990117

Internet of Things

IoT Communications and Networking Technologies and Protocols

Mehdi Rasti

Amirkabir University of Technology

Spring 2020

Contents

- شبکه عادی که ما داریم چه تفاوت هایی خواهد داشت زمانی که ما میخواهیم اون رو در اختیار اینترنت اشیاء قرار بدهیم؟
- آیا شبکه های ارتباطی فعلی مناسب برای اینترنت اشیاء هستند؟

Contents

- Introduction
  - Connecting Smart Objects
  - IoT Protocol Stack (Standards, Protocols and Technologies)
- Physical and Link Layers Protocols (IoT Access Technologies)
- Network Layer Protocols (IP as the IoT Network Layer)
- Transport Layer Protocols
- Application Layer Protocols

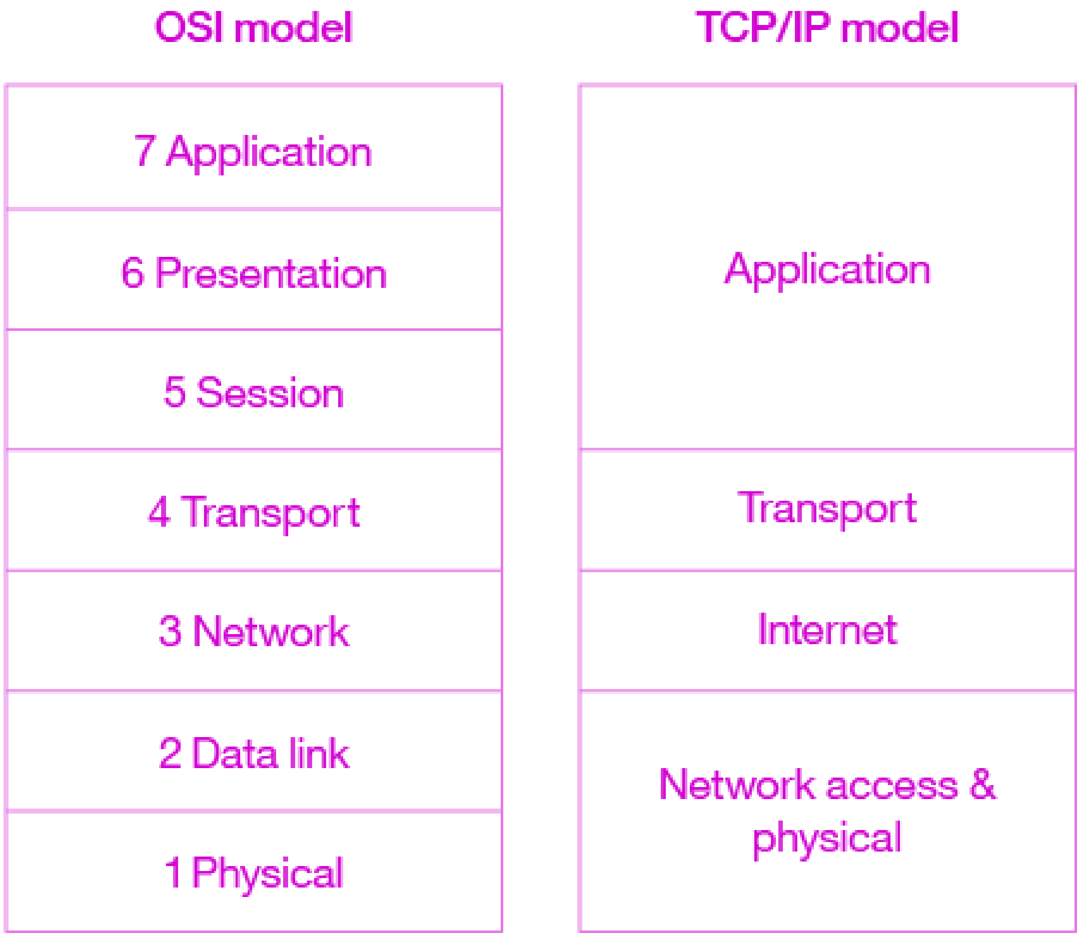
IoT Protocol Stack: Why layering

Dealing with complex systems:

- *explicit structure* allows *identification* relationship of complex system's pieces
  - layered ***reference model*** for discussion
- *modularization* eases maintenance, updating of system
  - change of implementation of layer's service ***transparent*** to rest of system
  - e.g., change in gate procedure doesn't affect rest of system

IoT Protocol Stack

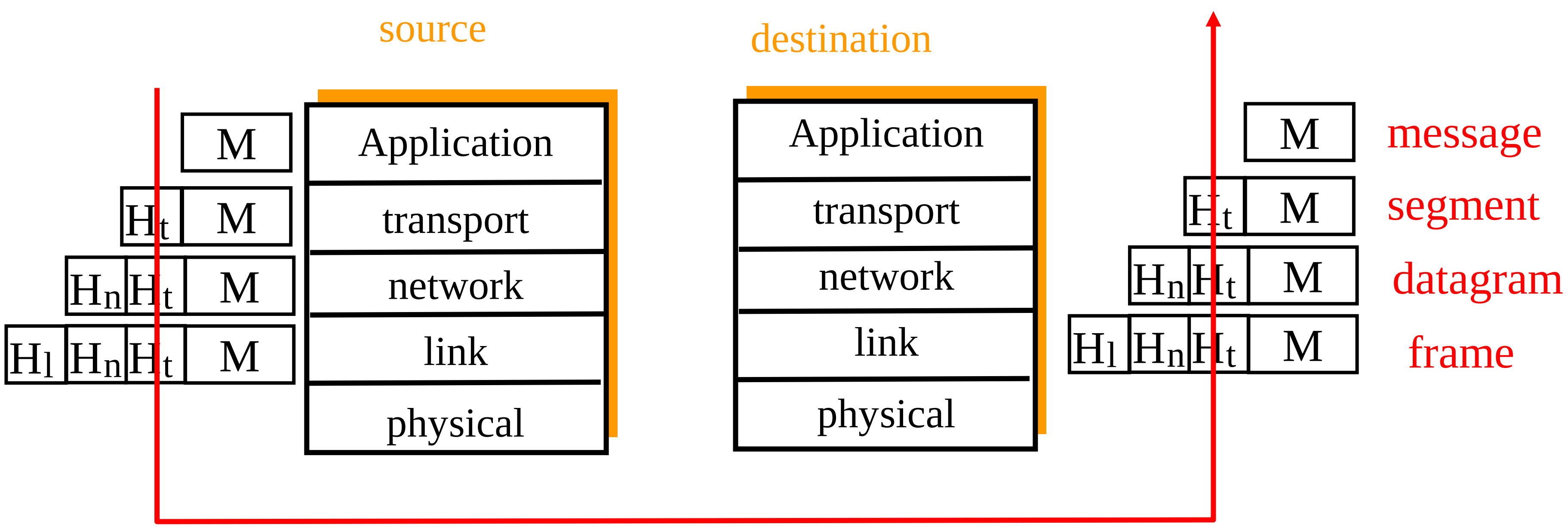
- OSI and TCP/IP Networking Models



Protocol layering and data

Each layer takes data from above

- adds header information to create new data unit
- passes new data unit to layer below



Physical and Link Layers Protocols- IEEE 802.15.4

- “Networking Technologies”
  - Enable IoT devices to communicate with other devices, applications, and services running in the cloud
    - **Network Access & Physical Layer,”** (*Chapter 4) .
    - **Internet Layer:** IP as the IoT Network Layer (*Chapter 5)
    - **Transport & Application Layers** (*Chapter 6)

  - As you look further down the stack toward physical transmission technologies, you face more challenges that are specific to IoT devices and IoT contexts.
    - هرچی پایین تر میایم ماهیت اینترنت اشیاء خودش رو بیشتر نشون میده.
    - لایه های پایین تر تغییرات عمده تر هستند.

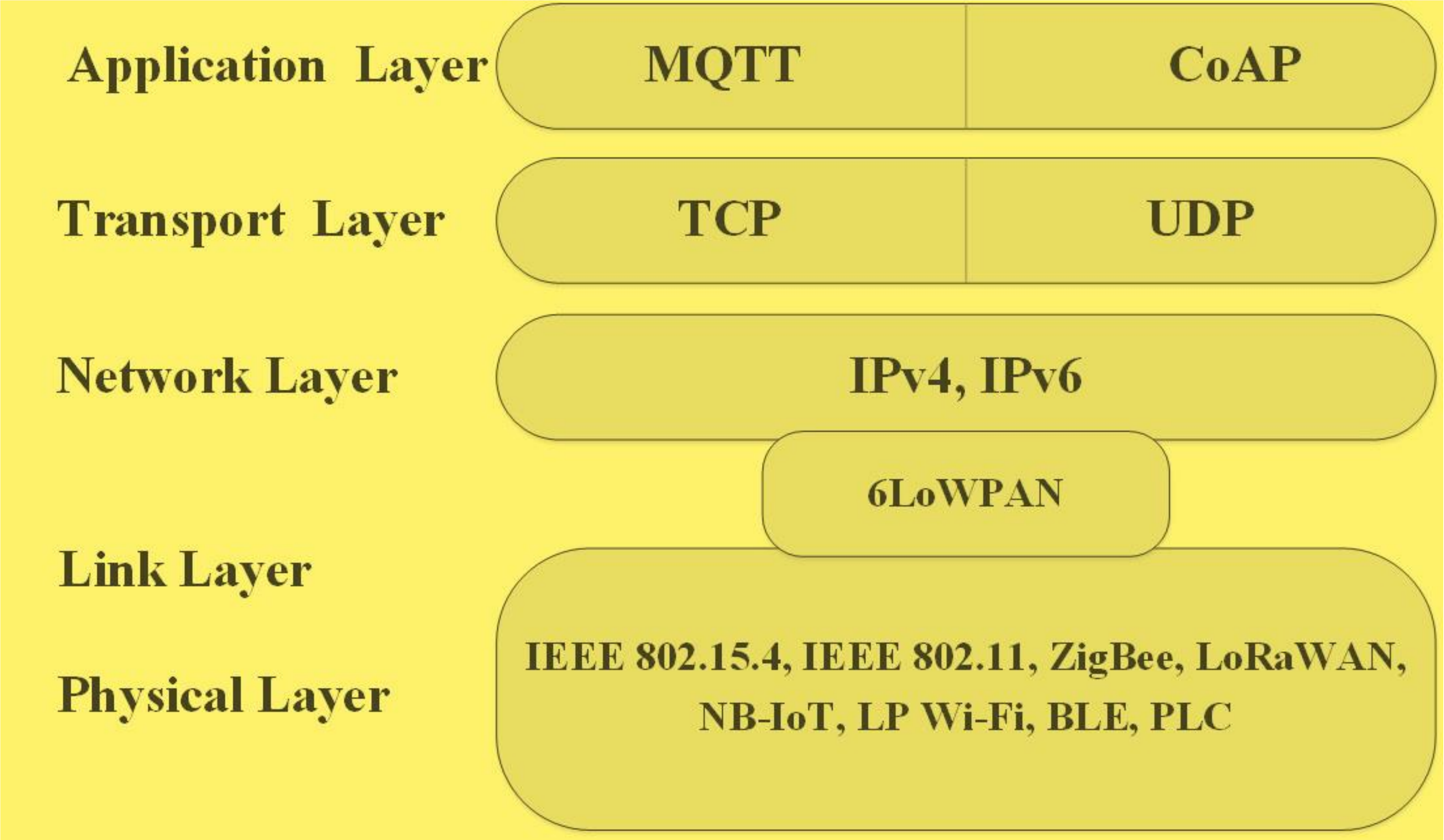
IoT Protocol Stack

- **IoT network protocols mapped to the TCP/IP model**

TCP/IP model	IoT protocols
Application	HTTPS, XMPP, CoAP, MQTT, AMQP
Transport	UDP, TCP
Internet	IPv6, 6LoWPAN, RPL
Network access & physical	IEEE 802.15.4 Wifi (802.11 a/b/g/n) Ethernet (802.3) GSM, CDMA, LTE

- جدول خیلی خوبه

IoT Protocol Stack



Contents

- Introduction
- Physical and Link Layers Protocols (IoT Access Technologies)
    - Physical Layer Issues ۴ الی ۵ جلسه
    - Communication Technologies Criteria
    - Communication Technologies and Protocols جزئیات اون پرتکل ها
- Network Layer Protocols (IP as the IoT Network Layer)
- Transport Layer Protocols
- Application Layer Protocols

Contents

Physical Layer issues

- Media (Electrical Channel)
- Frequency Ranges
- Signal
  - Signal Power
  - Signal Frequency Spectrum
  - Signal Propagation
- Transceivers Structure
  - Modulation and Demodulation
  - Coding

Physical Media

- Transmission Medium
  - Physical path between transmitter and receiver

- Categories of physical medium
  - Guided Media سیمی هستند
    - Waves are guided along a solid medium
    - E.g., copper twisted pair, copper coaxial cable, optical fiber
  - Unguided Media روی هوا
    - Provides means of transmission but does not guide electromagnetic signals
    - Usually referred to as wireless transmission
    - E.g., atmosphere, outer space

Difference Between Wireless and Wired Networks

- Layers Affected by the Wireless Transmission
  - Wireless and Wired Networks are not so different at application and transport layers!
  - They are mostly different at following layers:

- Physical Layer
  - Media (Electrical Channel)
  - Frequency range
  - Signal
  - Modulation and Demodulation
  - Multiplexing

- Data Link Layer
  - Logical link control (LLC)
  - Media Access Control (MAC)

- Network Layer
  - Packet Forwarding
  - Routing

Frequency Range

- **Radio**
  - **Signal carried in electromagnetic spectrum** **تعریف سیگنال رادیویی:**

  - **Propagation environment effects:**
    - **Reflection**
    - **Obstruction by objects**
    - **Interference**

Frequency Range

دلایل انتخاب ها

Frequency	Wavelength	Designation	Abbreviation	
3 - 30 Hz	10^5km-10^4km	Extremely low frequency	ELF	
30 - 300 Hz	10^4km-10^3km	Super low frequency	SLF	
300 - 3000 Hz	10^3km-100km	Ultra low frequency	ULF	
3 - 30 kHz	100km-10km	Very low frequency	VLF	
30 - 300 kHz	10km-1km	Low frequency	LF	
300 kHz - 3 MHz	1km-100m	Medium frequency	MF	
3 - 30 MHz	100m-10m	High frequency	HF	
30 - 300 MHz	10m-1m	Very high frequency	VHF	
300 MHz - 3 GHz	1m-10cm	Ultra high frequency	UHF	
3 - 30 GHz	10cm-1cm	Super high frequency	SHF	
30 - 300 GHz	1cm-1mm	Extremely high frequency	EHF	
300 GHz – 3 THz	1 mm – 0.1 mm	Tremendously high frequency	THF	

Radio Frequency **فرکانس هایی که اگر یک سیگنال در قالب اون ها ارسال بشه قابلیت رادییشن پیدا می کنه**

- **Required antenna size for good reception is inversely proportional to the signal frequency**
  - **<u>so moving to a higher frequency allows for more compact antennas</u>**
    - سایز آنتن با معکوس فرکانس رابطه داره.
    - *****اندازه آنتن یک چهارم طول موج هستش*****
    - نسل های جدید دارن به سمت فرکانس های بالاتر می روند.

- **Received signal power with nondirectional همه جهته antennas is proportional to the inverse of frequency squared.**
  - **So it’s hard to cover large distances with higher frequency signals (with nondirectional antennas)**
    - توان دریافتی حتماً از توان اولیته کمتره (تضعیف میشه) چون موج تضعیف میشه.
    - هرجی فرکانس بالاتر بره افت قدرت کمتر میشه. حال قانون بالایی رو میگیره.

Frequency Range

- **Radio frequency range**
  - 30 MHz to 30 GHz : فرکانس های رادیویی جذاب VHF – UHF – SHF ** **3GH TO 6GH** **
  - Suitable for omnidirectional applications
  - Frequencies of 1 GHz and above are conventionally called microwave
  - کنترل ها که مادون قرمز هستن تضعیف زیاد دارن و...
- **Millimeter Wave**
  - Frequencies of 30 GHz and above are designated .
- **Infrared frequency range**
  - Roughly, 3x10^11 (300 GHz) to 2x10^14 (200 THz)
  - Useful in local point-to-point multipoint applications within confined areas

Frequency Range

- **Most wireless applications reside in radio frequency between 30MHz to 30 GHz (VHF, UHF and SHF)**

- **Why these frequencies?**
  - They are not affected by earth curvature
  - Require only moderated size antennas

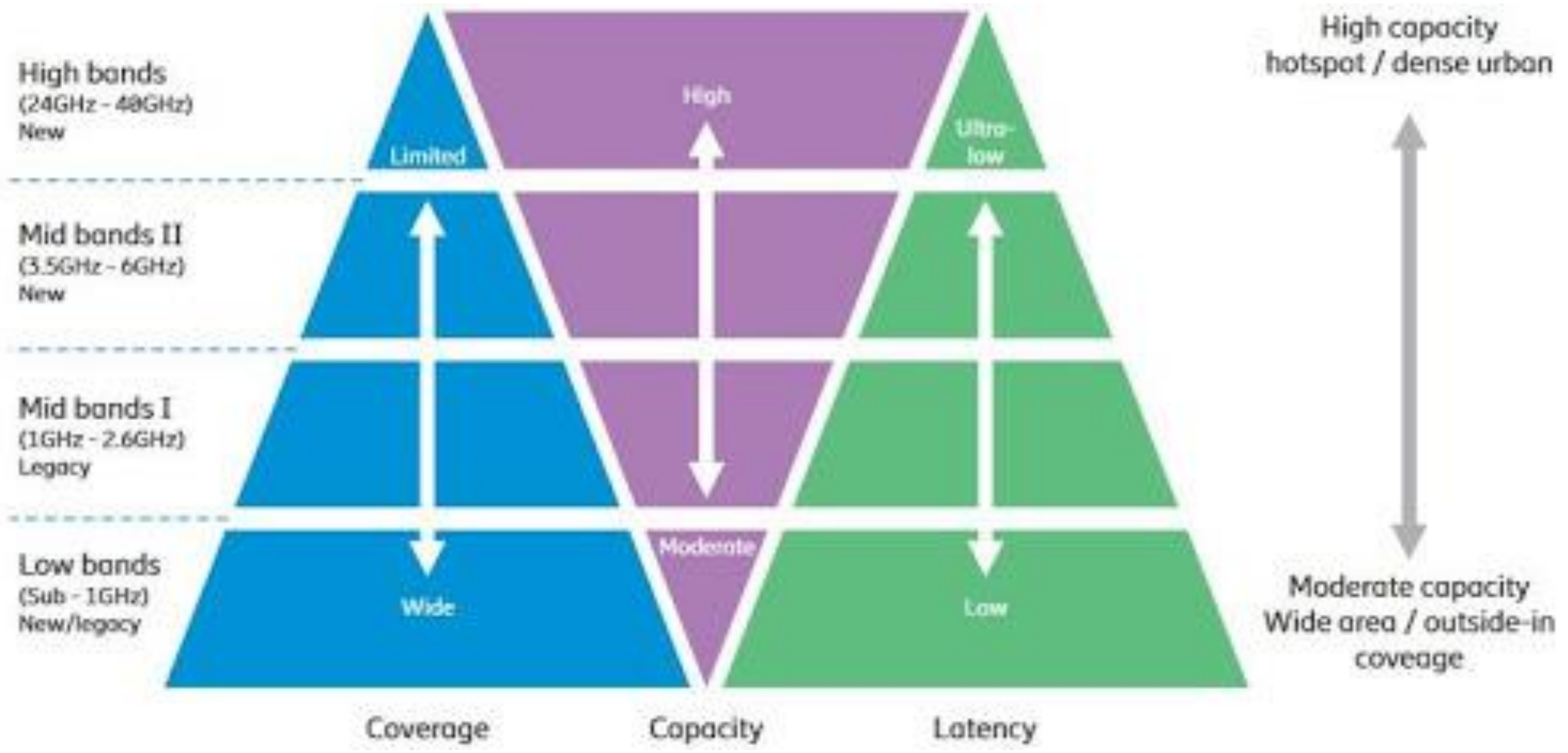
Example of ISM frequency allocation نیاز به مجوز نداره

Frequency range		Center frequency	Bandwidth	Type	Availability	Licensed users
6.765 MHz	6.795 MHz	6.78 MHz	30 kHz	A	Subject to local acceptance	FIXED SERVICE & Mobile service
13.553 MHz	13.567 MHz	13.56 MHz	14 kHz	B	Worldwide	FIXED & Mobile services except Aeronautical mobile (R) service
26.957 MHz	27.283 MHz	27.12 MHz	326 kHz	B	Worldwide	FIXED & MOBILE SERVICE except Aeronautical mobile service, CB Radio
40.66 MHz	40.7 MHz	40.68 MHz	40 kHz	B	Worldwide	Fixed, Mobile services & Earth exploration-satellite service
433.05 MHz	434.79 MHz	433.92 MHz	1.74 MHz	A	only in Region 1, subject to local acceptance	AMATEUR SERVICE & RADIOLOCATION SERVICE, additional apply the provisions of footnote 5.280. For Australia see footnote AU.
902 MHz	928 MHz	915 MHz	26 MHz	B	Region 2 only (with some exceptions)	FIXED, Mobile except aeronautical mobile & Radiolocation service; in Region 2 additional Amateur service
2.4 GHz	2.5 GHz	2.45 GHz	100 MHz	B	Worldwide	FIXED, MOBILE, RADIOLOCATION, Amateur & Amateur-satellite service
5.725 GHz	5.875 GHz	5.8 GHz	150 MHz	B	Worldwide	FIXED-SATELLITE, RADIOLOCATION, MOBILE, Amateur & Amateur-satellite service
24 GHz	24.25 GHz	24.125 GHz	250 MHz	B	Worldwide	AMATEUR, AMATEUR-SATELLITE, RADIOLOCATION & Earth exploration-satellite service (active)
61 GHz	61.5 GHz	61.25 GHz	500 MHz	A	Subject to local acceptance	FIXED, INTER-SATELLITE, MOBILE & RADIOLOCATION SERVICE
122 GHz	123 GHz	122.5 GHz	1 GHz	A	Subject to local acceptance	EARTH EXPLORATION-SATELLITE (passive), FIXED, INTER-SATELLITE, MOBILE, SPACE RESEARCH (passive) & Amateur service
244 GHz	246 GHz	245 GHz	2 GHz	A	Subject to local acceptance	RADIOLOCATION, RADIO ASTRONOMY, Amateur & Amateur-satellite service

Frequency Range

990117

- Frequency Bands



*

990119

- Signal:
  - **physical representation of data**
  - function of time and location
  - **signal parameters:**
    - parameters representing the value of data
  - classification

    continuous time/discrete time

    continuous values/discrete values

    analog signal = continuous time and continuous values

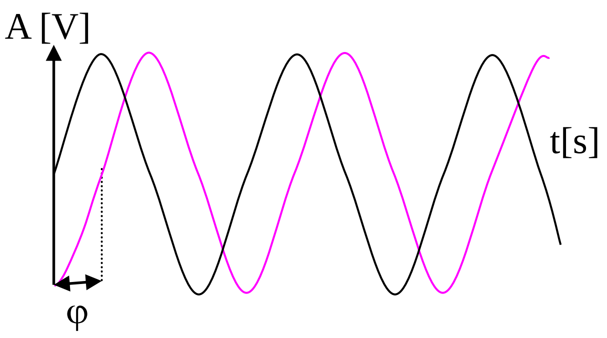
    digital signal = discrete time and discrete values
  - **signal parameters of periodic signals:**
    - **period T, frequency f=1/T, amplitude A, phase shift φ sine wave as special periodic signal for a carrier:**

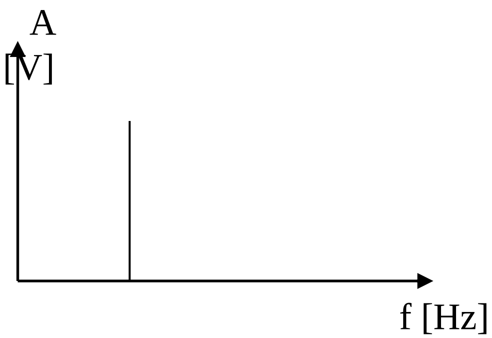
$$s(t) = A_t \sin(2 \pi f_t t + \varphi_t)$$

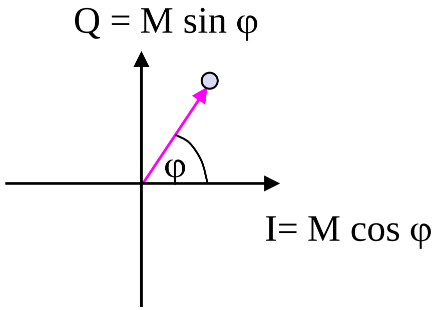
فاز – فرکانس – امپلیتود

Signal

- **Different representations of signals**
  - amplitude (amplitude domain)
  - frequency spectrum (frequency domain)
  - phase state diagram (amplitude M and phase φ in polar coordinates)







- **Composed signals transferred into frequency domain using Fourier transformation**
- **Digital signals need**
  - infinite frequencies for perfect transmission
  - modulation with a carrier frequency for transmission (analog signal!)

Signal Propagation Ranges

- **Propagation in free space always like light (straight line, line of sight)**
- **Receiving power proportional to**

  $1 / (d \times f)^2$ (ideal)

  $1/(d \times f)\alpha$ (α=3…4 realistically)

  d = distance between sender and receiver

- **Receiving power additionally influenced by**

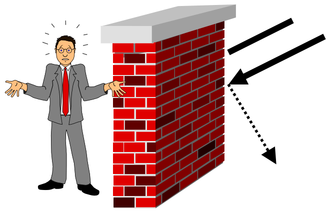
  fading (frequency dependent)

  shadowing

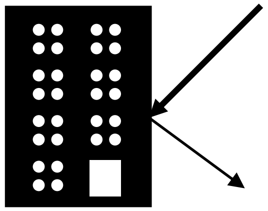
  reflection at large obstacles

  scattering at small obstacles

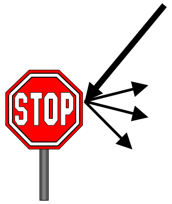
  diffraction at edges



shadowing



reflection



scattering

diffraction

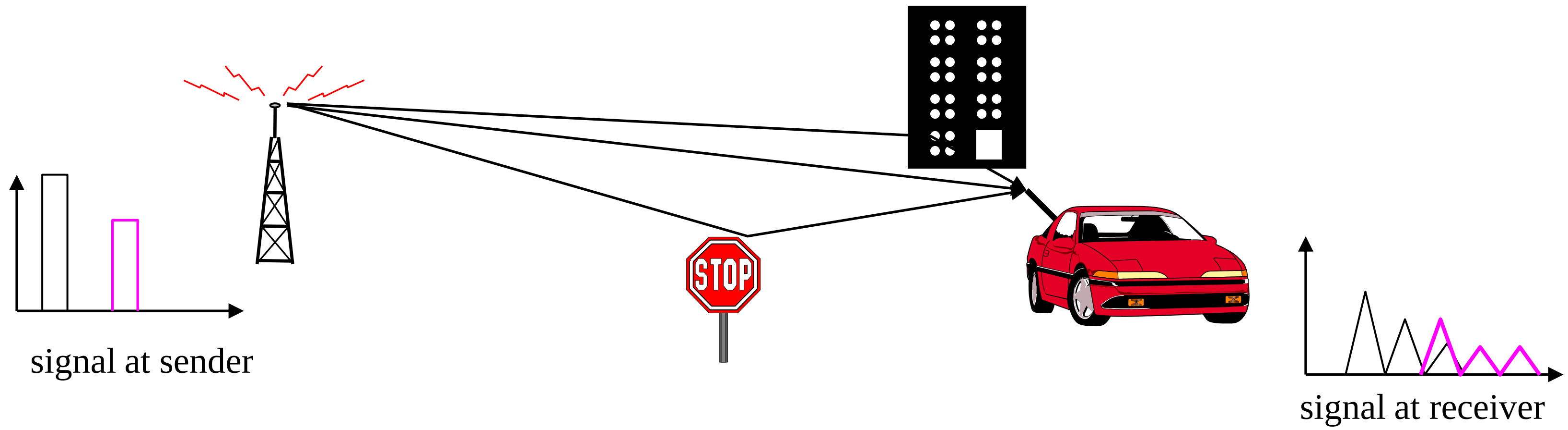
Multipath propagation

- **Time dispersion: signal is dispersed over time**

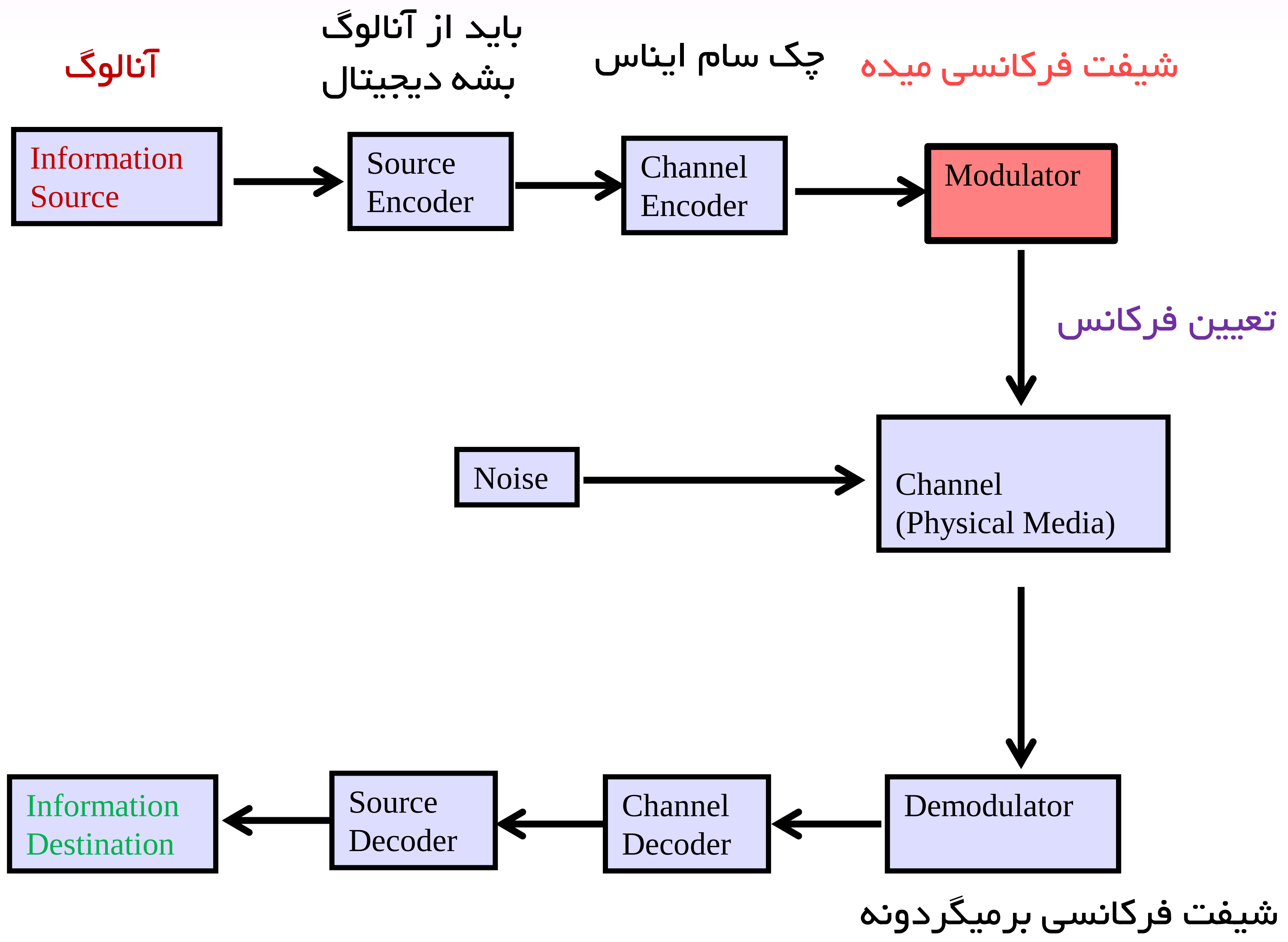
  interference with “neighbor” symbols, Inter Symbol Interference (ISI)

- **The signal reaches a receiver directly and phase shifted**

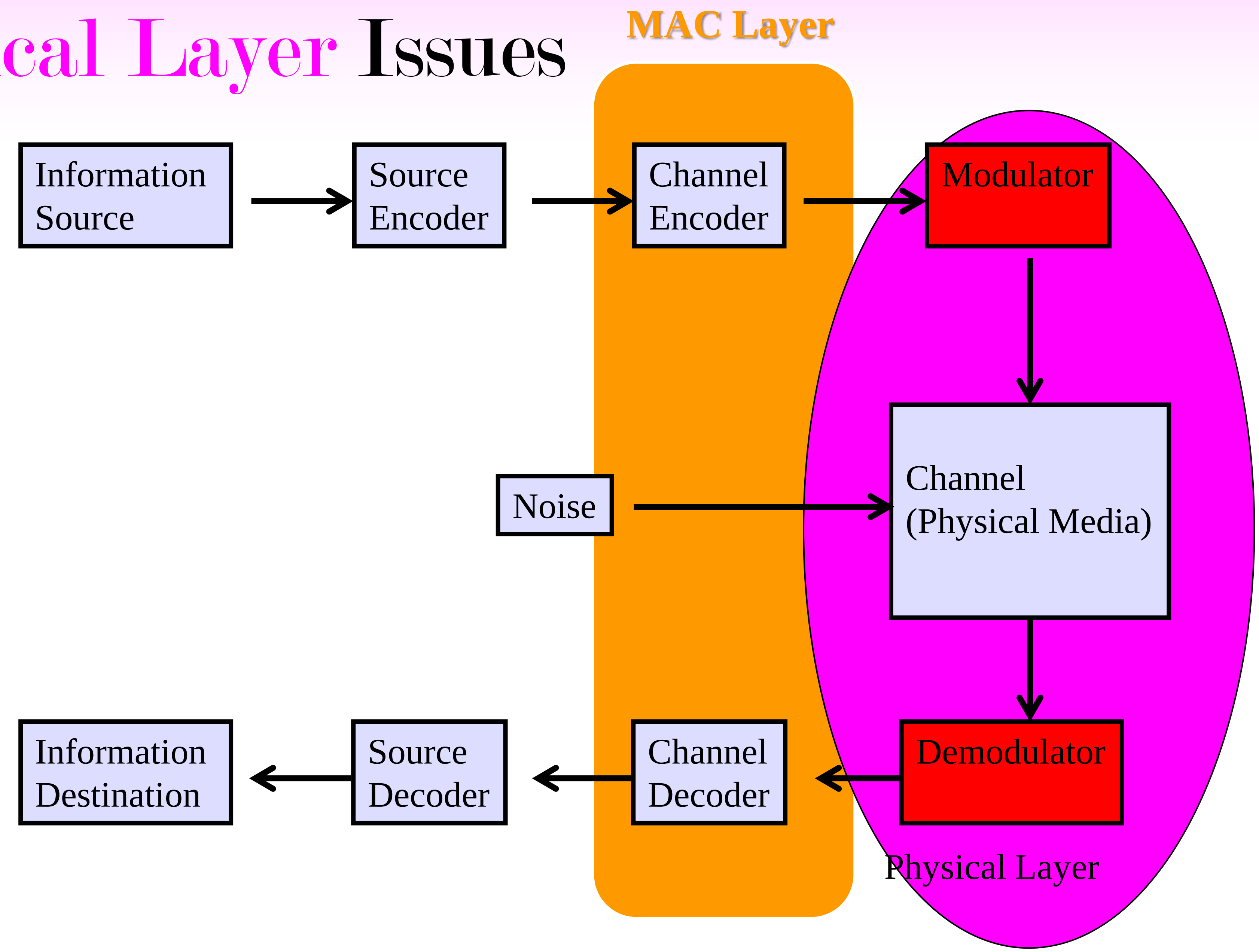
  distorted signal depending on the phases of the different parts



Transceiver Structure: Communications Block Diagram

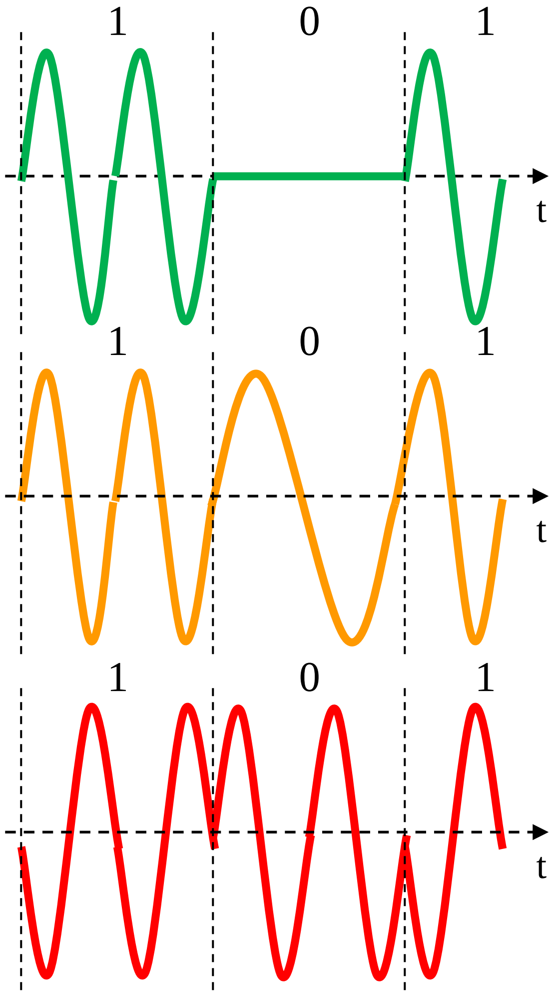


Physical Layer Issues



Modulation

- Transceiver Structure
  - **Digital modulation**
    - Digital data is translated into an analog signal (baseband) ASK, FSK, PSK
    - **Differences in spectral efficiency, power efficiency, robustness**
  - **Analog modulation**
    - Shifts center frequency of baseband signal up to the radio carrier
  - **Motivation**
    - Smaller antennas (e.g., $\lambda/4$)
    - Frequency Division Multiplexing
    - Medium characteristics



Contents

- Introduction
- Physical and Link Layers Protocols (IoT Access Technologies)
    - Physical Layer Issues
    - Communication Technologies Criteria معیار های انتخاب فناوری ارتباطی
    - Communication Technologies and Protocols
- Network Layer Protocols (IP as the IoT Network Layer)
- Transport Layer Protocols
- Application Layer Protocols

Physical and Link Layers Protocols- IEEE 802.15.4

- Two main sections divide this lecture:
  - “Communications Criteria,”
    - Describes the characteristics and attributes you should consider when selecting and dealing with connecting smart objects
  - “IoT Access Technologies,”
    - Provides an in-depth look at some of the technologies that are considered when connecting smart objects.

Communication Technologies Criteria

- Currently, the number of technologies (available or under development) connecting smart objects is quite extensive,
  - but you should expect consolidation, with certain protocols eventually winning out over others in the various IoT market segments.

- Before reviewing some of these access technologies, it is important to talk about the criteria to use in evaluating them for various use cases and system solutions.

Communication Technologies Criteria

1- Range

2- Frequency Bands

3- Power Consumption

4- Topology

5- Constrained Devices

6- Constrained-Node Networks

Communication Technologies Criteria: 1-Range

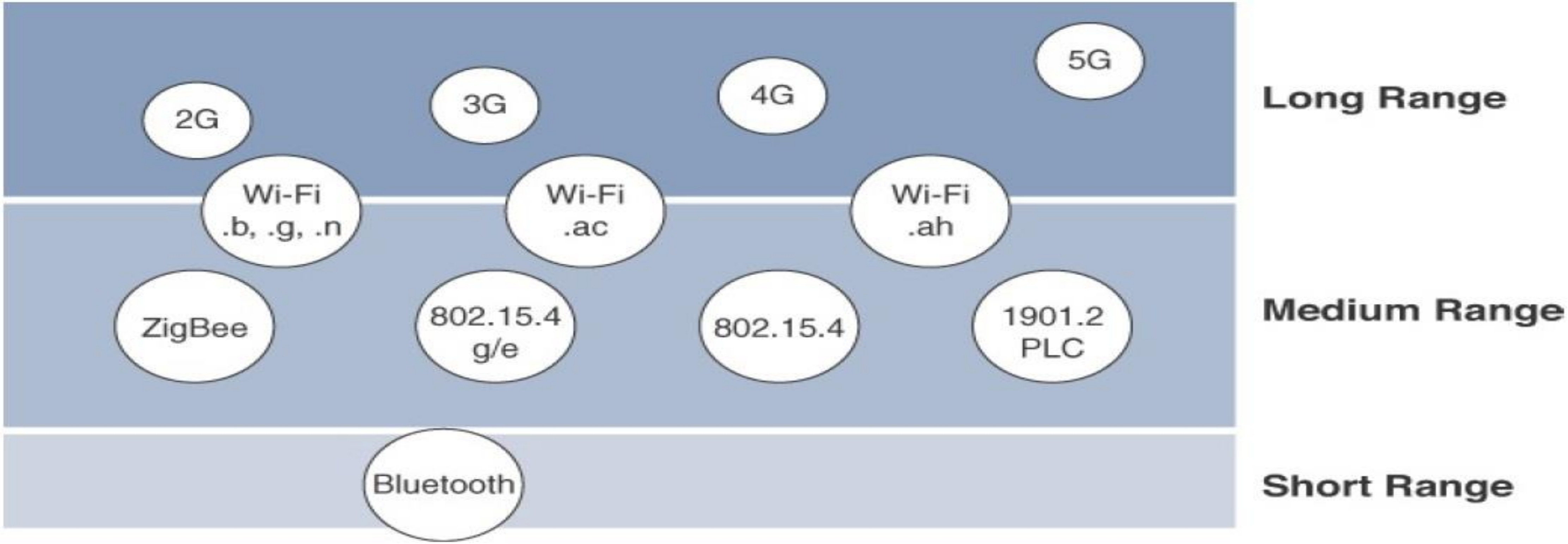
- **Short range:** **PAN - Body**
  - **Tens of meters** of maximum distance between **two device**
  - Example:
    - The classical wired example is a serial cable!
    - Wireless Examples:
      - IEEE 802.15.1 Zig B,
      - Bluetooth and
      - IEEE 802.15.7
      - Visible Light Communications (VLC).
- **Medium range**:
  - Tens to hundreds of meters
  - Examples:
    - IEEE 802.11
    - Wi-Fi,
    - IEEE 802.15.4, and
    - 802.15.4g WPAN.
    - Wired technologies such as IEEE 802.3 Ethernet and IEEE 1901.2 Narrowband PLC

Communication Technologies Criteria: 1- Range

- **Long range:**
  - Greater than 1 mile (1.6 km) between two devices require long-range technologies.
  - Examples:
    - cellular (2G, 3G, 4G) and
    - some applications of outdoor IEEE 802.11 Wi-Fi and
    - Low-Power Wide-Area (LPWA) technologies.

Communication Technologies Criteria: 1- Range

- **How far does the signal need to be propagated?**
  - the area of coverage for a selected wireless technology



Communication Technologies Criteria: 2-Frequency Bands

- **Licensed:**
  - Generally applicable to IoT long-range access technologies and allocated to communications infrastructures deployed by services providers, public services (for example, first responders, military), broadcasters, and utilities.
  - Examples: cellular, WiMAX, and Narrowband IoT (NB-IoT) technologies.
- **Unlicensed:**
  - For the industrial, scientific, and medical (ISM) portions of the radio bands, and they are used in many communications technologies for short-range devices (SRDs).
  - Examples: 2.4 GHz band as used by IEEE 802.11b/g/n Wi-Fi, IEEE 802.15.1 Bluetooth, and IEEE 802.15.4 WPAN.

Communication Technologies Criteria: 2-Frequency Bands

- **Licensed Frequency Bands**
  - Users must subscribe to services when connecting their IoT devices.
    - **This adds more complexity** to a deployment involving large numbers of sensors and other IoT devices,
  - The network operator can guarantee the exclusivity of the frequency usage over the target area and can therefore sell a better **guarantee of service**

Communication Technologies Criteria: 2-Frequency Bands

- **Unlicensed Frequency Bands**
  - An unlicensed band is not unregulated.
    - National and regional regulations exist for each of the allocated frequency bands (much as with the licensed bands).
    - These regulations mandate device compliance on parameters such as
      - transmit power,
      - duty cycle,
      - channel bandwidth, and
      - channel hopping.
  - It does not require a service provider.
    - However, it can suffer from more interference

Communication Technologies Criteria: 2-Frequency Bands

- **Unlicensed Frequency Bands**
  - The frequency of transmission directly impacts how a signal propagates and its practical maximum range.
    - Range and its importance to IoT access are discussed earlier
  - Either for indoor or outdoor deployments, the sub-GHz frequency bands
    - allow greater distances between devices
    - have a better ability than the 2.4 GHz ISM band to penetrate building infrastructures or go around obstacles, while keeping the transmit power within regulation.

Communication Technologies Criteria: 2-Frequency Bands

- **Unlicensed Frequency Bands**
  - The disadvantage of sub-GHz frequency bands is their lower rate of data delivery compared to higher frequencies.
  - However, most IoT sensors do not need to send data at high rates.
  - Therefore, the lower transmission speeds of sub-GHz technologies are usually not a concern for IoT sensor deployments

Communication Technologies Criteria: 2-Frequency Bands

- **Unlicensed Frequency Bands**
  - In most European countries, the 169 MHz band is often considered best suited for wireless water and gas metering applications.
    - This is due to its good deep building basement signal penetration.
  - In addition, the low data rate of this frequency matches the low volume of data that needs to be transmitted.
  - Several sub-GHz ranges have been defined in the ISM band.
    - The most well known ranges are centered on **169 MHz, 433 MHz, 868 MHz, and 915 MHz**.
    - However, most IoT access technologies tend to focus on the two sub-GHz frequency regions around 868 MHz and 915 MHz.

Communication Technologies Criteria: **3- Power Consumption**

- **Powered nodes**
  - have a direct connection to a power source

- **Battery-powered nodes:**
  - are often classified by the required lifetimes of their batteries.
  - For devices under regular maintenance, a battery life of 2 to 3 years is an option.

- Evolution of a new wireless environment known as Low-Power Wide-Area (LPWA) for battery-powered nodes

Communication Technologies Criteria: 4- Topology

- Topology (star, mesh, and peer-to-peer)
  - For long range and short-range technologies, a star topology is prevalent, as seen with cellular, LPWA, and Bluetooth networks.
  - Star topologies utilize a single central base station or controller to allow communications with endpoints.
  - For medium-range technologies, a star, peer-to-peer, or mesh topology is common, as shown in Figure 4-2. Peer-to-peer topologies allow any device to communicate with any other device as long as they are in range of each other.

Communication Technologies Criteria: 5- Constrained Devices

- Classes of Constrained Nodes, as Defined by RFC 7228
  - Constrained nodes have limited resources that impact their networking feature set and capabilities.
  - Classes of Constrained Nodes, as Defined by RFC 7228:
    - **Class 0:** are typically battery-powered nodes such as push button nodes that sends 1 byte of information when changing its status
      - Memory << 10 KB
      - Processing capability and storage << 100 KB
    - **Class 1:** are capable enough to use a protocol stack specifically designed for constrained nodes
      - Memory ~ 10 KB
      - Processing capability and storage ~ 100 KB
    - **Class 2:**
      - Memory > 50 KB
      - Processing capability and storage > 250 KB

Communication Technologies Criteria: 5- Constrained Devices

990119

Class	Definition
Class 0	This class of nodes is severely constrained, with less than 10 KB of memory and less than 100 KB of Flash processing and storage capability. These nodes are typically battery powered. They do not have the resources required to directly implement an IP stack and associated security mechanisms. An example of a Class 0 node is a push button that sends 1 byte of information when changing its status. This class is particularly well suited to leveraging new unlicensed LPWA wireless technology.
Class 1	While greater than Class 0, the processing and code space characteristics (approximately 10 KB RAM and approximately 100 KB Flash) of Class 1 are still lower than expected for a complete IP stack implementation. They cannot easily communicate with nodes employing a full IP stack. However, these nodes can implement an optimized stack specifically designed for constrained nodes, such as Constrained Application Protocol (CoAP). This allows Class 1 nodes to engage in meaningful conversations with the network without the help of a gateway, and provides support for the necessary security functions. Environmental sensors are an example of Class 1 nodes.
Class 2	Class 2 nodes are characterized by running full implementations of an IP stack on embedded devices. They contain more than 50 KB of memory and 250 KB of Flash, so they can be fully integrated in IP networks. A smart power meter is an example of a Class 2 node.

Communication Technologies Criteria: **6- Constrained-Node Networks**

- Several of the IoT access technologies, such as Wi-Fi and cellular, are applicable to laptops, smart phones, and some IoT devices,

- Some IoT access technologies are more suited to specifically connect constrained nodes.
  - Typical examples are IEEE 802.15.4 and 802.15.4g RF, IEEE 1901.2a PLC,
  - LPWA, and IEEE 802.11ah access technologies.
    - These technologies are discussed in more detail later in this chapter.

Communication Technologies Criteria: **6- Constrained-Node Networks**

- Constrained-Node Networks are often referred to as low-power and **lossy** networks (LLNs).

- Low-power refers to the fact that nodes must cope with the requirements from powered and battery-powered constrained nodes.

- Lossy networks indicates that network performance may suffer from interference and variability due to harsh radio environments.

Communication Technologies Criteria: **6- Constrained-Node Networks**

- Layer 1 and Layer 2protocols that can be used for constrained-node networks must be evaluated in the context of the following characteristics for use-case applicability:
  - **Data rate and throughput,**
  - **Latency,**
  - **Overhead and payload**

Communication Technologies Criteria: **6- Constrained-Node Networks**

- **Data rate and throughput** تابعی از لایه های دیتالینک و لایه فیزیکی است

- داده ها حساب میشه (هدر ها و چک خطا توش به حساب نمیاد)

  - The data rates available from IoT access technologies range from 100 bps with protocols such as Sigfox to tens of megabits per second with technologies such as LTE and IEEE 802.11ac.

  - However, the actual throughput is less sometimes much less than the data rate.

  - Technologies not particularly designed for IoT, such as cellular and Wi-Fi, match up well to IoT applications with high rate requirements.
    - For example, nodes involved with video analytics have a need for high data rates.
    - These nodes are found in retail, airport, and smart cities environments for detecting events and driving actions.
    - Because these types of IoT endpoints are not constrained in terms of computing or network bandwidth, the design guidelines tend to focus on application requirements, such as latency

Communication Technologies Criteria: **6- Constrained-Node Networks**

- **Data rate and throughput,**
  - While it may not be important for constrained nodes that send only one message a day, real throughput is often very important for constrained devices implementing an IP stack.
    - In this case, throughput is a lower percentage of the data rate, even if the node gets the full constrained network at a given time.
  - ۴ تا فرکانس داریم
  - For example, let’s consider an IEEE 802.15.4g subnetwork implementing 2FSK modulation at 150 kbps for the 915 MHz frequency band. (The IEEE 802.15.4g protocol is covered in more detail later)
  - **To cover the border case of distance and radio signal quality, Forward Error Correction (FEC) will be turned on, which lowers the data rate from 150 kbps to 75 kbps.**
  - **If you now add in the protocol stack overhead, the two-way communication handling, and the variable data payload size, you end up with a maximum throughput of 30 to 40 kbps.**
  - یا مثلاً امنیت بخوایم
  - This must be considered as the best value because the number of devices simultaneously communicating along with the topology and control plane overhead will also impact the throughput.

Communication Technologies Criteria: **6- Constrained-Node Networks**

- **Latency**
  - Much like throughput requirements, latency expectations of IoT applications should be known when selecting an access technology.
  - This is particularly true for wireless networks, where packet loss and retransmissions due to interference, collisions, and noise are normal behaviors.
  - On constrained networks, latency may range from a few milliseconds to seconds.
  - Applications and protocol stacks must cope with these wide ranging values.
    - For example, UDP at the transport layer is strongly recommended for IP endpoints communicating over LLNs.

Communication Technologies Criteria: **6- Constrained-Node Networks**

Overhead and payload

- When considering constrained access network technologies, it is important to review the MAC payload size characteristics required by applications.

- In addition, you should be aware of any requirements for IP. The minimum IPv6 MTU size is expected to be 1280 bytes.
  - Therefore, the fragmentation of the IPv6 payload has to be taken into account by link layer access protocols with smaller MTUs.

- The use of IP on IoT devices is an open topic of discussion.
  - For the more constrained classes of devices, like Class 0 and Class 1 devices, it is usually not possible or optimal to implement a complete IP stack implementation.

Communication Technologies Criteria: **6- Constrained-Node Networks**

- **Overhead and payload**
  - For technologies that fall under the LLN definition but are able to transport IP, such as IEEE 802.15.4 and 802.15.4g, IEEE 1901.2, and IEEE 802.11ah, Layer 1 or Layer 2 fragmentation capabilities and/or IP optimization is important.

  - For example,
    - The payload size for IEEE 802.15.4 is 127 bytes and requires an IPv6 payload with a minimum MTU of 1280 bytes to be fragmented.
    - On the other hand, IEEE 802.15.4g enables payloads up to 2048 bytes, easing the support of the IPv6 minimum MTU of 1280 bytes.

Communication Technologies Criteria: **6- Constrained-Node Networks**

- **Overhead and payload**
  - Most LPWA technologies offer small payload sizes.
    - **These small payload sizes are defined to cope with**
      - **Low data rate and**
      - **Low time over the air or duty cycle requirements of IoT nodes and sensors.**
  - For example, payloads may be as little as 19 bytes using LoRaWAN technology or up to 250 bytes, depending on the adaptive data rate (ADR).
  - While this doesn't preclude the use of an IPv6/6LoWPAN payload, as seen on some endpoint implementations, these types of protocols are better suited to Class 0 and 1 nodes, as defined in RFC 7228.

Contents

- Introduction
- Physical and Link Layers Protocols (IoT Access Technologies)
    - Physical Layer Issues
    - Communication Technologies Criteria
    - Communication Technologies and Protocols
- Network Layer Protocols (IP as the IoT Network Layer)
- Transport Layer Protocols
- Application Layer Protocols

Communication Technologies Criteria-Summary

- These criteria include: range, frequency bands, power consumption, network topology, the presence of constrained devices and/or networks, and data throughput.

- From a network engineer perspective, you must make sure an architecture is developed with the proper abstraction for a particular access technology.
  - This is especially true for constrained network nodes, where quite often your choices of protocols and solutions can be limited.

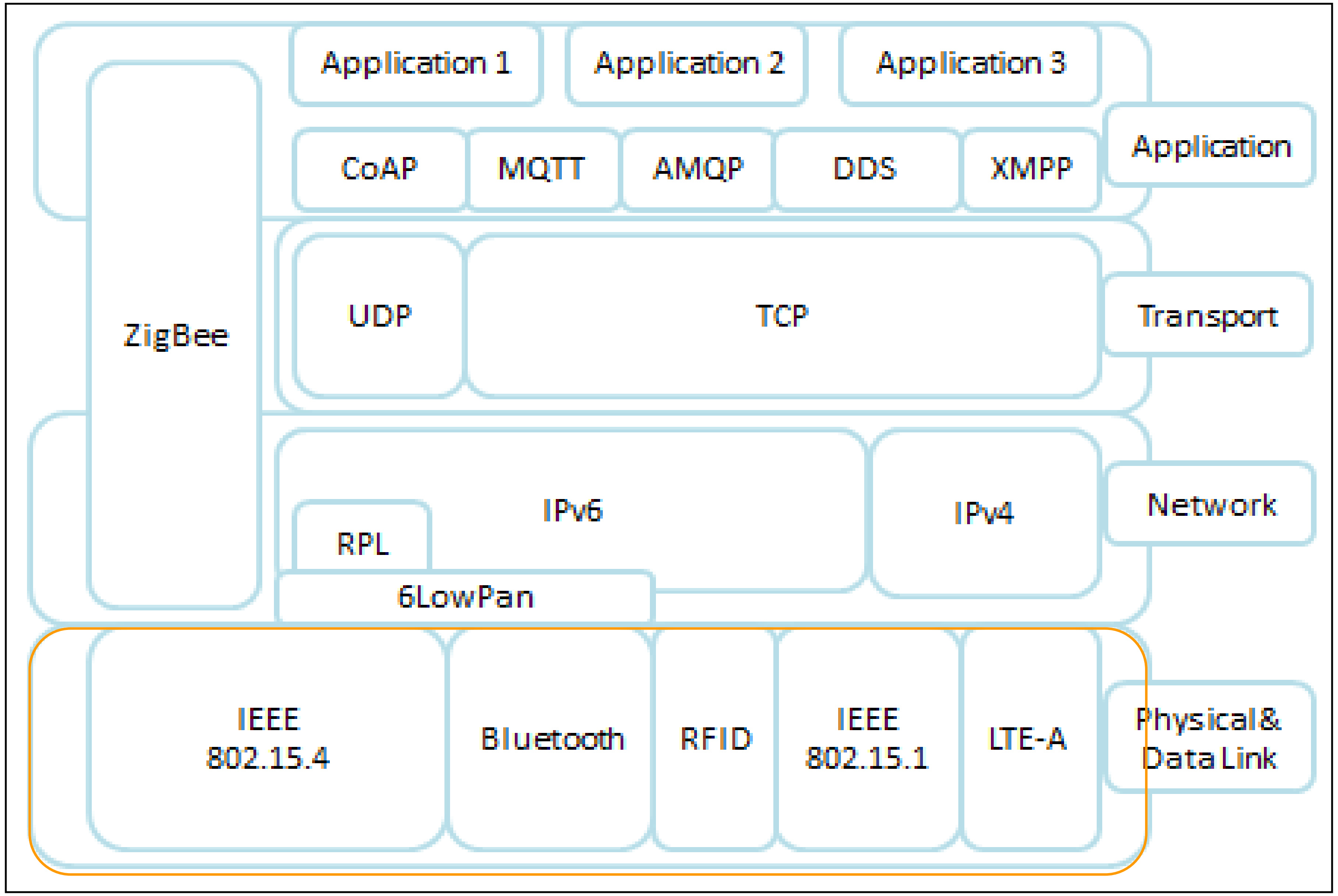
- The next section reviews the main IoT access technologies dedicated to constrained networks.

IoT Protocol Stack- Physical and Link Layers Protocols

990126 لایه دسترسی

- **IEEE 802.15.4**
- **IEEE 802.11**
- **ZigBee**
- **Bluetooth Low Energy (BLE)**
- **low-power Wi-Fi**
- **LoRaWAN**
- **SigFox**
- **NB-IoT**
- **power line communications (PLC)**

IoT Protocol Stack- Physical and Link Layers Protocols



IoT Protocol Stack- Physical and Link Layers Protocols

Session		**MQTT**, **SMQTT**, **CoRE**, **DDS**, **AMQP** , **XMPP**, **CoAP**, …
Network	Encapsulation	**6LowPAN**, **6TiSCH**, **6Lo**, Thread, …
	Routing	**RPL**, **CORPL**, **CARP**, …
Datalink		WiFi, **Bluetooth Low Energy**, **Z-Wave**, **ZigBee Smart**, **DECT/ULE**, 3G/LTE, NFC, **Weightless**, **HomePlug GP**, **802.11ah**, **802.15.4e**, **G.9959**, **WirelessHART**, **DASH7**, ANT+, **LTE-A**, **LoRaWAN**, …

Security
TCG, Oath 2.0, SMACK, SASL, ISASecure, ace, DTLS, Dice, …

Management
IEEE 1905, **IEEE 1451**, …

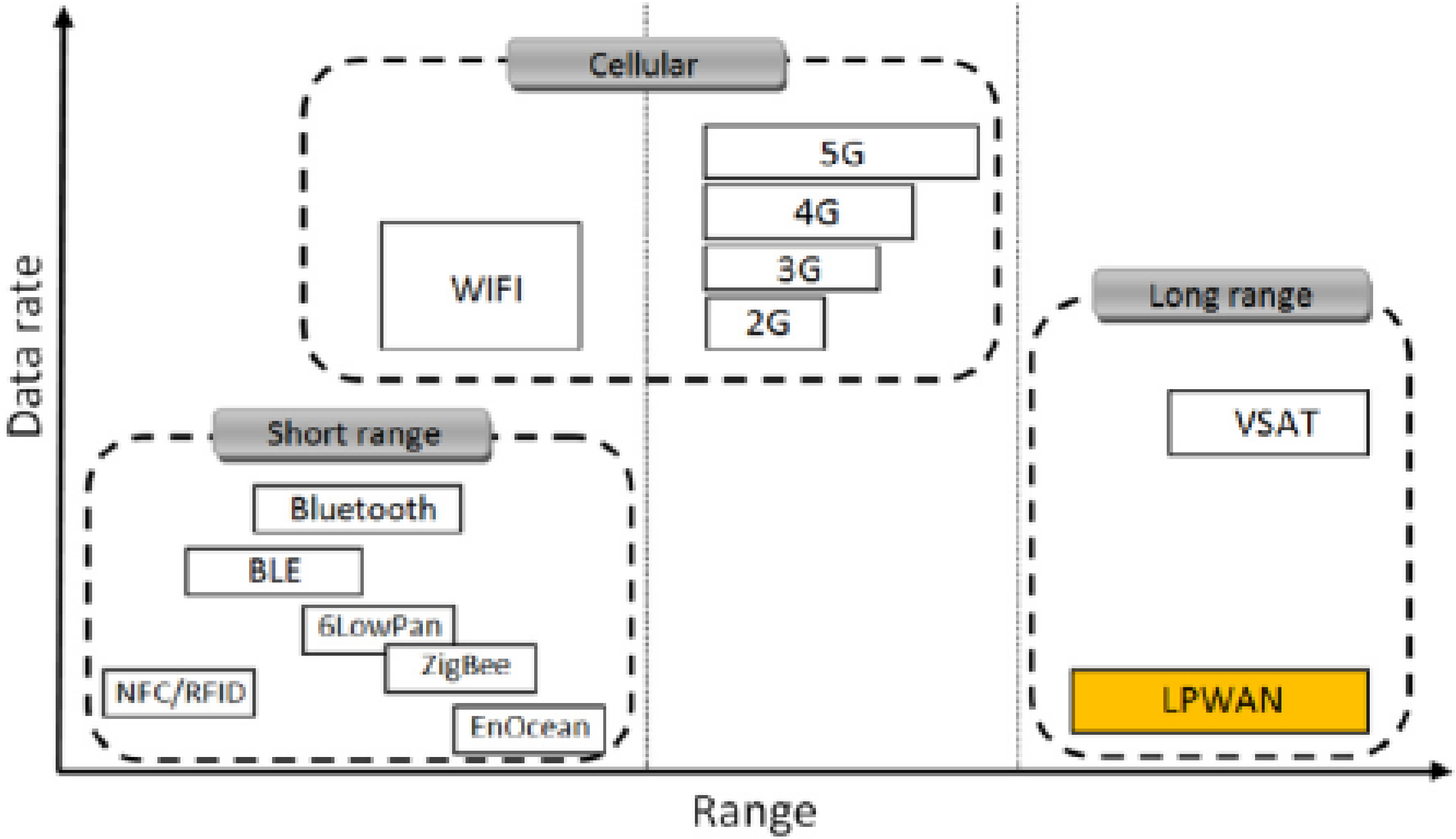
IoT Protocol Stack- Physical and Link Layers Protocols

- Short-range and low-power wireless networks:
  - Low Power BAN, PAN, Low power LAN
    - 802.15.4
    - Bluetooth Low Energy
    - 802.11h
    - NFC
    - …

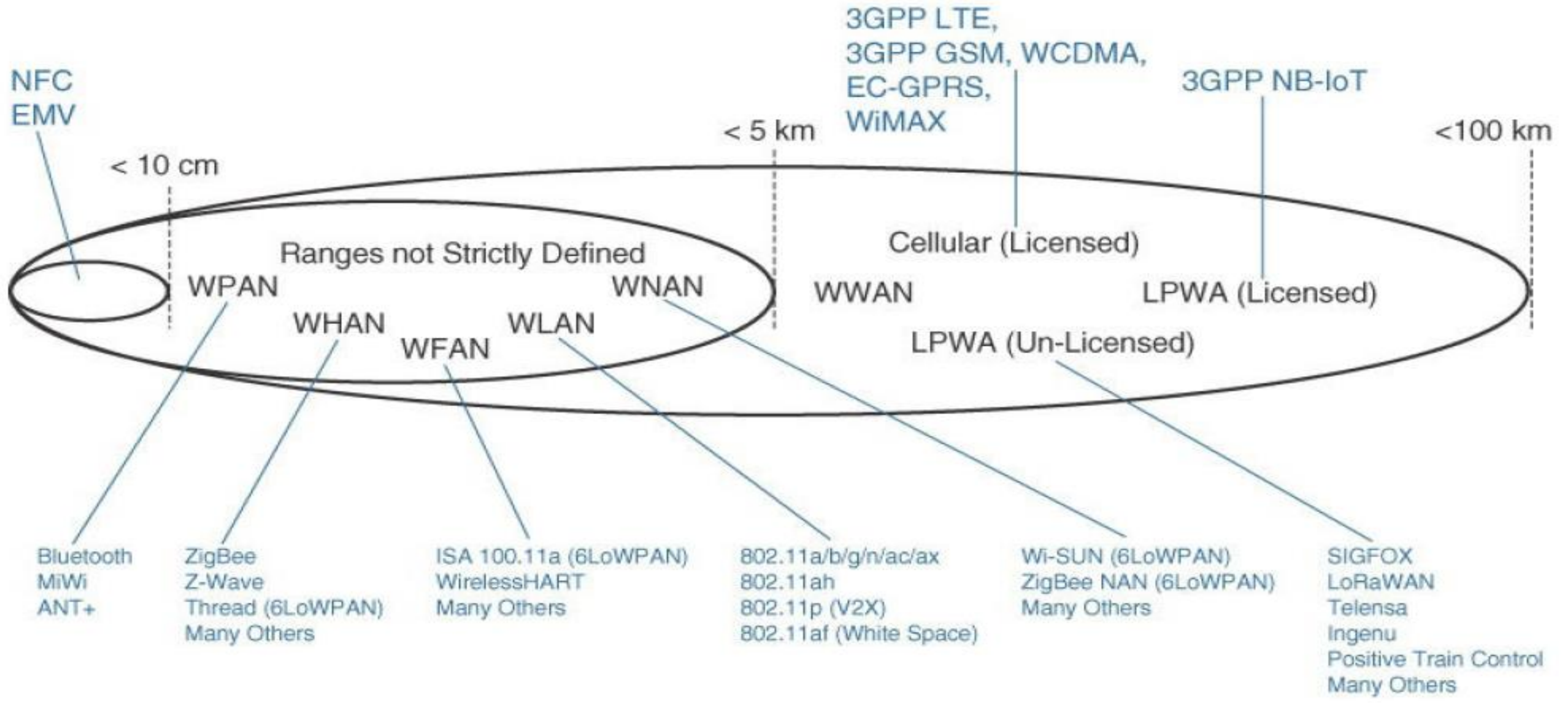
- Long-range and low-power wireless networks:
  - Low Power WAN (LPWAN)
    - LoRaWAN
    - NB-IoT
    - SigFox

IoT Protocol Stack- Physical and Link Layers Protocols

Required Data Rate vs. Range



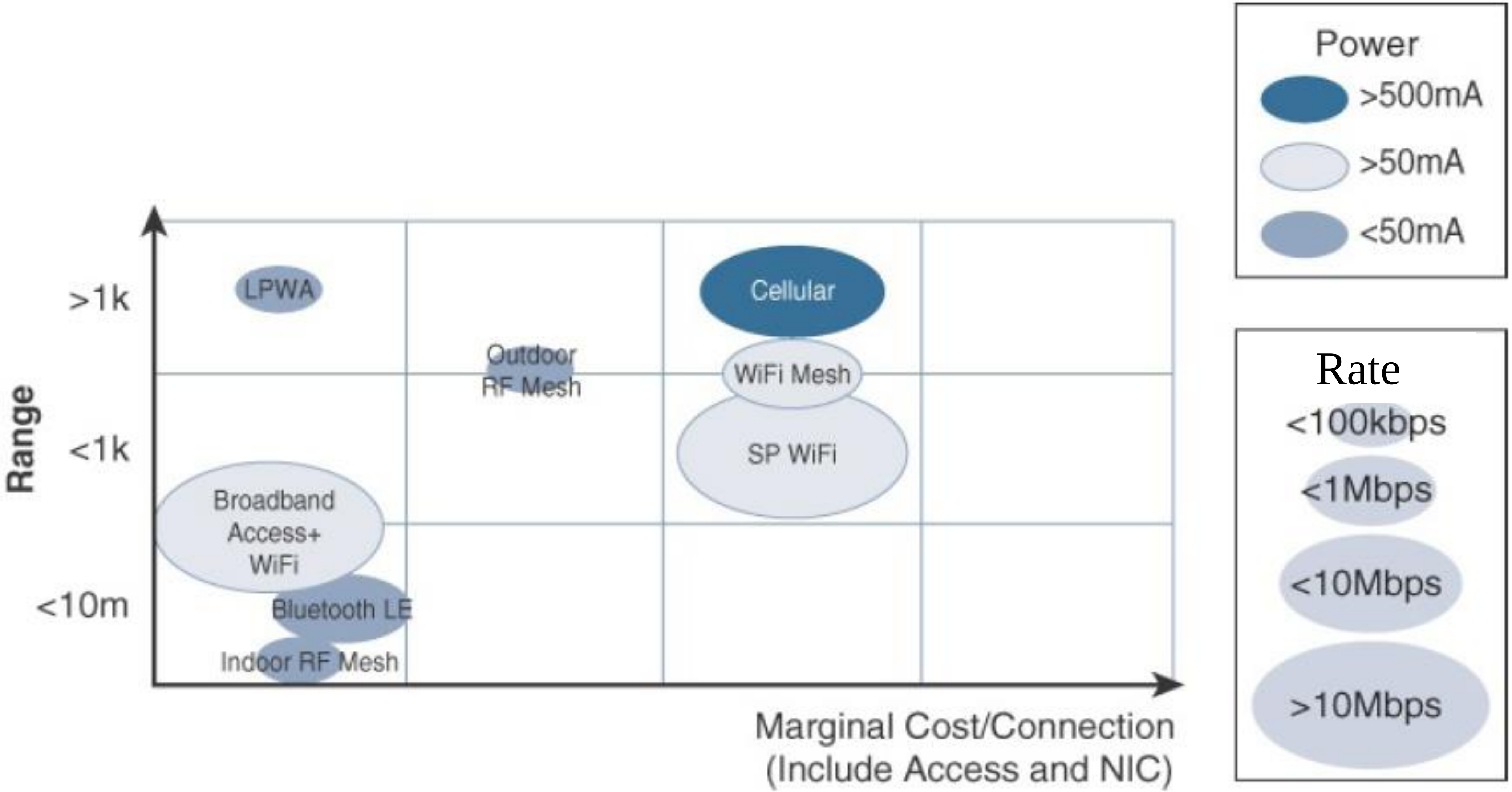
Access Technologies and Distances



WPAN: Wireless Personal Area Network
WHAN: Wireless Home Area Network
WFAN: Wireless Field (or Factory) Area Network
WLAN: Wireless Local Area Network

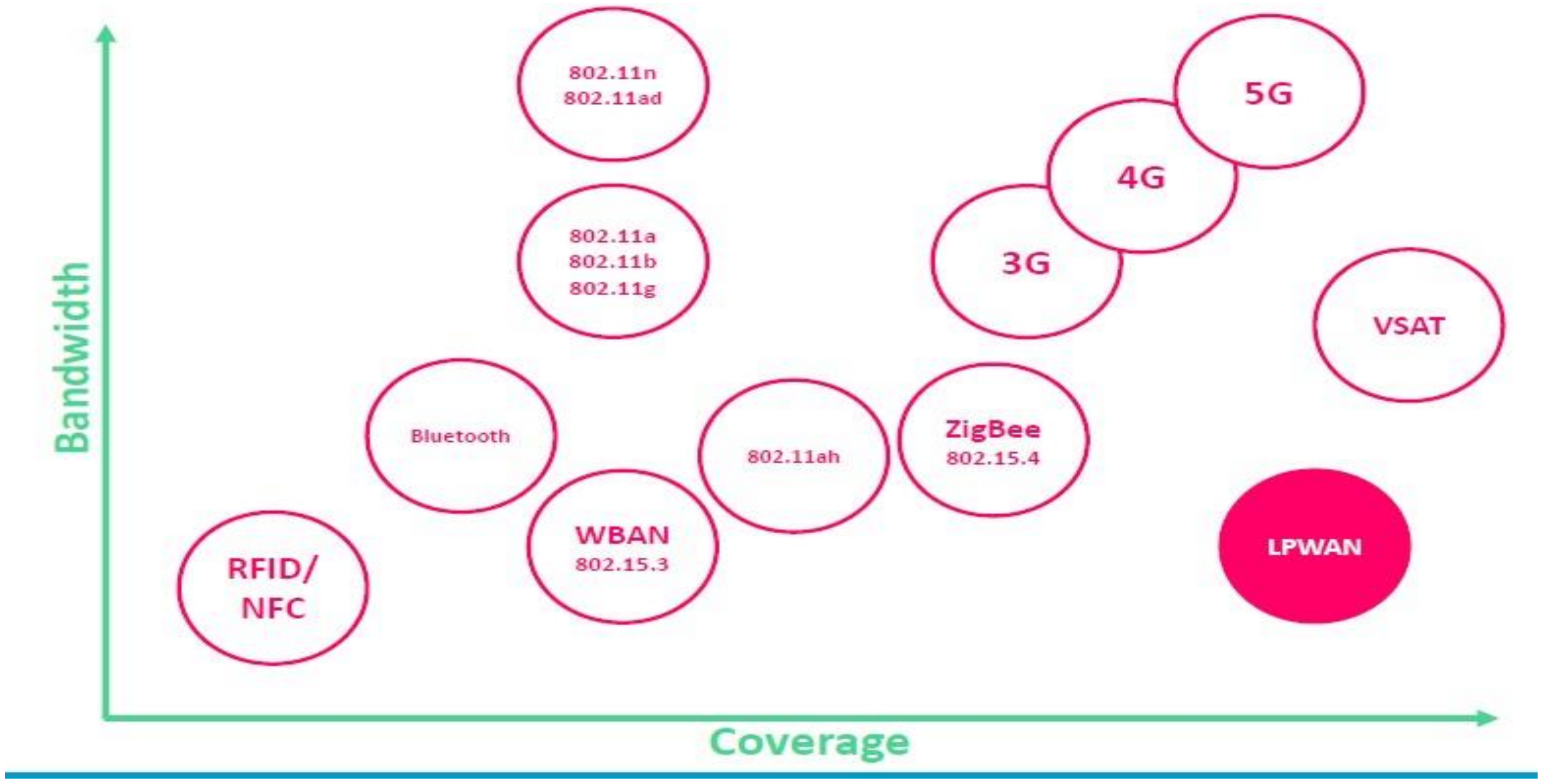
WNAN: Wireless Neighborhood Area Network
WWAN: Wireless Wide Area Network
LPWA: Low Power Wide Area

Comparison Between Common Access Technologies in Terms of Range Versus Power, Rate and Cost



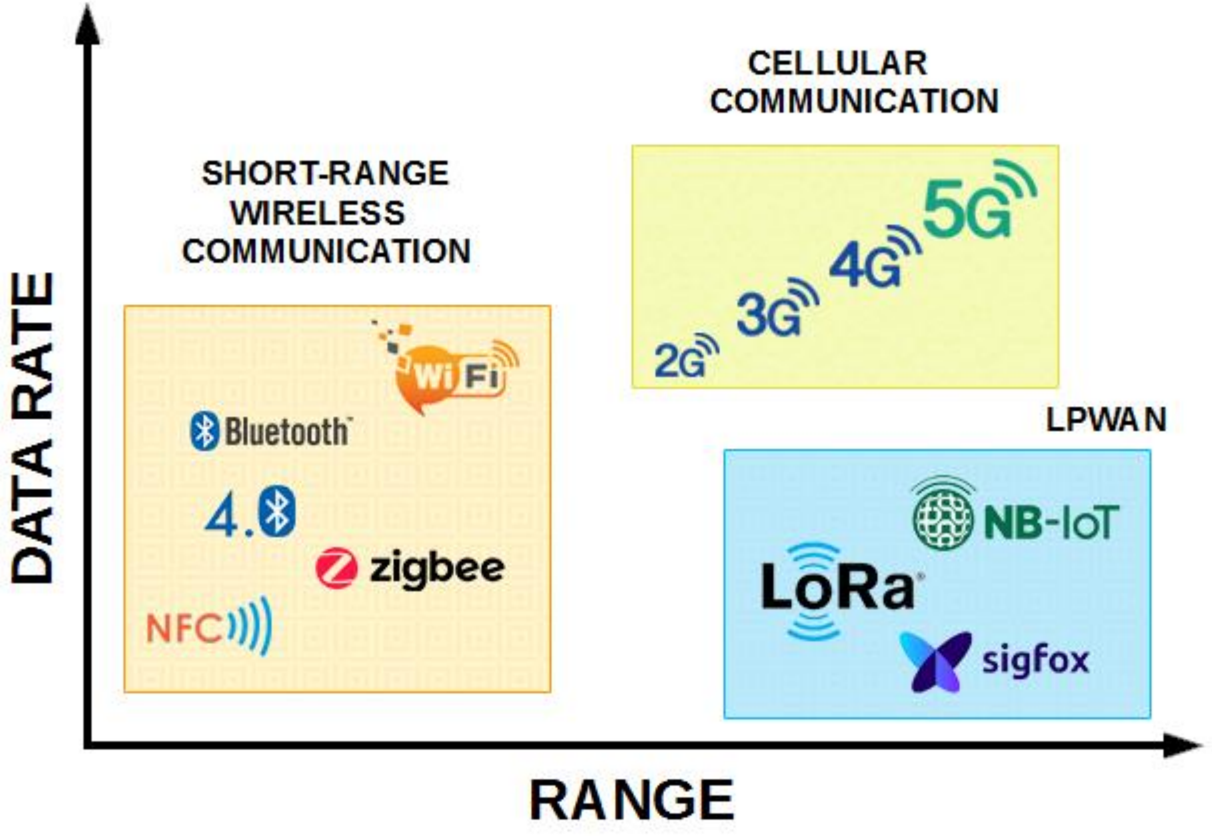
Communication Technologies Comparison

- Range vs Bandwidth



Communication Technologies Comparison

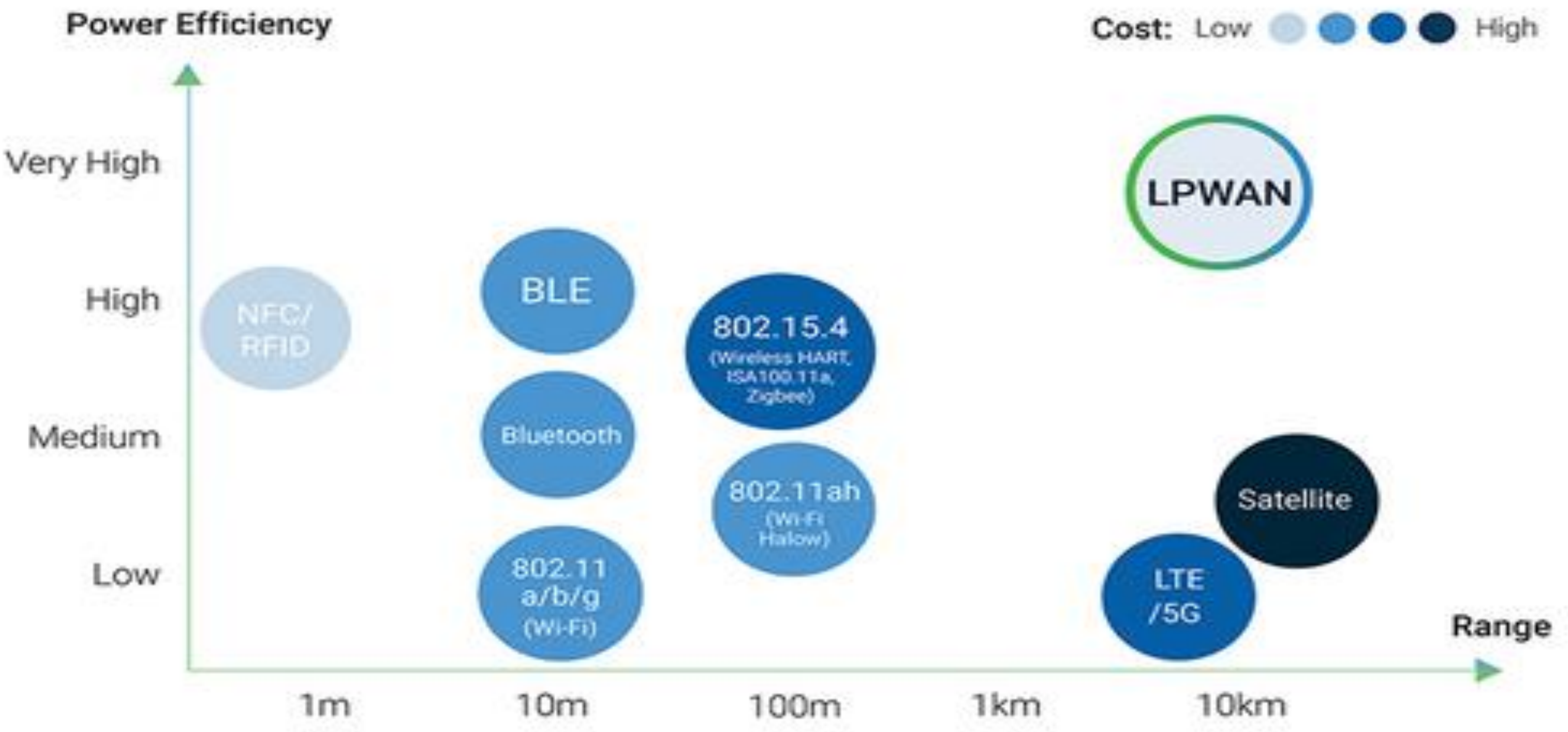
- Range vs Data Rate



*

Communication Technologies Comparison

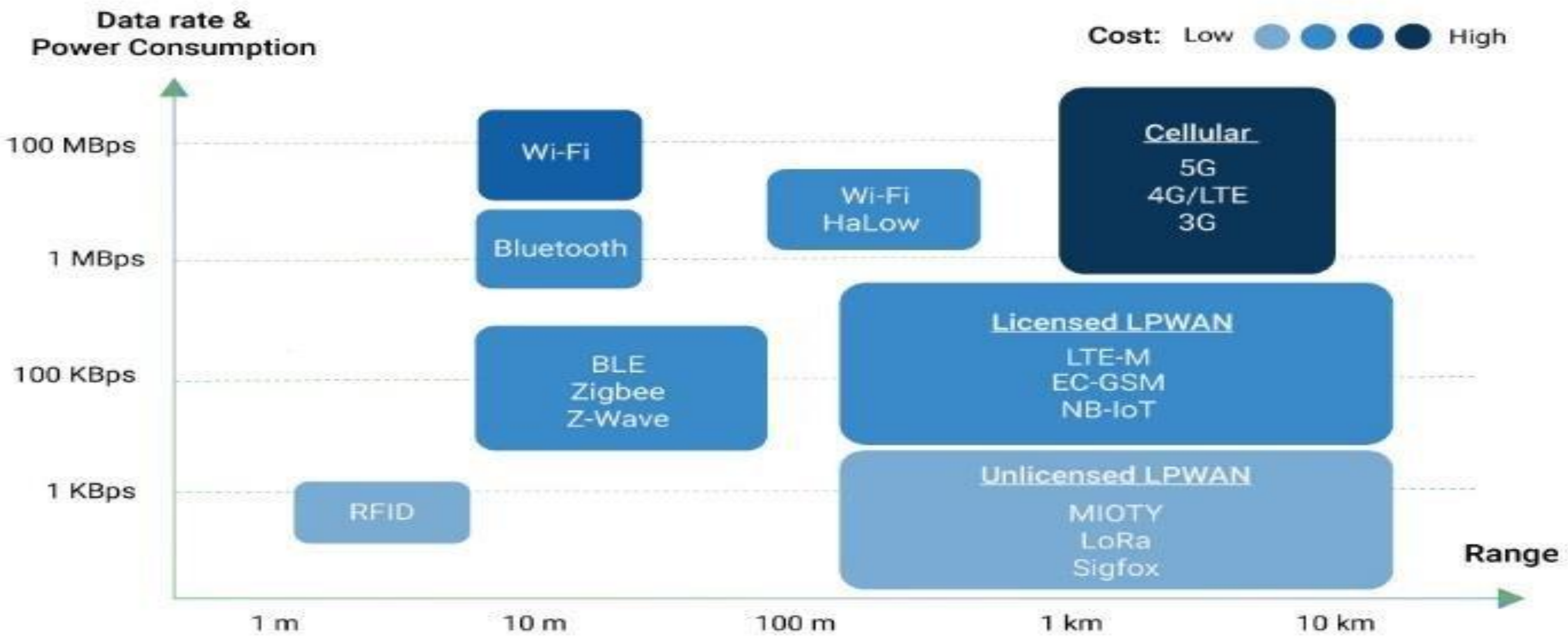
- Range vs Power Efficiency



*

Communication Technologies Comparison

- Data Rate vs Range and Power consumption



IoT Protocol Stack- Physical and Link Layers

Protocols

- For each of the IoT access technologies, a common information set is being provided:
  - **Standardization and alliances:** The standards bodies that maintain the
  - protocols for a technology
  - **Physical layer:** The wired or wireless methods and relevant
  - frequencies
  - **MAC layer:** Considerations at the Media Access Control (MAC) layer,
  - which bridges the physical layer with data link control
  - **Topology:** The topologies supported by the technology
  - **Security:** Security aspects of the technology
  - **Competitive technologies:** Other technologies that are similar and may be suitable alternatives to the given technology

Physical and Link Layers Protocols- IEEE 802.15.4

- IEEE 802.15.4 is a wireless access technology for low-cost and low-data-rate devices powered or run on batteries.
- IEEE 802.15.4 (or IEEE 802.15 Task Group 4)
  - Defines low-data-rate PHY and MAC layer specifications for wireless personal area networks (WPAN).
  - For low complexity wireless devices with low data rates that need many months or even years of battery life.
- Used in following types of deployments:
  - Home and building automation
  - Automotive networks
  - Industrial wireless sensor networks
  - Interactive toys and remote controls

Physical and Link Layers Protocols- IEEE 802.15.4

- Since 2003, the IEEE has published several iterations of the IEEE 802.15.4 specification, each labeled with the publication's year:
  - IEEE 802.15.4-2003
  - 802.15.4-2006,
  - 802.15.4-2011 and 802.15.4-2015.

- Newer releases typically supersede older ones, integrate addendums, and add features or clarifications to previous versions

Physical and Link Layers Protocols- IEEE 802.15.4

- IEEE 802.15.4 PHY and MAC layers are the foundations for several networking protocol stacks.

- فقط دو لایه پایین رو داره

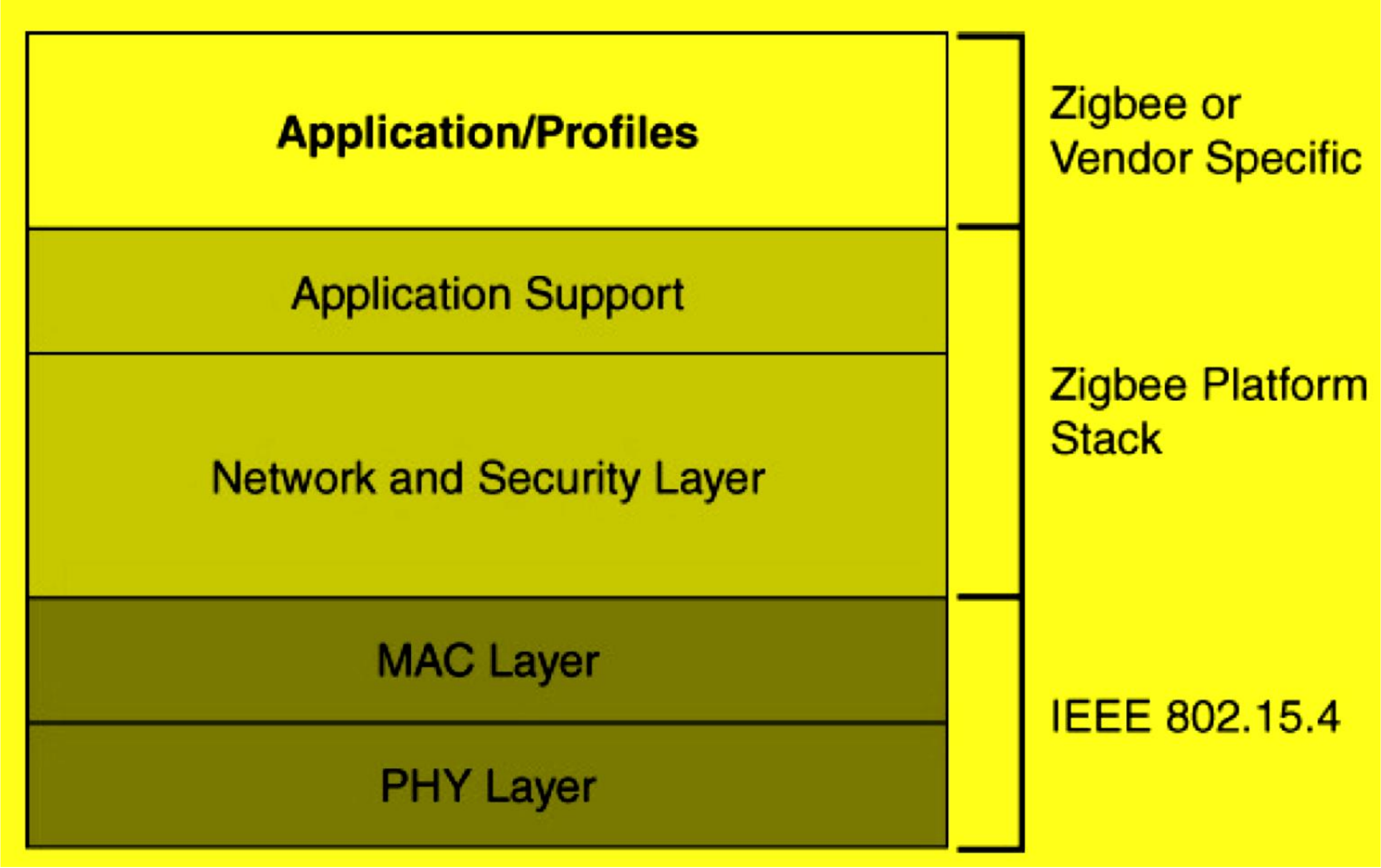
- **These protocol stacks make use of 802.15.4 at the physical and link layer levels, but the upper layers are different:**
  - ZigBee — این ی پرتکل استکی هست ک حالا توی دو تا لایه پایین خودش از ۸۰۲.۱۵.۴ استفاده می کنه
  - ZigBee IP
  - 6LoWPAN
  - ISA100.11a
  - WirelessHART
  - Thread

Protocol Stacks Using 802.15.4: ZigBee

- ZigBee utilizes the IEEE 802.15.4 standard at the lower PHY and MAC layers.
  - ZigBee specifies the network and security layer and application support layer that sit on top of the lower layers.
- The first ZigBee specification was ratified in 2004,
  - shortly after the release of the IEEE 802.15.4 specification the previous year.
- While not released as a typical standard, like an RFC, ZigBee still had industry support from more than 100 companies upon its initial publication.
  - This industry support has grown to more than 400 companies that are members of the ZigBee Alliance.

Protocol Stacks Using 802.15.4: ZigBee

- High-Level ZigBee Protocol Stack



Protocol Stacks Using 802.15.4: ZigBee

- On top of the 802.15.4 PHY and MAC layers, ZigBee specifies its own network and security layer and application profiles.

- While this structure has provided a fair degree of interoperability for vendors with membership in the ZigBee Alliance, it has not provided interoperability with other IoT solutions.

- However, this has started to change with the release of ZigBee IP, which is discussed next.

Protocol Stacks Using 802.15.4: ZigBee IP

- With the introduction of ZigBee IP, the support of IEEE 802.15.4 continues, but the IP and TCP/UDP protocols and various other open standards are now supported at the network and transport layers.

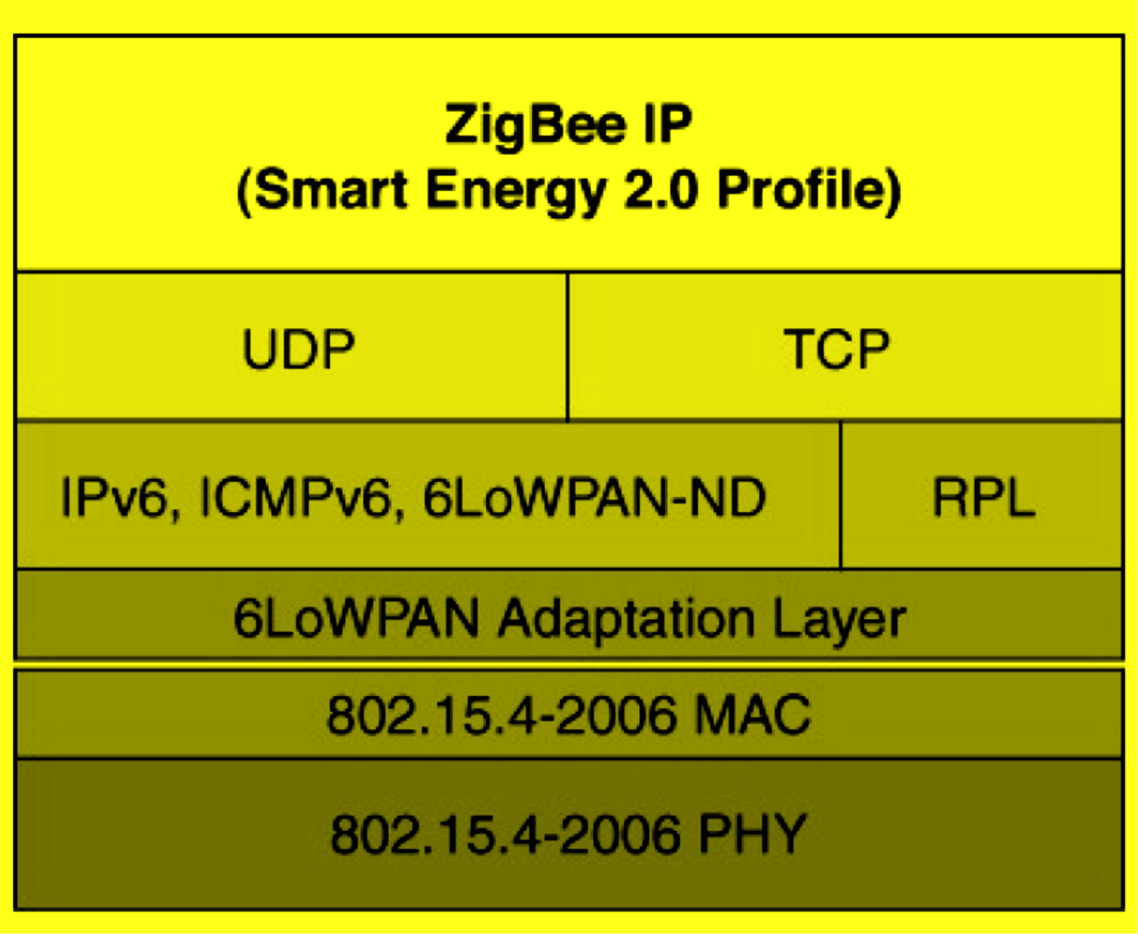
- The ZigBee-specific layers are now found only at the top of the protocol stack for the applications.

Protocol Stacks Using 802.15.4: ZigBee IP

- ZigBee IP was created to embrace the open standards coming from the IETF's work on LLNs, such as IPv6, 6LoWPAN, and RPL.
- They provide for low-bandwidth, low-power, and cost-effective communications when connecting smart objects.
- ZigBee IP is a critical part of the Smart Energy (SE) Profile 2.0 specification from the ZigBee Alliance.
  - SE 2.0 is aimed at smart metering and residential energy management systems.
  - In fact, ZigBee IP was designed specifically for SE 2.0 but it is not limited to this use case. Any other applications that need a standards-based IoT stack can utilize Zigbee IP.

Protocol Stacks Using 802.15.4: ZigBee

- The ZigBee IP stack



Physical and Link Layers Protocols- IEEE 802.15.4

- IEEE 802.15.4- **Physical layer**
  - The 802.15.4 standard supports an extensive number of PHY options that range from 2.4 GHz to sub-GHz frequencies in ISM bands.
  - The original physical layer transmission options were as follows:
    - 2.4 GHz, 16 channels, with a data rate of 250 kbps
    - 915 MHz, 10 channels, with a data rate of 40 kbps
    - 868 MHz, 1 channel, with a data rate of 20 kbps
  - only the 2.4 GHz band operates worldwide.
  - The 915 MHz band operates mainly in North and South America, and the 868 MHz frequencies are used in Europe, the Middle East, and Africa.

Physical and Link Layers Protocols- IEEE 802.15.4

- The original IEEE 802.15.4-2003 standard specified only three PHY options based on direct sequence spread spectrum (DSSS) modulation.

- DSSS is a modulation technique in which a signal is intentionally spread in the frequency domain, resulting in greater bandwidth

Physical and Link Layers Protocols- IEEE 802.15.4

- IEEE 802.15.4-2006, 802.15.4-2011, and IEEE 802.15.4-2015 introduced additional PHY communication options, including the following:
  - **OQPSK PHY**
    - This is DSSS PHY, employing offset quadrature phase shift keying (OQPSK) modulation. OQPSK is a modulation technique that uses four unique bit values that are signaled by phase changes.
    - An offset function that is present during phase shifts allows data to be transmitted more reliably.
  - **BPSK PHY**
    - This is DSSS PHY, employing binary phase-shift keying (BPSK) modulation.
    - BPSK specifies two unique phase shifts as its data encoding scheme.
  - **ASK PHY**
    - This is parallel sequence spread spectrum (PSSS) PHY, employing amplitude shift keying (ASK) and BPSK modulation.
    - PSSS is an advanced encoding scheme that offers increased range, throughput, data rates, and signal integrity compared to DSSS.
    - ASK uses amplitude shifts instead of phase shifts to signal different bit values.

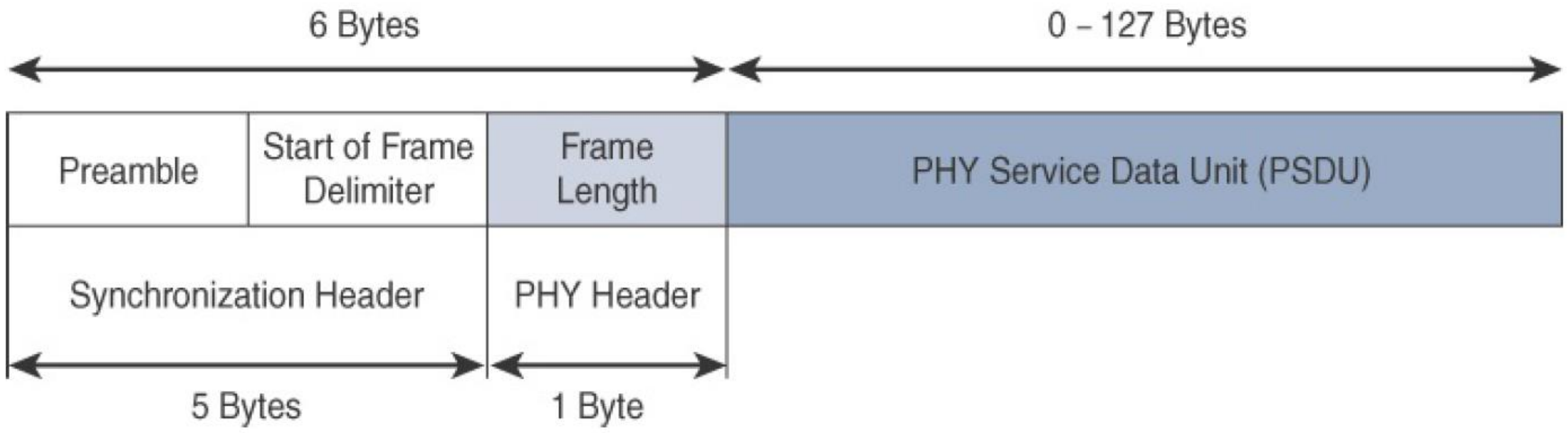
Physical and Link Layers Protocols- IEEE 802.15.4

- These improvements increase the maximum data rate for both 868 MHz and 915 MHz to 100 kbps and 250 kbps, respectively.

- The 868 MHz support was enhanced to 3 channels, while other IEEE 802.15.4 study groups produced addendums for new frequency bands. For example, the IEEE 802.15.4c study group created the bands 314–316 MHz, 430–434 MHz, and 779–787 MHz for use in China.

Physical and Link Layers Protocols- IEEE 802.15.4

- *IEEE 802.15.4 PHY Format:*



- The synchronization header (to synchronize the data transmission) for this frame is composed of
  - the Preamble and the
  - Start of Frame Delimiter fields.

- The Preamble field is a 32-bit 4-byte (for parallel construction) pattern that identifies the start of the frame and is used to synchronize the data transmission.
  - The Start of Frame Delimiter field informs the receiver that frame contents start immediately after this byte

Physical and Link Layers Protocols- IEEE 802.15.4

- Pay attention to which versions of 802.15.4 particular devices support.
  - The various versions and addendums to 802.15.4 over the years through various working groups have been made

- When providing details on the physical layer implementation, products and solutions must refer to:
  - Proper IEEE 802.15.4 specification,
  - Frequency band,
  - Modulation,
  - Data rate.

Physical and Link Layers Protocols- IEEE 802.15.4

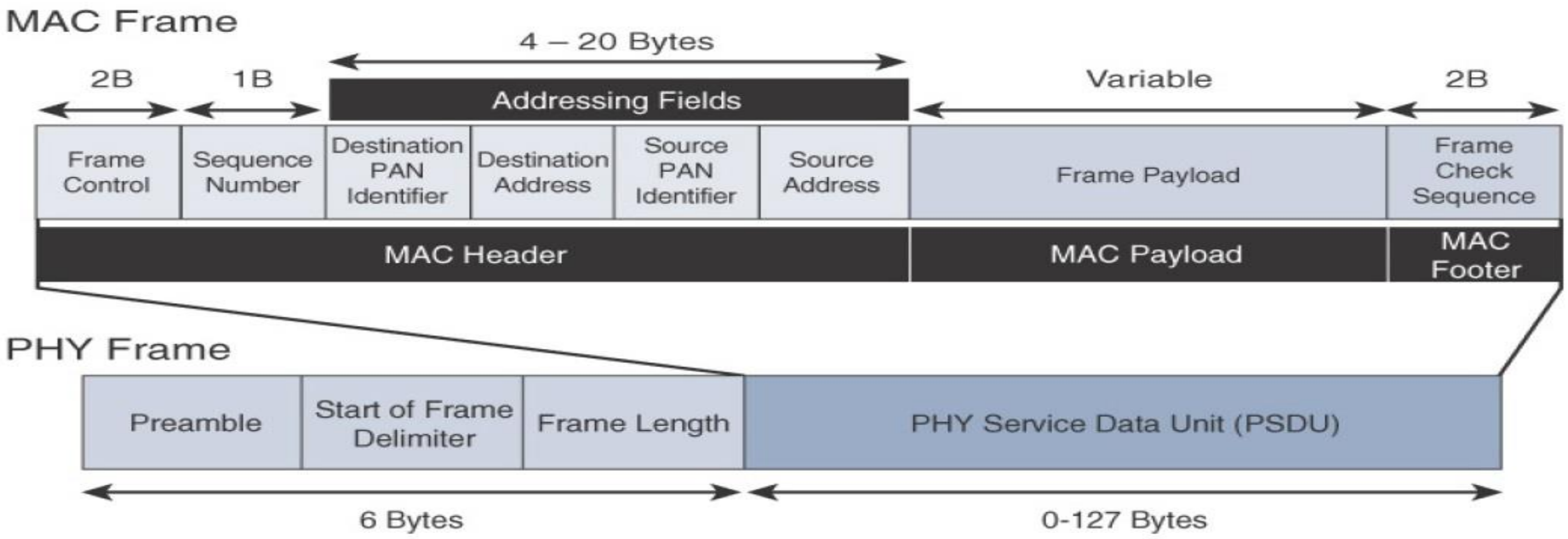
- IEEE 802.15.4- MAC layer
  - manages access to the PHY channel by defining how devices in the same area will share the frequencies
  - the scheduling and routing of data frames are also coordinated.
  - The 802.15.4 MAC layer performs the following tasks:
    - Network beaconing for devices acting as coordinators (New devices use beacons to join an 802.15.4 network)
    - PAN association and disassociation by a device
    - Device security
    - Reliable link communications between two peer MAC entities

Physical and Link Layers Protocols- IEEE 802.15.4

- To do MAC layer's tasks, four types of MAC frames are specified in 802.15.4 :
  - **Data frame:** Handles all transfers of data
  - **Beacon frame:** Used in the transmission of beacons from a PAN
  - coordinator
  - **Acknowledgement frame:** Confirms the successful reception of a
  - frame
  - **MAC command frame:** Responsible for control communication
  - between devices
- Each of these four 802.15.4 MAC frame types follows the frame format shown next.

Physical and Link Layers Protocols- IEEE 802.15.4

- IEEE 802.15.4 MAC layer frame format
  - The 802.15.4 MAC frame can be broken down into the MAC Header, MAC Payload, and MAC Footer fields.



Physical and Link Layers Protocols- IEEE 802.15.4

- The MAC Header field is composed of the
  - Frame Control
    - defines attributes such as frame type, addressing modes, and other control flags
  - Sequence Number
    - indicates the sequence identifier for the frame.
  - Addressing fields:
    - specifies the Source and Destination PAN Identifier fields as well as the Source and Destination Address fields

Physical and Link Layers Protocols- IEEE 802.15.4

- Within the Frame Control portion of the 802.15.4 header is the Security Enabled field.
- When this field is set to a value of 0, the frame format matches the previous Figure 4-6.
- Beginning with the 802.15.4-2006 specification, when this field is set to a value of 1, an Auxiliary Security Header field is added to the 802.15.4 frame, will be shown later.

Physical and Link Layers Protocols- IEEE 802.15.4

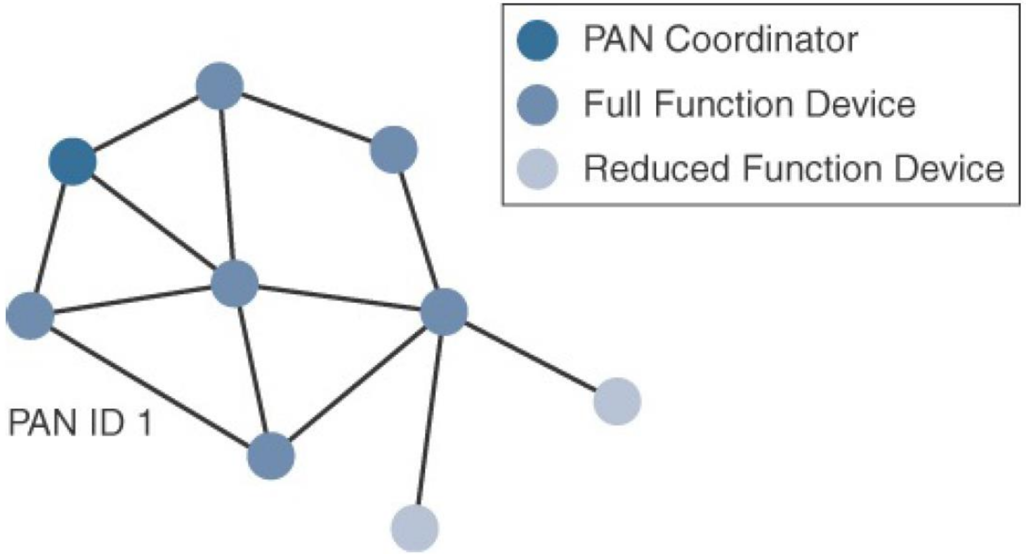
- The MAC Payload field varies by individual frame type. For example,
  - Beacon frames have specific fields and payloads related to beacons,
  - MAC command frames have different fields present.
- The MAC Footer field is nothing more than a frame check sequence (FCS).
  - An FCS is a calculation based on the data in the frame that is used by the receiving side to confirm the integrity of the data in the frame.
- IEEE 802.15.4 requires all devices to support a unique 64-bit extended MAC address, based on EUI-64.
- However, because the maximum payload is 127 bytes, 802.15.4 also defines how a 16-bit "short address" is assigned to devices.
  - This short address is local to the PAN and substantially reduces the frame overhead compared to a 64-bit extended MAC address.
  - However, you should be aware that the use of this short address might be limited to specific upper-layer protocol stacks.

Physical and Link Layers Protocols- IEEE 802.15.4

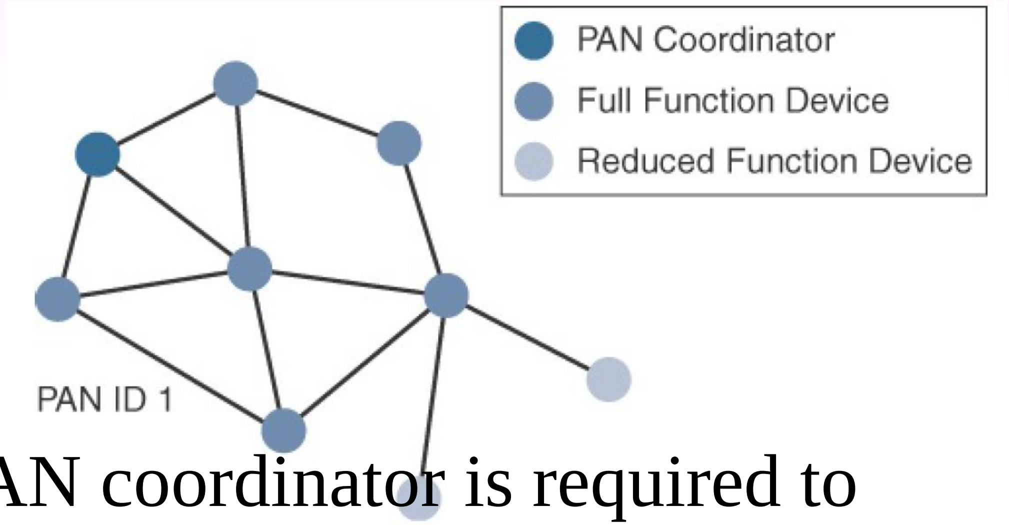
- IEEE 802.15.4
  - Topology
    - Star
    - Peer-to-Peer
    - Mesh

Physical and Link Layers Protocols- IEEE 802.15.4

- Please note that every 802.15.4 PAN should be set up with a unique ID.
  - All the nodes in the same 802.15.4 network should use the same PAN ID.
- This figure shows an example of an 802.15.4 mesh network with a PAN ID of 1.

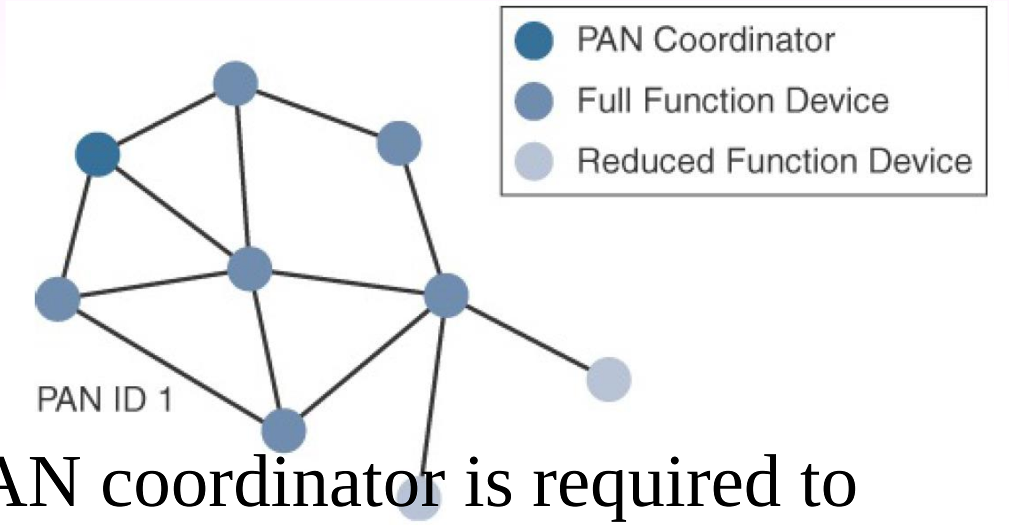


Physical and Link Layers Protocols- IEEE 802.15.4



- Two types of nodes:
  - Full-function devices (FFDs)
  - Reduced-function devices (RFDs)
- A minimum of one FFD acting as a PAN coordinator is required to deliver services that allow other devices to associate and form a cell or PAN.
- FFD devices can communicate with any other devices, whereas RFD devices can communicate only with FFD devices.

Physical and Link Layers Protocols- IEEE 802.15.4



- Two types of nodes:
  - Full-function devices (FFDs)
  - Reduced-function devices (RFDs)
- A minimum of one FFD acting as a PAN coordinator is required to deliver services that allow other devices to associate and form a cell or PAN.
- FFD devices can communicate with any other devices, whereas RFD devices can communicate only with FFD devices.

Physical and Link Layers Protocols- IEEE 802.15.4

- The IEEE 802.15.4 specification does not define a path selection within the MAC layer for a mesh topology.
  - *Mesh-under:* can be done at Layer 2 and is based on a proprietary solution.

  - *Mesh-over: T*he routing function can occur at Layer 3, using a routing protocol, such as the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) which will be discussed in network protocol section

IEEE 802.15.4- Security

- The IEEE 802.15.4 specification uses Advanced Encryption Standard (AES) with a 128-bit key length as the base encryption algorithm for securing its data.

- AES: Established by the US National Institute of Standards and Technology in 2001, and is one of the most popular algorithms used in symmetric key cryptography.
  - A *symmetric key* means that the same key is used for both the encryption and decryption of the data.

- AES is a block cipher,
  - which means it operates on fixed-size blocks of data

IEEE 802.15.4- Security

- Enabling these security features for 802.15.4 changes the frame format slightly and consumes some of the payload.
- The Security Enabled field in the Frame Control portion of the 802.15.4 is a single bit that is set to 1 for security.
  - a field called the Auxiliary Security Header is created after the Source Address field, by stealing some bytes from the Payload field.
- Frame Format with the Auxiliary Security Header Field for 802.15.4-2006 and Later Versions: