Mobile and Cyber-Physical Systems

Introduction

Network mobility history starts in the 80s with the first generation technology where a voice signal could be delivered using a circuit switched analog system. Circuit switching is a method to enable two nodes to communicate with each over a dedicated physical link is reserved in the network.

Since 2.5G the circuit switched communication is complemented by a packet switched one for data transmission while, at least in the older generations, the voice signal was still transmitted via circuit switching.

As seen in figure 1 the 5G technology provides an improvement of different orders of magnitude in respect to the existing standards. Still it is reductive to refer to 5G just as an improvement in respect to previous technologies: the softwarization of the network functions and the enlargement of the frequency bands are a radical change in communication science.

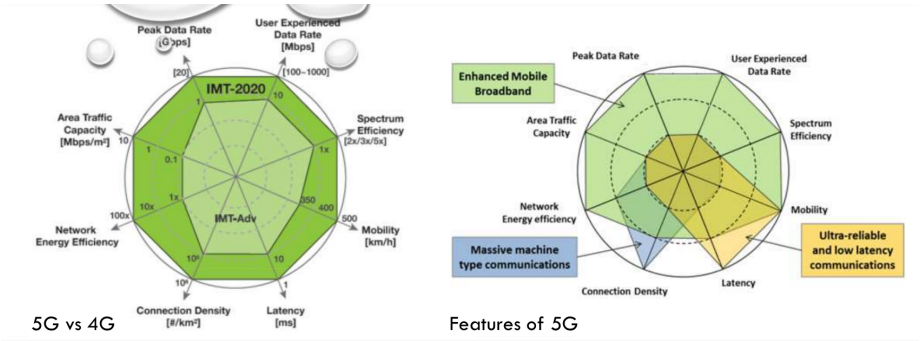

Figure 1: 5G feature comparison

MANETS

With the acronym MANETS, for Mobile ad-hoc networks, we refer to a decentralized type of wireless network. In a MANET the nodes are autonomous and independent, also since their mobile and dynamic behaviour they have to

be battery powered and able to communicate by exchanging packets via radio waves.

Originally the MANET approach was thought as a replacement for the first and second generation technologies of over twenty years ago. By now the applications are limited, but given its robustness and the rapid deploying they are now essential to very specific use cases like emergency management, or communication in remote or hostile environments.

The absence of a fixed network infrastructure is dealt by the nodes via cooperation in a peer-to-peer fashion, this realizes a pure distributed system able to be reconfigured on the fly. A fundamental concept in a MANET is the relation of neighborhood between nodes that share the same physical layer. Given the indefiniteness of radio waves boundaries a non trivial Media Access Control (MAC) protocol is required, leading to an high bit error rate.

In IP networks the address is strictly correlated to the position of the device, even in mobile connectivity the range is given by a fixed router. This does not hold for MANETS where frequent link failures and disconnections change arbitrarily the network topology, this implies the need for a dynamic multi-hop routing protocol where each node is a router.

Over the datalink and network layers, that are as we described different from the known IP stack, the usual transport layers protocols (TCP, UDP) are usable, providing a transparent implementation for the users.

Wireless Sensor Networks

The sensors are devices used to monitor an environment and gather informations. Conventionally they are thought to be simple transducers connect by a cable to a centralized control device.

Wireless sensors are instead smart and autonomous battery powered devices, that must handle the wireless communication logic. The need for a limited but unavoidable computational power can also be used to pre-process data and build a network when the communication is not limited to the sensor-controller channel.

The distribution of the devices and their peer-to-peer behaviour resembles the ad-hoc networks, but there are some fundamental differences that justify the separation of the two concepts. First of all the sensors of a WSN can be in number several orders of magnitude more than the nodes in a MANET, also the devices are strongly constrained in power, computational capacities and memory, so they're not general purpose but instead tightly integrated with their task.

The range of possible applications for WSN is wide and comprises different domains, it is interesting to deepen the user localization task to compare WSN to other simpler and cheaper technologies like barcodes and RFIDs. Both of them delegate the greatest part of the complexity to the reader and to obtain

informations the user have to activate them at a very short distance. While a barcode only carries a static information, RFIDs can be connected to little chemical sensors to provide dynamic information.

The greatest advantage of wireless sensors is the absence of user intervention. In the context of user localization we could think of a WSN that periodically sends signals from all of its sensors, then the receiver on the user can infer its position by interpolating the signal directions and strengths.

IOT

There are many definitions of IOT, choose one! The "things" are devices that are in some way related to electronics, software, sensors and network connectivity.

Currently the number of computer per person is rising up, surpassing in 2008 the number of living people in the world, with most of the devices that are not directly in use by human beings. It is reasonable to state that the IOT technology was born during the transition from IPv4 and IPv6, where the huge number of possible devices interconnected reasonably freed humanity from preparing for another painful transition and simplified the strategies to assign addresses.

There is a strict correlation between sensors and cloud, as of today the computation of the produced data is delegated to external data centers making intense use of technologies like NO-SQL databases that are more flexible and prone to horizontal scaling.

The usual path of the information goes from the sensor to the cloud using a gateway, and to actuators from the cloud always using a gateway. This multi-hop procedure can grow expensive in latency and other time measurements, leading to faults and inefficiencies when the relationship between sensors and actuators has real-time constraints.

The problem of this approach are even more evident in context where the sensors and the actuators are in the same environment, under the same gateway. In this scenario it is certainly a better choice to create a closed loop between sensors and actuator, by moving part of the logic to the devices. Of course this adaptation has costs and can be computational expensive to locally gather and process information from multiple sensors, given that in most cases the valuable informations are given by the WSN entirety and not by each single sensor. Despite of this many times this quasi-optimal technical solution is not implemented because of business constraints about the retain of user data in private cloud solutions to enforce vendor lock-in.