Intelligent distributed systems

Daniele Fontanelli

Department of Industrial Engineering
University of Trento
E-mail address: *daniele.fontanelli@unitn.it*

2022/2023

UNIVERSITÀ DI TRENTO | Dipartimento di Ingegneria Industriale

Outline

Outline

Industrial call for Ethernet

The proliferation of the internet has led to the pervasiveness of *Ethernet* in both homes and businesses.
Ethernet has only 1 bit of difference from the standard *IEEE 802.3*, that is the one concerning with CSMA/CD.
Because of its *low cost, widespread availability, and high communication rate*, Ethernet has been proposed as the ideal network for industrial automation.
Emerging real-time Industrial Ethernet solutions complement the fieldbus standards, e.g., by using common layers.

Industrial call for Ethernet

IEEE 802 family

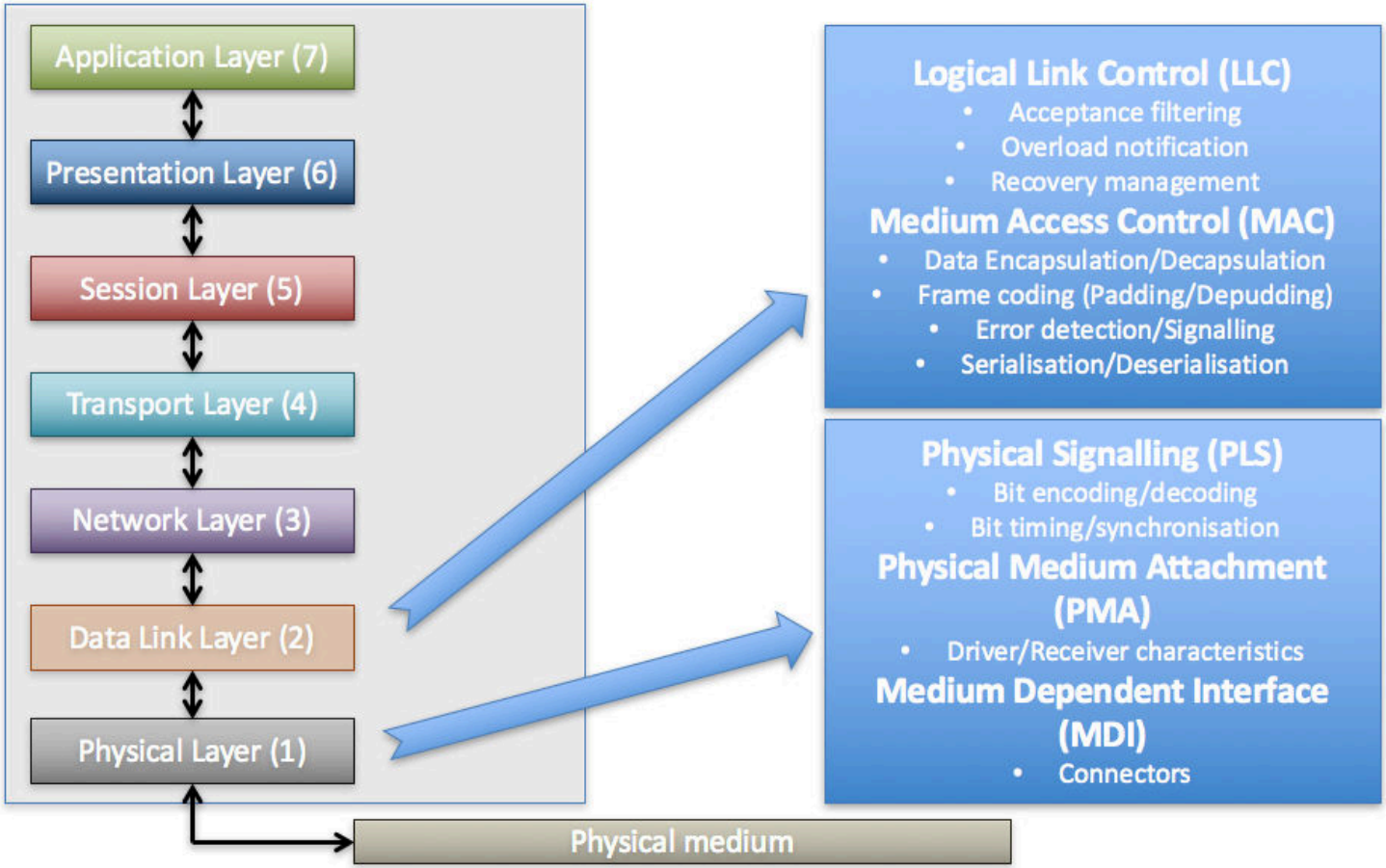

Figure: *IEEE 802* family purposes.

Industrial call for Ethernet

Standards

Standardisation started in the '80s with the *IEEE 802* bodies:

- *802.1*: Local Area Network (LAN) Internetworking;
- *802.2*: previously known as *ISO/IEC 8802-2*, defines the *Logical Link Control* (LLC) as the upper portion of the *Data-Link layer* of the OSI Model;
- *802.3*: CSMA/CD (i.e. Ethernet);
- *802.4*: *Token Bus*, which is a LAN in which the stations on the bus or tree form a logical ring;
- *802.5*: *Token Ring*, which is a token passing scheme on a ring topology LAN used in place of CSMA/CD;
- *802.6*: uses the Distributed Queue Dual Bus (DQDB) network form (i.e. a distributed multi-access network) used for Metropolitan Area Networks (MAN);

Industrial call for Ethernet

Standards

- *802.7*: Broadband Technical Advisory Group;
- *802.8*: Fibre-Optic Technical Advisory Group;
- *802.9*: Integrated Data and Voice Networks;
- *802.10*: Network Security;
- *802.11*: Wireless Networks (/a/b/g/h/f/s/n/p/ac/ax/...);

Industrial call for Ethernet

Standards

- *802.12*: deals with the *Data-Link layer*. The *IEEE 802.12 100 VG - AnyLAN* is a high-speed network with a data rate of 100 megabits per second (Mb/s);
- *802.15*: Personal Area Networks (PAN), such as *Bluetooth* (*802.15.1*) or ZigBee (*802.15.4*);
- *802.16*: Wireless MAN (e.g. *WiMax*);
- Others up to *802.22*.

Industrial call for Ethernet

Ethernet is only defined at the *Physical layer* and *Data-Link layer* of the OSI model and it has been conceived for standard non real-time traffic ($200/300$ ms of packet delays).
At the *Network layer* and *Transportation layer* (the third and the fourth level of OSI), Ethernet is used by TCP/IP or UDP/IP.
Notice that TCP and UDP are de facto the most used protocols, but *they are not part of IEEE 802.3*, and hence may or may not be used with Ethernet.

Industrial call for Ethernet

Add switches

Standard Ethernet is *not* a deterministic protocol, and network QoS cannot be guaranteed.
Non determinism is a natural consequence of the *collision detection* algorithm used at the MAC sublayer.

Industrial call for Ethernet

MAC with CSMA

Ethernet is a random access network, also often referred to as Carrier Sense Multiple Access (CSMA).
Once the carrier is clear, a node must wait for a specified amount of time, called the *interframe time* before sending a message.
To reduce collisions on the network, nodes wait an additional random amount of time, called the *backoff time*, before they start transmitting.
Priorities can be implemented by allowing for *shorter interframe times* for higher priority traffic.
If a collision is detected, the data is corrupted and the message *must be resent*.

CSMA/CD

Ethernet collisions

While transmitting, a node must also listen to detect a *message collision*.
Basically, a collision is detected if the sender simultaneously *receives* a bit from another source.
If so, a transmitting node *continues the transmission* by transmitting additional *jam bits*.
The *jam signal* is transmitted until minimum packet time is reached to ensure that *all* receivers detect the collision.
After a collision, the node waits a random length of time to retry its transmission.

CSMA/CD

Algorithm

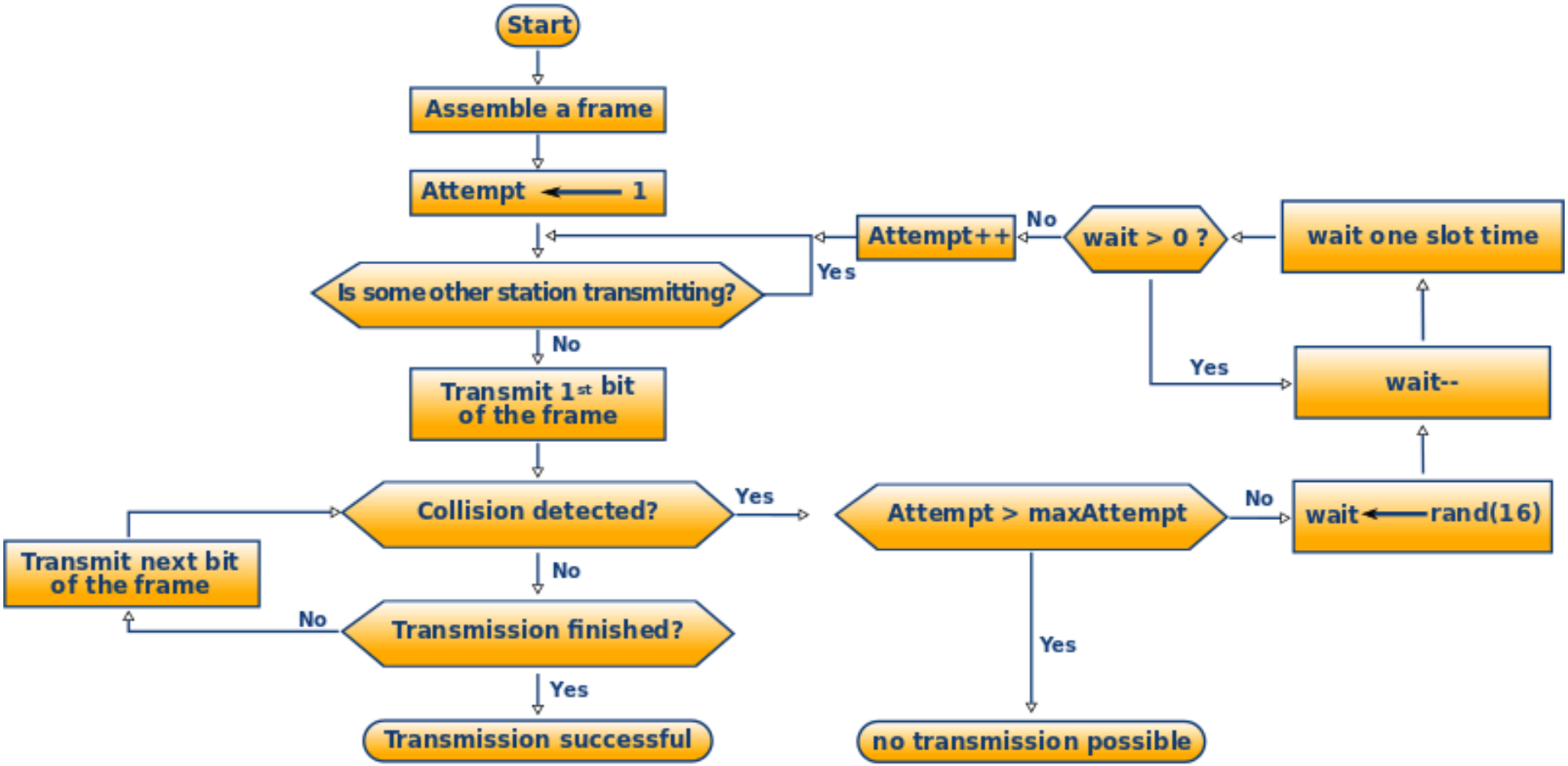

Figure: Simplified CSMA/CD algorithm.

Ethernet frame

Valid frame

The Ethernet standard states that valid frames must be at least *64 bytes* long, reaching 72 bytes including *preamble* and *start delimiter*.
There are two reasons for this minimum size limitation:

- It makes it easier to distinguish valid frames from *garbage*;
- It prevents a node from completing the transmission of a short frame before the first bit has reached the far end of the cable, where it may collide with another frame.

This size defines also the *slot time*: for a 10 Mb/s Ethernet with a maximum length of 2500 m and four repeaters, the time for *one bit* to travel the end-to-end cable with a speed of $2 \cdot 10^8$ m/s is $t_{pr} = 12.5$ μs, hence a round-trip (slot) time of 25 μs. With *64 bytes*, the *frame time* $t_{fr} = 51.2$ μs, thus greater than the *slot time*.

Ethernet frame

Data

The total *overhead*, i.e., data used to rules the transmission but not carrying any information, is 26 bytes, including *preamble* and *start delimiter*.
As a consequence, the minimum *data packet frame* size is $72 - 26 = 46$ bytes, while the maximum data size is 1500 bytes.
If the data portion of a frame is less than 46 bytes, the pad field is used to fill out the frame to the minimum size.

Ethernet frame

Algorithm

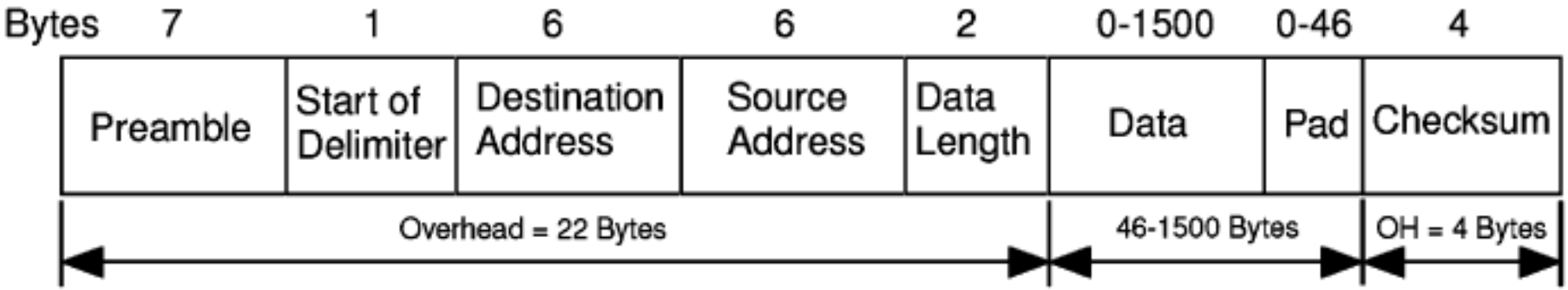

Figure: Ethernet (CSMA/CD) frame format; 20 byte interframe space not shown (James R. Moyne and Dawn M. Tilbury, "*The Emergence of Industrial Control Networks for Manufacturing Control, Diagnostics, and Safety Data*", 2007).

Hub-based Ethernet

Hub-based Ethernet uses *hubs* to interconnect the devices on a network.
When a packet comes into one hub interface, the hub *simply broadcasts* the packet to all other hub interfaces.
All of the devices on the same network receive the same packet simultaneously, and *message collisions are possible*.

Hub-based Ethernet

Issues

Due to the presence of CSMA/CD algorithm, standard Ethernet gives *some* stochastic guarantees only if the network shows *low traffic*.
With heavy traffic, no guarantee can be given.
Moreover, due to the *Binary Exponential Backoff* (BEB) algorithm, *end-to-end* communication is not deterministic as well.

Hub-based Ethernet

Possible workaround

Using standard Ethernet for *control applications* asks for alternative solutions:

- *Synchronisation*: message can be time-stamped to reduce non determinism in communications. This solution can be adopted ensuring *node clocks synchronisation*, e.g., adopting *Precision Time Protocol* (IEEE 1588);
- *Deterministic retransmission*: collided packets are retransmitted with a deterministic delay, which ensures *upper-bounded* delays. The price is an under-exploitation of the CSMA/CD protocol and of the available bandwidth;
- *Prioritised CSMA/CD*: improvements in the response time for time-critical packets, e.g., the networking platform *LonWorks*.

The most effective solution is to use *switches* instead of hubs.

Switched Ethernet

Switched Ethernet utilizes switches to subdivide the network architecture, hence *avoiding collisions, increasing network efficiency, and improving determinism*.
Switches "learn" the topology of the network and forward packets *to the destination port only*.
Switched Ethernet usually relies on the *star cluster* layout to achieve this collision-free property.
Switches use *buffers* to enqueue the messages on the output ports.

Switched Ethernet

Approaches

Two different solutions are adopted in switches:

- *Cut-through*: first *read the destination address*, i.e. *the MAC address*, and then *forward the packet* to the destination port according to the MAC address of the destination and the *forwarding table* on the switch.
- *Store-and-forward*: before applying the *cut-through*, these switches examine the complete packet analysing the *Cyclic Redundancy Check* (CRC) code. This way, even if a little bit slower, they do not forward corrupted packets.

Switched Ethernet

Store-and-forward

To better understand the *Store-and-forward*, imagine that node A sends a packet to node B, that has N_{bit} number of bits over a link with a *data rate* of m bs. How long does it take from A to B if we assume that $t_{tx} \approx t_{fr}$ (i.e. ignoring the t_{pr})?

- The source begins to transmit at time t_0;
- At time $t_0 + t_{tx}$, where $t_{tx} = N_{bit}/m$ s, the packet have entirely reached the switch and, hence, it can start the retransmission;
- Hence, at time $t_0 + 2t_{tx}$ the packet reached node B.

Without switches, the time would be $t_0 + t_{tx}$, but at price of *increasing traffic*.

Switched Ethernet

Forwarding table

Now it should be easier to understand why in the *Ethernet frame* the *destination address* should be present.
Imagine the work of a *switch*: when it receives the packet, it *analyses the destination address* and compare it to the stored *forwarding table*.
Then, it routes the message towards the *most efficient* next *switch* (e.g., based on traffic, distance, other performance policies).
Notice that the *destination address* is analysed with *increasing level of details*: this is exactly what a human being does when it has to reach a destination or asks for directions!

Switched Ethernet

Circuit versus Packet

There are two different approaches for *switches*:

- *Circuite switching*: the *resources needed along a path* (e.g., buffers, links) to provide for communication between the nodes are *reserved for the duration of the communication session* (e.g., telephone lines);
- *Packet switching*: the *resources are not reserved* but, instead, *used on demand*, which asks for the use of *message queues*.

As an analogy, the restaurants *with or without* the reservation.
Again, *circuit switching* leads to *under exploitation* of resources (as for *time based* approaches), while *packet switching* uses the resources *on demand* (as for *event based* approaches).

Outline

Real-Time Ethernet

Keywords

Keywords for real-time communication systems:

- *Determinism*: the ability of serving a request in a limited and *known* time. In other words, determinism implies that the *maximum latency* is known upfront;
- *Isochronous behavior*: the behavior is *repetitive* in time. In other words, *low jitter*;
- *Synchronisation*: of *communication* (e.g., TDM); of *Input/Output* (IO) operations; of the *applications*.

Outline

Profinet

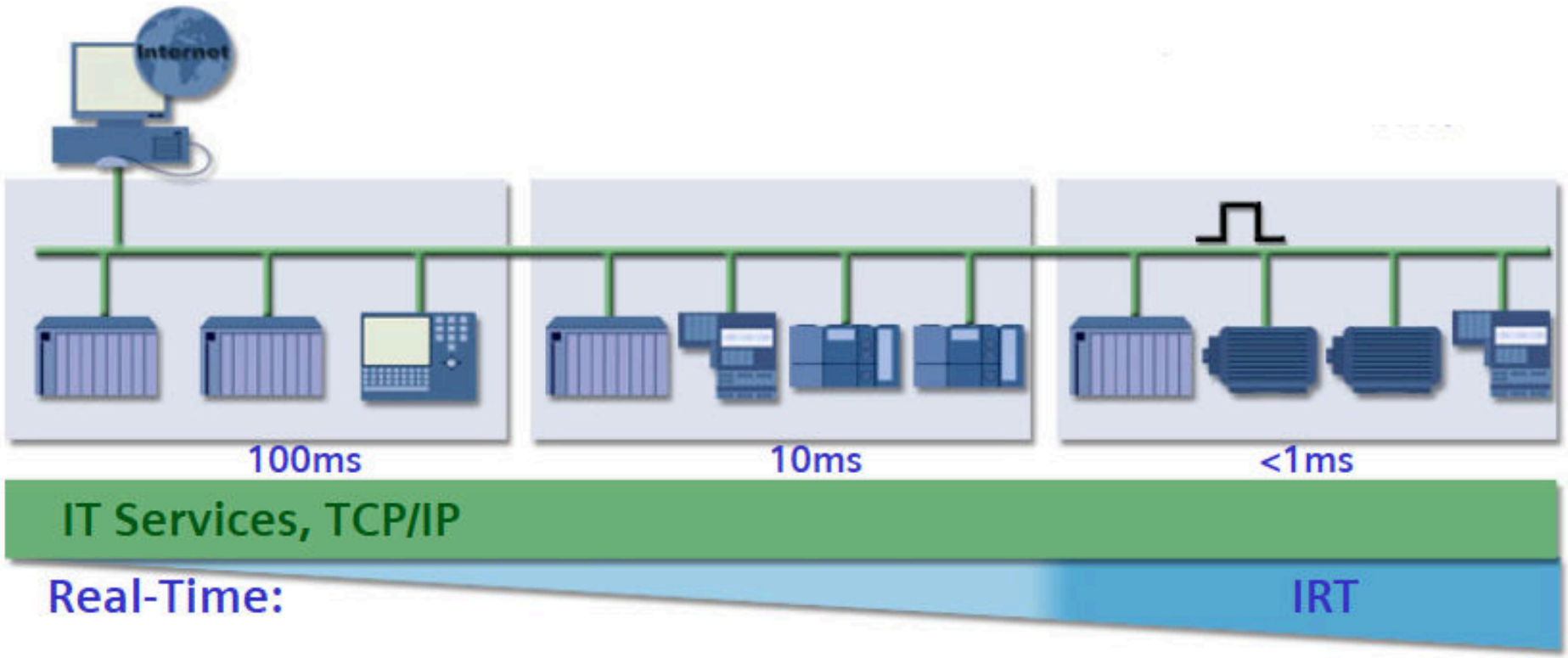

Figure: One solution offering different capabilities as a function of the desired traffic (courtesy of Paolo Ferrari, Università di Brescia).

Profinet

Incrementing the stack performances

Profinet makes use of a *Time Division Multiple Access* (TDMA) technique to guarantee fast and precise access to the transmission medium.
In practice, the traffic scheduling takes place according to a *cycle timing*.

Profinet

Incrementing the stack performances

Messages are divided into three types, with *increasing* time criticality:

(1) *TCP/IP standard*: used for devices set-up, diagnostics, start-up of the network;

(2) *Real-Time* (RT): used for high-performance data transfer, cyclic data, event-based data communication. Known as *RT_CLASS 1*;

(3) *Real-Time channel* (IRT): used for hi-performance data transfer with *isochronous* feature (i.e., jitter less than 1 μs). Known as *RT_CLASS 2* and *RT_CLASS 3*.

Profinet

Traffic typologies

In practice for *RT_CLASS 3* (the most critical), the communication takes place over *predefined physical paths* enforced by a *special kind of switches* purposely developed for Profinet (similar to the *circuit switches*).
For *RT_CLASS 2* (that is also isochronous), physical paths are *not* predefined (uses *packet switches*).
For *RT_CLASS 1* (real-time communications), which is the only *mandatory* one, access to the physical medium is regulated by the *priority* assigned to the frames, according to IEEE 802.1Q.

Profinet

TDMA

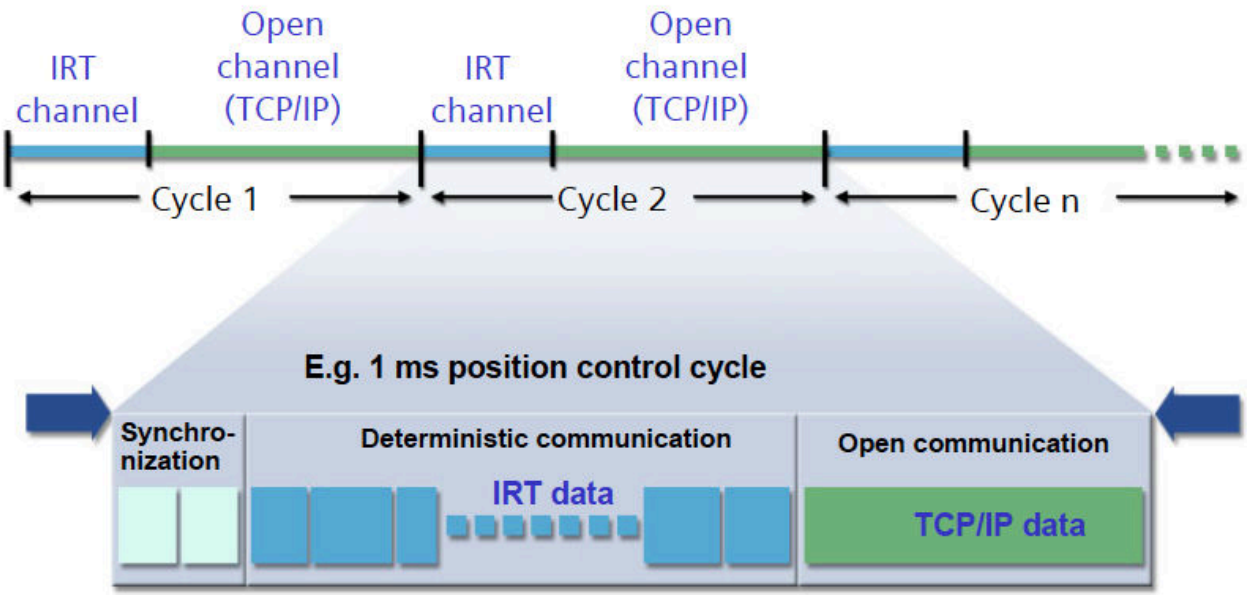

Figure: Time Division Multiple Access idea (courtesy of Paolo Ferrari, Università di Brescia).

Synchronisation is achieved by means of *Precision Transparent Clock Protocol* (PTCP).

Profinet

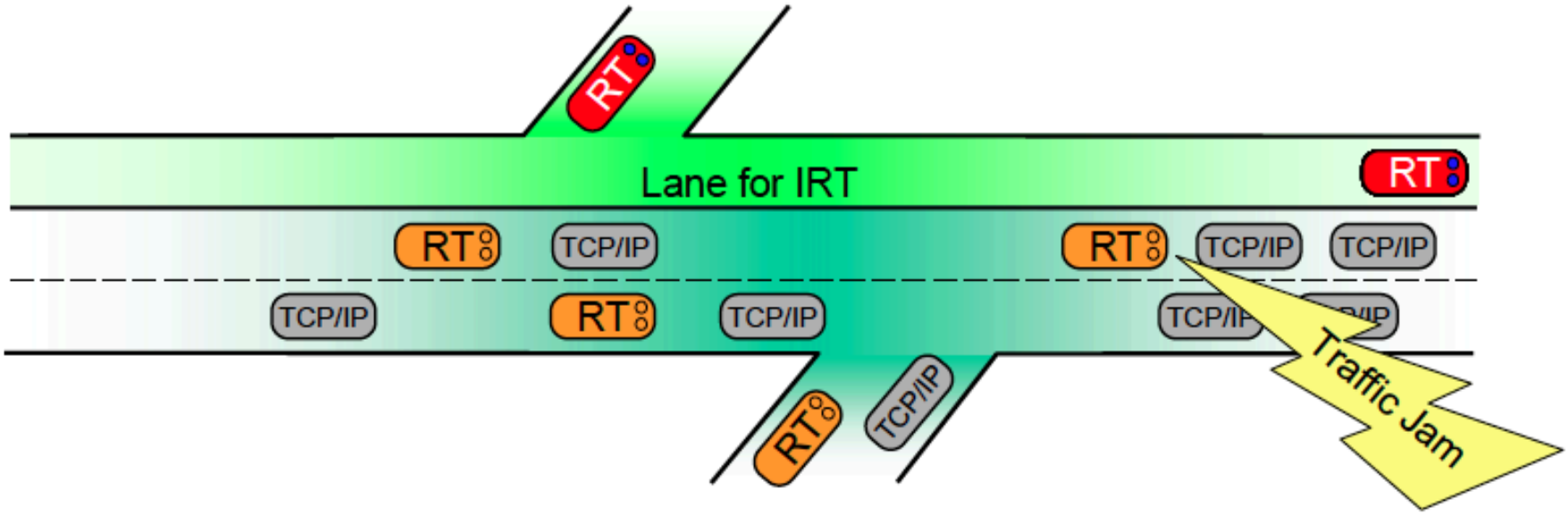

Figure: The basic idea (courtesy of Paolo Ferrari, Università di Brescia).

Profinet

Protocol stack

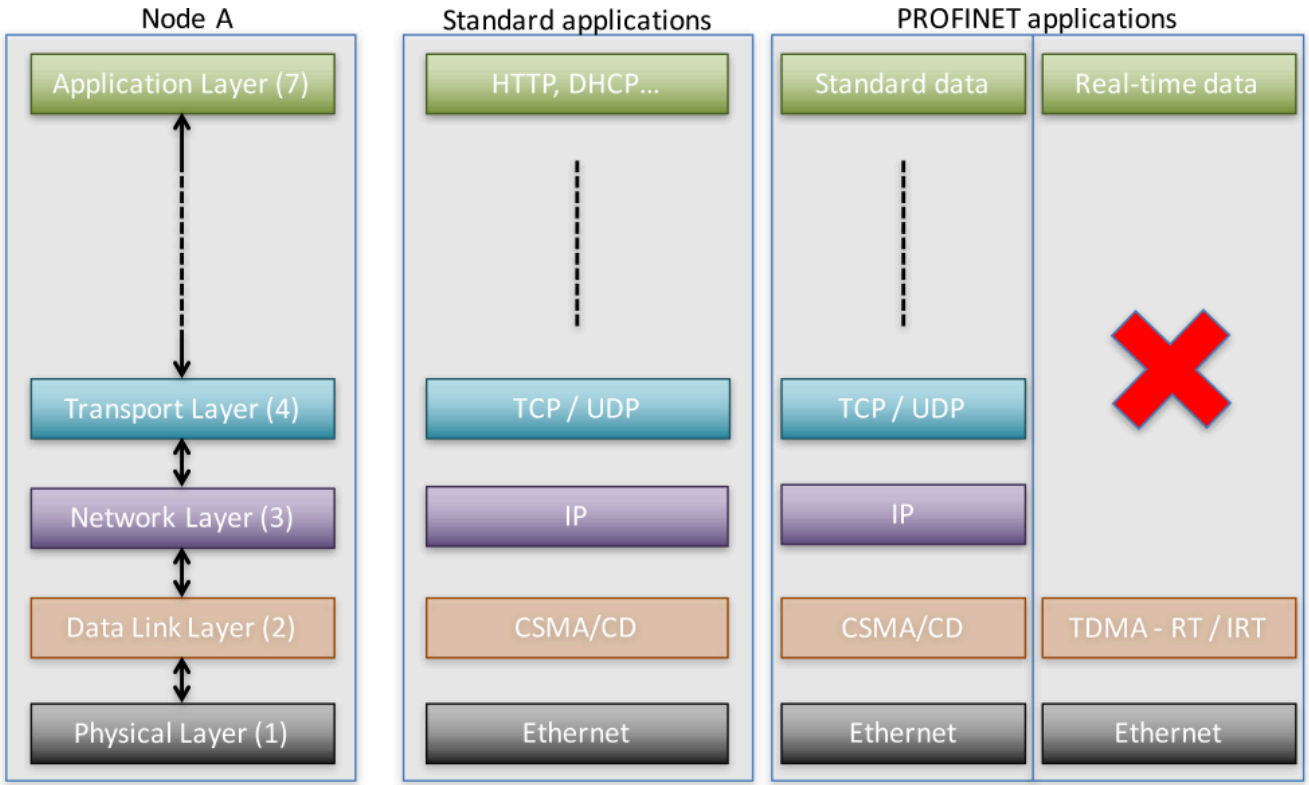

Figure: The implementation of the OSI model for Profinet.

Profinet

Performance

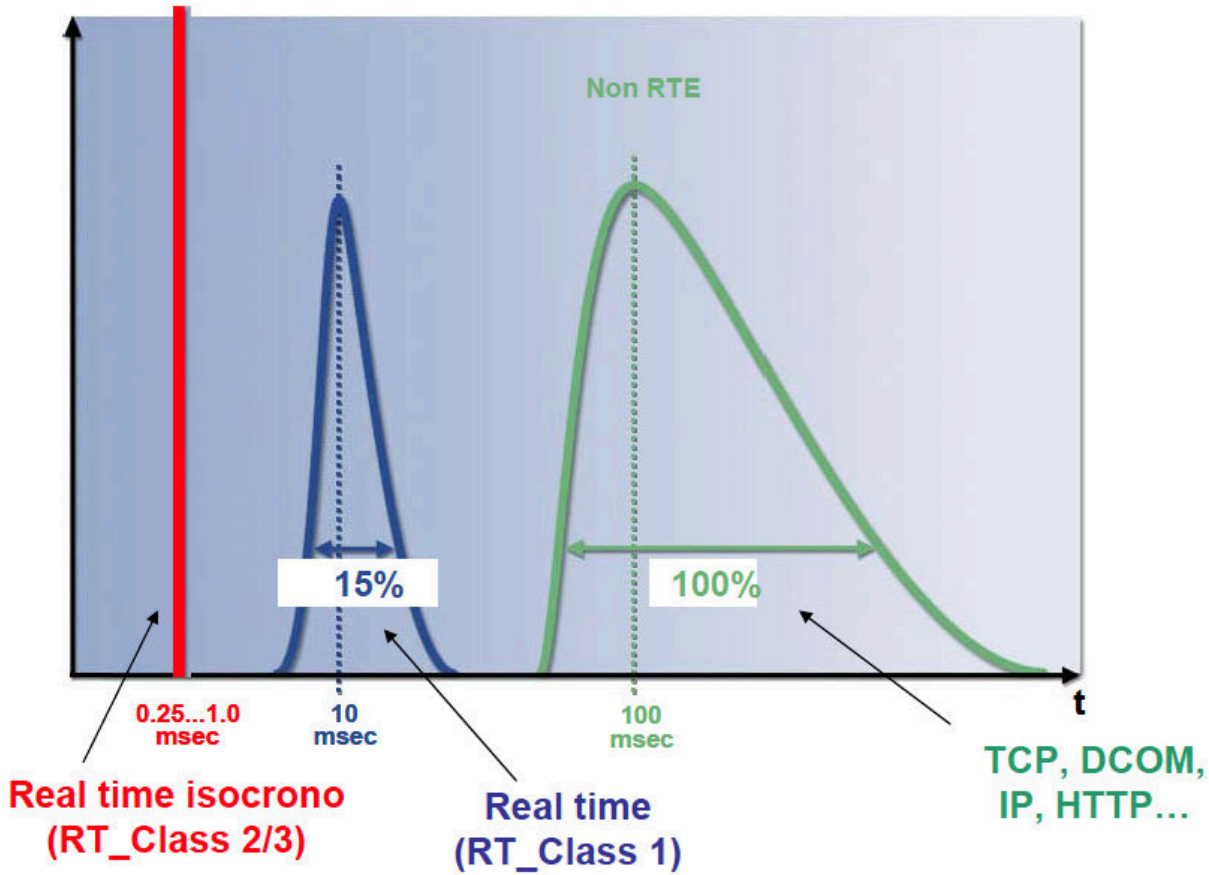

Figure: Performance achievable on the different channels (courtesy of Paolo Ferrari, Università di Brescia).

Outline

EtherCAT

Beckhoff, a German automation company, developed a fieldbus system called *Fast Lightbus* to correct the low bandwidth utilisation problem present in other Ethernet protocols. This protocol led to *Ethernet for Control Automation Technology* (EtherCAT) which Beckhoff released in 2003.
In 2004, Beckhoff helped to create a new group to promote the EtherCAT protocol. Their efforts led to the *EtherCAT Technology Group* (ETG). Beckhoff donated the rights to EtherCAT to the ETG.
The ETG works with the *International Electrotechnical Commission* (IEC), specifically serving as a liaison for the digital communications working group. The partnership has led to standardisation throughout the EtherCAT protocol's history.

EtherCAT

Characteristics

EtherCAT requires *full-duplex* on copper or fiber optic cables.
It supports *any network topology*, including bus.
It is based on *master-slave* and interoperates with TCP/IP or Profinet.
The EtherCAT master processes the RT traffic via *dedicated hardware and software*.

EtherCAT

Frames as telegrams

As noted previously, typical automation networks are characterised by short data length per node, typically *less* than the minimum payload of an Ethernet frame. Using one frame per node per cycle therefore leads to low bandwidth utilisation and thus to poor overall network performance.
The idea is to use *the same* frame to transmit *multiple messages*.
To overcome this limit, EtherCAT uses the *processing on the fly* approach: the Ethernet frame is *no longer* received, interpreted and copied as process data at every node, but rather uses the idea of *broadcasted telegram*.

EtherCAT

Frames as telegrams

The EtherCAT slave devices read the data addressed to them while the *telegram passes* through the device. Similarly, input data are inserted while the telegram passes through.
Both operations are computed in *hardware*, hence a delay of *nanoseconds* is generally introduced.
Many nodes - typically the entire network - can be addressed with just one frame.

EtherCAT

Frames

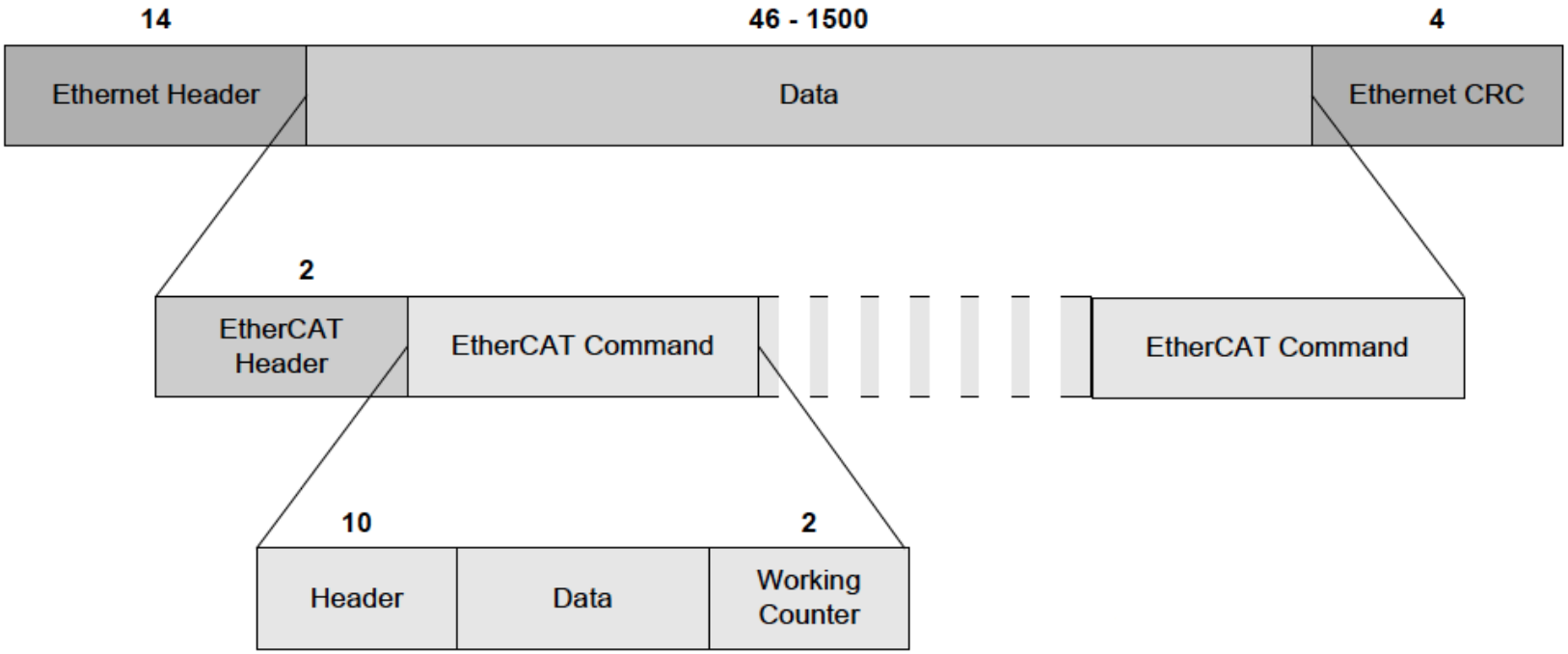

Figure: EtherCAT frame encapsulation (Paula Doyle, "Introduction to Real-Time Ethernet II", 2004).

EtherCAT

Final remarks

The EtherCAT uses special devices.
It also optionally adopts the *E-bus*, which is an EtherCAT *physical layer* for Ethernet offering *Low Voltage Differential Signal* (LVDS) scheme.
EtherCAT is a fast RTE solution, offering determinism if not used with intermediate switches or routers between master and slave.

Outline

Wireless in industry

Thanks to their peculiar features, *wireless networks* are currently becoming more and more attractive for use in industrial automation and manufacturing scenarios.
However, they *cannot be thought* as a total replacement for more traditional wired networks in such environments, at least at the moment.
This means that solutions exist *integrating* the existing industrial wired solutions and wireless solutions, in order to achieve enhanced *flexibility, efficiency, and performance* for the overall networked system.

Wireless in general

Fundamental difference

Wireless Network is a network where the access is on a *non-guided media* (aka theterless channel).
Cellular Network is a global network where the coverage is obtained with a set of *cells*, i.e. adjacent or overlapping areas. The mobile terminal can move from one cell to the other keeping the communication seamlessly active.

Wireless in general

IEEE 802 family

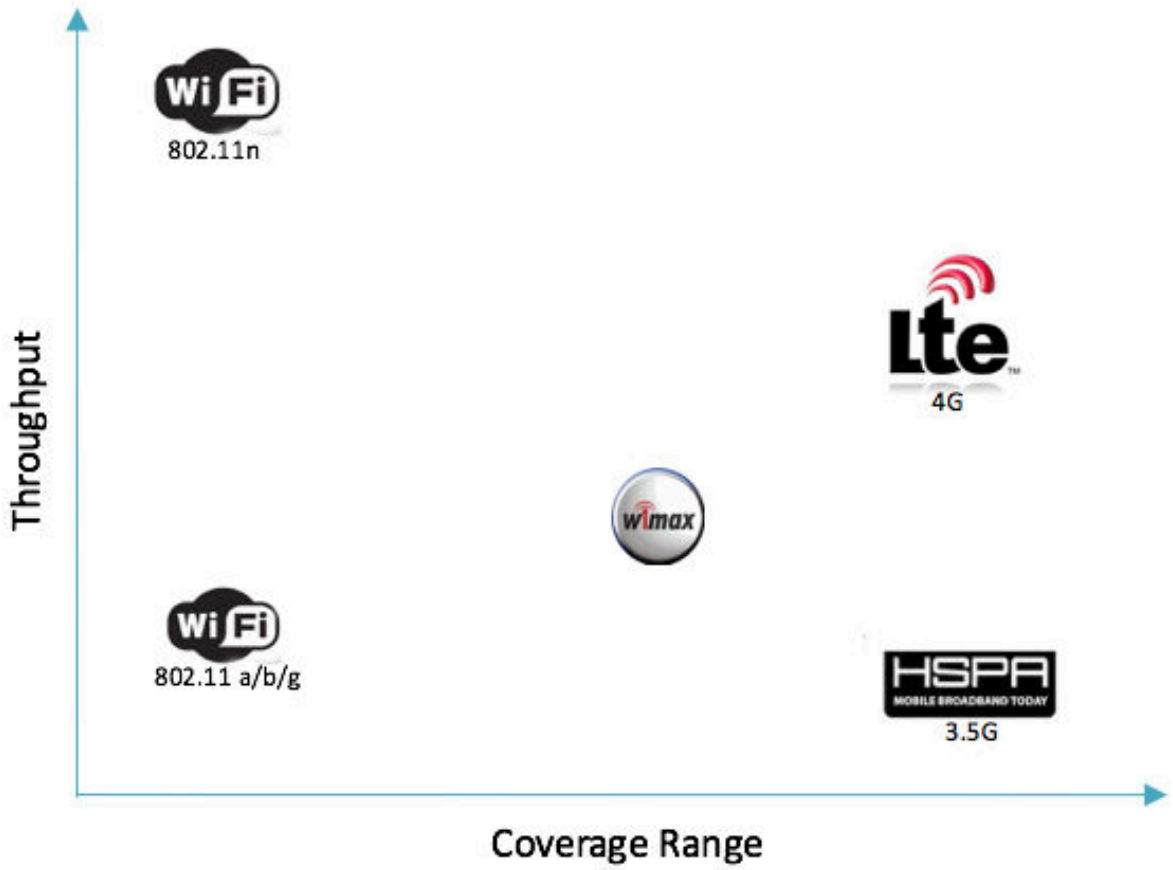

Figure: Different wireless solutions in *IEEE 802*.

Wireless in general

IEEE 802 family

Standard	Family	Downlink (Mbps)	Uplink (Mbps)	Coverage
WiFi	802.11	11/54/150/300		100m
WiMAX	802.16e	144	35	10km
UMTS (3G) /HSPA (3.5G)	3GPP	14.4	5.76	30km
LTE (4G)	3GPP	360	80	30km

Figure: Different wireless solutions: features.

Wireless in industry

Basis of communication

The *speed of light* is $c \approx 299792458$ m/s, while f [Hz] is the *frequency*. The *wave length* is then $\lambda = c/f$.

System	Frequency	Wavelength
FM radio	100 MHz	3 m
Cellular	800 MHz	37.5 cm
Ka band satellite	20 GHz	15 mm
Ultraviolet light	10^{15} Hz	10^{-7} m

Wireless in industry

Basis of communication

Classification Band	Initials	Frequency Range	Characteristics
Extremely low	ELF	< 300 Hz	Ground wave
Infra low	ILF	300 Hz - 3 kHz	
Very low	VLF	3 kHz - 30 kHz	
Low	LF	30 kHz - 300 kHz	
Medium	MF	300 kHz - 3 MHz	Ground/Sky wave
High	HF	3 MHz - 30 MHz	Sky wave
Very high	VHF	30 MHz - 300 MHz	Space wave
Ultra high	UHF	300 MHz - 3 GHz	
Super high	SHF	3 GHz - 30 GHz	
Extremely high	EHF	30 GHz - 300 GHz	
Tremendously high	THF	300 GHz - 3000 GHz	

Figure: Radio frequency bands (courtesy of John Hopkins University, Computer Science Department).

Wireless in industry

Basis of communication

The VHF/UHF ranges are used for *mobile radio*: simple, small antenna for cars; *deterministic propagation* characteristics, reliable connections.
SHF and higher for *directed radio links and satellite communication*: small antenna, large bandwidth available.
Wireless LANs use frequencies in UHF to SHF range, even though some systems planned up to EHF.
Limitations due to *absorption by water and oxygen molecules* (resonance frequencies), hence weather dependent fading, signal loss caused by heavy rainfall etc.

Wireless in industry

Basis of communication

Propagation in free space always *like light* (straight line): *line-of-sight* constraint.
Received power influenced by:

- Fading (frequency dependent);
- Shadowing;
- Reflection at large obstacles;
- Refraction depending on the density of a medium;
- Scattering at small obstacles;
- Diffraction at edges.

Wireless in industry

Basis of communication

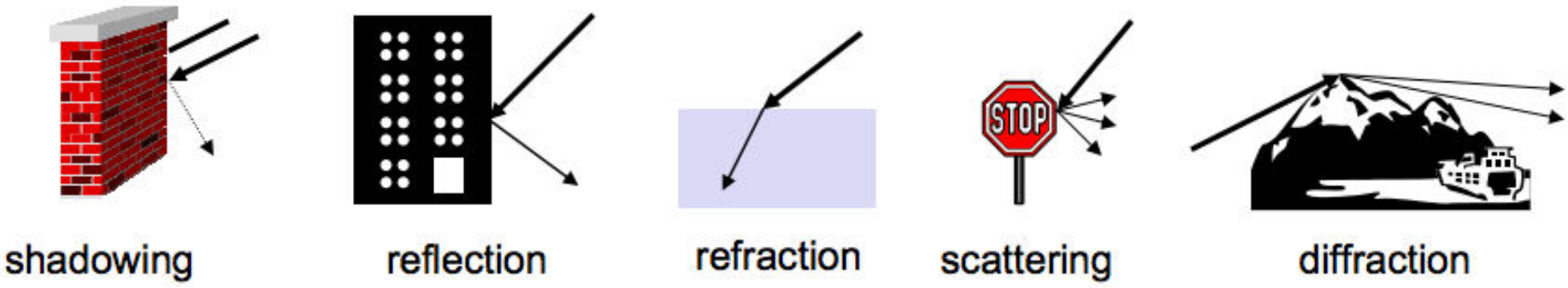

Figure: The effect of obstacles in wireless transmission (courtesy of John Hopkins University, Computer Science Department).

Wireless in industry

Basis of communication

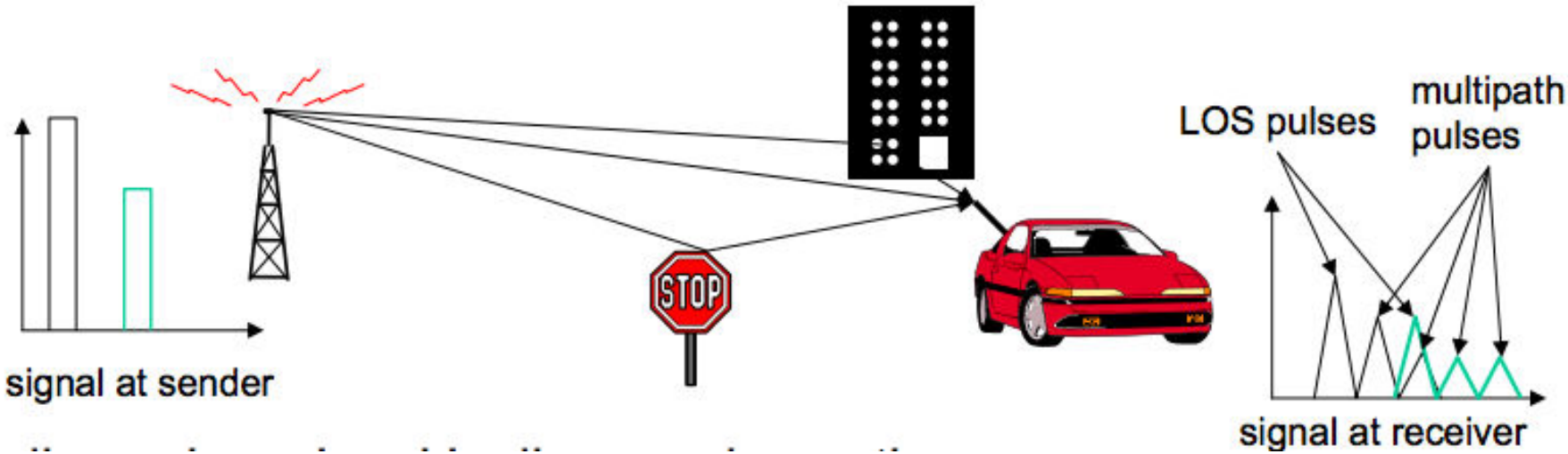

Figure: Multipath (courtesy of John Hopkins University, Computer Science Department).

Wireless in industry

Basis of communication

So, wireless communication is set-up using *radio channels*, which can be classified in three groups based on the *operational distance*:

- Very short distance (e.g., with one or two meters);
- LANs (e.g., ten to a few hundred meters);
- Wide Area Networks (WANs) (e.g., tens of kilometers).

Wireless in industry

Basis of communication

To conclude the discussion, there is also the *satellite communication*. Two possible approaches:

- Geostationary satellites, that *permanently remain above the same spot on Earth* by placing the satellite in orbit at 36000 km above the Earth's surface. This distance induces a *propagation delay* $t_{pr} = 280$ ms. The *data rate* is in the order of hundreds of Mbps and each satellite act as a *repeater*;
- Low-Earth Orbiting (LEO) satellites, placed much closer to Earth and, hence, *move with respect to the Earth's surface*.

Outline

Wireless protocol

The *IEEE 802.11* family includes several standard specifications for wireless LAN, short *WLAN*.
All devices belonging to such a family (also referred to as *WiFi*, i.e. *Wireless fidelity*) work in specific bands of the radio spectrum, centered around:

- 2.54 GHz: legacy 802.11, 802.11b, 802.11g;
- 5 GHz: 802.11a.

Very high data rates are foreseen in the 802.11 standard, ranging from 11 Mb/s for *IEEE 802.11b* to a (nominal) 54 Mb/s for *IEEE 802.11g/a*.
Moreover, *IEEE 802.11n*, whose standard has been released in 2009, may reach up to 300 Mb/s, acting in *dual band* (both 2.54 and 5 GHz).

Wireless protocol

WiFi

WiFi: Opportunistically use WiFi hotspots once they are available.
WiFi network topology:

- Point-to-Multipoint (*Access Point*);
- Point-to-Point (*Ad hoc*);
- Multipoint-to-Multipoint (*Mesh Network*).

Connects with almost any *WiFi CERTIFIED* device.
Designed for portable and stationary devices.

Wireless protocol

Architecture

The main difference with the *wired world* is the presence of the *base station*.
A *base station* is responsible for sending and receiving data (e.g., packets) *to and from* a *wireless host* that is associated with that base station.
A *base station* is often be responsible for coordinating the transmission of multiple wireless hosts with which it is associated.
A *wireless host* is *associated* with a base station when (1) the host is within the wireless communication distance of the base station, and (2) the host uses that base station to relay data between it and the larger network.
Cell towers in cellular networks and access points in 802.11 wireless LANs are examples of base stations.

Wireless protocol

Architecture

Hosts associated with a *base station* are often referred to as operating in *infrastructure mode*, since all traditional network services (e.g., address assignment and routing) *are provided by the base station*.
In *ad hoc networks*, wireless hosts have no such infrastructure with which to connect. In the absence of such infrastructure, *the hosts themselves must provide for services* such as routing, address assignment, DNS-like name translation, and more. To provide this services, usually *multi-hop* communication is needed.
When a mobile host moves beyond the range of one base station and into the range of another, it will change its point of attachment into the larger network (i.e., change the base station with which it is associated)—a process referred to as *handoff*.

Wireless protocol

Architecture

The *Basic Service Set* (BSS) defines the set of nodes using the same *coordination function* to access the channel.
Two BSS configuration modes:

- *Ad hoc* mode: stations can dynamically form a network without AP and communicate directly with each other (computer or laptop LANs, called *Independent BSS* - IBSS). Managed by the *IETF MANET* (Mobile Ad hoc Networks) working group;
- With *infrastructure*, i.e. the BSS is connected to a fixed infrastructure through a centralised controller, that is the AP.

The *Basic Service Area* (BSA) is the spatial area covered by a BSS, i.e. a WLAN.
Interconnections among several BSSs is possible at the MAC sublayer and, usually, there is a *network of APs* connected by a *backbone*, e.g. *Ethernet*.

Wireless protocol

Architecture

In general, to join a BSS three operations are needed: *Scanning*, *Authentication* (open system authentication, shared key authentication - WEP, per session authentication - WPA2) and *Association* (information exchange about the AP and node capabilities and roaming). Two different approaches:

- *With APs*: Both authentication and association are necessary for joining a BSS;
- *Ad-hoc*: No authentication nor association procedures are required for joining an IBSS.

Wireless protocol

Scanning

To "get in touch" with an AP:

- *Passive scanning*: the newcomer search for a *Beacon frame*, that is a particular frame sent by the AP every 100 ms;
- *Active scanning*: the newcomer *sends a Probe Request* frame on a given channel. All the receiving AP's *reply with a Probe Response* frame.

Wireless protocol

MAC sublayer

The IEEE 802.11 standard specifies two ways to access to the physical medium:

- *Distributed Coordination Function* (DCF): this is *mandatory* and it is based on CSMA/CA (CA stand for *Collision Avoidance*);
- *Point Coordination Function* (PCF): this is *non mandatory*. It is a centralized MAC protocol coordinated by a *Point Coordinator* which grants exclusive access to any wireless station, thus preventing collisions (very similar to the *TDMA*).

Although PCF is *not* currently supported by the vast majority of commercial WiFi boards, it nevertheless represents an *interesting option for industrial applications*.

Wireless protocol

MAC sublayer

Basically:

- *Distributed Coordination Function* (DCF): Asynchronous data transfer for best-effort traffic. It is based on CSMA/CA, which is based on carrier sense and a *back off* algorithm (as in Ethernet). The main difference is that it is very difficult to detect a collision while transmitting, hence an ACK from the AP is expected: if it does not arrive, a collision took place;
- *Point Coordination Function* (PCF): data transfer for real-time traffic. In this case it can also use the *Request to Send/Clear to Send* (RTS/CTS) handshake with the AP to ask for permissions to transmit.

Outline

Ad-hoc wireless interconnections

The *IEEE 802.15.4* family deals with *ad-hoc wireless interconnections* of electronic devices within a *limited transmission range* (some tens of meters) at *low data rates* (up to 250 kb/s).
It is a *general purpose* standard, whose applications can be found in home and building automation, simple cable replacement, smart tags, automotive sensing, etc.
Devices of the IEEE 802.15.4 family typically operate in the band centered around 2.4 GHz.

Ad-hoc wireless interconnections

PHY

The *Physical layer* (PHY) manages the physical *Radio Frequency* (RF) transceiver and performs channel selection and energy and signal management functions.
It works in the range between about 800 MHz and 2.5 GHz.
The standard *IEEE 802.15.4e* adopts *channel hopping strategy* to improve support for the *industrial markets*.
This way, it increases robustness against external interference and persistent multi-path fading.
Networks can be built as either *peer-to-peer* or *star* networks.

Outline

Fieldbus or RTE with wireless

Although technically feasible, wireless extensions of industrial networks to be used in place of fieldbuses or RTE networks are *not so straightforward*. This is due by three main reasons...

Fieldbus or RTE with wireless

First problem: transmission support

First problem: the wireless medium is *shared* among *all* the nodes.
Even operating at the maximum allowable speed (e.g., 54 Mb/s for currently available 802.11a/g/e networks), this may result in a *low throughput* compared to that of wired networks when the number of connected devices grows higher.
Related to this problem, wireless connection requires the *non negligible overheads* to perform *protocol control* and for *acknowledgement and reservation* mechanisms.
For example, transmit 8 bytes over on a standard WLAN takes about 100 μs, slightly shorter than a 1 Mb/s CAN bus.
Additionally, there is no provision for *full-duplex* operations.

Fieldbus or RTE with wireless

First problem: transmission support

Solutions to this first problem are twofold:

- *Technological*: make use of more performant WLAN protocols, such as IEEE 802.11n;
- *Infrastructure*: make use of a set of small sub-networks, interconnected by means of a *wired backbone* in order to limit the packet rate on each of them.

Fieldbus or RTE with wireless

Second problem: determinism

Second problem: *random access* techniques (e.g., CSMA/CA) are often employed by wireless networks.
As already mentioned, this choice implies *unpredictable (and unbounded) transmission delays* and, even worse, *network congestions* could be experienced.
In the presence of network congestions, the network may become *temporarily unavailable* to carry out timely data exchanges, which is not compatible with proper operation of distributed control systems.
Finally, *non negligible jitters* may affect the transmission even in the case of lightly loaded networks, unless some form of *prioritization scheme* is suitably adopted.

Fieldbus or RTE with wireless

Second problem: determinism

Solutions to this second problem are threefold:

- *PCF*: adopt TDMA based solution with a *central scheduler*;
- *Technological*: adopt TDMA based solution as in IEEE 802.15.4;
- *Priority*: adopt new prioritization features offered by the IEEE 802.11e standard, even though *strict determinism* cannot be reached.

Fieldbus or RTE with wireless

Third problem: robustness

Third problem: wireless channels are much more *error prone* than wired cabling, especially with high electromagnetic interference as in industrial environments.
This problem generates communication *latencies and jitters*.
Moreover they affect the network *reliability* and, consequently, the *robustness* of the overall system.
There is a non negligible chance that messages sent over the air *never reach* the intended destination (e.g., consistency problems in multicast messages).

Fieldbus or RTE with wireless

Third problem: robustness

Solutions to this third problem are twofold:

- *Antennas*: make use of *multiple antennas* to increase message delivery reliability;
- *Band*: adopt the 5 GHz band for communication, thus *reducing interferences* with other mobile phones, Bluetooth enabled equipment, notebooks with wireless connections.

Outline

Ethernet RT and Wireless Networks

Ethernet-based networks are becoming of increasing interest despite their native *unpredictability* of communications.
Real-time Ethernet ensures determinism of communications by ruling the access to the shared medium.
Profinet uses a *Time Division Multiple Access* to rule the coexistence of different types of traffic over the network.
EtherCAT ensures determinism with special hardware.
Ethernet Powerlink uses a *Time Division Multiple Access* solution.
Wireless solutions offer higher flexibility than wired connections, but with a lower *Quality of Service*.
Solutions exist for industrial applications that integrates hybrid solutions, i.e. wired/wireless, *with major issues to be addressed*.