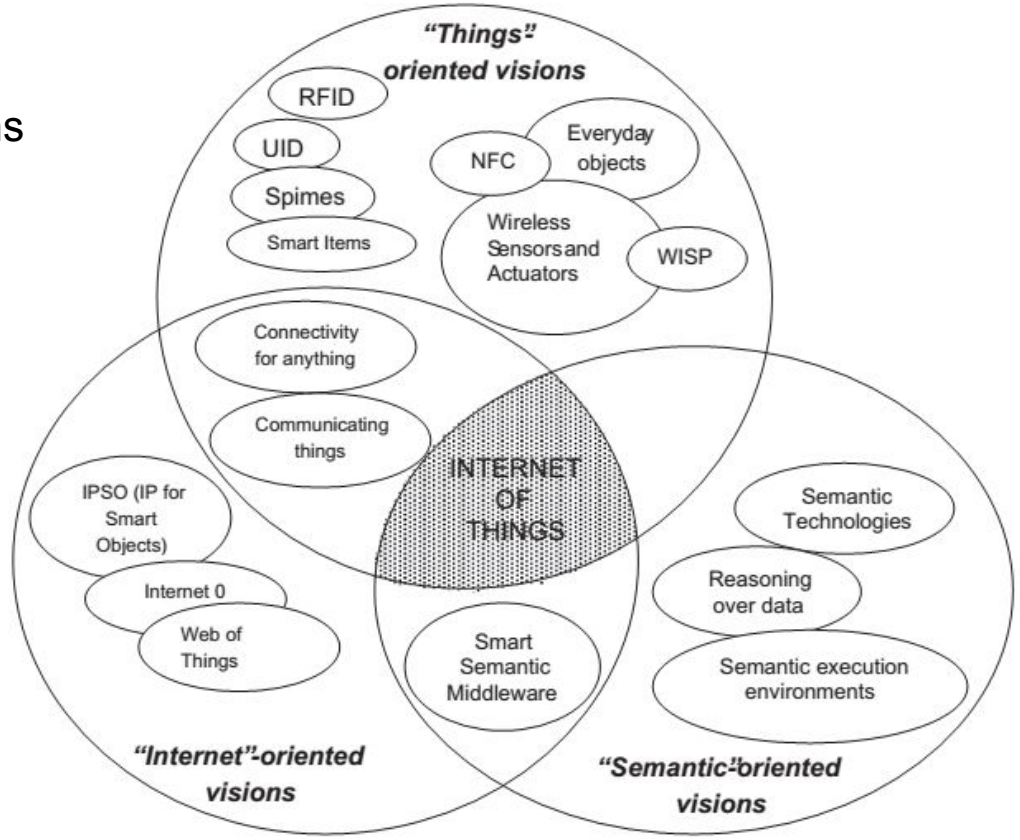
Internet of Things

Internet of Things

•Different Visions

- "Things" - oriented visions
- "Internet" - oriented visions
- "Semantic" - oriented visions



KEY:Enabling Technologies

•Identification , sensing and communication technologies

- RFID system

conposed of one or more reader(s) and several RFID tags.

- Sensor network

consist of a certain number (which can be very high) of sensing nodes communicating in a wireless multi-hop fashion.

- Sensing RFID system(RFID snesor network)

consist of small,RFID-based sensing and computing devices,and RFID readers,which are the sinks of the data generated by the sensing RFID tags and provide the power for the network operation.

Comparison between RFID systems, wireless sensor networks, and RFID sensor networks.

	Processing	Sensing	Communication	Range (m)	Power	Lifetime	Size	Standard
RFID	No	No	Asymmetric	10	Harvested	Indefinite	Very small	ISO18000
WSN	Yes	Yes	Peer-to-peer	100	Battery	<3 years	Small	IEEE 802.15.4
RSN	Yes	Yes	Asymmetric	3	Harvested	Indefinite	Small	None

KEY:Enabling Technologies

- Middleware

  - Application

  - Service composition

    On this layer there is no notion of devices and the only visible assets are services.

  - Service management

    This layer provides the main functions that are expected to be available for each object and that allow for their management in the IoT scenario.

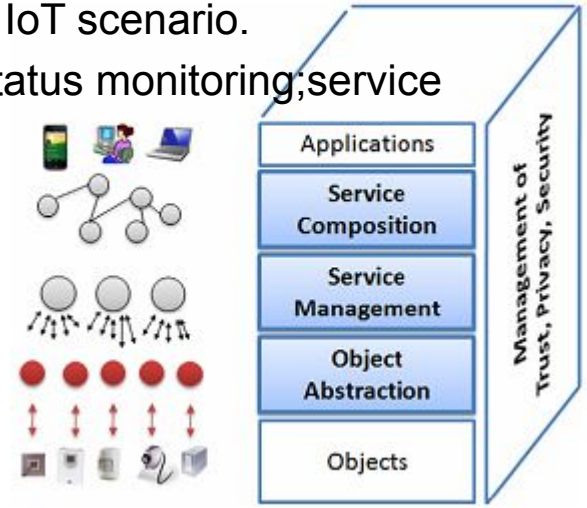
    basic set of services:object dynamic discovery;status monitoring;service configuration;

  - Object abstraction

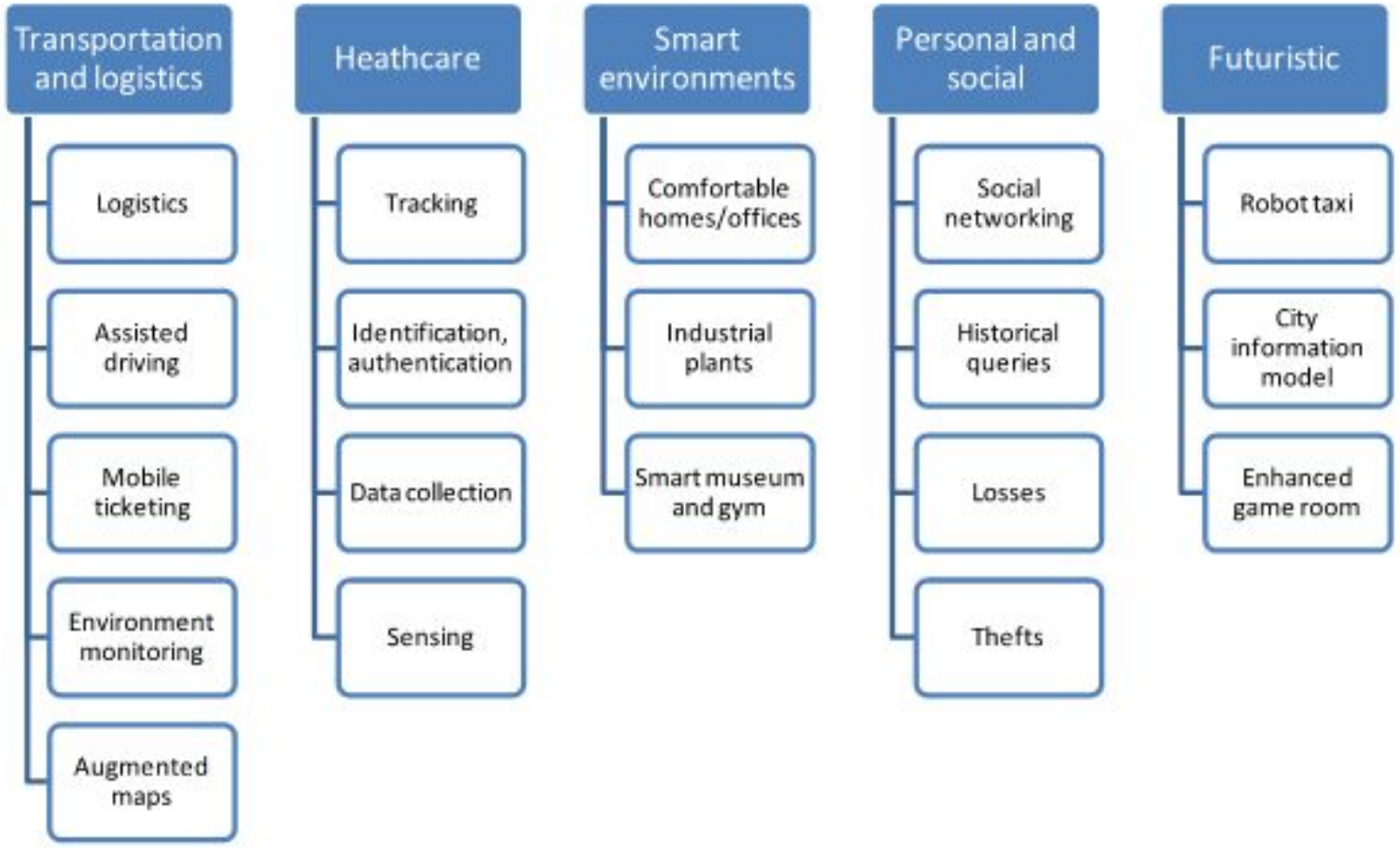
    - interface sub-layers

    - communication sub-layers

  - Trust,privacy and security management



Applications



Open Issues

- Standardization activity
  - EPCglobal
    - Electronic Product Code(EPC)
  - M2M
    - Machine-to-Machine
  - NFC
    - Near Field Communication
  - Wireless Hart
  - ZigBee
- Addressing and networking issues
- Security and Privacy
  - Security
  - Privacy

M2M networks

- **Machine-to-machine(M2M)**

  M2M communications enable direct connectivity among devices,which can be organized as a network in order to exchange information and perform actions without human intervention.

- **Requirements and properties**

  - low costs
  - low energy consumption

    M2M devices can be deployed at locations without main power and operate only on battery power.

  - wide coverage

    numerous M2M devices are widely distributed in a wide variety of locations,some of which are difficult to reach either because they are underground or located deep inside buildings.

  - tolerable-low latency
  - relatively low data throughput
  - etc.

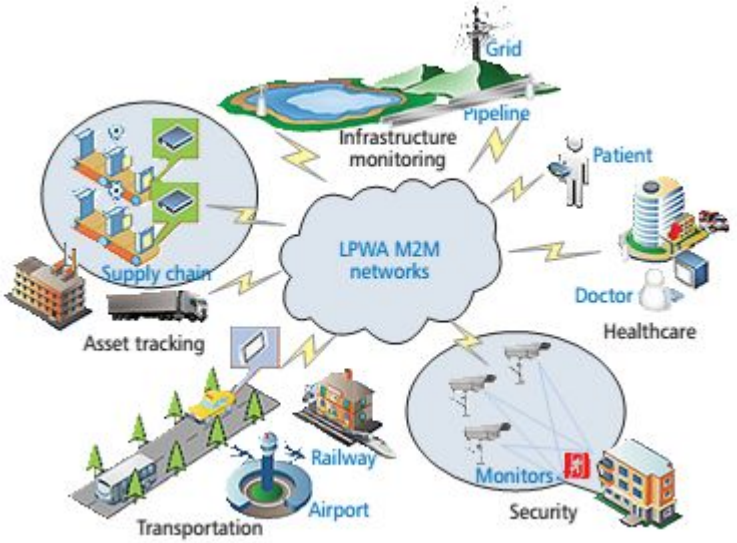
Key：LPWA

- LPWA(low power wide area)

  LPWA has been specifically designed with the objectives of low energy consumption and wide coverage.

- Application scenarios

  - Infrastructure Monitoring
  - Transportation
  - Asset Tracking
  - Security
  - Healthcare



Requirements of LPWA M2M Applications

Application category	Typical user case	Coverage	Power consumption	Data traffic	Periodicity	Mobility	Real-time requirement	Security/reliability requirement
Infrastructure monitoring	Water/Electric/Gas meter	Urban areas	Low	Medium	Tens of minutes	No	Medium	Low
	Agriculture/soil & oil/gas pipeline monitoring	Open fields	Low	Low	Event driven	No	Low	Medium
Transportation	Traffic congestion monitoring	Urban areas	Low	High	Tens of minutes	High	Medium	Low
	Public transport management	Urban areas	Low	Medium	Event driven	High	Medium	Medium
Asset tracking	Supply chain monitoring	Urban areas/ in-building	Low	Low	Event driven	Medium	Low	Low
	Vehicle tracking	Urban areas/ open fields	Low	High	Several minutes	High	Medium	Low
Security	Access control & building security systems	In-building	Low	Low	Event driven	No	High	High
	Natural disasters preparedness	Urban areas/ open fields	Low	Low	Event driven	No	High	Medium
Healthcare	Health status monitoring	Urban areas/ in-building	Low	Medium	Tens of minutes	Medium	Low	Low
	Medical alert	Urban areas/ in-building	Low	Low	Event driven	Medium	High	Low

Key Technology

•PHY Techniques

- UNB modulation (ultra-narrowband modulation)
- DSSS (direct sequence spread spectrum modulation)

•MAC Techniques

- Star Topology

The feature of LPWA M2M network are greatly different from those of WSNs and the main concerns for the LPWA system when selecting a proper topology are the low costs and energy consumption.The star topology with only a single hop is considered to be the best choice for LPWA M2M network.

- Channel Access

There are two main categories of channel access methods for sharing access to the wireless medium:reservation-based/contention-based access.

Early Standards

•IEEE 802.15.4k

- aims to low energy critical intrastructure monitoring networking,to facilitate point-to-point communications for monitoring and managing critical infrastructure applications.

- Two PHY modes are specified to support LECIM application.

•Weightless

- The Weightless specifications define not only the PHY and MAC layer,but also an upper layer , dubbed the server layer.

- A basic transmitter block diagram of PHY is depicted in the following picture.

- 3GPP,IETF,and so on

The IEEE 802.15.4k and Weightless standards have different attributes and also share some common features. To elaborate, a detailed comparison between IEEE 802.15.4k and Weightless is summarized in next table .

Early S

	Attribute	IEEE 802.15.4k (DSSS)	Weightless
PHY	Operation frequency band	470 ~ 510 MHz; 779 ~ 787 MHz; 863 ~ 870 MHz; 902 ~ 928 MHz; 915 ~ 928 MHz; 917.1 ~ 923.5 MHz; 920 ~ 928 MHz; 921 ~ 928 MHz and 2.4 ~ 2.4835 GHz in different counties	470 ~ 790 MHz in Europe; 470 ~ 698 MHz in U.S.
	Channel bandwidth	100 kHz; 200 kHz; 400 kHz; 600 kHz; 800 kHz and 1 MHz	8 MHz in Europe; 6 MHz in U.S.
	Effective isotropic radiated power (EIRP)	Minimum: – 3 dBm; Maximum: limited by local regulatory bodies	4 ~ 32 dBm
	FEC	Convolutional encoding: rate 1/2, constraint length 7	Convolutional encoding: rate 3/4 or 1/2, constraint length 7
	Interleaving	Pruned bit reversal interleaving algorithm	Matrix interleaving with 8 columns
	Spreading sequence	Gold code: SF 16 ~ 32768	Gold code and Kasami code: SF 15 ~ 1023
	Modulation	BPSK; OQPSK	16-QAM; pi/4-QPSK; pi/2-BPSK; pi/4-DQPSK; pi/2-DBPSK
	Frequency hopping	No	Yes
	Minimum receiver sensitivity threshold	– 148 dBm	Downlink: – 128 dBm; Uplink: – 140 dBm
	Typical coverage	Up to 20 km in LoS and 5 km in NLoS	Up to 10 km
	Data rate	0.00153 ~ 125 kb/s	Downlink: 0.0025 ~ 16.0 Mb/s; Uplink: 0.00025 ~ 0.5 Mb/s
	Sync sequence length	Preamble: 0/2/4 octets; SFD: 0/1 octets	8 ~ 2048 Symbol (No need to multiply by spreading sequence any more)
MAC	Packet length	16/24/32 octets	0 ~ 255 octets
	Topology structure	Star	Star, with multi-hop relay capability
	Channel access method	CSMA/CA; CSMA/CA with PCA; Aloha with PCA	TDMA/FDMA
	Traffic priority	Yes	Yes

Open Issues

- Standardization activity
- Addressing and networking issues
  - Addressing issues
  - Networking issues
- Security and Privacy

Addressing and networking issues

- Addressing issues
  - The IoT will include an incredibly high number of nodes, each of which will produce content that should be retrievable by any authorized user regardless of her/his position. This requires effective addressing policies. Currently, the IPv4 protocol identifies each node through a 4-byte address. It is well known that the number of available IPv4 addresses is decreasing rapidly and will soon reach zero.
  - IPv6 addresses are expressed by means of 128 bits and therefore, it is possible to define 1038 addresses, which should be enough to identify any object which is worth to be addressed. Accordingly, we may think to assign an IPv6 address to all the things included in the network.
- Networking issues

Addressing and networking issues

- Addressing issues
- Networking issues
  - Naming
    - Object Name Servers (ONS), like DNS, are needed to map a reference to a description of a specific object and the related identifier, and vice versa
  - Transport protocol
    - Existing transport protocols fail in the IoT scenarios since their connection setup and congestion control mechanisms may be useless; furthermore, they require excessive buffering to be implemented in objects
  - Traffic characterization and QoS support
    - The IoT will generate data traffic with patterns that are expected to be significantly different from those observed in the current Internet. Accordingly, it will also be necessary to define new QoS requirements and support schemes

Open Issues

- Standardization activity
- Addressing and networking issues
- Security and Privacy
  - Security
  - Privacy

Security and Privacy

- Security
  - the major problems related to security concern authentication and data integrity.
  - authentication
    - Authentication is difficult as it usually requires appropriate authentication infrastructures and servers that achieve their goal through the exchange of appropriate messages with other nodes. In the IoT such approaches are not feasible given that passive RFID tags cannot exchange too many messages with the authentication servers. The same reasoning applies (in a less restrictive way) to the sensor nodes as well.
  - data integrity
    - Data integrity solutions should guarantee that an adversary cannot modify data in the transaction without the system detecting the change. The problem of data integrity has been extensively studied in all traditional computing and communication systems and some preliminary results exist for sensor networks. However, new problems arise when RFID systems are integrated in the Internet as they spend most of the time unattended.
- Privacy

Security and Privacy

- Security
- Privacy
  - privacy should be protected by ensuring that individuals can control which of their personal data is being collected, who is collecting such data, and when this is happening.
  - the personal data collected should be used only in the aim of supporting authorized services by authorized service providers.
  - the above data should be stored only until it is strictly needed.