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.

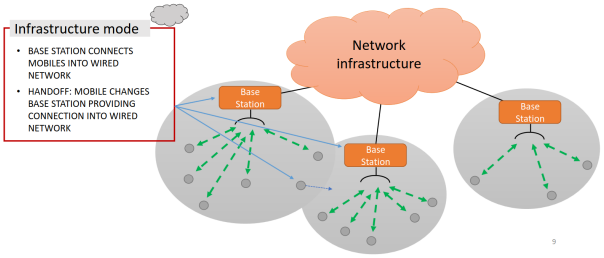
Chapter 2

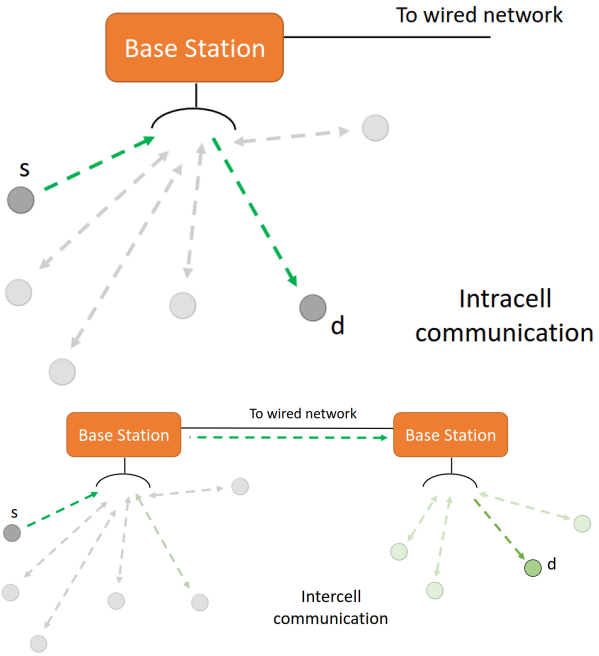
Wireless Networks

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

Recall that *wireless* $\neq$ *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 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.

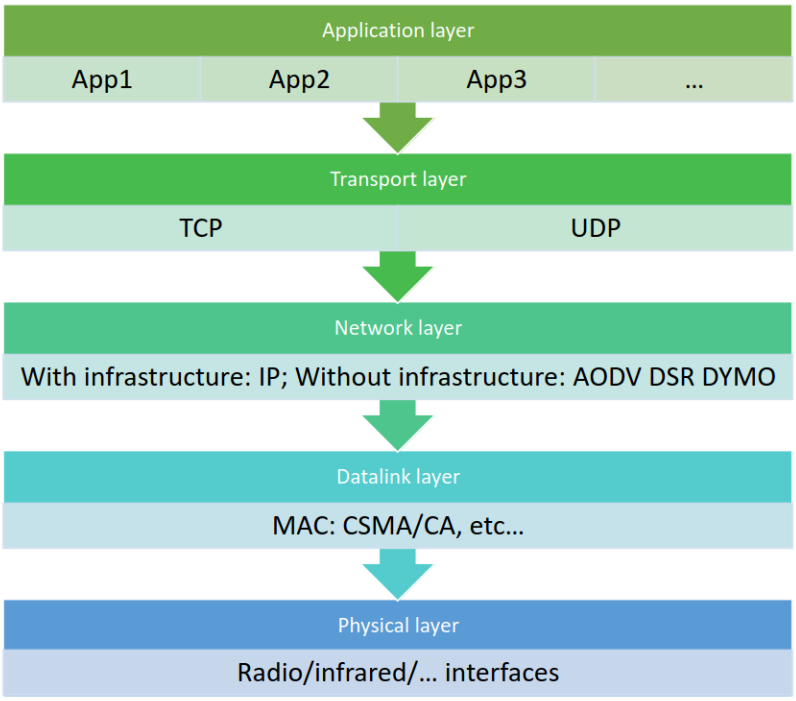
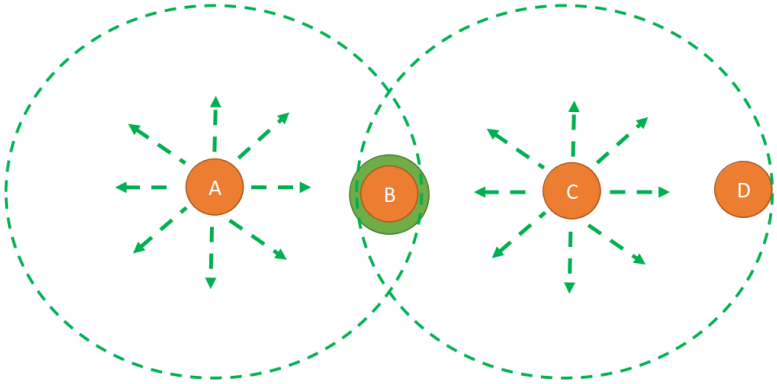
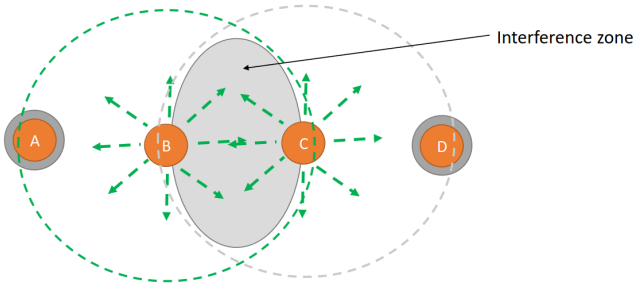


Figure 2.1: Protocol stack



A is sending to B
C senses the medium: it will NOT hear A, out of range
C transmits to anybody (either B or to D): **COLLISION at B!**

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



1. B is transmitting to A, C wants to transmit to D
2. C senses the medium, concludes: **cannot transmit** to D
3. The two transmissions can actually happen in parallel.

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

2.1.2 MACA

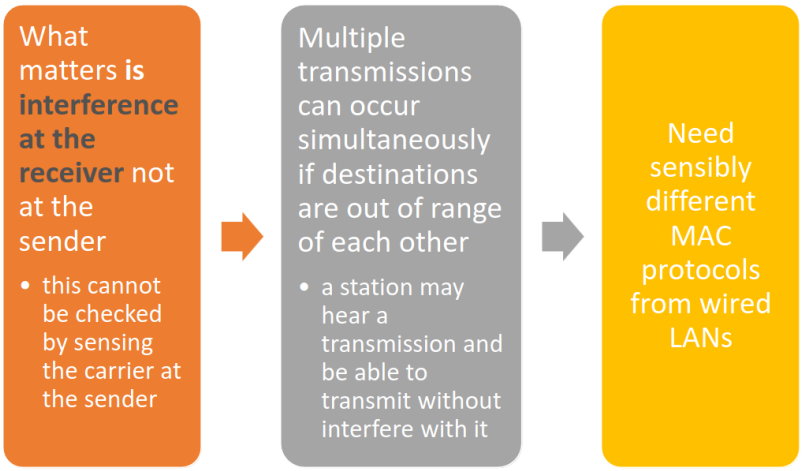


Figure 2.4: MACA Motivations

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