Mobile and Cyber Physical Systems - Appunti

Francesco Lorenzoni

February 2024

Contents

Course info

...

Chapter 1

Internet of Things

The main topics addressed aside from **IoT** itself are how it relates to *Machine Learning* and *Cloud* computing processes, but also *IoT interoperability*, known *Standards*, and the *security* concerns about IoT.

1.1 IoT introduction

Cyber and Physical Systems (CPS) operate in both the Physical and Cyber worlds, thus we can see IoT as an embodiement of CPSs.

In a *smart environment*, smart objects are both physical and cyber, hence they are subject to "physical experiences" such as being placed, moved, damaged and so on.

But actually...
What is a *smart environment*?

The answer actually ain't trivial.

1.2 Platforms for IoT

Sensors and actuators are the edge of the cloud. In general the purpose of IoT is to gather and send data, send it somewhere where it gets transformed into information ultimately used to provide some functionality for an end user, or it simply presented to them.

A **Platform for IoT** is essentially a —complex— software hosted on the cloud, which, first of all, **collects** data gathered by IoT devices, but *not* only that:

- Identification
- Discovery
- Device Management
- Abstraction/virtualization
- Service composition
  Integrating services of different IoT devices and SW components into a composite service
- Semantics
- Data Flow management
  - *sensors* $\longrightarrow$ *applications*
  - *applications* $\longrightarrow$ *sensors*
  - Support for aggregation, processing, analytics

1.3 No-SQL Databases

No-SQL DBs address the problem of the several changes of data formats, sources, cardinality and so on, which happen throughout time.

A common example is **MongoDB**, which stores records in JSON-like objects called *documents*, which are stored in *collections*, the entity corresponding to tables in relational DBs, with the key difference that multiple documents in a single collection may be structured differently.

1.4 IoT Issues

◇ Performance
◇ Energy Efficiency
◇ Security
◇ Data analysis/processing
  – Adaptability/personalization

The course will cover the basics of signal processing, with mentions to machine learning

◇ Communication/brokerage/binding
◇ Data representation
◇ Interoperability

Standard discussed will be ZigBee, MQTT, and IEEE 802.15.4 (?)

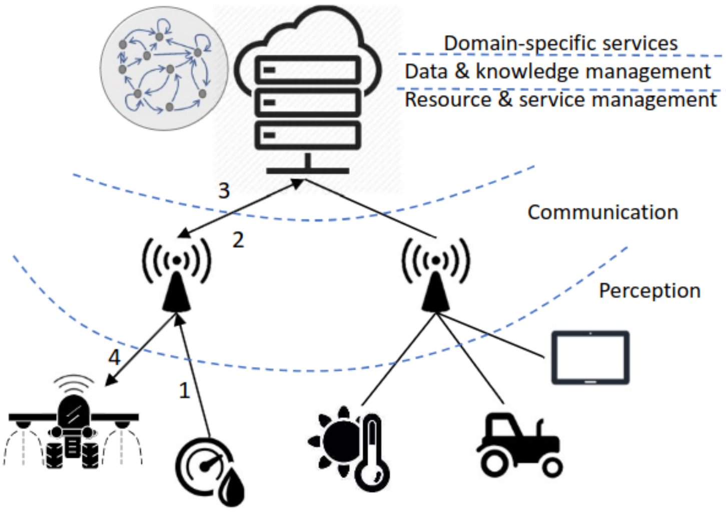


Figure 1.1: Communication outline in IoT

IoT systems are distributed, and servers may be dislocated around the globe, making room for **latency** and **reliability** issues.

To confine the problem displayed in Fig. 1.1 there are proposal to move the ability to make a decision on the data closer to the edge, but this in general isn't trivial.

Key Issues

1. Producing and handling fast-streaming heterogeneous sensed data
2. Make devices context-aware & allow them for continuous adaptation
3. Handle strong computing and energy constraints

1.4.1 Edge and Fog computing

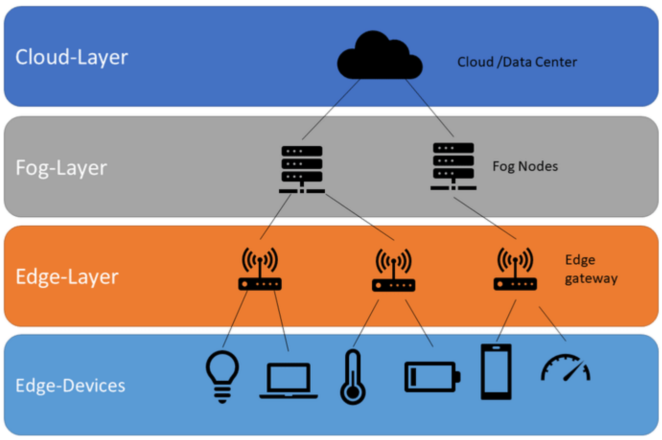


Figure 1.2: Layers scheme

A solution forsees to split the network in 4 layers, allowing for different response times and decisional capabilities.

A gateway on the **edge** interconnects the IoT-enabled devices with the higher-level communication networks, performing protocol translations.

A basic task performed at the fog layer is aggregating and collecting data, and then flushing it to the cloud periodically.

However, some decisions on the aggregated data may be taken at the fog node without querying the cloud, for instance determining where is a nest of tortoises, whether an explosion has occurred (by analyzing data from multiple sensors), and —maybe, one day in a not-so-far future— recognize human language.

prof. Chessa developed an 8 bit controller implementing a model for determining where is a nest of tortoises.
Alexa and *Google Home* currently send audio samples to the cloud for processing, but in the futurue this may be done locally.

1.4.2 Artificial Intelligence

AI splits into **Machine Learning** and **Curated Knowledge**.

ML focuses on mimicking how humans *learn* on new knowledge, while *curated knowledge* focuses on mimicking how humans *reason* on a known set of data.

Machine Learning reveals itself to be particularly useful in aggregatin multiple heterogeneous time-series sensed data about the same environment.

Supervised and Reinforcement learning are more promising than

1.4.3 Blockchain & IoT

A **blockchain** may act as a shared ledger between companies in a supply chain, with IoT devices to track goods and to monitor their quality along the chain, i.e. production stages, shipping and distribution.
With a blockchain each actor along the supply chain can query the ledger to check the —certified— state of the goods.

1.4.4 Interoperability

Vertical Silos

Developing a straight implementation of an IoT solution, starting from physical up to the application layer, is not a problem by itself.
In this way solution you implemented will work only on your devices, making your intervention needed for any change or update; besides, products by other vendors will be incompatible.

Vertical Silos business model leads to **vendor lock-in**s, which basically are service limitations which prevent the users from purchasing and using products from other vendors.

The solution to avoid —or limit— such issues is to introduce **standards**.

For what concerns wireless communication, standards are mainly differentiated by *Range* and *Data Rate*.

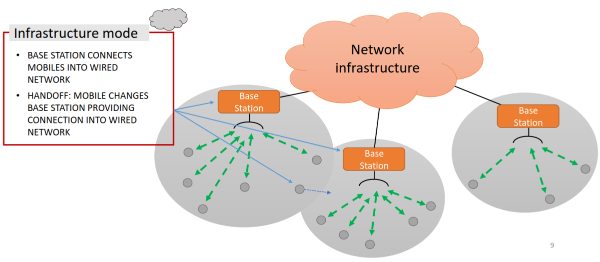
Chapter 2

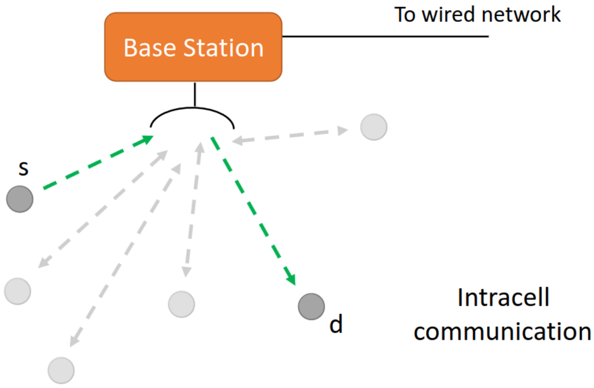
Wireless Networks

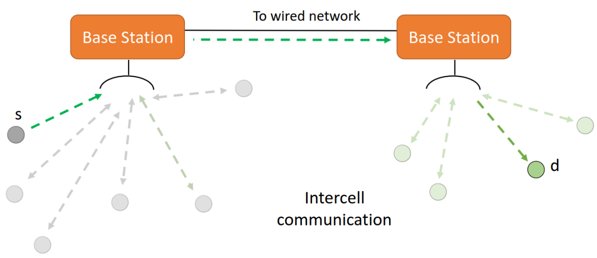
Wireless Networks are composed of **hosts**, which are end-system devices that run applications, typically battery powered.

Recall that *wireless ≠ mobility*

In general Wireless Networks may be based on the interaction *hosts longrightarrow base station* —or access point— or *hosts longrightarrow hosts*. The two resulting functioning modes are called *Infrastructure* and *Ad hoc networking*.







2.1 Link Layer

2.1.1 CSMA/CD

Basic idea of CSMA/CD:

1. When a station has a frame to send it listens to the channel to see if anyone else is transmitting
2. if the channel is busy, the station waits until it becomes idle
3. when channel is idle, the station transmits the frame
4. if a collision occurs the station waits a random amount of time and repeats the procedure.
   Refer to the slides of 21 February for more in depth usage examples

In short: CSMA/CD performs poorly in wireless networks. Firstly because CSMA/CD detects collisions while transmitting, which is ok for wired networks, but not for wireless ones. Secondarily, what truly matters is the interference at the *receiver*, **not** at the *sender*, causing the two problems known as *hidden* and *exposed terminal* problems; to

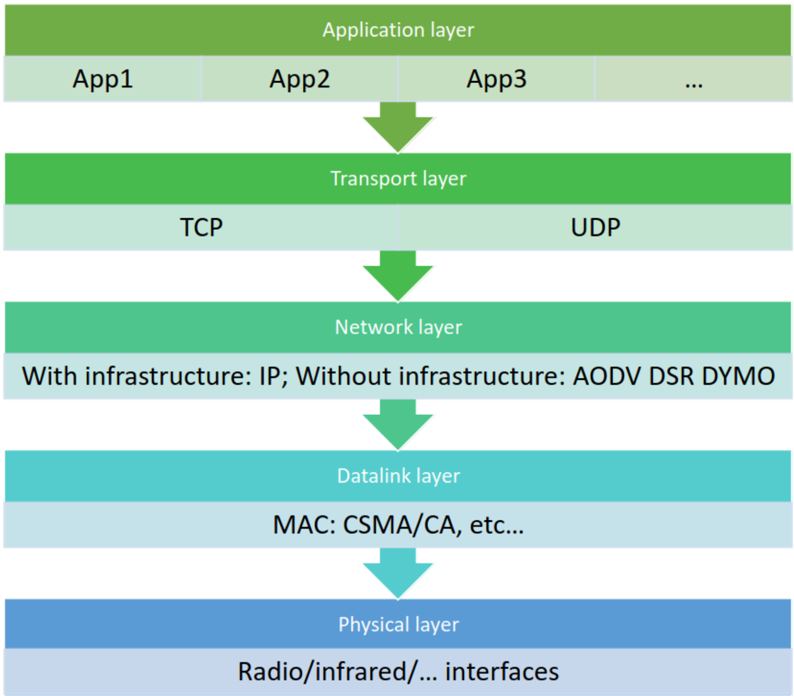


Figure 2.1: Protocol stack

better understand this point, look at the following figure, consider that at the sender, the signal strength of its own transmission (self-signal) would be too strong to detect a collision by another transmitter, making collisions happen at the receiver.

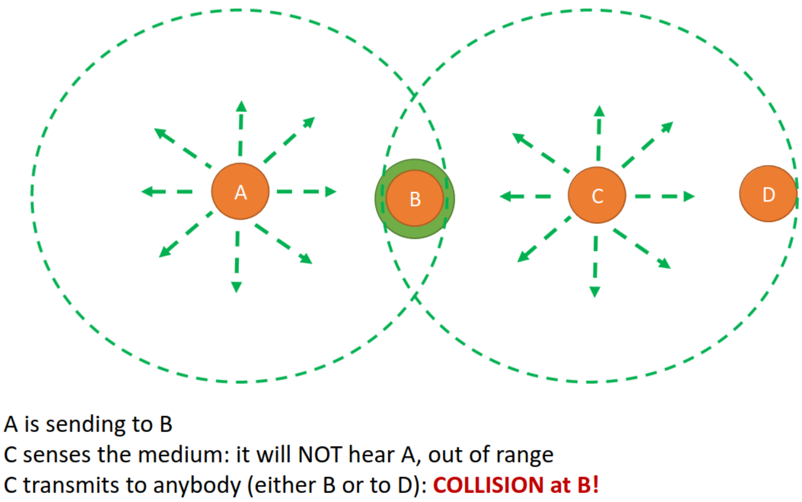


Figure 2.2: **Hidden Terminal** problem
Two or more stations which are out of range of each other transmit simultaneously to a common recipient

2.1.2 MACA

MACA stands for *Multiple Access with Collision Avoidance*

1. stimulate the receiver into transmitting a short frame first
2. then transmit a (long) data frame
3. stations hearing the short frame refrain from transmitting during the transmission of the subsequent data frame

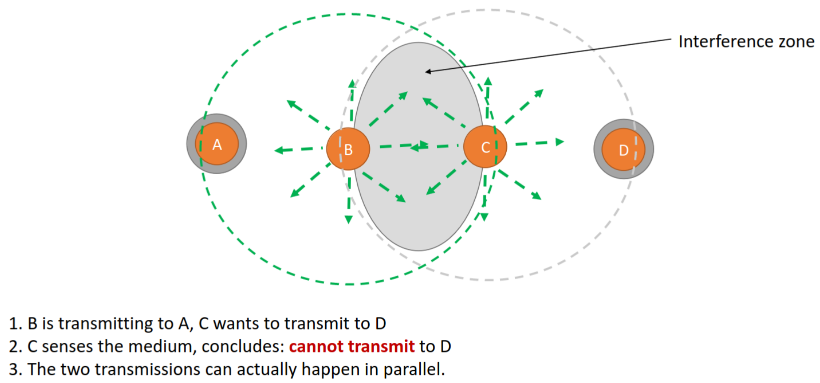


Figure 2.3: **Exposed Terminal** problem
A transmitting station is prevented from sending frames due to interference with another transmitting station

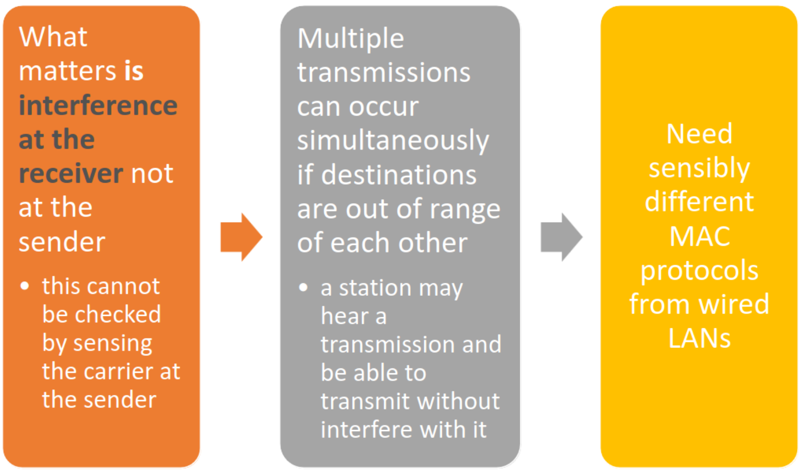


Figure 2.4: MACA Motivations