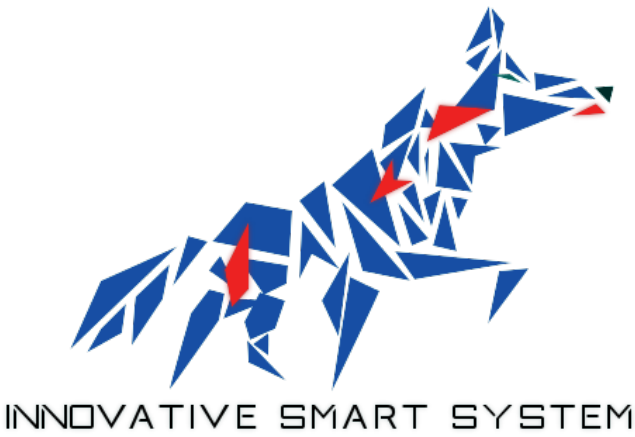


INSA Toulouse - 5ISS

Wireless sensor networks

Machine to machine & LTE-M

Students :
Remi Goalard
Stig Griebenow
David Lacoste
Thang Truong

Teacher :
Daniela Dragomirescu

December 2, 2023

Contents

1 Machine to machine concept

M2M, or "machine to machine" is a concept of direct communication between devices. In M2M, devices communicate straightaway from one to another, without having their data transiting by the cloud, and **without any human action being involved** in the process.

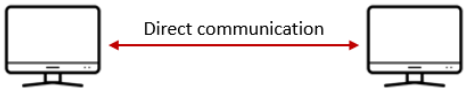


Figure 1: M2M communication between 2 devices

Nowadays, we can find machine to machine systems in a large variety of fields, from road light monitoring to smart house management.

A tricky point about M2M is to understand the difference from the concept of IoT. An IoT system is a collection of devices, servers, and sensors that share volumes of data across a network, often based on a cloud architecture. In M2M, devices communicate **directly** from one to the other, without sharing their data through a cloud. The conceptual difference between both is represented in the figure below.

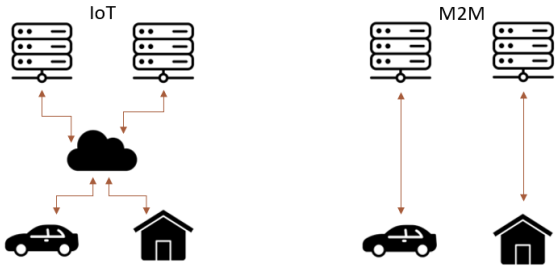


Figure 2: IoT VS M2M

Machine to machine only being a concept with few 'requirements', anyone can create its own m2m system. To balance the freedom this concept provides, companies and independent groups created consortia. Those consortia often publish releases, describing specifications ones can follow to create M2M systems according to the wanted standard. One of the most common standard in Europe is "oneM2M" Those specifications cover various aspects :

- Power consumption
- Scalability
- Security
- Latency
- Interoperability

Once the concept of machine to machine is clear, an important question is still to determine. Which communication protocol to use to share data between devices? Indeed various protocols can be used : Zigbee / Sigfox / NB-IoT / WiFi / BLE... In the following we are going to focus on the study of one of those protocols : **LTE-M(5G)**.

2 LTE-M protocole : layers and characteristics

LTE-M is a **low-power**, **wide-area** network communication protocol standard developed by 3GPP. It is particularly effective to deploy M2M or IoT networks. LTE-M protocol is also known as LTE Cat-M1 or eMTC. LTE-M is build around various layers, each of them dedicated to precise activities : PDCP / RLC / MAC / Physical (annexes 1-2 for more information). In the following, we do the focus on MAC & Physical layers.
There are two types of node in LTE-M networks : eNodeB (base stations) & UE (user equipment = devices). The number of nodes in a network depends on its configuration, but each cell (i.e each eNodeB) can theoretically connect up to **50.000 UE's**.

2.1 Physical layer

The physical layer establish the interface to transfer the data from the MAC layer to another device. In the case of wireless LTE-M, the aforementioned interface is the air. To fulfill its function, the physical layer must deal with various features (annex 2). LTE-M physical layer is a derivative from LTE standard, with a focus on **low-power and wide-area** requirements of IoT applications. This physical layer can be divided into two parts: downlink (annex 3) & uplink (annex 4) :

1. Downlink : Uses OFDM (Orthogonal Frequency Division Multiplexing) to divides the bandwitch into subcarriers. Each subcarriers can be modulated with QPSK - 16QAM - 64QAM. Multiple antenna techniques (transmit diversity - spatial multiplexing) are supported to improve reliability & data rate. Resources elements (one subcarrier in one symbol period) are used to map the channels & signals that form downlink physical layer (annex 5).
2. Uplink : Uses SC-FDMA (Single Carrier Frequency Division Multiple Access), similar to OFDM with lower peak-to-average power ratio. Subcarrier modulations and antennad techniques available are the same as Downlink layer. The big difference lies in the channels and signals deployed (annex 6).

2.2 MAC layer

The MAC layer is responsible for mapping between logical channels and transport channels, multiplexing and demultiplexing of MAC SDUs (Service Data Units) from different logical channels onto transport blocks, scheduling and prioritization of data transmission, HARQ (Hybrid Automatic Repeat Request) retransmission management, and power headroom reporting

2.2.1 Logical channels

The logical channels are defined by the type of data they carry, such as control or traffic data. There are two types of logical channels: control channels and traffic channels. Control channels are used to transmit control information between the network and the user equipment (UE), such as paging, random access, and uplink grants. Traffic channels are used to transmit user data, such as voice, video, or text. There are four types of control channels: PCCH (Paging Control Channel), BCCH (Broadcast Control Channel), CCCH (Common Control Channel), and DCCH (Dedicated Control Channel). There are

two types of traffic channels: DTCH (Dedicated Traffic Channel) and MTCH (Multicast Traffic Channel).

2.2.2 Transport channels

The transport channels are defined by how the data is transmitted over the air interface, such as frequency, time, and coding. There are two types of transport channels: downlink and uplink. Downlink transport channels are used to transmit data from the network to the UE, while uplink transport channels are used to transmit data from the UE to the network. There are four types of downlink transport channels: BCH (Broadcast Channel), DL-SCH (Downlink Shared Channel), PCH (Paging Channel), and MCH (Multicast Channel). There are two types of uplink transport channels: RACH (Random Access Channel) and UL-SCH (Uplink Shared Channel).

2.3 LTE-M frames

LTE standard relies on 2 frames structures :

1. Type 1 : uplink & downlink transmissions separated by frequency (FDD - Frequency Division Duplexing) => 10ms frames divided into ten 1ms sub-frames. Each sub-frame is divided into 2 resource blocks called 'slots' (annex 7).
2. Type 2 : uplink & downlink transmissions separated in time (TDD - Time Division Duplexing) => 10ms frames divided into two 5ms half-frames. Each half-frame follows the structure of type 1 frames, with two 0.5ms 'slots'. Any half-frame contain one 'special frame' used to switch from downlink to uplink (annex 8)

2.4 LTE-M features

LTE-M was created to be a **low-power and wide-area** communication protcol. The following table gives indications about some of the protocol features and their impact on its use :

Feature	Value	Impact
Bandwidth	1.4MHz-5MHz	Narrower than standard LTE bandwidth. Reduces complexity & cost & improves coverage
Device transmit power	20dBm-23dBm	Less than standard LTE (23dBm) Extend battery life => up to 10 years
Duplex mode	full/half	Half duplex mode simplifies device design + reduces interference
Antenna need	only need one	Reduce cost & size (2 antennas in standard LTE)
Peak rate	downlink : 1Mbit/s uplink : 1-7Mbit/s	more than LoRa Bluetooth/2
Extended coverage	5-100km range	18dB more than standard LTE Deeper indoor & rural area reach
Latency	Around 10ms	Low latency : LoRa = 1s / SigFox = 50s NB-IoT = 1.6s / bluetooth = 3ms

Table 1: LTE-M features table

3 Today main concerns : security and energy efficiency

Nowadays, system & network architecture choices are driven both by technical requirements and modern issues. Two main objectives we try to pursue in any project other than creating a working system are **Security** and **Energy efficiency**. Let's have a look at LTE-M protocol through those prisms.

3.1 Security

Unlike previous iterations of mobile network, LTE uses full packet switching and IP. This update allows new attacks that were not possible before. Some LTE network implementations and mobile applications are currently vulnerable at several scales. This leads to loss of confidentiality, incorrect billing and data tampering.

3.1.1 Definition of security

In general terms : "security is a set of measures used to ensure the protection of goods/values". In the IT field, there are two types of assets to protect :

- Data.
- Systems : all the physical/numeric tools used to share data (servers - networks - applications - workstations...).

To protect those assets, security relays on three features :

1. **Authentication** : refers to the procedure by which an entity <A> with which it communicates is authorised. Authenticating a UE therefore involves the network ensuring that it is indeed in contact with the desired person. .
2. **Confidentiality** : data can only be shared with authorized entities. The nature & number of element with which it can be shared is indicated by the level of confidentiality. It is linked to the sensitivity of the data.
3. **Integrity** : ensure the data had not been altered during it's transfer & check the source of the message is the one indicated in the message.

3.1.2 LTE security architecture

In the case of LTE protocol, security architecture is defined by 3GPP's TS 33.401. The following are four main points to look at to secure an LTE network :

- SIM cards & UICC tokens.
- Device & network authentication.
- Air interface protection (Uu).
- Backhaul and network protection (S1-MME, S1-U).

3.1.3 Security method

Let's look at various methods used to protect LTE networks :

1. User or terminal rating : based on crypto card or UICC (Universal Integrated Circuit Card). Sensitive data stored on hardware, can be coupled with encryption operations for authentication.

2. Device and Network Authentication : authentication & access to LTE network based on AKA protocol. Completion of AKA protocol generates the required keys for encryption.
3. Radio network side :The connection between the UE and the eNodeB is referred to as the air interface
4. IPSEC tunnels : using those links between U-TRAND & EPC offers protection by reinforcing integrity & confidentiality.

Despite security measures, there are still threats on the user side, such as identity theft or call interception, as well as physical, deterioration or software attacks on the network core.

3.2 Energy efficiency

the energy consumption & efficiency of a system is very complex to determine, as it depend on the protocols used, but also all the hardware equipment and their condition. In the case of data transmission protocol, one of the best indicator is to look at the energy needed to transfer each bit of data.
For LTE-M protocol, an empirical result was searched in a study from 2020 (Ekman, T., & Jönson, S. (2020). An empirical study of cellular-IoT). Results in the following table :

	100 B	1000 B
Avg. E/B	0.96 [mJ]	0.11 [mJ]
Ratio		0.11065

Table 4.2: Energy per Byte and ratio between 1000 B and 100 B transmitted, LTE-M.

Ekman, T., & Jonsson, S. (2020). An empirical study of cellular-IoT

Figure 3: Energy efficiency

4 Conclusion

Among all the protocols available to create machine to machine networks, it can be hard to make a choice and decide which one to use. Various protocol characteristics, features or facilities have to be taken into account to evaluate which one is the more relevant.
The previous sections tried to cover number of those criteria, to help anyone who wants to design it's own M2M system to know if LTE-M is the protocol he should rely on.
Annex 10 contains all the LTE-M specific characteristics that we consider important. In addition, Appendices 11 to 13 are a good complement for anyone who would like to compare, or use a tool to choose which protocol to use.

5 References

1. LTE Overview : https://rfmw.em.keysight.com/wireless/helpfiles/89600B/WebHelp/subsystems/lte/content/lte_overvew.htm?fbclid=IwAR2HjezMC2DVnPG1Q1G4i5KcYobR1Mgli1MvUvKWFhoakQBZSpS8M6ZApQQ

2. LTE Protocol Stack Layers : https://www.tutorialspoint.com/lte/lte_protocol_stack_layers.htm

3. Physical Layer Overview : https://rfmw.em.keysight.com/wireless/helpfiles/89600B/WebHelp/subsystems/lte/content/lte_overview.htm?fbclid=IwAR2HjezMC2DVnPG1Q1G4i5KcYobR1Mgli1MvUvKWFhoakQBZSpS8M6ZApQQ

4. LTE info : https://www.gsma.com/iot/wp-content/uploads/2019/08/201906-GSMA-LTE-M-Deployment-Guide-v3.pdf

5. LTE-M, les points essentiels à maîtriser avant de choisir ce réseau : https://www.matooma.com/fr/s-informer/actualites-iot-m2m/ltem-avantages-specificites-techniques

6. LTE-M wikipedia : https://en.wikipedia.erg/wiki/LTE-M

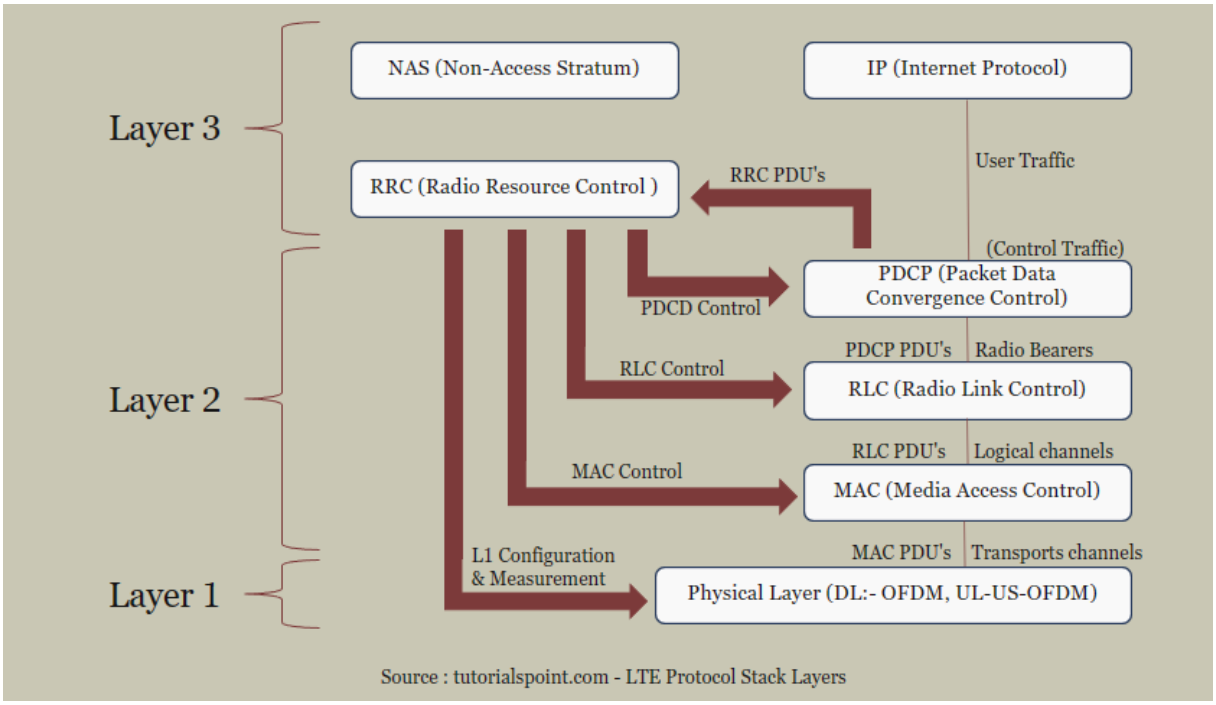
7. LTE communication channels : https://www.tutorialspoint.com/lte/lte_communication_channels.htm

8. LTE-M Protocol Stack | Protocol layers of LTE-M stack : https://www.rfwireless-world.com/Terminology/LTE-M-Protocol-Stack.html

A Annexe :

Complementary information - additional resources

A.1 LTE protocol stack



Source : tutorialspoint.com - LTE Protocol Stack Layers

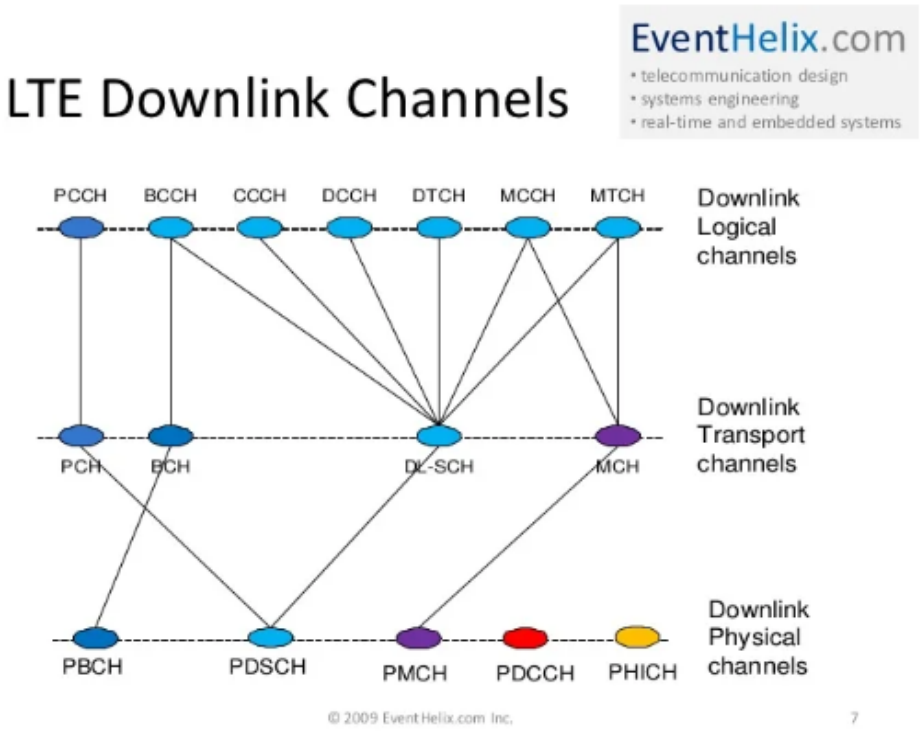
A.2 LTE protocol stack & functions

LTE-M layers & associated functions

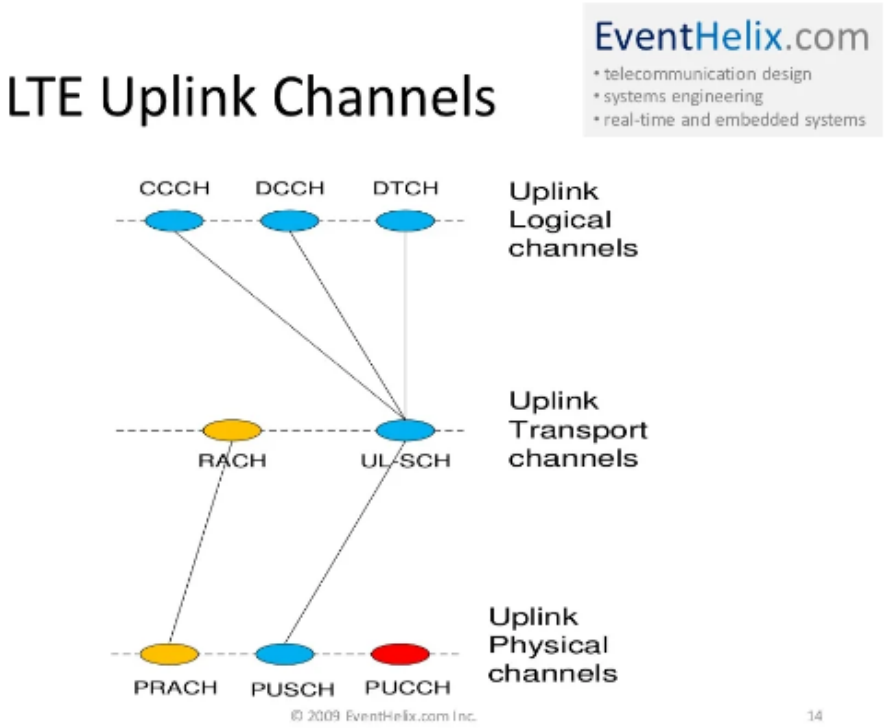
PDCP : Packet Data Convergence Control	Sequence number addition - Handover data handling - Integrity protection – Ciphering - Header compression - In sequence delivery - Duplicate packet detection - Integrity validation – Deciphering - Header decompression
RLC : Radio Link Control	Buffer status report - Segmentation and concatenation - ARQ (for AM mode) - Re-ordering – Assembly - ARQ (for AM mode)
MAC : Medium Access Control	Channel mapping – Multiplexing - Handling control elements - Random access procedure - Logical channel priority – HARQ - Sending BSRs
Physical	CRC attachment - Coding block - Scrambling/descrambling - Modulation/de-modulation – Measurement - Resource element mapping/demapping – HARQ - MIMO

Source : tutorialspoint.com – LTE Protocol Stack Layer

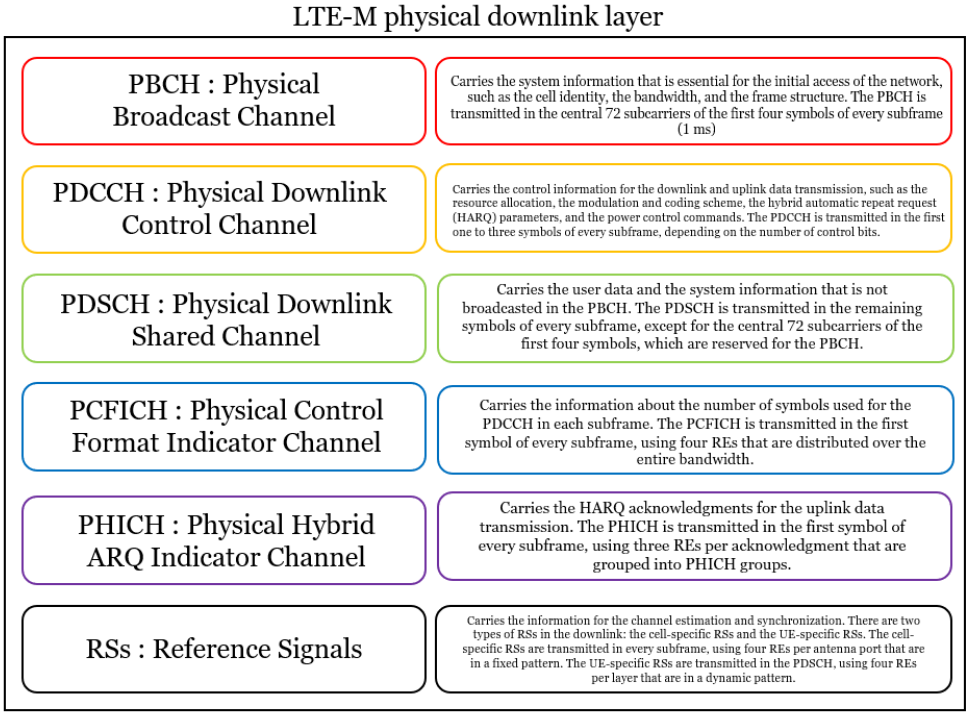
A.3 LTE downlink channels



A.4 LTE uplink channels

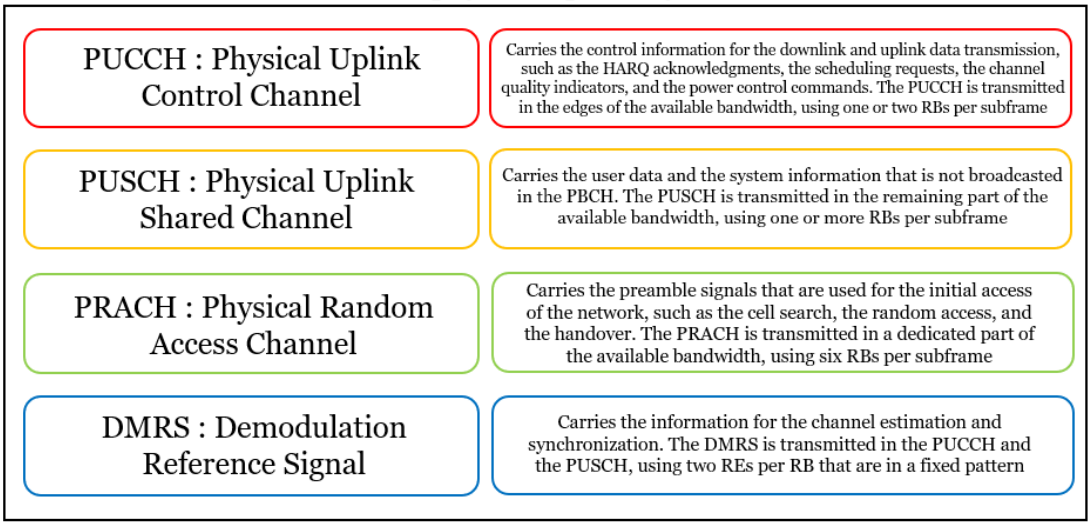


A.5 LTE-M physical downlink layer



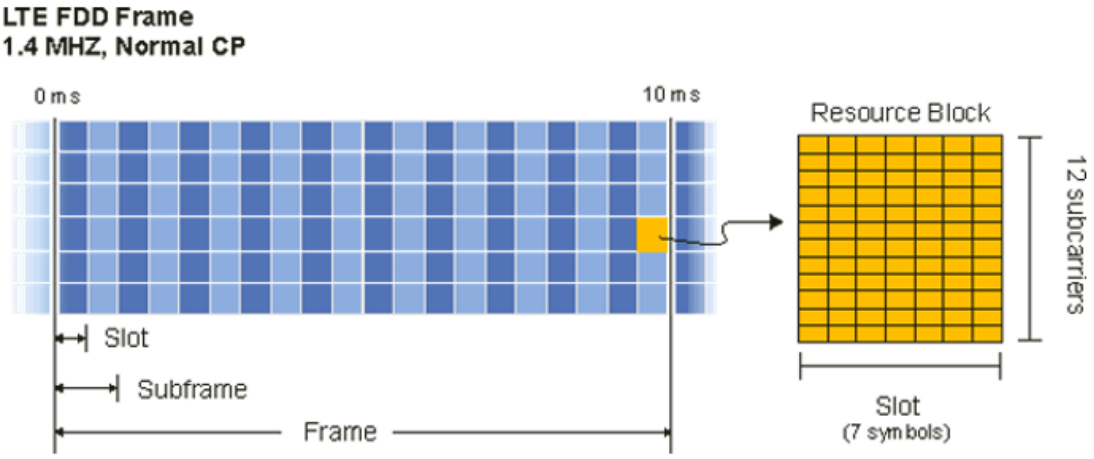
Source : EventHelix.com – LTE Downlink channels

A.6 LTE-M physical uplink layer



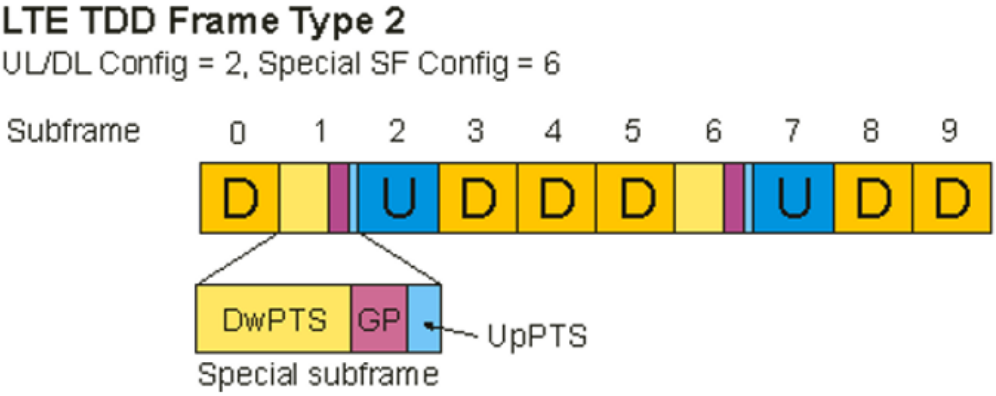
Source : EventHelix.com – LTE uplink channels

A.7 LTE-M type 1 frames



Source : https://rfmw.em.keysight.com/wireless/helpfiles/89600B/WebHelp/subsystems/lte/content/lte_overview.htm

A.8 LTE-M type 2 frames



Source : https://rfmw.em.keysight.com/wireless/helpfiles/89600B/WebHelp/subsystems/lte/content/lte_overview.htm

A.9 Energy efficiency empiric study

	100 B	1000 B
Avg. E/B	0.96 [mJ]	0.11 [mJ]
Ratio		0.11065

Table 4.2: Energy per Byte and ratio between 1000 B and 100 B transmitted, LTE-M.

Ekman, T., & Jinsson, S. (2020). An empirical study of cellular-IoT.

A.10 LTE-M protocol characteristics recap

Number of nodes per network	50.000
Range	From 5 to 100km
Data rate	1-7Mbit/s (depend on mode) => quite high
Energy per byte	0.96-0.11 mJ/byte
Latency	10 ms
Power consumption	Best at medium data rates
Indoor penetration	Good
Bandwidth	1.4 Mhz or 5 Mhz
Device cost	Medium to high

A.11 LTE-M compared to other protocols

Feature	LTE-M	LoRaWAN	Bluetooth	Sigfox	NB-IoT
Bandwidth	1.4 MHz or 5 MHz	125 kHz, 250 kHz, or 500 kHz	1 MHz or 2 MHz	100 Hz	200 kHz
Data rate	Up to 1 Mbit/s (uplink and downlink)	Up to 50 kbit/s (uplink and downlink)	Up to 2 Mbit/s (Bluetooth 5.0)	Up to 100 bit/s (uplink) and 600 bit/s (downlink)	Up to 250 kbit/s (uplink and downlink)
Latency	About 10 ms	About 1 s	About 3 ms (Bluetooth 5.0)	About 50 s	About 1.6 s
Mobility	Full duplex or half duplex mode, handover support	Half duplex mode, no handover support	Full duplex mode, handover support	Half duplex mode, no handover support	Half duplex mode, no handover support
Voice support	VoLTE or CSFB	VoIP (third-party)	Yes	VoIP (third-party)	No
Deployment	Existing LTE networks	Dedicated gateways and base stations	Peer-to-peer or mesh network	Dedicated gateways and base stations	Existing 2G or 4G networks
Spectrum	Licensed	Unlicensed	Unlicensed	Unlicensed	Licensed
Device transmit power	20 dBm or 23 dBm	Up to 14 dBm	Up to 10 dBm (Bluetooth 5.0)	Up to 16 dBm	20 dBm or 23 dBm
Device battery life	Up to 10 years	Up to 10 years	Up to 5 years	Up to 10 years	Up to 10 years
Device cost	Medium to high	Low to medium	Low	Low	Medium to high

A.12 How to choose your protocol?