Grant Agreement Number: 101014517
Project Acronym: AB4Rail
Project title: Alternative Bearers for Rail

DELIVERABLE D [2.1]
[Technologies for ABs]

Project acronym:	AB4Rail
Starting date:	01-01-2021
Duration (in months):	24
Call (part) identifier:	S2R-OC-IP2-02-2020
Grant agreement no:	Number 101014517 – IP/ITD/CCA - IP2
Grant Amendments:	N/A
Due date of deliverable:	31-01-2021
Actual submission date:	25-05-2021
Coordinator:	Franco Mazzenga (Radiolabs)
Lead Beneficiary:	Alessandro Vizzarri (Radiolabs)
Version:	0.1
Type:	Report
Sensitivity or Dissemination level[1]:	PU
Contribution to S2R TDs or WAs[2]	TD2.1
Taxonomy/keywords:	Adaptable Communication System; ACS; Alternative Bearers technologies; wireless technologies for railway; optical technologies for railway;

This project has received funding from the Shift2Rail Joint Undertaking (JU) under grant agreement No. 101014517. The JU receives support from the European Union's Horizon 2020 research and innovation programme and the Shift2Rail JU members other than the Union.

[1] PU: Public; CO: Confidential, only for members of the consortium (including Commission Services)

[2] https://projects.shift2rail.org/s2r_matrixtd.aspx

The document history table provides a summary of all the changes in reverse chronological order (latest version first).

Document history

Date	Name	Affiliation	Position/Project Role	Action/ Short Description
27 Febr. 2021	Alessandro Vizzarri	Radiolabs (RDL)	Technical Manager/WP leader	Description of the selected ABs for rail.
25 May 2021	Alessandro Vizzarri	Radiolabs (RDL)	Technical Manager/WP leader	The updated document includes all the revisions provided by PO.

Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author's view – the Shift2Rail Joint Undertaking is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Table of Contents

Executive Summary

This document constitutes the first issue of Deliverable D2.1 “Technologies for Alternative Bearers” according to Shift2Rail Joint Undertaking programme of the project titled “Alternative Bearer for Rail” (Project Acronym: AB4Rail, Grant Agreement No 101014517 — IP/ITD/CCA — IP2).

The main objective of this deliverable relays in an overview of the prior state-of-art in the areas of selected alternative communication bearers (ABs), which are expected to be of interest for improving capabilities of the Adaptable Communication System (ACS). A set of candidate communication technologies are investigated as potential ones for railway applications. The methodology is based on the most important communication features not only from a technological perspective (i.e., standard, protocol, security, and performance) but also considering (but not limited to) others factors as maturity, ease of development and deployment costs, together with economic and business implications.

The review provides the state-of-the-art of ABs, both based on radio frequency (RF) and optical wireless technologies. The RF wireless technologies offer capabilities depending on intrinsic characteristics. In fact, the wireless short-range bearers are suitable for connections in proximity (from one to a few tens meters) with low data rate (a few tens of kbps) and a reduced power consumption. In ten meters, UWB provides high data rate (over 100 Mbps), while Bluetooth 5.2 enhances both the coverage range (around 200 m) and the data rate (up to 2 Mbps) although a considerable power consumption. The wireless long-range bearers, as LPWA (LoRaWAN) and NB-IoT, offer more coverage range (up to 15 km), a data rate up to 100 kbps and a network capacity of thousands of nodes. The aerial communication platforms increase both the coverage area (from 50-90 radius km to 1 million km2) and the data rate (up to 33 Gbps).

The optical wireless technologies, specifically in the visible and infrared ranges, show unique features that distinguish them from well-known RF technologies. More in details, we have investigated the use of optical wireless links from a LED device to a photodetector (i.e., VLC LoS links), providing high data rates, security and directivity of the light beam. VLC represents a green technology, guaranteeing high performance from short (<10 m) to medium (<300 m) ranges, both in indoor and outdoor scenarios. Furthermore, the use of FSO technology can achieve direct communication links in outdoor, reaching very long distances, in the order of kilometers (>20 km).

The most important limitations to mention about the wireless ABs refer to the reduced data rate for low latency or bandwidth-consuming applications. Some wireless short-range technologies are affected by a non-massive diffusion in the market, and usually are not backward compatible (as for Bluetooth 5.2). The energy autonomy and considerable costs for deployment are important limitations as well as the security issues especially for safety and security applications, and railway applications. On the other side, the optical wireless technologies present other limitations, such as (i) the mobility issues, which can affect the directivity of LoS links, (ii) weather conditions (i.e., fog, sunlight, rain, etc.) that can increase the attenuation of the optical signal, (iii) occlusions that cause connectivity outage, and (iv) energy source required.

Leveraging on different pros and cons of selected ABs, and according to the technology evolution, different ABs can be suitable for specific railway scenarios or inter-connection schemes, which make ABs possible candidates for ACS. Possible ABs have to be analysed for ACS and rail applications suitability, together with the benefit-cost analysis and the return of investment calculation. The next step will address a complete assessment of candidate ABs for railway applications. This task represents the focus of next deliverable D2.2, dealing with the assessment of ABs benefits, challenges and impact on infrastructure with Radio Access Technology tool and Communication Traffic Analysis.

List of abbreviations, acronyms, and definitions

Acronym	Definition
3GPP	Third Generation Partnership Project
A2A	Aerial to Aerial
AB	Alternative Bearer
AC	Alternating Current
ACS	Adaptable Communication System
ADR	Adaptive Data Rate
APD	avalanche photo diode
ARIB	Association of Radio Industries and Businesses
B5G WNs	Beyond 5G Wireless Networks
BB	Broadband
BIP	Bearer Independent Principle
BLE	Bluetooth Low Energy
BSs	Base Stations
CENELEC	European Committee for Electrotechnical Standardization
D2D	Device-to-Device
DC	Direct Current
DCNs	Data Centre Networks
DDoS	Distributed Denial of Service
DSSN	Dense Small Satellite Networks
EMI	Electromagnetic Interference
EPR	Einstein, Podolsky, and Rosen
EPRI	Electric Power Research Institute,
ERTMS	European Rail Traffic Management System
FCC	Federal Communications Commission
FOV	Field of View
FSO	Free Space Optics
FSOIs	Free-Space Optical Interconnects
G2A	Ground to Aerial
GSL	Ground-to-Satellite Link
GSM-R	Global System for Mobile Communications – Railway

HAPS	High Altitude Platform Station
HD	High Definition
HDR	High Data Rate
HPC	High Performance Computing platforms
IC	Integrated Circuit
IEEE	Institute of Electrical and Electronics Engineers
IM/DD	Intensity Modulation /Direct Detection
IoT	Internet of Things
IP	Internet Protocol
IPSP	Internet protocol support profile
IR	Infrared
ISL	Inter-satellite link
ITU	International Telecommunication Union
LDR	Low Data Rate
LED	Light Emitting Diode
LEO	Low-Earth Orbit
Li-Fi	Light-Fidelity
LoS	Line-Of-Sight
M2M	Machine-To-Machine
NB	Narrow band
NWK	ZigBee network layer
OAM	Orbital Angular Momentum
OCC	Optical Camera Communications
OLEDs	Organic LEDs
OOK	On-Off keying
OVLC	Organic VLC
OWC	Optical Wireless Communications
PAM	Pulse Amplitude Modulation
PAT	Pointing, Acquisition and Tracking
PCB	Printed Circuit Board
PDs	Photodectors
PIS	Passenger Information Systems

PLC	Power Line Communications systems
PLMN	Public Land Mobile Networks
PPM	Pulse Position Modulation
PSTN	Public Switched Telephone Network
PtP	Point-to-Point
QKD	Quantum Key Distribution
QSDC	Quantum Secure Direct Communication
RF	Radio Frequency
RLL	Run Length Limited
RS	Reed Solman
Rx	Receiver
SF	Spreading Factor
SR	Short-Range
LR	Long-Range
T2T	Train-to-Train
TB	Traditional Bearer
ToF	Time of Flight
Tx	Transmitters
UNB	Ultra-narrow band
UV	Ultraviolet
UW	underwater
UWB	Ultra-wideband
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VCSEL	Vertical Cavity Surface Emitting Laser
VL	Visible
VLC	Visible Light Communication
WA	Wireless Access
WDM	Wavelength Division Multiplexing

List of Figures

List of Tables

1. Introduction

This document constitutes the Deliverable D2.1 “Technologies for ABs” according to Shift2Rail Joint Undertaking programme of the project titled “Alternative Bearer for Rail” (Project Acronym: AB4Rail, Grant Agreement No 101014517 — IP/ITD/CCA — IP2). On 22nd July 2020, the European Commission awarded a grant to the AB4Rail consortium of the Shift2Rail / Horizon 2020 call (S2R-OC-IP2-02-2020). AB4Rail is a project connected to the development of a new Communication System planned within the Technical Demonstrator TD2.1 of the 2nd Innovation Programme (IP2) of Shift2Rail JU: Advanced Traffic Management & Control Systems.

The IP2 “Advanced Traffic Management & Control Systems” is one of the five asset-specific Innovation Programmes (IPs), covering all the different structural (technical) and functional (process) sub-systems related to control, command, and communication of railway systems.

1.1 **Purpose and scope of the document**

The aim of this document is to provide a detailed overview of the technologies that can be considered as potentials Alternative Bearers (AB) to be integrated into the Adaptable Communication System (ACS). These technologies include: optical communication system, innovative LEO/MEO satellite constellations, High Altitude Platform Station (HAPS) and Power Line-based wired technologies. Internet of Things (IoT) radio technologies are also analyzed for their possible integration into the ACS.

Looking at the future, the deliverable also includes a short presentation of the main innovative and promising features of the quantum and THz communication technologies.

1.2 **Document organization**

The document is organized according to AB4Rail Grant Agreement Number 101014517 (RD-1) and AB4Rail Consortium Agreement (RD-2). The document structure is the following. Section 3 presents the list of novel technologies that will be investigated for railway applications. Section 4 and 5 are dedicated to optical wireless communications, while Section 6 illustrates main features of power line communications. It follows Section 7, 8 and 9 with IoT technologies for short-range applications i.e., Bluetooth, Zigbee and Ultra-wide Band, respectively. On the other side, Section 10 is dedicated to Low Power Area Networks (LPWAN) long-range wireless technologies i.e., LoRa and Narrow-Band IoT (NB-IoT), respectively. Section 11 and 12 present aerial based technologies, such as HAPS and novel LEO satellites, respectively. Finally, Section 13 describes selected future technologies, such as quantum and THz communications. Conclusions are then drawn in Section 14.

1.3 **Reference Documents**

Table 1: Reference Documents.

Document Number	**Document Description**
RD-1	AB4Rail Grant Agreement Number 101014517 - IP/ITD/CCA - IP2
RD-2	AB4Rail Consortium Agreement

2. The technological context

Nowadays, the last trends in telecommunications for rail are envisioning the need of innovative technologies that can guarantee a consistent increase of required throughput and low latency in communications. Such technologies should be integrated with previous Third Generation Partnership Project (3GPP)-based ones, and should take into account both the obsolescence of Global System for Mobile Communications – Railway (GSM-R) and the need of additional Radio Spectrum, which is limited in case of GSM-R.

In fact, GSM-R has been introduced as radio communication technology for the European Rail Traffic Management System (ERTMS) since 1990. Although the end of life for GSM-R is expected to be around 2030, GSM-R is still used and rollout in Europe. But the GSM-R obsolescence is the biggest challenge for the railway sector, and a complete digitalization of the railway sector is just started, since IP-based systems are going to replace those based on circuit-switched technologies.

In the post-GSM R era, the connectivity in railway applications is provided by Public Land Mobile Networks (PLMNs), in order to guarantee interoperability, inter-connection with other IP-based networks, network availability, service reliability, and compliance with service requirements (i.e., performance, QoS and security). Currently, railway applications can rely on Traditional Bearers (TBs) (i.e., Wi-Fi, GSM-R, LTE, LTE-A, 5G and satellites). According to a proof-of-view vision of railway sector evolution, novel technologies should be investigated to be placed as alternative and integrated solutions w.r.t. TBs. The coexistence with TBs should be also guaranteed, as well as the backward compatibility.

Notice that the same approach adopted for the investigation of PLMNs should be applied to ABs to identify common and different features w.r.t. TBs.

In this rapidly evolving context, the ACS platform plays a crucial role for railway application delivery based on both TBs and Abs. In fact, the ACS is an open platform that can be enriched by adding additional bearers with mature technologies, to complement the traditional communication bearers.

As known, ACS is designed in accordance with the bearer independent principle (BIP). This means that the ACS can interface with several and different communication bearers (wired/wireless) to provide end-to-end connectivity for railway applications. Interfacing of ACS with the bearers is made at IP level to fully implement the BIP concept. Communication of applications over the ACS can be provided over one or more IP-based bearer both alternative and/or traditional, commercial or private, without assuming that the bearer provides any capability beyond data transmission using the Internet Protocol (IP).

Several joint initiatives, carried out by academies and industrial companies, are already ongoing and are mainly oriented to analyse and develop new communication systems for rail, using IP-based communications, such as 4G and 5G. In this way, it is possible to guarantee high reliability, high availability, and broadband radio connections with low latency and high data throughput. Similar considerations are applied to Low-Earth Orbit (LEO) satellites, High Altitude Platform Station (HAPS) technology, and also wireless optical technologies i.e., Visible Light Communications (VLC) and Free Space Optics (FSO), which in Europe are expected to be largely applied in the rail sector.

In this deliverable, the authors investigate novel ABs, expected to be adopted in railway applications, and playing a complementary role with respect to traditional bearer technologies mostly based on 3GPP and IEEE 802 standards.

3. Considered technologies

In this document, we consider a set of candidate technologies that can be suitable to be adopted in ACS for railway applications. This set has been already identified in the AB4Rail proposal and is hereafter listed in Table 4. As it can be noticed, we have identified technologies both from radio frequency (RF) and optical wireless (OW) spectrum, ranging from very low frequency as for PLC up to THz band. Pros and cons of each technology will be investigated, as well as the main applications and features. Also, notice that we considered Ultra-wide Band (UWB) instead of IPv6 over Low -Power Wireless Personal Area Networks (6LowPAN), as reported in the final version of the proposal.

The technologies already identified for AB4Rail studies are listed in Table 2, considering them in terms of:

- Fixed technologies;
- Wireless short-range (SR) technologies;
- Wireless long-range (LR) technologies;
- Future technologies

Table 2: List of Alternative Bearers technologies.

Category	**Technology**	**Examples of current/proposed Railway applications (including references)**
Optics	Visible Light Communication (VLC)	• Monitoring of railways health state (*e.g.*, vibrations and other critical data) to ensure the security of trains traffic • Indoor positioning and venue navigation
	Free Space Optics (FSO)	• To enable connectivity between trackside gateways • High-speed communication services such as internet access and video-on-demand
PLC	Power Line Communications systems	• Transmission of data for control of railway (*e.g.*, semaphore Signaling in Railway Tracks, automatic brake testing, train integrity checks, automatic coupling) • Coach and train communication networks for Passenger Information Systems (PIS) services and video surveillance
IoT (SR)	Bluetooth 5.2	• Monitoring the railway infrastructure such as bridges, rail tracks, track beds, and track equipment along with vehicle health monitoring such as chassis, bogies, wheels, and wagons, for example for derailment detection and data collection in freight trains
	ZigBee	
	Ultra-wideband (UWB)	
IoT (LR)	LPWAN (e.g. LoRa, NB-IoT)	• On-board monitoring with sensors and on-board LoRa gateway
HAPS	High Altitude Platform Station	• High-data-rate applications to trains such as high-data rate internet access

Update tech.	Novel Sat LEO constellations	• High-data-rate applications from infrastructure-to-train such as broadband internet service • Novel antennas can work with traditional Satellites, as well as the new generation of compact LEO spacecraft in mega constellations (SpaceX, OneWeb, Amazon, Facebook etc.)
Future tech.	Quantum communications	• They can be exploited for future high-data-rate applications from infrastructure-to-train
	THz communications	• High-data-rate applications such as on-board and wayside high definition (HD) video surveillance, on-board real-time high-data-rate connectivity, train operation information, real-time train dispatching HD video, and journey information

4. Visible Light Communications

Optical Wireless Communications (OWC) is considered a key emerging technology for future wireless transmissions, including sixth generation (6G), especially in indoor environments. In a general sense, OWC covers the optical bands of infrared (IR), visible (VL) and ultraviolet (UV). FSO communications and VLC are commonly-used terms in the literature to describe various forms of OWC. FSO mainly refers to the use of outdoor/space laser links at the IR band, while VLC relies on the use of light emitting diodes (LEDs) at the VL band mostly in indoor environments. Figure 1 shows the optical bandwidth available for wireless communications.

Figure 1. Available spectrum for the optical bandwidth.

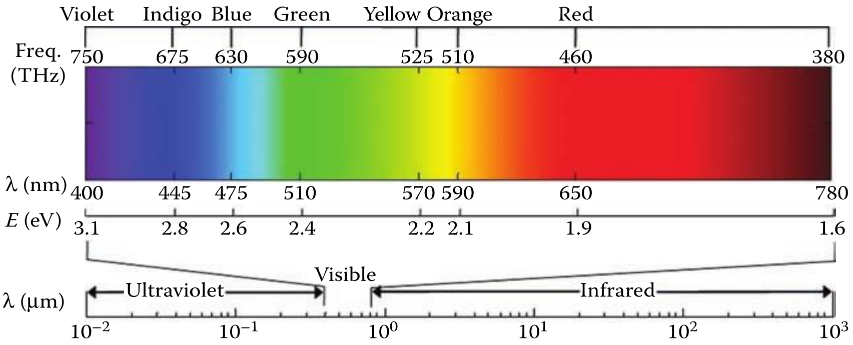
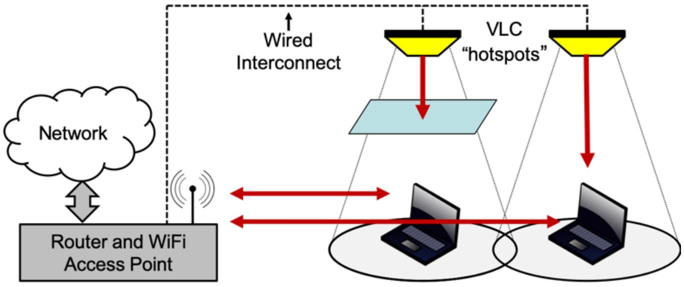


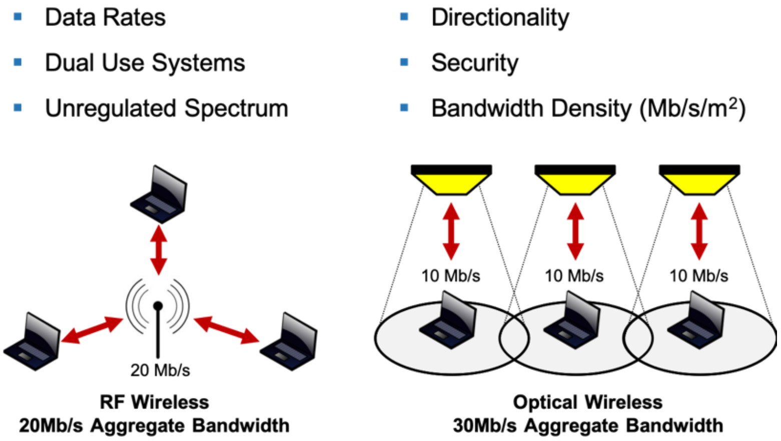
Figure 2. VLC system, comprised of RF uplinks. LoS blockage can cause connectivity disruption and outage



Since its infancy, OWC has shown a strong potential to outdo -and sometimes, replace- the conventional RF wireless solutions in selected use-cases. Specifically, unlike other wireless communication technologies, VLC is safe for the human health and does not affect the functionality of the highly sensitive electronic systems and thus, can be used in RF restricted places such as airplanes, hospitals, chemical or nuclear plants. It is then defined as a green technology due to its twofold paradigm of both illumination and data communication, simultaneously by the same physical carrier. The interest in OW is fostered by its key features, e.g., intrinsic physical layer security, no electro-magnetic pollution, and robustness to strong radio-frequency noise background. The VLC technology is also fully compatible to RF communications, so the two can complement each other, forming hybrid or heterogeneous networks and further enhancing the communication performances. Indeed, usually a typical VLC system is comprised of optical downlink connectivity and RF uplink. Figure 2 depicts the schematic of a VLC system, with RF uplinks. Notice the presence of obstacles can cause connectivity outage. As a comparison with RF system, VLC can provide higher directionality between Tx and Rx, use of unregulated spectrum, higher security level, data rates and higher aggregate bandwidth. Of course, the dual use of both communication/positioning and lighting with the same carrier is typical of VLC systems. Figure 3 shows the benefits of VLC as compared to RF technology.

VLC technology has gained great interest in the last years, mainly due to the development of LEDs, as well as to its “green” feature. Indeed, the worldwide deployment of lamps based on LEDs, which can work as OW transmitters, offers an effective synergy between lighting and pervasive (distributed) communication. VLC uses the visible light in the range (380 – 780 nm) as a carrier for the data, and thus it offers a 1000 times greater bandwidth compared to the RF communications. For this reason, the visible light spectrum is not regulated, and the cost of the technology can be significantly reduced. The huge available spectrum enables VLC to achieve very high data rates that can reach few tens of Gb/s [22]. Table 3 collects and compares the main features of OW and RF technologies.

Figure 3. Comparison of VLC to RF systems. Higher data rates and security are provided as compared to RF system.

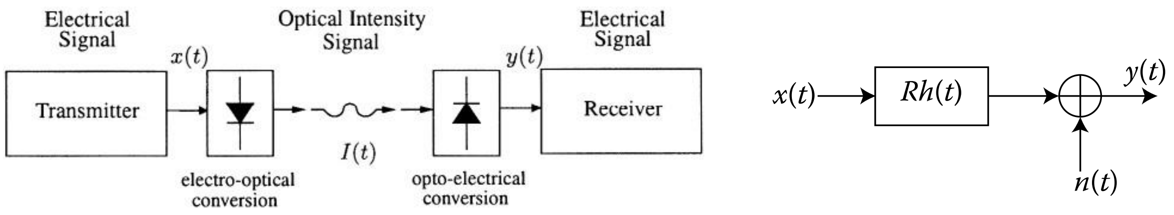


The fundamental components of a VLC system are: the transmitter (e.g., LED and camera), the receiver (e.g., photodetector and camera) and the VLC channel. Concerning the transmitter, different light sources can be considered even though the most popular is LED for VLC. LED is an incoherent source, namely photons are emitted spontaneously with different uncorrelated phases.

Table 3. Comparison of main features of wireless optical and radio technologies.

Property	Wireless optical	Radio
Cost	low	high
RF circuit design	No	Yes
Bandwidth regulated	No	Yes
Data rates	100’s Mbps	10’s Mbps
Security	High	Low

Figure 4. Principle scheme of a Tx-Rx a VLC system: (a) Block diagram of an optical intensity, direct detection communications channel, and (b) its approximation.



(a) (b)

Photodectors (PDs), as receivers in a VLC system, absorb the photons impinging on their frontend surface and generate an electrical signal. Channel modeling in VLC plays a crucial role for realizing effective, robust yet low complex systems. The easiest and the most cost-effective modulation is based on Intensity Modulation (IM)/Direct Detection (DD), which is not concerned by frequency and phase of the signal.

Figure 4(a) describes the block diagram of the IM/DD channel.

The output at the receiver block is the signal $y(t)$, which is expressed as follows:

$$y(t) = R\, x(t) \otimes h(t) + n(t), \qquad (1)$$

where $x(t)$ is the transmitted signal before the electro-optical conversion block, R is the responsivity, $h(t)$ is the channel response and $n(t)$ is the additive noise, modelled as an Additive White Gaussian noise. Eq.(1) shows the received signal according to the channel model in Figure 4 (b).

Typically, a VLC transmitter is considered as a Lambertian emitter and therefore, its radiant intensity distribution $R_0(\phi)$ can be approximated as

$$R_0(\phi) = \begin{cases} \left(\frac{m+1}{2\pi}\right)\cos^m(\phi), & for\ \ \phi \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \\ 0, & otherwise \end{cases} \qquad (2)$$

where ϕ is the angle with respect to the transmitter and m is the Lambertian order depending on the half power angle $\phi_{1/2}$ of the transmitter, such as $m = -\ln 2 / \ln(\cos\phi_{1/2})$. It follows that the irradiation pattern R_{Tx} [W/cm2] of the VLC transmitter is defined as:

$$R_{Tx} = \begin{cases} \frac{P_{Tx}}{d^2}\left(\frac{m+1}{2\pi}\right)\cos^m(\phi), & for\ \ \phi \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \\ 0, & otherwise \end{cases} \qquad (3)$$

where P_{Tx} [W] is the transmitter emission power and d [m] is the distance from the transmitter to the receiver.

Figure 5 depicts the scenario with a transmitter and a receiver in Line of Sight (LoS). In this case, the received power at the photodetector is given as:

$$P_{Rx} = A_{PD}\frac{P_{Tx}}{d^2}\left(\frac{m+1}{2\pi}\right)\cos^m(\phi)\, T_s(\psi) g(\psi) \cos(\psi) \quad \text{for } \ 0 \le \psi \le \psi_{con} \ (4)$$

where ψ is the angle of incidence with respect to the axis normal to the receiver surface, $T_s(\psi)$ is the filter transmission coefficient, $g(\psi)$ and ψ_{con} are the concentrator gain and the Field of View (FOV), respectively.

The gain of the optical concentrator at the receiver is defined by

$$g(\psi) = \begin{cases} \frac{n_{con}^2}{(\sin \psi_{con})^2}, & 0 \leq \psi \leq \psi_{con} \\ 0, & \psi > \psi_{con} \end{cases} \tag{5}$$

where n_{con}^2 is the refractive index of the optical concentrator. As an example, Figure 6 Figure 6 depicts the received power distribution in a 8 × 8 m2 room, where 4 LEDs are positioned in the ceiling, transmitting a 100 Watt power. Notice the Lambertian profile of the power emitted by each LED.

Figure 5. VLC transmitter-receiver LoS link.

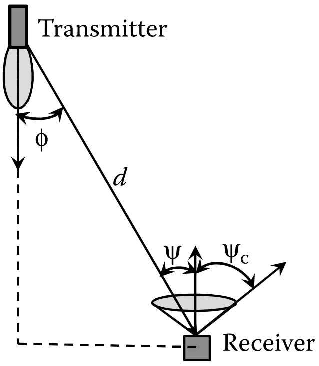
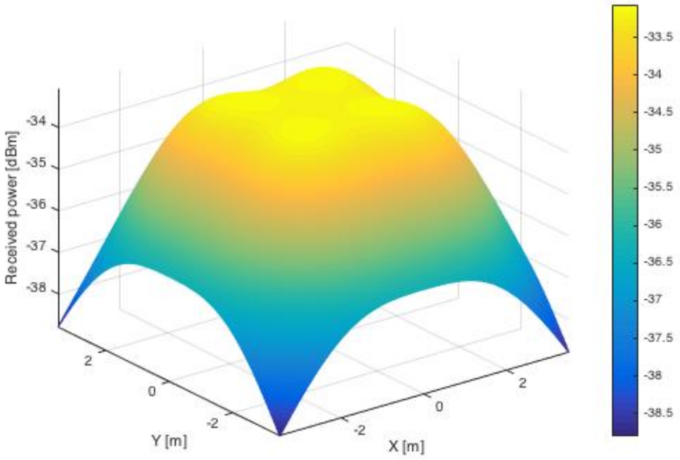


Figure 6. Received power distribution[dBm] in a 8x8 m2 room, where 4 LED transmitters are deployed in the ceiling.



In comparison to RF, OWC systems offer significant technical and operational advantages including, but not limited to:

1. High capacity, e.g., a recent FSO system with a world record data rate of 13.16 Terabits/sec (Tbps) over a distance of 10 km [23], and multiple Gigabits/sec (Gbps) indoor VLC links [24];
2. Operation in unregulated spectrum, thus no license fees and associated costs;
3. Immunity to RF electromagnetic interference (EMI);

4. A high degree of spatial confinement, offering virtually unlimited frequency reuse capability, inherent security at the PHY layer, and no interference with other devices;
5. A green technology with high energy efficiency due to low power consumption and reduced interference.

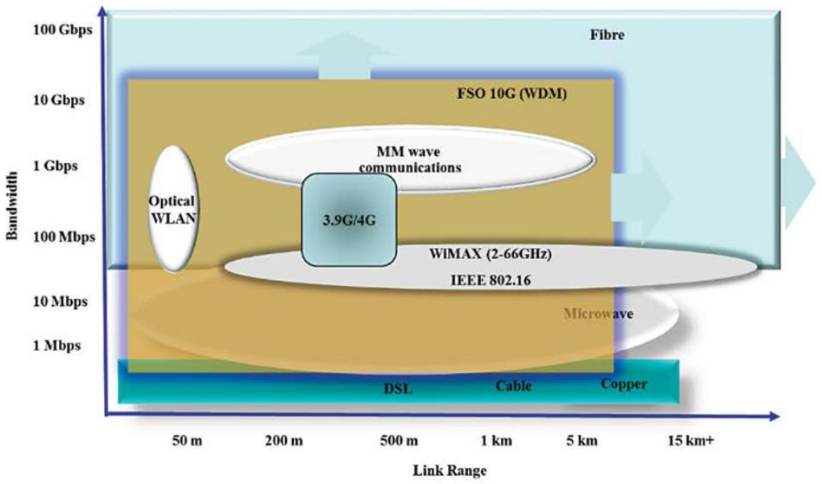
With such features, OWC is well positioned to be a powerful alternative or a complementary technology to RF solutions from micro- to macro-scale applications, including intra/inter-chip connections, indoor WA and localization, ITS, underwater (UW), outdoor and space point-to-point (PtP) links, etc. This opens up opportunities for high-impact research, which will revolutionize the telecommunications market still dominated by RF.

Among the main advantages of VLC are the exploitation of portion of spectrum that is not used by other technologies. The absence of obstacles makes this type of communication a very interesting candidate for a robust communication paradigm, with the most interesting perspective of a lower impact in terms of energy consumption. One of the most important challenges for integrating VLC in mobile scenarios is represented by a deep analysis of the specific characteristics of the channel and a precise channel modeling. Right now, VLC has been mostly applied for indoor applications and the presence of environmental source of interference (e.g., sunlight), if not properly addressed, could prevent the effective working of such a kind of technology.

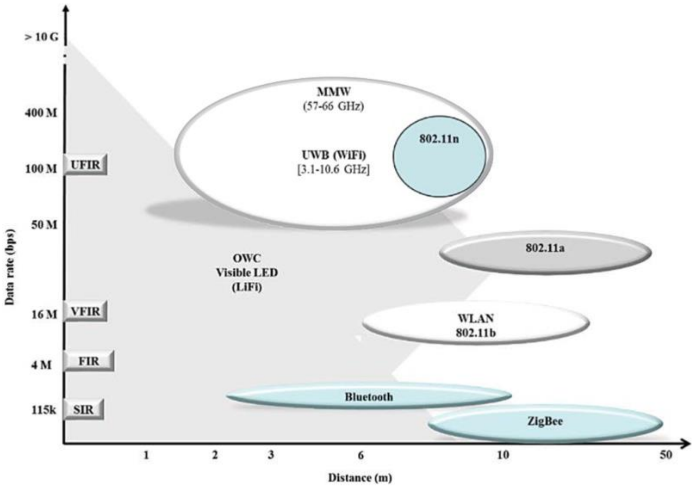
Figure 7 shows a simple block diagram of the network performance of VLC systems and more in general of OWC systems. A comparison with traditional RF system is provided. Commercially available outdoor OWC systems have come close to delivering high data rates over a link space up to 5 km, which are significantly faster than the latest radio LAN products currently available. From Figure 7, we observe OWC systems (indoor and outdoor) covering a wide unlicensed spectral band of 700–10,000 nm offer data rates exceeding 10 Gbps for both indoor and outdoor links. In the specific case of VLC systems, in the recent years, we have seen novel devices mechanically robust with a high energy efficiency, offering simultaneous illumination and intensity modulation at a data rate in excess of 100 Mbps.

Figure 7. Bandwidth capabilities for a range of optical and RF technologies for (a) long range and (b) short range.

(a)



(b)



The standardization progress related to OWC is still ongoing. There exist two main standardization organizations that focused on standardization activities on OWC, and in particular on VLC i.e., (i) the International Telecommunication Union (ITU) and (ii) the Institute of Electrical and Electronics Engineers (IEEE). The first standard for optical communication is IrDA, elaborated for short range communication. It has been proposed for the first time in 1993, but there have been several evolutions. In 2009, IEEE proposes the first standard for VLC, the IEEE 802.15.7. The next versions of this standard also include infrared, ultraviolet and optical camera communications (OCC). In 2018, a new working group for VLC, namely the IEEE 802.11bb, started activities for integrating the Li-Fi (Light-Fidelity) in order to make this technology interoperable with the Wi-Fi standard IEEE 802.11. This standard mainly focuses on MAC layer.

At the same time, the IEEE 802.15.3 working group defines the optical wireless communications for wavelengths comprised between 10 µm and 190 nm with a bit rate of multi-Gbps. Finally, the International Telecommunication Union (ITU) works on a standard for indoor optic communication, i.e., the ITU-G99991.

The architecture of the VLC system generally consists of three common layers: (i) physical, (ii) MAC, and (iii) application. The topologies supported by the MAC layer are peer-to-peer, broadcast, and star. Three different types of physical implementations of VLC are defined in the IEEE 802.15.7. For PHY I, PHY II, and PHY III, the data rates are 11.67–266.6 kbps, 1.25–96 Mbps, and 12–96 Mbps, respectively. The different channel coding schemes supported by 802.15.7 are convolutional codes and Reed Solman (RS) codes for the PHY I and run length limited (RLL) code for the PHY II (intended for indoor use) to address flicker mitigation and DC balance.

4.1 Applications

The main applications of OWC can be classified based on the distance reached by the transmitter optical wireless signals. As depicted in Figure 8 and Figure 9, the main applications of OWC distinguish based on the connectivity range of optical links i.e., (i) short-range links and (ii) medium/long-range links, and scenarios i.e., (i) indoor and (ii) outdoor. As it will be described hereafter, shorter links are provided by VL technology, while medium and longer range links are experienced by FSO.

Briefly, we observe that in indoor scenarios (e.g., office, home, shopping malls, museums, hospitals, airplanes, etc.) VLC are mostly employed, providing high data rates with LoS or diffuse propagation (see Figure 10). In contrast, in outdoor scenarios (i.e., mostly vehicular networks) FSO links are preferred due to higher coverage and performance.

Figure 8. Main overview of OWC indoor/outdoor applications.

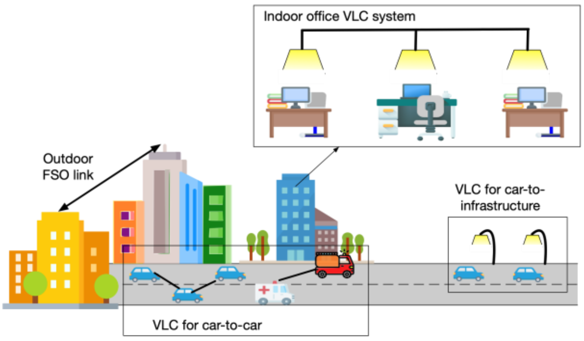


Figure 9. Schematic of main VLC applications, both in indoor and outdoor scenarios, with the purpose of PtP communications and localization.

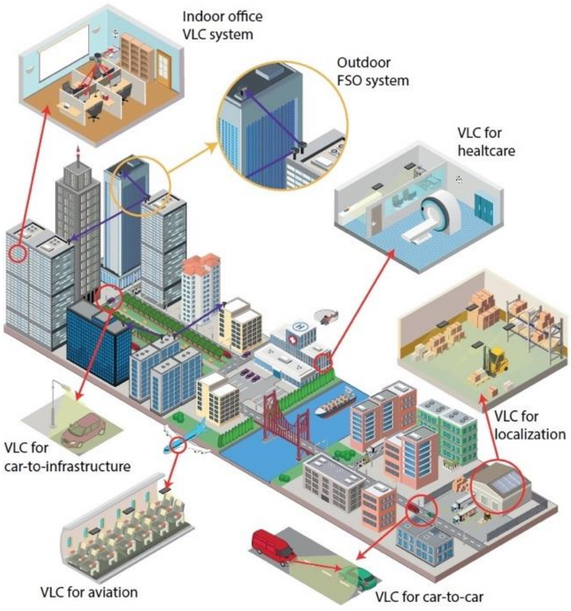
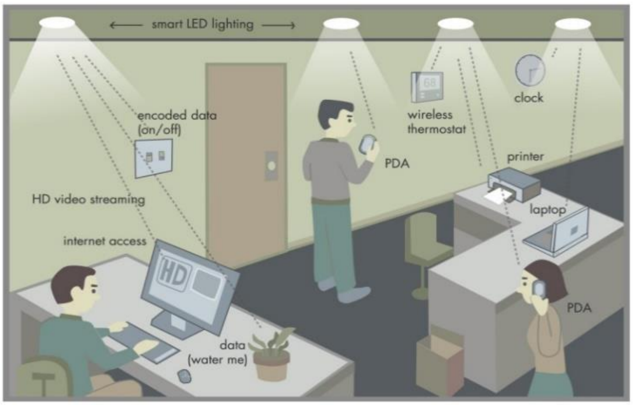


Figure 10. VLC home/office applications.

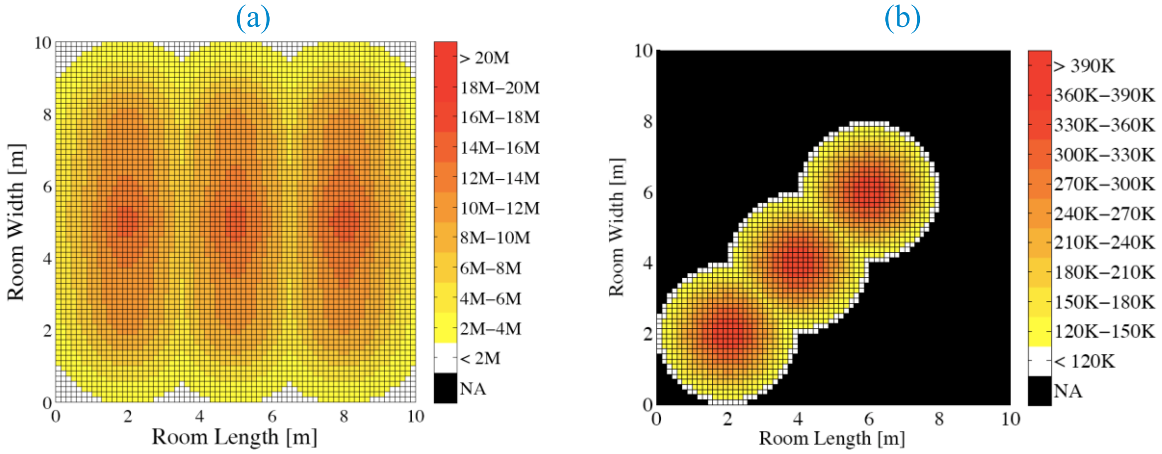


4.1.1 Short-range links

This area concerns OWC links of range up to a few meters and focuses on the application areas including indoor wireless access (WA), short-range IoT, as well as localization and sensing.

In indoor WA, VLC (also referred to as Li-Fi) effectively utilizes the current-day ubiquitous presence of LED-based lights to provide multiple functionalities of illumination, data communication and localization. Most of the existing works on Li-Fi are limited to PtP links used in home and office environments with static channel characteristics [25]. Diffuse and spotlight transmission modes allow to obtain different coverage through larger or narrower Field of View (FOV) of the transmitter. Figure 11 shows the data rate achievable in case of different VLC transmission mode i.e., diffuse and spotlight.

Figure 11. Comparison between VLC (a) diffuse and (b) spotlight transmission modes.



While initial works have demonstrated the potential of Li-Fi, significant amount of research and innovation is required to transform it into a multi-user, scalable, high performance, and fully networked technology as part of Beyond 5G Wireless Networks (B5G WNs), in particular in mobile and user-dense scenarios. This particularly requires the joint consideration of the optical channel, and PHY, MAC and NET layers to support adaptability and heterogeneity, as well as low latency. Recent works on multiple-subcarrier modulation-based systems have demonstrated the potential of high data rate transmission [26]. Nevertheless, innovative PHY layer designs and optimized waveforms considering non-negativity of optical signal are still required to come close to the channel capacity limits. The envisioned fully networked Li-Fi systems further require extensive research on the handover, interference management, scheduling, multiple access, and inter-connection with the backbone network, which have so far received relatively little attention.

On the other hand, short-range IoT applications include smart spaces and buildings, future smart manufacturing, indoor positioning, and healthcare and assisted living for the elderly people, among others. In particular, in smart factories of the future, there is the need for autonomous machine-to-machine (M2M) communication links with no human assistance. With the large BW, potentially lower energy consumption, and inherent security in comparison to RF, VLC could be an effective WA technology for M2M links. The potential of highly accurate positioning and sensing offered by VLC are among the other strong aspects of this technology particularly in smart manufacturing and healthcare. Some early examples include indoor positioning systems using smartphone's camera as a Rx, and smart lighting control [27]. The required paradigm shift to convert IoT into "Internet of Lights" involves a fundamental redesign of the algorithms and protocols at PHY, MAC and NET layers to adapt to the directional radiation of optical sources and inherent VLC channel characteristics as well as to maintain low power, low delay, and high system capacity characteristics associated with future IoT applications.

On-going research focuses on how to support massive connectivity for machine-type communications, reliable communications through mitigation of interference/contention among devices, and co- existence among different wireless technologies.

Within this context, two other recent techniques consider the use of organic LEDs (OLEDs) and photo-detectors (PDs) for moderate data rate D2D communications, and OCC for low data rate applications. In organic VLC (OVLC) the main challenge is the limited BW of the organic devices [28], whereas in OCC achieving high data rates and link robustness (i.e., considering blurring, shadowing, and pointing errors) are issues that need addressing [29].

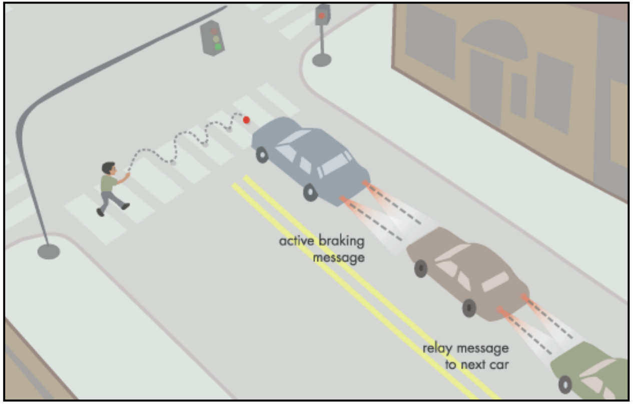
4.1.2 Medium-range links

This area concerns OWC links with a typical range of few metres to few kilometres and focuses on vehicular networking, PtP WA links, and UW communications.

In vehicular networking, which includes vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, research activities and standardization efforts have mainly focused on the RF-based solutions. Given that, LEDs are being widely used for vehicle lights, traffic lights, etc., VLC emerges as a natural candidate for V2V and V2I communications [30].

Figure 12 depicts the alerting application for security on roads in outdoor vehicular networks; warning messages are sent in V2V transmission mode.

Figure 12. VLC alerting application for outdoor vehicular scenario.



Research on this topic is rather sparse and requires further work to take it to advanced levels [31]. E.g., as part of channel modelling, additional noise sources due to the background radiations as well as visibility-limiting weather conditions need to be considered. In addition, there is the requirement for dedicated design and implementation of (i) PHY layer to support both safety functionalities (where latency and reliability are the primary issues) and infotainment applications (where transmission data rate is the priority); and (ii) MAC protocols considering the inherent directionality of VLC links. In vehicular networking, neighbour discovery, link establishments while on the move, and ensuring link availability on multi-lane highways impose further challenges for VLC-based wireless connectivity, which has not yet been fully addressed.

In UW applications, VLC is well recognized as a promising technology enabling high data rate, low latency, and high energy efficiency, which outperforms acoustic and RF communications. Such links are critically required given the on-going expansion of human activities in various application domains including environmental monitoring, UW exploration, port security, disaster prevention, etc. for data communications between UW mobile units, submarines, or within UW sensor networks. The strong intensity attenuation of the aquatic channel (especially in turbid waters) and the LoS requirement impose several challenges on the deployment of these links.

Current research focuses on the design of high-sensitivity Rxs and powerful error-correcting codes allowing extension of the communication range, as well as effective localization and pointing, acquisition and tracking (PAT) solutions for improving the link reliability [28].

5. Free Space Optics (FSO)

5.1 Free Space Optics (FSO)

Free space optical (FSO), together with VLC, are commonly used terms to describe various forms of OWC. FSO mainly refers to the use of outdoor/space laser links at the infrared band, where data is transmitted by propagation of light in free space allowing optical connectivity. FSO communications have been proposed as a promising technique to overcome the RF drawbacks, then providing high-speed transmissions in the unregulated bands. Furthermore, license free spectrum, immunity to the electromagnetic interference and inherent security are some advantages of FSO systems compared to the conventional RF-based wireless communication systems.

The use of FSO communication is considered as a promising and efficient technology for establishing high data rate point-to-point communication links, which can offer high bandwidth and ease deployment. As similar to VLC technology, FSO system consists of an optical transceiver at both ends to provide full duplex (bidirectional) capability. FSO is a LoS (line of sight) technology, where data, voice, and video communications are achieved with maximum 10 Gbps of data rate by full duplex (bidirectional) connectivity. High data rate can be obtained -comparable to the optical fiber cable's data rate- but error rate is very low and the extremely narrow laser beam enables having unlimited number of FSO links to be installed in a specific area. Furthermore, FSO is a secure system because of line of sight operation between transmitter and receiver. Finally, as similar to VLC, no interference to RF technology occurs, as the electromagnetic and radio-magnetic interference cannot affect the transmission in FSO link.

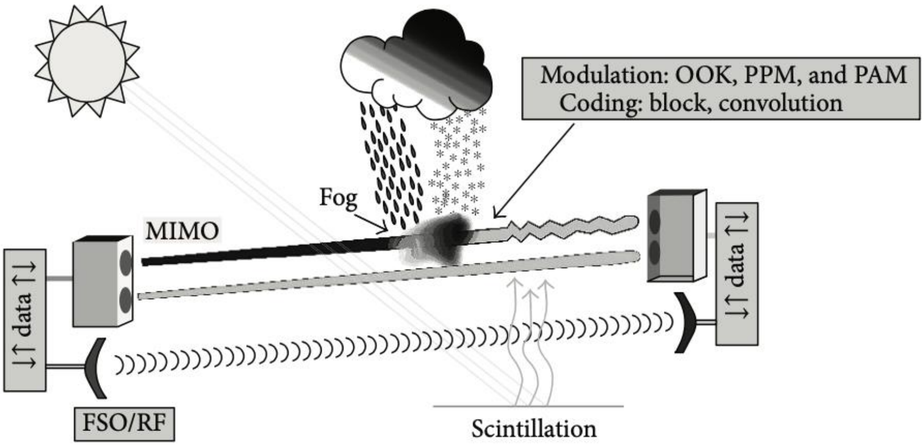
As known, the reliability of FSO links can be seriously affected by the link distance, which is typically longer than a few kilometers. One of the main disadvantages of FSO communications is related to weather interference. Different weather conditions have various impacts on the FSO link performance, which leads to the signal loss, and then on the reduction of effective data rate. Channel capacity in a FSO link is negatively affected not only by atmospheric turbulence induced fading, but also on the pointing error due to the position deviations of tall buildings (physical obstructions). Based on the scale size of turbulence cell, different type of effects can be caused i.e.,

1. If the size of turbulence cell is of larger diameter than optical beam, then the optical beam displaces rapidly (beam wander)
2. If the size of turbulence cell is of smaller diameter than optical beam, then the intensity of fluctuation or scintillation of the optical beam is a dominant effect.

Atmospheric attenuation is another cause of FSO optical signal degradation. This is defined as the process whereby some or all of the electromagnetic wave energy is lost when traversing the atmosphere. Thus, atmosphere causes signal degradation and attenuation in a FSO system link in several ways, including absorption, scattering, and scintillation. The atmospheric attenuation is the resultant of fog and haze normally, and also depends upon dust and rain. Haze is traditionally an atmospheric phenomenon where dust, smoke and other dry particles obscure the clarity of the sky. It is wavelength dependent, while attenuation in fog weather condition is wavelength independent. Finally, scattering phenomena is another effect that can occur in FSO systems. It happens when the optical beam and scatterer collide. It is wavelength dependent phenomenon, which leads to the reduction in the intensity of beam for longer distance.

Other effects are due to scintillation (i.e., temperature variations in the air medium can cause fluctuations in amplitude of the signal which causes "image dancing" at the FSO receiver), geometric losses (i.e., optical beam attenuation due to the spreading of beam), absorption (i.e., water molecules which are suspended in the terrestrial atmosphere absorb photons and then the power density of the optical beam is decreased), as shown in Figure 13.

Figure 13. Atmospheric effects occurring in a FSO system [35].



All these effects are varying with time and depend on the current local conditions and weather. In general, the atmospheric attenuation τ is expressed by the Beer's law equation i.e.:

$$\tau = exp(-\beta L),$$

where L [km] is the distance between transmitter and receiver, and β is the total attenuation coefficient, given as

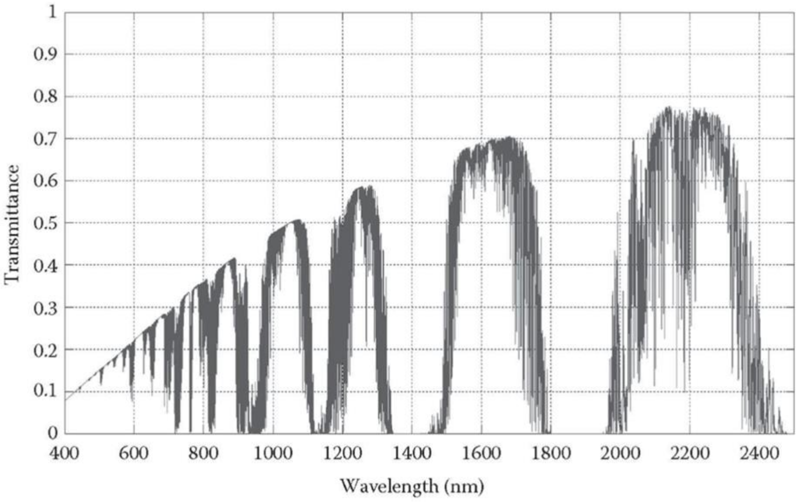
$$\beta = \beta_{abs}\beta_{scat},$$

with β_{abs} as the molecular and aerosol absorption, and β_{scat} as the molecular and aerosol scattering. The absorption coefficient β_{abs} can be computed from the concentration of the particle and the effective cross section such as:

$$\beta_{abs} = \alpha_{abs}N_{abs}[km^{-1}],$$

where α_{abs} is the effective cross section of the absorption particles [km^2], N_{abs} is the concentration of the absorption particles [km^{-3}]. An absorption line at visible and near infrared wavelengths are narrow and generally well separated. Thus, absorption can generally be neglected at wavelength of interest for free space laser communication. It depends on the type of gas molecules, and on their concentration. Molecular absorption is a selective phenomenon, resulting in the spectral transmission of the atmosphere presenting transparent zones, also known as atmospheric transmission windows, as shown in Figure 14. These windows are created by atmospheric gases and occur at various wavelengths. They allow specific frequencies of light to pass through it. As shown in Figure 14, based on the EM spectrum, several transmission windows exist and are nearly transparent, with attenuation value lower than 0.2 dB/km, in the wavelength range from 780 nm to 1600 nm. Specifically, four windows exist and are located around several specific centre wavelengths, such as (i) 850 nm, (ii) 1060 nm, (iii) 1250 nm, and (iv) 1550 nm.

Figure 14. Atmospheric transmission windows vs. wavelength.



The first region is centered at 850 nm, and is characterized by low attenuation. For such a reason, this window is very suitable for FSO operation, and is reliable, high-performance, and inexpensive transmitter and detector components are generally available and commonly used in today's service provider networks and transmission equipment. Highly sensitive silicon avalanche photo diode (APD) detector technology and advanced vertical cavity surface emitting laser (VCSEL) technology can be used for operation in this atmospheric window.

Then, other transmission windows are that at 1060 nm and 1250 nm, which show extremely low attenuation values. However, transmission components to build FSO system at 1060 nm are very limited and are typically bulky (e.g., YdYAG solid state lasers). Because this window is not specially used in telecommunications systems, high-grade transmission components are rare. Semiconductor lasers especially tuned to the nearby 980 nm wavelength (980 nm pump lasers for fiber amplifiers) are commercially available. However, the 980 nm wavelength range experiences atmospheric attenuation of several dB/km even under clear weather conditions. At the same time, transmitters operating at 1250 nm are rare. Lower power telecommunications grade lasers operating typically between 1280-1310 nm are commercially available. However, atmospheric attenuation increases drastically at 1290 nm, making this wavelength only marginally suitable for free space transmission.

Finally, the 1550 nm band is well suited for free space transmission due to its low attenuation, as well as the proliferation of high-quality transmitter and detector components. Components include very high-speed semiconductor laser technology suitable for WDM operation, as well as amplifiers (i.e., EDFA, SOA) used to boost transmission power. Because of the attenuation properties and component availability at this range, development of WDM free space optical systems is feasible.

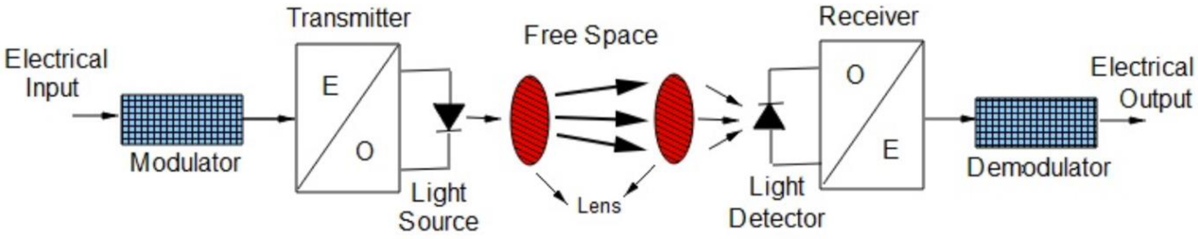
In general, the total attenuation is a combination of atmospheric attenuation in the atmosphere and geometric loss. The total FSO attenuation is given as:

$$\frac{P_r}{P_t} = \frac{d_2^2}{d_1 + (L\theta)} \times exp(-\beta L),$$

where P_t is the transmitted power [mW], P_r is the received power [mW], θ is the beam divergence [mrad], β is the total scattering coefficient [km^{-1}], d_1 and d_2 are the diameter transmitter and receiver aperture [m], respectively.

Figure 15 depicts the block diagram of a FSO optical link from a transmitter to a receiver. FSO contains three components i.e., the transmitter, free space transmitted channel line of sight, and the receiver. The transmitter is considered as an optical source laser diode (LD) or light emitting diode (LED) to transmit of optical radiation through the atmosphere and follows the Beer-Lamberts's law.

Figure 15. Block diagram of an optical wireless link showing the front end of an optical transmitter and receiver.



The selection of a laser source for FSO applications depends on various factors. It is important that the transmission wavelength is correlated with one of the atmospheric windows. As noted earlier, good atmospheric windows are around 850 nm and 1550 nm in the shorter InfraRed (IR) wavelength range. In the longer IR spectral range, some wavelength windows are present between 3–5 micrometers (especially 3.5–3.6 micrometers) and 8–14 micrometers. However, the availability of suitable light sources in these longer wavelength ranges is pretty limited at the present moment. In addition, most sources need low temperature cooling, which limits their use in commercial telecommunication applications.

5.2 Applications

Several FSO applications exist, mainly in telecommunication and computer networking area. Medium and long-range links (i.e., many kilometers) are the mostly used for FSO communications, and concern ground, aeronautical and aerospace applications. The main application is related to outdoor wireless access, where FSO is used by wireless service providers for communication and it requires no license of the EM spectrum. In general, FSO optical links are used to form wireless networks, such as storage area networks, in order to provide access to consolidated, block level data storage.

Outdoor PtP terrestrial FSO links are well known as a promising connectivity solution for first- and last-mile access and backhaul/fronthaul WNs. In fact, the backhaul capacity requirements are expected to scale up to tens of Gbps and the currently proposed mmW links may find it extremely difficult to keep up with these projections. Furthermore, future hyper dense small cell WNs will dictate strict interference avoidance/management requirements. With its high capacity (>10 Gbps per wavelength) and immunity to RF EMI, FSO is well positioned to address these requirements. In the last decade, the literature on FSO has steadily increased and provided a clear understanding of its fundamentals [32]. It is now time to push the limits of FSO technology to the next level with the potential of delivering fibre-like data rates, particularly taking advantage of unique and inherent optical carrier characteristics, which is not possible in RF technologies. For instance, recent works on orbital angular momentum (OAM) multiplexed FSO systems have demonstrated that Tbps transmission data rates are possible [33]. While intensity modulation and direct detection (IM/DD) is commonly preferred in commercial FSO systems, advanced coherent detection techniques coupled with advanced techniques of network coding, multi-carrier modulations, and relay-assisted transmission should be investigated to boost the system performance in terms of error rate and spectral efficiency. Furthermore, custom-designed networking protocols are required for degree constrained FSO WNs.

Figure 16. A relay-assisted FSO system augmented with a moving buffer-aided UAV relay [130].

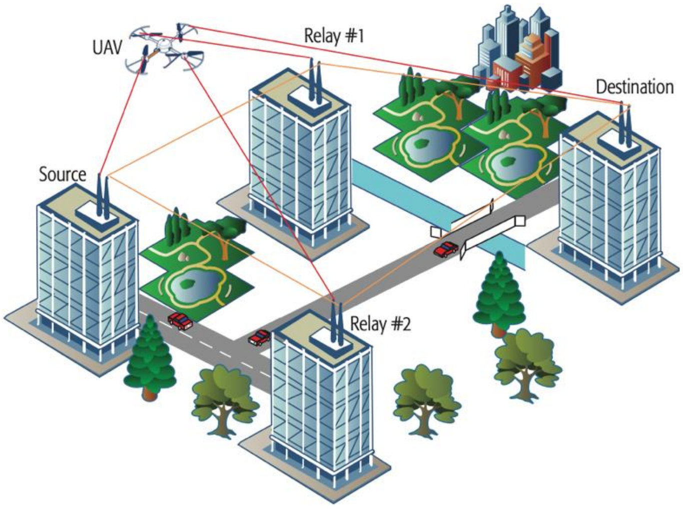
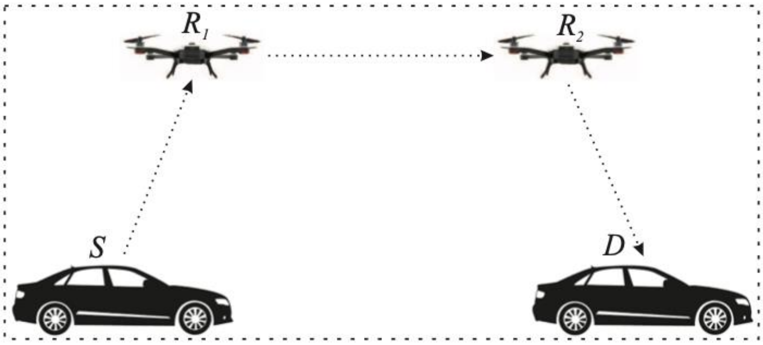


Figure 17. Use of FSO links for vehicular applications, through the use of UAVs [131].



The use of FSO technology for establishing high data rate links between a ground station and a moving platform has also attracted a great deal of attention very recently. Typical applications include connectivity with high-speed trains for providing high-quality broadband services to passengers, and with low-altitude drones -also called unmanned aerial vehicles (UAVs)- in order to form flexible relay nodes for temporary FSO links [130, 131]. Here, the challenges that need addressing are highly accurate and agile pointing, acquisition and tracking (PAT) mechanisms, Tx-Rx synchronization, and efficient MAC and NET layer protocols for frequent hand-overs.

PtP FSO links find also application for communication between terminals in data centre networks (DCNs), with typical link ranges up to a few tens of meters for intra-DCNs. The main advantage being cost-effectiveness, high data rates, and simple deployment, compared to the use of optical fibres. Here, the main challenges include vibrations, dust disposal, and turbulence, as well as beam focusing and steering in dynamic or reconfigurable scenarios, in particular in high-density (i.e., tens to hundreds of server racks) intra-DCN deployments due to the directionality of optical beams.

Furthermore, FSO technology is adopted for the last-mile access, along with other networks. This is particularly used in order to reduce cables of users in the last mile, which is very costly for service providers. FSO can be used to solve such problem by implementing it in the last mile. Indeed, nowadays, more than 95% of the buildings do not have access to the fiber optic infrastructure due to the development of communication systems after the metropolitan areas. FSO technology allows the connection of end- users to the service providers or to other existing networks, providing high-speed connection up to Gbps. FSO provide PtP LoS links, both for military application as well as metro network extensions and backhaul wireless access. Interesting, FSO links are adopted also for communications between spacecraft, including elements of satellite constellation.

The adoption of FSO for high data rate links between a ground station and a mobile node has attracted a great deal of attention very recently. FSO has received growing attention as directional Ground to Aerial (G2A) and Aerial to Aerial (A2A) links for airborne vehicles. Typical applications include the “Airborne Internet”, which is a vision of a largescale multi-hop wireless mesh network consisting of airborne vehicles, which will provide cellular and Internet services to geographical areas where infrastructure is not available or is costly to deploy. In addition to the need for efficient pointing, acquisition and tracking solutions [36], a better understanding of optical propagation is required for vertical/slant G2A links. Figure 16 and Figure 17 show typical applications of FSO links through G2A and A2A wireless links. Furthermore, the presence of clouds and their types have significant implications on the link budget [38]. Innovative PHY designs including synchronization and fading mitigation using adaptive optics, advanced multi-hop relaying, and site diversity, as well as advanced upper-layer techniques are required to enable seamless coverage. The use of quantum cryptography and quantum key distribution (QKD) for long-range FSO and space links are among other current research directions with the aim of enabling quantum-secured communications [39].

The capacity of current satellites working in the Ka-Band reaches hundreds of Gbps but the demand will reach Tbps data rates in the next few years. The FSO technology offers the potential of implementing such high-capacity space-to-ground optical data links, particularly as feeder links for geostationary telecommunications or multimedia satellites [37]. In comparison to RF counterparts, FSO offers reduced electrical power consumption and more compact system designs. One of the first operational satellite systems, which is already using the FSO technology, is the European Data Relay System. Other recent successfully-tested low-Earth-orbit satellite-to-ground links include SOTA (Small Optical Transponder) by NICT-Japan in SOCRATES mission, OPALS (Optical Payload for Lasercomm Science) on-board ISS (International Space Station), and various versions of OSIRIS (Optical space IR link System) by German Aerospace Centre (DLR). Further developments are expected in the near future in Europe, Japan, and the United States, while standardization efforts are also on-going.

Long range links (>20km) can also be established using the UV-C band, thanks to the recent advances in miniaturized semiconductor Tx/Rx devices, able to efficiently operate in the solar blind regime, although the related applications must comply with eye and skin exposure safety limitations [34]. The unique characteristic of atmosphere scattering facilitates the propagation of UV waves for non-LoS channels by relaxing or eliminating PAT requirements. Research focusing in this field, which mostly concerns non-civilian applications, is on the design of low-power Tx/Rx devices, propagation characterization, and advanced channel coding.

6. Power Line Communications systems

Power line communications (PLC) is a communication technology, which exploits the existing infrastructures (i.e., power lines), acting to deliver Alternating Current (AC) (50 Hz or 60 Hz) or Direct Current (DC) electric power [132]. Hence, PLC uses high-frequency signals with frequency components starting from a few hundred Hz up to a few hundred MHz. There exist different frequency bands used for PLC, which are related to different applications and their data-rate requirements, the specifics of grid topologies over which PLC is applied, as well as the ability of PLC technology to deal with the harsh communication environment.

The transmission of data on a power line can be affected by several factors, such as (i) the attenuation at frequencies of interest, (ii) noise, (iii) interference from electronic devices connected to the system, and (iv) channel variability in both time and frequency. Nevertheless, PLC also present some strengths such as (i) the network is already constructed and ready to be used, and (ii) the possibility to use the same channel to provide both electricity and data to users.

The power line channel is a very harsh and noisy transmission medium that can be very difficult to model. The power line channel is frequency-selective and time-varying, and is impaired by colored background noise and impulsive noise. Additionally, the structure of the grid differs from country to country and also within a country and the same applies for indoor wiring practices. Specifically, the channel transfer function of the power line channel may vary abruptly when the topology changes, i.e., when devices are plugged in or out, and switched on or off. However, the power line transfer function exhibits a time-varying behavior even if the topology of the network and the load (appliances) attached to it do not undergo abrupt changes.

In particular, the power line channel exhibits a short-term variation because the high-frequency parameters of electrical devices depend on the instantaneous amplitude of the main voltage, which can translate in periodic variations of the load impedances. In addition, the noise injected into the channel by appliances is also dependent on the instantaneous amplitude of the mains voltage. Therefore, a cyclo-stationary behavior on the time selectivity of the channel as well as on the noise arises, and the period is typically half the main period.

PLC can be divided into three different classes i.e.:

(i) **ultra-narrow band (UNB)**: very low data rates (about 100 bps) are reached in the field of Ultra Low Frequency (i.e., 0.3-3 kHz) or at the top of the Super Low Frequency (i.e., 30-300 Hz). Very long distances, even exceeding 150 km, can be reached. The UNB-PLC transmissions are already mature, and implemented by at least two decades, but unfortunately, they adopt proprietary technologies;

(ii) **narrowband (NB)**: NB class operates in the frequency bands VLF/LF/MF (i.e., in the range 3-500 kHz). This range includes the European CENELEC band (3- 148.5 kHz), the American FCC band (10-490 kHz), the Japanese ARIB band (10-450 kHz) and the Chinese band (3-500 kHz). The NB-PLC can be further divided between (i) Low Data Rate (LDR) and (ii) High Data Rate (HDR). In LDR, we have a single-carrier technology with capacity data rate of a few kbps. Typical examples of LDR NB-PLC are LonWorks standards, IEC 61334, X10, HomePlug C&C and SITRED. On the other side, HDR is a multicarrier technology capable of data rates ranging from tens of kbps up to 500 kbps. Typical examples are technologies based on ITU-T standards by G.hn, IEEE P1901.2, PRIME and G3-PLC.

(iii) **broadband (BB)**: the BB class operates at frequencies of HF/VHF (i.e., 1.8-250 MHz) with a data rate range from a few Mbps to several hundred Mbps. Considering the NB, in different regions of the world there are different allocations of the frequency band. BB features data rates at the physical layer from a few Mbps to Gbps and it is sometimes also referred to as Broadband over Power Lines (BPL). Broadband technology standards are covered by several organizations such as Universal Powerline Association (UPA), Open PLC European Research Alliance (OPERA), Consumer Electronics Power line Communication Alliance (CEPCA), Institute of

Electrical and Electronics Engineers (IEEE), International Telecommunication Union (ITUT-T) and HomePlug Powerline Alliance. Typical examples of BB-PLC technologies are: HomePlug 1.0 (and following version), IEEE 1901, ITU-T G.hn, etc

The main organizations that regulate the use of the frequency bands are (i) CENELEC - European Committee for Electrotechnical Standardization, (ii) ARIB – Association of Radio Industries and Businesses, (iii) EPRI – Electric Power Research Institute, and (iv) FCC – Federal Communications Commission. Table 4 collects the different frequencies used in different areas according to specific organizations.

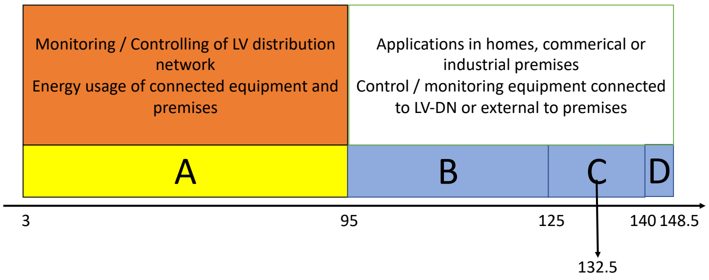
Table 4. Frequency bands in different areas.

Area	Organization	Frequency band [kHz]
Europe	CENELEC	3-95; 95-125; 125-140; 140-148.5
China	EPRI	3-90; 3-500
Japan	ARIB	10-450
USA	FCC	10-490

In Europe, CENELEC established the ranges of frequencies for powerline communications systems in low voltage with EN 50065-1. It introduced a unique regulation in the countries that join it. Four different bands of use are defined, as also collected in Figure 18:

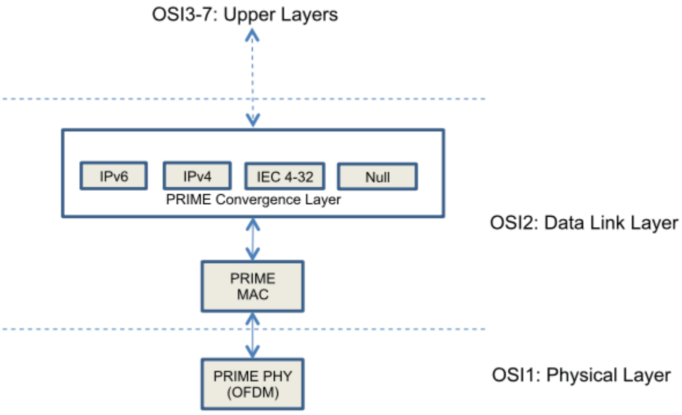
- CENELEC A (3 kHz - 95 kHz): the frequencies in this band are to be used only for monitoring and control applications for low voltage distribution network, including the use of energy equipment and premises connected including energy use of the equipment and premises connected.
- CENELEC B (95 kHz – 125 kHz): it can be used by all applications, and no protocol required for access.
- CENELEC C (125 kHz – 140 kHz): this is used for home networking system.
- CENELEC D (140 kHz - 148.5 kHz): this is used for security and alarm systems.

Figure 18. CENELEC frequency standards.


Monitoring / Controlling of LV distribution network
Energy usage of connected equipment and premises
Applications in homes, commerical or industrial premises
Control / monitoring equipment connected to LV-DN or external to premises
A
B
C
D
3
95
125
140
148.5
132.5

Regarding the standardization, PLC actually comprises several standards focusing on different performance factors and issues relating to specific applications and operating environments. Two of the most well-known are PRIME and G3. PRIME (PoweRline Intelligent Metering Evolution) is a standard acting at the physical and MAC layers, as shown in Figure 19. It was developed to provide an OFDM based narrowband PLC standard over the CENELEC A-band. It defines a narrowband transmission system PLC network implemented on the low-voltage supply network i.e., it is designed to transmit and receive on electrical networks distribution at 50-60 Hz AC. The physical layer exploits a frequency band ranging from 3 kHz to 95 kHz, as defined by EN50065-1, and so included in the CENELEC A band. The noise and distorting effects introduced by the channel frequencies below 40 kHz make PRIME working in the sub-interval of 41.992 kHz and 88 867 kHz with a 47 kHz bandwidth.

Figure 19. OSI reference model of ITU-T G.9904 PRIME standard.



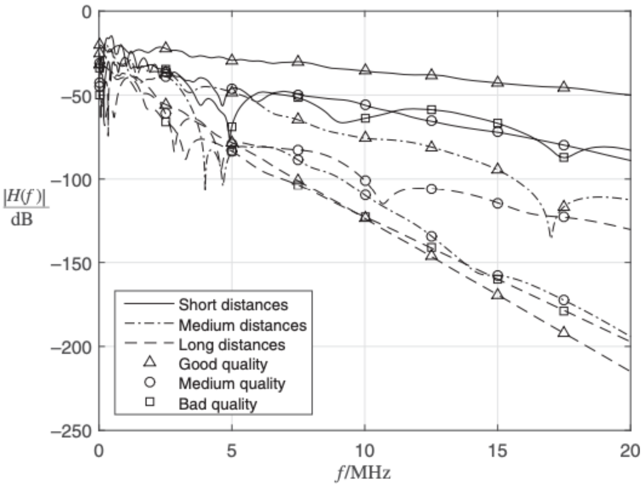
G3 operates on CENELEC-A band (3-95 kHz) in Europe and can be extended across the full band FCC to provide a higher data rate in other countries. G3 allows bi-directional communications with an effective data rate of 20-40 kbps in CENELEC-A band and up to 200-400 kbps whole gang FCC (G3-FCC). G3 uses OFDM to provide high resilience to interference and attenuation. As a result, reliable communications up six miles can be obtained, while crossing between medium voltage transformers. The standard also allows communication on the low voltage and medium voltage (LV/MV) crossing transformation for a total distance of up to 2-3 km, depending on the condition of the channel.

It follows that different length classes have been selected to define reference channels:

- short: approx. 150 m;
- medium: approx. 250 m;
- long: approx. 350 m.

Three levels of quality have been specified for the 150 m and 350 m class, and two levels for the 250 m class. Furthermore, one so-called model channel has been defined. Thus, in total there is a set of nine reference channels covering power line networks in the access domain. The frequency responses of such channel models are shown in Figure 20. Notice that although there is no European Harmonized Standard for PLC above 148,5 kHz available, a few initiatives developed inhouse PLC systems between 1,6-30 MHz.

Figure 20. Magnitude frequency responses for reference PLC channels.



The characterization of low voltage distribution lines inside homes and small offices as a transmission medium for broadband communications is the main common usage of PLC. The most interesting aspects of indoor PLC channels is their strong selectivity in frequency domain and their time-variation.

The basic principle of PLC is that of carrier waves. A typical scheme of a PLC modem considers the low-frequency voltage wave (i.e., 50-60 Hz) with modulated higher frequency data signals at the transmitter side. Signals at different frequencies are admitted on the same cable, and separated with appropriate filters by the receiver.

Regarding the limitation of PLC systems, we remind some limits that slow down PLC developing and standardization process. The first issue is related to the power supply providers that try to keep actual distribution network structures in order to maintain their control. On the other hand, ICT manufacturers push to develop PLC technology applied in the Smart Grid scenario as a new promising field.

In the electrical supply system it is possible to distinguish three different network levels that are used to transport electrical power in order to distribute it to home users and industries i.e.:

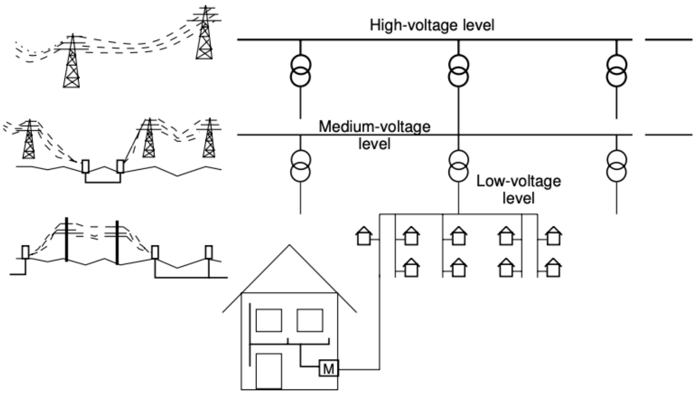
(i) **High-voltage networks**: from about 100 to 500 kV, they are usually realized with overhead supply cables and are mainly used to connect power station with large supply regions or big customers. They are also employed to exchange power between different states or continents as they are suitable for very long distance link;

(ii) **Medium-voltage networks**: from about 10 to 30 kV, they are realized as both overhead and underground networks. Spanned distance are significantly shorter than in the high-voltage networks, and they are used for supply larger areas such as metropolitan and large industrial or commercial customers;

(iii) **Low-voltage networks**: they are different in each country (i.e., in Europe they are distributed with 230/400 V, whereas in U.S.A they are distributed with 120 V system). The cable length is shorter, few hundred meters, due to the power loss introduced by underground connection cables. These networks are used to supply end-users either as individual costumers or as single users of a bigger costumers.

Figure 21 depicts the schematic of different voltage networks used for electrical supply. We observe that low voltage supply distribution networks are the most widely spread networks, and they are used of a huge number of connected users. On the other hand, low voltage networks cover few hundreds of meters between the transformer unit and the costumers, therefore PLC offers an alternative solution of the realization of the so-called “last mile” access.

Figure 21. Schematic of the structure of electrical supply networks, with low, medium and high voltage networks.



Finally, another issue is related to the interference level on radio emitters. In order to avoid interferences between the power line communication and radio transmission, a shared regulatory was developed. The power level emitted by PLC is usually few Watt and the inducted electromagnetic field is comparable on ones of mobile phones, and is lower than the ones emitted by television and radio transmission.

It follows that, since power line carrier was not designed for data transmission, it provides a harsh environment for it. For this aim, the channel has to be analysed and modelled accordingly. Indeed, the channel cannot be modelled as an easy Additive White Gaussian Noise (AWGN), but the transfer function is extremely complicated. Power line networks are usually made of a variety of conductor types, joined almost a random, and terminating into loads of varying impedance. The amplitude and phase response on such transmission medium may vary widely with frequency. Moreover, the channel transfer function itself is time varying since plugging in or switching off devices connected to the network would change the network topology. Hence, the channel may be described as random and time varying with a frequency dependent SRN over the transmission bandwidth.

7. Bluetooth

7.1 Introduction

Bluetooth is a standard of wireless communication systems used for transferring data between fixed and mobile devices in short distances and a personal area network (PAN) context. It uses UHF radio waves belonging to the industrial, scientific and medical (ISM) radio bands, from 2.402 GHz to 2.480 GHz.

Bluetooth was standardized from IEEE as IEEE 802.15.1 initially but from 1998 it has been managed by the Bluetooth Special Interest Group (SIG). The Bluetooth SIG is a non-for-profit organization committed to maintain and update the Bluetooth standard. Its headquarter is in Kirkland (Washington) and it is constituted by more than 35,000 companies operating in ICT and electronic sectors. The Bluetooth Low Energy (BLE) is the version of Bluetooth designed for very low power transmissions. It uses the 2.4 GHz frequency band and adopts the frequency-hopping spread spectrum technique, together with 40 channels for exchanging data. The Bluetooth LE is characterized by some flexible features. For example, different PHY options supporting data rates (from 125 kbps to 2 Mbps), different power levels (from 1 mW to 100 mW) and several security options. From a network point of view, BLE also supports different topologies including point-to-point, broadcast, and mesh networking. Table 5 compares the main features of BLE and Bluetooth [40].

Table 5. Comparison of main features of BLE and Bluetooth.

Features	Bluetooth Low Energy (LE)	Bluetooth Classic (1.0/2.0/3.0/4.0)
Frequency Band	2.4GHz ISM Band (2.402 – 2.480 GHz Utilized)	2.4GHz ISM Band (2.402 – 2.480 GHz Utilized)
Channels	40 channels with 2 MHz spacing	79 channels with 1 MHz spacing
	(3 advertising channels/37 data channels)	
Channel Usage	Frequency-Hopping Spread Spectrum (FHSS)	Frequency-Hopping Spread Spectrum (FHSS)
Modulation	GFSK	GFSK, π/4 DQPSK, 8DPSK
Power Consumption	~0.01x to 0.5x of reference	1 (reference value)
	(depending on use case)	
Data Rate	LE 2M PHY: 2 Mbps	EDR PHY (8DPSK): 3 Mbps
	LE 1M PHY: 1 Mbps	EDR PHY (π/4 DQPSK): 2 Mbps
	LE Coded PHY (S=2): 500 kbps	BR PHY (GFSK): 1 Mb/s
	LE Coded PHY (S=8): 125 kbps	
Max Tx Power (*)	Class 1: 100 mW (+20 dBm)	Class 1: 100 mW (+20 dBm)
	Class 1.5: 10 mW (+10 dBm)	Class 2: 2.5 mW (+4 dBm)
	Class 2: 2.5 mW (+4 dBm)	Class 3: 1 mW (0 dBm)
	Class 3: 1 mW (0 dBm)	
Network Topologies	Point-to-Point (including piconet)	Point-to-Point (including piconet)
	Broadcast	
	Mesh	

(*) Devices shall not exceed the maximum allowed transmit power levels set by the regulatory bodies that have jurisdiction over the locales in which the device is to be sold or intended to operate. Implementers should be aware that the maximum transmit power level permitted under a given set of regulations might not be the same for all modulation modes.

From the Physical layer point of view, the BT system operates in the 2.4 GHz ISM band at 2400-2483.5 MHz (Table 6). It uses 40 RF channels. These RF channels have center frequencies $2402 + k * 2$ MHz, where $k = 0, \ldots, 39$.

Table 6. BT frequencies [41].

Regulatory Range	RF Channels
2.400 – 2.4835 GHz	$f = 2402 + k * 2$ MHz, with $k = 0, \ldots, 29$

7.2 The different Versions of Bluetooth

The Bluetooth technology is characterized by an important evolution: from the first release 1.0, we have several releases (e.g., 1.2, 2.0, 2.1, 3.0, 4.0, 4.1 and 4.2). Now, it is currently at 5.2 version. Every Bluetooth release introduced new features. For example, in the 2.0 version we have the radio frequency interference management based on the frequency hopping technique, together with high data rate and low power consumption. In 2.1 release (2007) we have more security during data exchange, lower power consumption and a better pairing system (no PIN to be put). Bluetooth 3.0 (2009) provides Wi-Fi connection integration with higher data speed. The first Bluetooth releases (from 1.0 to 3.0) are considered as “Bluetooth Classic”. During its evolution, three factors have been enhanced: higher range, higher data speed and lower power consumption, depending on modulation scheme and data packet.

The version 1.0 of Bluetooth was far slower than the current ones:

The data speeds were limited to 1 Mbps and the range only reached as far as 10 meters in the Bluetooth 1.0, since they are based on Gaussian Frequency Shift Keying (GFSK) modulation scheme. Bluetooth 2.0 adopted two different modulation schemes (p/4-DQPSK and 8DPSK), able to reach data speeds around 2 Mbps and 3 Mbps, respectively. Bluetooth 3.0 improves data speeds supporting the 802.11 standard (for up to 24 Mbps of data transfer). Bluetooth 4.0 (also known as Bluetooth Low Energy, BLE), provided Low Energy function, in order to be used in IoT devices with remote control and energy-harvesting. Suitable for low power consumption-based applications, BLE offers lower data date (up to a maximum of 1 Mbps using GFSK modulation scheme). For this reason, BLE is not used by applications requiring a continuous data stream (e.g., wireless headphones). It is only used for applications transferring small amounts of data (in bits) periodically (e.g., fitness devices). Bluetooth 5.0 enhances previous BLE releases in terms of lower power applications, data rate and range. It can provide four different data rates: 2 Mbps, 1 Mbps, 500 kbps, and 125 kbps.

The following Table 7 summarizes the different versions of Bluetooth and BT [42].

Table 7. Evolution of BT.

Core version	Issue Year	Features	Major Improvements
1.0	1999	GFSK modulation scheme	-
1.2	2003	GFSK modulation scheme	Adaptive frequency hopping, inquiry based RSSI

2.0	2004	p/4-DQPSK and 8DPSK modulation scheme	2.1 Mbps peak data rates
2.1	2007	p/4-DQPSK and 8DPSK modulation scheme	3.0 Mbps peak data rates
3.0	2009	addition of 802.11	24 Mbps peak data rates
4.0	2010	GFSK modulation scheme	Lower energy consumption, broadcasting, lower connection latency
4.1	2013	Classic Secure Connections Dual Mode Topology L2CAP Dedicated Channels	• Improved device power management by pairing that allows automatic powering up and down • Provides 128-bit AES encryption strength • Enables a device to act as a Bluetooth dual-mode hub and Bluetooth LE peripheral at the same time • Enables IPv6 over Bluetooth LE
4.2	2014	Internet protocol support profile (IPSP) LE Privacy 1.2 LE Secure Connections LE Data Length Extension	• Improved security, low energy data packet length extension, link layer privacy • A Bluetooth LE sensor can access the Internet through a gateway device • Keeps Bluetooth LE devices from being tracked • Provides 128-bit AES encryption strength for Bluetooth LE • Increases data throughput up to 2.5x
5.0	2016	2 Mbps LE LE Long Range LE Advertising Extension	• Higher data rates (48 Mbps), better energy efficiency, higher broadcasting message capacity, larger range and strong point-to-point connection and reliability • Extends the data rates supported by Bluetooth LE up to 2 Mbps, thus doubling the speed • Extends the range supported by Bluetooth LE devices to four times the range • Support for longer advertisement messages for more feature rich Bluetooth beacons
Bluetooth	2017	LE Topography	Mesh networking significantly extends

Mesh		Extension	the area covered by a cooperative Bluetooth LE network
5.1	2019	Direction finding	Improves indoor positioning, asset tracking, proximity applications, and indoor navigation
5.2	2019	Isochronous channels LE power control (LEPC) Low Energy (LE) Audio, Enhanced Attribute Protocol (EATT) LE Isochronous Channels (ISOC)	• Enables audio streaming and synchronized data transfer over Bluetooth LE • Allows dynamic optimization of power consumption over Bluetooth LE • Supports concurrent transactions with the aim to reduce the end-to-end latency of one or more applications and improve user experience in terms of responsiveness

7.3 Bluetooth 5.2

The Bluetooth release actually used is 5.2 version. It was released by Bluetooth SIG on 31 December 2019. The most important features are [43] [44] [45]:

- LE Isochronous Channels:
  - Audio enablement over BLE and High Data rate
  - Broadcast Audio to multiple devices
  - Time-based data distribution to different devices
  - Enhanced Attribute Protocol (EAP) making concurrent Attribute Protocol (ATT) transactions
  - Reduced latency
- More efficient connections and lower power:
  - LE Power Control
  - Reduction of power consumption by dynamic power management
  - active maintenance of receiver signal strength (for efficient connections)
  - coexistence with other wireless devices with 2.4 GHz frequency range and present in the same area

From a technical point of view, the most important features are:

a) Low Energy (LE) Audio
b) Enhanced Attribute Protocol (EATT)
c) LE Power Control LE (LEPC)
d) LE Isochronous Channels (ISOC)

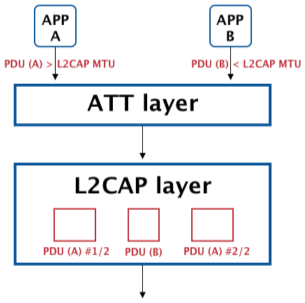
a) Low Energy (LE) Audio

The LE Audio introduces a new audio codec with higher quality and lower power, Low Complexity Communications Coded (LC3). It can provide higher quality than SBC codec used in Bluetooth Classic releases. It can support multiple and synchronized audio data streams (e.g., broadcasting audio streams to multiple devices), e.g., for multiple languages and audio content sharing.

b) Enhanced Attribute Protocol (EATT)

The Enhanced Attribute Protocol (EATT) is an evolution version of the previous Attribute Protocol (ATT). If ATT is a sequential protocol, the EATT enables multiple and parallel communications between a BT client and a server, reducing the latency. EATT is optional, it requires the adoption of encryption schemes between the BT devices. From a protocol point of view, EATT separates the L2CAP layer Maximum Transmission Unit (MTU) from the Attribute layer's MTU.

Figure 22. ATT and L2CAP layer separation in BT5.2.



If L2CAP layer MTU is smaller than the Attribute layer MTU, the L2CAP layer fragments the PDUs coming from the Attribute layer into smaller chunks and interleaves the PDU chunks coming from different applications.

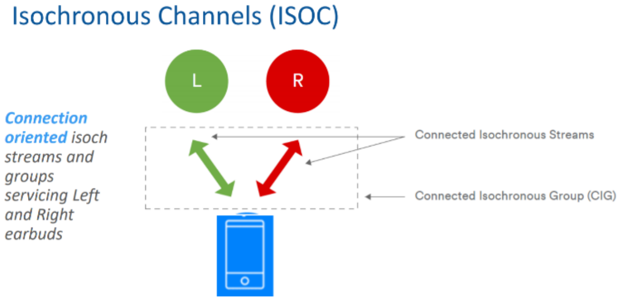
c) LE Power Control (LEPC)

The received signal strength indicator (RSSI) is used to estimate the distance of wireless devices if the original transmit power is known to the receiver. Using LEPC and the RSSI value, a BT5.2 device can better control the quality of the radio signal, reducing error rates at the receiver and improve the coexistence (Note: optional feature) with other wireless signals in the 2.4 GHz band (e.g., Wi-Fi and Zigbee).

d) LE Isochronous Channels (ISOC)

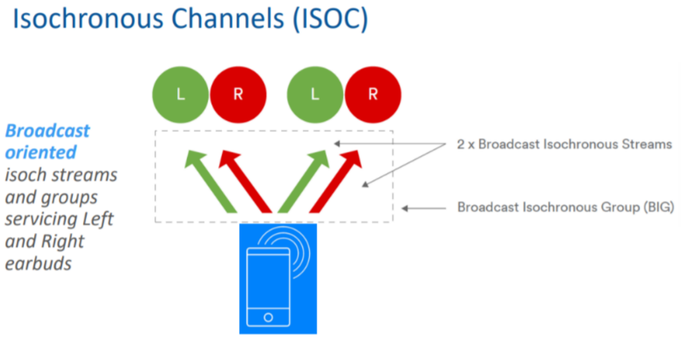
The Isochronous Physical Channel (ISOC) allows the data communication to several devices for time-synchronized processing. ISOC is fundamental for LE Audio implementation and enables the BT5.2 to provide both time-depending data transmissions and their synchronized rendering, by involving multiple devices. ISOC is used for each LE PHYs: 1M, 2M PHY, and LE Coded PHY (both s=2 and s=8). ISOC supports both connection-oriented (connections) and connectionless communication (broadcasts). In case of connections, each stream is related to as a Connected Isochronous Stream (CIS). If several CISes need to be synchronized (e.g., some directed to left channel and other to right channel), they are grouped into Connected Isochronous Group (CIG). A single device can create multiple CIGs.

Figure 23. BT5.2 connections (connection-oriented): Connected Isochronous Streams (CIS) and Connected Isochronous Groups (CIG).


Isochronous Channels (ISOC)
L
R
Connection oriented isoch streams and groups servicing Left and Right earbuds
Connected Isochronous Streams
Connected Isochronous Group (CIG)

In case of connectionless communication (broadcasts), a group of synchronized streams are used to stream data from a single source to multiple devices. Each stream is related to a Broadcast Isochronous Stream (BIS). A group of BISes are related to a Broadcast Isochronous Group (BIG). For example, it happens when audio data coming from a TV streaming are sent to multiple devices (e.g., different individuals wearing earbuds).

Figure 24. BT5.2 broadcasts (connection-oriented): Broadcast Isochronous Streams (BIS) and Broadcast Isochronous Groups (BIG)


Isochronous Channels (ISOC)
L
R
L
R
Broadcast oriented isoch streams and groups servicing Left and Right earbuds
2 x Broadcast Isochronous Streams
Broadcast Isochronous Group (BIG)

The ISO Interval defines a specific event interval, and it can range from 5 ms to 4 seconds typically. Each event is divided into multiple subevents. In case of connections, the master will send a packet to the slave in each subevent and the slave will respond with a packet. In broadcasts, only the master will send a packet in each subevent. Data retransmissions are supported by ISOC. In case of broadcasts, retransmissions are only sent by the Master, while in case of connections, retransmissions are sent when a slave has not acknowledged a packet. Finally, the retransmissions are sent on different channels from that one used by the original packet. It can reduce the packet loss or corruption situation.

7.3.1 Architecture

The Bluetooth Core system is formed by a Host, a Primary Controller and zero or more Secondary Controllers [41] [43], as shown in Figure 25. The Bluetooth BR/EDR core system implements all these four protocol layers and the common service layer protocol defined by Bluetooth standard. The Service Discovery Protocol (SDP) and the general profile requirements are specified in the Generic Access Profile (GAP). The BR/EDR Core system includes support of Alternate MAC/PHYs (AMPs) including an AMP Manager Protocol and Protocol Adaptation Layers (PALs) supporting externally referenced MAC/PHYs. Bluetooth LE core system implements these four layers and the common service layer protocols defined by Bluetooth standard. The Security Manager (SM), Attribute Protocol (ATT) and profile requirements are specified in the Generic Attribute Profile (GATT) and Generic Access Profile (GAP).

Figure 25. Bluetooth core system architecture.

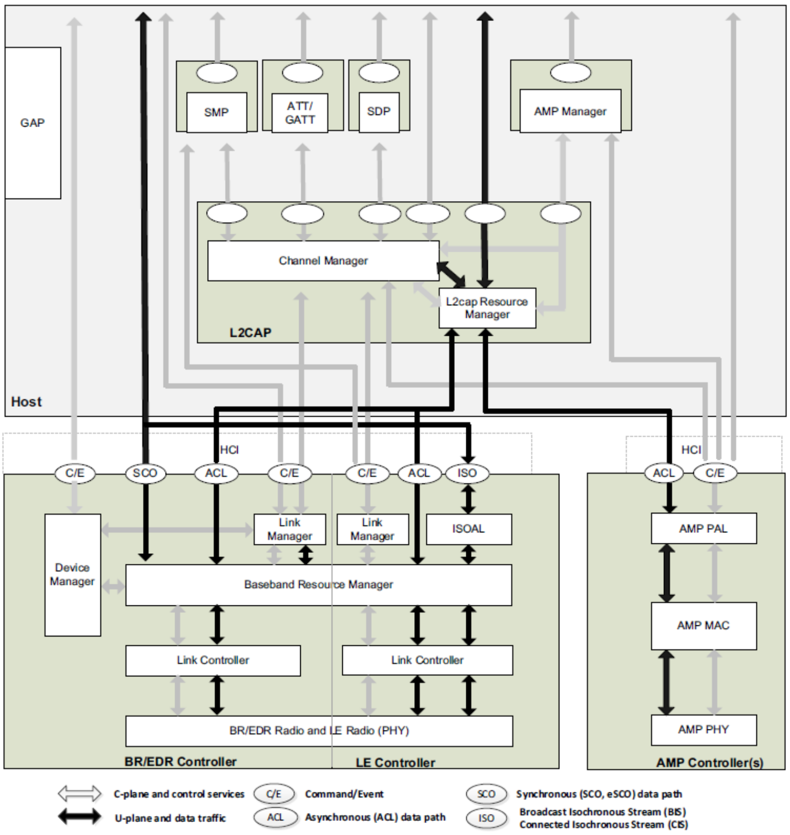


Figure 25 shows the Core blocks of Bluetooth core system. Link Manager, Link Controller and BR/EDR Radio blocks include a BR/EDR Controller. An AMP PAL, AMP MAC, and AMP PHY include an AMP Controller. Link Manager, Link Controller and LE Radio blocks include an LE Controller. L2CAP, SDP and GAP blocks include a BR/EDR Host. L2CAP, SMP, Attribute protocol, GAP, and Generic Attribute Profile (GATT) blocks include an LE Host. The Bluetooth specification enables interoperability between different Bluetooth releases using the definition of protocol messages exchanged at equivalent layers.

The Bluetooth core system protocols are the Radio (PHY) protocol, Link Control (LC) and Link Manager (LM) protocol or Link Layer (LL) protocol, AMP PAL, Logical Link Control and Adaptation protocol (L2CAP), and AMP Manager protocol (Table 8). Moreover, the Service Discovery protocol (SDP) and the Attribute protocol (ATT) are service layer protocols that can be required and used by some Bluetooth applications.

Table 8. Bluetooth Core Architectural Blocks.

Bluetooth CORE ARCHITECTURAL BLOCKS		
Host architectural blocks	*Channel manager*	The channel manager is responsible for creating, managing and closing L2CAP channels for the transport of service protocols and application data streams. The channel manager uses the L2CAP protocol to interact with a channel manager on a remote

		(peer) device to create these L2CAP channels and connect their endpoints to the appropriate entities.
	L2CAP resource manager	The L2CAP resource manager block is responsible for managing the ordering of submission of PDU fragments to the baseband and some relative scheduling between channels to ensure that L2CAP channels with QoS commitments are not denied access to the physical channel due to Controller resource exhaustion.
	Security Manager Protocol	The Security Manager Protocol (SMP) is the peer-to-peer protocol used to generate encryption keys and identity keys. The protocol operates over a dedicated fixed L2CAP channel. The SMP block also manages storage of the encryption keys and identity keys and is responsible for generating random addresses and resolving random addresses to known device identities.
	Attribute Protocol	The Attribute Protocol (ATT) block implements the peer-to-peer protocol between an attribute server and an attribute client. The ATT client communicates with an ATT server on a remote device over a dedicated fixed L2CAP channel. The ATT client sends commands, requests, and confirmations to the ATT server. The ATT server sends responses, notifications and indications to the client.
	AMP Manager protocol	The AMP manager is a layer that uses L2CAP to communicate with a peer AMP Manager on a remote device. It also interfaces directly with the AMP PAL for AMP control purposes
	Generic Attribute Profile	The Generic Attribute Profile (GATT) block represents the functionality of the attribute server and, optionally, the attribute client. The profile describes the hierarchy of services, characteristics and attributes used in the attribute server. GATT is used on LE devices for LE profile service discovery.
	Generic Access Profile	The Generic Access Profile (GAP) block represents the base functionality common to all Bluetooth devices such as modes and access procedures used by the transports, protocols and application profiles. GAP services include device discovery, connection modes, security, authentication, association models and service discovery.
BR/EDR/LE Controller architectural blocks	Device manager	The device manager is the functional block in the baseband that controls the general behavior of the Bluetooth device. It is responsible for all operations of the Bluetooth system that are not directly related to data transport, such as inquiring for the presence of nearby Bluetooth devices, connecting to Bluetooth devices.
	Link manager	The link manager is responsible for the creation, modification and release of logical links (and, if required, their associated

		logical transports), as well as the update of parameters related to physical links between devices. The link manager achieves this by communicating with the link manager in remote Bluetooth devices using the Link Manager Protocol (LMP) in BR/EDR and the Link Layer Protocol (LL) in LE.
	Baseband resource manager	The baseband resource manager is responsible for all access to the radio medium. It has two main functions. At its heart is a scheduler that grants time on the physical channels to all of the entities that have negotiated an access contract. The other main function is to negotiate access contracts with these entities. An access contract is effectively a commitment to deliver a certain QoS that is required in order to provide a user application with an expected performance.
	Link Controller	The Link Controller is responsible for the encoding and decoding of Bluetooth packets from the data payload and parameters related to the physical channel, logical transport and logical link.
	PHY	The PHY block is responsible for transmitting and receiving packets of information on the physical channel. A control path between the baseband and the PHY block allows the baseband block to control the timing and frequency carrier of the PHY block. The PHY block transforms a stream of data to and from the physical channel and the baseband into required formats.
	Isochronous Adaptation Layer	The Isochronous Adaptation Layer (ISOAL) enables the upper layer to send or receive isochronous data to or from the Link Layer in a flexible way such that the size and interval of data packets in the upper layer can be different from the size and interval of data packets in the Link Layer. The ISOAL uses fragmentation/recombination or segmentation/reassembly operations to convert upper layer data units into lower layer data units (or the other way around).
AMP Controller architectural blocks	AMP HCI	The AMP HCI is the logical interface between an AMP Controller and Host (L2CAP and AMP manager). HCI is an optional layer used when the Host and AMP Controller(s) are physically separated. Support for AMPs requires additional HCI commands and events.
	AMP PAL	The AMP PAL is the AMP layer interfacing the AMP MAC with the Host (L2CAP and AMP Manager). It translates commands from the Host into the specific MAC service primitives and primitives into commands, and it translates primitives from the AMP MAC into understandable event(s) for the Host. The AMP PAL provides support for AMP channel management, data traffic according to specified flow specifications, and power efficiency.

	AMP MAC	The AMP MAC is the MAC layer as defined in the IEEE 802 reference layer model. It provides services such as addressing and mechanisms to control and access channels. The AMP MAC is in between AMP PHY and AMP PAL layers.
	AMP PHY	The AMP PHY is the AMP physical layer.

7.3.2 Performance

Bluetooth 5.2 provides a significant increase of the covered range [45]. Bluetooth 4.x can reach distances between 50 and 100 m (outdoor context) and about 10-20 m (indoor context). Bluetooth 5.2 promises to quadruple the coverage range of BLE devices. In fact, this range is about 200 m (outdoor environments) and about 40 m (indoor environments). The choice of the right data rate (125 kbps or 500 kbps) is crucial in terms of coverage range: the decision depends on the application. In fact, using a 500 kb/s data rate we can have twice the range of standard BLE at 1 Mbps, while using 125 kbps data rate we can have twice the range of 500 kbps can be reached.

Greater Speed

Bluetooth 5.2 provides a powerful improvement in the data rate. Bluetooth 4.x can reach a maximum speed of 1 Mbps, while Bluetooth 5 (and upper versions) can support a maximum speed of 2 Mbps.

Beacons Everywhere

Bluetooth 5.2 can also send special data packets, called “advertising packets”, useful to scan nearby areas and search for other Bluetooth devices. In Bluetooth 5.2 beacon messages and packets can be transmitted continuously among transmitters and receivers without requiring the pairing. It means that a beacon message can be delivered to all Bluetooth devices in the same area, e.g., for marketing or infotainment applications. In case of Bluetooth 4.x, the beacons’ message maximum size is 31 bytes, while in case of BT5.2 is 255 bytes. The Table 9 provides a technical comparison of Bluetooth versions.

Table 9. Technical comparison of Bluetooth versions [45].

Feature	Bluetooth Classis	Bluetooth 4.x	Bluetooth 5.x
Radio Frequency (MHz)	2400 to 2483.5	2400 to 2483.5	2400 to 2483.5
Distance/range (meters)	Up to 100	Up to 100	Up to 200
Medium Access technique	Frequency Hopping	Frequency Hopping	Frequency Hopping
Nominal Data rate (Mbps)	1-3	1	2
Latency (ms)	< 100	< 6	< 3
Network Topology	Piconet, scatternet	Star-bus, mesh	Star-bus, mesh
Multihop solution	Scatternet	Yes	Yes
Profile concept	Yes	Yes	Yes
Nodes/active slaves	7	Unlimited	Unlimited
Messager Size (Bytes)	Up to 358	31	255
Certification body	Bluetooth SIG	Bluetooth SIG	Bluetooth SIG

7.3.3 Physical Layer

The different PHY layers

The PHY Layer Bluetooth is a full protocol stack [41] [43] [46]. Bluetooth 5 (and upper layers) adds two new PHY variants to the PHY specification used in Bluetooth 4. Each PHY variant is characterized by specific features with specific scopes. The Host Controller Interface (HCI) is deputed to select one of the three current BT PHY. Their names are LE 1M, LE 2M, and LE Coded, as described in Table 10.

Table 10. BT Physical layers [41] [46].

Physical Layer	Characteristics
LE 1M	LE 1M is the PHY used in Bluetooth 4. It uses Gaussian Frequency Shift Keying. Symbol rate: 1 mega symbol per second (Msym/s). LE 1M uses a frequency deviation of at least 185 kHz for inter-symbol interference mitigation. It is mandatory for Bluetooth.
LE Coded (S=2)	Uses forward error correction to improve reliability at lower signal-to-noise ratios (SNRs) and hence increases range while reducing the data rate. An approximate doubling of range can be achieved with the parameter S set to 2, with data rate being halved. Support for LE Coded is optional.
LE Coded (S=8)	Uses forward error correction to improve reliability at lower signal-to-noise ratios (SNRs) and hence increases range while reducing the data rate. An approximate quadrupling of range can be achieved with the parameter S set to 8, with data rate being reduced to one eighth. Support for LE Coded is optional.
LE 2M	Symbol rate: 2 mega-symbol per second symbol. Support for LE 2M is optional. It uses 2-level Gaussian Frequency Shift Keying (GFSK). LE 2M PHY uses a frequency deviation of at least 185 kHz for inter-symbol interference mitigation.

From a performance BT PHY point of view, the following table summarizes the related key metrics for Bluetooth 5 (and upper versions) [41] [46], as summarized in Table 11.

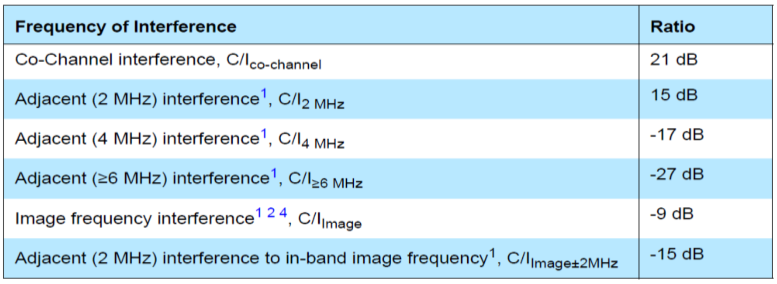
Table 11. Main metrics of BT Physical layers.

PHY Metrics	LE1M	LE Coded S=2	LE Coded S=8	LE2M
Symbol rate	1 Mbps	1 Mbps	1 Mbps	2 Mbps
Data rate	1 Mbps	500 kbps	125 kbps	2 Mbps
Error detection	CRC	CRC	CRC	CRC
Error correction	NONE	FEC	FEC	NONE
Range multiplexer (approx.)	1	2	4	0.8
Modulation scheme	1 Msym/s	1 Msym/s	1 Msym/s	2 Msym/s
Bluetooth 5 (and upper versions) requirement	Mandatory	Optional	Optional	Optional

7.3.4 Interference Management

The signal interference level is measured using a desired signal 3 dB over the target sensitivity level of the 2400-2483.5 MHz frequency band. The Bit Error Rate (BER) must be ≤0.1% for all the signal-to-interference ratios in the case of LE 2M PHY is listed in the following Table 12 [41] [46].

Table 12. Interference performance for LE 2M PHY.



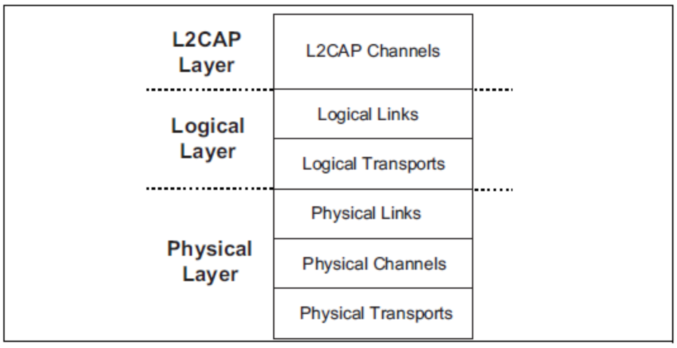
Frequency of Interference	Ratio
Co-Channel interference, $C/I_{co\text{-}channel}$	21 dB
Adjacent (2 MHz) interference[1], $C/I_{2\ MHz}$	15 dB
Adjacent (4 MHz) interference[1], $C/I_{4\ MHz}$	-17 dB
Adjacent (≥6 MHz) interference[1], $C/I_{\geq 6\ MHz}$	-27 dB
Image frequency interference[1 2 4], C/I_{Image}	-9 dB
Adjacent (2 MHz) interference to in-band image frequency[1], $C/I_{Image\pm 2MHz}$	-15 dB

For further information about the other BT PHYs, see [41].

7.3.5 Data Transport Architecture

The Bluetooth data transport system follows a layered architecture [41] [43], as shown in Figure 26.

Figure 26. Bluetooth generic data transport architecture.

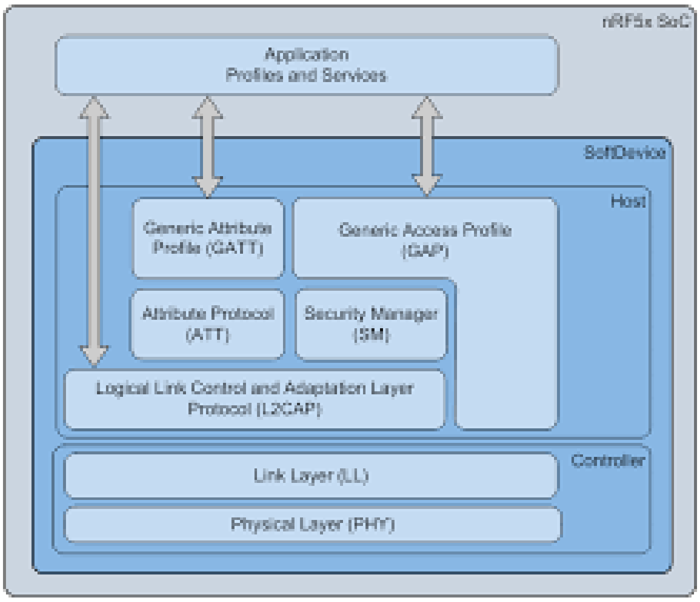


The Bluetooth data transport architecture divides the logical layers into logical links and logical transports. The logical link is referred to an independent transport between several devices, while the logical transport sub-layer is referred to the relationship between some logical links.

7.3.6 Protocol Stack

A Bluetooth Low Energy (LE) protocol stacks is formed by two main components, the host and controller. Each of them contains several stack layers [41] [43] [46]. The Host Controller Interface (HCI) commands are deputed to communicate with the controller.

Figure 27. BT protocol stack [41].



Attribute Protocol. Bluetooth devices contains set of special data, called services, characteristics, and descriptors. Each of them is an attribute type. The Attribute Protocol (ATT) is used by an ATT client to search for attribute details in the attribute table located in a remote device (ATT server) using the PDUs and the Generic Attribute Profile (GATT) defined by the Bluetooth standard.

Logical Link Control and Adaptation Protocol (L2CAP). L2CAP performs the multiplexing, flow control, segmentation, and service data units (SDUs) management.

Link Manager Protocol (LMP). It performs the connection establishment between devices, together with the authentication and the link configuration/control. The LMP is formed by PDUs (Protocol Data Units) exchanged between Bluetooth devices.

Host Controller Interface (HCI). HCI provides a command interface for the controller and for LMP, together with the access layer for all Bluetooth devices. HCI performs the discovery of other Bluetooth devices in the same area.

Logical Link Control and Adaptation Protocol (L2CAP). L2CAP protocol multiplexes multiple logical connections between two Bluetooth devices using different level protocols. This L2CAP protocol (e.g. LLC) is deputed to manage the link layer protocol services between the entities.

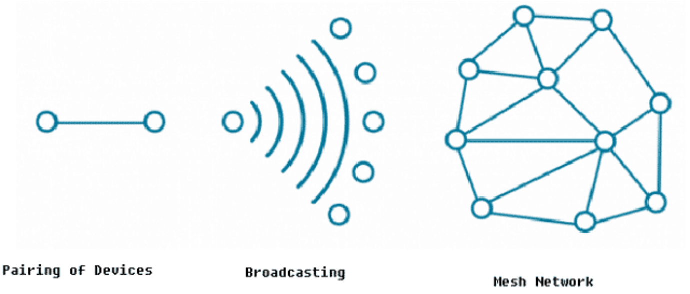
When a Bluetooth device is connected, we can have four operative modes:

- In the Active mode, Bluetooh device is connected to the channel
- In the Sniff mode, Bluetooth device slave device listens only specified slots for messages sent to it
- In the Hold mode, the Bluetooth device does not transmit data
- In the Park mode, Bluetooth device has a little activity (with a very low power consumption)

7.3.7 Network Topology

A Bluetooth 5 (and upper versions) can perform the pairing between two different devices, a broadcast delivering of messages (without pairing) and the connections in a mesh topology, as shown in Figure 28).

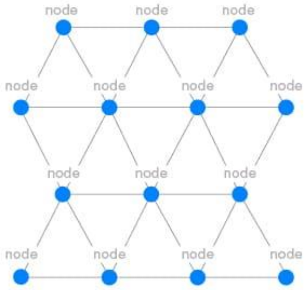
Figure 28. BT Network Topology.



When Bluetooth devices are in the same area, the link management protocol (LMP) layer performs link establishment and the packet size definition. Then, the service delivery protocol enables a Bluetooth device to participate to the Bluetooth network. The Bluetooth Global ID is exchanged and used for the connection establishment.

Bluetooth 5 (and upper versions) devices can be connected in a mesh network topology, using the frequency hopping within the time slots. In a mesh network, each Bluetooth device known as node, can send/receive messages in a broadcast modality, as well as perform the data relaying over several nodes. This topology, as shown in Figure 29, can be used for several applications, as manufacturing facilities, office buildings, shopping centres, business campuses [47].

Figure 29. BT mesh network topology.



Network Nodes

The Bluetooth nodes can be characterized by different features, depending on the specific function to perform, as described below.

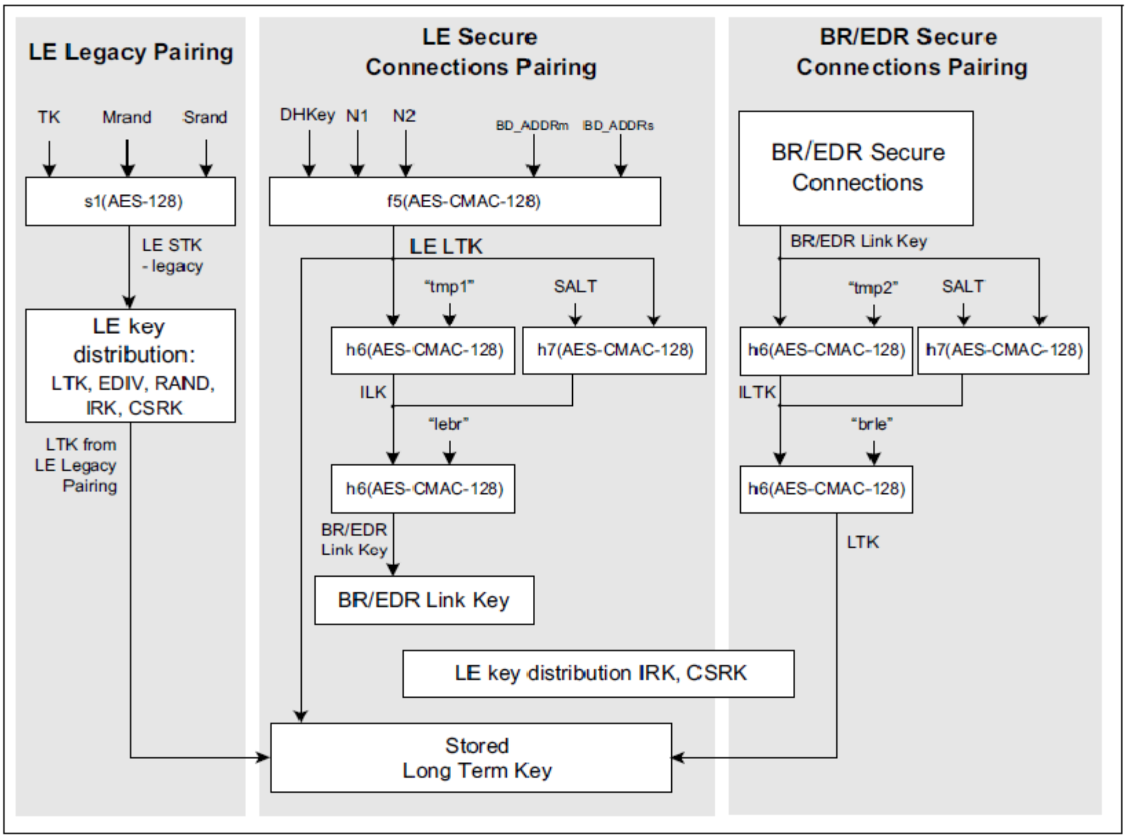
- **Low-Power Feature**: Low-power nodes (LPNs) are power-limited. They can use low power to save it and they work with friend nodes.
- **Friend Feature**: Friend nodes are not power-limited, they store messages sent to LPNs. The friend node delivers the message to LPN if requested.
- **Relay Feature**: Relay nodes can exchange messages across multiple nodes.
- **Proxy Feature:** Proxy nodes exchange mesh messages between GATT and Bluetooth mesh nodes.

7.3.8 Security

BT Security Architecture

The security key hierarchy for BT is shown in the following Figure 30 [41] [48]. The key hierarchy is different depending on the specific physical link used.

Figure 30. BT key hierarchy.



The 5.2 version of the Core Specification enables transmission and reception of encrypted isochronous data over the Broadcast Isochronous Stream (BIS) logical transport. Moreover, the LE Legacy Pairing uses AES-CCM encryption and also provides signed data. The LE physical transport enhances the LE Legacy Pairing through the AES-CMAC and P-256 elliptic curve algorithms.

BT Security model

The Bluetooth security model is based on five different security features: pairing, bonding, device authentication, encryption, and message integrity. The following Table 13 summarizes them.

Table 13. BT 5.2 Security features.

BT 5.2 Security features	Details
Pairing	The process for creating one or more shared secret keys
Bonding	The act of storing the keys created during pairing for use in subsequent connections in order to form a trusted device pair.
Device authentication	verification that the two devices have the same keys
Encryption	message confidentiality
Message integrity	protects against message forgeries

BT5.2 vulnerability

The document (NIST SP 800 121) provides a brief analysis of Bluetooth technology and the main features of the different releases [49], as follows:

- Technical specifications: data rate, range, power, RF physical performance, etc.
- Device authentication and encryption algorithms: AES-CCM, E0/SAFER+, E1/SAFER, and HMAC-SHA-256 algorithms
- Specification compliances by other related organizations: Wi-Fi Alliance and the IEEE
- Communication functions using the Host Controller Interface (HCI): host protocols, SDP and L2CAP
- Bluetooth architecture and network topology: star and mesh topologies.

NIST defines five different Service Levels (SL) of security for Bluetooth devices in the form of

- Level 4: Authenticated link key through Secure Connections is required
- Level 3: Authenticated link key is required
- Level 2: Unauthenticated link key is required
- Level 1: No security is required
- Level 0: No security is required. (Only allowed for Service Discovery Protocol)

These five levels (SL 0, 1, 2, 3, and 4) also defines the typical attacks to Bluetooth devices as:

a) Man-in-the-Middle (MitM) threats;
b) Distributed Denial of Service (DDoS) attacks;
c) user interaction
d) encryption strength used.

The following Table 14 summarizes them, while Table 15 summarizes the main BT vulnerabilities.

Table 14. BT 5.2 Service Levels (SL) of security.

Mode (4 level)	FIPS Approved Algorithms	Provide MITM protection	User interaction during Pairing	Encryption required
4	Yes	Yes	Acceptable	Yes
3	No	Yes	Acceptable	Yes
2	No	No	Minimal	Yes
1	No	No	Minimal	Yes
0	No	No	None	No

The SP 800 121 document also defines a set of mitigation actions, as follows:

- **Link Keys**: For Bluetooth applications a secret symmetric key should be generated. The document specifies how it can be generated
- **Authentication**: Bluetooth devices authenticate as a challenge-response manner. Some devices can verify putting a PIN/legacy pairing, but in case of advanced applications (e.g. in automotive sector) the authentication can be performed through Secure Simple Pairing (SSP) and the P-256 Elliptic Curve
- **Encryption**: The NIST recommends the combination between AES-CMAC and P-256 elliptic curve as the security highest level (SL 4)
- **Vulnerabilities**: The NIST identifies the several vulnerabilities for Bluetooth and the corresponding mitigation actions. The most important ones are referred to eavesdropping, key reuse, insecure

storage of keys, device spoofing, short PIN, key sharing in a piconet or mesh network, implementation of weak encryption algorithms

Table 15. BT5.2 Vulnerabilities.

BT5.2 Vulnerability	Details
Bluesnarfing	Bluesnarfing enables attackers to gain access to a Bluetooth-enabled device by exploiting a firmware flaw in older (circa 2003) devices. This attack forces a connection to a Bluetooth device, allowing access to data stored on the device including the device's international mobile equipment identity (IMEI). The IMEI is a unique identifier for each device that an attacker could potentially use to route all incoming calls from the user's device to the attacker's device.
Bluejacking	Bluejacking is an attack conducted on Bluetooth-enabled mobile devices, such as cell phones. An attacker initiates bluejacking by sending unsolicited messages to the user of a Bluetooth-enabled device. The actual messages do not cause harm to the user's device, but they may entice the user to respond in some fashion or add the new contact to the device's address book. This message-sending attack resembles spam and phishing attacks conducted against email users. Bluejacking can cause harm when a user initiates a response to a bluejacking message sent with a harmful intent.
Bluebugging	Bluebugging exploits a security flaw in the firmware of some older (circa 2004) Bluetooth devices to gain access to the device and its commands. This attack uses the commands of the device without informing the user, allowing the attacker to access data, place phone calls, eavesdrop on phone calls, send messages, and exploit other services or features offered by the device.
Car Whisperer	Car Whisperer is a software tool developed by European security researchers that exploits the use of a standard (non-random) passkey in hands-free Bluetooth car kits installed in automobiles. The Car Whisperer software allows an attacker to send to or receive audio from the car kit. An attacker could transmit audio to the car's speakers or receive audio (eavesdrop) from the microphone in the car.
Denial of Service	Like other wireless technologies, Bluetooth is susceptible to DoS attacks. Impacts include making a device's Bluetooth interface unusable and draining the device's battery. These types of attacks are not significant and, because of the proximity required for Bluetooth use, can usually be easily averted by simply moving out of range.
Fuzzing Attacks	Bluetooth fuzzing attacks consist of sending malformed or otherwise non-standard data to a device's Bluetooth radio and observing how the device reacts. If a device's operation is slowed or stopped by these attacks, a serious vulnerability potentially exists in the protocol stack.

Pairing Eavesdropping	PIN/Legacy Pairing (Bluetooth 2.0 and earlier) and low energy Legacy Pairing are susceptible to eavesdropping attacks. The successful eavesdropper who collects all pairing frames can determine the secret key(s) given sufficient time, which allows trusted device impersonation and active/passive data decryption.
Secure Simple Pairing Attacks	A number of techniques can force a remote device to use Just Works SSP and then exploit its lack of MITM protection (e.g., the attack device claims that it has no input/output capabilities). Further, fixed passkeys could allow an attacker to perform MITM attacks as well

7.3.9 Issues

Bluetooth 5.2 presents some issues in terms of practical development [50].

- **Backwards Compatibility**

Bluetooth 5.2 is only backward compatible with versions 4.0, 4.1 and 4.2. A Bluetooth 5 device needs to connect to another BT5.2 device in order to benefit of the last advanced features. Otherwise, it will operate as Bluetooth 4.2 during a connection to a Bluetooth 4.2 device.

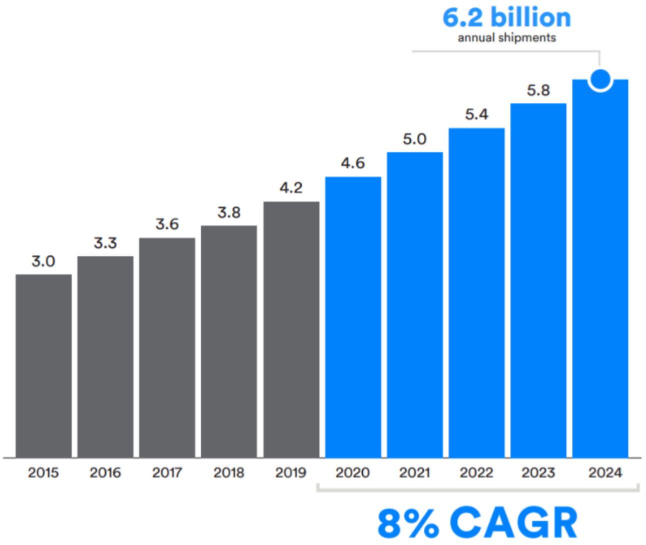
- **Bluetooth 5.2 support is still limited**

In the last months, support for BT5.2 have been increased but it has not received a large adoption, yet. Bluetooth 4.2 is still an industry standard, and it takes more time to implement the innovative features of the last BT5.2. Apple introduced the BT5.2 support with the iPhone 8. After this, Samsung also introduced it with the Galaxy S8.

7.3.10 Applications

The BT5.2 is crucial for several applications. The following Figure 31 shows the context and the corresponding evolution. Request for Bluetooth devices continue to increase: “by 2024, annual Bluetooth enabled device shipments will exceed six billion” [51].

Figure 31. Total Annual Bluetooth Device Shipments (numbers in billions), with a compound annual growth rate (CAGR) of 8% [51].



In case of IoT use cases requiring higher communication performance in terms of ranges, speed and broadcast messaging capacity, the Bluetooth 5.2 have a crucial role. Application from Smart Factory (industrial), Smart Home and Smart Building, as well as partly Smart Grid and Smart City use cases, can benefit from the innovative features of this new standard.

The following applications are considered as enabler of BT5.2:

- Bluetooth 5.2 technology can be incorporated into peripherals as wireless keyboards, mouse, smartphones and headsets
- Car audio systems can enable hands free pairing with mobile devices
- Virtual Reality and Augmented Reality systems
- High-Definition video and audio streaming applications
- Sports and fitness tracking devices and applications
- Healthcare and medical systems
- Home and Industrial automation using Bluetooth 5 (and upper versions)
- Internet of Things wireless sensors for security applications

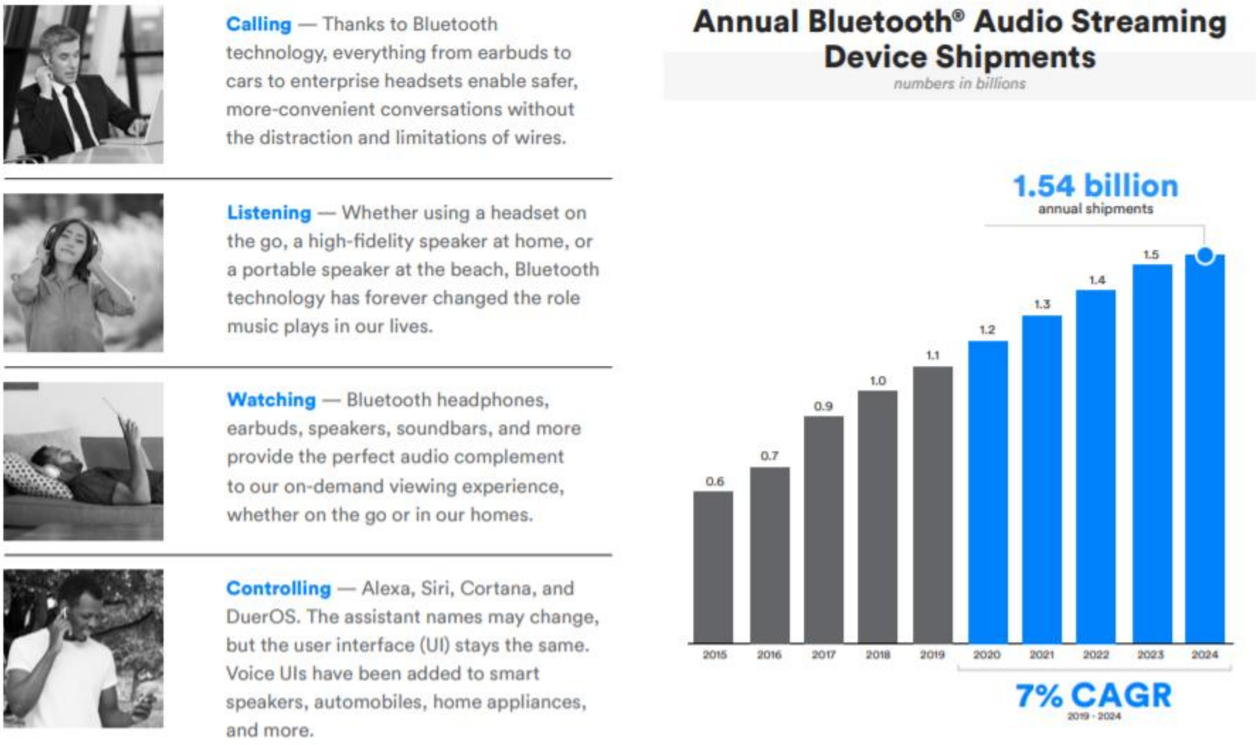
Moreover, Bluetooth technology expanded into low-power data transfer and now it meets the needs of location service and large-scale device network solutions. The following Table 16 summarizes the most important applications for Bluetooth.

Table 16. BT5.2 Applications.

Bluetooth Application	Details
Audio Streaming	Stripping away the hassle of wires, Bluetooth technology revolutionized audio and has forever changed the way we consume media. With the introduction of LE Audio, Bluetooth technology is poised once again to transform the way we experience audio and connect with the world around us.
Data Transfer	From household appliances and fitness trackers to health sensors and medical innovations, Bluetooth technology connects billions of everyday devices and enables the invention of countless more.
Location Services	Bluetooth technology is the developer tool of choice for creating proximity solutions used for point of interest information and item finding as well as positioning systems for asset tracking and wayfinding.
Device Networks	Bluetooth mesh networking is ideally suited for creating control, monitoring, and automation systems where tens, hundreds, or thousands of devices need to communicate with one another reliably and securely.

The following figures shows the main concepts of Bluetooth Applications [51].

Figure 32. Audio Streaming for Bluetooth.



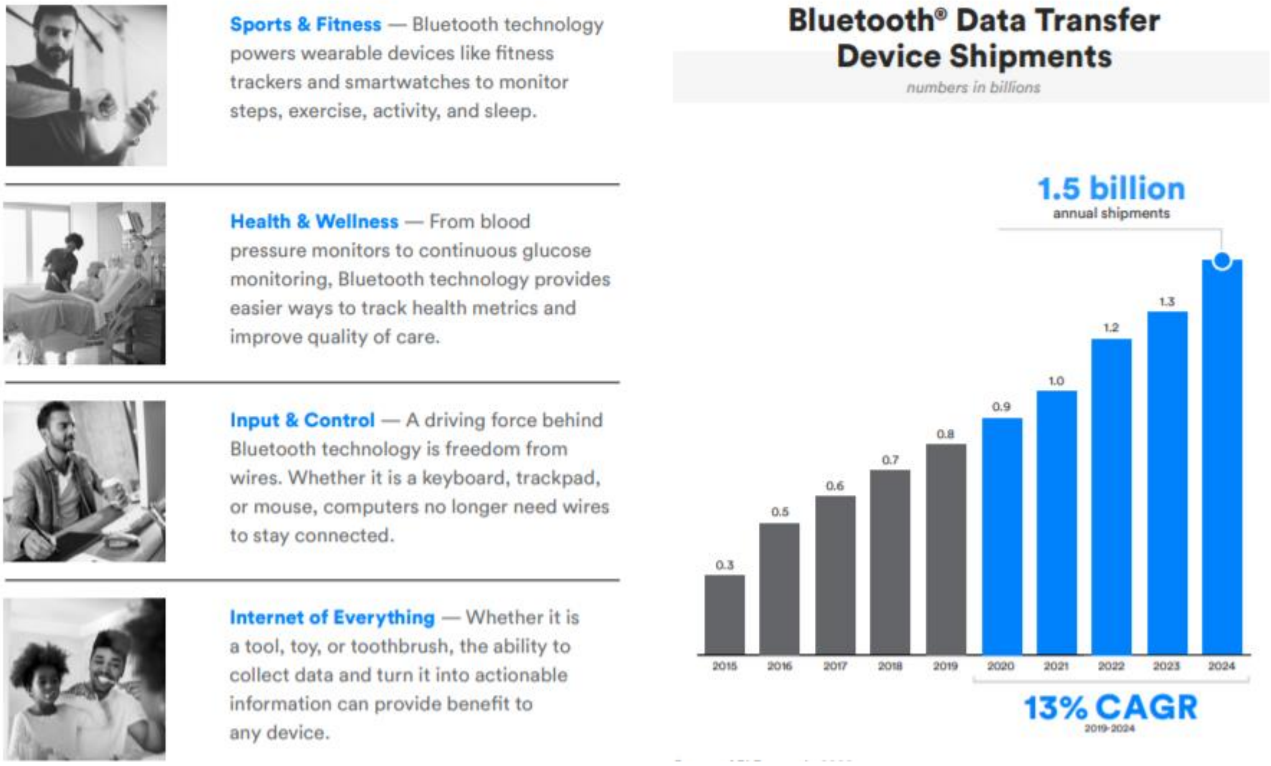
Calling — Thanks to Bluetooth technology, everything from earbuds to cars to enterprise headsets enable safer, more-convenient conversations without the distraction and limitations of wires.

Listening — Whether using a headset on the go, a high-fidelity speaker at home, or a portable speaker at the beach, Bluetooth technology has forever changed the role music plays in our lives.

Watching — Bluetooth headphones, earbuds, speakers, soundbars, and more provide the perfect audio complement to our on-demand viewing experience, whether on the go or in our homes.

Controlling — Alexa, Siri, Cortana, and DuerOS. The assistant names may change, but the user interface (UI) stays the same. Voice UIs have been added to smart speakers, automobiles, home appliances, and more.

Figure 33. Data Transfer.



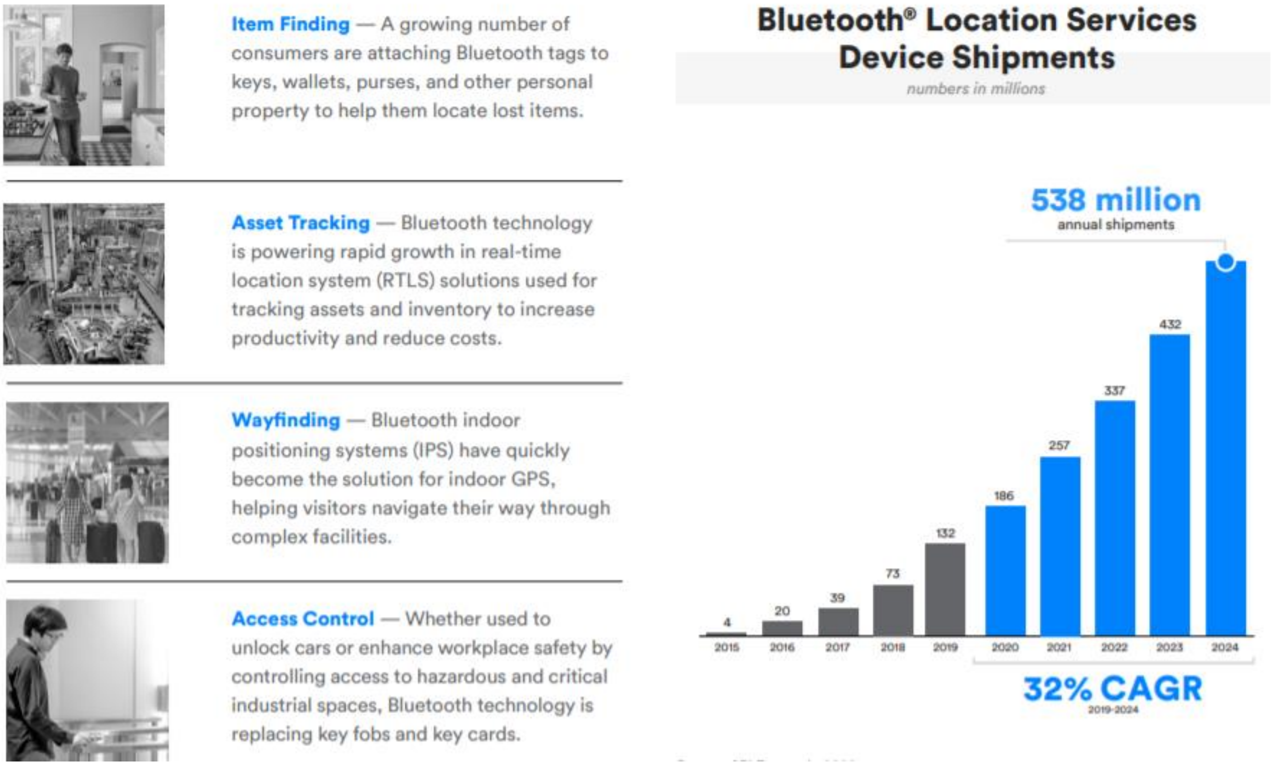
Sports & Fitness — Bluetooth technology powers wearable devices like fitness trackers and smartwatches to monitor steps, exercise, activity, and sleep.

Health & Wellness — From blood pressure monitors to continuous glucose monitoring, Bluetooth technology provides easier ways to track health metrics and improve quality of care.

Input & Control — A driving force behind Bluetooth technology is freedom from wires. Whether it is a keyboard, trackpad, or mouse, computers no longer need wires to stay connected.

Internet of Everything — Whether it is a tool, toy, or toothbrush, the ability to collect data and turn it into actionable information can provide benefit to any device.

Figure 34. Location Services.



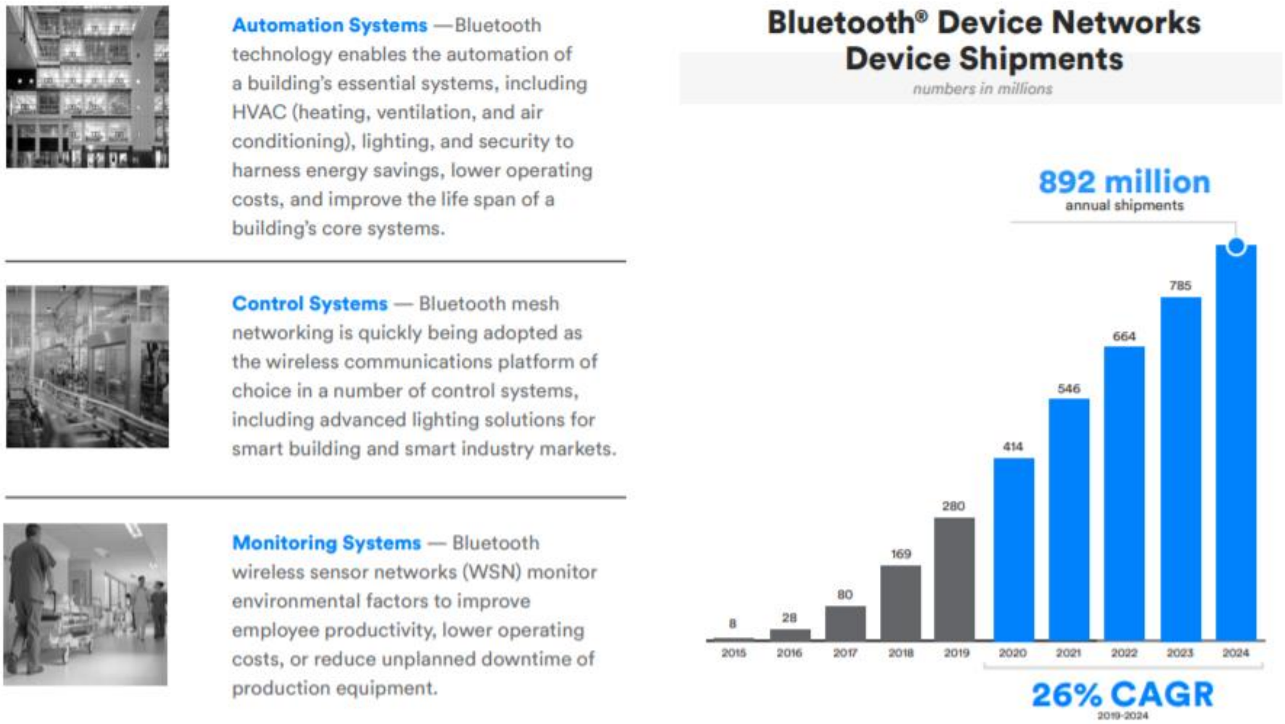
Item Finding — A growing number of consumers are attaching Bluetooth tags to keys, wallets, purses, and other personal property to help them locate lost items.

Asset Tracking — Bluetooth technology is powering rapid growth in real-time location system (RTLS) solutions used for tracking assets and inventory to increase productivity and reduce costs.

Wayfinding — Bluetooth indoor positioning systems (IPS) have quickly become the solution for indoor GPS, helping visitors navigate their way through complex facilities.

Access Control — Whether used to unlock cars or enhance workplace safety by controlling access to hazardous and critical industrial spaces, Bluetooth technology is replacing key fobs and key cards.

Figure 35. Device Networks.



Automation Systems —Bluetooth technology enables the automation of a building's essential systems, including HVAC (heating, ventilation, and air conditioning), lighting, and security to harness energy savings, lower operating costs, and improve the life span of a building's core systems.

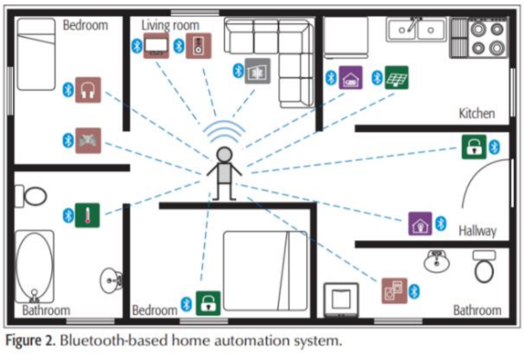
Control Systems — Bluetooth mesh networking is quickly being adopted as the wireless communications platform of choice in a number of control systems, including advanced lighting solutions for smart building and smart industry markets.

Monitoring Systems — Bluetooth wireless sensor networks (WSN) monitor environmental factors to improve employee productivity, lower operating costs, or reduce unplanned downtime of production equipment.

7.3.11 Scenarios and use cases

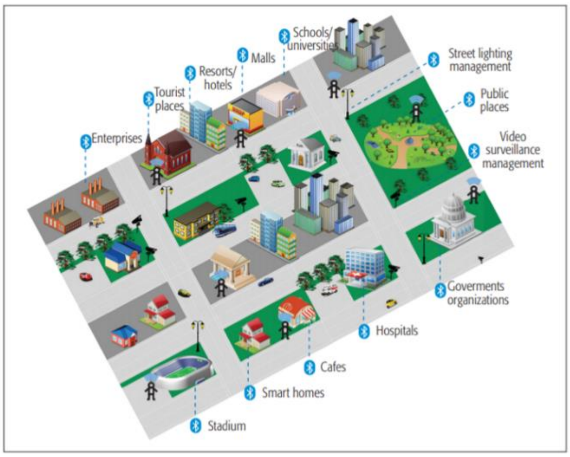
The innovative features of Bluetooth 5.5 in terms of covered range, higher data rate can accelerate its adoption in a IoT ecosystem. We can have a smart home scenario (Figure 36), where Bluetooth audio speakers can be reachable from another room or can be connected to smartphones and smart watches [45].

Figure 36. Bluetooth-based home automation system.



IoT technologies (Figure 37) in a smart city context enable to build up the infrastructure, location-based and automatic services.

Figure 37. BT5.2: enabling the connected smart city [45].



In a smart city environment, we can deploy a mesh network infrastructure (both public and private) based on Bluetooth beacons to exchange data to a centralized gateway, enabling lower-cost solutions. These applications can involve government, businesses, and citizens in a digital environment, e.g., to control street lighting systems, reduce energy loss, deliver data in a broadcast way (location-based information, multimedia or marketing messages) to/from different Bluetooth devices (included self-driving cars, sensors and traffic lights)

7.3.12 Applications for railway

In [52] a first analysis about the BT feasibility for railway control applications is presented. The work analyses main parameters, as Discovery and Association delay, Received Signal Strength

Indicator, the radio range, number of Connected Slave Nodes and wake up time. The Bluetooth 5.2 typical range is around 200 m but it allows no more than 8 connections at the same time.
Although this limitation, the applicability of Bluetooth is analyzed for bidirectional ground-train communication [53]. The experiments were carried out considering:

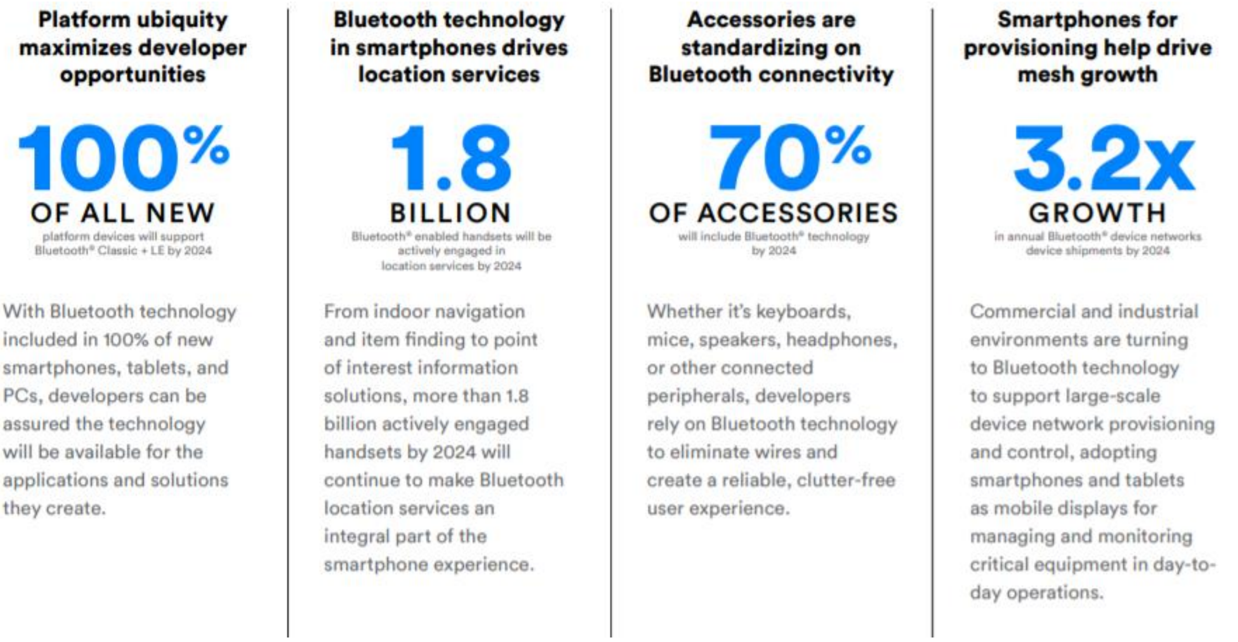
- The connectivity time
- Received Signal Strength Indication (RSSI)
- Throughput of the link established between the devices installed along the railway infrastructure and on-board devices (velocity up to 300 km/h).

The experimental results showed that Bluetooth have worked properly at the high speed (305 km/h) in terms of RSSI value and coverage range.

7.3.13 Market analysis

The Bluetooth 5.2 promises to enlarge its applicability within IoT context. As analyzed in [51], Bluetooth 5.2 can be used in several sector, as shown in the following figures.

Figure 38. BT5.2 and market trends on Phone, Tablet & PC.



Platform ubiquity maximizes developer opportunities

100%

OF ALL NEW

platform devices will support Bluetooth® Classic + LE by 2024

With Bluetooth technology included in 100% of new smartphones, tablets, and PCs, developers can be assured the technology will be available for the applications and solutions they create.

Bluetooth technology in smartphones drives location services

1.8

BILLION

Bluetooth® enabled handsets will be actively engaged in location services by 2024

From indoor navigation and item finding to point of interest information solutions, more than 1.8 billion actively engaged handsets by 2024 will continue to make Bluetooth location services an integral part of the smartphone experience.

Accessories are standardizing on Bluetooth connectivity

70%

OF ACCESSORIES

will include Bluetooth® technology by 2024

Whether it's keyboards, mice, speakers, headphones, or other connected peripherals, developers rely on Bluetooth technology to eliminate wires and create a reliable, clutter-free user experience.

Smartphones for provisioning help drive mesh growth

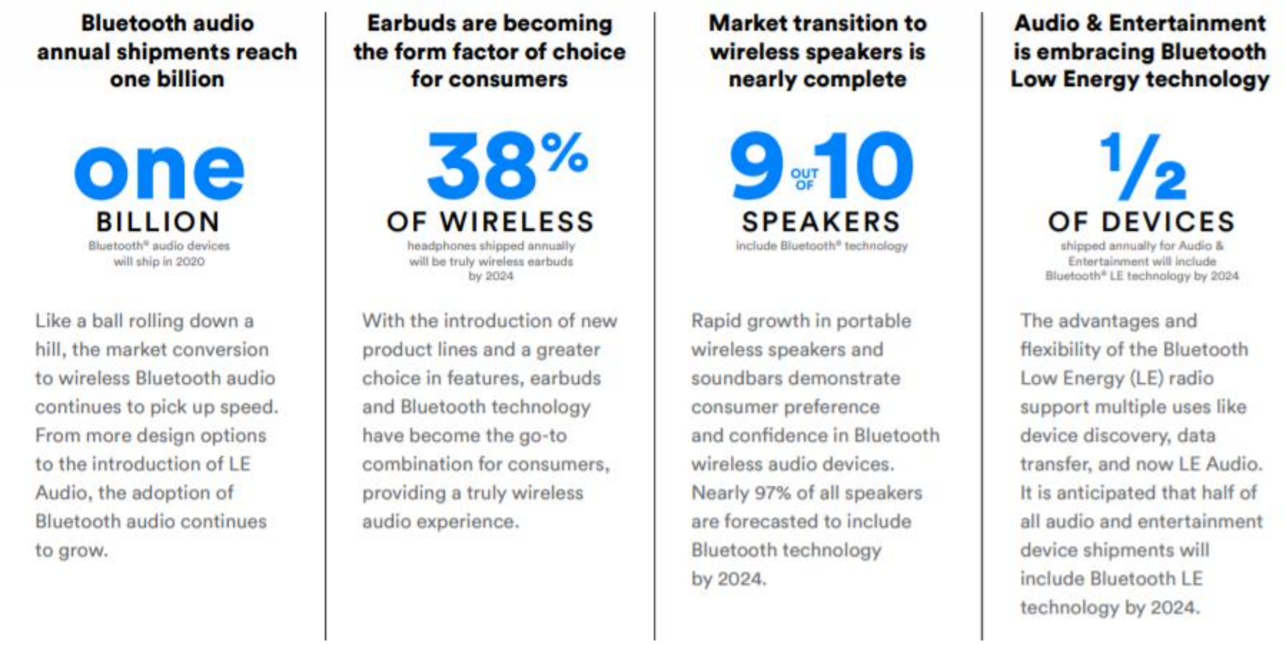
3.2x

GROWTH

in annual Bluetooth® device networks device shipments by 2024

Commercial and industrial environments are turning to Bluetooth technology to support large-scale device network provisioning and control, adopting smartphones and tablets as mobile displays for managing and monitoring critical equipment in day-to-day operations.

Figure 39. BT5.2 and market trends on Audio & Entertainment.



Bluetooth audio annual shipments reach one billion

one BILLION

Bluetooth® audio devices will ship in 2020

Like a ball rolling down a hill, the market conversion to wireless Bluetooth audio continues to pick up speed. From more design options to the introduction of LE Audio, the adoption of Bluetooth audio continues to grow.

Earbuds are becoming the form factor of choice for consumers

38% OF WIRELESS

headphones shipped annually will be truly wireless earbuds by 2024

With the introduction of new product lines and a greater choice in features, earbuds and Bluetooth technology have become the go-to combination for consumers, providing a truly wireless audio experience.

Market transition to wireless speakers is nearly complete

9 OUT OF 10 SPEAKERS

include Bluetooth® technology

Rapid growth in portable wireless speakers and soundbars demonstrate consumer preference and confidence in Bluetooth wireless audio devices. Nearly 97% of all speakers are forecasted to include Bluetooth technology by 2024.

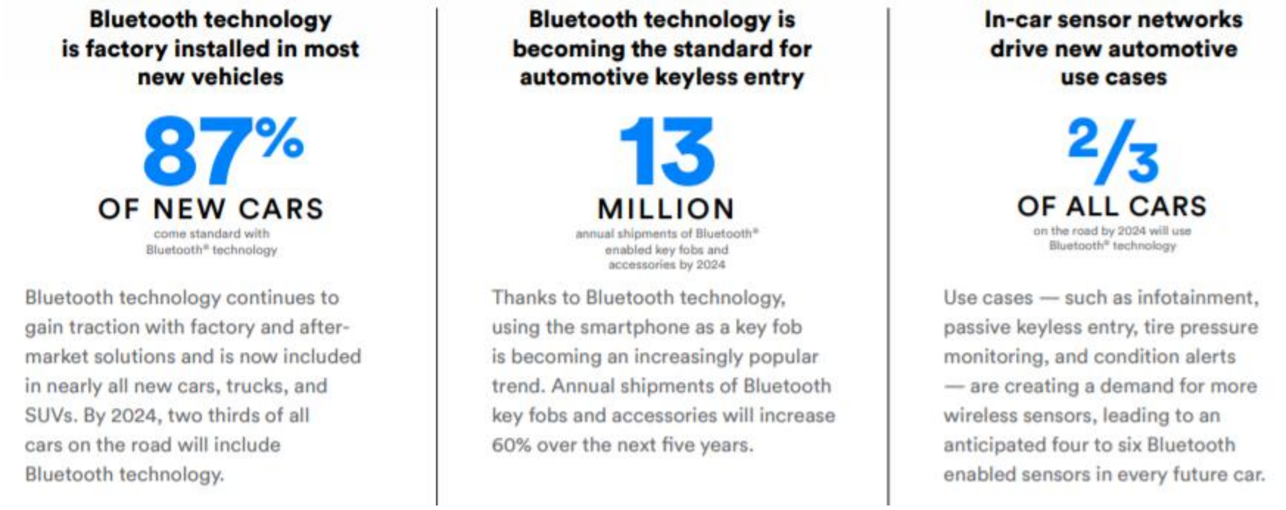
Audio & Entertainment is embracing Bluetooth Low Energy technology

½ OF DEVICES

shipped annually for Audio & Entertainment will include Bluetooth® LE technology by 2024

The advantages and flexibility of the Bluetooth Low Energy (LE) radio support multiple uses like device discovery, data transfer, and now LE Audio. It is anticipated that half of all audio and entertainment device shipments will include Bluetooth LE technology by 2024.

Figure 40. BT5.2 and market trends on Automotive.



Bluetooth technology is factory installed in most new vehicles

87% OF NEW CARS

come standard with Bluetooth® technology

Bluetooth technology continues to gain traction with factory and after-market solutions and is now included in nearly all new cars, trucks, and SUVs. By 2024, two thirds of all cars on the road will include Bluetooth technology.

Bluetooth technology is becoming the standard for automotive keyless entry

13 MILLION

annual shipments of Bluetooth® enabled key fobs and accessories by 2024

Thanks to Bluetooth technology, using the smartphone as a key fob is becoming an increasingly popular trend. Annual shipments of Bluetooth key fobs and accessories will increase 60% over the next five years.

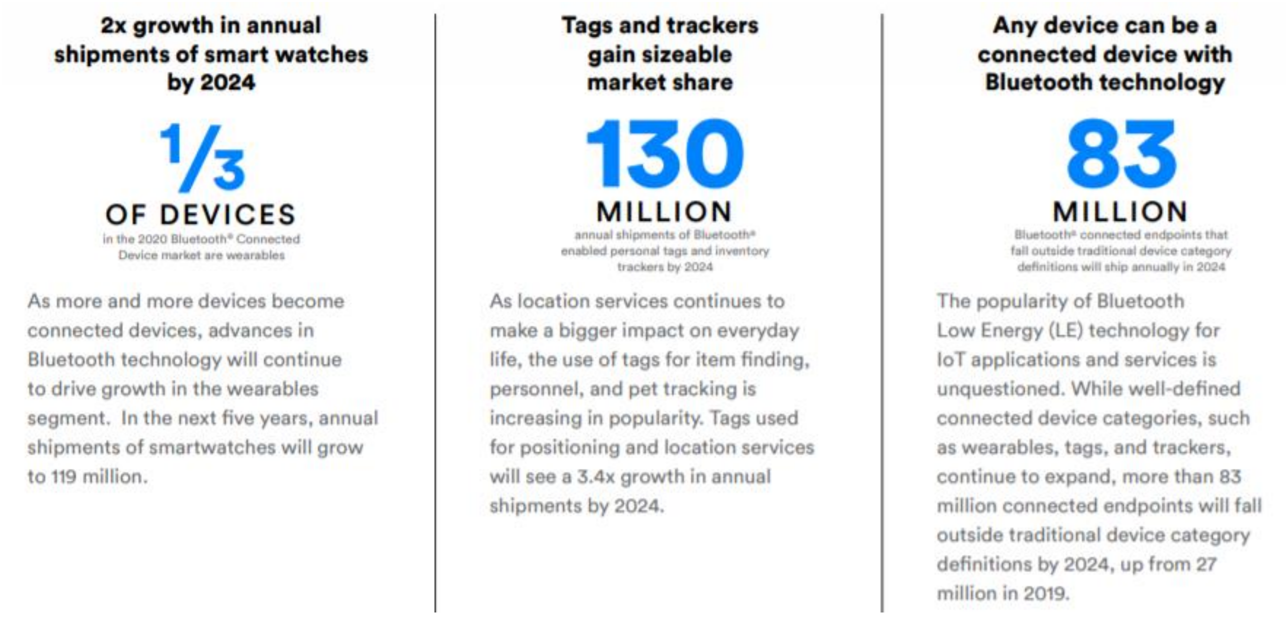
In-car sensor networks drive new automotive use cases

2/3 OF ALL CARS

on the road by 2024 will use Bluetooth® technology

Use cases — such as infotainment, passive keyless entry, tire pressure monitoring, and condition alerts — are creating a demand for more wireless sensors, leading to an anticipated four to six Bluetooth enabled sensors in every future car.

Figure 41. BT5.2 and market trends on Connected Devices.



2x growth in annual shipments of smart watches by 2024

1/3 OF DEVICES

in the 2020 Bluetooth® Connected Device market are wearables

As more and more devices become connected devices, advances in Bluetooth technology will continue to drive growth in the wearables segment. In the next five years, annual shipments of smartwatches will grow to 119 million.

Tags and trackers gain sizeable market share

130 MILLION

annual shipments of Bluetooth® enabled personal tags and inventory trackers by 2024

As location services continues to make a bigger impact on everyday life, the use of tags for item finding, personnel, and pet tracking is increasing in popularity. Tags used for positioning and location services will see a 3.4x growth in annual shipments by 2024.

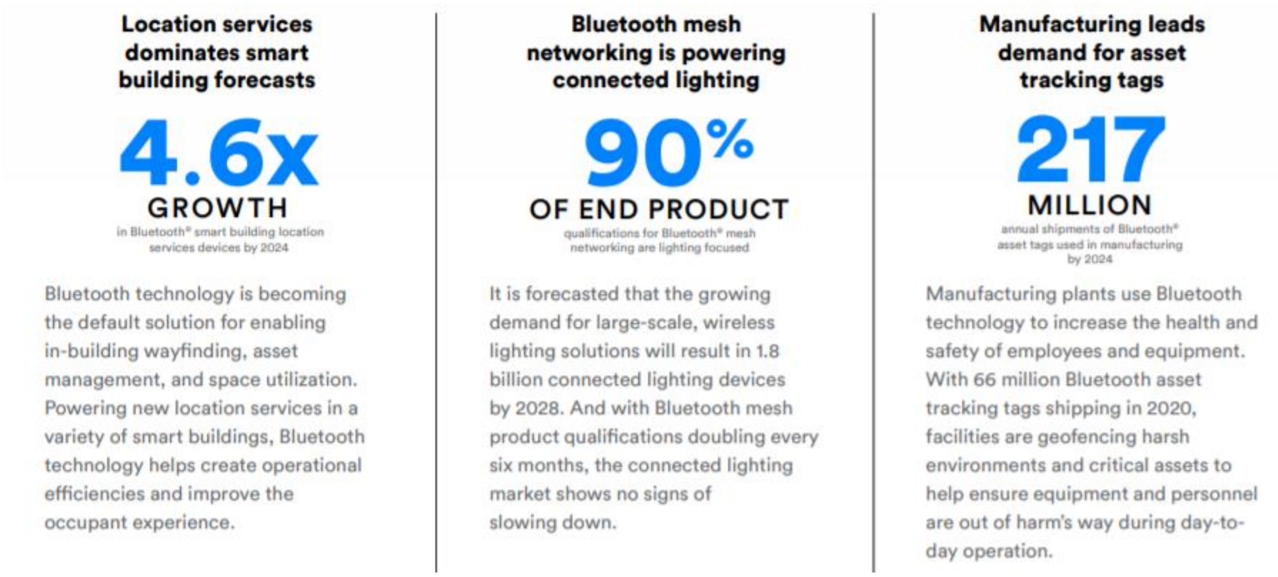
Any device can be a connected device with Bluetooth technology

83 MILLION

Bluetooth® connected endpoints that fall outside traditional device category definitions will ship annually in 2024

The popularity of Bluetooth Low Energy (LE) technology for IoT applications and services is unquestioned. While well-defined connected device categories, such as wearables, tags, and trackers, continue to expand, more than 83 million connected endpoints will fall outside traditional device category definitions by 2024, up from 27 million in 2019.

Figure 42. BT5.2 and market trends on Smart Building.



Location services dominates smart building forecasts

4.6x GROWTH

in Bluetooth® smart building location services devices by 2024

Bluetooth technology is becoming the default solution for enabling in-building wayfinding, asset management, and space utilization. Powering new location services in a variety of smart buildings, Bluetooth technology helps create operational efficiencies and improve the occupant experience.

Bluetooth mesh networking is powering connected lighting

90% OF END PRODUCT

qualifications for Bluetooth® mesh networking are lighting focused

It is forecasted that the growing demand for large-scale, wireless lighting solutions will result in 1.8 billion connected lighting devices by 2028. And with Bluetooth mesh product qualifications doubling every six months, the connected lighting market shows no signs of slowing down.

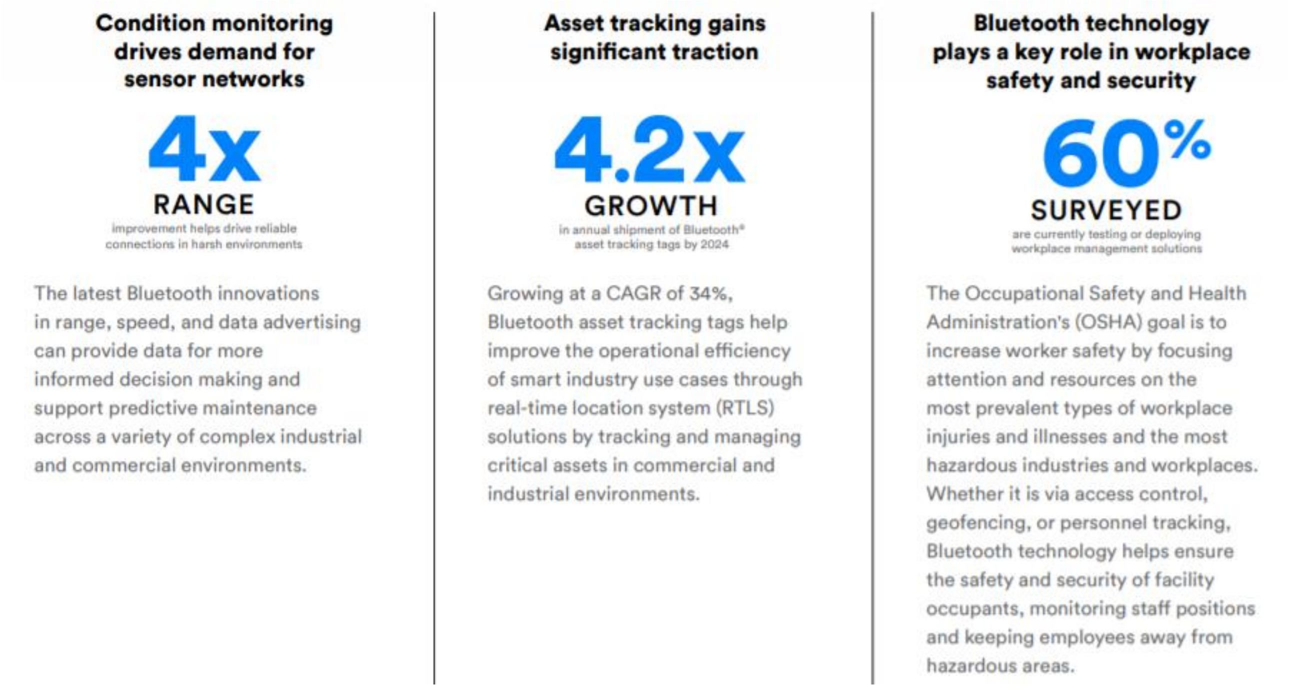
Manufacturing leads demand for asset tracking tags

217 MILLION

annual shipments of Bluetooth® asset tags used in manufacturing by 2024

Manufacturing plants use Bluetooth technology to increase the health and safety of employees and equipment. With 66 million Bluetooth asset tracking tags shipping in 2020, facilities are geofencing harsh environments and critical assets to help ensure equipment and personnel are out of harm's way during day-to-day operation.

Figure 43. BT5.2 and market trends on Smart Industry.



Condition monitoring drives demand for sensor networks

4x RANGE

improvement helps drive reliable connections in harsh environments

The latest Bluetooth innovations in range, speed, and data advertising can provide data for more informed decision making and support predictive maintenance across a variety of complex industrial and commercial environments.

Asset tracking gains significant traction

4.2x GROWTH

in annual shipment of Bluetooth® asset tracking tags by 2024

Growing at a CAGR of 34%, Bluetooth asset tracking tags help improve the operational efficiency of smart industry use cases through real-time location system (RTLS) solutions by tracking and managing critical assets in commercial and industrial environments.

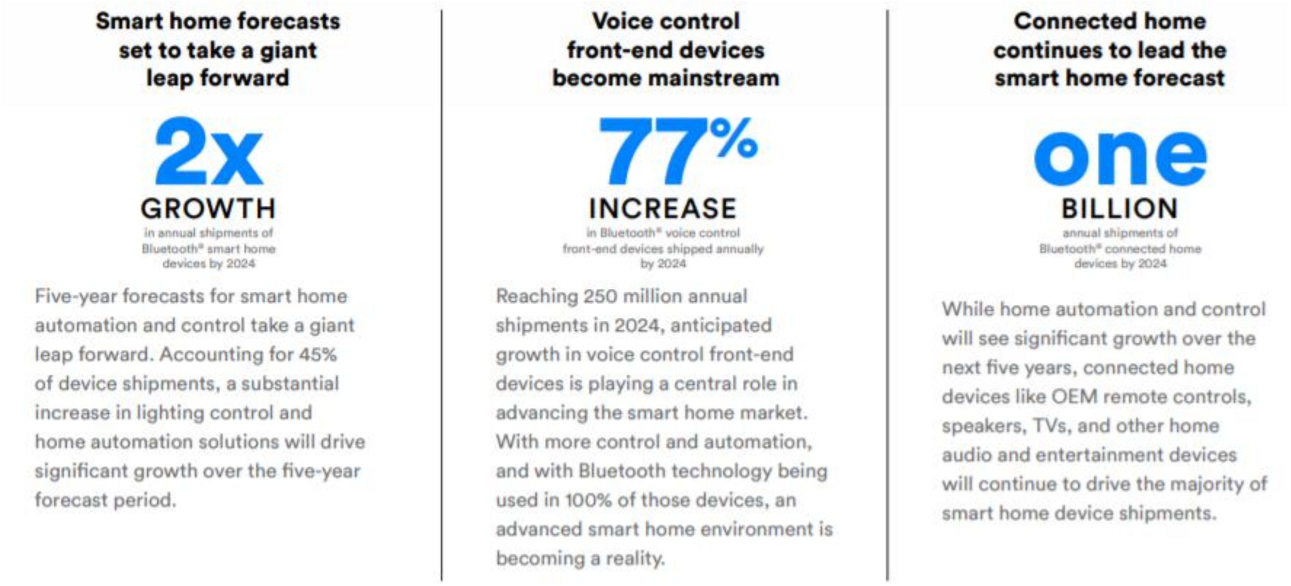
Bluetooth technology plays a key role in workplace safety and security

60% SURVEYED

are currently testing or deploying workplace management solutions

The Occupational Safety and Health Administration's (OSHA) goal is to increase worker safety by focusing attention and resources on the most prevalent types of workplace injuries and illnesses and the most hazardous industries and workplaces. Whether it is via access control, geofencing, or personnel tracking, Bluetooth technology helps ensure the safety and security of facility occupants, monitoring staff positions and keeping employees away from hazardous areas.

Figure 44. BT5.2 and market trends on Smart Home.



Smart home forecasts set to take a giant leap forward

2x GROWTH

in annual shipments of Bluetooth® smart home devices by 2024

Five-year forecasts for smart home automation and control take a giant leap forward. Accounting for 45% of device shipments, a substantial increase in lighting control and home automation solutions will drive significant growth over the five-year forecast period.

Voice control front-end devices become mainstream

77% INCREASE

in Bluetooth® voice control front-end devices shipped annually by 2024

Reaching 250 million annual shipments in 2024, anticipated growth in voice control front-end devices is playing a central role in advancing the smart home market. With more control and automation, and with Bluetooth technology being used in 100% of those devices, an advanced smart home environment is becoming a reality.

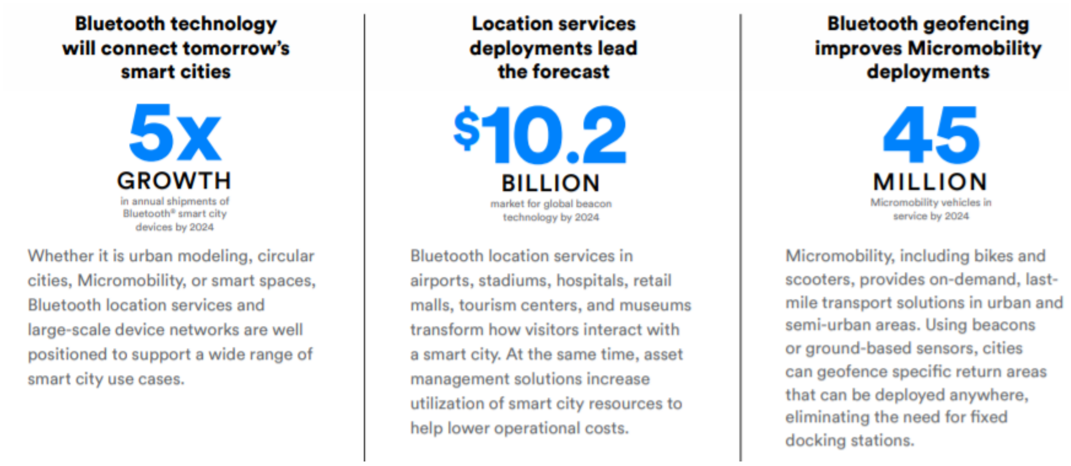
Connected home continues to lead the smart home forecast

one BILLION

annual shipments of Bluetooth® connected home devices by 2024

While home automation and control will see significant growth over the next five years, connected home devices like OEM remote controls, speakers, TVs, and other home audio and entertainment devices will continue to drive the majority of smart home device shipments.

Figure 45. BT5.2 and market trends on Smart City.



Bluetooth technology will connect tomorrow's smart cities

5x GROWTH

in annual shipments of Bluetooth® smart city devices by 2024

Whether it is urban modeling, circular cities, Micromobility, or smart spaces, Bluetooth location services and large-scale device networks are well positioned to support a wide range of smart city use cases.

Location services deployments lead the forecast

$10.2 BILLION

market for global beacon technology by 2024

Bluetooth location services in airports, stadiums, hospitals, retail malls, tourism centers, and museums transform how visitors interact with a smart city. At the same time, asset management solutions increase utilization of smart city resources to help lower operational costs.

Bluetooth geofencing improves Micromobility deployments

45 MILLION

Micromobility vehicles in service by 2024

Micromobility, including bikes and scooters, provides on-demand, last-mile transport solutions in urban and semi-urban areas. Using beacons or ground-based sensors, cities can geofence specific return areas that can be deployed anywhere, eliminating the need for fixed docking stations.

7.3.14 Final remarks

Advantages of Bluetooth 5.2 Technology

Some of the advantages of BT5.2 are listed below:

- Multiple devices can communicate among them in an easier way
- Bluetooth 5.2 can be useful in different sectors as Automotive, Home Automation, Consumer Electronics, Medical and Health, Mobile phones and Smartphones, Sports and Fitness, PC & peripherals etc.
- The data rate is 8 times larger than the previous releases
- It better manages the interferences with other wireless technologies

Disadvantages of Bluetooth 5.2 Technology

The disadvantages of BT5.2 are listed below:

- When it is enabled, it slowly consumes energy since it performs a continuous signal scan and search for other devices in the same area
- Its security is weaker than Wi-Fi and other wireless data standards.
- Bluetooth can manage a maximum of 8 different connections

7.3.15 Applicability of BT5.2 to rail environment

From a rail environment point of view, the BT5.2 can be used for many important applications. It is characterized by a better robustness for interference management with other wireless technologies. It is very useful in proximity areas when the trains are moving with a low speed or are in a stationary position (e.g., station or a rail smart environment) and several communication equipment are present in the same area. The possibility to guarantee a good robustness to interference together considerable coverage areas (up to 200 m), makes the BT5.2 an interesting communication technology for rail applications. From a capacity point of view, the BT5.2 can provide an efficient wireless data transfer (up to 2 MBps) very useful in case of a local data exchange. The involvement up to n. 8 BT5.2 devices in a mesh network configuration is also suitable for an efficient data collection in a rail environment, e.g. the monitoring of the status of train (or vehicle) and infrastructure, together with the derailment detection, data gathering in freight trains and other location services. Finally, the support for an efficient security approach and support for high-speed trains (from a pairing setup time) should be deeply analyzed, in order to enhance the practical applicability of BT5.2 to the rail environment.

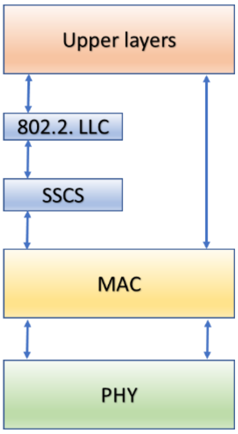
8. ZigBee

The Zigbee is one of the most important communication protocols used for Personal Area Network (PAN) systems. It is based on IEEE 802.15.4 standard for lower layers.

8.1 The IEEE 802.15.4 standard

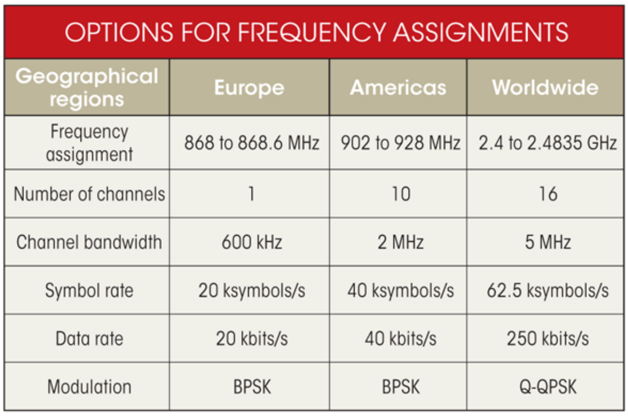
The 802.15.4 standard defines the PHY and MAC layers, on top of which adds the logical link control (LLC) and service specific convergence sub-layer (SSCS) to communicate with the layer 3 and above [134].

Figure 46. IEEE 802.15.4 protocol stack [134].



The goal of 802.15.4 standard is to provide the basis for other protocols to be added at layer 3 and above. The 2.4-GHz frequency band is the most used.

Table 17. Zigbee radio frequencies.



OPTIONS FOR FREQUENCY ASSIGNMENTS

Geographical regions	Europe	Americas	Worldwide
Frequency assignment	868 to 868.6 MHz	902 to 928 MHz	2.4 to 2.4835 GHz
Number of channels	1	10	16
Channel bandwidth	600 kHz	2 MHz	5 MHz
Symbol rate	20 ksymbols/s	40 ksymbols/s	62.5 ksymbols/s
Data rate	20 kbits/s	40 kbits/s	250 kbits/s
Modulation	BPSK	BPSK	Q-QPSK

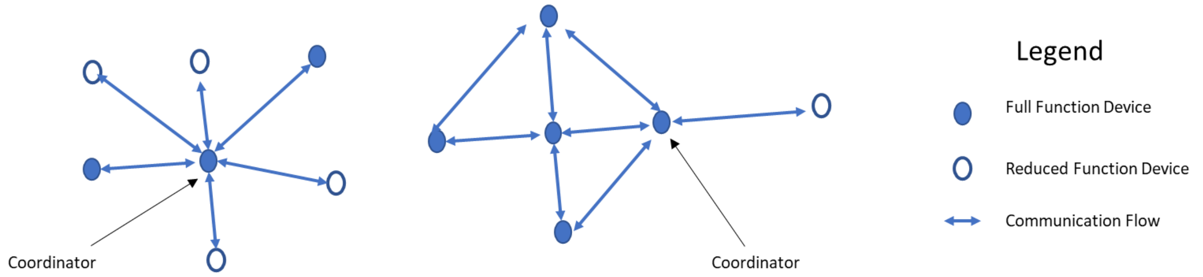
The standard uses Direct Sequence Spread Spectrum (DSSS) modulation. It provides a strong management of noise and interference management. Binary Phase-Shift Keying (BPSK) modulation is used in the two lower speed versions, while Offset-Quadrature Phase-Shift Keying (O-QPSK) is used for the higher speed versions.

Regarding channel access, 802.15.4 uses Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA). It enables the access to same channel by multiple nodes at different times avoiding

the interference. Short packets are used with a very low duty cycle (<1 %). It reduces the power consumption. The minimum power level is – 3 dBm or 0.5 mW. Most modules use 0 dBm or 1 mW. The coverage range depend on the specific path and conditions, in particular if we are in a Line of Sight (LOS) condition. Under the best conditions the range can be around 1000 meters with a free outdoor path, but many applications cover a shorter range from 10 to 75 meters.
With regard to network scheme, 802.15.4 defines two topologies, as shown in Figure 47 [134]:

a) Star topology: all nodes must communicate with the central coordinator node.
b) Peer-to-peer (P2P) topology: each device may can communicate with the other ones. It can evolve in a mesh topology.

Figure 47. IEEE 802.15.4 network topology: (a) star (b) peer-to-peer [134].



8.2 Zigbee protocol

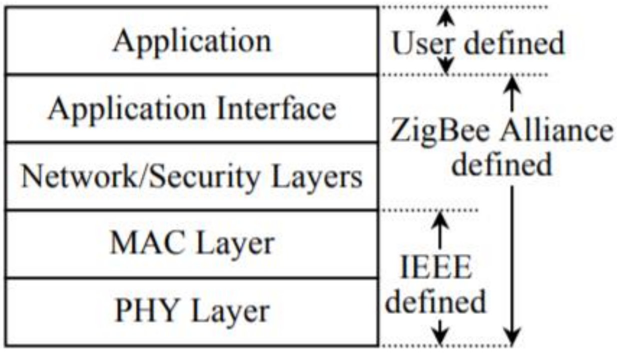
8.2.1 Standard

Zigbee, standard from the ZigBee Alliance, benefits from the IEEE 802.15.4 physical radio standard (PHY and MAC layers) and the possibility to use unlicensed bands at 2.4GHz (global), 915Mhz (Americas) and 868Mhz (Europe). Zigbee can provide data rate of 250Kbs at 2.4GHz (16 channels), 10kbs at 915 – 921Mhz (27 channels) and 100kbs at 868Mhz (63 channel). Transmission distances can vary from 10 to 100 meters: they depend on transmission power and environmental conditions (e.g., LoS). Sub GHz channels transmission can reach 1 km [54]. ZigBee defines layer 3 and above layers on top on PHY and MAC layer already standardized by 802.15.4.

8.2.2 Architecture

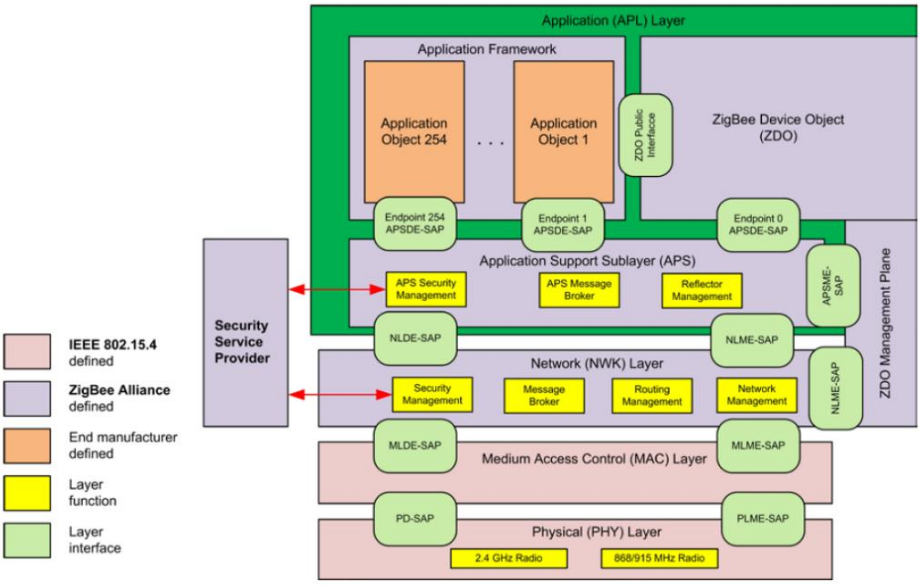
The ZigBee stack architecture is formed by different layers. Each layer performs a specific set of services in favor of the layer above. A data entity enables a data transmission service, and each service entity uses an interface through a service access point (SAP). Each SAP supports a set of several service primitives to perform a specific functionality.
The IEEE 802.15.4 standard defines the two lower layers: the physical (PHY) layer and the medium access control (MAC) sub-layer (Figure 48) [56]. The ZigBee Alliance builds on this foundation by providing the network (NWK) layer and the framework for the application layer. The application layer framework consists of the application support sub-layer (APS) and the ZigBee device objects (ZDO).

Figure 48. IEEE 802.15.4 and Zigbee protocol relationship.



The Zigbee architecture is shown in Figure 49 [54].

Figure 49. The Zigbee architecture.

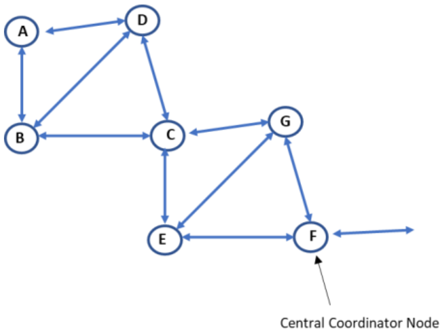


1. **Physical layer**: it performs the modulation/demodulation of transmitted/received signals, respectively. It can use different frequencies, data rates, and channels. The PHY layer uses two frequency bands (868 in Europe, 915 MHz in USA/Australia and 2.4 GHz worldwide)
2. **MAC Layer**: it controls access to the radio channel using a CSMA-CA mechanism. It also performs the beacon message transmission and synchronization
3. **Network Layer**: it performs network actions, as manage the connection/disconnection at network level (e.g. among router and other devices) and routing
4. **Application support sublayer:** it enables Zigbee to support different object applications by other devices. The communication is at network level
5. **Application framework:** it sends two types of information, as key esteem and non-specific message administrations. Nonspecific message is a developer characterized structure, while the key esteem match is utilized for getting properties inside the application objects. ZDO gives an interface between application items and APS layer in ZigBee devices

8.2.3 Network Topology

The NWK supports star, tree, and mesh topologies. In a star topology, the network is controlled by one single device called the ZigBee coordinator, responsible for initiating and maintaining the devices on the network. All other devices can communicate among them passing through the ZigBee coordinator. In tree networks, the nodes are deployed according to a hierarchy. Finally, the mesh networks allow full peer-to-peer communication: the ZigBee coordinator is responsible for starting the network and for choosing certain key network parameters. In a mesh topology, all nodes are self-configuring and self-healing and can also communicate among them through multiple relay nodes (Figure 50).

Figure 50. The Zigbee mesh network topology.



8.2.4 Security

ZigBee protocol provides security services as encryption, data integrity and authentication [57], based on AES-128 encryption scheme.
There are some features in security of ZigBee technology as following [58]:

1. ZigBee provides data integrity check. Thanks to message integrity codes (MIC), it can prevent the data modification.
2. ZigBee supports the identity authentication service based on public-key cryptography
3. ZigBee encryption adopts AES algorithm as encryption scheme
4. In a ZigBee network a Trust Center is present [59]. It can decide if admit new devices, informing all reached devices through with the primal encrypted network key
5. ZigBee technology gives three keys: Master, Network and Link. Master key is the basic key among communicating of nodes. It may be installed during manufacturing devices or may added manually. Thanks to the encrypting link key, the network key can be obtained. Network encryption uses a network key for all devices in the network.

Security attacks

ZigBee nodes can be invalidated, destroyed, or captured [57] [60]. The attackers intend to disturb the communication between the nodes trying to add malicious nodes or deliver false messages. The most important attacks are Sinkholes, Sybil, and Wormholes. The features about data integrity and authentication are effective countermeasures.

8.2.5 Applications

Some of applications supported by Zigbee include:

- Building automation for commercial monitoring and control of facilities
- Remote control (RF4CE or RF for consumer electronics)
- Smart energy for home energy monitoring
- Health care for medical and fitness monitoring
- Home automation for control of smart homes
- Input devices for keyboards, mice, touch pads, wands, etc.
- Light Link for control of LED lighting
- Retail services for shopping related uses
- Telecom services
- Network services related to large mesh networks

In particular, the following applications gained a particular interest [61]:

- Combining ZigBee and GPRS for wireless data transmission Using GPRS wired network transmission based on Zigbee
- Medical Monitoring System
- Wireless Ordering System (e.g., restaurant and bar)
- Intelligent Traffic Control System (e.g. traffic light)

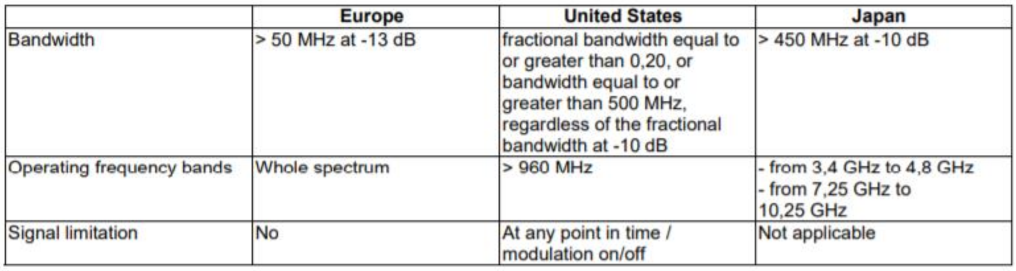
9. Ultra-wide Band (UWB)

9.1 UWB System Architecture

Introduction to UWB

Ultra-wide Band (UWB), is a wireless communication technology referred to a signal characterized by a fractional bandwidth equal to or greater than 0.20 with respect to its central transmitting frequency or 500 MHz. UWB technology can transmit very short and low power electro-magnetic signals. The UWB signal is characterized by short pulse RF wave and large bandwidth, high time resolution and high immunity to multipath.
In Table 18, spectrum requirements for UWB radio in Europe, United States and Japan are shown [62].

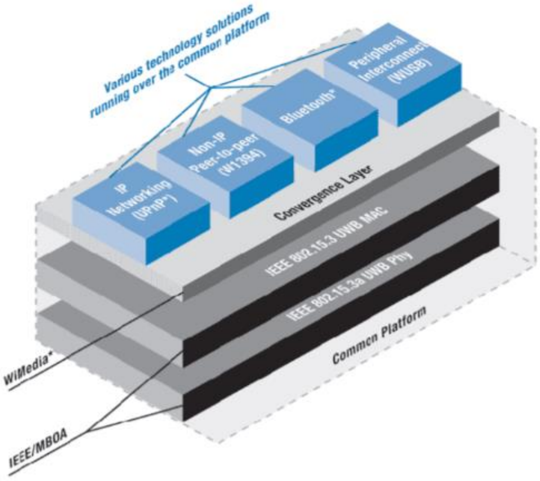
Table 18. UWB radio frequencies.



	Europe	United States	Japan
Bandwidth	> 50 MHz at -13 dB	fractional bandwidth equal to or greater than 0,20, or bandwidth equal to or greater than 500 MHz, regardless of the fractional bandwidth at -10 dB	> 450 MHz at -10 dB
Operating frequency bands	Whole spectrum	> 960 MHz	- from 3,4 GHz to 4,8 GHz - from 7,25 GHz to 10,25 GHz
Signal limitation	No	At any point in time / modulation on/off	Not applicable

The UWB protocol is based on 802.15.3a standard [63], which provides the Physical and MAC level to UWB protocol.

Figure 51. IEEE 802.15.3a and UWB relationship.



A UWB signal can be modelled as a series of low power derivative-of-Gaussian pulses. The time interval is very brief (from 10 to 1,000 ps) and shorter than a single bit. The frequency spectrum can be around several gigahertz. UWB technology is also called "zero carrier" radio since it can manage the antenna using a baseband signal.

Modulation schemes

The modulation schemes adopted by UWB protocol are:

- Pulse Amplitude Modulation (PAM): the symbol is characterized by pulse length

- On-Off keying (OOK): the symbol is characterized by the presence of pulse
- Pulse Position Modulation (PPM): the symbol is characterized by different delays (ps)

Types of UWB Transmission

The UWB transmissions can be Impulse Radio (IR-UWB) and Multi-band UWB. The IR-UWB technique uses extremely short pulses (with a duration of ns), because they have very large bandwidth (a few GHz). The Multi-band UWB technique uses sub-bands (e.g., 500 MHz) to transmit information in a concurrent way.

9.2 UWB Features and challenges

9.2.1 Features

UWB data rates can overcome 100 Mbit/s, using a few transmission powers and producing a irrelevant interference. Other important benefits of UWB are:

a) **High Data Rate**: UWB can manage a large type of applications (as streaming video) with data rate much higher than 802.11 or Bluetooth
b) **Low Power Consumption**: UWB transmits short impulses constantly with a power around -41.3 dBm
c) **Interference Immunity**: Due to low power and high frequency transmission, UWB can reduce signal amplitude fluctuations
d) **Low Probability of interception and detection**: thanks to low transmission power, UWB is more robust to detection and intercept
e) **Reasonable Range**: UWB can overcome the 10 mt, as minimum range at speed 100Mbps defined by IEEE 802.15.3a Study Group
f) **Low Complexity, Low cost**: Since UWB do not use modulated signal, the transceiver structure is very simple and low cost
g) **Large Channel Capacity**: thanks to bandwidth around several GHz, UWB can provide high data rate transmissions
h) **Accurate delay estimation**: thanks to high frequency pulses, UWB can provide position accuracy (a few centimeters)
i) **Flexibility**: it can manage difference data rate based on coverage range

9.2.2 Challenges

The main challenges offered by the UWB standard are:

a) **Pulse-Shape Distortion:** UWB pulses are more difficult to manage with respect to narrowband signals. In fact, while narrowband signals can remain sinusoidal within the transmission channel, UWB signals can be distorted during the transmission
b) **Channel Estimation**: Although UWB receivers can correlate the received signal with target signal, they need to predict the channel radio condition
c) **High Frequency Synchronization**: Time synchronization is a crucial issue for UWB signals due to the necessity to perform the sampling and synchronization of very short pulses (around ns)
d) **Multiple-Access Interference**: the presence of interference from other devices is an important limitation to channel capacity and the performance of UWB receivers

9.3 UWB applications

The main application areas enabled by UWB standard are:

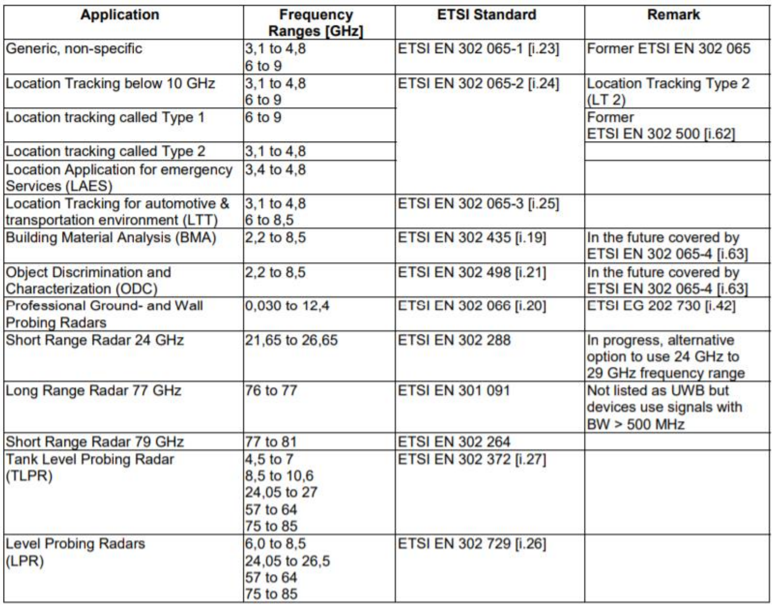
a) Communications
- Wireless Audio, Data & Video Distribution
- RF Tagging & Identification
- High Speed WLANs, Mobile Ad-Hoc wireless networks, Ground wave Communications, Handheld and Network Radios, Intra-home and Intra-office communication

b) Radar
- Collision/Obstacle Avoidance
- Precision Altimetry
- Intrusion Detection
- Ground Penetrating Radar

c) Precision Geolocation
- Asset Tracking: Precision Geolocation Systems and high-resolution imaging. Indoor and outdoor tracking down to less than a centimetre, emergency services, inventory tracking, and asset safety and security. Personnel identification, lost children, prisoner tracking, inventory tracking, tagging and identification, asset management.
- Personnel localization
- Collision Detection (e.g., automotive)
- Home Entertainment, Computing, Mobile Devices, Automotive, Content Transfer, Low power and high data rate use, content streaming.

The European Telecommunications Standards Institute (ETSI) in TR 103 181-1 V1.1.1 (2015-07) categorized the main UWB applications, as shown in Table 19.

Table 19. Overview UWB application in CEPT/ECC, EC and ETSI.



Application	Frequency Ranges [GHz]	ETSI Standard	Remark
Generic, non-specific	3,1 to 4,8 6 to 9	ETSI EN 302 065-1 [i.23]	Former ETSI EN 302 065
Location Tracking below 10 GHz	3,1 to 4,8 6 to 9	ETSI EN 302 065-2 [i.24]	Location Tracking Type 2 (LT 2)
Location tracking called Type 1	6 to 9		Former ETSI EN 302 500 [i.62]
Location tracking called Type 2	3,1 to 4,8		
Location Application for emergency Services (LAES)	3,4 to 4,8		
Location Tracking for automotive & transportation environment (LTT)	3,1 to 4,8 6 to 8,5	ETSI EN 302 065-3 [i.25]	
Building Material Analysis (BMA)	2,2 to 8,5	ETSI EN 302 435 [i.19]	In the future covered by ETSI EN 302 065-4 [i.63]
Object Discrimination and Characterization (ODC)	2,2 to 8,5	ETSI EN 302 498 [i.21]	In the future covered by ETSI EN 302 065-4 [i.63]
Professional Ground- and Wall Probing Radars	0,030 to 12,4	ETSI EN 302 066 [i.20]	ETSI EG 202 730 [i.42]
Short Range Radar 24 GHz	21,65 to 26,65	ETSI EN 302 288	In progress, alternative option to use 24 GHz to 29 GHz frequency range
Long Range Radar 77 GHz	76 to 77	ETSI EN 301 091	Not listed as UWB but devices use signals with BW > 500 MHz
Short Range Radar 79 GHz	77 to 81	ETSI EN 302 264	
Tank Level Probing Radar (TLPR)	4,5 to 7 8,5 to 10,6 24,05 to 27 57 to 64 75 to 85	ETSI EN 302 372 [i.27]	
Level Probing Radars (LPR)	6,0 to 8,5 24,05 to 26,5 57 to 64 75 to 85	ETSI EN 302 729 [i.26]	

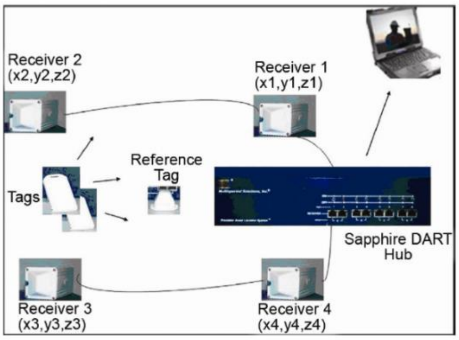
9.4 UWB Localization application

With three or more UWB receivers a 2D localization can be provided, while a fine 3D localization requires four or more UWB receivers a [64]. Figure 52 shows an UWB system formed by:

1. processing computer equipped by Graphical User Interface (GUI) and a central hub
2. four UWB receivers with different height levels: they can record three-dimensional signal data in a real-time way and with a view of 90° (mid gain), 60° (high gain), and omni-directional
3. CAT–5e shielded wires
4. low- and high-powered UWB tags (5 mW, 1 W) with different transmission rates (1, 15, 30 or 60 Hz)

Three or more receivers are placed in a specific area with known coordinates. A calibration procedure is performed. A central hub receives UWB short-pulse signals from UWB tags at a specific frequency (from 1 and 60 Hz). All receivers calculate the Time Differences Of Arrival (TDOA) and send the results to central hub.

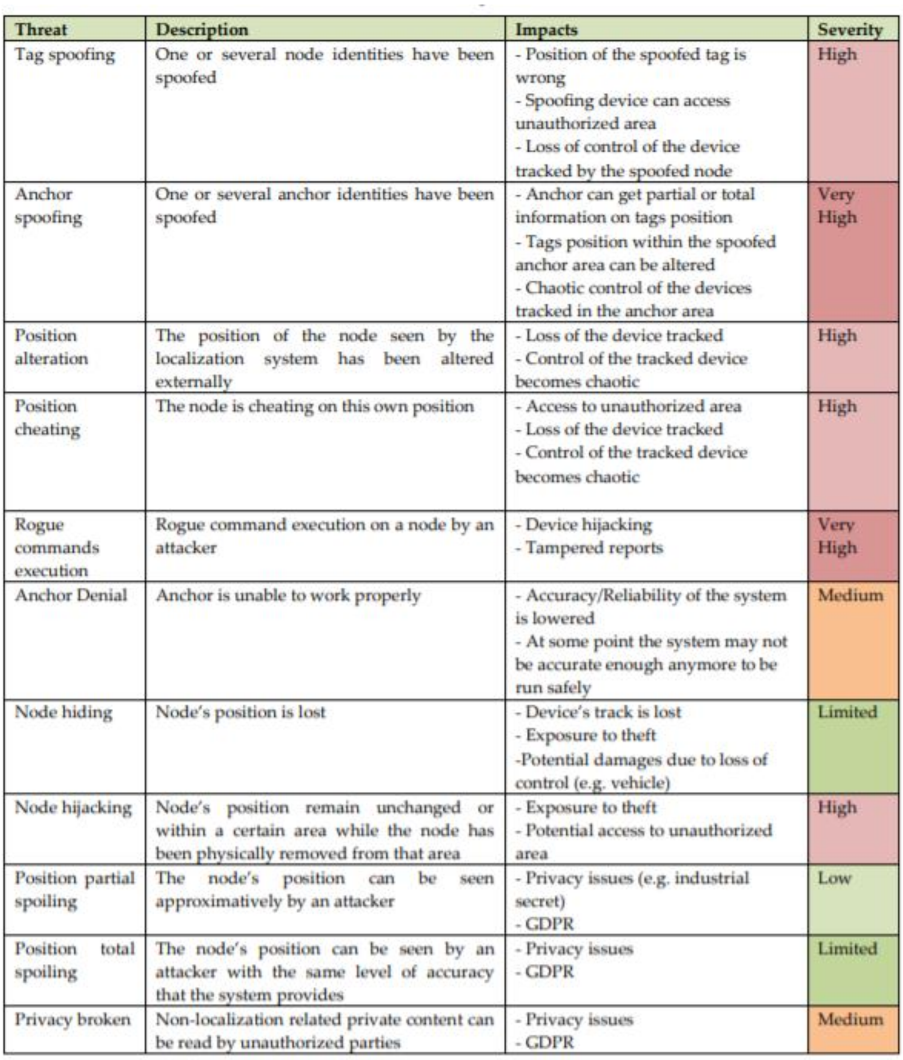
Figure 52. Sapphire UWB tracking system (Khoury and Kamat 2009).



9.5 Security in UWB communications

The relay attacks aim to measure the distance between the key. If a UWB device receives a weak signal strength, the key is far. If the signal strength is strong, the key is nearby. In a relay attack, the wanted signals is used to unlock the door and start the car if they are captured and intercepted. The rapid measurements of UWB signals can calculate the distance with high accuracy. Moreover, the IEEE 802.15.4z HRP UWB PHY adds a scrambled information (timestamp) into the packet. The idea is to avoid the access to Time of Flight (ToF)-based data using cryptographic keys and number randomness to the PHY packet. The major threats identified for industrial UWB are listed in Table 20 [65].

Table 20. Threats against UWB IPS.



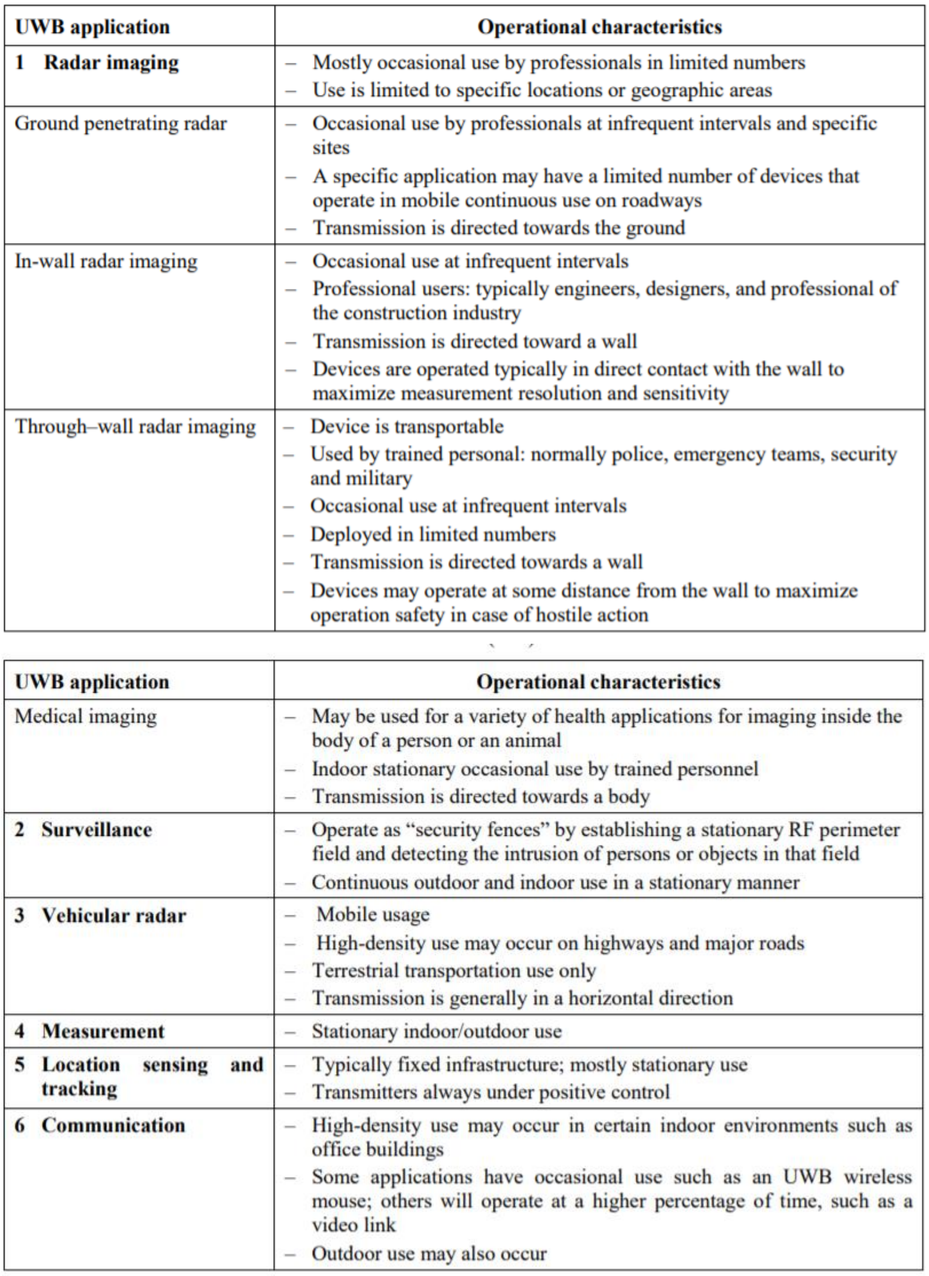
Threat	Description	Impacts	Severity
Tag spoofing	One or several node identities have been spoofed	- Position of the spoofed tag is wrong - Spoofing device can access unauthorized area - Loss of control of the device tracked by the spoofed node	High
Anchor spoofing	One or several anchor identities have been spoofed	- Anchor can get partial or total information on tags position - Tags position within the spoofed anchor area can be altered - Chaotic control of the devices tracked in the anchor area	Very High
Position alteration	The position of the node seen by the localization system has been altered externally	- Loss of the device tracked - Control of the tracked device becomes chaotic	High
Position cheating	The node is cheating on this own position	- Access to unauthorized area - Loss of the device tracked - Control of the tracked device becomes chaotic	High
Rogue commands execution	Rogue command execution on a node by an attacker	- Device hijacking - Tampered reports	Very High
Anchor Denial	Anchor is unable to work properly	- Accuracy/Reliability of the system is lowered - At some point the system may not be accurate enough anymore to be run safely	Medium
Node hiding	Node's position is lost	- Device's track is lost - Exposure to theft -Potential damages due to loss of control (e.g. vehicle)	Limited
Node hijacking	Node's position remain unchanged or within a certain area while the node has been physically removed from that area	- Exposure to theft - Potential access to unauthorized area	High
Position partial spoiling	The node's position can be seen approximatively by an attacker	- Privacy issues (e.g. industrial secret) - GDPR	Low
Position total spoiling	The node's position can be seen by an attacker with the same level of accuracy that the system provides	- Privacy issues - GDPR	Limited
Privacy broken	Non-localization related private content can be read by unauthorized parties	- Privacy issues - GDPR	Medium

The anchor spoofing and rogue command executions are the most important threats with a "very high" severity level. Anchors must verify all the mobile tags; a malicious anchor can potentially compromise the whole Indoor Positioning System (IPS). Rogue command execution implies enable an unauthorized access and control of a device (e.g., drone or robot). Tag spoofing, position alteration, position cheating and node hijacking are threats with "high severity". Tag spoofing or position alteration enable an unauthorized access. It means a malicious attacker can get a partial control over a device, e.g., vehicle along a specific path. Position cheating and node hijacking can bring the system to ignore triggers and alarms. If a node is hijacked, the attacker can exclude a specific node from a context.

9.6 UWB operational characteristics

The main operational characteristics of UWB applications are summarized in the following Table 21 prepared by ETSI [66].

Table 21. Operational characteristics of applications.



UWB application	Operational characteristics
1 Radar imaging	– Mostly occasional use by professionals in limited numbers – Use is limited to specific locations or geographic areas
Ground penetrating radar	– Occasional use by professionals at infrequent intervals and specific sites – A specific application may have a limited number of devices that operate in mobile continuous use on roadways – Transmission is directed towards the ground
In-wall radar imaging	– Occasional use at infrequent intervals – Professional users: typically engineers, designers, and professional of the construction industry – Transmission is directed toward a wall – Devices are operated typically in direct contact with the wall to maximize measurement resolution and sensitivity
Through–wall radar imaging	– Device is transportable – Used by trained personal: normally police, emergency teams, security and military – Occasional use at infrequent intervals – Deployed in limited numbers – Transmission is directed towards a wall – Devices may operate at some distance from the wall to maximize operation safety in case of hostile action
Medical imaging	– May be used for a variety of health applications for imaging inside the body of a person or an animal – Indoor stationary occasional use by trained personnel – Transmission is directed towards a body
2 Surveillance	– Operate as “security fences” by establishing a stationary RF perimeter field and detecting the intrusion of persons or objects in that field – Continuous outdoor and indoor use in a stationary manner
3 Vehicular radar	– Mobile usage – High-density use may occur on highways and major roads – Terrestrial transportation use only – Transmission is generally in a horizontal direction
4 Measurement	– Stationary indoor/outdoor use
5 Location sensing and tracking	– Typically fixed infrastructure; mostly stationary use – Transmitters always under positive control
6 Communication	– High-density use may occur in certain indoor environments such as office buildings – Some applications have occasional use such as an UWB wireless mouse; others will operate at a higher percentage of time, such as a video link – Outdoor use may also occur

For the future, UWB technology promises to increase the commercial impact due to high precise location and high-level security to protect access credentials and data communications [65]. UWB technology can offer signals easy to identify and resistant to noise and reflection, very useful for distance measurement applications and location-based services, including secure transactions in mobile devices (e.g., hands-free access, payments, identification, and device-to-device interactions).

10. LPWAN

Low Power Wide Area Networks (LPWAN) refers to the communication technologies able to coverage wide areas thank to low power-based wireless signal transmissions.

They can be divided into two main categories:

- Non-3GPP standard: LoRA
- 3GPP standard: Narrow Band-IoT (NB-IoT)

10.1 LoRAWAN

The Technical Specifications for LoRAWAN are included in the document "ETSI TR 103 526 V1.1.1 (2018-04)" [67]

10.1.1 The radio aspects

In Europe the LPWAN-CSS (Chirp Spread Spectrum) (LoRaWAN) are characterized by a 125 kHz bandwidth and radio frequencies as follow:

1) 867,1 MHz (1 % duty cycle, uplink and downlink)
2) 867,3 MHz (1 % duty cycle, uplink and downlink)
3) 867,5 MHz (1 % duty cycle, uplink and downlink)
4) 867,7 MHz (1 % duty cycle, uplink and downlink)
5) 867,9 MHz (1 % duty cycle, uplink and downlink)
6) 868,1 MHz (1 % duty cycle, uplink and downlink)
7) 868,3 MHz (1 % duty cycle, uplink and downlink)
8) 868,5 MHz (1 % duty cycle, uplink and downlink)
9) 869,525 MHz (downlink only, 10 % duty cycle)

Three channels (channels 6, 7 and 8) are also called "default channels" and must be implemented by every end node.

The radio signals (**LPWA-CSS signals**) used by both the end nodes and the gateway have the same characteristics in terms of modulation and spreading. They are chirp Spread Spectrum Signals tagged by a Spreading Factor (SF) value from 7 to 12. The SF controls the slope and the length in time of the signals. According to the LoRaWAN Specifications, the actual spreading factor is from 128 (SF=7) to 4096 (SF=12). The LPWAN-CSS signals are sent Over The Air (OTA) in asynchronous way and the LPWAN-CSS packet is constituted by a preamble, a PHY header and payload. The first information is used to detect and synchronize the devices, the PHY header indicates the payload length (from 13 to 255 bytes). It means the minimum size of a LoRaWAN physical payload is 13 bytes and a 16-bit CRC is also transmitted. The Table 22 shows the time used for the transmission and the payload data rate as function of the SF.

Table 22. Payload Data Rate and Time overhead (per packet, excluding data) as a function of the SF index.

SF index	Payload Data rate	Time overhead
7	5.5 kbps	40 ms
8	3.1 kbps	80 ms
9	1.8 kbps	150 ms
10	0.98 kbps	280 ms
11	0.44 kbps	570 ms
12	0.25 kbps	1100 ms

Table 23 summarizes the different values of bit rate provided by the LoRaWAN-CSS networks depending on SF and occupied bandwidth.

Table 23. Data rates allowed by the LoRaWAN protocol.

Data Rate	**Configuration (SF for LPWAN-CSS or FSK, occupied bandwidth)**	**bit rate (bit/s)**
0	LPWAN-CSS: SF12 / 125 kHz	250
1	LPWAN-CSS: SF11 / 125 kHz	440
2	LPWAN-CSS: SF10 / 125 kHz	980
3	LPWAN-CSS: SF 9 / 125 kHz	1760
4	LPWAN-CSS: SF 8 / 125 kHz	3125
5	LPWAN-CSS: SF 7 / 125 kHz	5470
6	LPWAN-CSS: SF7 / 250 kHz	11000
7	FSK	50000

This radius strongly depends on a number of factors such as antenna height, terrain, buildings height and density, location of the devices. The Table 24 shows the typical values of LoRaWAN-CSS coverage radius.

Table 24. Typical coverage radius of LoRaWAN™ protocol.

Environment	**Typical coverage radius**
Urban	1 km
Rural	10 km

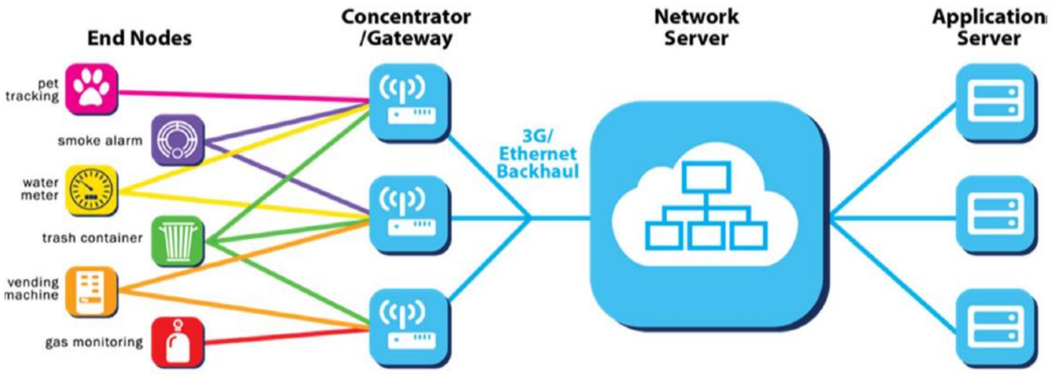
10.1.2 LPWAN Architecture

The LPWAN-CSS technology is mainly oriented for IoT applications. It includes four components:

- the end-device (or end-node)
- the Gateway
- the Network Server (NS)
- the Application Server (AS).

The architecture describing the relationship between these entities is depicted in Figure 53. The Gateway, the Network Server and the Application Server are part of the infrastructure of the network.

Figure 53. LoRaWAN architecture.



The end nodes are devices with a LPWAN-CSS radio transceiver. They are limited in terms of transmission power, memory and energy. Gateways are devices able to exchange the LPWAN-CSS signals with the end nodes. It provides a more powerful signal processing and high computation features. If each LPWAN-CSS end node can communicate with one or more gateways, each gateway is connected to a Network Server (NS) providing interconnection with external networks. LPWAN-CSS provides long-range, low power and low-cost two-way communications. The network topology is based on a star-of-stars network architecture: each node transmit data to multiple gateways in the same area. The gateway provides the encapsulation/deencapsulation and packet forwarding of LoRaWAN packets from/to the NS and then outside the LoRaWAN network. Each end node can select a specific SF, in order to reach the target data rate. This feature is **Adaptive Data Rate** (ADR).

End Node

The end node is a sensor/actuator with LPWAN-CSS transceivers controlled by a limited microprocessor.

Gateway

The gateway is a radio transceiver, working in half duplex mode, much similar to a base station in cellular networks, except for a much lower complexity and power consumption. Its role in the uplink communication path is to “collect” the packets arriving on the air from end nodes and forwarding them, through the IP backhaul connection, to the network server, timestamping them (with high precision if equipped with a GPS receiver, otherwise getting the time information from the backhaul IP link) and attaching to them a link quality indicator. On the downlink, the gateway receives the packets to send to the nodes from the network server along with the time it should send them on air and transmits them on air on the radio channel and with the SF indicated once again by the network server.

Network Server

The Network Server (NS) is the center of a LoRaWAN network.
The NS performs the following tasks:

- Node allocation in terms of radio channels
- Gateway selection
- Downlink control
- Authentication of the end nodes and admission control.

- Encryption of protocol commands and related data.
- Management of the gateways (e.g., in terms of the allocation the receivers).
- Localization of the end devices (when supported by the gateways).
- Network Operation Administration and Maintenance.

Application Server

Each end node has an AppKey used for an end-to-end encryption of the application data exchanged with the Application Server (AS).

10.1.3 LPWAN Security

As other IoT technologies, the Lora devices can be affected by security vulnerabilities and possible attacks performed by malicious attackers [68]. The following Table 25 summarizes the main security vulnerability for LoRa systems.

Table 25. LoRaWAN vulnerabilities.

Vulnerability	Details
Compromising Device and Network Keys	LoRaWAN provides end-to-end security using application and network keys. However, an attacker with physical access may compromise the LoRa end-devices. If an attacker gains physical access to a device, he/she may extract the keys
Jamming Techniques	Malicious entities can transmit a powerful radio signal in the proximity of application devices and disrupt the radio transmissions. Typically, such attacks require dedicated hardware, which minimizes the possibility of jamming attacks in real-world devices.
Replay Attacks	A replay attack is an attack on security protocol, re-sending or repeating the valid data transmission by the malicious entity. The main purpose of this attack is fooling the device or module by using handshake messages or old data from the network. In order to perform the attack in wireless networks, the entity should know the communication frequencies and channels to sniff data from transmission between devices
Wormhole Attacks	In this type of attack, one malicious device captures the packets from one device and transmits them to another distant located device to replay the captured packet. This can easily be launched by malicious entity without prior knowledge of the network or cryptographic mechanism

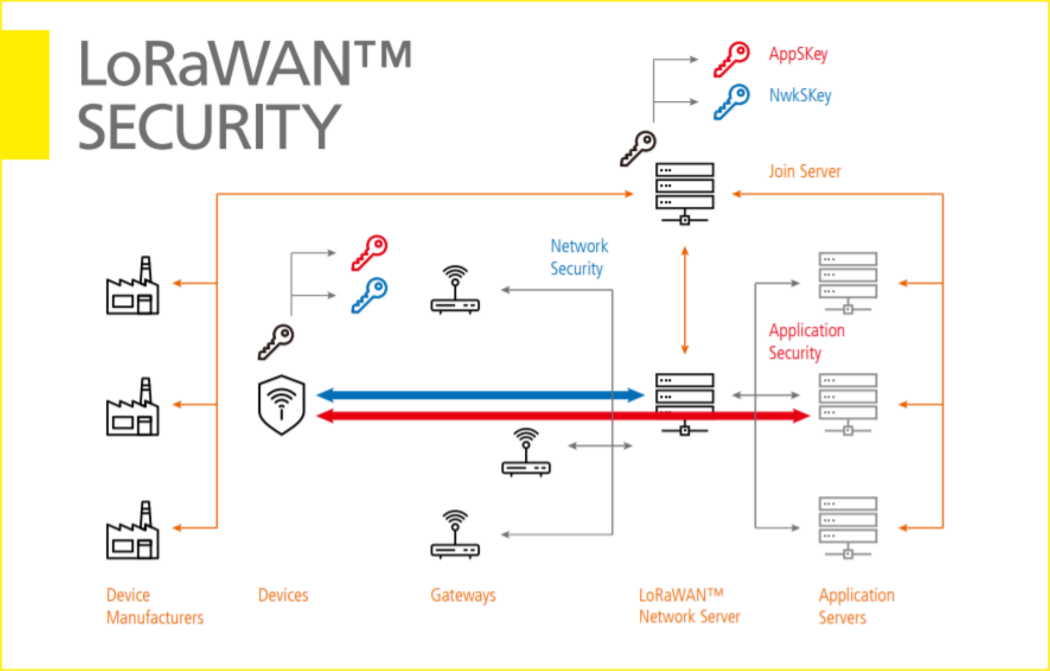
LoRaWAN protocol enables the end-to-end encryption of application payloads exchanged between end node and the AS [69]. The protection of data integrity is guaranteed thanks to the “hop-by-hop” nature of communications and secure transport solutions such as HTTPS and VPNs.

Mutual authentication

The Over-the-Air Activation allows to verify if both the end device and the network are aware of AppKey. The verification is guaranteed by adopting AES-CMAC4 encryption scheme. Then, two session keys are extracted: the first one (called NwkSKey) is used for integrity protection and encryption of the LoRaWAN MAC commands and application payload. The second one (called the

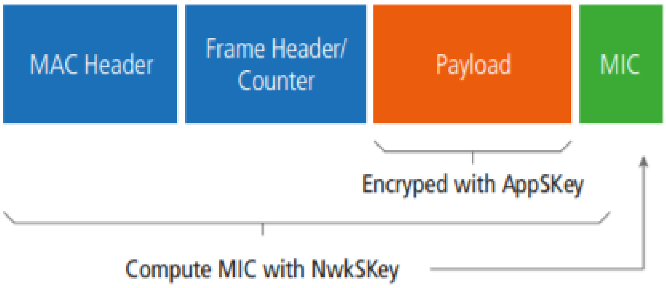
AppSKey) only for the end-to-end encryption of application payload. The NwkSKey is distributed to the LoRaWAN Network to verify the packet authenticity and integrity, while the AppSKey is distributed to the application server in order to encrypt/decrypt the application payload. Figure 54 shows the security model of LoraWAN [69].

Figure 54. LoRaWAN security model [69].



All LoRaWAN data are protected through two session keys. The payload is encrypted by AES-CTR scheme and carries a number as frame counter and a Message Integrity Code (MIC) obtained by AES-CMAC algorithm. Figure 55 shows the structure of a LoRaWAN packet and the corresponding protection [69].

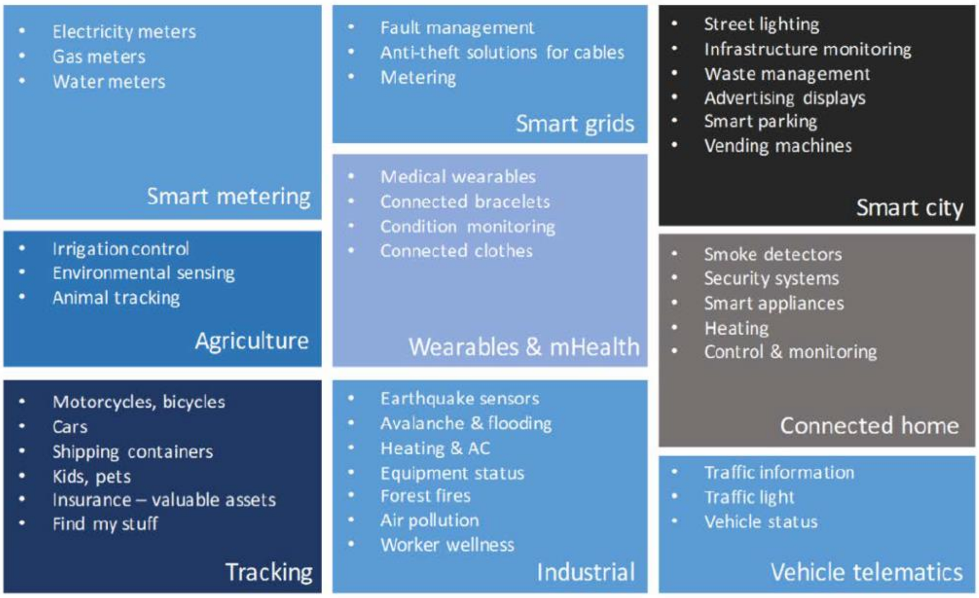
Figure 55. LoRaWAN packet structure and corresponding protection.



10.1.4 LPWAN Applications

LPWAN-CSS technology is used for different applications belonging to various sectors [70]. Figure 56 shows the main applications and sectors od interest of LoRaWAN.

Figure 56. LoRaWAN™ main verticals and use cases (source LoRa Alliance™).



- Electricity meters
- Gas meters
- Water meters

Smart metering

- Irrigation control
- Environmental sensing
- Animal tracking

Agriculture

- Motorcycles, bicycles
- Cars
- Shipping containers
- Kids, pets
- Insurance – valuable assets
- Find my stuff

Tracking

- Fault management
- Anti-theft solutions for cables
- Metering

Smart grids

- Medical wearables
- Connected bracelets
- Condition monitoring
- Connected clothes

Wearables & mHealth

- Earthquake sensors
- Avalanche & flooding
- Heating & AC
- Equipment status
- Forest fires
- Air pollution
- Worker wellness

Industrial

- Street lighting
- Infrastructure monitoring
- Waste management
- Advertising displays
- Smart parking
- Vending machines

Smart city

- Smoke detectors
- Security systems
- Smart appliances
- Heating
- Control & monitoring

Connected home

- Traffic information
- Traffic light
- Vehicle status

Vehicle telematics

One of the main applications where LPWAN-CSS technology benefits are key is water metering and flow monitoring (Figure 57).

Figure 57. Water flow monitoring using LoRaWAN.

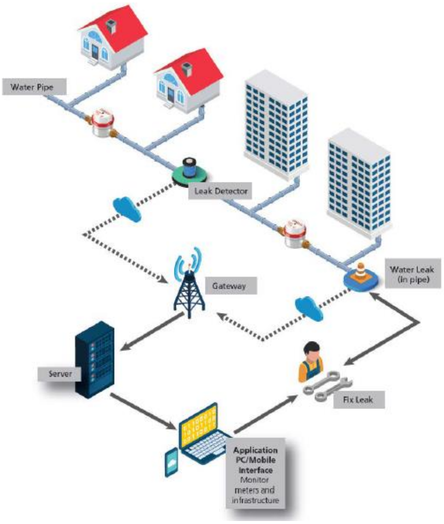
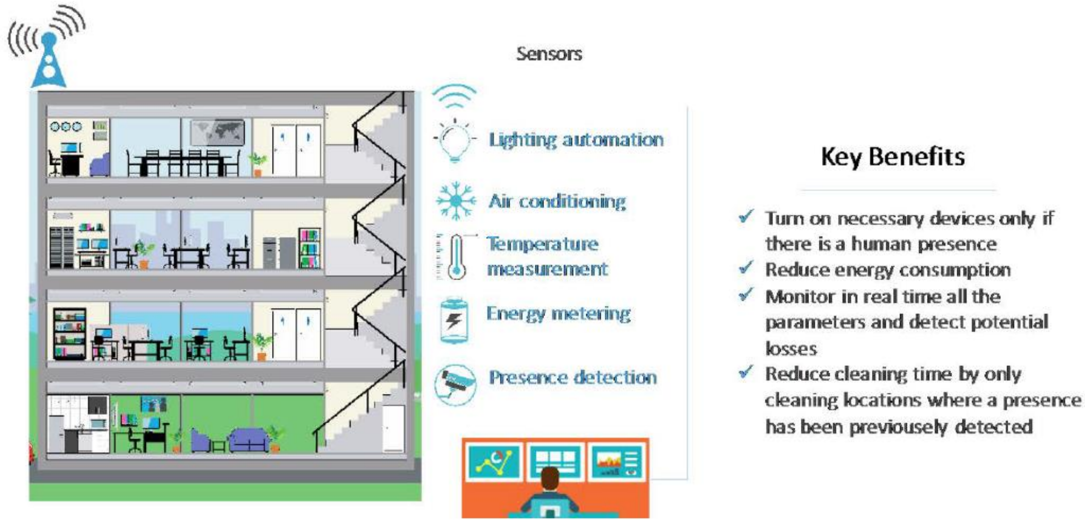
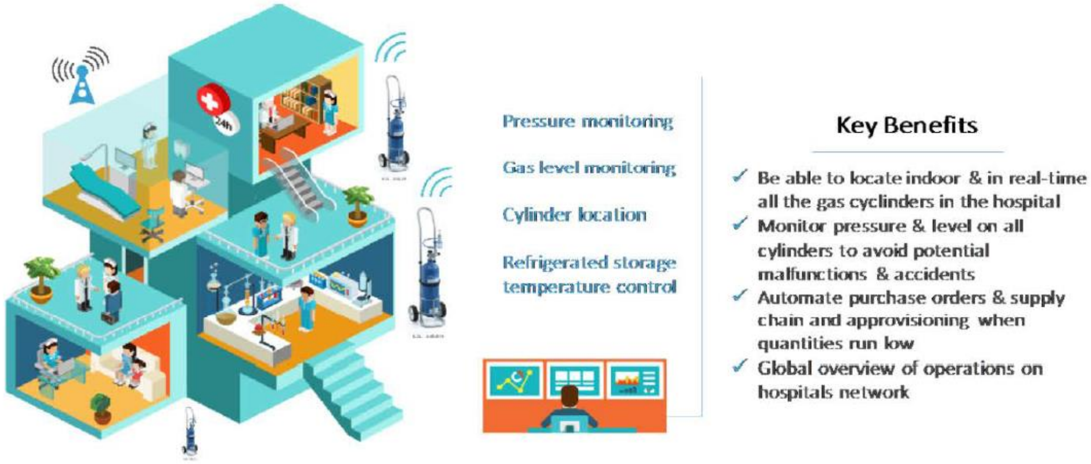


Figure 58. Facility management using LoRaWAN.



- ✓ Turn on necessary devices only if there is a human presence
- ✓ Reduce energy consumption
- ✓ Monitor in real time all the parameters and detect potential losses
- ✓ Reduce cleaning time by only cleaning locations where a presence has been previousely detected

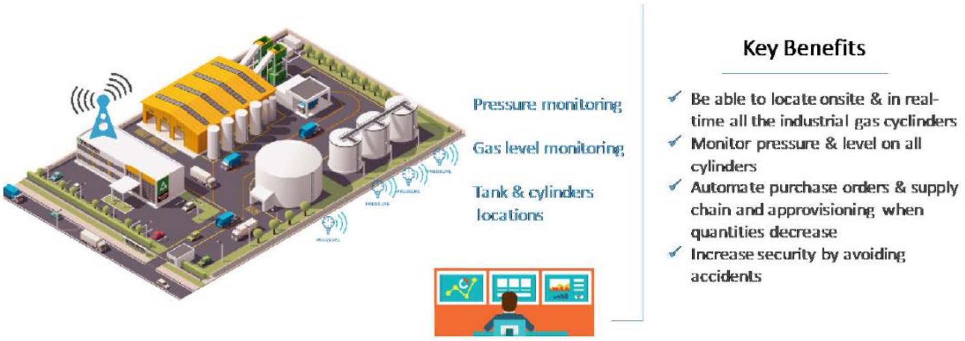
Figure 59. Healthcare using LoRaWAN.



- ✓ Be able to locate indoor & in real-time all the gas cyclinders in the hospital
- ✓ Monitor pressure & level on all cylinders to avoid potential malfunctions & accidents
- ✓ Automate purchase orders & supply chain and approvisioning when quantities run low
- ✓ Global overview of operations on hospitals network

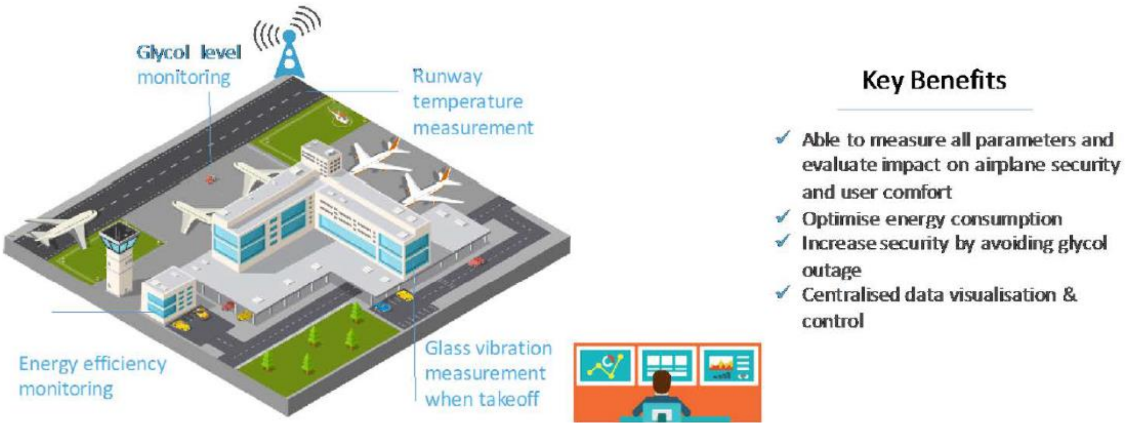
The other area where LPWAN-CSS technology plays an important role is Smart Industry, especially for the flexibility between private and public networks.

Figure 60. Factory and industry management using LoRaWAN.



- ✓ Be able to locate onsite & in real-time all the industrial gas cyclinders
- ✓ Monitor pressure & level on all cylinders
- ✓ Automate purchase orders & supply chain and approvisioning when quantities decrease
- ✓ Increase security by avoiding accidents

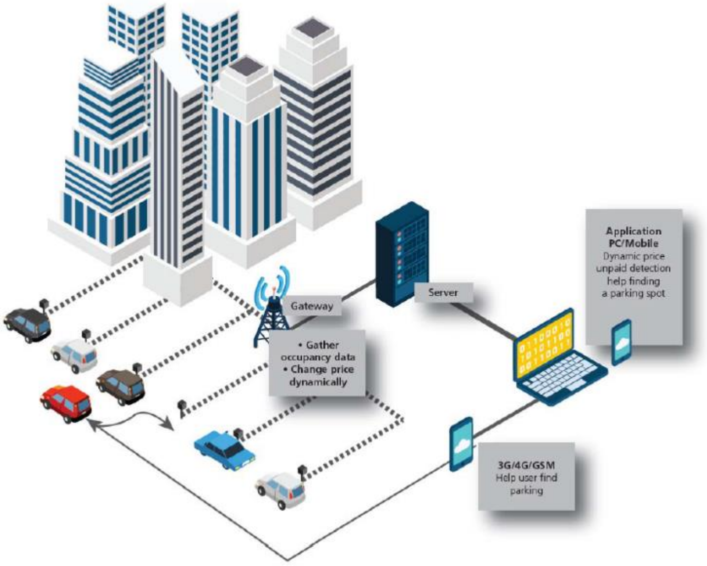
Figure 61. Airport Service Management using LoRaWAN.


Glycol level monitoring
Runway temperature measurement
Energy efficiency monitoring
Glass vibration measurement when takeoff

Key Benefits

- ✓ Able to measure all parameters and evaluate impact on airplane security and user comfort
- ✓ Optimise energy consumption
- ✓ Increase security by avoiding glycol outage
- ✓ Centralised data visualisation & control

Figure 62. Main smart city applications using LoRaWAN.



10.1.5 LPWAN market

The LoRa Alliance is the consortium committed to maintain the LoRaWAN protocol and it is formed by more than 450 members after two years of existence, as mobile network operators, sensor and gateway manufacturers, chipset and module manufacturers, large enterprises, network management services, and application software providers.

The LoRa Alliance only defines the specification for LoRaWAN protocol and certification. This open ecosystem enables different business models.

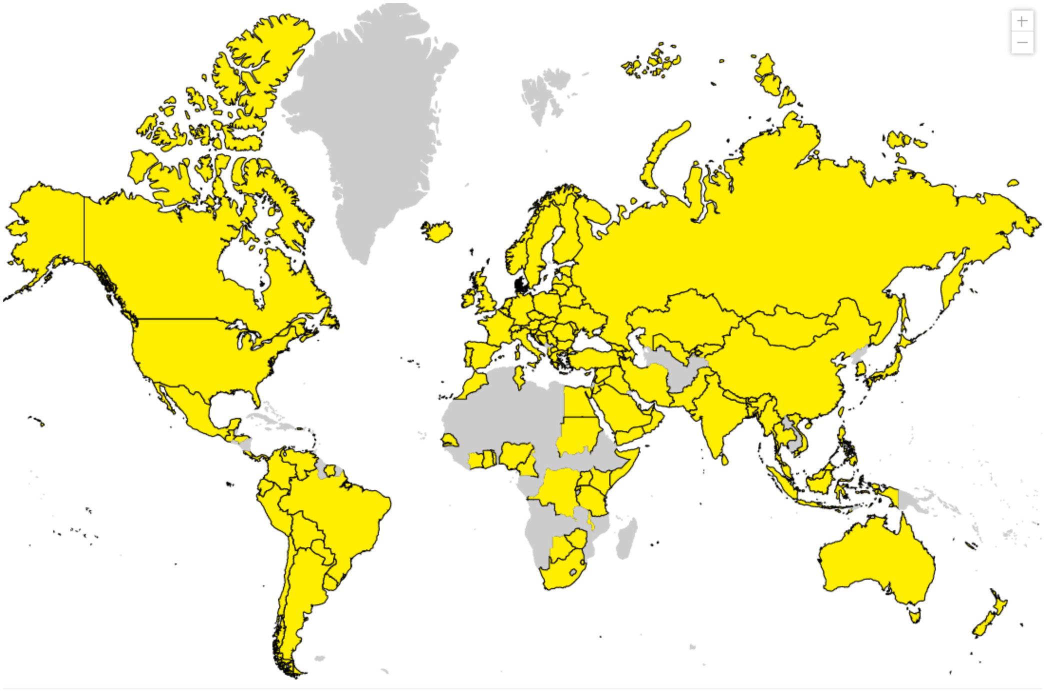
The LoRaWA protocol can be used to implement:

a) A private (closed) network: an entity (e.g., a company in its own premises, a municipality, etc.) can deploy all the elements of the LoRaWAN network.

b) A public (open) network: an entity (a network provider) can deploy all the elements of the LoRaWAN network and the connectivity to other entities is provided.

Figure 63 only shows the announced and available open networks. We can observe 148 LoRaWAN Network Operators and 162 Countries involved.

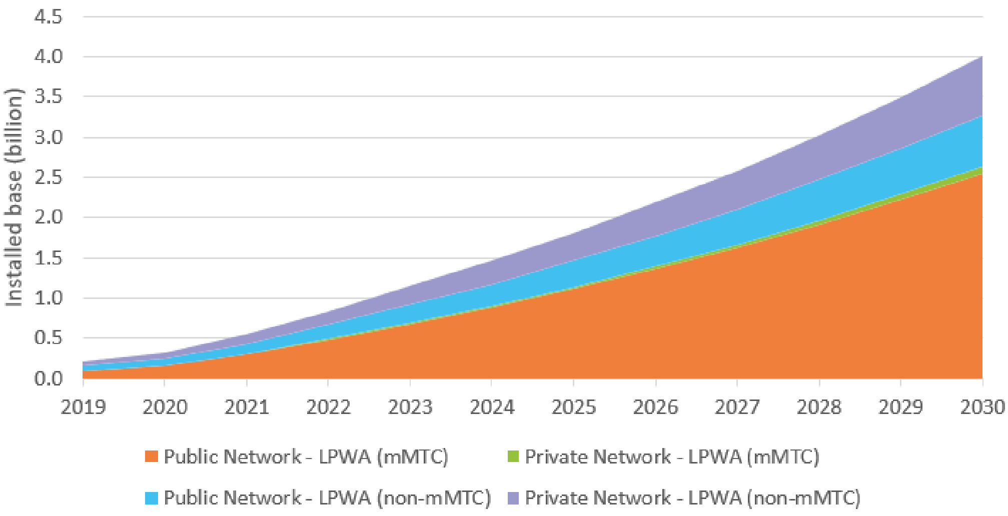
Figure 63. LoRaWAN Global Coverage (February 2021).



For the next years, Transforma Insights predicts 4 billion LPWA connections in 2030 (up from 220 million at the end of 2019). Almost two-thirds will be accounted for by 5G mMTC (massive Machine-Type Communications) namely NB-IoT and LTE-M, operating in licensed spectrum. The remaining one-third will be covered by technologies such as LoRa and Sigfox operating in unlicensed spectrum [71].
The mMTC devices are mainly (97%) connected via public networks managed by mobile network operators, while the 1.4 billion non-mMTC LPWA devices connected both via public networks (46%) and via private network (54%).

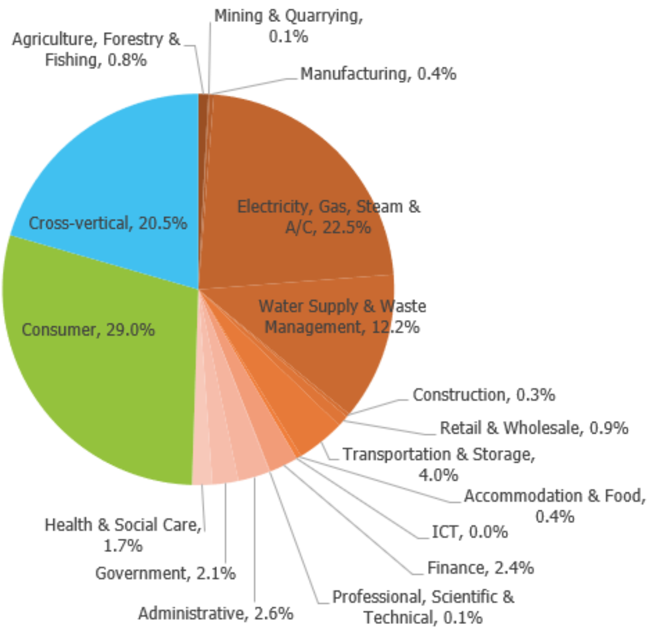
Figure 64 illustrates how the four categories are split.

Figure 64. Global Low Power Wide Area Connections 2019-2030 [Source: Transforma Insights, 2020].



In 2030 the half of all connections (50.5%) are used by specific applications, 29% by consumer and 20.5% by "cross-vertical" applications. In the considered period (2019-2030), energy is the most important enterprise sector for LPWA connections (over 20%) with the smart metering as the crucial application. The water metering application will grow from 5% of LPWA connections today to 12% in 2030, as shown in Figure 65.

Figure 65. Vertical split of LPWA connections in 2030 [Source: Transforma Insights, 2020].



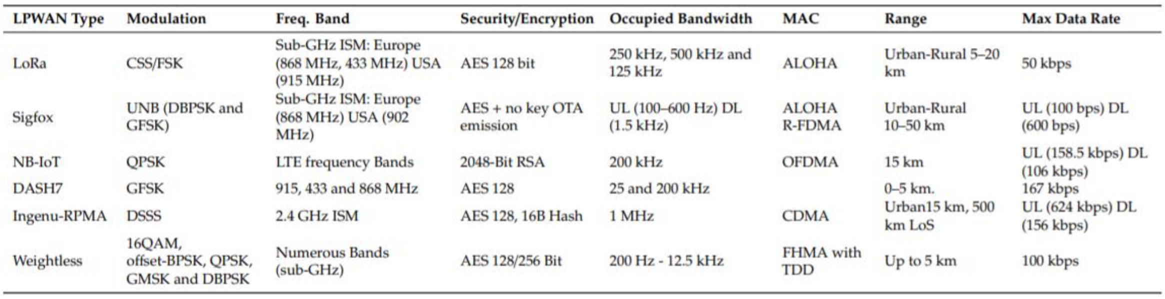
10.2 Narrow-band IoT (NB-IoT)

10.2.1 Introduction

The Narrow-Band Internet of Things (NB-IoT) is a massive LPWA technology proposed in the 3GPP Release 13 for intelligent low data rate applications [72]. Based on cellular telecommunication bands, it is a technology with long battery duration and large coverage area [73]. NB-IoT [74] was standardized by 3GPP on the basis of LTE (Long Term Evolution). The frequency band is 700 MHz, 800 MHz and 900 MHz. NB-IoT enhances the power consumption, spectrum efficiency and system capacity of devices, as shown in Table 26.

NB-IoT can handle about 5000 connections per cell and it supports 40 devices per household. NB-IoT use Orthogonal Frequency-Division Multiple Access (OFDMA) for downlink and Single-Carrier Frequency-Division Multiple Access (SC-FDMA). It allows data rate up to 158.5 kbps (in uplink) and 106 kbps (in downlink). The transmitting power is +23 dB and the maximum payload size for each message is 1600 bytes. A single NB-IoT module costs around less than 5$.

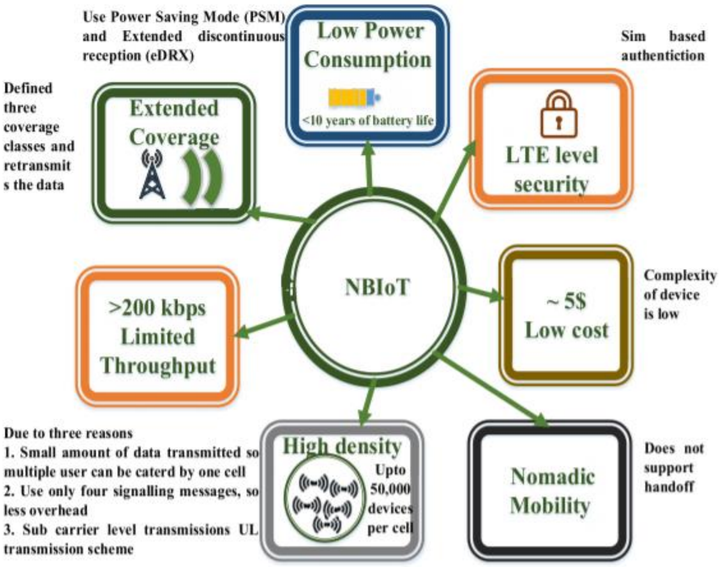
Table 26. Some prominent low power wide area network (LPWAN) technologies and their technical features.



LPWAN Type	Modulation	Freq. Band	Security/Encryption	Occupied Bandwidth	MAC	Range	Max Data Rate
LoRa	CSS/FSK	Sub-GHz ISM: Europe (868 MHz, 433 MHz) USA (915 MHz)	AES 128 bit	250 kHz, 500 kHz and 125 kHz	ALOHA	Urban-Rural 5–20 km	50 kbps
Sigfox	UNB (DBPSK and GFSK)	Sub-GHz ISM: Europe (868 MHz) USA (902 MHz)	AES + no key OTA emission	UL (100–600 Hz) DL (1.5 kHz)	ALOHA R-FDMA	Urban-Rural 10–50 km	UL (100 bps) DL (600 bps)
NB-IoT	QPSK	LTE frequency Bands	2048-Bit RSA	200 kHz	OFDMA	15 km	UL (158.5 kbps) DL (106 kbps)
DASH7	GFSK	915, 433 and 868 MHz	AES 128	25 and 200 kHz		0–5 km.	167 kbps
Ingenu-RPMA	DSSS	2.4 GHz ISM	AES 128, 16B Hash	1 MHz	CDMA	Urban15 km, 500 km LoS	UL (624 kbps) DL (156 kbps)
Weightless	16QAM, offset-BPSK, QPSK, GMSK and DBPSK	Numerous Bands (sub-GHz)	AES 128/256 Bit	200 Hz - 12.5 kHz	FHMA with TDD	Up to 5 km	100 kbps

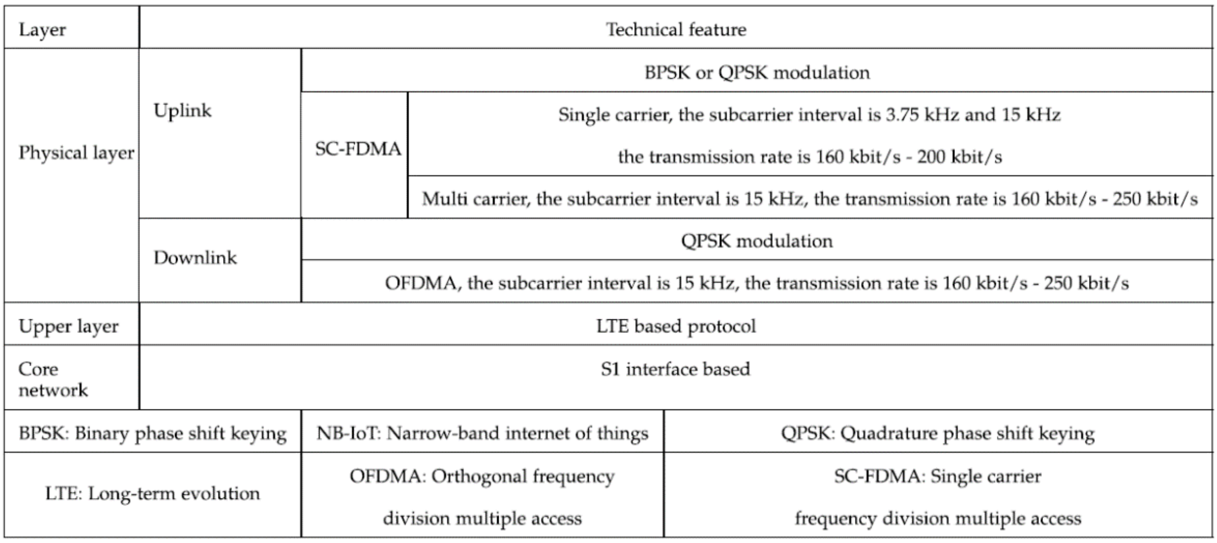
NB-IoT is the technology identified and standardized in a brief time, to meet the demand for low data rate connections [75]. It can address the needs of mMTC (massive Machine Type Communication) by following features (Figure 66):

Figure 66. NB-IoT main features.


Use Power Saving Mode (PSM) and Extended discontinuous reception (eDRX)
Low Power Consumption
<10 years of battery life
Sim based authentiction
Defined three coverage classes and retransmits the data
Extended Coverage
LTE level security
NBIoT
~ 5$ Low cost
Complexity of device is low
>200 kbps Limited Throughput
Due to three reasons
1. Small amount of data transmitted so multiple user can be caterd by one cell
2. Use only four signalling messages, so less overhead
3. Sub carrier level transmissions UL transmission scheme
High density
Upto 50,000 devices per cell
Nomadic Mobility
Does not support handoff

The development of NB-IoT is based on LTE [72] (Figure 67). The NB-IoT bandwidth at physical layer is 200 kHz. In downlink, NB-IoT uses a QPSK modulation scheme and OFDMA technology with sub-carrier spacing of 15 kHz [76]. In uplink, BPSK or QPSK modulation schemes and SC-FDMA technology including single sub-carrier/multiple subcarriers. The with sub-carrier spacing is 3.75 kHz and 15 kHz.

Figure 67. Main technical features of NB-IoT [72].



Layer	Technical feature		
Physical layer	Uplink	BPSK or QPSK modulation	
		SC-FDMA	Single carrier, the subcarrier interval is 3.75 kHz and 15 kHz the transmission rate is 160 kbit/s - 200 kbit/s
			Multi carrier, the subcarrier interval is 15 kHz, the transmission rate is 160 kbit/s - 250 kbit/s
	Downlink	QPSK modulation	
		OFDMA, the subcarrier interval is 15 kHz, the transmission rate is 160 kbit/s - 250 kbit/s	
Upper layer	LTE based protocol		
Core network	S1 interface based		
BPSK: Binary phase shift keying	NB-IoT: Narrow-band internet of things	QPSK: Quadrature phase shift keying	
LTE: Long-term evolution	OFDMA: Orthogonal frequency division multiple access	SC-FDMA: Single carrier frequency division multiple access	

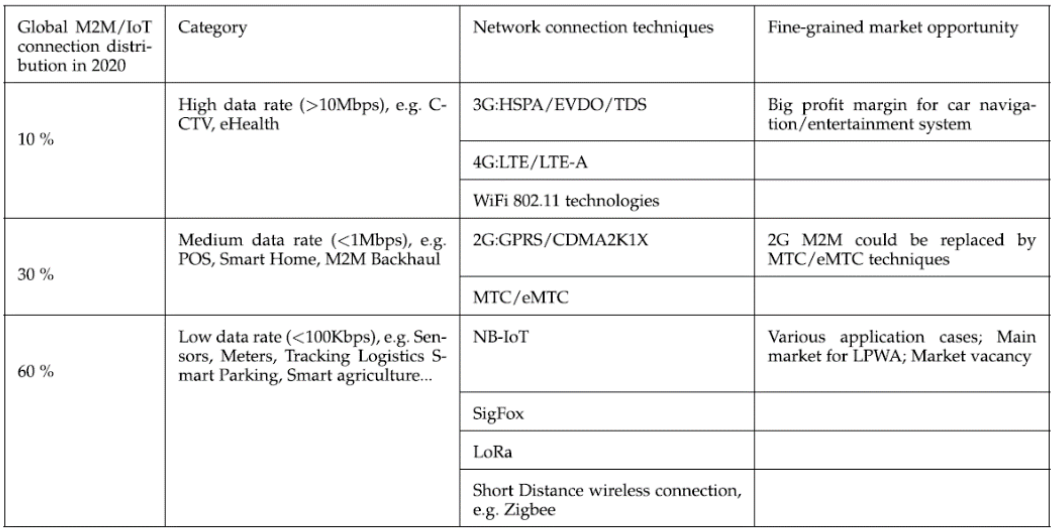
WORKING MODE OF NB-IOT

According to specifications described in RP-151621, NB-IoT actually supports only FDD transmission mode with bandwidth of 180 kHz and 3 following types of deployment scenes [77], [78]:

- **Independent deployment** (Stand-alone mode): it uses independent frequency band (without overlap with LTE frequencies)
- **Guard-band deployment** (Guard-band mode): it uses LTE edge frequencies
- **In-band deployment** (In-band mode): it uses LTE frequencies (requiring n. 1 LTE Physical Resource Block)

Due to the rapid growth of low-data-rate IoT applications, LPWA market share has increased gradually. According to the report of Hequan Wu in 2016 China Internet of Things Conference, the intelligent IoT applications can be divided into three main categories based on data transmission rate requirements in 2020 (Table 27).

Table 27. Distribution figure for connection technology of intelligent IoT in 2020.



Global M2M/IoT connection distribution in 2020	Category	Network connection techniques	Fine-grained market opportunity
10 %	High data rate (>10Mbps), e.g. C-CTV, eHealth	3G:HSPA/EVDO/TDS	Big profit margin for car navigation/entertainment system
		4G:LTE/LTE-A	
		WiFi 802.11 technologies	
30 %	Medium data rate (<1Mbps), e.g. POS, Smart Home, M2M Backhaul	2G:GPRS/CDMA2K1X	2G M2M could be replaced by MTC/eMTC techniques
		MTC/eMTC	
60 %	Low data rate (<100Kbps), e.g. Sensors, Meters, Tracking Logistics S-mart Parking, Smart agriculture...	NB-IoT	Various application cases; Main market for LPWA; Market vacancy
		SigFox	
		LoRa	
		Short Distance wireless connection, e.g. Zigbee	

HIGH DATA TRANSMISSION RATE

The data rate is higher than 10 Mbps. Access to 3G, 4G and Wi-Fi technologies is provided. The typical applications are TV broadcast, healthcare, automotive navigation, vehicle entertainment system, etc. The expected market share is 10%.

MEDIUM DATA TRANSMISSION RATE

The data rate is lower than 1 Mbps. Access to 2G and MTC/eMTC technologies is provided. The typical applications are related to POS machines and smart home. The expected market share is 30%.

LOW DATA TRANSMISSION RATE

The data rate is lower than 100 Kbps. Access to NB-IoT, SigFox, LoRa and short-range wireless technologies (e.g., ZigBee) is provided. The typical applications include sensors, smart metering, tracking, logistics and intelligent agriculture. The expected market share is 60%. The comparison between LPWAN represented by NB-IoT and other communication technologies is presented in Figure 68.

Figure 68. Comparison among LPWAN, NB-IoT and other wireless communication technologies.

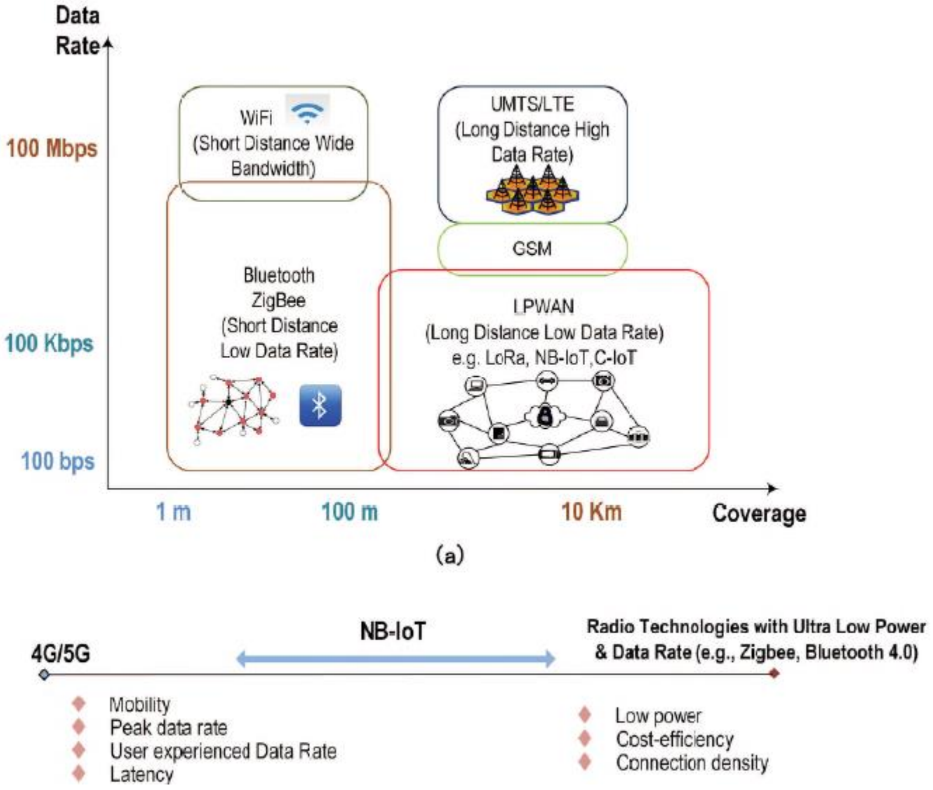
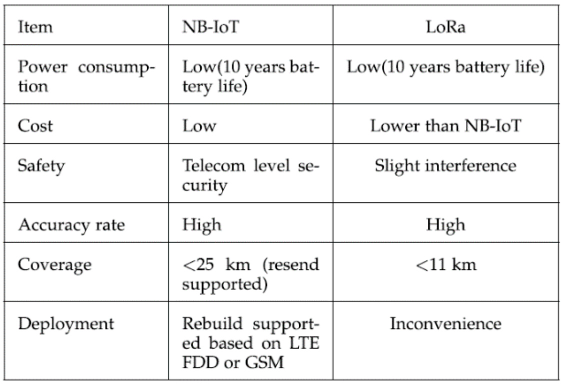

Data Rate
100 Mbps
100 Kbps
100 bps
WiFi
(Short Distance Wide Bandwidth)
UMTS/LTE
(Long Distance High Data Rate)
GSM
Bluetooth
ZigBee
(Short Distance Low Data Rate)
LPWAN
(Long Distance Low Data Rate)
e.g. LoRa, NB-IoT,C-IoT
1 m
100 m
10 Km
Coverage
(a)
4G/5G
NB-IoT
Radio Technologies with Ultra Low Power & Data Rate (e.g., Zigbee, Bluetooth 4.0)
Mobility
Peak data rate
User experienced Data Rate
Latency
Low power
Cost-efficiency
Connection density

Table 28 shows the comparison between NB-IoT e LoRaWAN technologies. The NB-IoT guarantees larger coverage areas, higher density and low-cost features for IoT devices. LoRaWAN is rapidly increasing and can be deployed in smart cities and within vertical industrial sectors.

Table 28. Comparison between NB-IoT e LoRaWAN.

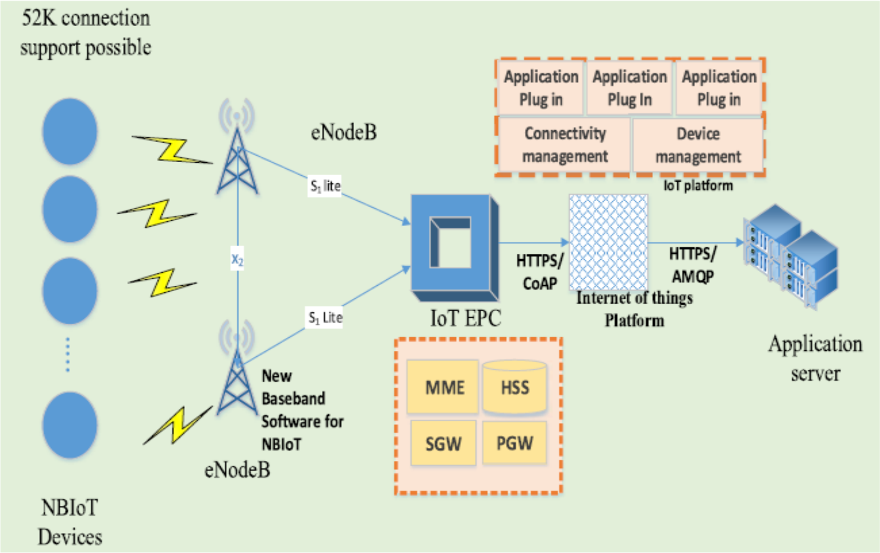


Item	NB-IoT	LoRa
Power consumption	Low(10 years battery life)	Low(10 years battery life)
Cost	Low	Lower than NB-IoT
Safety	Telecom level security	Slight interference
Accuracy rate	High	High
Coverage	<25 km (resend supported)	<11 km
Deployment	Rebuild supported based on LTE FDD or GSM	Inconvenience

10.2.2 NB-IoT Network Architecture

The reference architecture of NBIoT is shown in Figure 69 [75].

Figure 69. NB-IoT architecture.



Here NB-IoT device communicates with the eNodeB, while the eNodeB is connected to IoT Evolved Packet Core (EPC). It includes: the Serving Gateway (S-GW), the Packet Data Network (P-GW), the Mobility Management Plane entity (MME) and the Home Subscriber Server (HSS). The eNodeB sends the Non-Access Stratum (NAS) messages[3] to EPC using s1-lite interface. Then EPC enables the Access Stratum (AS) and then transfers the messages to the IoT platform. The IoT platform sends the data to the application servers. This data is then processed by the Application server.

10.2.3 NB-IoT Security

The issue of security is very critical for NBIoT technology [80]. The devices are limited in terms of power and then more vulnerable to security attacks, as false data injection or interference during the transmission.
NB-IoT adopts the LTE’s authentication and encryption [73]. The security requirements for NB-IoT are based on main three layers [81]:

- perception layer
- transmission layer
- application layer

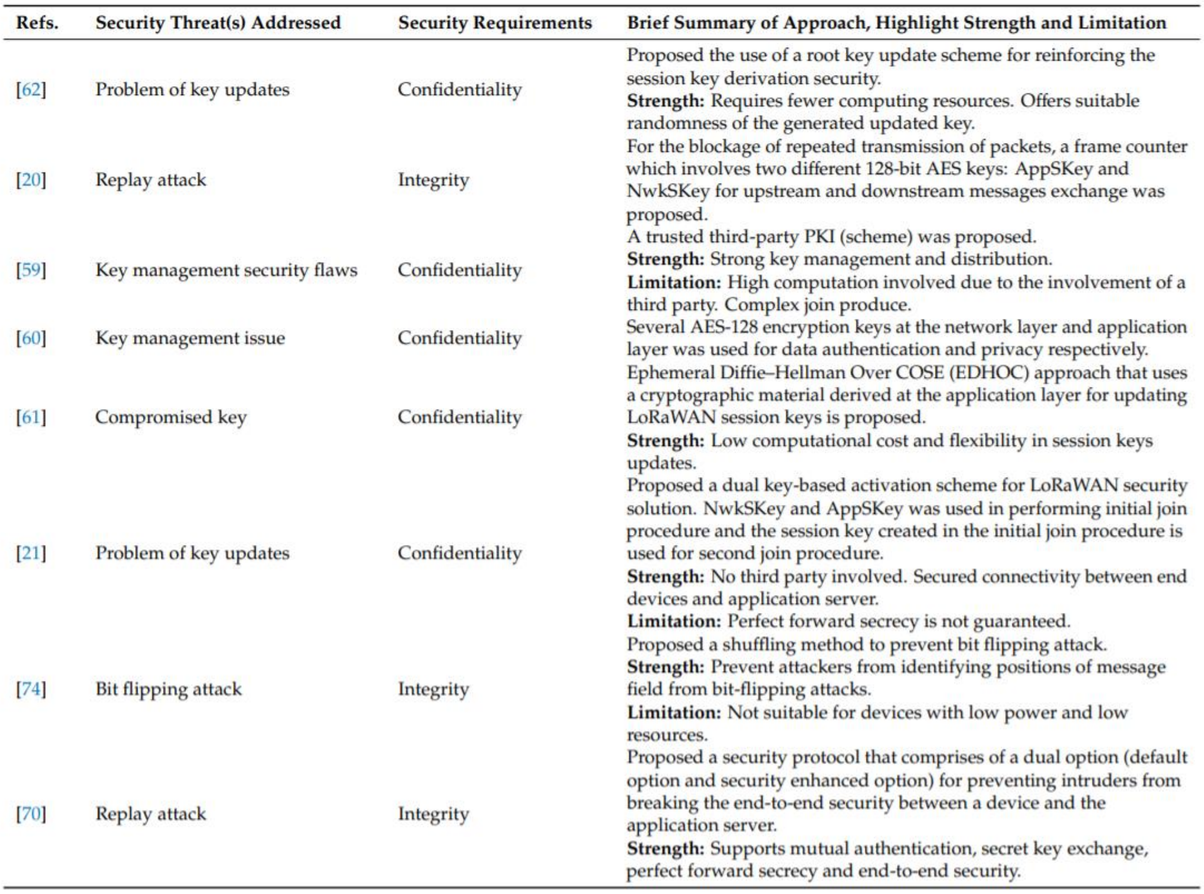
The perception layer is affected by both active and passive attacks. In passive attack the attacker will monitor the network traffic, while the active attacks are oriented to manipulate the integrity of message. The adoption of cryptographic algorithm is useful for data encryption, integrity authentication and verification. In perception layer, each node can exchange data with the Base

[3] It is a signaling message. NAS is a protocol deputed to send non-radio signal between the user equipment and MME for session and mobility management.

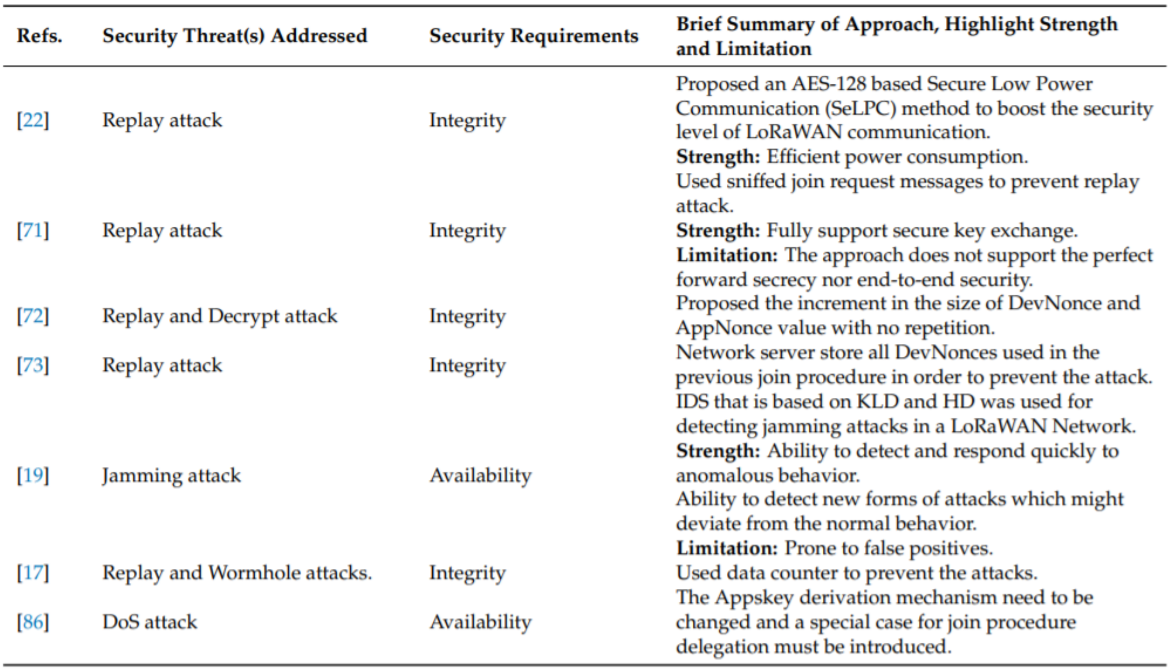
Station (eNB). In transmission layer, NB-IoT can modify the network scheme basing on the transmission feedback. In the NB-IoT application layer in NB-IoT the data are stored. The main security requirements regard the identification and processing of this massive heterogeneous data, data integrity and authentication. In the literature, several research papers have been published on IoT and LPWAN [81]. Regarding the LPWAN security research works, most of them are focused mainly on threats and vulnerability analysis.

Table 29 presents the comparison of different LPWAN security features and the adopted methodology.

Table 29. Comparison of Different Scheme Employed to Prevent LPWAN Attack.



Refs.	Security Threat(s) Addressed	Security Requirements	Brief Summary of Approach, Highlight Strength and Limitation
[62]	Problem of key updates	Confidentiality	Proposed the use of a root key update scheme for reinforcing the session key derivation security. **Strength:** Requires fewer computing resources. Offers suitable randomness of the generated updated key.
[20]	Replay attack	Integrity	For the blockage of repeated transmission of packets, a frame counter which involves two different 128-bit AES keys: AppSKey and NwkSKey for upstream and downstream messages exchange was proposed.
[59]	Key management security flaws	Confidentiality	A trusted third-party PKI (scheme) was proposed. **Strength:** Strong key management and distribution. **Limitation:** High computation involved due to the involvement of a third party. Complex join produce.
[60]	Key management issue	Confidentiality	Several AES-128 encryption keys at the network layer and application layer was used for data authentication and privacy respectively.
[61]	Compromised key	Confidentiality	Ephemeral Diffie–Hellman Over COSE (EDHOC) approach that uses a cryptographic material derived at the application layer for updating LoRaWAN session keys is proposed. **Strength:** Low computational cost and flexibility in session keys updates.
[21]	Problem of key updates	Confidentiality	Proposed a dual key-based activation scheme for LoRaWAN security solution. NwkSKey and AppSKey was used in performing initial join procedure and the session key created in the initial join procedure is used for second join procedure. **Strength:** No third party involved. Secured connectivity between end devices and application server. **Limitation:** Perfect forward secrecy is not guaranteed.
[74]	Bit flipping attack	Integrity	Proposed a shuffling method to prevent bit flipping attack. **Strength:** Prevent attackers from identifying positions of message field from bit-flipping attacks. **Limitation:** Not suitable for devices with low power and low resources.
[70]	Replay attack	Integrity	Proposed a security protocol that comprises of a dual option (default option and security enhanced option) for preventing intruders from breaking the end-to-end security between a device and the application server. **Strength:** Supports mutual authentication, secret key exchange, perfect forward secrecy and end-to-end security.

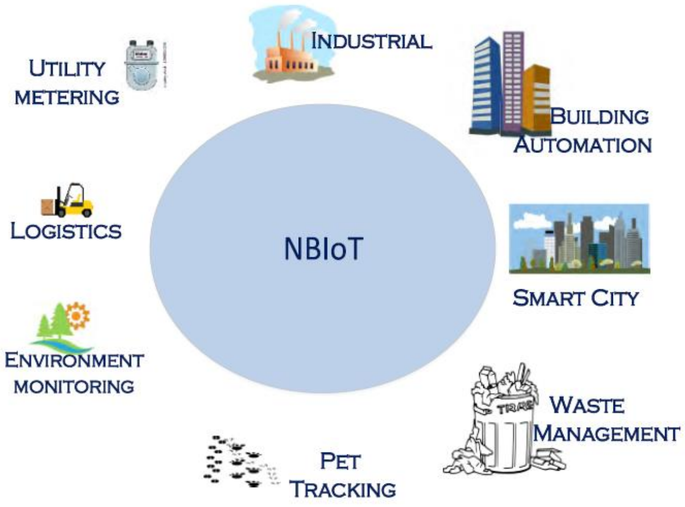


Refs.	Security Threat(s) Addressed	Security Requirements	Brief Summary of Approach, Highlight Strength and Limitation
[22]	Replay attack	Integrity	Proposed an AES-128 based Secure Low Power Communication (SeLPC) method to boost the security level of LoRaWAN communication. **Strength:** Efficient power consumption.
[71]	Replay attack	Integrity	Used sniffed join request messages to prevent replay attack. **Strength:** Fully support secure key exchange. **Limitation:** The approach does not support the perfect forward secrecy nor end-to-end security.
[72]	Replay and Decrypt attack	Integrity	Proposed the increment in the size of DevNonce and AppNonce value with no repetition.
[73]	Replay attack	Integrity	Network server store all DevNonces used in the previous join procedure in order to prevent the attack.
[19]	Jamming attack	Availability	IDS that is based on KLD and HD was used for detecting jamming attacks in a LoRaWAN Network. **Strength:** Ability to detect and respond quickly to anomalous behavior. Ability to detect new forms of attacks which might deviate from the normal behavior. **Limitation:** Prone to false positives.
[17]	Replay and Wormhole attacks.	Integrity	Used data counter to prevent the attacks.
[86]	DoS attack	Availability	The Appskey derivation mechanism need to be changed and a special case for join procedure delegation must be introduced.

10.2.4 NB-IoT Application

The most important NB-IoT applications are smart metering and intelligent environment monitoring [75] [82] [83]. The NB-IoT supports multiple connections with low power devices [84], wide area coverage, together with a control plane [85] and data plane [86], [87]. Since it is supported by the cellular communication network [88], it is a promising technology [89]. For these reasons, several market analysts predict the revenue in the future due to the support to a wide range of applications, as smart metering, industry automation, smart logistics, smart cities, waste management, environmental monitoring, agriculture, and wearables, etc… (Figure 70).

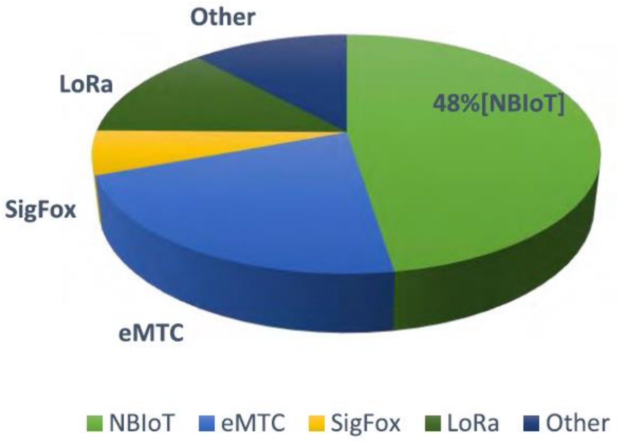
Figure 70. Application of NB-IoT.



10.2.5 NB-IoT Market

In the first quarter of 2018, we assisted to an IoT market growth in all vertical sectors [75]. LPWAN is one of the IoT enablers for IoT. The IoT Analytics report forecasts a Compound Annual Growth Rate (CAGR) for LPWA connections around 81% during the 2018-2025 period [90]. According to Machina, the NB-IoT market share will be around 48% by 2025 (Figure 71) [89].

Figure 71. NB-IoT market share.



10.3 LoRAWAN and NB-IoT: applicability to a railway environment

According to GSMA report [135]: *“Both LoRaWAN and NB-IoT end devices have lower power consumption by shifting to sleep mode when not in operation. As a synchronous protocol, NB-IoT consumes significantly more energy than LoRaWAN, which is an asynchronous protocol, and when measured on the same data throughput, NB-IoT consumes higher peak current required for OFDM/FDMA modulation. Regardless, the characteristics of these two technologies are critical for many application segments that require deep indoor coverage and years of battery life.”*

Regarding the applicability to the rail context, LoRaWAN and NB-IoT present some differences. The first one is related to the spectrum: LoRaWAN uses unlicensed spectrum, while NB-IoT uses licensed spectrum provided by Mobile Network Operator (MNO). While LoraWan a is a good option if bidirectionality is requested due to symmetric link (e.g. command-and-control functionality). Moreover, LoRaWAN devices are characterized by longer battery life than NB-IoT devices. NB-IoT devices need for MNO coverage, so they are more suitable for indoor and dense urban areas. It has faster response times than LoRa and can guarantee a better quality of service.

LoRaWAN provides lower data rates and longer latency time than NB-IoT. It requires a gateway to work but not a network provided by MNO, as in case of NB-IoT. It means LoRaWAN technologies are suitable for On-board monitoring, facility arrangement and tracking, station service management (e.g. train in movement towards the station area) and smart environment applications (train and station data transmission). No other communication entities are needed to be involved.

On the other hand, NB-IoT can suffer from network handovers in case of assets in movement at high speed. It is more suitable for sensors and meters in a fixed location. Smart metering and smart logistics application can regard the data coming from the train, but monitoring of rail infrastructure, train passing, and rail crossing can be enabled by NB-IoT.

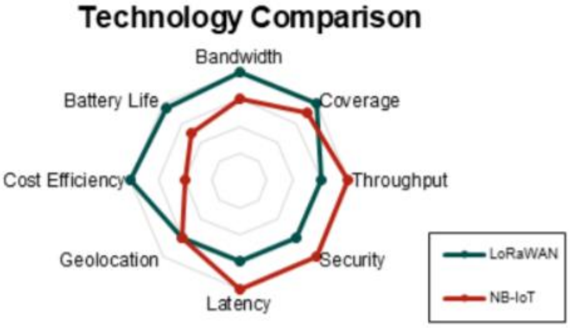
The MNO involvement is needed in terms of Service Level Agreement. Table 30 compare the main features of LoRAWAN and NB-IoT [136].

Table 30. LoRAWAN and NB-IoT comparison.

General Features (*)	LoRAWAN	NB-IoT
Spectrum	Unlicensed	Licensed
MNO involvement	NO	YES
Network	Customizable by end user	MNO proprietary
Typical coverage radius	1 km (urban), 10 km (rural)	15 km
Deployment cost	Low	High
Technology Parameters	**LoRAWAN**	**NB-IoT**
Bandwidth	125 kHz	180 kHz
Coverage	165 dB	164 dB
Battery Life	15+ years	10+ years
Peak Current	32 mA	120 mA
Sleep Current	1 µA	5 µA
Throughput	50 kbps	60 kbps
Latency	Device Class Dependent	< 10 s
Security	AES 128 bit	3GPP (128 to 256 bit)
Geolocation	YES (TDOA)	Yes (in 3GPP Rel 14)
Cost Efficiency (Device and Network)	High	Medium

Figure 72 depicts the radar diagram of the most important features of LoRaWAN and NB-IoT technologies.

Figure 72. Radar diagram of LoRaWAN and NB-IoT main features.



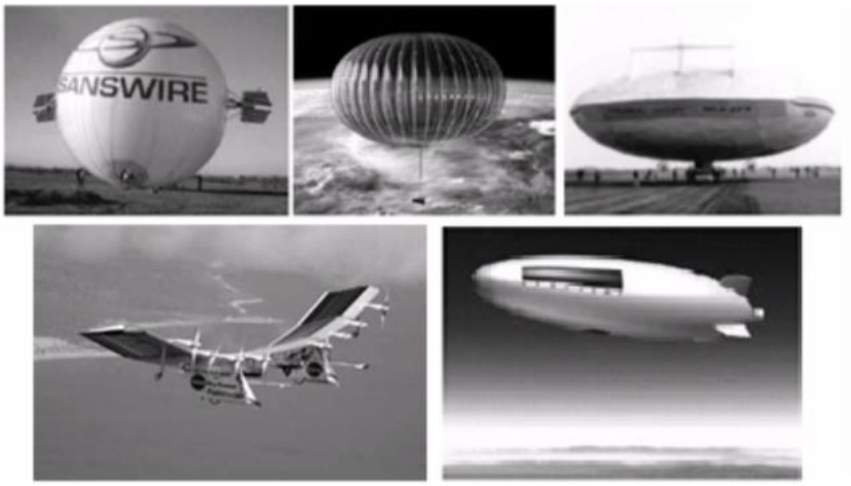
11. High Altitude Platform Station

11.1 Introduction

ITU Radio Regulations (RR) define High Altitude Platform (HAP) as radio stations located on an object at an altitude of 20-50 kilometers and at a specified, nominal, fixed point relative to the Earth [92]. High Altitude Platform Station (HAPS) operate for a large period at an altitude of around 20 km in order to extend the satellite services as Earth Observation, Telecommunication and Navigation.

Some companies are testing the possibility to offer the broadband access via HAPS using lightweight, solar-powered aircraft and airships staying at an altitude of 20-25 kilometers for a duration of several months (Figure 73). HAPS systems can provide both wireless broadband connections to the end user and backhauling links between the mobile and core networks, especially in remote areas, as mountains, coasts, and deserts.

Figure 73. Some successful HAPS vehicle shapes [92].



In particular situations, HAPS can be rapidly deployed, e. g. to provide disaster recovery communications or inter-HAPS links [92] [93] [94]. In 1996 ITU started the study on HAPS, but in the last years HAPS have gained more interested thanks to technologies as solar panel efficiency, power consumption, lightweight composite materials, autonomous avionics, and antennas. The World Radiocommunication Conference (WRC-19) facilitated the development and the adoption of HAPS services. The HAPS are also an important contribution to Sustainable Development Goal 9 (industry, innovation, and infrastructure) due to the possibility to offer broadband connectivity and telecommunication services in remote areas.

11.2 Network topology

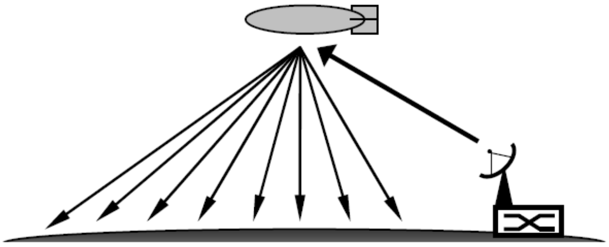
The HAPS operative modalities are mainly three [95]:

- HAPS as part of Radio Access Network
- HAP as an Independent System
- HAPS as Inter-Platform Links and satellite backhaul link

HAPS as a Part of a Radio Access Network

HAPS is used only as a base transceiver station (Figure 74). Subscribers (even served by one platform) are connected by a switching center installed on its surface.

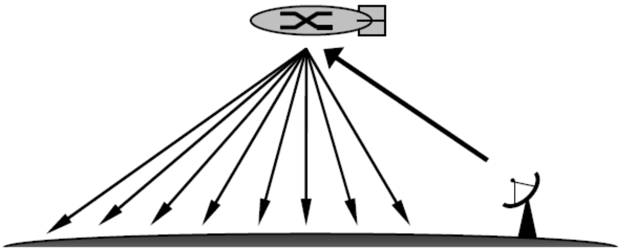
Figure 74. HAPS working as base transceiver station.



HAPS as an Independent System

If HAPS is an independent system, all devices (switching center included) are installed on board (Figure 75). The connection to the ground base station is used to communicate with other networks.

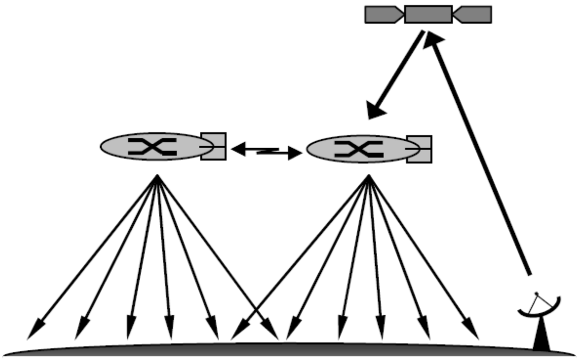
Figure 75. HAPs as an Independent System.



Connection with terrestrial network can be also put through the satellite link

Two or more HAPs can be interconnected through Inter-Platform Links (Figure 76). Optical links can be realized by optical and wireless technologies [96] and they can act as backhaul link to ground base station [97]. It reduces the usage of radio frequency bandwidths.

Figure 76. Two HAPS connected with Inter-Platform Link and with the satellite backhaul link.



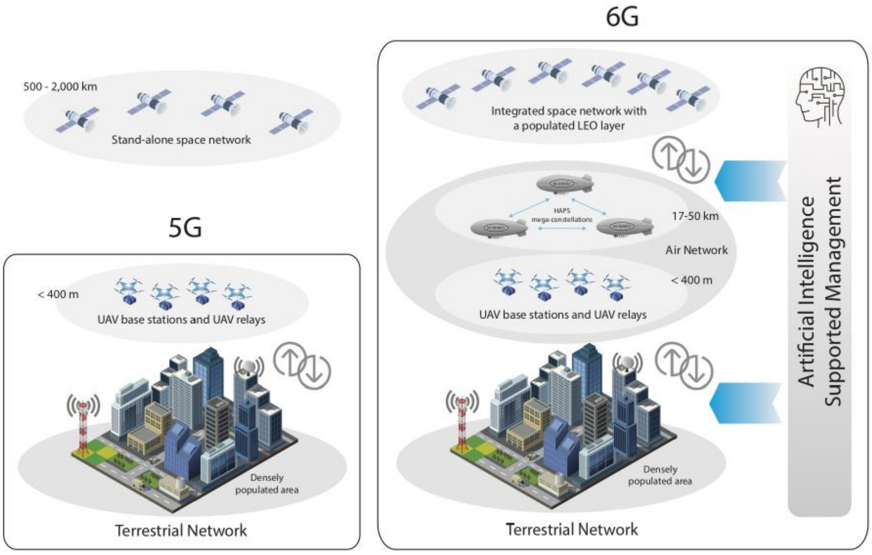
11.3 HAPS and VHetNet

The actual paper known in literature [93] [98] are focused on LTE-based HAPS. The necessity to support tens of Mbps of throughputs is a big issue. Since they support the usage of large bandwidth and millimeter wave (mmWave) systems, they are very important for 5G-based HAPS. In fact, the current mmWave systems are used for small cells (with a radius of a few hundred meters). Thanks to HAPS, a 5G nodeB (gNB) deployed can cover larger cells (with at least a few tens of kilometers). If we consider the current state-of-the-art of the Sixth Generation (6G) network architecture, a three-layer Vertical Heterogeneous Network (VHetNet) has been proposed. This vision is compliant with the 3GPP activities regarding the Non-Terrestrial Network (NTN).
The three layers are composed by:

- the satellites (space) network
- the aerial network
- and the terrestrial network

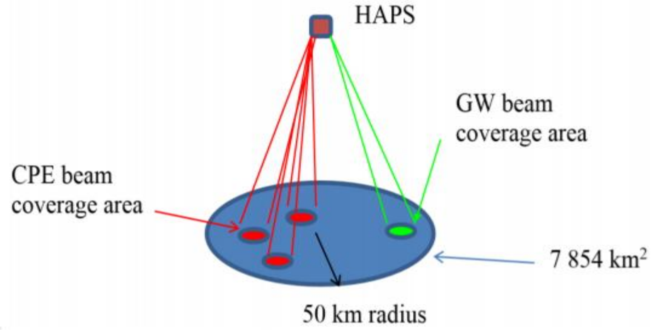
High Altitude Platform Station (HAPS) is an integral component of VHetNets. HAPS is a network node operating in the stratosphere, with an altitude around 20 km and a quasi-stationary position. Several research activities with HAPS were carried out in 1990s [99]. In the last years, HAPS have gained a lot of interest within the future networks. The energy source is an important issue for HAPS. In this context, solar power and energy storage are the primary energy source for HAPS, thanks to the large spaces used to accommodate solar panel films [100]. HAPS can also provide wireless services to the terrestrial networks [101] due to the intrinsic low-delay features. The possibility to create a constellation of HAPSs is also analyzed. They are called HAPS mega-constellation (similar to satellite mega-constellation) and they can provide access to high-capacity network, offloading of processing, and data analytics tools.

Figure 77. An overview of the transition from 5G to 6G. a fully integrated Vertical heterogeneous Network (VHetNet) is envisioned in 6G [93].


6G
500 - 2,000 km
Stand-alone space network
5G
< 400 m
UAV base stations and UAV relays
Densely populated area
Terrestrial Network
Integrated space network with a populated LEO layer
HAPS mega-constellations
17-50 km
Air Network
< 400 m
UAV base stations and UAV relays
Densely populated area
Terrestrial Network
Artificial Intelligence Supported Management

HAPS can be deployed quickly to cover wide service areas (e.g., with a 50 km radius), using a minimal ground infrastructure, as shown in Figure 78. They are reliable thanks to progress in aeronautics and energy consumption.

Figure 78. HAPS coverage area.



11.4 The frequency issues

In 1997, Radio Regulations (RR) identified the first frequency bands destinated to HAPS [91]. From that event, Radio Regulations have been updated with the additional frequency bands for HAPS. Three world radiocommunication conferences (WRC-97, WRC-2000 and WRC-12) identified the spectrum for HAPS in the frequency bands 47/48 GHz, 2 GHz, 27/31 GHz and 6 GHz respectively. The current ITU-R studies identify for HAPS systems a radio spectrum from 396 MHz to 2969 MHz in case of ground-to-HAPS platform links and from 324 MHz to 1 505 MHz in case of HAPS-platform-to-ground links [91]. Specific applications (e.g., disaster relief missions) and connectivity applications are foreseen. Since these frequencies are not sufficient for HAPS, in occasion of WRC-19, the ITU Member States agreed identify additional radio-frequency bands for HAPS systems.

ITU'S CONTRIBUTION and the frequency allocation

Delegates at WRC-19 agreed that the frequency bands 31-31.3 GHz, 38-39.5 GHz allocated to fixed services can be suitable for HAPS. They also confirmed the applicability of the 47.2 – 47.5 GHz and 47.9 – 48.2 GHz frequency bands for HAPS [102]. They agreed to:

- the use of the frequency bands 21.4-22 GHz and 24.25-27.5 GHz by HAPS in the fixed service in Region 2
- the limits regarding the link directions and protection of other services

11.5 Operative modalities

Solar cells and regenerative hydrogen-oxygen fuel cells are the efficient energy sources of HAPS. The HAPS uses a differential GPS sensor for controlling its position (with 400 m radius circle and a vertical dimension to ±700 m as altitude). HAPS total coverage area is divided into three zones, in order to provide a consistent broadband service across a coverage area around 1000 km in diameter.

The zones are (Table 31):

- **UAC**: it extends the coverage area from 36 to 43 km
- **SAC**: it extends the coverage area to 76.5/90.5 km, depending on the operating altitude
- **RAC**: its elevation angles are from 15° to 5°. It is dedicated to high-speed point-to-point access and wide-area coverage at lower frequency bands (e.g., from 800 MHz to 5 GHz bands)

Table 31. HAPS coverage areas.

Coverage area	Elevation angles (degrees)	Ground range (km)	
		Platform at 21	Platform at 25
UAC	90-30	0-36	0-43
SAC	30-15	36-76.5	43-90.5
RAC	15-5	76.5-203	90.5-234

A typical HAPS platform payload uses array antennas, able to control 700 beams in each of the UAC and SAC zones, and to perform an overage selection in the RAC zone up to 700 beams. A 7:1 frequency reuse factor is considered.

To maximize spectral efficiency, a Dynamic Assignment Multiple Access (DAMA) scheme is used for bandwidth sharing. For this purpose, Asynchronous Transfer Mode (ATM) switches and ATM multiplexers are used on board for the user traffic multiplexing. Both uplink and downlink use QPSK modulation. Interleave coding is also used to mitigate burst errors. Due to the efficient bandwidth sharing, it is estimated that a maximum upload speed of 2.048 Mbit/s and download speed of 11.24 Mbit/s (with a frequency allocation of only 2 × 100 MHz) can be offered to all 110560 users. Considering a contemporaneity coefficient of 10%, a single HAPS can serve one million users (with 2 × 100 MHz allocation) or more than five million subscribers (with to 2 × 300 MHz allocation).

The system also integrates Multiple Gateway Ground stations with Time Division Multiplexing (TDM) used for feeder traffic interconnecting HAPS-PSTN-Internet. The speed of feeder link is up to 0.72 Gbit/s for a 300/300 MHz frequency allocation. To optimize the available bandwidth, a 64-QAM modulation scheme is adopted. HAPS can support a very large number of users in densely populated areas. The following Table 32 summarizes the main issues related to HAPS and a first comparison with Very Low Earth Orbit (VLEO) & LEO satellite [103] [133].

Table 32. Issues related to HAPS and comparison with GEO, LEO and VLEO satellites.

Issue	High Altitude Platform
Deployment	Faster deployment than space-based platforms. Less “build -out” than terrestrial networks. Very fast response to emergency situations
Upgrading	Access to platform/ payload after deployment enables service upgradeability like terrestrial. Enhanced flexibility and adaptability
Link Budget	Shorter distances to HAPS make the Link budget favorable compared to satellite links. Smaller antenna coverage area permits high focus on areas of interest getting capacity higher density (x100) than GEO Satellites
	HAPS are quasi-stationary. This significantly reduces the Doppler shift due to platform motion
Ground Terminals	Smaller / simpler terrestrial terminals than satellite exhibit data rates
Free space path loss (dB)	~147 – 155 for HAPS, ~169 – 175 for VLEO, ~175 – 187 for LEO

Antenna Pointing & Directivity	Mobile LTE services and TETRA are based on omnidirectional links
Latency	Very low, equivalent to terrestrial networks. Latency ~ 10 ms versus ~30ms for LEO and ~250 ms for GEO
Geographic Coverage	Hundreds of miles per platform (~125 miles radius) between terrestrial (few miles) and space GEO (up to 33% of the Earth surface)
Operational altitude (km)	~20 – 50 for HAPS, ~250 – 500 for VLEO, ~ 500 – 2000 for LEO
Resource limitation	Low (empowered by solar battery charging for HAPS, high for VLEO and LEO
Mobility	Quasi-stationary for HAPS, fast for VLEO/LEO

According to [103], the following Table 33 summarizes the main capabilities of HAPS respect to Terrestrial and Satellite Systems for Telecommunications.

Table 33. HAPS Capabilities Compared to Terrestrial and Satellite Systems for Telecommunications.

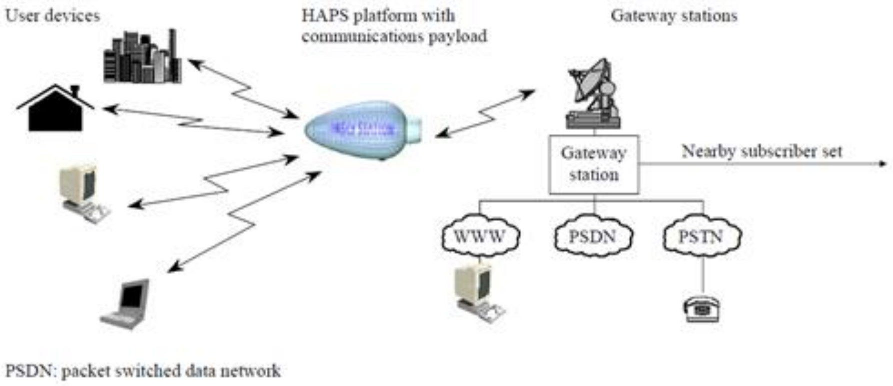
ISSUE	TERRESTRIAL	SATELLITE	HAPS
Health and safety	Low power handsets are used	GEO and MEO. High power handsets needed to overcome large path losses	Similar to terrestrial except for large coverage areas
Technology risk	Mature technology	New technology for LEO & MEO. GEO behind terrestrial in cost, volume & performance	Terrestrial wireless technology supported by spot beams. Research on smarter antenna in progress
Deployment timing	Development staged -substantial build-out to provide coverage	Entire system needs to be built to operate	BIG advantage: needs only one platform and one ground station to initiate operations
System growth	Easy upgradable. Cell splitting to increase capacity	Capacity is increased by adding new satellites. Hardware upgrades are possible if replacing satellites	Spot beam resizing and adding more platforms used to increase capacity; hardware upgrades easier than satellites

Complexity	User terminals are mobile. Operations well understood	Mobile satellites in LEO and MEO are complex.	Modern mobility platforms; operations not complex. Platforms need refueling.
RF Channel quality	Good signal quality through proper antenna placement	GEO distance limits spectrum. Ricean fading	Free space like channel at distances ~ terrestrial
Indoor coverage	Might be achieved. Research in progress on outdoor-to-indoor penetration	Not available due to large path loss at satellite communication frequencies	Coverage via repeaters but not outdoor-to-indoor penetration
Breadth of geographical coverage	A few miles per base station	Large regions in GEO. Global for MEO and LEO	100's of miles per platform
Cost	Varies. Much lower than satellite systems	>$200 MM for GEO; ~$2 Billion for LEO	~$50 MM but less than terrestrial network
Cell diameter	0.06214 -> 0.6214 miles	31 miles for LEO; 310 miles for GEO	0.6214 to 6.214 miles

11.6 HAPS Communication performance

HAPS network topology is a star configuration, the HAPS platform acts as the main hub [104], as shown in Figure 79.

Figure 79. HAPS network configuration.


User devices
HAPS platform with communications payload
Gateway stations
Gateway station
Nearby subscriber set
WWW
PSDN
PSTN
PSDN: packet switched data network

User terminals are portable devices that communicate with the satellite payload, deputed to switch the user-to-user communications through an ATM switch. Gateway stations allow user access to the existing public networks (e.g., Public Switched Telephone Network (PSTN) and the Internet).

Typically, gateway stations are placed in carrier central office (CO) or an Internet service provider (ISP) point-of-presence (PoP). Inter-HAPS communications can be performed by gateway stations, with a capacity of 4-12 Gbit/s (around the 60% of all user traffic). The total capacity of the payload is therefore 11-33 Gbit/s. The HAPS can provide variable rate, full duplex and small office/home office (SOHO), supporting multimedia applications (e.g., videoconferencing) together with the broadband Internet access.

The HAPS system uses a couple of bands in the 47.2-48.2 GHz frequency range, with a bandwidth of 100 MHz to 300 MHz. Each uplink TDMA time slot carries one single ATM cell.

11.7 HAPS Enablers and applications

The enablers for HAPS are [105]:

- Satellite Communications (SatCom):
    - ✓ to deploy and remotely command and control HAPS, offering a higher flexibility in their mission
    - ✓ to relay remote sensing data collected by HAPS' payload to the ground
    - ✓ to relay data between gateways and HAPS, when HAPS is used for providing broadband/broadcast connectivity
- Satellite navigation (SatNav)
    - ✓ for navigation purposes, relying on GNSS systems and possibly complemented with satellite augmentation systems such as EGNOS
    - ✓ for geo-localising EO data collected by HAPS sensors
- Satellite Earth Observation (SatEO)
    - ✓ to provide an enhanced operational picture to end users, via the fusion of data collected by remote sensing satellites with data from HAPS

From the application point of view, the following Table 34 summarizes the most important ones for HAPS [103] [106].

Table 34. HAPS Platform Advanced Telecommunications Services in various stages of engineering and development.

Dream	Service
Direct-To-Home (DTH)	DTH broadband: useful in unserved areas with no infrastructure or poor connectivity. Mimics a satellite or terrestrial tower
Trunking	Large number of users under a HAPS footprint can connect and share a single satellite connection. Good balance between coverage and signal degradation
Backhauling	HAPS provides very high capacity backhaul links between network nodes (cell towers) and backbone. Costly optical fiber or terrestrial microwave links are avoided
High Throughput	HAPS service to Offload congested GEO spot beams
Tactical	Communication usually in UHF, HAPS services are scalable, agile, reliable, affordable, defendable, rapidly deployable and requires minimum in theater ground infrastructure

Mobile Broadband	Normally provided by terrestrial wireless networks. If none available existing satellite (Iridium, Inmarsat, etc.) can provide. HAPS provides a higher capacity equivalent due to favorable link budgets
5G	HAPS infrastructure supports 5G services.

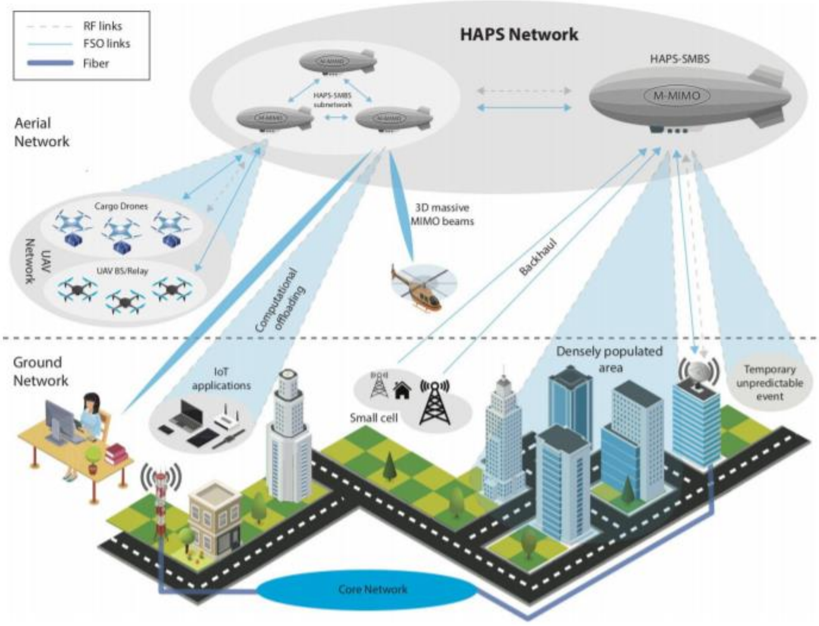
11.8 HAPS advantages

The main advantages provided by HAPS are [107]:
Favorable channel conditions: The lower altitude and the Line Of Sight (LoS) cause a low channel attenuation for HAPS, with a high signal-to-noise ratio (SNR) for the downlink.
Geostationary positions: The position of a HAPS is relatively stationary, with an attenuated Doppler effect and an efficient performance in terms of capacity and mobility management.
Smaller footprint compared to satellites: The small dimensions of HAPS provide a higher throughput in a specific area.
Large platform: the position of HAPS can be considered in a cylinder with a 400m radius of 400 m and ±700 m altitude [10]. For this reason, it enables Multiple Input Multiple Output (MIMO) and massive-MIMO (M-MIMO) communications.
Even lower latency: due to its low altitude, HAPS also provides a distance from 40 km to 100 km, corresponding to a Round Trip Delay (RTD) from 0.13 ms to 0.33 ms. For this reason, HAPS is suitable for low latency applications.
Hybrid connectivity: ITU has defined a spectrum bandwidth of 600 MHz for HAPS [107]. In addition to this, Free Space Optics (FSO) is a good candidate for multi-connectivity (RF combined with FSO) and high data rate communications.

11.9 HAPS Super Macro Base Station (HAPS-SMBS)

HAPS as based Super Macro Base Station (HAPS-SMBS) is the most important approach to HAPS [107], as shown in Figure 80. HAPS-SMBS can be very useful to the terrestrial network as response to a continuous growing of the demand for connections.

Figure 80. Representation of target use cases of HAPS-SMSBS networks [107].



The main features of HAPS-SMBS are:

HAPS-SMBS for IoT applications: HAPS-SMBS is very important for IoT applications due to its capability both to manage many low power and low-cost devices and to offer a large coverage.

HAPS-SMBS for backhauling outdoor small cell BSs: Recent research on HAPS and FSO evidence their applicability to backhauling small cell BSs [109]. Figure 80 shows the achievable data rate of an FSO link.

HAPS-SMBS to cover temporary unpredictable events: HAPS-SMBS can provide additional coverage to avoid network congestion in particular situations.

HAPS-SMBS to support agile computational offloading: HAPS-SMBS are very useful for off-loading the computation and processing activities.

HAPS-SMBS as a flying data center: HAPS-SMBS can host flying data centers with a data back-up features.

HAPS-SMBS for coverage holes: HAPS-SMBS can support the terrestrial networks by providing coverage holes.

HAPS-SMBS to cover a massive amount of aerial UE: HAPS-SMBS can also be used for providing coverage for multiple aerial UE and autonomous drones in a platoon configuration.

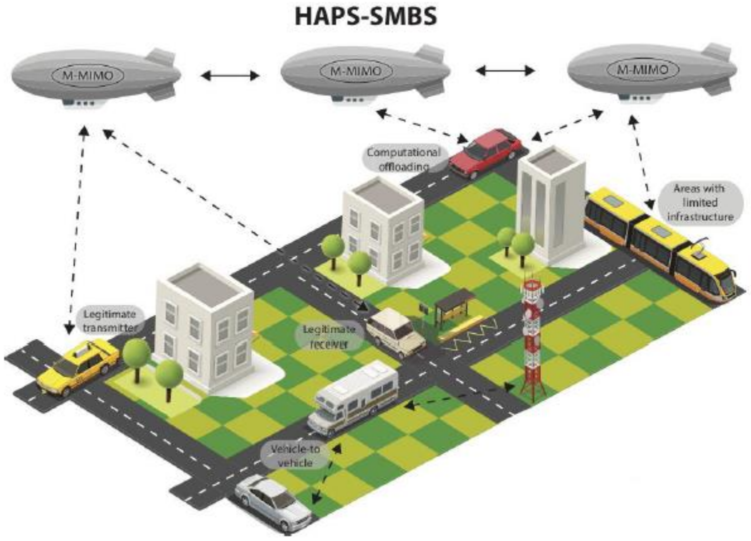
HAPS-SMBS as an intelligent aerial network enabler: HAPS-SMBS can provide computational support for limited-resources aerial network nodes (e.g., artificial intelligence, machine learning).

HAPS-SMBS as an interface to provide seamless communication to LEO satellites: since LEO satellites are affected by numerous disconnections and handovers, HAPS-SMBS can support the frequent handover of LEO satellites.

11.10 HAPS for mobility

HAPS-SMBS are very important for the ubiquitous coverage of intelligent transportation systems (ITS)/connected and autonomous vehicle (CAV) scenarios (Figure 81), requiring extra resources for an efficient data fusion and processing. In ITS sector, vehicles are characterized by a considerable mobility and by numerous handovers. In this context, HAPS-SMBS can provide both large coverage and processing features with low delay transmission, reducing the frequent handovers in vehicular networks.

Figure 81. HAPS-SMSBS constellation to support ITS applications.

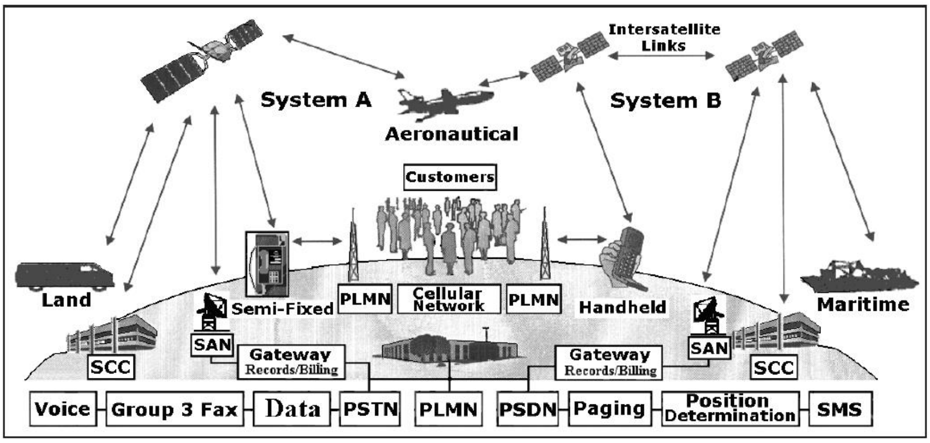


12. Low Earth Orbit (LEO) Satellite

12.1 Introduction of the LEO Systems

The Low Earth Orbit (LEO) systems are satellites with elliptical or circular orbits between 500 and 2000 km above the Earth surface and below the Inner Van Allen Belt, as shown in Figure 82. The orbit period goes from 90 minutes to a couple of hours [110], while the radius of LEO system from 3,000 to 4,000 km.

Figure 82. LEO System concepts [ITU].



When a satellite goes down below the local horizon, a rapid handover procedure is needed involving other satellite in the same/adjacent orbit [111]. LEO satellites are affected by atmospheric drag, LEO/MEO (Medium Earth Orbit) satellites by orbital perturbation and very LEO (VLEO) satellites by aerodynamic drag and precession of the perigee argument. A multi-satellite constellation is more robust since the orbit perturbation disturbs all satellites of the constellation in the same way [112]. The major advantages of LEO satellites are as follows:

a) LEO can cover areas not server by mobile systems, providing broadband data communications.
b) LEO can support satellite positioning and tracking applications.
c) Due to the small distance between them and gateway stations, LEO can connect terminals with low power and reduce the speed-of-light propagation delay.
d) The spatial diversity of satellite paths can avoid the signal interruption caused by the path obstruction.

The disadvantages of LEO are as follows [113]:

a) With an altitude of 1,000 km, the orbit period of LEO satellite is about 100 min. It requires from 40 to 80 satellites deployed on six or seven planes. A LEO multi constellation requires a considerable number of satellites, increasing the network cost.
b) Numerous handovers are necessary in order to maintain the communications.
c) Due to the eclipsed about one-third of the orbit period, LEO needs a lot of energy amount, with up to 5,000 charge/discharge cycles per year. In this way, the LEO lifetime is reduced to 3–7 years.
d) A minimum number of 40 satellites is considered for direct launch into the orbit of several satellites. So, the total cost increases considerably.

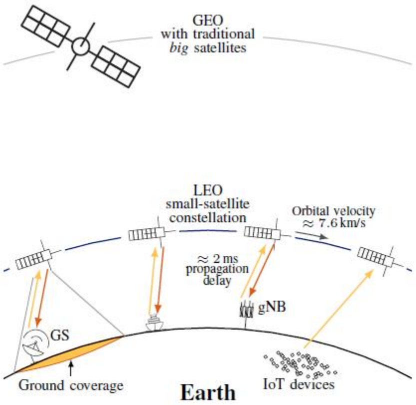
12.2 LEO Constellations

LEO Constellations are very attractive for supporting and integrating 5G New Radio (NR) and Beyond-5G (B5G) communications [114] - [118] and they are deployed at altitudes from 500 and 2000 km. The integration with 5G NR will increase the covered areas for the following applications:

1) enhanced mobile broadband (eMBB)
2) massive Machine-Type Communications (mMTC)
3) Ultra-Reliable Communications (URC)

On the contrary of Unlike Geostationary Earth Orbit (GEO) satellites, LEO satellites have a high speed (with respect to the Earth) and small ground coverage, as shown in Figure 83. For example, the coverage of a LEO satellite deployed at 600 km altitude and with an elevation angle of 30° is around 0.45% of the Earth's surface. Due to the low altitude, LEO satellites can communicate with several ground terminals, as ground stations (GSs), 5G gNBs, ships, vehicles, IoT devices.

Figure 83. Overview of the unique characteristics of LEO small-satellite constellations with respect to traditional GEO satellites [114].



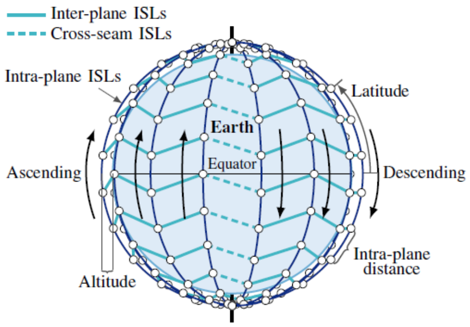
12.3 LEO Physical links

The LEO physical links can be [114]:

- Ground-to-Satellite Link (GSL)
- Inter-satellite link (ISL)

A GSL link between a Ground Station (GS) and a satellite is also named "feeder link". A GSL is available by the ground coverage and the orbital velocity (see the previous Figure 83). LEO satellites are characterized by high orbital speed and short movements. Numerous handovers are needed in order to maintain the connections with the ground terminals. An ISL links can be divided into intra-plane and inter-plane ISL. The first ones are referred to satellites in the same orbital plane, while the second ones to satellites in different orbital planes. Figure 84 illustrates a Walker star constellation formed by seven orbital planes.

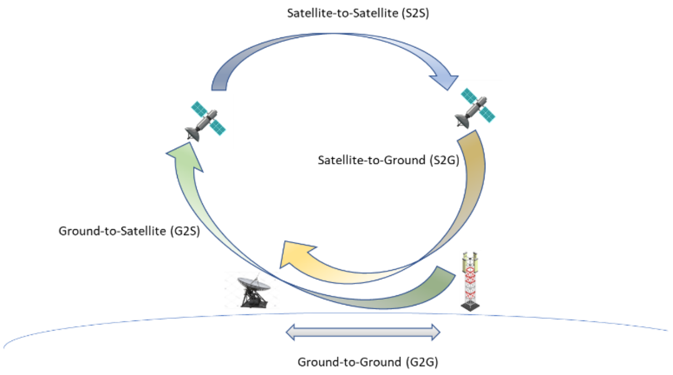
Figure 84. Diagram of a Walker star LEO constellation with the established intra- and inter-plane (including cross-seam) ISLs.



12.4 LEO Logical links

In a LEO system a satellite [S] and a ground terminal [G] are the two endpoints that can establish four logical links, as shown in Figure 85. A logical link can use one or more physical links, GSL and ISL [114].

Figure 85. Sketch of the four logical links in a LEO constellation.


Satellite-to-Satellite (S2S)
Satellite-to-Ground (S2G)
Ground-to-Satellite (G2S)
Ground-to-Ground (G2G)

The following Table 35 summarizes the classification of logical links for a LEO system.

Table 35. Classification of logical links for a LEO system.

Logical link	Details
Ground to ground [G2G]	In this case, the information is relayed between two distant points on the ground. It is also used for handover, routing, and coordination of relays.
Ground to satellite [G2S]	It is used for maintenance and control operations initiated by the ground station (e.g., ISL establishment and routing, caching and telecontrol).
Satellite to ground [S2G]	It is important when the satellites collect and transmit application data (e.g., Earth observation), for handover and link establishment with GSs, radio resource management (RRM), fault detection, and telemetry.
Satellite to satellite	It is relevant for satellite-related control applications (e.g., distributed

[S2S]	processing, sensing, and routing), topology management, link establishment, etc.

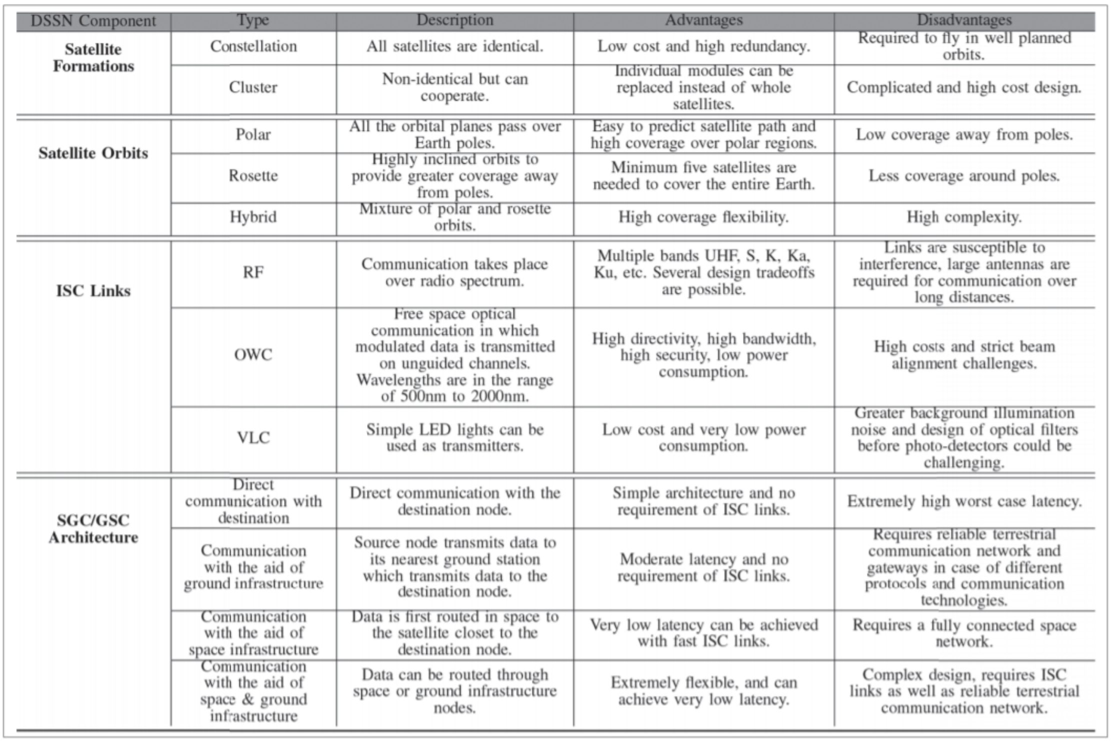
12.5 LEO and Dense Small Satellite Networks (DSSN)

In the last years LEO satellites gained more interest due to the growing demands for high data rate applications, massive connectivity, universal internet access, IoT and wireless sensor networks (WSNs) [120]. LEO satellites typically weigh less than 500 kg and have lower both costs for development/launch and propagation delays than the traditional MEO and GEO satellites. On the other hand, LEO satellites have less features and resources. Several companies as SpaceX, OneWeb, Kepler, and SPUTNIX have announced the launch of thousands of satellites constituting Dense Small Satellite Networks (DSSN).

DSSN INFRASTRUCTURE

LEO satellites in DSSN configuration are placed at altitudes from 160 km to 2000 km. These have high speed (several thousand km/h). Table 36 summarizes the most important features of DSSN.

Table 36. Dense Small Satellite Networks (DSSN) Infrastructure.



DSSN Component	Type	Description	Advantages	Disadvantages
Satellite Formations	Constellation	All satellites are identical.	Low cost and high redundancy.	Required to fly in well planned orbits.
	Cluster	Non-identical but can cooperate.	Individual modules can be replaced instead of whole satellites.	Complicated and high cost design.
Satellite Orbits	Polar	All the orbital planes pass over Earth poles.	Easy to predict satellite path and high coverage over polar regions.	Low coverage away from poles.
	Rosette	Highly inclined orbits to provide greater coverage away from poles.	Minimum five satellites are needed to cover the entire Earth.	Less coverage around poles.
	Hybrid	Mixture of polar and rosette orbits.	High coverage flexibility.	High complexity.
ISC Links	RF	Communication takes place over radio spectrum.	Multiple bands UHF, S, K, Ka, Ku, etc. Several design tradeoffs are possible.	Links are susceptible to interference, large antennas are required for communication over long distances.
	OWC	Free space optical communication in which modulated data is transmitted on unguided channels. Wavelengths are in the range of 500nm to 2000nm.	High directivity, high bandwidth, high security, low power consumption.	High costs and strict beam alignment challenges.
	VLC	Simple LED lights can be used as transmitters.	Low cost and very low power consumption.	Greater background illumination noise and design of optical filters before photo-detectors could be challenging.
SGC/GSC Architecture	Direct communication with destination	Direct communication with the destination node.	Simple architecture and no requirement of ISC links.	Extremely high worst case latency.
	Communication with the aid of ground infrastructure	Source node transmits data to its nearest ground station which transmits data to the destination node.	Moderate latency and no requirement of ISC links.	Requires reliable terrestrial communication network and gateways in case of different protocols and communication technologies.
	Communication with the aid of space infrastructure	Data is first routed in space to the satellite closet to the destination node.	Very low latency can be achieved with fast ISC links.	Requires a fully connected space network.
	Communication with the aid of space & ground infrastructure	Data can be routed through space or ground infrastructure nodes.	Extremely flexible, and can achieve very low latency.	Complex design, requires ISC links as well as reliable terrestrial communication network.

Satellite Formations

Large number of small satellites may be deployed in two different configurations:

1) Constellation: there are multiple copies of the same satellite, with same hardware and functionalities.
2) Cluster: it is a group of different satellites cooperating with a specific role.

Constellation is the preferred configuration due to the simple manufacturing and deployment costs of DSSN.

Satellite Orbits

LEO can be deployed in a DSSN scheme using several orbital planes characterized by different altitudes and inclinations. For this reason, it is crucial to design the right orbital planes for DSSN and then to predict the best ones to facilitate handovers, energy savings, positioning, and resource allocation.

The traditional methods to design satellite orbits are the following:

1) Polar: all the orbital planes have one/more satellites and overcome Earth poles;
2) Rosette: orbital planes are highly inclined with respect to equator. Almost five satellites are needed;
3) Hybrid: it is a combination of the previous methods, useful to plan coverage in different areas;

Inter-Satellite Communication

A network of satellites as DSSN need ISC links, since they provide communication and cooperation services (e.g., routing, throughput and latency management, etc.) [120].

The following technologies can also be used for satellite-to-ground communication (SGC) and ground-to-satellite communication (GSC) links:

1) Radio Frequency (RF) links: There are several RF bands suitable for ISC links
2) Optical Wireless Communication (OWC) links: light signals are modulated and transmitted in free space using lasers with wavelengths from 500 nm to 2000 nm. However, the costs for OWC links are expensive
3) Visible Light Communication (VLC) links: LED lights transmit signals in Visible Light Spectrum (350 nm – 750 nm). Due to the presence of sun background illumination in LEO orbits[4], optical filters must be installed before the photodetectors. The use of VLC is suitable for links with short and medium range.

In DSSN configuration, ISC links are characterized by satellite weight and power autonomy. Smart antennas with high gain, multi-band, and multi-beam can make robust the transmissions [121] [122] during a dynamic behavior of the network topology.

SGC / GSC System Architectures

If we consider the source node (in DSSN) and the destination node (on ground), the SGC system architecture for Mobile Terrestrial Communication Systems (MTCS). The four communication paths are shown in Figure 86.

Figure 86. SGC system architectures in various MTCS scenarios.

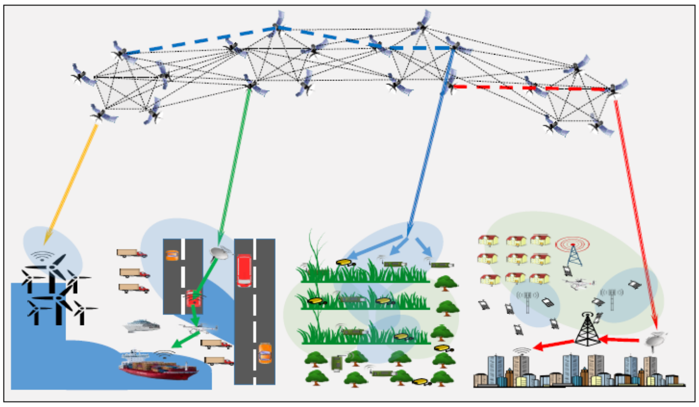


Table 37 summarizes the most important information of them.

[4] Around 580 W/m^2

Table 37. Main features of communication paths of SGC/GSC systems.

Communication Path	Details
Direct communication with destination	In this communication system architecture, source node in DSSN directly communicates with the destination node on ground. LEO satellites are non-stationary and in this case source node can only communicate when the destination node is in its coverage area. This is a simple architecture, and it can be used when DSSN does not support ISC links and there is no supporting communication infrastructure on ground.
Communication with the aid of ground infrastructure	In this communication system architecture, when the source node has data for the destination node it immediately transmits this data to its nearest ground station. Once the data is at the ground station, it is transmitted to the destination node using traditional terrestrial communication networks. This method is also helpful when DSSN has no ISC links. Latency would primarily depend on the performance of the terrestrial network.
Communication with the aid of space infrastructure	This communication system architecture is only possible in DSSN with ISC links. In this method, data is first routed from source node to the satellite closest to the destination node. The intermediate DSSN satellite then transmits data to the destination node. This approach has the potential to drastically reduce latency.
Communication with the aid of space & ground infrastructure	This is the most flexible communication system architecture. In this architecture, the source node transmits information through intermediate satellites and ground infrastructure for faster delivery of data. This method can make the best use of all the available resources but it requires the availability of DSSN with ISC links and ground infrastructure.

12.6 LEO and Security

Ground Segment Threats

The ground segment includes both satellite communications transmission and reception devices, as GPS receivers [123]. It can be affected by malicious attacks, both at physical and network layers, as summarized by Table 38. The first ones are related to the diffusion of bomb-making techniques and explosive materials, while the second ones to Denial of service (DoS) through detected probes and scans.

Table 38. Vulnerabilities of LEO Ground Segment.

Vulnerability
Physical attack
Computer network intrusion
Jamming
Bomb-making techniques and explosive material

Communications (Link) Segment Threats

Both the ground-segment and the space-segment nodes are connected through links [123] identified as control or mission links. Control links are used to manage the satellite, while mission links are referred to data exchanged with satellite. These links can be affected by multiple attacks. The Table 39 summarizes the vulnerability and the corresponding details for Communications (Link) Segment.

Table 39. Vulnerabilities of LEO Communications (Link) Segment.

Vulnerability	**Details**
Uplink Jamming	There are two types of satellite uplink signals: signals for retransmission (payload signals such as TV and communications) and the command uplinks to the satellite. Uplink jamming against a payload signal is an attractive EA strategy because all recipients of the target transmission are affected. The jamming uplink signal is a radio frequency (RF) signal of approximately the same frequency as the target uplink signal. It is transmitted up to the satellite onto the same transponder as the target signal and affects the transponder's ability to distinguish the true signal from the jamming signal.
Downlink Jamming	There are two main targets for downlink jamming: SATCOM broadcasts and navigation satellite (NAVSAT) broadcasts. In a downlink jamming scenario, the objective of the EA is to disrupt or temporarily keep the spacecraft's transmission (communication or navigation signal) from being received by select ground users. A downlink jamming system accomplishes this by broadcasting an RF signal of approximately the same frequency as the targeted downlink signal but with more power. This jamming signal is transmitted toward a terrestrial (ground-based) or airborne satellite downlink reception antenna where it overpowers the satellite's signal. With smart jamming (vice brute force jamming), the jamming signal attempts to emulate the satellite's signal and, if successful, can provide the targeted user with false data or information.
Spoofing	Spoofing is the ability to capture, alter, and retransmit a communication stream in a way that misleads the recipient. Attacking the communication segment via spoofing involves taking over the space system by appearing as an authorized user. Once established as a trusted user, false commands can be inserted into a satellite's command receiver, causing the spacecraft to malfunction or fail its mission.

Space Segment

Attacks in the space segment are very expensive and difficult to realize [123] and can be related to energy (laser and high-powered RF). An attacker can be interested in destroying aerial devices. Table 40 summarizes the Vulnerabilities of LEO Space Segment.

Table 40. Vulnerabilities of LEO Space Segment.

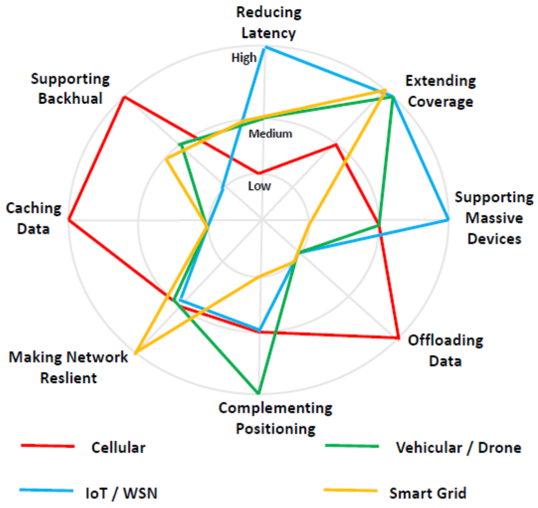
Vulnerability	Details
Kinetic-Energy Weapons	Kinetic-impact weapons cause structural damage by impacting the target with one or more high-speed masses. Small pieces of debris can inflict substantial damage or destroy a satellite.
Directed-Energy Weapons	Directed-energy weapons include laser, RF, and particle-beam weapons. Directed energy weapons are considered “standoff” weapons because they are primarily either ground- or air-based systems that never get very close to their target. Most of these concepts are technically sophisticated and attack the target from longer ranges than most kinetic interceptors. In addition, these technologies are capable of engaging multiple targets, whereas interceptors tend to be single-shot systems.
Laser Weapons	Laser systems, including coherent radiation, aligned waveform, and other devices operating at or near the optical wavelengths, operate by delivering energy onto the surface of the target. The gradual or rapid absorption of this energy leads to several forms of thermal damage. Generally, an antisensor laser weapon could be used against satellites at any altitude. This leads to the requirement for the laser beam to propagate over very long ranges (tens to hundreds or even thousands of kilometers) and still deliver lethal power to the target.
Radio Frequency Weapons	RF weapons concepts include ground- and space-based RF emitters that fire an intense burst of radio energy at a satellite, disabling electronic components. RF weapons are usually divided into two categories: high-power microwave (HPM) weapons and ultrawideband (UWB), or video pulse, weapons. UWB weapons generate RF radiation covering a wide frequency spectrum—nominally from about 100 MHz to more than 1 GHz—with limited directivity. Because of the UWB weapon’s low-energy spectral density and directivity, permanent damage to electronic components would be very difficult to achieve, except at very short ranges. The UWB enters through the satellite’s antenna at it receive frequency, as well as through openings in the system’s shielding. If enough power is applied, the received radiation may cause major damage to the satellite’s internal communications hardware.
Particle-Beam Weapons	Particle-beam weapon concepts are space-based systems that fire an intense beam of elementary particles at a satellite, disabling electronic components. These weapons accelerate atomic particles, such as negative hydrogen or deuterium ions, to relativistic velocities (significant fractions of the speed of light) toward their target. They can cause permanent damage by radiating enough energy to overload the satellite’s internal electronics.
Interceptor Types	Interceptor systems and system concepts can be divided into a number

	of distinct categories: low-altitude, direct-ascent interceptors; low-altitude, short-duration orbital interceptors; high-altitude, short-duration orbital interceptors; and long-duration orbital interceptors. These weapons are typically ground- or air-launched into intercept trajectories or orbits that are nearly the same as the intended target satellite. Radar or optical systems on board the satellite guide it to close proximity of the target satellite
Long-Duration Orbital Interceptors	The long-duration orbital system is an orbital interceptor that is launched into a storage orbit for an extended period of time, possibly months to years, before it maneuvers to engage and attack the target satellite. The weapon may be stand-alone or covertly placed on or in a "mothership" satellite. Feasible concepts, in order of increasing sophistication, include the farsat, nearsat, space mine, fragmentation or pellet ring, and space-to-space missile

12.7 LEO Applications

The most important benefits and applications of DSSN systems for MTCS are depicted in the following Figure 87 [119].

Figure 87. Potential DSSN benefits for MTCS.



The following Table 41summarizes the most important benefits of DSSN systems for MTCS [119].

Table 41. Benefits of DSSN systems for MTCS.

Benefits of DSSN for MTCS	Details
Extending Coverage	A wide area coverage can influence mobile users, sensors, and vehicles in remote, challenging, and under-developed regions. Extended coverage through DSSN can also benefit several smart grid applications such as, remote monitoring of offshore renewable wind farms, distributed sub-stations, and transmission & distribution networks. It can also provide autonomous vessel support, which cannot be easily done with today's telecom networks. A single LEO satellite can approximately cover 1 million km^2 area on Earth. Due to huge coverage area of each satellite, spot beam coverage and hybrid wide-spot beam coverage schemes are typically employed. In spot beam coverage scheme, each satellite provides multiple spot beams whose footprint on Earth also moves along with the satellite trajectory.
Increasing throughput	Due to the large amount of nano-satellites and the aggregated bandwidth, DSSN allows an efficient throughput increase. This aspect should be balanced with the deployment cost.
Reducing Latency	Due to lower altitude orbits, round trip time of signals between a LEO satellite and a ground terminal is only few ms (30 ms for OneWeb system and 10-15 ms for SpaceX Starlink system). This latency is enough to fulfill the requirements of many IoT, smart grid, and vehicular communication applications. The objective of cellular systems such as, 5G and beyond is to achieve 1 ms latency, which cannot be directly attained with the help of DSSN. However, DSSN may indirectly facilitate 5G networks in reducing latency by providing alternate backhaul and data caching options. It is also important to note that as compared to free space, the speed of light is 30-40% slower in fiber. Therefore, for long distance communication, DSSN has the potential to provide lower latency as compared to any terrestrial network of comparable length. However, due to relative movement between satellites, latency may vary, communication links may become unstable and handovers may increase.
Supporting Massive Devices	DSSN is also more cost-efficient for IoT devices deployed in deserts, forest, oceans and other challenging areas. Due to the mobility of LEO satellites, devices can communicate with LEO satellites at different elevation angles thus providing more tolerance to terrestrial obstacles. Path loss due to lower orbital altitudes of LEO satellites is also smaller, which can help support more low-powered devices. However, key challenges include, interoperability issues, efficient medium access protocols, and optimization of available resources.
Offloading Data	DSSN can be integrated in cellular networks by creating LEO small cells (LSC). In LSC, a terrestrial node with satellite connectivity acts as a base station (BS) and serves multiple cellular users. LSCs can coexist with traditional small cells or macro BS. In this arrangement, some data traffic can be offloaded from the terrestrial network. LSCs maybe set up in areas with heavy traffic spikes or in rural areas with no terrestrial communication

	networks. LSCs can also be dynamically created in geographical regions experiencing demand spikes with the help of Unmanned Aerial Vehicle (UAV) and autonomous vehicles. Such setup is more useful in dense urban environments with huge data rate demands or in highly stressed data networks, and would require advance traffic prediction algorithms. Such integration opportunities can also be exploited in any MTCS supporting a large number of devices with limited resources and can further enhance network resilience.
Complementing Positioning	The knowledge of exact location of user or device is often required to provide useful location-based services. In cellular systems, prediction of user or device mobility can facilitate content caching. In vehicular communication systems, positioning and navigation are essential to avoid accidents. In IoT and smart grid networks, positioning may also be needed for asset tracking. DSSN can complement GPS by providing an alternate way to determine the location of users and devices whenever GPS signals are out of range. The high mobility of LEO satellites results in an extremely large Doppler shift and Doppler frequency rate of change. With some information about satellite orbits and positions, ground receivers can use Doppler measurements for localization. Furthermore, time difference of arrival and frequency difference of arrival measurements can also be used to determine the location of the ground receiver. However, achieving very high positioning accuracy with DSSN is an open research challenge.
Making MTCS more Resilient	DSSN can enhance the overall resilience of MTCS. Network congestion and overloading can be avoided with the help of additional and redundant DSSN connections. These connections would also be valuable in case of emergency and disasters scenarios. For critical smart grid infrastructure, resilient communication network is also critical. DSSN is more tolerant to extreme topographies and is also more robust against challenging terrestrial environments.
Caching Data	Data caching entails storing popular or frequently accessed content closer to the end users. It is an important method to reduce latency and backhaul congestion in cellular networks. With vast coverage, DSSN can help bring content closer to the end users. To save resources in terrestrial networks, some data can also be cached in DSSN. Satellites in DSSN also can multi-cast data and quickly update the cached content at multiple locations. Development of effective caching strategies involving DSSN are interesting research directions. The use of information centric networking paradigm in which the content can be retrieved by its name and every network node has some cache space can also be explored for managing content caching and content delivery in such systems. However, each LEO satellite has limited storage and computing capabilities, therefore, limited content placement opportunities exist, which could also create strong competition among MTCS, and several interesting game theoretic models may be applied to determine the price of data caching in DSSN.
Supporting Backhaul	The amount of traffic generated by users and devices is exponentially increasing. Ultra-dense deployment of small cells is a major technique to support huge traffic demand in 5G networks. However, data generated in these small cells and frequent handover requests due to user mobility can

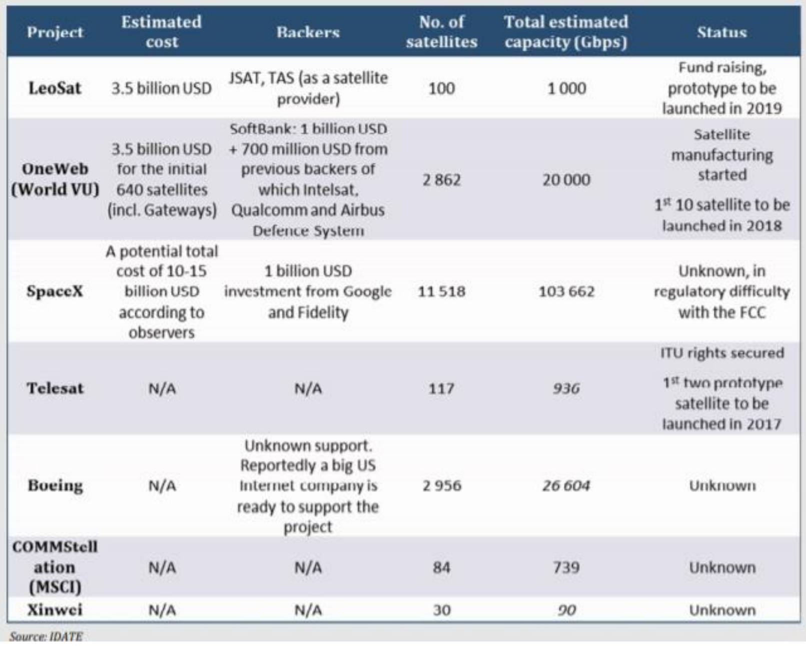
	put huge pressure on the backhaul resources. DSSN can help resolve backhaul capacity issues by providing wideband communication links. Multiple LEO satellites also provide more dimensions for backhaul capacity maximization. Backhaul capacity of DSSN links can dynamically vary depending on the satellite orbital paths and the technology used on various communication links. These variations can be exploited to advantage through developing dynamic scheduling and resource optimization algorithms.

12.8 LEO market

The European Commission in “Low-Earth Orbit satellites: Spectrum access” analyzed the LEO satellites and the network densification to increase the communication capacity, reduce the transmission latency and the stimulate the market [124]. More than 15 LEO projects have been carried out in the 2014-2017 period and with new players interested in this context. Three of the most known projects are carried out by OneWeb, LeoSat and SpaceX. All these LEO projects will bring more than 17,000 satellites with an overall capacity of more than 150 Tbps. The main question about it is about the possible success of all players. It is more probable that only a few players will succeed in launching their constellation. With their capability to drastically reduce the cost to deliver 1 Gbps, LEOs could indeed stimulate the competition in some markets, but they can also cause economic difficulties even to the biggest satellite operators traditionally present in the market (e.g., Intelsat, Eutelsat, SES…). The race for a connectivity through cheaper satellite is still on going. GEO connectivity prices have already decreased in the last years. Considering 3 satellites, the cost to produce a 1 Gbps capacity could be below the 1 million USD price.

In a competitive environment, LEO and MEO satellites are considered ss complementary to GEO satellite. If LEO satellites can provide high capacity and low latency communications suitable for the new bandwidth-consuming applications, GEO satellites remains the most adapted for broadcast applications.

Table 42. Main broadband-focused LEO constellations.



Project	Estimated cost	Backers	No. of satellites	Total estimated capacity (Gbps)	Status
LeoSat	3.5 billion USD	JSAT, TAS (as a satellite provider)	100	1 000	Fund raising, prototype to be launched in 2019
OneWeb (World VU)	3.5 billion USD for the initial 640 satellites (incl. Gateways)	SoftBank: 1 billion USD + 700 million USD from previous backers of which Intelsat, Qualcomm and Airbus Defence System	2 862	20 000	Satellite manufacturing started 1st 10 satellite to be launched in 2018
SpaceX	A potential total cost of 10-15 billion USD according to observers	1 billion USD investment from Google and Fidelity	11 518	103 662	Unknown, in regulatory difficulty with the FCC
Telesat	N/A	N/A	117	*936*	ITU rights secured 1st two prototype satellite to be launched in 2017
Boeing	N/A	Unknown support. Reportedly a big US Internet company is ready to support the project	2 956	*26 604*	Unknown
COMMStellation (MSCI)	N/A	N/A	84	739	Unknown
Xinwei	N/A	N/A	30	*90*	Unknown

Source: IDATE

The following Table 43 summarizes the main differences among terrestrial, HAPS, LEO, MEO and GEO communication systems.

Table 43. Market potential compared, by technology in low-density areas.

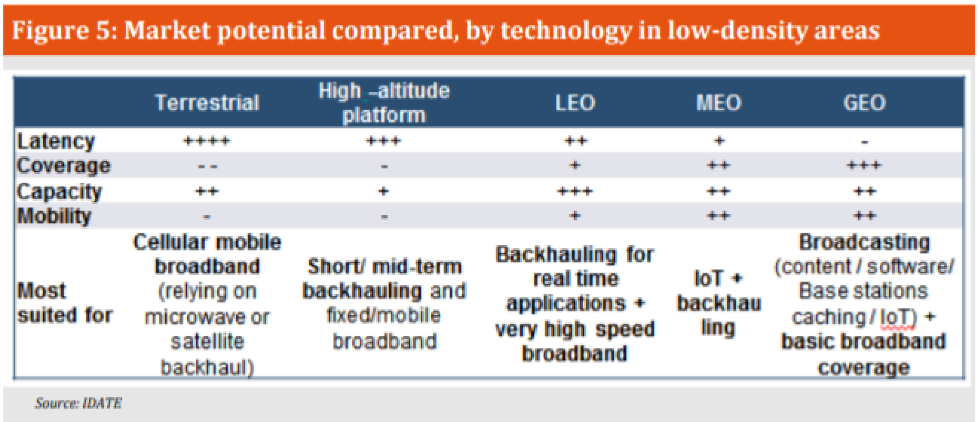
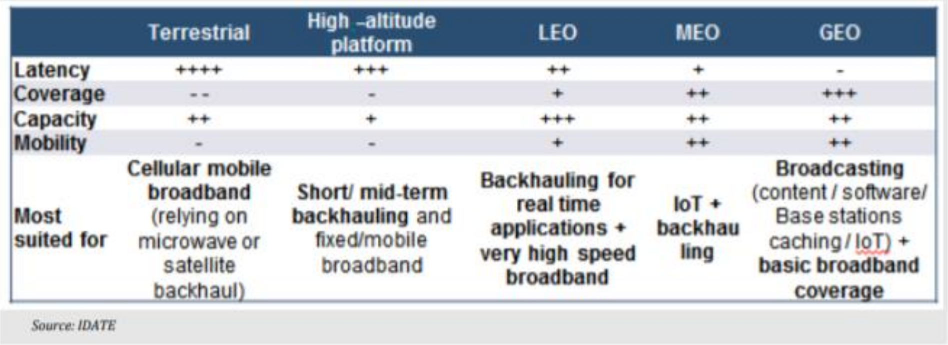


Figure 5: Market potential compared, by technology in low-density areas

	Terrestrial	High –altitude platform	LEO	MEO	GEO
Latency	++++	+++	++	+	-
Coverage	- -	-	+	++	+++
Capacity	++	+	+++	++	++
Mobility	-	-	+	++	++
Most suited for	**Cellular mobile broadband** (relying on microwave or satellite backhaul)	**Short/ mid-term backhauling** and fixed/mobile broadband	**Backhauling for real time applications + very high speed broadband**	**IoT + backhauling**	**Broadcasting** (content / software/ Base stations caching / IoT) + **basic broadband coverage**

Source: IDATE



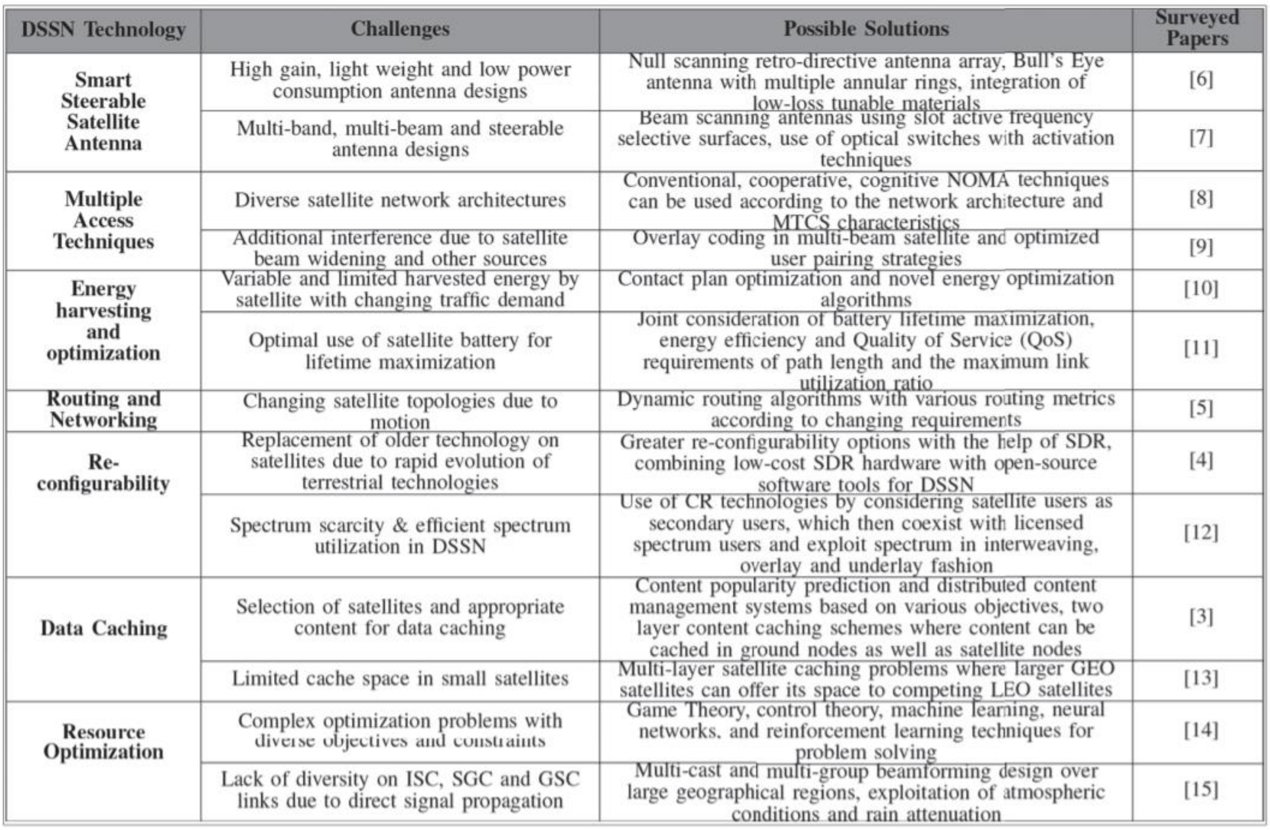
	Terrestrial	High –altitude platform	LEO	MEO	GEO
Latency	++++	+++	++	+	-
Coverage	- -	-	+	++	+++
Capacity	++	+	+++	++	++
Mobility	-	-	+	++	++
Most suited for	**Cellular mobile broadband** (relying on microwave or satellite backhaul)	**Short/ mid-term backhauling** and fixed/mobile broadband	**Backhauling for real time applications + very high speed broadband**	**IoT + backhauling**	**Broadcasting** (content / software/ Base stations caching / IoT) + **basic broadband coverage**

Source: IDATE

12.9 LEO: the last trend

From a future perspective, the DSSN will be characterized by different technologies, associated challenges, and possible solutions are also provided in Table 44 [119].

Table 44. DSSN technologies, challenges, and solutions.



DSSN Technology	Challenges	Possible Solutions	Surveyed Papers
Smart Steerable Satellite Antenna	High gain, light weight and low power consumption antenna designs	Null scanning retro-directive antenna array, Bull's Eye antenna with multiple annular rings, integration of low-loss tunable materials	[6]
	Multi-band, multi-beam and steerable antenna designs	Beam scanning antennas using slot active frequency selective surfaces, use of optical switches with activation techniques	[7]
Multiple Access Techniques	Diverse satellite network architectures	Conventional, cooperative, cognitive NOMA techniques can be used according to the network architecture and MTCS characteristics	[8]
	Additional interference due to satellite beam widening and other sources	Overlay coding in multi-beam satellite and optimized user pairing strategies	[9]
Energy harvesting and optimization	Variable and limited harvested energy by satellite with changing traffic demand	Contact plan optimization and novel energy optimization algorithms	[10]
	Optimal use of satellite battery for lifetime maximization	Joint consideration of battery lifetime maximization, energy efficiency and Quality of Service (QoS) requirements of path length and the maximum link utilization ratio	[11]
Routing and Networking	Changing satellite topologies due to motion	Dynamic routing algorithms with various routing metrics according to changing requirements	[5]
Re-configurability	Replacement of older technology on satellites due to rapid evolution of terrestrial technologies	Greater re-configurability options with the help of SDR, combining low-cost SDR hardware with open-source software tools for DSSN	[4]
	Spectrum scarcity & efficient spectrum utilization in DSSN	Use of CR technologies by considering satellite users as secondary users, which then coexist with licensed spectrum users and exploit spectrum in interweaving, overlay and underlay fashion	[12]
Data Caching	Selection of satellites and appropriate content for data caching	Content popularity prediction and distributed content management systems based on various objectives, two layer content caching schemes where content can be cached in ground nodes as well as satellite nodes	[3]
	Limited cache space in small satellites	Multi-layer satellite caching problems where larger GEO satellites can offer its space to competing LEO satellites	[13]
Resource Optimization	Complex optimization problems with diverse objectives and constraints	Game Theory, control theory, machine learning, neural networks, and reinforcement learning techniques for problem solving	[14]
	Lack of diversity on ISC, SGC and GSC links due to direct signal propagation	Multi-cast and multi-group beamforming design over large geographical regions, exploitation of atmospheric conditions and rain attenuation	[15]

13. Future technologies

In this section, we will present main features of future technologies that are expected to be very prominent in the next few areas in ICT sector, and then in railway too. Two future technologies are investigated in this section i.e., (i) quantum communications and (ii) THz communications.

The choice of these two technologies relays on the performance that can be reached. For instance, the Quantum Internet [128] i.e., the interconnection of quantum devices, is able to support functionalities with no direct counterparts in the classical world, such as secure communications, blind computing, exponential increase of the quantum computing power, and advanced quantum sensing techniques. All these functionalities have the potential of fundamentally changing markets and industries, such as commerce, intelligence and military affairs. Quantum teleportation is the core functionality of the Quantum Internet, which facilitates the "transfer" of qubits without the physical transfer of the particle storing the qubit.

On the other hand, due to the huge demand of increased connectivity and data rate, the need of available bandwidth to be exploited for communications has pushed toward the exploration of THz band. As a matter, only in the terahertz (THz) frequency range, i.e., beyond 300 GHz, ultra-high bandwidths beyond 20 GHz can be identified, and therefore, over 100 Gbps data rates can be accommodated even only with moderate spectral efficiencies.

13.1 Quantum communications

Classical well-known networks are meant to provide an ecosystem of networks flexibly, efficiently and effectively interconnecting heterogeneous radio access technologies.

In the classic information theory, the smallest information element is the bit, which assumes two possible values i.e., 0 and 1. On the other side, in quantum systems, bits do not exist, but are replaced with the qubits. The state of any quantum-mechanical system shows a linear behavior similar to that of continuous waves and signals. The unit of quantum information can store information on the unit vectors of a two-dimensional complex vector space. Two possible states for a qubit are denoted by the states $|0\rangle$ and $|1\rangle$. These states can be regarded as the states 0 and 1 for a classical bit. However, unlike a classical bit that must be in a state either 0 or 1, just like for continuous signals, the sum of $|0\rangle$ and $|1\rangle$ states is another state that is different from probabilistically generating either of the two. A qubit can be expressed in the following form:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where α and β are complex numbers.

Figure 88. Geometrical representation of a qubit through the Bloch sphere.

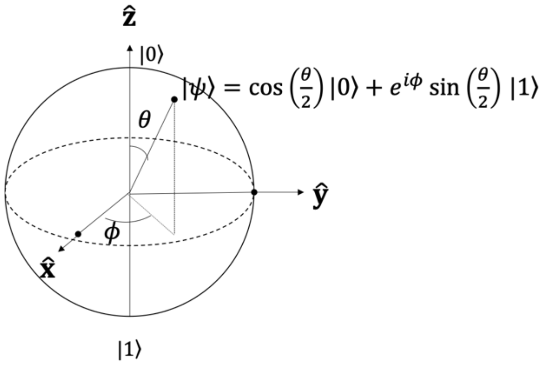

$\hat{\mathbf{z}}$
$|0\rangle$
$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$
θ
$\hat{\mathbf{y}}$
ϕ
$\hat{\mathbf{x}}$
$|1\rangle$

Figure 88 illustrates the Bloch sphere, that is a geometrical representation of the pure state space of a two-level quantum mechanical system (qubit), named after the physicist Felix Bloch. Specifically, any pure quantum state is represented by a point on the sphere's surface, with θ and φ denoting the spherical coordinates. A pure state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be represented by a point on the sphere surface, with $\alpha = \cos\left(\frac{\theta}{2}\right)$ and $\beta = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$.

This special phenomenon is called *superposition*, [129]. While n classical bits are only ever in one of the 2^n possible states at any given moment, an n-qubit register can be in a superposition of all of the possible states. Note that it is impossible to determine whether a qubit is in state $|0\rangle$ or $|1\rangle$ by examining the values of α and β. However, when we measure a qubit in superposition state, the entire qubit system would collapse into one of its bases (e.g., either $|0\rangle$ or $|1\rangle$). As for which state we would obtain, it is determined by the absolute square of its coefficient. In other words, we get the qubit in state $|0\rangle$ with probability $\|\alpha\|^2$, or in state $|1\rangle$ with probability $\|\beta\|^2$. Thus, α and β are often called probability amplitudes. In addition, since the sum of probabilities must equal 1 to satisfy the axiom of probability, we get the equation that $\|\alpha\|^2 + \|\beta\|^2 = 1$.

Furthermore, two or more qubit systems can be built up by composing multiple independent qubits. Take a two classical bit system as an example; there would be four possible states, 00, 01, 10, and 11. Accordingly, a two-qubit system also has four possible states. And they can be expressed by $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. Similarly, a two-qubit system can be represented as a linear combination of these four states in the following form:

$$|\varphi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle,$$

where the probability amplitudes α, β, γ and δ are complex numbers, such that $\|\alpha\|^2 + \|\beta\|^2 + \|\gamma\|^2 + \|\delta\|^2 = 1$. Finally, in order to compose two or more single qubit systems together, the tensor product operator $\otimes$ is adopted. For example, a two-qubit system composed of two single qubit systems $|\varphi\rangle = a|0\rangle + b|1\rangle$ and $|\phi\rangle = c|0\rangle + d|1\rangle$ can be represented as $|\varphi\rangle\otimes|\phi\rangle = |\varphi\phi\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$.

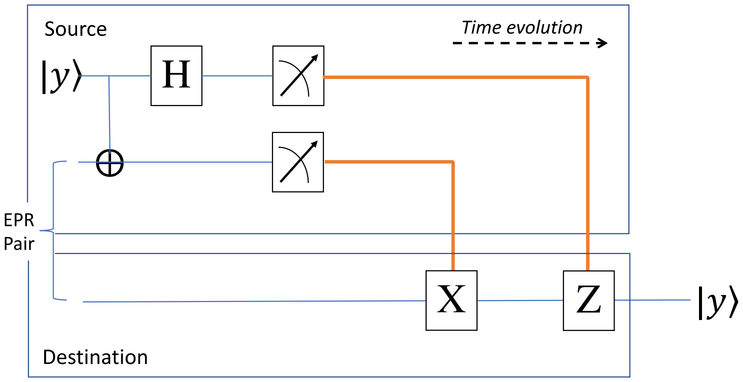
Quantum teleportation is a technique used to teleport a quantum state from a source node to a destination node. Quantum teleportation exploits a particular quantum property called as quantum entanglement. This allows quantum devices to transport a specific quantum state to another site, by transmitting classical bits rather than quantum bits. For this aim, shared entanglement is needed and can be accomplished by generating an EPR (named after Einstein, Podolsky, and Rosen) pair and distributing the pair to the source and destination through quantum wires.

An EPR pair can be seen as a bridge between quantum devices, and quantum teleportation can be regarded as transporting a specific qubit by passing it through the bridge. An EPR pair is a two-qubit system in maximally entangled state and can be denoted by $(1/\sqrt{2})(|00\rangle + |11\rangle)$. In the beginning, an EPR pair is shared between source and destination, with the source (e.g., Alice) keeps one qubit and the destination (e.g., Bob) holds the other qubit, then, with the aid of the EPR pair, Alice can communicate qubit information with Bob at a distance by only performing local operations and classical communication. So EPR pairs are called entanglement-assisted quantum channels.

Quantum teleportation has been experimentally verified over distances between 500-1400 kilometers. Specifically, to realize quantum teleportation a pair of parallel resources are needed i.e., one classical and one quantum. Figure 89 shows the quantum circuit of quantum teleportation. Blue lines represent quantum data, while the orange lines stand for classical information. Two bits must be transmitted from the source to the destination. Then, an entangled pair of qubits must be generated and shared between the source and the destination. As a consequence, quantum teleportation requires two parallel communication links, a classical link for transmitting the pair of classical bits and a quantum link for entanglement generation and distribution.

In case of secure transmissions, when Alice wants to deliver a qubit $|y\rangle$ to Bob, she sends her two qubits through a CNOT gate. After that, she performs a Hadamard gate on the first qubit. Afterwards, she measures the qubits and transmits the measurement outcomes to Bob through the classical channel. Once Bob receives the two classical bits, he knows that Alice has teleported a qubit state to him. Based on the received two classical bits, the quantum state $|y\rangle$ can be reconstructed by the appropriate operations.

Figure 89. Quantum circuit for quantum teleportation.



Unfortunately, quantum mechanics does not allow an unknown qubit to be copied or observed/measured. The transmission of a qubit occurs by mapping the qubit to a photon that can be directly transmitted to a remote node via a fiber link or free space. So, if the traveling photon is lost due to attenuation or it is corrupted by noise, the associated quantum information cannot be recovered via a measuring process or by re-transmitting a copy of the original information. Then, classical mitigation techniques do not apply to the qubits. It follows that the direct transmission of qubits remains limited to relatively short distances at the time of writing in the context of specific applications that can tolerate low transmission success rate, such as QKD and Quantum Secure Direct Communication (QSDC) networks. However, for long-distance quantum communications, quantum teleportation relies on quantum repeaters that counteract photon losses and gate errors in a variety of ways, depending on loss rates, memory lifetimes and available resources.

13.2 THz communications

In the vision of 6G requirements, dealing with handling a huge amount of data, as well as very high throughput per devices (from multiple Gbps up to several Tbps) and per area efficiency (bps/km^2), THz band is a candidate to surpass the gap between the mmWave and optical communications band. In 2017, IEEE 802.15.3d-2017 is published as the first wireless communication standard operating at carrier frequencies around 300 GHz. It focuses on fixed point-to-point links, and refers to applications as intra-device communication, kiosk downloading, complementary links in data centers and backhaul/fronthaul links. Furthermore, at IEEE 802.15, the THz Interest Group is actively working towards identification of further additional applications, which would require a further amendment of the current standard. In terms of spectrum for THz communications the radio regulations allow the use of spectrum beyond 275 GHz.

Through the deployment of large antenna arrays for coverage extension, it is possible to enable extremely narrow beams, which reduces the probability of eaves-dropping. In fact, THz communications can establish high-speed communication links through the selection of the optimal beam pattern. In this context, the large channel bandwidth of THz allows for specific protection measures against various attacks like jamming. THz links could be also utilized between UAVs and airplanes, and for HAPS where the UAV will act as a relay node in the sky linking ground station and airplane.

THz band represents a promising solution to the current spectrum crunch, and also able to provide a considerably larger bandwidth enabling the development of high data rate applications. A main drawback of THz is that, the implementation of communications in outdoor environment is very challenging, due to the inevitable loss caused by molecular absorption and weather conditions (i.e., rain). However, in case of moisture and at high altitudes, the THz attenuation is negligible, thus allowing reliable and high-capacity point-to-point wireless backhaul.

In the vision of "smart rail mobility", infrastructure, trains, and travelers will be interconnected to achieve optimized mobility, higher safety, and lower costs. The use of THz band for railway applications has been recently adopted in several research activities [125] [126]. The main goal is to increase railway capacity for passengers and freight through train-to-train (T2T) communications. T2T links require large bandwidth for high-data rate and low latency. The T2T channel is characterized through UWB channel sounding and ray tracing at THz band.

However, how to include the railway features in THz channel models is an open challenge. This is mainly due to the lack of standard channel models and reference scenarios exclusively for railways. Furthermore, accurate and efficient ray-tracing simulations for railway communications in the THz band are another challenge, because a large number of objects will affect the channel properties, and therefore, should be included in the scenarios. In the current railway network deployment, very fast adaptive beamforming technique can be needed due to the high mobility of the train. However, there is a chance of avoiding the requirement of such challenging beamforming, which is deploying the Tx antennas towards the same direction along the rail and moving the handover from the middle of two base stations (BSs) to the region when the train is very near the BS.

In LoS signal propagation, at THz frequencies, molecular absorption in the atmosphere plays a major role. Due to the higher impact of molecular absorption on free-space propagation property as well as the frequency dependence of effects, such as diffraction and reflection coefficients, the resulting path loss at THz greatly depends on the operating frequency.

THz band is very susceptible to environmental effects, such as gaseous (oxygen and water vapor) absorption, rain loss, and foliage loss, which exhibit a high degree of frequency-dependent variation. Atmospheric gas loss is approximately 0.50 dB/km at frequencies between 70 and 100 GHz. Yet, even for the most susceptible frequencies, such as 60, 200 GHz, etc., the atmospheric gas loss is smaller than 11 dB/km. Similar conclusion occurs for rain effects; for instance, a carrier at 100 GHz will experience a 4 dB loss per 200 m in heavy rain (25 mm/h). However, when looking at several THz bands, the molecular absorption by water vapor molecules plays a critical role, and, therefore, it defines several transmission windows whose positions and widths depend on the distance and molecular composition of the medium.

In the THz band, reflections within the material or multiple reflections at the interfaces of layered media have to be taken into account, causing highly frequency-dependent reflection behavior [13]. Moreover, the wavelength in the THz band is on the order of magnitude of surface height variations. For most building materials, such as concrete or plaster, diffuse scattering from walls covered with rough materials becomes highly relevant. Considering the huge bandwidths, the propagation phenomena themselves have to be treated as frequency dependent. This frequency dispersion of the channel necessitates the broadband channel simulation in the frequency domain and can cause a certain distortion of transmitted pulse shapes.

Another important aspect of THz propagation is polarization. The power degradation due to polarization mismatch between the antennas and depolarization caused by the channel can be as high as 10–20 dB. Last, very high diffraction attenuations (of 30 dB and more) in the THz band makes diffraction effects in the shadowing region behind objects negligible. However, it is of importance to investigate how fast the signal drops and rises again in case of a dynamic shadowing effect. Thus, modeling diffraction is useful to describe the dynamics of shadowing effects caused by various obstacles, such as human movement, buildings, or other trains, in the different defined smart rail mobility scenarios. The impact of different shadowing effects on the communication reliability is of great importance, particularly for rail control and safety.

14. Conclusions

In the post GSM-R era, the connectivity in railway applications is provided by PLMNs, in order to guarantee interoperability, inter-connection with other IP-based networks, network availability, service reliability, and compliance with service requirements (i.e., performance, QoS and security). Currently, railway applications can rely on TBs (i.e., Wi-Fi, GSM-R, LTE, LTE-A, 5G and satellites). According to a proof-of-view vision of railway sector evolution, novel technologies should be investigated to be placed as alternative and integrated solutions w.r.t. TBs. The coexistence with TBs should be also guaranteed, as well as backward compatibility.

The feasibility study of ABs to be implemented into ACS faces different aspects, such as security, QoS performance, impact on existing infrastructure, market implication and coexistence with existing TBs. As a first step, we have provided an overview of the state-of-the-art of selected ABs, from optical wireless technologies, short and long-range IoT, LEO satellites and HAPS to the future ones, such as Quantum and THz technologies.

The main objective of this deliverable relays in an overview of the prior state-of-art in the areas of selected alternative communication bearers (ABs), which are expected to be of interest for improving capabilities of the ACS. A set of candidate communication technologies have been investigated as potential ones for railway applications.

The methodology and the approach are based on the Abs investigation in terms of communication features, technology characteristics and Key Performance Indicators. The selected ABs will be enlisted from a technological assessment perspective, based on (but not limited to) the following technological and market areas, as reference standard, protocol stack, security, deployment issues, applications and market share and trends.

The following technical features (but not limited to) are investigated for each AB: spectrum and frequencies (e.g., channel bandwidth, frequency band), physical characteristics (e.g., transmission transfer interval, duplex mode), data rate and efficiency (e.g., peak downlink/uplink data rate, average throughput), mobility (e.g., maximum supported speed, measures against doppler), service quality (e.g., maximum user plane latency, jitter) , coverage, multiple access schemes and multiplexing and end-to-end AB architecture.

Other features will be also considered, such as general support of railway functionalities and interference with other communication technologies in the same bandwidth. This review will also include the service requirements concerning critical and business application classes to be considered in AB4Rail activities. These are reported in [1] and include the FRMCS USR services and incorporate the additional requirements in ACS TD 2.1 [2] [3] [4] [5].

The following Table 45 summarizes the relevant findings and the identified limitations, coming from the overview of different ABs, carried out in this deliverable.

The results have provided an overview of several technologies, each of them showing specific characteristics. The heterogeneous nature of different ABs allows to provide a plethora of available communication technologies to be potentially used by the ACS for different railway scenarios. All the selected ABs provide the IP interconnection feature since they are Integrated within OSI reference model.

In this way, the Table 45 collects the planned objectives of deliverable D2.1, expressed as a technological overview of selected ABs, as possible candidates coexisting with TBs for supporting railway applications.

This deliverable will be the input for next T2.2, which will provide D2.2, where selected ABs will be analysed in terms of RAT methodology.

As future work, we will take into account the following tasks:

- new updates and evolutions of selected technologies, coming from standardization bodies and rail companies

- the interoperability and coexisting issue that can raise from different new technology versions,
- first experimental trials of selected AB.

Table 45. Summary of the most important features for selected ABs.

Category	Technology	Properties	Limitation	Applicability to railway
Optics	Visible Light Communication (VLC)	• high secure • high data rate (>100 Mbps) • directivity • immunity to RF • green technology • both indoor and outdoor • Coverage range: <10m	• limited mobility • outage due to occlusions • short range	• Monitoring of railways health state for train safety • Indoor positioning and venue navigation
	Free Space Optics (FSO)	• Medium-long range • Outdoor scenarios (coverage range < 5km) • High data rate (>10 Gbps) • immunity to RF	• limited mobility • outage due to occlusions • weather interference • atmospheric attenuation	• To enable connectivity between trackside gateways • High-speed communication services such as Internet access and video-on-demand
PLC	Power Line Communications systems (PLC)	• Use of existing infrastructure • Dual use of electricity • Variable data rates depending on frequency bands (from kbps up to 200 Mbps) • Coverage: order of hundred meters	• Attenuation • Interference from electronic devices	• Transmission of data for rail control • Coach and train communication networks for Passenger Information Systems services and video surveillance
IoT (SR)	Bluetooth 5.2	• Data rate: up to 2 Mbps • Coverage: up to 200 m (outdoor), 50 m (indoor) • Beacons Everywhere (message size: 255 Bytes) • Mobility: allowed (limited)	• Backwards Compatibility • Bluetooth 5 support is still limited • High Power consumption • Weaker security Wi-Fi • Maximum 8 connections for each device	• Audio Streaming • Data Transfer • Location Services • Device Networks • Smart environment • Vehicle health monitoring • Railway infrastructure monitoring • Derailment detection and data collection in freight trains

	ZigBee	• Data rate: 20 kbps • Coverage: 75-100 m • Mobility: allowed (limited) • Low Power consumption	• Low data rate • Low coverage range	• Audio Streaming • Data Transfer • Location Services • Device Networks • Smart environment • Vehicle health monitoring • Mesh Network services for asset tracking (e.g. train asset) • Railway infrastructure monitoring and maintenance • Train monitoring and maintenance
	Ultra-wideband (UWB)	• Data Rate: over 100 Mbps • Low Power Consumption • Coverage: 10 mt • Low Cost • Mobility: allowed (limited)	• Interfere due to large frequency range • Distortion due to multipath • Equalization is needed	• Communications • Radar • Precision Geolocation (asset tracking)
IoT (LR) - LPWAN	LoRaWAN	• Data Rate: 5.5 Kbps • Coverage range: 1 km (urban), 10 km (rural) • Low Power Consumption • Network capacity (> 1.000 nodes per gateway) • Mobility: allowed	• Duty cycle limitation (1%) • Interferences in ISM band	• On-board monitoring • Facility arrangement • Factory and industry management • Station Service Management • Smart environment applications
	Narrow Band-IoT (NB-IoT)	• Data Rate: 160 Kbps (DL) • Coverage range: 15 km • Better indoor coverage • High network capacity (over 100.000 nodes per cell) • Low cost • Mobility: allowed	• Not suitable for seamless handover • Not suitable for low latency applications (Voice/VoIP)	• Smart metering • Industry automation • Smart logistics • Smart environment • Environmental monitoring • Rail infrastructure monitoring • Train passing notification • Rail crossing monitoring
HAPS	High Altitude Platform Systems	• Data rate: from 11 to 33 Gbps • Coverage range: from 10 km to 50 km (up to 90 km) • Very Low Round-trip time: from 0.13 ms to 0.33	• Energy autonomy • Payload limited to a few tenths of kilograms	• Satellite Communications (SatCom) - communications between trains (train-to-train communications) - communications between train and RBC server - communications between train and

		• Number of cells: from 1 to more than 100 • Low propagation delay • Reduced Doppler shift • Better Link budget • Fast deployment • Scalable • Reduced cost than LEO satellite • Mobility: allowed		railway infrastructures • Satellite navigation (SatNav) - Train navigation over specific paths - Train localization - Railway localization (e.g. rail crossing, rail traffic lights,..) • Satellite Earth Observation (SatEO)
Update tech.	Novel Sat LEO constellations	• Data rate: from 5 to 20 Gbps • Coverage area: 1 million km^2 area per each satellite • Low Round-trip time: from 3.33 – 13.33 ms (up to 30 ms) • Supporting Massive Devices • Mobility: allowed	• Frequent handovers • Data routing issues • Reduced volume, mass and energy resources	• Broadband Internet service • Offloading and caching Data • Complementing Positioning • Support for backhaul
Future tech	Quantum communications	• High data rates • Very long distances (500-1400 km) • Secure transmissions	• Different from classical theory • Attenuation	• Future high-data-rate applications from infrastructure-to-train
	THz communications	• Ultra-high bandwidth • Narrow beams	• Molecular absorption • Loss due to weather conditions • Shadowing effects	• High-data-rate applications such as on-board and wayside high definition (HD) video surveillance, • On-board real-time high-data-rate connectivity, • Journey information

15. References

[1] "Future Railway Mobile Communication System. User Requirements Specification", UIC, https://uic.org/IMG/pdf/fu-7100-3.0.0.pdf

[2] X2R-T7.3-D-CFS-006-06_-_D7.2_-_Railway_requirements_and_standards_application_conditions

[3] X2R1-WP3-D3.3-Annex Guideline of Technology-DB-001-1.0-I

[4] X2R1-WP3-D3.3-Communicationsystem_Specification_and_Technology_Guideline

[5] X2R-WP03-D-NRI-005-02_-_D3.1_-_User_&_System_Requirements_(Telecommunications)

[6] D. Krichen, W. Abdallah and N. Boudriga, "An optical wireless network for railways condition monitoring," 2016 22nd Asia-Pacific Conference on Communications (APCC), Yogyakarta, 2016, pp. 153-160, doi: 10.1109/APCC.2016.7581506.

[7] S. Ahamed, "Visible light communication in railways," The International Conference on Railway Engineering (ICRE) 2016, Brussels, 2016, pp. 1-5, doi: 10.1049/cp.2016.0516.

[8] S. Haruyama et al., "New ground-to-train high-speed free-space optical communication system with fast handover mechanism," 2011 Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference, Los Angeles, CA, 2011, pp. 1-3.

[9] J. Nishiyama, H. Sugahara, T. Okada, T. Kunifuji, Y. Fukuta, M. Matsumoto, "A signal control system by optical LAN and design simplification," 2007 IEEE International Conference on Systems, Man and Cybernetics, Montreal, Que., 2007, pp. 1711-1716, doi: 10.1109/ICSMC.2007.4413872.

[10] K. Sri Dhivya Krishnan, M. Barathi Selvaraj, P. Rekha, S. Gowtham, Analysis and Implementation of Semaphore Signalling in Railway Tracks, International Journal of Science, Technology and Society. Vol. 3, No. 2, 2015, pp. 65-68. doi: 10.11648/j.ijsts.20150302.15

[11] Report "Power Line Communication Train Backbone PTB – cost effective data communication on freight trains", plc-tec AG, SBB Cargo AG

[12] D. Amato, G. Chili, R. Battani, "Powerline Solutions for Train Coupling, Rolling Stock Backbone and Passenger Information Systems (PIS) Services", World Congress on Railway Research (WCRR) May-June 2016.

[13] V. J. Hodge, S. O'Keefe, M. Weeks and A. Moulds, "Wireless Sensor Networks for Condition Monitoring in the Railway Industry: A Survey," in IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 3, pp. 1088-1106, June 2015, doi: 10.1109/TITS.2014.2366512.

[14] M. Macucci, S. Di Pascoli, P. Marconcini and B. Tellini, "Derailment Detection and Data Collection in Freight Trains, Based on a Wireless Sensor Network," in IEEE Transactions on Instrumentation and Measurement, vol. 65, no. 9, pp. 1977-1987, Sept. 2016, doi: 10.1109/TIM.2016.2556925.

[15] TRACe LoRa-MQTTfor Rail Application https://www.railway-technology.com/products/trace-lora-mqtt-fanless-lora-mqtt-iot-gateway/

[16] G. P. White and Y. V. Zakharov, "Data Communications to Trains From High-Altitude Platforms," in IEEE Transactions on Vehicular Technology, vol. 56, no. 4, pp. 2253-2266, July 2007, doi: 10.1109/TVT.2007.897185.

[17] I. Zakia, "Coordinated beamforming for high-speed trains in multiple HAP networks," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-4, doi: 10.1109/TSSA.2017.8272953.

[18] Starlink satellite lauching, https://www.space.com/space-starlink-satellites-launch-rocket-landing-success-april-2020.html

[19] "New Antenna to Fuel Satellite Based WiFi on Some UK Trains", 27 Feb. 2020, available at: https://www.ispreview.co.uk/index.php/2020/02/new-antenna-to-fuel-satellite-based-wifi-on-some-uk-trains.html

[20] K. Guan et al., "On Millimeter Wave and THz Mobile Radio Channel for Smart Rail Mobility," in IEEE Transactions on Vehicular Technology, vol. 66, no. 7, pp. 5658-5674, July 2017, doi: 10.1109/TVT.2016.2624504.

[21] K. Guan, D. He, A. Hrovat, B. Ai, Z. Zhong and T. Kürner, "Challenges and chances for smart rail mobility at mmWave and THz bands from the channels viewpoint," 2017 15th International Conference on ITS Telecommunications (ITST), Warsaw, 2017, pp. 1-5, doi: 10.1109/ITST.2017.7972207.

[22] Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, "Optical Wireless Communications System and Channel Modelling with MATLAB," Second Edition, 2019, CRC Press.

[23] "DLR and ADVA set a new world record in optical free-space data transmission," Press Release from German Aerospace Center, 10 May 2018, available at https://www.dlr.de/dlr/en/desktopdefault.aspx/tabid-10081/151_read-27323/#/gallery/30516

[24] G. Cossu et al., "Gigabit-class optical wireless communication system at indoor distances (1.5 – 4 m)," Optics Express, vol. 23, no. 12, June 2015.

[25] D. Karunatilaka et al., "LED based indoor visible light communications: State of the art," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, 2015

[26] D. Tsonev, S. Videv, H. Haas, "Unlocking Spectral Efficiency in Intensity Modulation and Direct Detection Systems," IEEE Journal Selected Areas in Communications, vol. 33, no. 9, Sept. 2015.

[27] N.B. Hassan, Z. Ghassemlooy, S. Zvanovec, M. Biagi, A.M. Vegni, M. Zhang, and P. Luo, "Non-Line-of-Sight MIMO Space-Time Division Multiplexing Visible Light Optical Camera Communications," in IEEE/OSA Journal of Lightwave Technology, vol. 37, no. 10, pp. 2409-2417, 15 May, 2019. doi: 10.1109/JLT.2019.2906097.

[28] Z. Ghassemlooy et al., Visible Light Communications, Theory and Applications, CRC Press, 2017.

[29] P. Luo et al., "Experimental demonstration of RGB LED-based optical camera communications," IEEE Photonics Journal, vol. 7, no. 5, Oct. 2015.

[30] P. H. Pathak et al., "Visible Light Communication, Networking, and Sensing: A Survey, Potential and Challenges", IEEE Communications Surveys & Tutorials, vol. 17, no. 4, Nov. 2015.

[31] A.M. Cailean, M. Dimian, "Current Challenges for Visible Light Communications Usage in Vehicle Applications: A Survey," IEEE Communications Surveys & Tutorials, vol. 19, no.4, 2017.

[32] M.A. Khalighi, M. Uysal, "Survey on Free Space Optical Communication: A Communication Theory Perspective", IEEE Communications Surveys & Tutorials, vol. 16, no. 4, 2014.

[33] A. E. Willner, "Communication with a twist", IEEE Spectrum, vol. 53, no.8, Aug. 2016.

[34] Z. Xu, B.M. Sandler, "Ultraviolet Communications: Potential and State-of-the-Art," IEEE Communications Magazine, vol. 46, no. 5, May 2008.

[35] Aditi Malik, Preeti Singh, "Free Space Optics: Current Applications and Future Challenges", International Journal of Optics, vol. 2015, Article ID 945483, 7 pages, 2015. https://doi.org/10.1155/2015/945483

[36] M. Sharma, D. Chadha, V. Chandra, "High-altitude platform for free-space optical communication: Performance evaluation and reliability analysis," IEEE/OSA Journal of Optical Communications and Networking, vol. 8, no. 8, Aug. 2016.

[37] H. Kaushal, G. Kaddoum, "Optical Communication in Space: Challenges and Mitigation Techniques", IEEE Communications Surveys & Tutorials, vol. 19, no. 1, Feb. 2017.

[38] M. Uysal et al., Eds. Optical Wireless Communications- An Emerging Technology, Springer 2016.

[39] R. J. Hughes, J. E. Nordholt, "Free-space communications: Quantum space race heats up," Nature Photonics, vol. 11, no. 8, Aug. 2017.

[40] Bluetooth Radio Versions (https://www.bluetooth.com/learn-about-bluetooth/radio-versions/)

[41] Bluetooth Core Specification v5.2, Vol 1, Part A (https://www.bluetooth.com/wp-content/uploads/2020/01/Bluetooth_5.2_Feature_Overview.pdf)

[42] Sherali Zeadally et al, "25 Years of Bluetooth Technology", Future Internet, Vol. 11, Fasc. 9, (2019): 194. DOI:10.3390/fi11090194. https://www.mdpi.com/1999-5903/11/9/194

[43] Overview of Bluetooth versions and their features (https://www.u-blox.com/en/technologies/bluetooth)

[44] The Ultimate Guide to What's New in Bluetooth version 5.2 (https://www.novelbits.io/bluetooth-version-5-2-le-audio)

[45] M. Collotta, G. Pau, T. Talty and O. K. Tonguz, "Bluetooth 5: A Concrete Step Forward toward the IoT," in IEEE Communications Magazine, vol. 56, no. 7, pp. 125-131, July 2018, doi: 10.1109/MCOM.2018.1700053.

[46] Bluetooth 5, "Go Faster. Go Further" (https://www.bluetooth.com/wp-content/uploads/2019/03/Bluetooth_5-FINAL.pdf)

[47] The Fundamental Concepts of Bluetooth Mesh Networking Part 1

(https://www.bluetooth.com/blog/the-fundamental-concepts-of-bluetooth-mesh-networking-part-1/)

[48] Da-Zhi Sun and Li Sun, "On Secure Simple Pairing in Bluetooth Standard v5.0-Part I: Authenticated Link Key Security and Its Home Automation and Entertainment Applications," (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6427610/pdf/sensors-19-01158.pdf)

[49] NIST SP 800 121, Guide to Bluetooth Security (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf)

[50] S. Böcker, C. Arendt and C. Wietfeld, "On the suitability of Bluetooth 5 for the Internet of Things: Performance and scalability analysis," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-7, doi: 10.1109/PIMRC.2017.8292720.

[51] Bluetooth, "Market Update 2020" (https://www.bluetooth.com/wp-content/uploads/2020/03/2020_Market_Update-EN.pdf)

[52] M. Samra, S. Sidahmed, S. Greedy and A. Mndez, "Feasibility analysis of wireless technologies for railway signalling systems [Technical Program]," 2016 IEEE International Conference on Intelligent Rail Transportation (ICIRT), Birmingham, UK, 2016, pp. 1-6, doi: 10.1109/ICIRT.2016.7725793.

[53] Jorge Higuera1, Elli Kartsakli1 and Jos L. Valenzuela," Experimental study of Bluetooth, ZigBee and IEEE 802.15.4 technologies on board high-speed trains", Technical University of Catalonia (UPC) Department of Signal Theory and Communications (TSC).

[54] ZigBee Alliance, ZigBee Specification, "Document 05-3474-21" (August 5, 2015) https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

[55] ZigBee Alliance, ZigBee Specification, "Document 05-3474-21" (August 5, 2015)

[56] Roy, Uttam et alii, "Analysis and Optimization Of Routing Protocols In Wireless Personal Area Networks", IASTED International Conference on Parallel and Distributed Computing and Systems (PDCS 2005).

[57] M. Sun and Y. Qian, "Study and Application of Security Based on ZigBee Standard," 2011 Third International Conference on Multimedia Information Networking and Security, Shanghai, China, 2011, pp. 508-511, doi: 10.1109/MINES.2011.79.

[58] X. L. Ren, H. B. Yu. Study on Security of ZigBee Wireless Sensor, Network [J] Chinese Journal of Scientific Instrument (in Chinese), Vol28, No 12, December 2007, pp 2132-2137

[59] Y. Xiao, V. K. Rayi and B. Sun, A survey of key management schemes in wireless sensor networks, Computer Communications, vol. 30, no. 11-12, 2007, pp. 2314–2341.

[60] S. Khanji, F. Iqbal and P. Hung, "ZigBee Security Vulnerabilities: Exploration and Evaluating," 2019 10th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2019, pp. 52-57, doi: 10.1109/IACS.2019.8809115.

[61] S. Long and F. Miao, "Research on ZigBee wireless communication technology and its application," 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chengdu, China, 2019, pp. 1830-1834, doi: 10.1109/IAEAC47372.2019.8997928.

[62] Jiang, Shaohua, Skibniewski, Miroslaw, Yuan, Yongbo and Sun, Chengshuang, "Ultra-Wide Band Applications in Industry: A Critical Review. Journal of Civil Engineering and Management", 2011. 17. 437-444. 10.3846/13923730.2011.596317.

[63] G. R. Hiertz, Y. Zang, J. Habetha and H. Sirin, "IEEE 802.15.3a Wireless Personal Area Networks - The MBOA Approach," 11th European Wireless Conference 2005 - Next Generation wireless and Mobile Communications and Services, Nicosia, Cyprus, 2006, pp. 1-7.

[64] Mr. Kartik Ramesh Pate, "Ultra-Wideband (UWB) Wireless System", International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2014.

[65] Baptiste Pestourie, "UWB Secure Ranging and Localization", Embedded Systems, 2020, Université Grenoble (https://hal.archives-ouvertes.fr/tel-03136561/document)

[66] ITU-R Recommendation SM.1755-0 (05/2006) (https://www.itu.int/rec/R-REC-SM.1755-0-200605-I)

[67] ETSI TR 103 526 V1.1.1 (2018-04) (https://www.etsi.org/deliver/etsi_tr/103500_103599/103526/01.01.01_60/tr_103526v010101p.pdf)

[68] E. Aras, G. S. Ramachandran, P. Lawrence and D. Hughes, "Exploring the Security Vulnerabilities of LoRa," 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, 2017, pp. 1-6,

doi: 10.1109/CYBConf.2017.7985777.

[69] LoRaWAN SECURITY, Lora Alliance (https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf)

[70] ETSI TR 103 526 V1.1.1 (2018-04) (https://www.etsi.org/deliver/etsi_tr/103500_103599/103526/01.01.01_60/tr_103526v010101p.pdf)

[71] Transforma Insights, "Low Power Wide Area (LPWA) IoT connections to grow to 4 billion in 2030", October 20, 2020 (https://transformainsights.com/news/low-power-wide-area-lpwa-iot-connections-4-billion-2030#:~:text=Transforma%20Insights%20today%20unveiled%20its,at%20the%20end%20of%202019).&text=global%20LPWA%20connections.-,At%20the%20end%20of%202019,57%25%20of%20the%20global%20total)

[72] M. Chen, Y. Miao, Y. Hao and K. Hwang, "Narrow Band Internet of Things," in IEEE Access, vol. 5, pp. 20557-20577, 2017, doi: 10.1109/ACCESS.2017.2751586.

[73] Smilty Chacko and Mr. Deepu Job, "Security mechanisms and Vulnerabilities in LPWAN", 2018 IOP Conf. Ser.: Mater. Sci. Eng. 396 012027

[74] Ergeerts Glenn, Nikodem Maciej, Subotic Dragan, Surmacz Tomasz, Wojciechowski Bartosz, De Meulenaere Paul and Weyn Maarten, DASH7 Alliance Protocol in Monitoring Applications, 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing

[75] Popli, Sakshi et al. "A Survey on Energy Efficient Narrowband Internet of Things (NBIoT): Architecture, Application and Challenges." IEEE Access 7 (2019): 16739-16776.

[76] Q. Xiaocong and M. Mingxin, ''NB-IoT standardization, technical characteristics and industrial development,'' Inf. Res., vol. 5, pp. 23–26, May 2016

[77]] Z. Yulong, D. Xiaojin, and W. Quanquan, ''Key technologies and application prospect for NB-IoT,'' ZTE Technol., vol. 23, no. 1, pp. 43–46, 2017.

[78] Q. Xiaocong and M. Mingxin, ''NB-IoT standardization, technical characteristics and industrial development,'' Inf. Res., vol. 5, pp. 23–26, May 2016

[79] ITU-T, "Security requirements and framework for narrowband Internet of things", SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1364-202003-I!!PDF-E&type=items

[80] Glenn Ergeerts, Maciej Nikodem, Dragan Subotic, Tomasz Surmacz, Bartosz Wojciechowski, Paul De Meulenaere, Maarten Weyn DASH7 Alliance Protocol in Monitoring Applications,10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2015.

[81] Adefemi Alimi, K.O.; Ouahada, K.; Abu-Mahfouz, A.M.; Rimer, S. A Survey on the Security of Low Power Wide Area Networks: Threats, Challenges, and Potential Solutions. Sensors 2020, 20, 5800. https://doi.org/10.3390/s20205800

[82] N. Shafiee, S. Tewari, B. Calhoun, and A. Shrivastava, ''Infrastructure circuits for lifetime improvement of ultra-low power iot devices,'' IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 64, no. 9, pp. 2598–2610, Sep. 2017.

[83] M. Chen, Y. Miao, Y. Hao, and K. Hwang, ''Narrow band Internet of Things,'' IEEE Access, vol. 5, pp. 20557–20577, 2017

[84] A. Rico-Alvarino et al., ''An overview of 3GPP enhancements on machine to machine communications,'' IEEE Commun. Mag., vol. 54, no. 6, pp. 14–21, Jun. 2016.

[85] M. Elsaadany, A. Ali, and W. Hamouda, ''Cellular LTE-A technologies for the future Internet-of-Things: Physical layer features and challenges,'' IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2544–2572, 4th Quart., 2017.

[86] R. S. Sinha, Y. Wei, and S.-H. Hwang, ''A survey on LPWA technology: LoRa and NB-IoT,'' ICT Express, vol. 3, no. 1, pp. 14–21, Mar. 2017.

[87] ''NARROWBAND IOT ground breaking in the Internet of Things,'' Deutsche Telekom, Bonn, Germany, White Paper. [Online]. Available: https://www.b2b-europe.telekom.com/downloads/Telekom-B2BNBIOT_whitepaper.pdf?1543236504

[88] K. L. Lueth et al., ''State of the IoT 2018: Number of IoT devices now at 7B—Market accelerating,''

IoT Anal., Hamburg, Germany, Tech. Rep., Aug. 2018.

[89] C. Babla. LPWA Connectivity for IoT. http://www.armtechforum.com.cn/attached/article/B5_ConnectYourIoTDevice20171226160035.pdf

[90] K. L. Lueth et al., ‘‘State of the IoT 2018: Number of IoT devices now at 7B—Market accelerating,’’ IoT Anal., Hamburg, Germany, Tech. Rep., Aug. 2018

[91] ITU, "HAPS – High-altitude platform systems" (https://www.itu.int/en/mediacentre/backgrounders/Pages/High-altitude-platform-systems.aspx)

[92] "HIGH ALTITUDE PLATFORMS FOR COMMUNICATIONS AND OTHER WIRELESS SERVICES", Acta Electrotechnica et Informatica No. 2, Vol. 7, 2007 (http://www.aei.tuke.sk/papers/2007/2/Macekova.pdf)

[93] Kurt, G., Khoshkholgh, M.G., Alfattani, S., Ibrahim, A., Darwish, T., Alam, M.S., Yanikomeroglu, H., & Yongaçoglu, A, "A Vision and Framework for the High Altitude Platform Station (HAPS) Networks of the Future", 2020. ArXiv, abs/2007.15088.

[94] Dutta, Sourjya & Hsieh, Frank & Vook, Frederick. "HAPS Based Communication using mmWave Bands", 2019. 1-6. 10.1109/ICC.2019.8761640.

[95] Malinowski, Andrzej & Zielinski, Ryszard. (2010). High Altitude Platform — Future of Infrastructure. International Journal of Electronics and Telecommunications. 56. 10.2478/v10177-010-0025-0.

[96] J. Thorton, D. Grace, "Effect of Lateral Displacement of a High-Altitude Platform on Cellular Interference and Handover," IEEE Transactions on Wireless Communications, vol. 4, no. 4, July 2005.

[97] Test Results Summary Report, CAP-22a-WP44-CGS-PUB-01, FP6 Project CAPANINA

[98] D. Grace, "Radio Resource Management and Handoff for Cellular Architectures"

[99] X. Cao, P. Yang, M. Alzenad, X. Xi, D. Wu, and H. Yanikomeroglu, "Airborne communication networks: A survey," IEEE Journal on Selected Areas in Communications, vol. 36, no. 9, pp. 1907–1926, Sep. 2018.

[100] J. Qiu, D. Grace, G. Ding, M. D. Zakaria, and Q. Wu, "Air-ground heterogeneous networks for 5G and beyond via integrating high and low altitude platforms," IEEE Wireless Communications, vol. 26, no. 6, pp. 140–148, Dec. 2019.

[101] K. Hoshino, S. Sudo, and Y. Ohta, "A study on antenna beamforming method considering movement of solar plane in HAPS system," in IEEE 90th Vehicular Technology Conference (VTC2019-Fall), 2019, pp. 1–5

[102] Joanne WILSON, "Results of the 2019 World Radiocommunication Conference (WRC-19)", 29th World Radio Communication Seminar, 30 november -11 december 2020 (https://www.itu.int/en/ITU-R/seminars/wrs/2020/Plenary%20Sessions%20%20Presentations/01.%20Opening%20and%20General%20-%2030%20Nov%202020/P4.%20Results%20of%20the%20WRC-19.pdf)

[103] Randall K. Nichols et alii, "Unmanned Aircraft Systems in the Cyber Domain - Second Edition", Wayne D. Lonstein, VFT Solutions, 2019.

[104] ITU-R, Recommendation ITU-R F.1500, "Preferred characteristics of systems in the fixed service using high altitude platforms operating in the bands 47.2-47.5 GHz and 47.9-48.2 GHz" (https://www.itu.int/dms_pubrec/itu-r/rec/f/R-REC-F.1500-0-200005-I%21%21PDF-E.pdf)

[105] Rita Rinaldo et alii, "SERVICES ENABLED BY HIGN ALTITUDE PSEUDO SATELLITES (HAPS) COMPLEMENTED BY SATELLITES", ESA Webinar, 15/09/2017 (https://business.esa.int/sites/default/files/HAPS%20FS_Webinar%20presentation_final.pdf)

[106] Jesús Gonzalo, et alii, "On the capabilities and limitations of high altitude pseudo-satellites", Progress in Aerospace Sciences, Volume 98, 2018, Pages 37-56, ISSN 0376-0421, https://doi.org/10.1016/j.paerosci.2018.03.006.

[107] Alam, M.S., Kurt, G., Yanikomeroglu, H., Zhu, P., & DJao, N.D, "High Altitude Platform Station based Super Macro Base Station (HAPS-SMBS) Constellations", 2020. https://arxiv.org/pdf/2007.08747.pdf

[108] E. Cianca, R. Prasad, M. De Sanctis, A. De Luise, M. Antonini, D. Teotino, and M. Ruggieri, "Integrated satellite-HAP systems," IEEE Commun. Mag., vol. 43, no. 12, pp. 33–39, Dec. 2005.

[109] M. Alzenad, M. Z. Shakir, H. Yanikomeroglu, and M.-S. Alouini, "FSO-based vertical backhaul/fronthaul framework for 5G+ wireless networks," IEEE Commun. Mag., vol. 56, no. 1, pp.

218–224, Jan. 2018

[110] Stojce Dimov Ilcev, “Non-GEO GMSC Systems”, Global Mobile Satellite Communications, 2005. Springer, Boston, MA. https://doi.org/10.1007/1-4020-2784-2_8

[111] Evans B. G., “Satellite Communication Systems”, IEE, London, 1991

[112] Gallagher B., “Never Beyond Reach”, Inmarsat, London, 1989

[113] Group of authors, “Utilisation des satellites pour les recherches et le sauvetage”, Cepadues, Toulouse, 1984.

[114] I. Leyva-Mayorga et al., “LEO Small-Satellite Constellations for 5G and Beyond-5G Communications,” in IEEE Access, vol. 8, pp. 184955-184964, 2020, doi: 10.1109/ACCESS.2020.3029620.

[115] Study on Scenarios and Requirements for Next Generation Access Technologies, Standard TR 38.913 V16.0.0, 3GPP, Jul. 2020.

[116] Study on Using Satellite Access in 5G, Standard TR 22.822 V16.0.0, 3GPP, Jun. 2018.

[117] Solutions for NR to Support non-Terrestrial Networks (NTN), Standard TR 38.821 V16.0.0, 3GPP, Dec. 2019.

[118] B. Di, L. Song, Y. Li, and H. V. Poor, ‘‘Ultra-dense LEO: Integration of satellite access networks into 5G and beyond,’’ IEEE Wireless Commun., vol. 26, no. 2, pp. 62–69, 2019

[119] Hassan, N.U., Huang, C., Yuen, C., Ahmad, A., & Zhang, Y. (2020). Dense Small Satellite Networks for Modern Terrestrial Communication Systems: Benefits, Infrastructure, and Technologies. IEEE Wireless Communications, 27, 96-103.

[120] R. Radhakrishnan, W. W. Edmonson, F. Afghah, R. M. RodriguezOsorio, F. Pinto, and S. C. Burleigh, “Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view,” IEEE Communications Surveys & Tutorials, vol. 18, no. 4, pp. 2442–2473, 2016.

[121] S. Gao, Y. Rahmat-Samii, R. E. Hodges, and X.-X. Yang, “Advanced antennas for small satellites,” Proceedings of the IEEE, vol. 106, no. 3, pp. 391–403, 2018.

[122] Z. Zheng, N. Hua, Z. Zhong, J. Li, Y. Li, and X. Zheng, “Time-sliced flexible resource allocation for optical low earth orbit satellite networks,” IEEE Access, vol. 7, pp. 56 753–56 759, 2019.

[123] Garino, M.B., & Gibson, M.J. (2009). 273 Chapter 21 Space System Threats.

[124] European Commission, “Digital Transformation Monitor Low-Earth Orbit satellites: Spectrum access”, July 2017. https://ec.europa.eu/growth/tools-databases/dem/monitor/content/low-earth-orbit-satellites-spectrum-access

[125] K. Guan et al., “On Millimeter Wave and THz Mobile Radio Channel for Smart Rail Mobility,” in IEEE Transactions on Vehicular Technology, vol. 66, no. 7, pp. 5658-5674, July 2017, doi: 10.1109/TVT.2016.2624504.

[126] K. Guan, D. He, A. Hrovat, B. Ai, Z. Zhong and T. Kürner, “Challenges and chances for smart rail mobility at mmWave and THz bands from the channels viewpoint,” 2017 15th International Conference on ITS Telecommunications (ITST), Warsaw, 2017, pp. 1-5, doi: 10.1109/ITST.2017.7972207.

[127] K. Guan et al., “Channel Sounding and Ray Tracing for Train-to-Train Communications at the THz Band,” 2019 13th European Conference on Antennas and Propagation (EuCAP), Krakow, Poland, 2019, pp. 1-5.

[128] A. S. Cacciapuoti, M. Caleffi, R. Van Meter and L. Hanzo, “When Entanglement Meets Classical Communications: Quantum Teleportation for the Quantum Internet,” in IEEE Transactions on Communications, vol. 68, no. 6, pp. 3808-3833, June 2020, doi: 10.1109/TCOMM.2020.2978071.

[129] Sheng-Tzong Cheng, Chun-Yen Wang and Ming-Hon Tao, “Quantum communication for wireless wide-area networks,” in IEEE Journal on Selected Areas in Communications, vol. 23, no. 7, pp. 1424-1432, July 2005, doi: 10.1109/JSAC.2005.851157.

[130] W. Fawaz, C. Abou-Rjeily and C. Assi, “UAV-Aided Cooperation for FSO Communication Systems,” in IEEE Communications Magazine, vol. 56, no. 1, pp. 70-75, Jan. 2018, doi: 10.1109/MCOM.2017.1700320.

[131] K. Dautov, S. Arzykulov, G. Nauryzbayev and R. C. Kizilirmak, “On the Performance of UAV-enabled Multihop V2V FSO systems over generalized α-μ Channels,” 2018 International Conference on Computing and Network Communications (CoCoNet), Astana, 2018, pp. 69-73, doi:

10.1109/CoCoNet.2018.8476910.

[132] L. Lampe, A. M. Tonello, and T. G. Swart, “Power Line Communications: Principles, Standards and Applications from Multimedia to Smart Grid,” Second Edition, ISBN:9781118676714, 2016 John Wiley & Sons.

[133] Anttonen, A., Ruuska, P., & Kiviranta, M., “3GPP non terrestrial networks: A concise review and look ahead”, VTT Technical Research Centre of Finland, VTT Research Report No. VTT-R-00079-19, 2019

[134] IEEE Std 802.15.4™-2006, “Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)” IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements, 2006

[135] ABI research, “LORAWAN® AND NB-IOT: COMPETITORS OR COMPLEMENTARY?”, 2018 https://lora-alliance.org/resource_hub/lorawan-and-nb-iot-competitors-or-complementary/#:~:text=Low%2DPower%20Wide%2DArea%20(,support%20massive%20numbers%20of%20connections.

[136] ETSI, “ETSI TR 103 526 V1.1.1 (2018-04) “ (https://www.etsi.org/deliver/etsi_tr/103500_103599/103526/01.01.01_60/tr_103526v010101p.pdf)