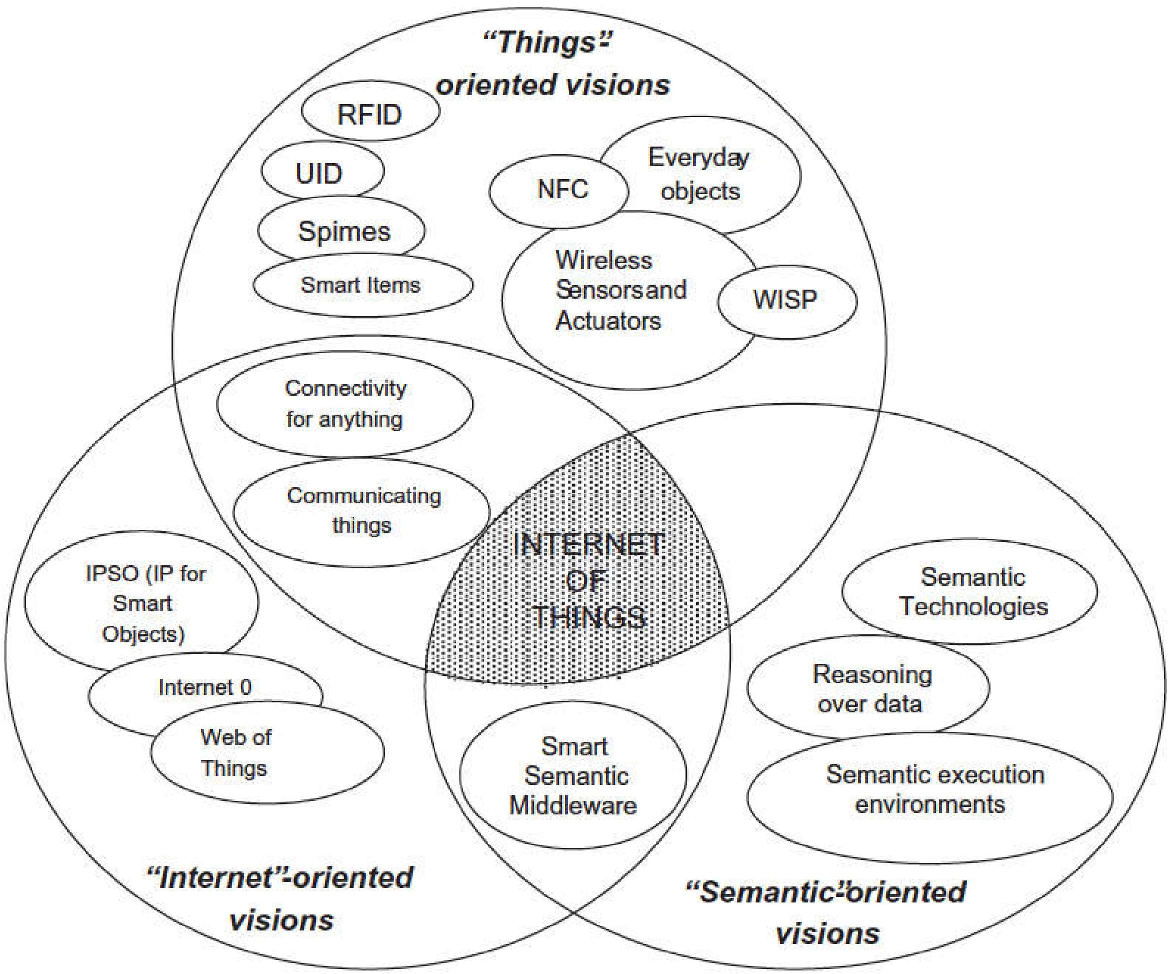
Outline

- Introduction to IoT
- Enabling technologies
- Open problems and future challenges
- Applications

What is IoT?

- A phenomenon which connects a variety of ***things***
  - Everything that has the ability to communicate

Connection of Multiple Visions



Source: Atzori et al. 2010

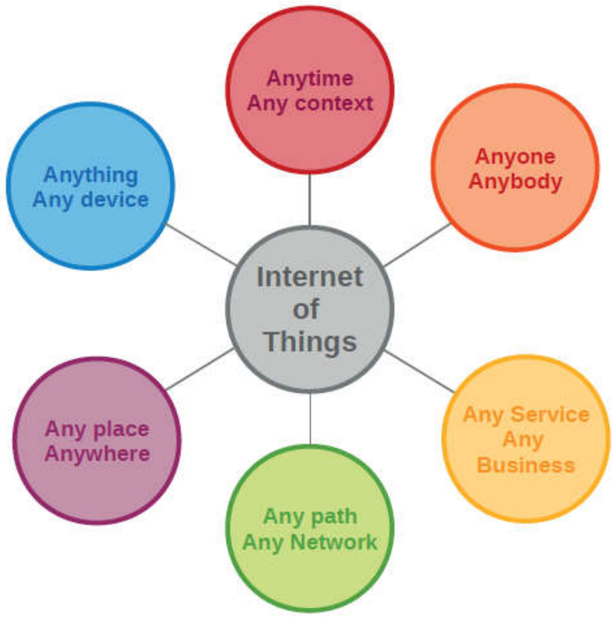
IoT Definitions

- The Internet of Things, also called The Internet of Objects, refers to a wireless network between objects, usually the network will be wireless and self-configuring, such as household appliances. **(Wikipedia)**

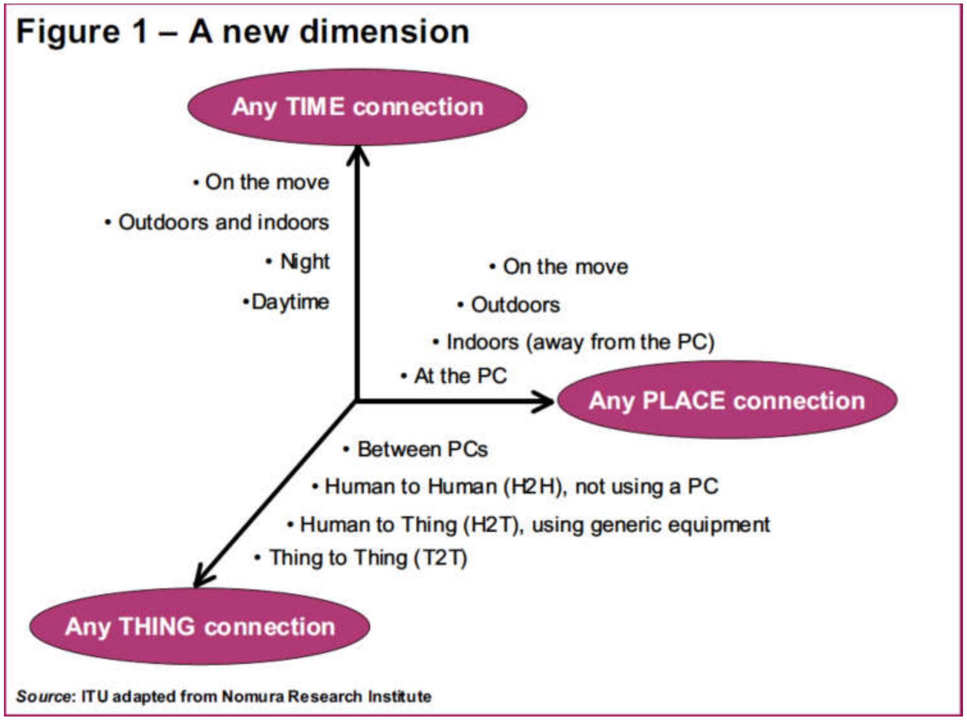
- The term "Internet of Things" has come to describe a number of technologies and research disciplines that enable the Internet to reach out into the real world of physical objects. **(IoT 2008)**

- “Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts”. **(IoT in 2020)**

Any-X Point of View



Source: Perera et al. 2014

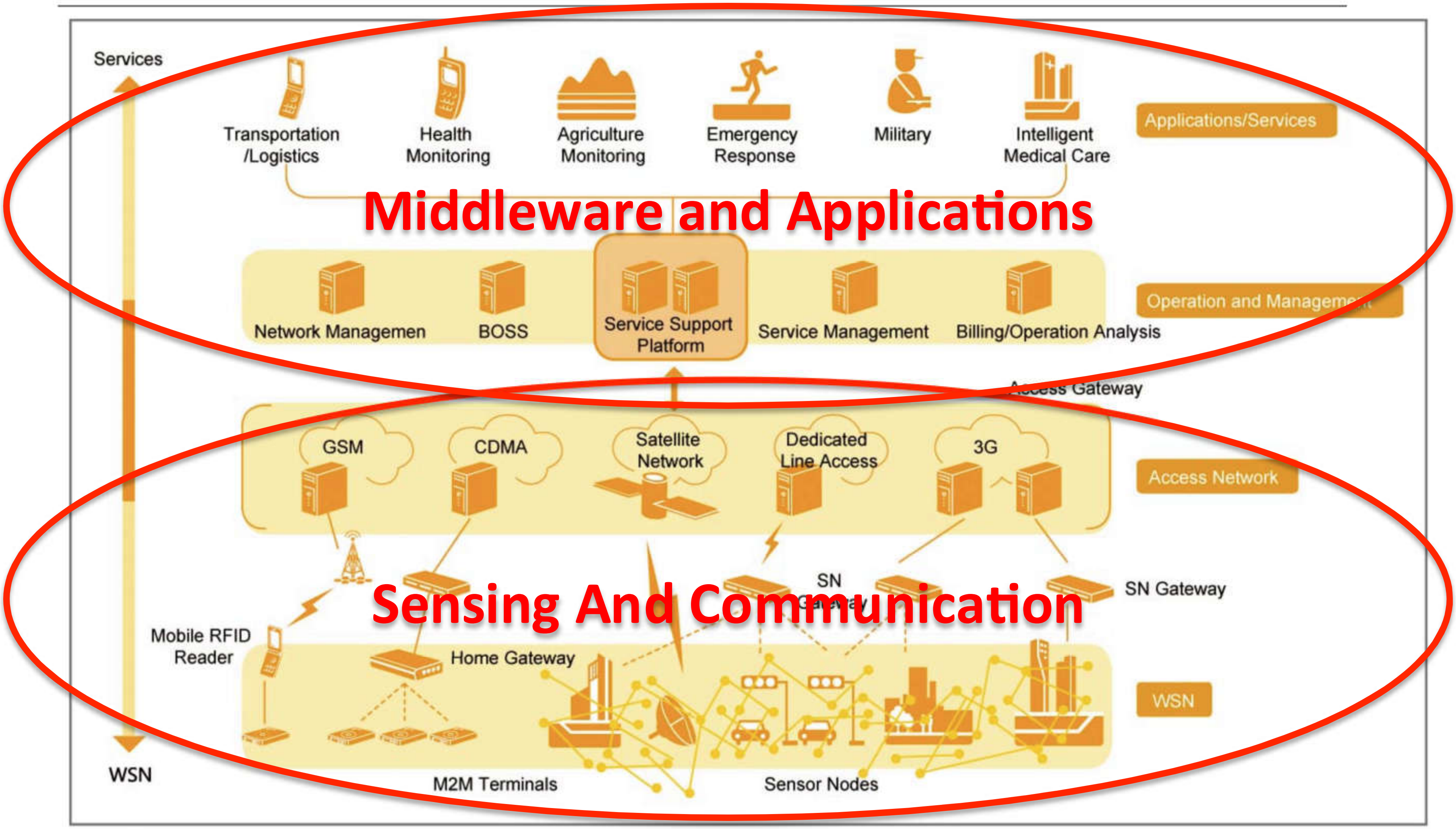


- The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/ network and Any service.

Characteristics of IoT

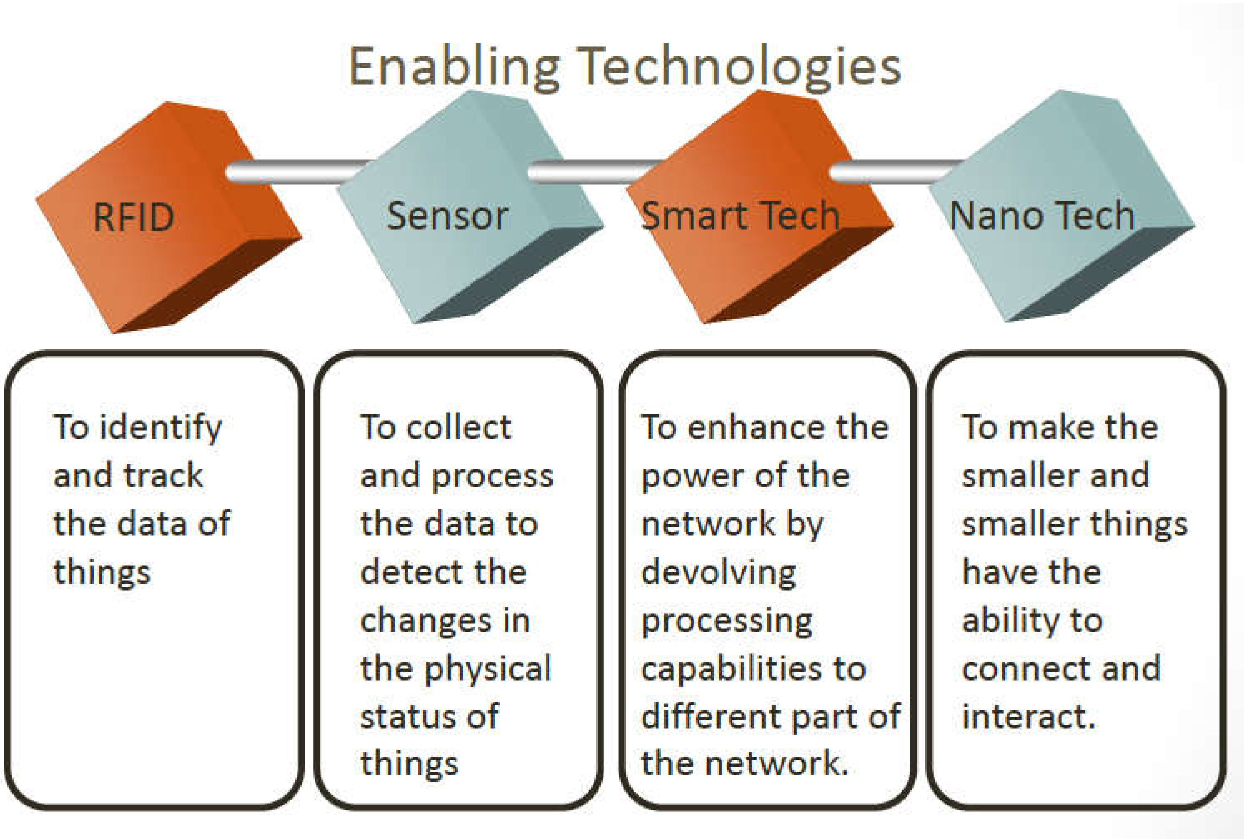
1. Intelligence
   – Knowledge extraction from the generated data
2. Architecture
   – A hybrid architecture supporting many others
3. Complex system
   – A diverse set of dynamically changing objects
4. Size considerations
   – Scalability
5. Time considerations
   – Billions of parallel and simultaneous events
6. Space considerations
   – Localization
7. Everything-as-a-service
   – Consuming resources as a service

IoT Layered Architecture



Source: ZTE

Networking and Communication

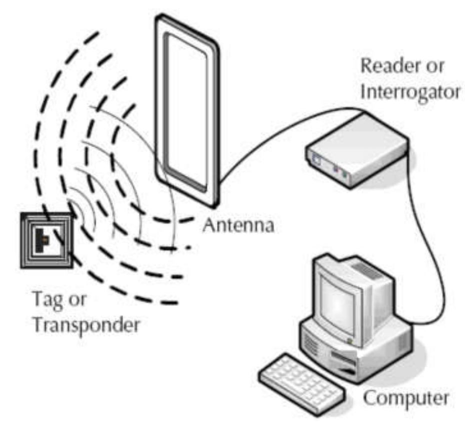


- RFID to smallest enabling technologies, such as chips, etc.

Source: Qian Zhang. Lecture notes. 2013

RFIDs

- The reduction in terms of size, weight, energy consumption, and cost of the radio takes us to a new era
  - This allows us to integrate radios in almost all objects and thus, to add the world "anything" to the above vision which leads to the IoT concept
- Composed of one or more readers and tags
- RFID tag is a small microchip attached to an antenna
- Can be seen as one of the main, smallest components of IoT, that collects data



Wireless Technologies

- Telecommunication systems
  - Initial/primary service: mobile voice telephony
  - Large coverage per access point (100s of meters – 10s of kilometers)
  - Low/moderate data rate (10s of kbit/s – 10s of Mbits/s)
  - Examples: GSM, UMTS, LTE
- WLAN
  - Initial service: Wireless Ethernet extension
  - Moderate coverage per access point (10s – 100s meters)
  - Moderate/high data rate (Mbits/s – 100s)
  - Examples: IEEE 802.11(a-g), Wimax

Source: Geert Heijenk. Mobile and Wireless Networking. Lecture Notes. 2014

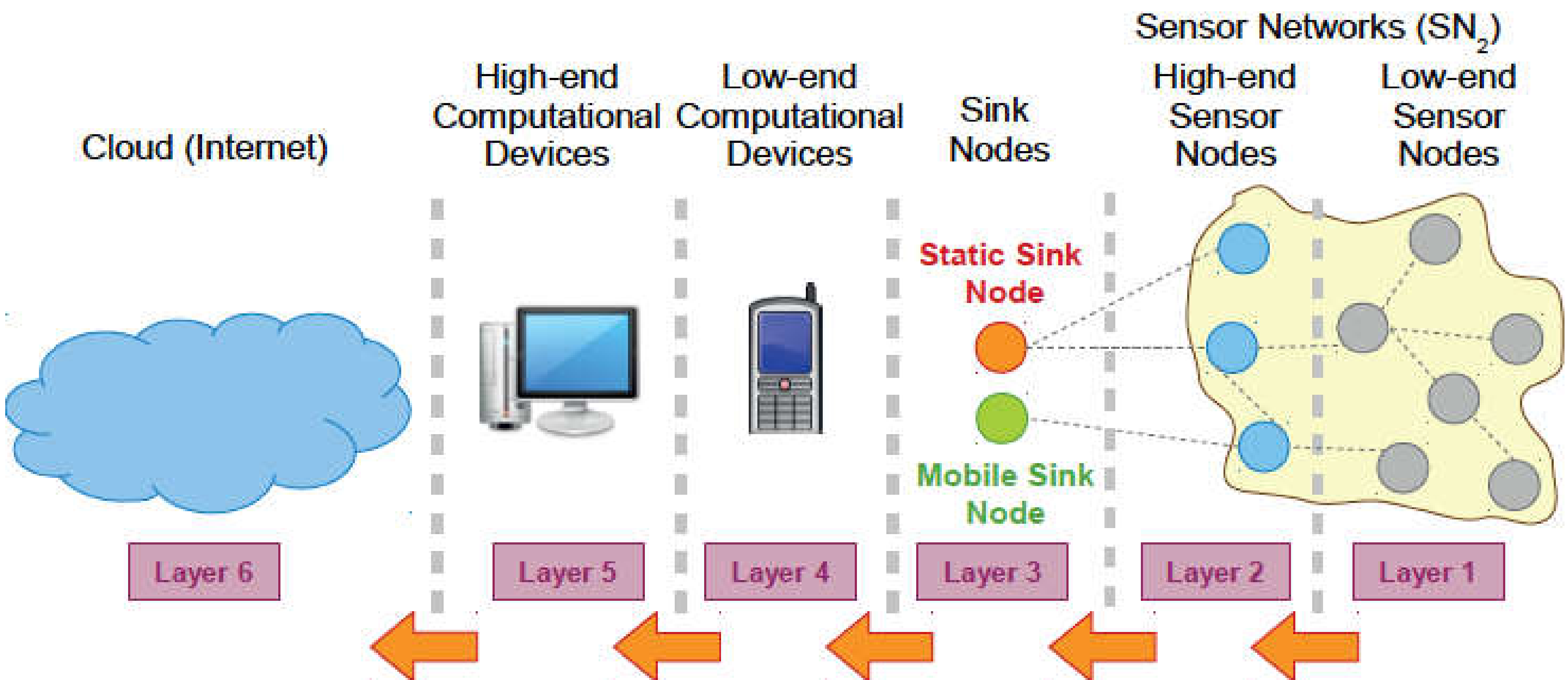
Wireless Technologies

- Short range:
  - Direct connection between devices – sensor networks
  - Typical low power usage
  - Examples: Bluetooth, Zigbee, Z-wave (house products)
- Other examples:
  - Satellite systems
    - Global coverage
    - Applications: audio/TV broadcast, positioning, personal communications
  - Broadcast systems
    - Satellite/terrestrial
    - Support for high speed mobiles
  - Fixed wireless access
    - Several technologies including DECT, WLAN, IEEE802.16, etc.

Source: Geert Heijenk. Mobile and Wireless Networking. Lecture Notes. 2014

Sensor Networks (SNs)

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



Source: Perera et al. 2014

Sensor Networks (SNs)

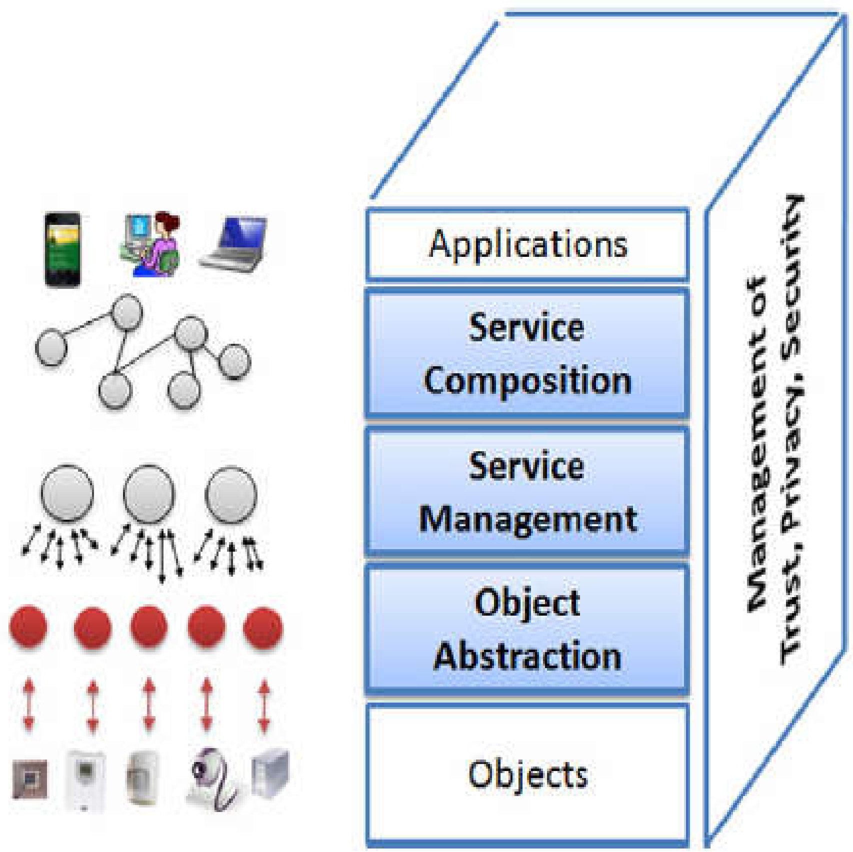
- SNs generally exist without IoT but IoT cannot exist without SNs
- SNs have been designed, developed, and used for specific application purposes
  – Environmental monitoring, agriculture, medical care, event detection etc.
- For IoT purposes, SNs need to have a middleware addressing these issues:
  – Abstraction support, data fusion, resource constraints, dynamic topology, application knowledge, programming paradigm, adaptability, scalability, security, and QoS support

Middleware

- *Middleware is a software layer that stands between the networked operating system and the application and provides well known reusable solutions to frequently encountered problems like heterogeneity, interoperability, security, dependability [Issarny, 2008]*

- IoT requires stable and scalable middleware solutions to process the data coming from the networking layers

Service Oriented Architecture (SOA)



Source: Atzori et al. 2010

- Middleware solutions for IoT usually follow SOA approaches
- Allows SW/HW reuse
  - Doesn't impose specific technology
- A layered system model addressing previous issues
  - Abstraction, common services, composition

Other Middleware Examples

- Fosstrak Project
  - Data dissemination/aggregation/filtering/interpretation
  - Fault and configuration management, lookup and directory service, tag ID management, privacy
- Welbourne et al.
  - Tag an object/create-edit location info/combine events collected by antennas
- e-Sense Project
  - Middleware only collects data in a distributed fashion and transmits to actuators
- UbiSec&Sens Project
  - Focuses on security → secure data collection, data store in memory, etc.

Open Problems and Challenges

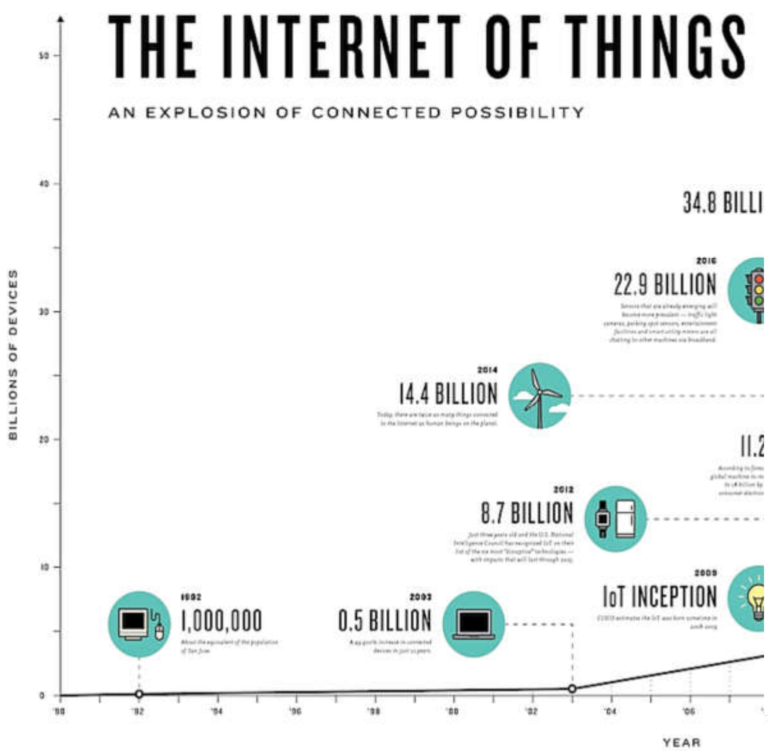
- Lack of standardization
- Scalability
  - Addressing issues
  - Understanding the big data
- Support for mobility
- Address acquisition
- New network traffic patterns to handle
- Security/Privacy issues

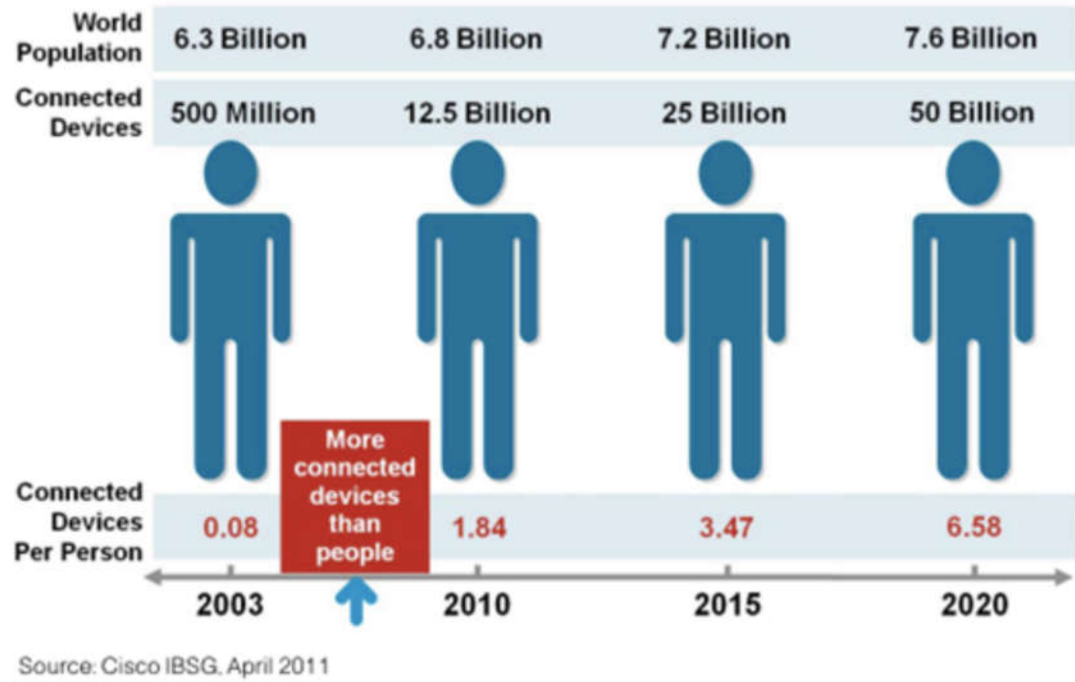
Standardization

- Several standardization efforts but not integrated in a comprehensive framework
- Open Interconnect Consortium: Atmell, Dell, Intel, Samsung and Wind River
- Industrial Internet Consortium: Intel, Cisco, GE, IBM
- AllSeen Alliance: Led by Qualcomm, many others

Standard	Objective	Status	Comm. range (m)	Data rate (kbps)	Unitary cost ($)
Standardization activities discussed in this section					
EPCglobal	Integration of RFID technology into the electronic product code (EPC) framework, which allows for sharing of information related to products	Advanced	~1	~10^2	~0.01
GRIFS	European Coordinated Action aimed at defining RFID standards supporting the transition from localized RFID applications to the *Internet of Things*	Ongoing	~1	~10^2	~0.01
M2M	Definition of cost-effective solutions for machine-to-machine (M2M) communications, which should allow the related market to take off	Ongoing	N.S.	N.S.	N.S.
6LoWPAN	Integration of low-power IEEE 802.15.4 devices into IPv6 networks	Ongoing	10–100	~10^2	~1
ROLL	Definition of routing protocols for heterogeneous low-power and lossy networks	Ongoing	N.S.	N.S.	N.S.
Other relevant standardization activities					
NFC	Definition of a set of protocols for low range and bidirectional communications	Advanced	~10^{-2}	Up to 424	~0.1
Wireless Hart	Definition of protocols for self-organizing, self-healing and mesh architectures over IEEE 802.15.4 devices	Advanced	10–100	~10^2	~1
ZigBee	Enabling reliable, cost-effective, low-power, wirelessly networked, monitoring and control products	Advanced	10–100	~10^2	~1

Scalability

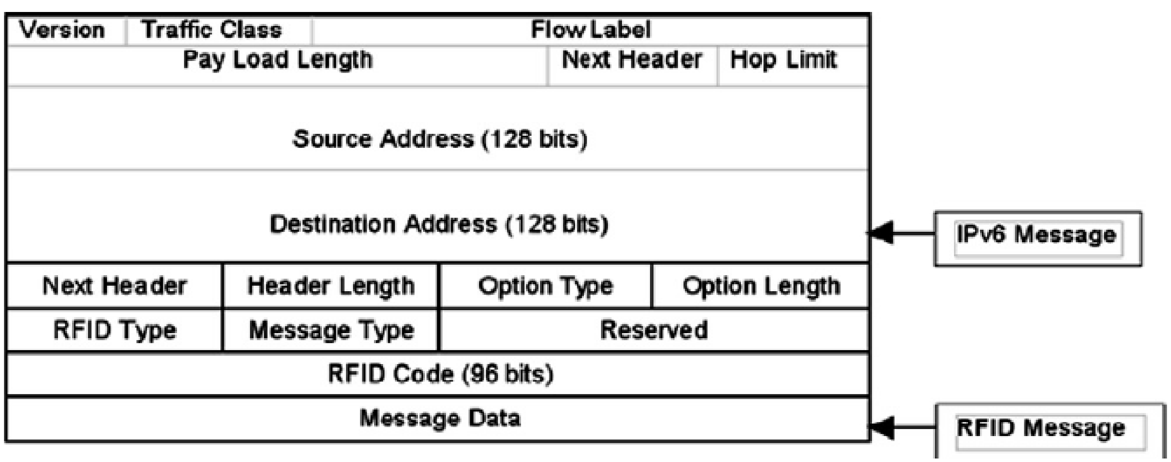




- Number of devices increasing exponentially
  - How can they uniquely be tagged/named?
  - How can the data generated by these devices be managed?

Addressing Issues

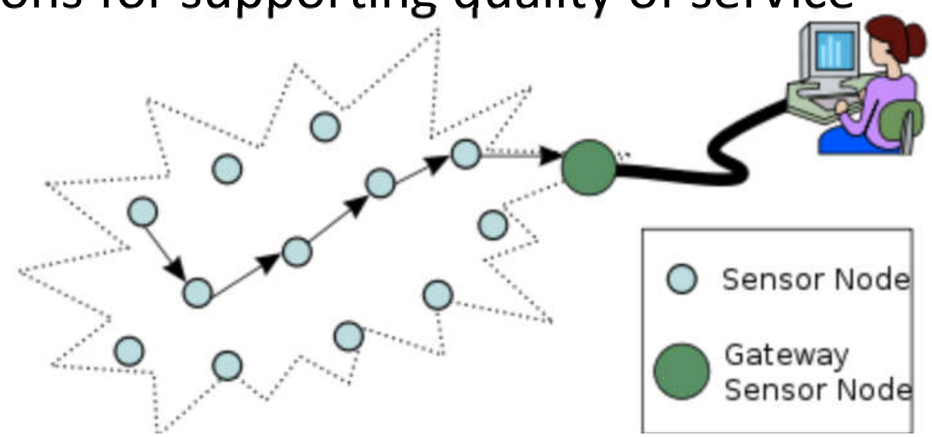
- Incredibly high number of nodes, each of which will produce content that should be retrievable by any authorized user
  - This requires effective addressing policies
  - IPv4 protocol may already reached its limit. Alternatives?
  - IPv6 addressing has been proposed for low-power wireless communication nodes within the 6LoWPAN context
- IPv6 addresses are expressed by means of 128 bits →1038 addresses, enough to identify objects worth to be addressed
- RFID tags use 64–96 bit identifiers, as standardized by EPCglobal, solutions to enable the addressing of RFID tags into IPv6 networks



Encapsulation of RFID message into an IPv6 packet.
Source: Atzori et al. (2010)

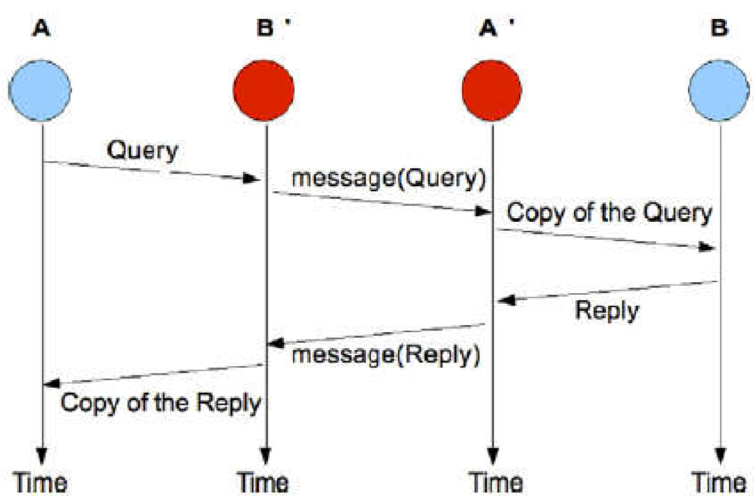
New Traffic to Handle

- The characteristics of the smart objects traffic in the IoT is still not known
  - Important → basis for the design of the network infrastructures and protocols
- Wireless sensor networks (WSNs) traffic characterization
  - Strongly depend on the application scenario
  - Problems arise when WSNs become part of the overall Internet
  - The Internet will be traversed by a large amount of data generated by sensor networks deployed for heterogeneous purposes → extremely different traffic characteristics
  - Required to devise good solutions for supporting quality of service



Security

- The components spend most of the time unattended
  - It is easy to physically attack them
- IoT components are characterized by low capabilities in terms of both energy and computing resources
  - They can't implement complex schemes supporting security
- Authentication problem
  - Proxy attack, a.k.a. man in the middle attack problem

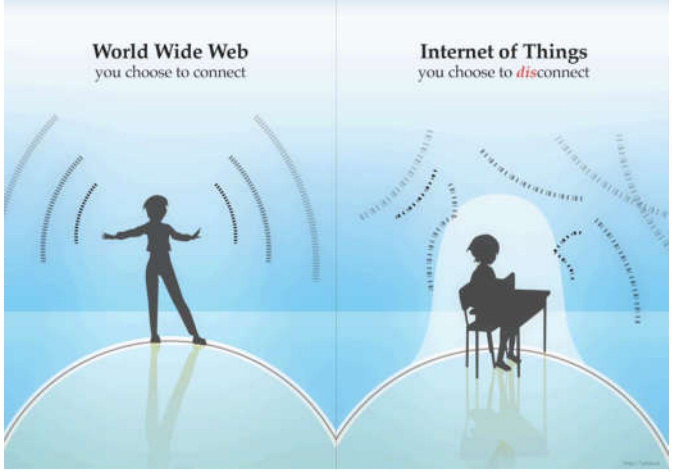


Man in the middle attack Source: Atzori et al. (2010)

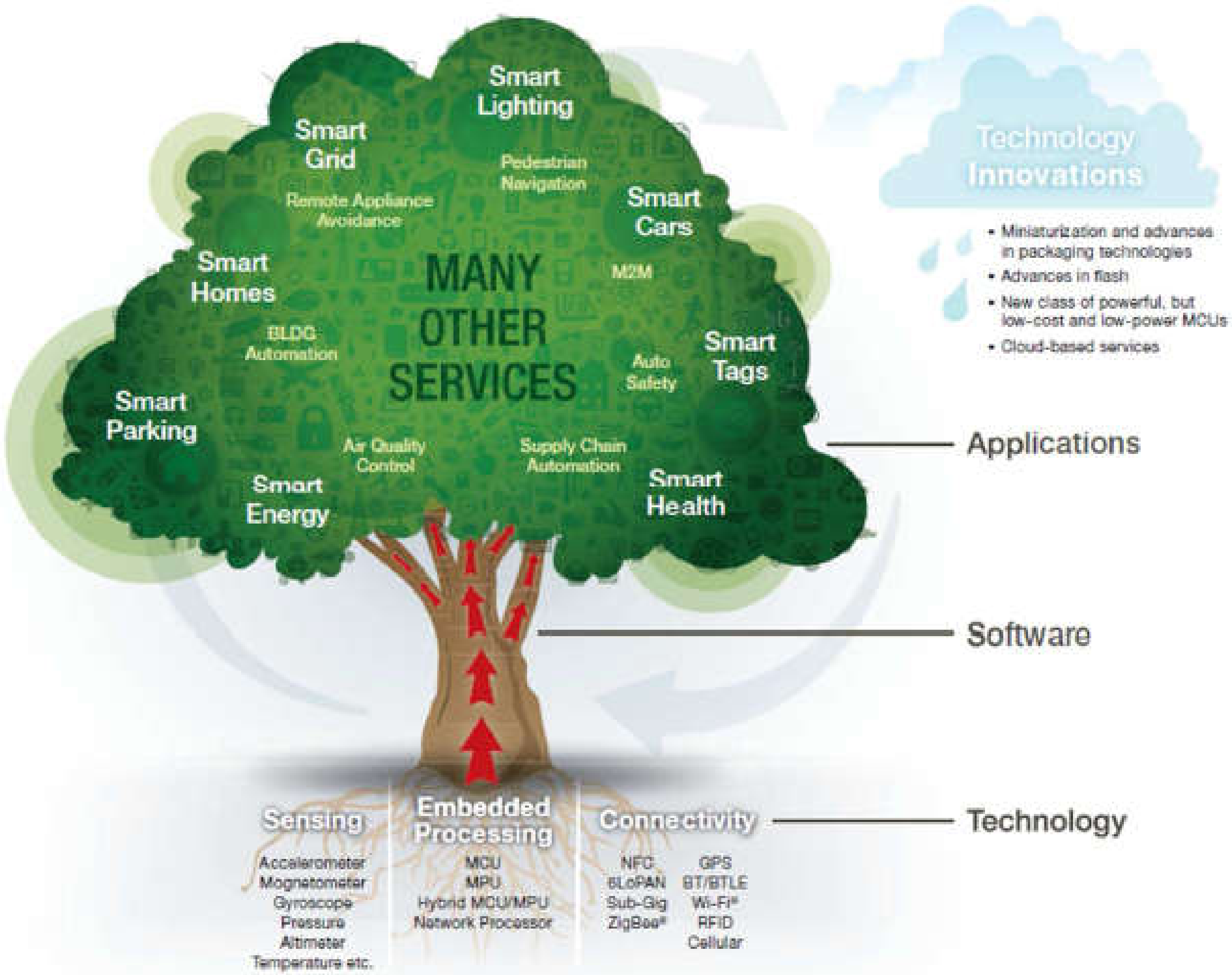
- Data integrity
  - Data should not be modified without the system detecting it
  - Attacks on the node
    - Memory protection
  - Attacks over the network
    - Keyed-Hash Message Auth. Code

Privacy

- How is it different than traditional privacy?
  - Legislative issues
  - Ethics issues
- Easy for a person to get involved in IoT even if he/she does not know
- Data can be stored indefinitely
- Current solutions are not enough
  - Encryption, pseudo-noise signal, privacy broker

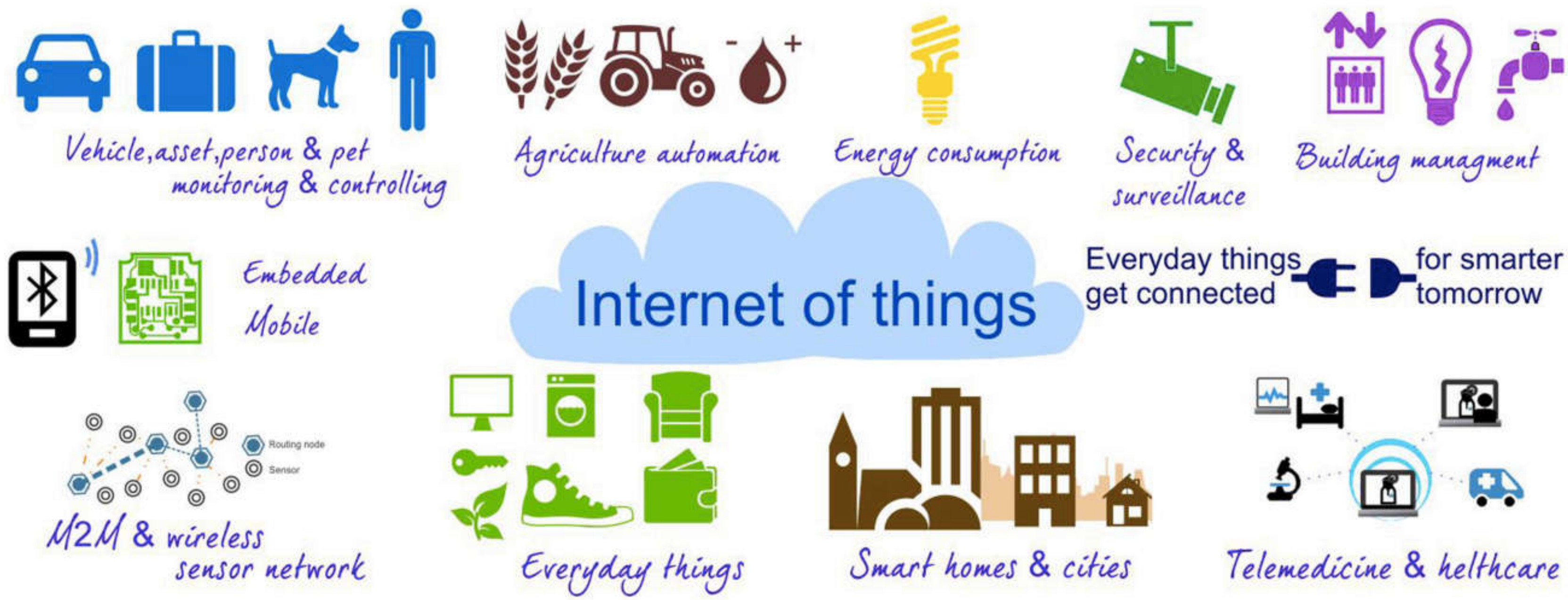


Again - Overall Picture



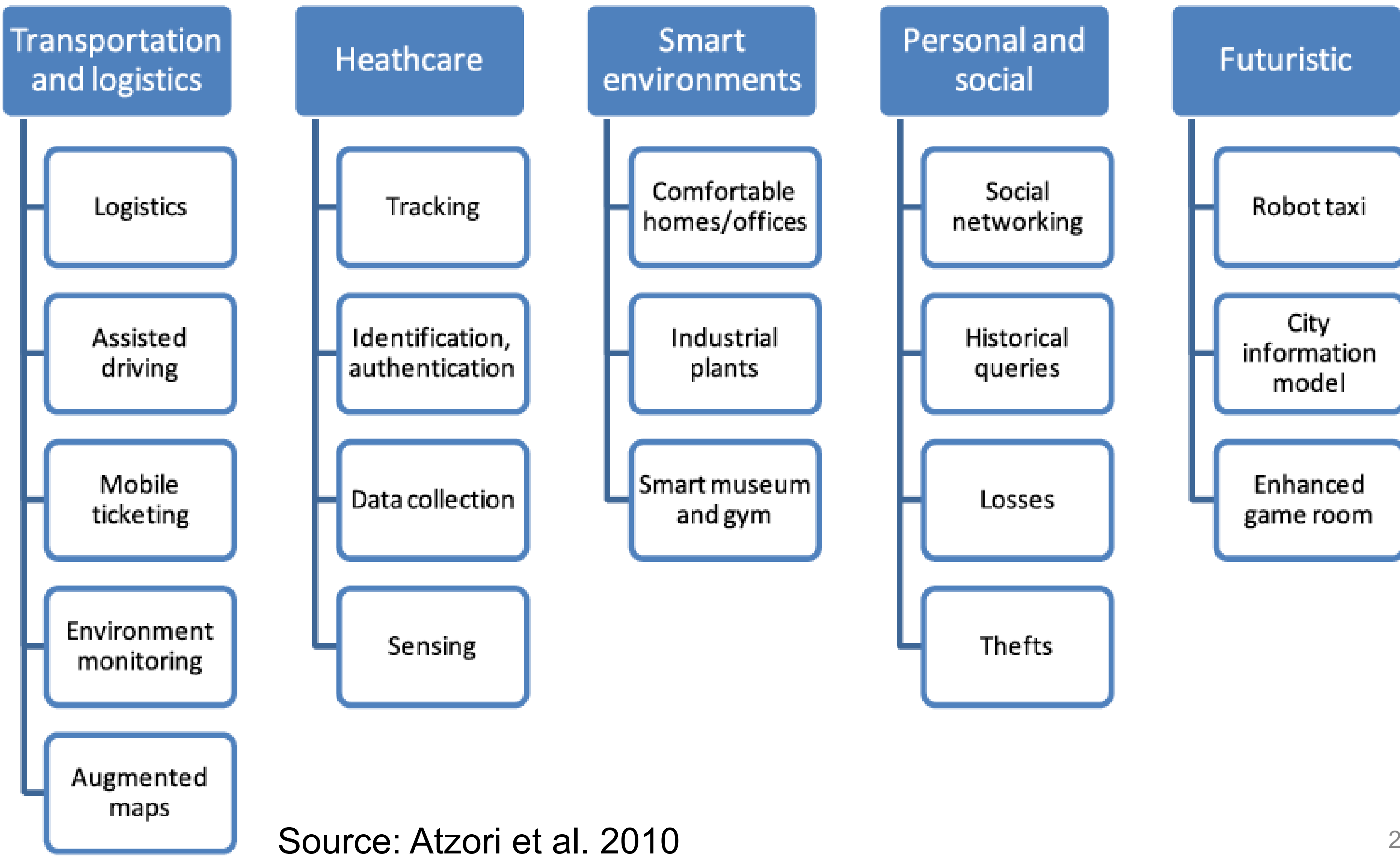
Source: "What the Internet of Things (IoT) Needs to Become a Reality," White Paper, by K. Karimi and G. Atkinson

Applications



- Several different domains
  - Transportation and logistics
  - Healthcare
  - Smart environment (home, office, etc.)
  - Personal and social domain

Application Domains and Scenarios



Source: Atzori et al. 2010

Healthcare Applications

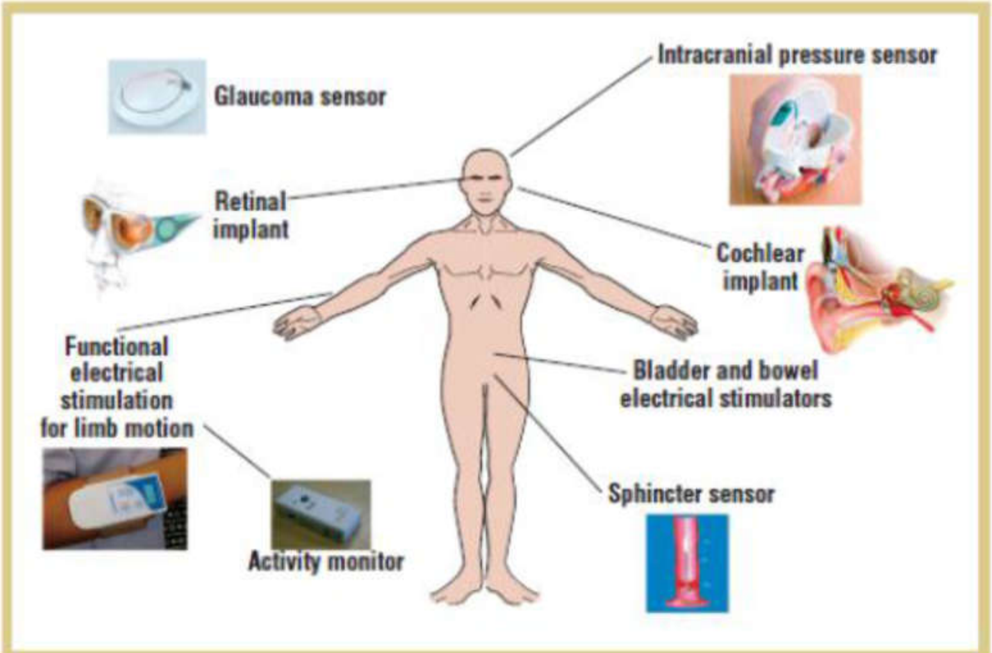


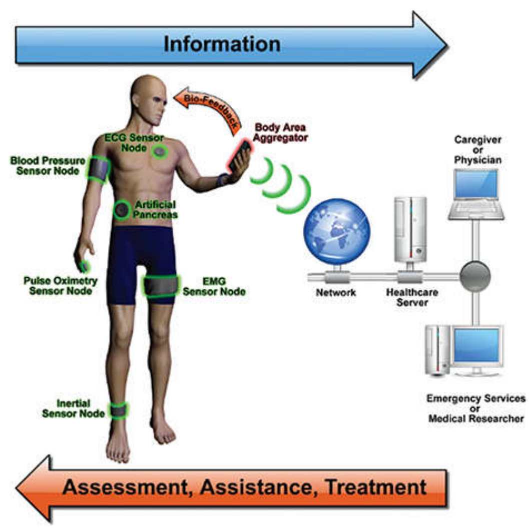
Figure 6. Fully implantable wireless sensor for the intracranial pressure monitoring system.

Source: Qian Zhang. Lecture notes. 2013

- Various sensors for various conditions
- Example ICP sensor: Short or long term monitoring of pressure in the brain cavity
- Implanted in the brain cavity and senses the increase of pressure
- Sensor and associated electronics encapsulated in safe and biodegradable material
- External RF reader powers the unit and receives the signal
- Stability over 30 days so far

Healthcare Applications

- Other applications:
  - National Health Information Network
  - Electronic Patient Record
  - Home monitoring and control
    - Pulse oximeters, blood glucose monitors, infusion pumps, accelerometers
  - Bioinformatics
    - Gene/protein expression
    - Systems biology
    - Disease dynamics

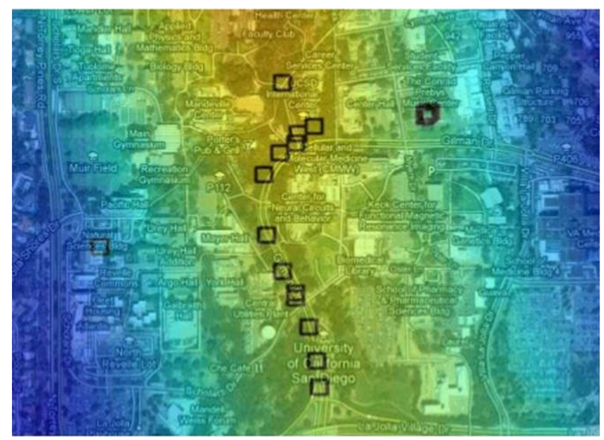


Source: Qian Zhang. Lecture notes. 2013

Environmental Application: CitiSense

- Air quality monitoring project in UCSD CSE

- Environmental application

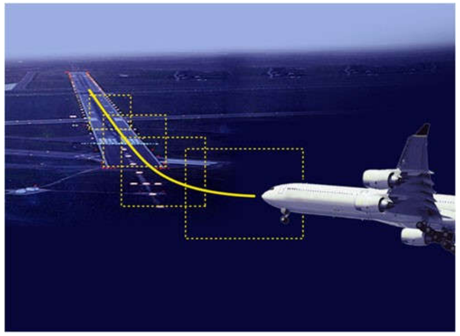


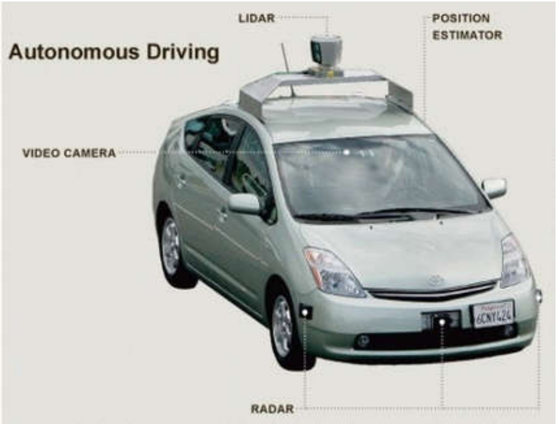
- Electrochemical **sensors**, **microcontroller** for data collection and transmission to an **Android** app

- **Actuation**: air quality is immediately reported, as well as retransmitted to a backend for larger-scale analysis

Transportation Applications

- **Vehicle control:** Airplanes, automobiles, autonomous vehicles
  - All kinds of sensors to provide accurate, redundant view of the world
  - Several processors in cars (Engine control, break system, airbag deployment system, windshield wiper, door locks, entertainment system, etc.)
  - Actuation is maintaining control of the vehicle
  - Very tight timing constraints and requirements enforced by the platforms



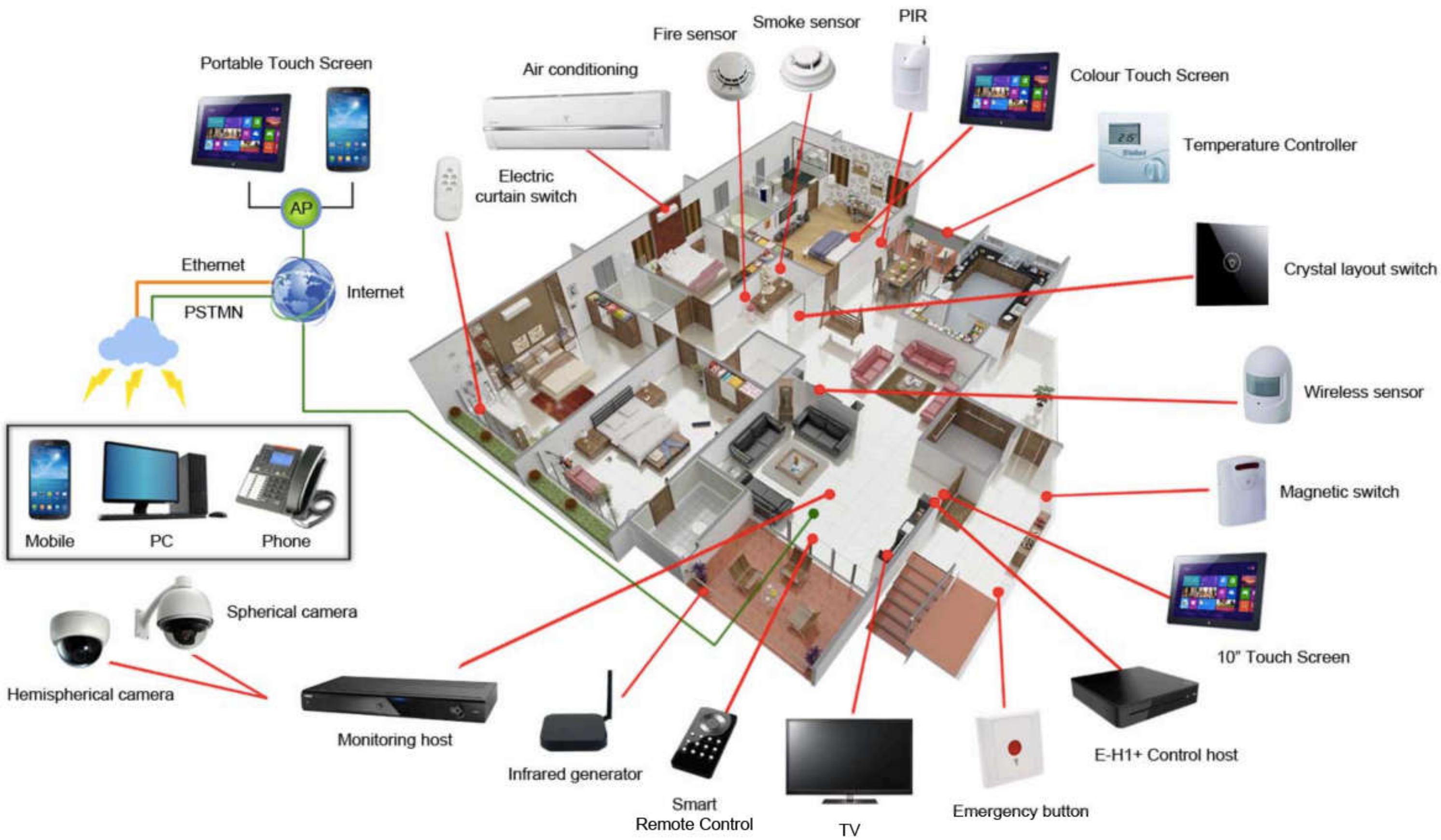


Example Transportation Scenarios

1. A network of sensors in a vehicle can interact with its surroundings to provide information
   - Local roads, weather and traffic conditions to the car driver
   - Adaptive drive systems to respond accordingly
2. Automatic activation of braking systems or speed control via fuel management systems.
   - Condition and event detection sensors can activate systems to maintain driver and passenger comfort and safety through the use of airbags and seatbelt pre-tensioning
3. Sensors for fatigue and mood monitoring based on driving conditions, driver behavior and facial indicators
   - Ensuring safe driving by activating warning systems or directly controlling the vehicle

Source: Qian Zhang. Lecture notes. 2013

Smart Home Applications



- Smart meters, heating/cooling, motion/temperature/ lighting sensors, smart appliances, security, etc.

A Futuristic Application: Shopping

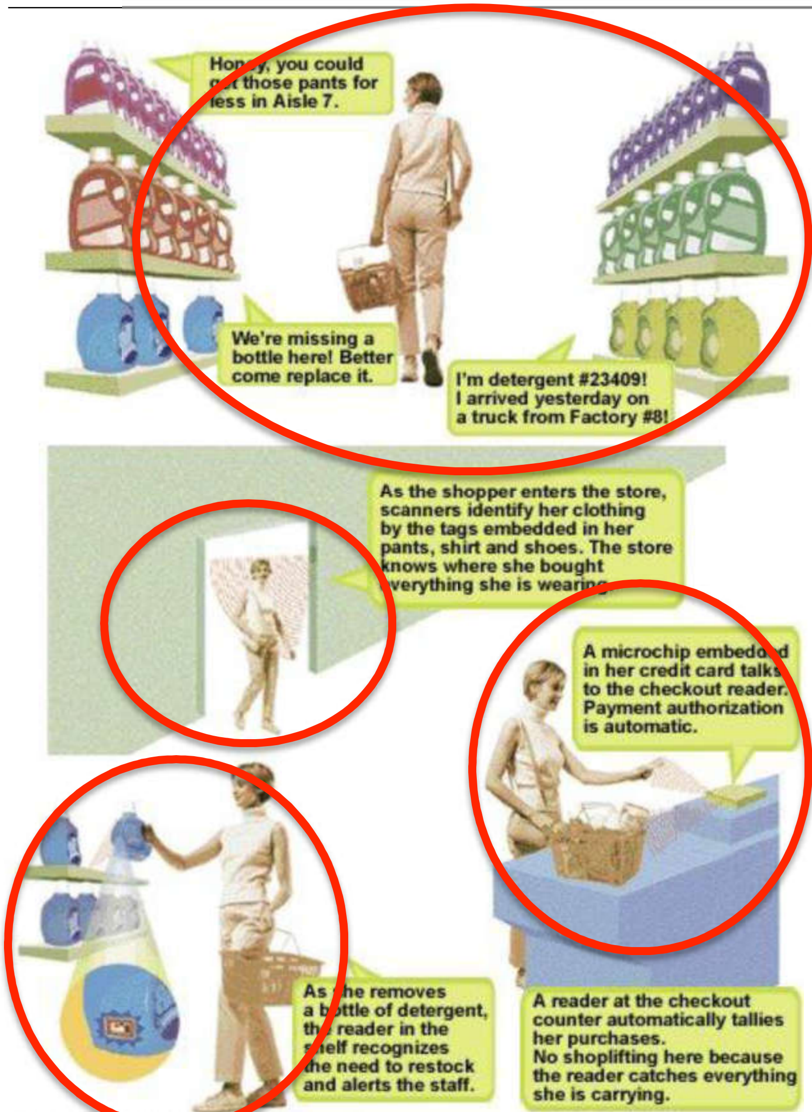


Illustration by Lisa Knouse Braiman for Forbes

- When entering the doors, scanners will identify the tags on her clothing.
- When shopping in the market, the goods will introduce themselves.
- When paying for the goods, the microchip of the credit card will communicate with checkout reader.
- When moving the goods, the reader will tell the staff to put a new one.

Source: Qian Zhang. Lecture notes. 2013

An exciting future!