Internet of Things

Spread Spectrum Multiple Access

- Spread spectrum multiple access (SSMA) uses signals which have a transmission bandwidth whose magnitude is greater than the minimum required RF bandwidth.
  - There are two main types of spread spectrum multiple access techniques
    - Frequency hopped spread spectrum (FHSS)
    - Direct sequence spread spectrum (DSSS)

- **Frequency Hopped Spread Spectrum (FHSS)**
  - This is a digital multiple access system in which the carrier frequencies of the individual users are varied in a pseudo random fashion within a wideband channel
  - The digital data is broken into uniform sized bursts which is then transmitted on different carrier frequencies
- **Direct Sequence Spread Spectrum (DSSS)**
  - This is the most commonly used technology for CDMA
  - In DSSS, the message signal is multiplied by a Pseudo Random Noise Code
  - Each user is given his own code word which is orthogonal to the codes of other users and in order to detect the user, the receiver must know the code word used by the transmitter

GSM → Groupe' Speciale' Moble'

GSM

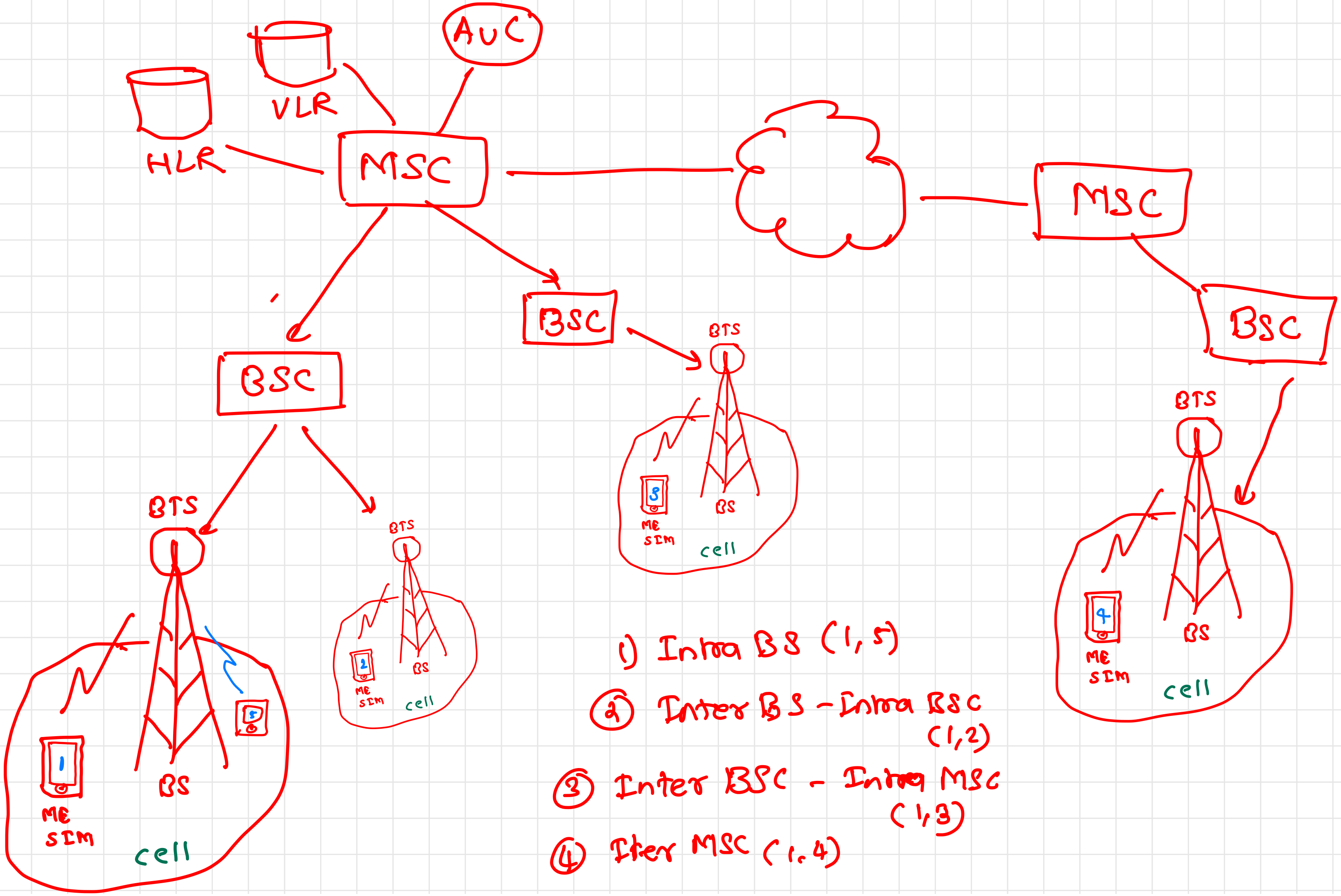
Cellular Network

Cellular Network

- Cellular network is an underlying technology for mobile phones, personal communication systems, wireless networking etc
- The technology is developed for mobile radio telephone to replace high power transmitter/receiver systems
- Cellular networks use lower power, shorter range and more transmitters for data transmission

Features of Cellular Systems

- Offer very high capacity in a limited spectrum
- Reuse of radio channel in different cells
- Enable a fixed number of channels to serve an arbitrarily large number of users by reusing the channel throughout the coverage region
- Communication is always between mobile and base station (not directly between mobiles)
- Each cellular base station is allocated a group of radio channels within a small geographic area called a cell
- Neighboring cells are assigned different channel groups
- By limiting the coverage area to within the boundary of the cell, the channel groups may be reused to cover different cells
- Keep interference levels within tolerable limits
- Frequency reuse or frequency planning
- Organization of Wireless Cellular Network



1) Intra BS (1, 5)

② Inter BS - Intra BSC (1,2)

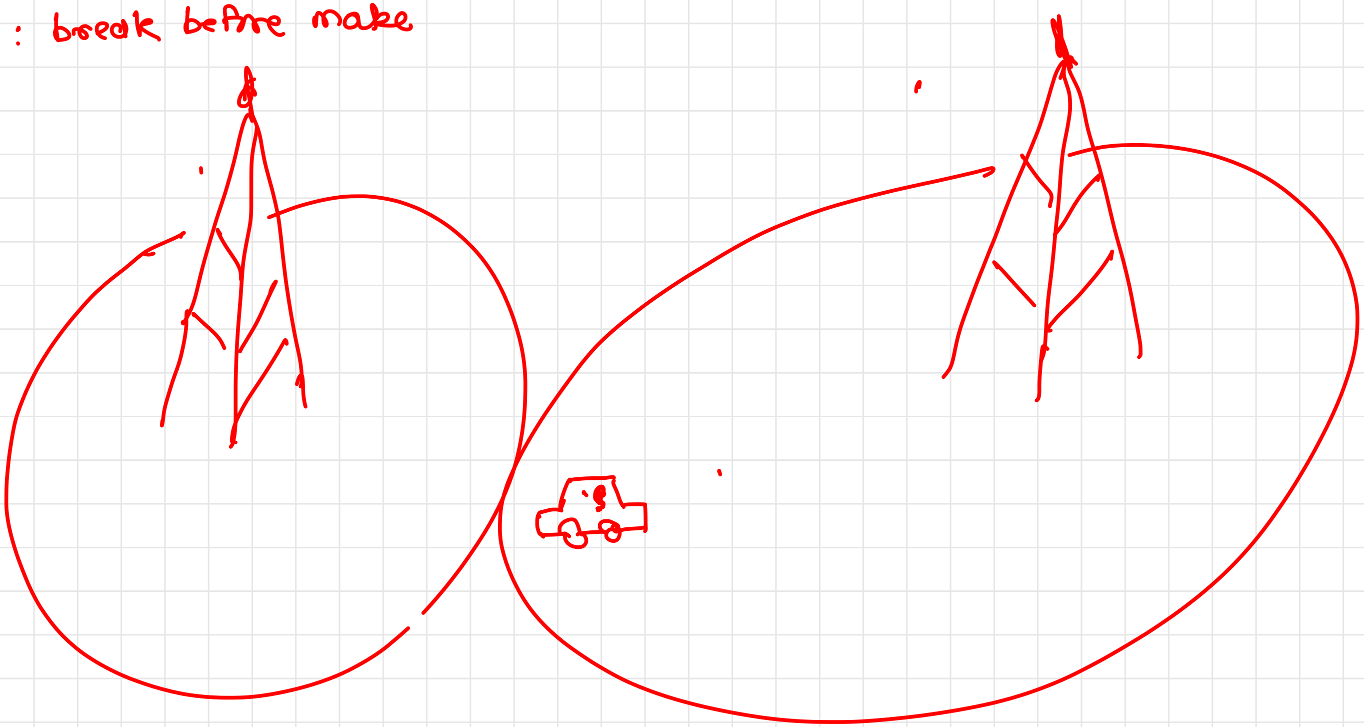
③ Inter BSC - Intra MSC (1,3)

④ Iter MSC (1, 4)

Handoff

→ soft : make before break

→ hard : break before make



Terminologies

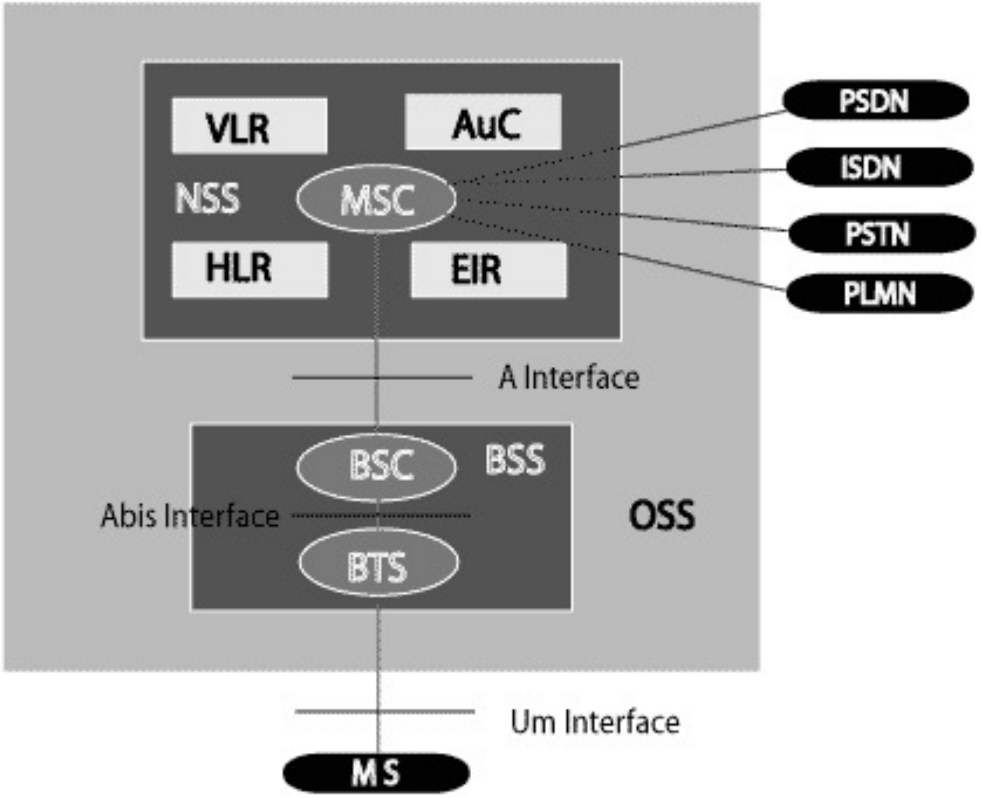
- **Mobile Station (MS)**
  - The Mobile Station (MS) communicates the information with the user and modifies it to the transmission protocols of the air interface to communicate with the BSS
  - The user information communicates with the MS through a microphone and speaker for the speech, keyboard and display for short messaging and the cable connection for other data terminals
  - The mobile station has two elements Mobile Equipment (ME) and Subscriber Identity Module (SIM)
- **Mobile Equipment (ME)**
  - ME is a piece of hardware that the customer purchases from the equipment manufacturer
  - The hardware piece contains all the components needed for the implementation of the protocols to interface with the user and the air-interface to the base stations
- **Subscriber Identity Module (SIM)**
  - This is a smart card issued at the subscription to identify the specifications of a user such as address and type of service
  - The calls in the GSM are directed to the SIM rather than the terminal
  - SMS are also stored in the SIM card
  - It carries every user's personal information which enables a number of useful applications.

Terminologies

- **Base Station (BS)**
  - A base station transmits and receives user data
  - When a mobile is only responsible for its user's data transmission and reception, a base station is capable to handle the calls of several subscribers simultaneously
- **Base Transceiver Station (BTS)**
  - The user data transmission takes place between the mobile phone and the base station (BS) through the base transceiver station
  - A transceiver is a circuit which transmits and receives, i.e., does both
- **Mobile Switching Center (MSC)**
  - MSC is the hardware part of the wireless switch that can communicate with PSTN switches using the Signaling System 7 (SS7) protocol as well as other MSCs in the coverage area of a service provider
  - The MSC also provides for communication with other wired and wireless networks as well as support for registration and maintenance of the connection with the mobile stations

Architecture

- The Mobile Station (MS)
- The Base Station Subsystem (BSS)
- The Network Switching Subsystem (NSS)
- The Operation Support Subsystem (OSS)
- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Equipment Identity Register (EIR)
- Authentication Center (AuC)
- SMS Serving Center (SMS SC)
- Gateway MSC (GMSC)
- Chargeback Center (CBC)
- Transcoder and Adaptation Unit (TRAU)



Overview

- standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for 2G cellular network
- first deployed in Finland in December 1991
- Generations
  - First Generation (1G)
  - Second Generations (2G)
  - Third Generations (3G)
  - Fourth Generation (4G)
  - Fifth Generation (5G)

First Generation

- Speed-2.4 kbps
- Allows voice calls in 1 country
- Use of analog signal
- Poor voice quality
- Poor battery life
- Large phone size
- Limited capacity
- Poor handoff reliability
- Poor security

Second Generation (2G)

- Data speed was upto 64kbps
- Use of digital signals
- Provides better quality and capacity
- Unable to handle complex data such as videos.
- Required strong digital signals to help mobile phones work. If there is no network coverage in any specific area, digital signals would weak
- 2.5 G
  - Implemented GPRS
  - Send/receive e-mail messages
  - Web browsing
  - Speed : 64-144 kbps
  - Camera phones
  - Take a time of 6-9 mins. to download a 3 mins. MP3 song.
- 2.75 G
  - Implemented EDGE

Third Generation (3G)

- Speed 2 Mbps
- Typically called smart phones
- Increased bandwidth and data transfer rates to accommodate web-based applications and audio and video files.
- Provides faster communication
- Send/receive large email messages
- High speed web/more security/video conferencing/3D gaming
- Large capacities and broadband capabilities
- TV streaming/mobile TV/Phone calls
- Expensive fees for 3G licenses services

Fourth Generation (4G)

- Capable of provide 10Mbps-1Gbps speed
- High quality streaming video
- Combination of Wi-Fi and Wi-Max
- High security
- Provide any kind of service at any time as per user requirements anywhere
- Expanded multimedia services
- Low cost per-bit
- Battery uses is more
- Need complicated hardware
- Expensive equipment required to implement next generation network

Fifth Generation (5G)

- It is highly supportable to WWWW (wireless World Wide Web)
- High speed, high capacity
- Provides large broadcasting of data in Gbps.
- Multi-media newspapers, watch TV programs with the clarity(HD Clarity)
- Faster data transmission that of the previous generation
- Large phone memory, dialing speed, clarity in audio/video

IoT security

What is IoT security?

- IoT security refers to the methods of protection used to secure internet-connected or network-based devices
- The term IoT is incredibly broad, and with the technology continuing to evolve, the term has only become broader
- From watches to thermostats to video game consoles, nearly every technological device has the ability to interact with the internet, or other devices, in some capacity
- IoT security is the family of techniques, strategies and tools used to protect these devices from becoming compromised
- Ironically, it is the connectivity inherent to IoT that makes these devices increasingly vulnerable to cyberattacks

IoT security issues

- The more ways for devices to be able to connect to each other, the more ways threat actors can intercept them.
- Protocols like HTTP are just a few of the channels that IoT devices rely on that hackers can intercept
- The IoT umbrella doesn't strictly include internet-based devices either. Appliances that use Bluetooth technology also count as IoT devices and, therefore, require IoT security. Oversights like this have contributed to the recent spike in IoT-related data breaches.
- Challenges
  - Remote exposure
  - Lack of industry foresight
  - Resource constraints
-

How to protect IoT systems and devices

- Introduce IoT security during the design phase
- PKI and digital certificates
- Network security
- API security

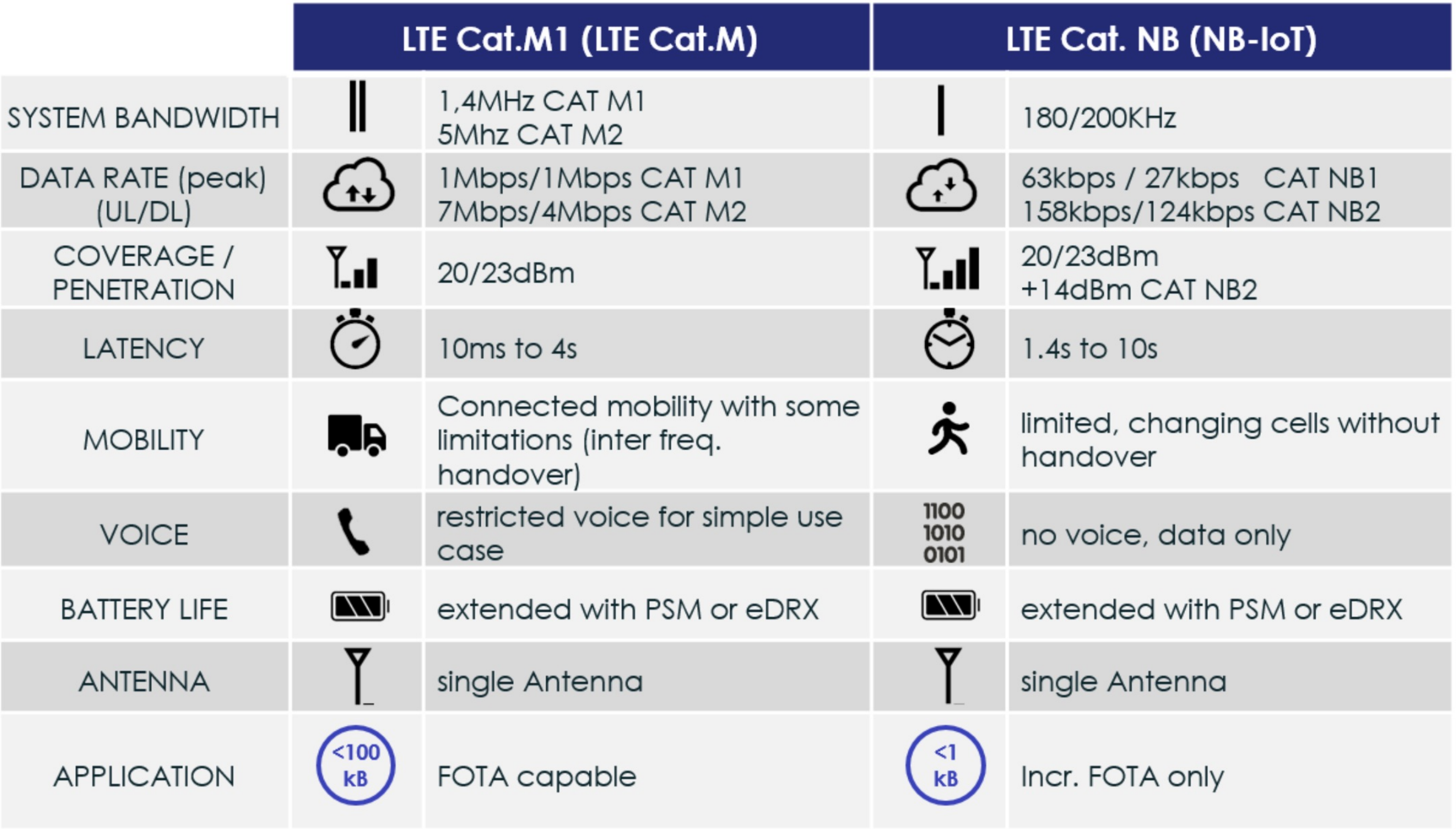
Additional IoT security methods

- **Network access control**
  - NAC can help identify and inventory IoT devices connecting to a network
  - This will provide a baseline for tracking and monitoring devices
- **Segmentation**
  - IoT devices that need to connect directly to the internet should be segmented into their own networks and have restricted access to the enterprise network
  - Network segments should be monitoring for anomalous activity, where action can be taken, should an issue be detected
- **Security gateways**
  - Acting as an intermediary between IoT devices and the network, security gateways have more processing power, memory and capabilities than the IoT devices themselves, which provides them the ability to implement features such as firewalls to ensure hackers cannot access the IoT devices they connect
- **Patch management/continuous software updates**
  - It is critical to provide the means of updating devices and software either over network connections or through automation
  - Having a coordinated disclosure of vulnerabilities is also important for updating devices as soon as possible
  - Consider end-of-life strategies as well

LPWAN

- Low Power Wide Area (LPWA) technology emerged as a term in 2013 not as a new technology standard, but rather as a class of wireless technologies that are well suited to the specific needs of machine-to-machine (M2M) and IoT devices
- The majority of IoT devices, especially those in smart city and industrial sectors, don’t require the same speed and bandwidth of consumer cellular devices. However, they do need the longevity of traditional LTE cellular networks.
- LPWA technology gained prominence as the preferred choice for IoT applications in 2015 when the GSMA wireless industry association defined a series of LPWA Network (LPWAN) standards to help network operators meet the specific cost, coverage and power consumption needs of IoT applications.
- These standards included LTE-M and NB-IoT
- Simultaneously, the LoRa Alliance was formed to strengthen another emerging LPWAN technology adding another wireless connectivity option for low bandwidth, low latency IoT applications.

NB IoT vs LTE M



	LTE Cat.M1 (LTE Cat.M)		LTE Cat. NB (NB-IoT)	
SYSTEM BANDWIDTH	‖	1,4MHz CAT M1 5Mhz CAT M2	|	180/200KHz
DATA RATE (peak) (UL/DL)	☁	1Mbps/1Mbps CAT M1 7Mbps/4Mbps CAT M2	☁	63kbps / 27kbps CAT NB1 158kbps/124kbps CAT NB2
COVERAGE / PENETRATION	📶	20/23dBm	📶	20/23dBm +14dBm CAT NB2
LATENCY	⏱	10ms to 4s	⏱	1.4s to 10s
MOBILITY	🚚	Connected mobility with some limitations (inter freq. handover)	🏃	limited, changing cells without handover
VOICE	☎	restricted voice for simple use case	1100 1010 0101	no voice, data only
BATTERY LIFE	🔋	extended with PSM or eDRX	🔋	extended with PSM or eDRX
ANTENNA	Y	single Antenna	Y	single Antenna
APPLICATION	<100 kB	FOTA capable	<1 kB	Incr. FOTA only