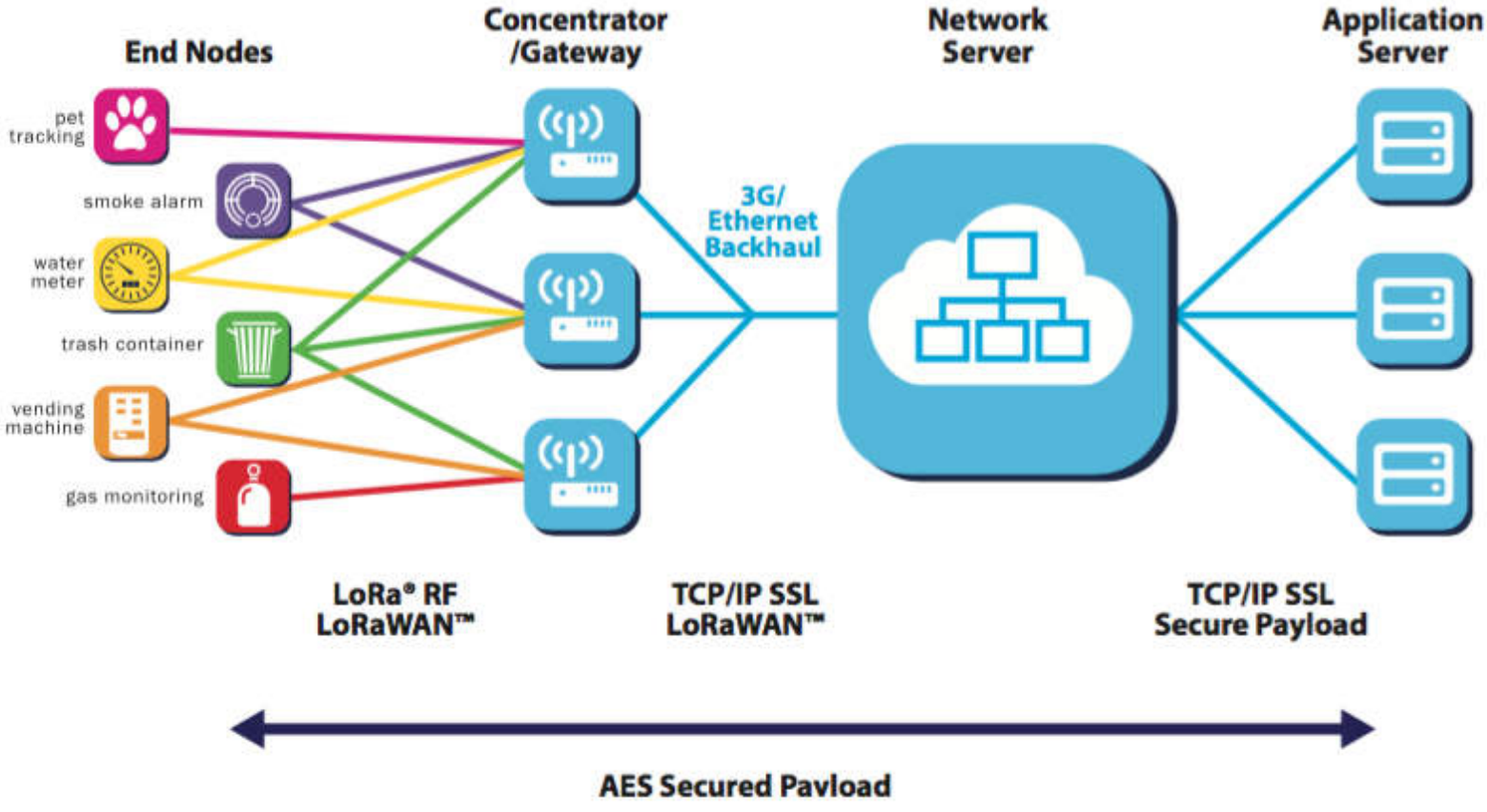
Details:

https://www.lora-alliance.org/What-Is-LoRa/Technology

LoRaWan / 4 / topologies & entities

- **Star-of-stars topology**
- **Gateways** are transparent bridges relaying messages between **end-devices** and a central **network server** in the backend.
- **Gateways are connected** to the network server via **standard IP connections** while end-devices use single-hop wireless communication to one or many gateways.
- All end-point communication generally **bi-directional**, supports **multicast** enabling **software upgrade over the air** or other mass distribution messages

LoRaWan / 5 / architecture



LoRaWan / 6 / device classes

Device classes

A Battery powered, small loads, long breaks, long latency, unicast

B low latency, scheduled receive slots, periodic beacon from gateway, uni/multicast, higher power, 14-30 mA

C no latency, uni/multi, constantly receiving, power hungry

Classes can be dynamically assigned / changed

Source, Details:

https://www.lora-alliance.org/What-Is-LoRa/Technology

LoRaWan / 7 / addressing

Devices and applications

have a 64 bit / 8 byte unique identifier (DevEUI and AppEUI).

When a device joins the network, it receives a dynamic (non-unique) 32-bit / 4 byte address (DevAddr).

Source, Details:

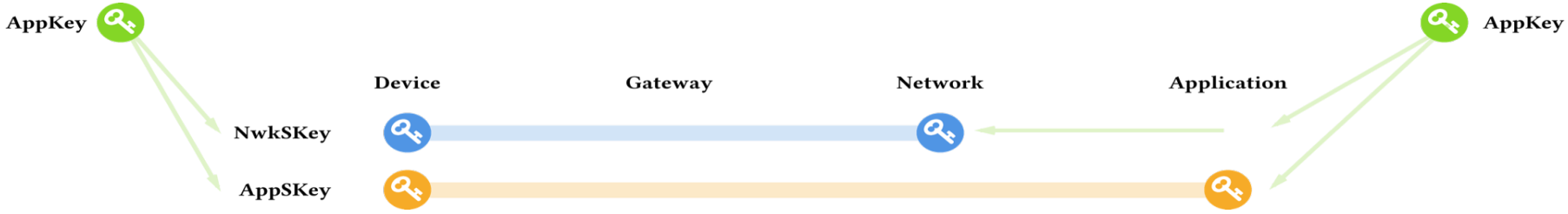
https://www.thethingsnetwork.org/docs/lorawan/

LoRaWan / 8 / Security / keys

Security measures:
three distinct 128-bit AES keys:
The **application key AppKey** is only known by the device and by the application. When a device joins the network (this is called a join or activation), an application session key **AppSKey** and a network session key **NwkSKey** are generated. The NwkSKey is shared with the network, while the AppSKey is kept private.

Source, Details:

https://www.lora-alliance.org/What-Is-LoRa/Technology



LoRaWan / 9 / Security / frame counter

The **frame counter in LoRaWAN** messages is a security measure used to detect **replay attacks**. After validating the MIC, the Broker checks if the Frame counter is valid. As frame counters can only increase, a message with a frame counter that is lower than the last known frame counter should be dropped. Additionally, the Broker has to verify that the gap between the last known frame counter and the counter in the message is not too big. According to the LoRaWAN specification, the maximum gap is 16384.

Source, Details:

https://www.lora-alliance.org/What-Is-LoRa/Technology

LoRaWan / 10 / data rates

LoRaWAN abstracts the PHY data rates of LoRa - for EU / CN:

- EU 863-870 MHz (LoRaWAN Specification (2015), Page 35, Table 14)
- CN 779-787 MHz (LoRaWAN Specification (2015), Page 44, Table 25)
- EU 433 MHz (LoRaWAN Specification (2015), Page 48, Table 31)

DataRate	Modulation	SF	BW	bit/s
0	LoRa	12	125	250
1	LoRa	11	125	440
2	LoRa	10	125	980
3	LoRa	9	125	1'760
4	LoRa	8	125	3'125
5	LoRa	7	125	5'470
6	LoRa	7	250	11'000
7	FSK 50 kbps			50'000

https://blog.dbrgn.ch/2017/6/23/lorawan-data-rates/

LoRaWan / 11 / duty cycles

LoRaWAN implements duty cycle rules made by regulators:

In Europe, duty cycles are regulated by section 7.2.3 of the ETSI EN300.220 standard. This standard defines the following sub-bands and their duty cycles:

- **g** (863.0 – 868.0 MHz): 1%
- **g1** (868.0 – 868.6 MHz): 1%
- **g2** (868.7 – 869.2 MHz): 0.1%
- **g3** (869.4 – 869.65 MHz): 10%
- **g4** (869.7 – 870.0 MHz): 1%

+ duty cycle for join channel: 1%

On top of that, specific networks might have fairplay rules.