Internet of Things

Opportunities, technologies, and challenges

Giacomo Morabito

Dipartimento di Ingegneria Elettrica, Elettronica, e Informatica
University of Catania

July 7, 2011

Outline

Reading material

This lecture is mostly based on:

L. Atzori, A. Iera, and G. Morabito. "The Internet of Things: A Survey". Computer Networks. Vol. 54, No. 15, pp.: 2787-2805, October 2010.

1. Introduction

Background

- **Radio/Humans** ≈ 1
  $\rightarrow$ *Anywhere, anytime, anymedia*.
- **Radio/Humans** $>> 1$
  $\rightarrow$ *Anywhere, anytime, anymedia,* **anything**.
  Radio transceivers and some processing capabilities embedded in most objects we use in our everyday life.

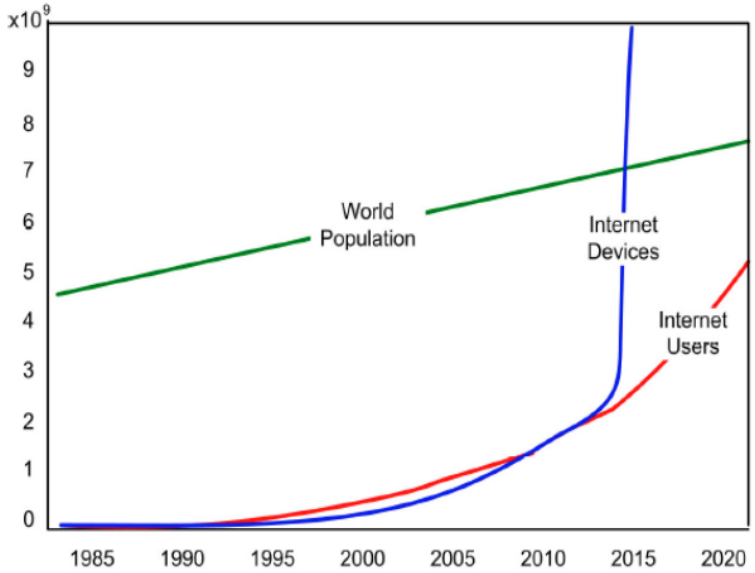


Figure: Number of people, Internet users, Internet devices: forecast.

$\rightarrow$ the **Internet of Things (IoT)**

What is it?

Definition (The Internet of Things is...)

a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols.

The Internet of Things integrates:

- Static fixed nodes
- Handheld wireless devices
- Wireless sensor and actor nodes
- RIFD readers/tags

Some high level visions

- **ITU** *From anytime, anyplace connectivity for anyone, we will now have connectivity for anything*[1].
- **EC-INFSO**: The IoT involves *things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts*[2].
- **George Carlin**: *Too much stuff...*

[1] ITU Internet Reports, "The Internet of Things", November 2005.
[2] INFSO & EPOSS, "Internet of Things in 2020, Roadmap for the Future", May 2008.

Major characteristics

- **Scale**: The number of nodes will be order of magnitude higher than the current Internet.
- **Heterogeneity**: Many technologies (very different one from the other) will need to interact with each other.
- **Pervasivity**: Computing and communication technologies will be embedded in our environments.

Impact

The IoT will radically change life for:

- Private users: domotics, assisted living, e-health, enhanced learning.
- Business users: automation and industrial manufacturing, logistics, business/process management, intelligent transportation of people and goods.

Is it important?

- The *US National Intelligence Council* reports the IoT in the list of the 6 civilian disruptive technologies with impact on US national power.
  The list:
  - Biogerontechnology
  - Energy Storage Materials
  - Biofuels and Bio-Based Chemicals
  - Clean Coal Technologies
  - Service Robotics
  - The Internet of Things.
- There are large investments:
  - In far east Asia: especially in China and Japan.
  - In Europe large funding from European Commission.
  - In US, IBM reports it in the list of the hot topics for two years in a row.

2. Applications

Application domains and scenarios

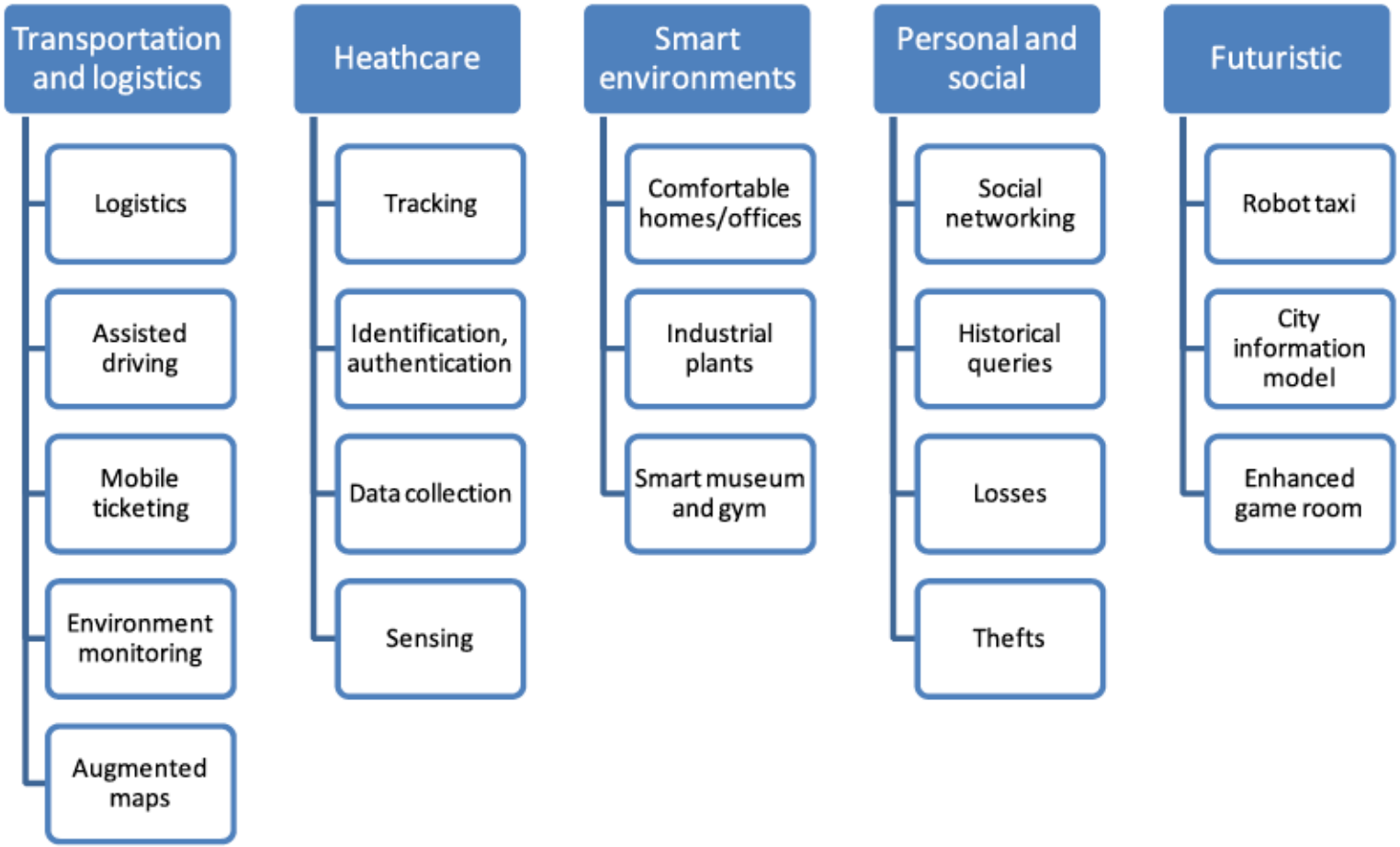
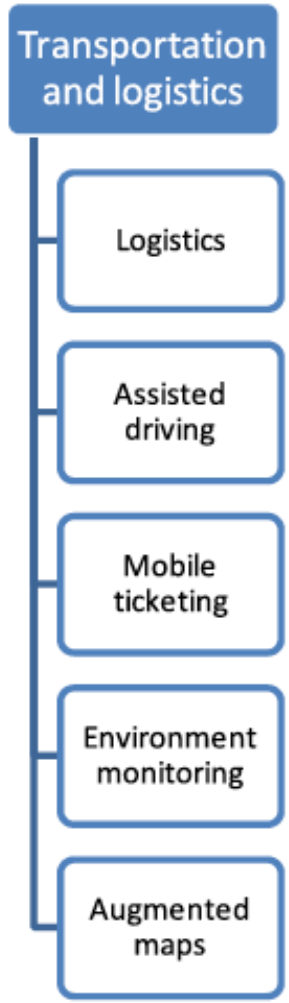


Figure: Exemplary domains and scenarios.

Transportation and logistic domain

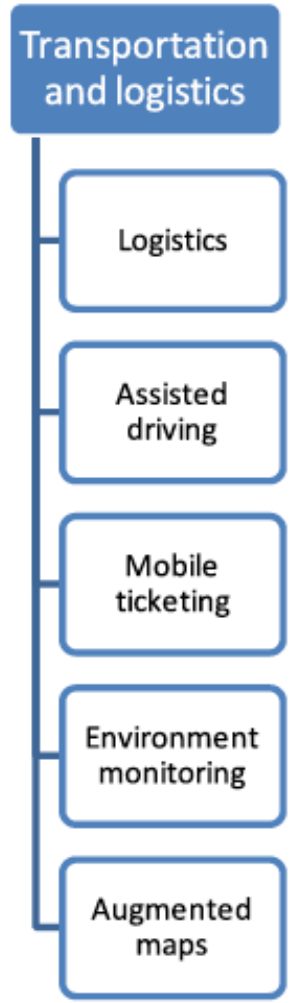
- Technologies are available that can be integrated according to the IoT paradigm to build advanced:
  - *Vehicles*: cars, buses, bicycles, etc.
  - *Transportation infrastructures*: roads and/or rails.
  - *Payload*: goods and assets.
- These can be used for
  - Logistics: real time monitoring of items is possible at every step of the supply chain. Result: traditionally the reaction time (from customer requirements to supply of the commodoty) of enterprises was 120 days (average); for enterprises applying modern technologies it is few days[a].
  - Assisted driving: communications/cooperation between vehicles and between vehicles and transportation infrastructure enable a large number of new services which can improve safety, traffic flow (time and energy saving), forecasts of arrival/delivery time



[a] R. Yuan, L. Shumin, Y. Baogang, *Value Chain Oriented RFID System Framework and Enterprise Application*, Science Press, Beijing, 2007.

Transportation and logistic domain

- These technologies can be used for:
  - Mobile ticketing: Posters or panels providing information (description, costs, schedule) of transportation services can be equipped with NFC tags. Users may be redirected to the web to obtain much more information and buy related tickets[a].
  - Environment monitoring: Perishable goods (vital part of our nutrition) cover thousands of kilometers from the producer to the consumer. Monitoring environmental parameters is fundamental to improve their quality at the consumer and (in turn) to avoid transporting *perished* goods that cannot be used[b].
  - Augmented maps: These can be equipped with tags so that smartphones can browse web services providing information about hotels, restaurants, monuments[c].



[a] G. Broll, et al. *PERCI: pervasive service interaction with the internet of things*, IEEE Internet Computing, 13 (6) (2009) 74 – 81.

[b] A. Ilic, et al., *Using sensor information to reduce the carbon footprint of perishable goods*, IEEE Pervasive Computing, 8 (1) (2009) 22 – 29.

[c] D. Reilly, et al., *Just point and click? Using handhelds to interact with paper maps*, ACM MobileHCI05, September 2005.

3. One paradigm, many visions (and architecture)

The fuzziness starts with the name

The name "Internet of Things" is syntactically composed of two terms:

- Internet, which focuses on the network.
- Things, which focuses on integration of objects (and their functionality)

A semantic-oriented vision also has been adopted as unique addressing as well as representation and storing of exchanged information are extremely challenging issues.

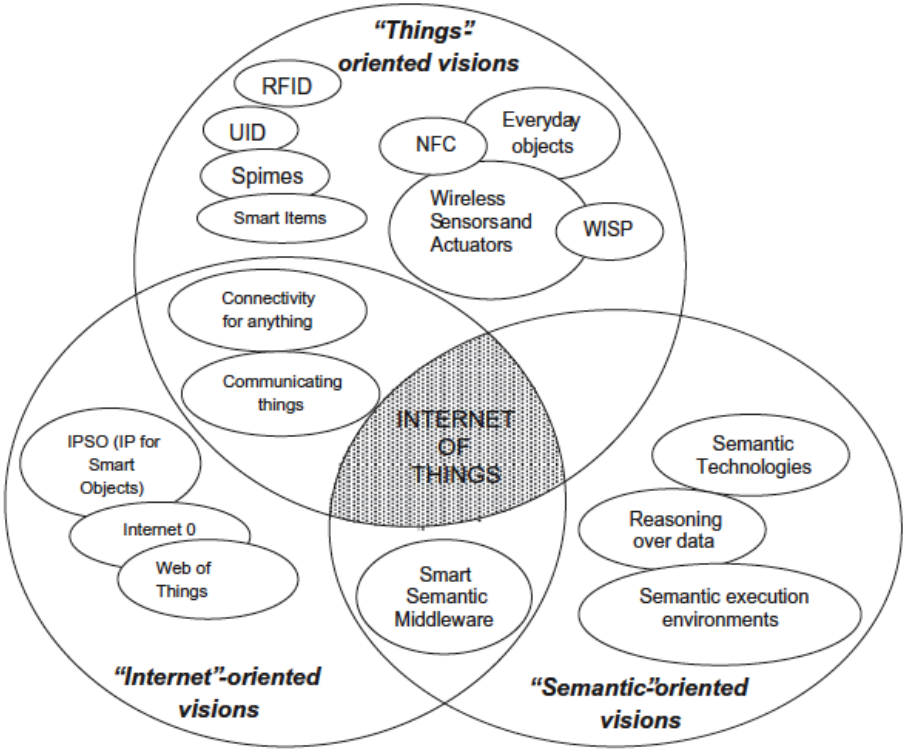


Figure: "Internet of Things" paradigm as the result of a convergence of different visions.

- Differences in the IoT visions depend on the interests, finalities and backgrounds of the major stakeholders.
- The IoT paradigm will be the result of the convergence of the above visions.

Things-oriented vision

- It has been the very first proposed vision.
- The term "Internet of Things" has been introduced by The AutoID Labs[3]:
  - Their **focus:** To extend the the Electronic Product Code (EPC) to support the spread use of RFID in world-wide trading networks and create industry-driven global standard for the EPCglobal network.
  - Their **primary interest**: improve object visibility (i.e., traceability of an object and the awareness of its status, current location, etc.).
  - Their **ultimate objective:** To architect the IoT in cooperation with EPCglobal.
- The Unique/Universal/Ubiquitous IDentifier (uID) architecture has mostly the same objectives (in both cases proposed solutions are middleware-based).
- The things-oriented vision should extend the *portfolio* of technologies to include[4]
  - Near field communications (NFC)
  - Wireless sensor and actuator networks (WSAN)
  - Wireless Identification and Sensing Platforms (WISP)

[3] http://www.autoidlabs.org

[4] M. Presser, A. Gluhak, *The Internet of Things: Connecting the Real World with the Digital World*, EURESCOM mess@ge The Magazine for Telecom Insiders, vol. 2, 2009.

Spimes

Definition (Spime)

An object that can be tracked through space and time throughout its lifetime and that is sustainable, enhanceable, and uniquely identifiable[a]

[a] B. Sterling, *Shaping Things* Mediawork Pamphlets, The MIT Press, 2005.

This theoretical concept finds some real-world implementations in the so called *smart items*. This are sort sensors equipped with wireless communication, memory, and elaboration capabilities (as usual) but enriched with

- Autonomous and proactive behavior.
- Context awareness
- Collaborative communications and elaboration capabilities.

From a *Thing-oriented* to an *Internet-oriented* vision

CASAGRAS[5] focuses on a "world where things can automatically communicate with computers and each others to provide services to the benefit of the human kind.
Accordingly, CASAGRAS

- proposes a vision of the IoT as a global infrastructure which connects virtual and physical generic objects.
- highlights the importance of including existing and evolving Internet and network developments in the IoT vision.

Therefore, the IoT becomes the enabling architecture for deployment of federated services and applications, characterized by a high degree of

- Autonomous data capture
- Event transfer
- Network connectivity and interoperability

[5] http://www.rfidglobal.eu

Internet-oriented vision

It is based on the fact that currently IP connects a huge amount of communication devices and runs on tiny, battery operated embedded devices.

- IP over Smart Objects (IPSO)[6]: A forum of 25 founding companies promoting the use of the Internet Protocol for connecting Smart Objects. Key aspects – in line with 6LOWPAN[7]:
  - a wise adaptation of IP
  - integration of IEEE 802.15.4 in the IP architecture
- Internet 0[8]: Complexity of IP should be reduced to route IP over anything. Key aspects:
  - Simplification of current IP to be implemented in low capability devices.
  - Global objects addressability and reachability.
- Web of things[9]: Web technologies are reused to connect and integrate in the Web every day-life objects equipped with embedded devices or computers.

---

[6] A. Dunkels, et al. "IPSO Alliance – White Paper #1", September 2008.

[7] J. Hui, et al. "6LOWPAN: Incorporating IEEE 802.15.4 into the IP Architecture – IPSO Alliance White Paper #3", January 2009.

[8] N. Gershenfeld, et al., "The Internet of Things", *Scientific American*, 2004.

[9] D. Guinard, et al., "Towards the Web of Things: Web meshups for Embedded Devices", *WWW 2009*. April 2009.

Semantic-oriented vision

- The number of nodes generating information will be huge $\rightarrow$
- It is critical how to accomplish information representation, storage, interconnection, search, and organization.
- Semantic technologies can exploit modeling solutions for[10]
  - *things* description
  - reasoning over generated data
  - semantic execution of environments
  - architectures that accommodate IoT requirements and scalable storing and communication infrastructure
- Therefore, semantic technologies may play a key role.

[10] I. Toma et al., "A Joint Roadmap for Semantic Technologies and the Internet of Things", *Third STI Roadmapping Workshop*, June 2009.

Applications - Healthcare domain

- In the healthcare domain IoT technologies can be used for
  - Tracking for healthcare: this is important to locate patients, medical personnel and appliances as well as to prevent lefts-in during surgery.
  - Patient and staff identification and authentication: this reduces incidents such as wrong drug/dose/time/procedure and improves the level of privacy/security.
  - Medical data collection: this enables the automatic filing and management of medical records and their utilization by different healthcare service providers[a].
  - Patient vital parameter sensing: real-time monitoring enables continuous healthcare service delivery as well as telemedicine services[b].

[a] A. M. Vilamovska, et al., *RFID Application in Healthcare* RAND Europe, February 2009.

[b] D. Niyato, et al., *Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization*, IEEE JSAC, 27 (4) (2009) 412 - 423.

4. Enabling technologies

Disclaimer

- We will not provide a comprehensive survey of all involved technologies.
- We will, instead, provide a *survey* of their role in the IoT
- Interested readers can select technical papers covering specific aspects among the references in
  - L. Atzori, A. Iera, and G. Morabito. "The Internet of Things: A Survey". Computer Networks. Vol. 54, No. 15, pp.: 2787-2805, October 2010.
- We distinguish enabling technologies as follows:
  - Identification, sensing, and communication technologies
  - Middleware technologies

Identification technologies

- RF Identification (RFID) systems consists of:
  - One or more RFID reader(s)
  - Several RFID tags

  Operation principles of RFID systems are the following:
  1. *Tags* are characterized by a unique identifier and applied to objects (even *persons* or *animals*).
  2. *Readers* trigger tags' transmission by generating an appropriate signal which represents a *query*
  3. *Tags* reply sending their ID
- RFID systems can be used to monitor objects in real time (no need of *line-of-sight*) $\rightarrow$
- Mapping of the *physical world* in the *digital world* $\rightarrow$
- They can be used in a large set of heterogeneous scenarios (spanning from logistic to e-health and security)

Figure: RFID reader.

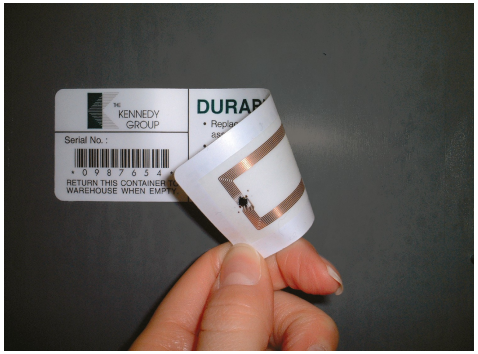
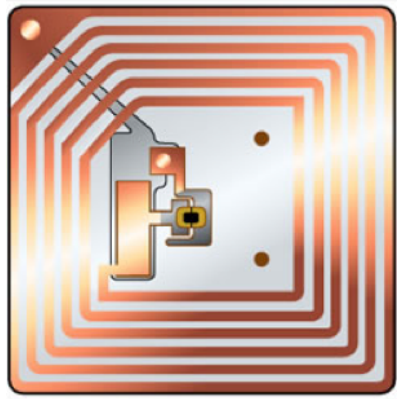


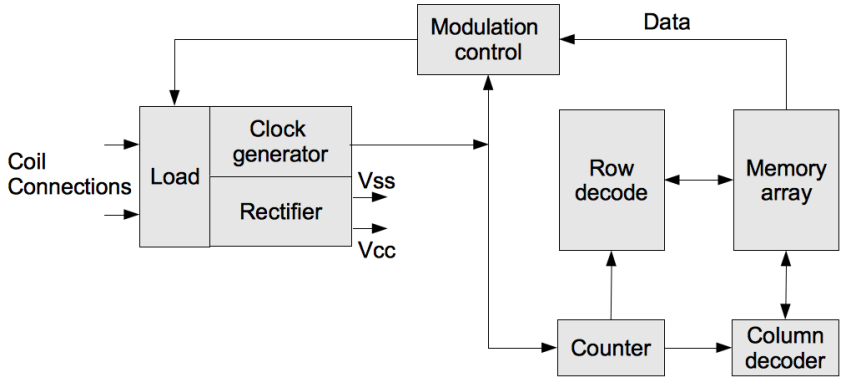
Figure: RFID tag.

Architecture of RFID tags

An RFID tag consists of

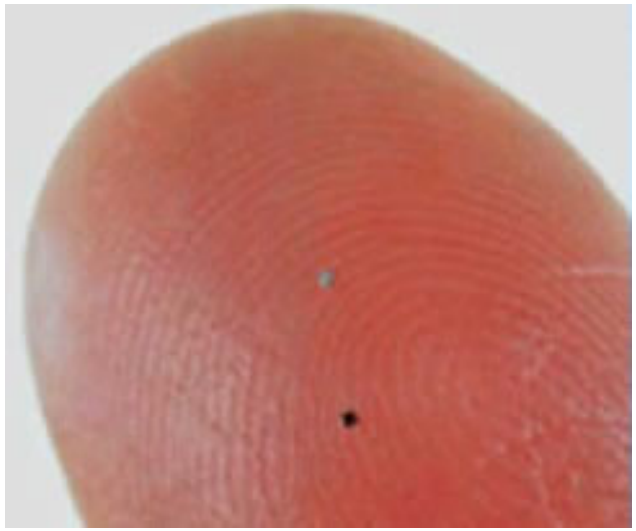
- A small microchip which is responsible for interpreting the *command* from the reader and, in case, modulates the signal reflected by the antenna.
  - Tags are being studied (chipless tags[a]) with no microchips $\longrightarrow$
  - production cost decreases!
- An antenna used for both rx and tx
- The above elements are attached to a package (similar to an adhesive sticker)
- Overall dimensions can be very low:
  - Hitachi developed a tag with dimensions 0.4 mm x 0.4 mm x 0.15 mm

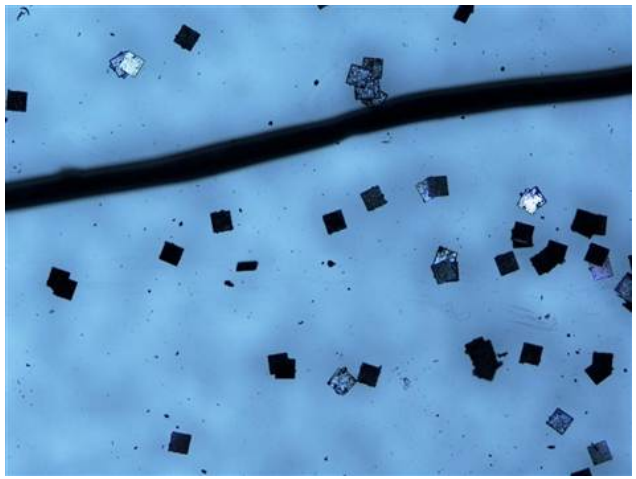




[a] S. Tedjini et al., "Chipless, the next RFID frontier", *TIWDC 2009*. 2009.

Hitachi μ-tag





Passive RFID tags

- Passive RFID tags do not have on-board power supply $\rightarrow$ they harvest the energy for transmitting their ID from the *query* transmitted by the reader.
- The query signal generates a current in the tag by electromagnetic *induction*.
- This current is utilized to power the microchip which modulates the signal reflected by the antenna.
- Overall gain (power level of the signal received by the reader divided by the power level of the signal transmitted by the reader) is very low.
- Readers have extremely directive antenna $\rightarrow$ tags ID can be received within a radio range of a few meters.
- Several frequency bands can be utilized ranging from:
  - Low frequencies (LF): 124–135 kHz.
  - Ultra High Frequencies (UHF): 860–960 MHz

Energy harvesting technologies

Energy Source	Harvested Power
Vibration/Motion	
Human	4 μW/cm²
Industry	100 μW/cm²
Temperature Difference	
Human	25 μW/cm²
Industry	1–10 mW/cm²
Light	
Indoor	10 μW/cm²
Outdoor	10 mW/cm²
RF	
GSM	0.1 μW/cm²
WiFi	0.001 mW/cm²

Figure: Comparison between different energy harvesting techniques[11].

[11] Figure taken by: M. Raju, "Energy Harvesting – ULP meets energy harvesting: A game-changing combination for design engineers," *Texas Instruments – White paper*, November 2008.

Non passive RFID tags

We can distinguish:

- Semi-passive RFID tags: Batteries power the microchip while receiving the signal from the reader.
  - The radio is powered by the energy harvested by the reader signal.
- Active RFID tags: Batteries power the radio as well.

Obviously,

- *Radio coverage* is higher for active tags.
- *Production cost and energy consumption* is lower for semi-passive tags.

Read-only and Read/Write RFID tags

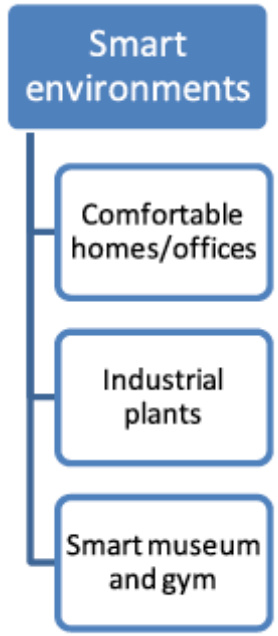
- Read-only tags are programmed with unique information stored on during the manufacturing process. Information on read-only chips can not be changed.
  - *Advantage*: **low cost**
- Read/write tags: user can **add** information or **overwrite** existing information when the tag is within the radio coverage of the reader.
  - *Advantage*: **more complex applications** can be supported.
- Write Once Read Many (WORM): It can be written once and then becomes a *read-only* tag.

Operations supported by RFID systems

Operation	Function	Data Flow
Inventory	Singulate tags and receive their EPCs	Reader to network
Read	Read tag memory	Bidirectional
Write	Write tag memory	Bidirectional
Lock	Permalock, lock, or unlock tag memory	Bidirectional
Kill	Render a tag permanently inoperative	Bidirectional

Applications - Smart environment domain

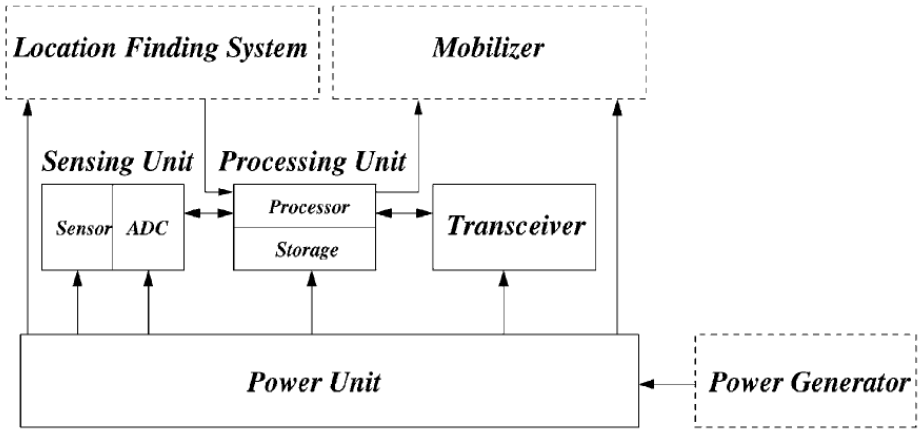
- This is the result of the cooperation between
  - *sensing technologies*: monitor the state of the environment
  - *actuator technologies*: regulate the state of the environment
  - *identification technologies*: recognize users and retrieve their profile/preferences
- These can be used for
  - Comfortable homes and offices: The IoT technologies can make our homes and offices more comfortable with lower energy cost[a] (The IoT is a **green** technology!).
  - Smart industrial plants: IoT technologies can recognize production parts so as to extend automation possibilities, and identify critical conditions during production $\longrightarrow$ specific quality checks can be performed on individual components.
  - Smart entertainment environments (gym): Trainer uploads the profile for each trainee. This is recognized by the machine that configures itself accordingly. Health parameters are kept under controlled during the session.

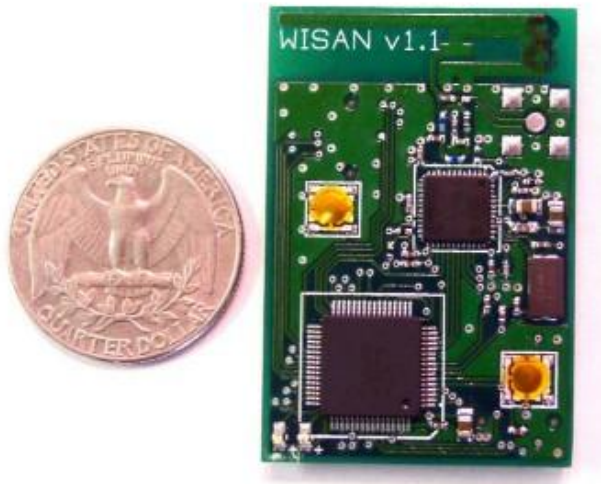


[a] C. Buckl, et al., *Services to the field: an approach for resource constrained sensor/actor networks*, WAINA09, May 2009.

Wireless sensor networks in the IoT

- Wireless sensor networks (WSN) will play a crucial role in the IoT as they are a further bridge between the *physical* and *digital* world. In fact, they can cooperate with RFID systems to better track the *status* of things and of the environment
  - Location, temperature, movements, etc.
- Sensor networks consists of a certain (large) number of sensing nodes communicating in wireless, multihop fashion. Architecture of a sensor node is shown below:





- Nodes report the results of their sensing to a small number (in most cases, *one*) special nodes called sinks.

Solutions for WSN

- Major design objectives:
  - **Energy efficiency**: Energy is the most scarce resource in most WSN scenarios – when batteries are exhausted the lifetime of the sensor node is over!
  - **Scalability**: The number of nodes involved in a WSN can be much larger than in other wireless networks – e.g., ad hoc networks.
  - **Reliability**: WSN may be used to report alarm events.
  - **Robustness**: WSN nodes are likely to fail the network should continue to work.
  - **Security and privacy**: Information gathered by WSN should be protected against interceptions and modifications.
- There is a huge literature on the subject[12]:
  - **Please stop with energy efficient MAC/routing/etc. protocols for WSN**!

[12] I. F. Akyildiz, et al., "Wireless Sensor Networks: A Survery", *Computer Networks*, 2002.

Integrating WSNs in the IoT

- IEEE 802.15.4 is the standard *de facto* for commercial WSNs.
- IEEE 802.15.4 defines physical and MAC layers. It does not define higher layers of the protocol stack, which is necessary for integrating WSN in the IoT.
- Identifying solutions for the higher layer is difficult because:
  - Sensor networks may consist of a very large number of nodes. **There are no enough IPv4 addresses** $\longrightarrow$ Migration to IPv6?
  - The largest physical layer packet in IEEE 802.15.4 has 127 byte $\longrightarrow$ largest frame size = 102 byte $\longrightarrow$ **Too small for typical IP packets**. Need for a standard convergence layer?
  - Nodes spend most of the time in a sleep mode to save energy. **They cannot communicate in these time interval**. Need for some node representative which is always on?
- **Large standardization activities to provide solutions to most of the above problems!**

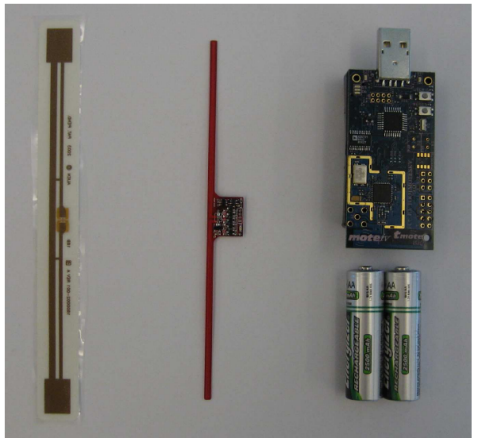
RFID Sensor Networks (RSN)

- Integration of sensing capabilities and passive RFID capabilities enables completely new applications.
  - especially into the e-health domain.
- Several activities in this area according to two major approaches:
  - Exploit the response of the antenna to changes in the environmental parameter of interest[13] $\longrightarrow$
    $\longrightarrow$ Changes in such parameter involve changes in the characteristics of the e.m. field received by the reader $\longrightarrow$
    $\longrightarrow$ The reader can achieve estimates of the environmental parameter of interest by observing variations in the e.m. field characteristics.
    - ⋆ Obviously, tags should be designed in such a way that impact of the parameter of interest on the e.m. field characteristics is maximized.
  - Integrate a sensor (and the required circuitry) into RFID tags (see below).
- Integration of RFIDs and sensing technologies leads to the RSN concept.

[13] G. Marrocco, "Pervasive Electromagnetics: Sensing Paradigms by Passive RFID Technology", *IEEE Wireless Communications*, December 2010.

Wireless Identification Sensing Platform (WISP)

- WISP is a project of the Intel Labs.
- WISP tags are passive devices are powered and read by standard RFID readers.
- Besides usual identification capabilities they are equipped with some sensor.



Current WISPs have the following characteristics:

- 3 m range with harvested RF power
- Ultra-low power microcontroller
- 32K of progr. space, 8K of storage
- Light, temp and 3D-accelerometers
- Backscatter comm. to reader
- Reader to WISP comm. (ASK)
- Real-time clock
- Works without reader
- Voltage sensor (for stored charge)
- Extensible HW (for new sensors)
- Works with EPC standard readers
- Software to sense and upload data
- Reader application to drive WISP
- Industry standard development tools
- Access to HW design and source code

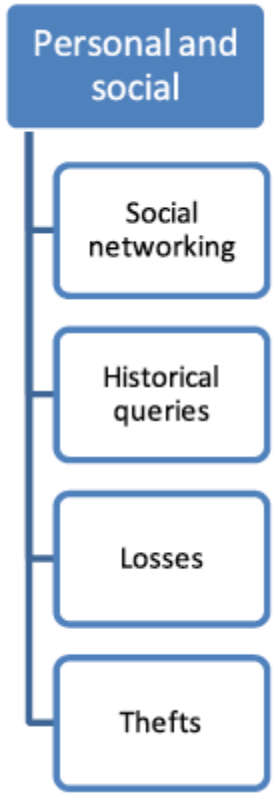
Comparison

Table 1
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

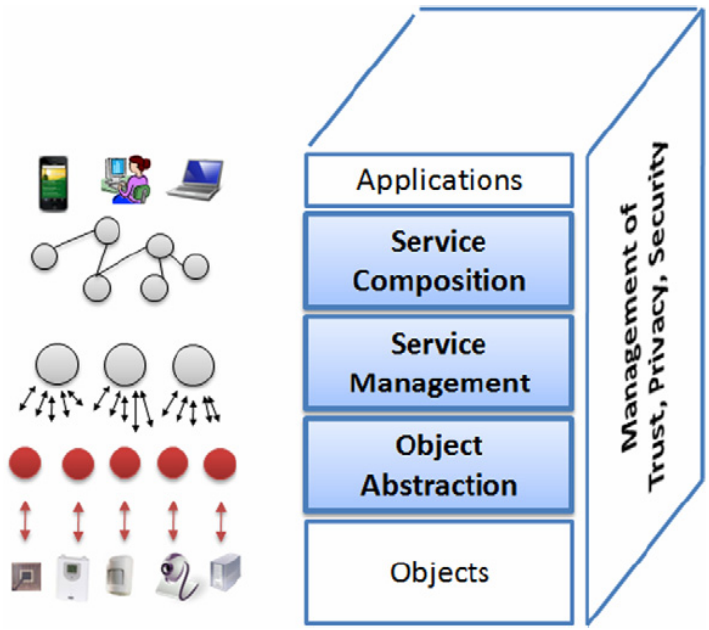
Applications - Personal and social domain

- Application in this domain enable users to interact with other people and build and manage social relationships (objects can send messages to friends (or their things) with information about our current activities/state).
- In the personal and social domain the IoT can be used for:
  - Social networking: Things may provide real-time information about the activity/location of their owner.
  - Historical queries: These can be used to study trends of people activities over time – useful for business projects and collaborations.
  - Losses: A web-based RFID application storing may provide information about the location where an object has been *read* for the last time.
  - Thefts: A similar application may alert/inform user when an object has been moved from a restricted, well defined area.



Middleware

- The middleware is a software layer (or a set of sub-layers) between the application and technological layers.
- It excepts the programmer from the detailed knowledge of the technologies utilized at the lower layers.
- Most middleware solutions proposed for the IoT comply with the Service Oriented Architecture (SOA)



- SOA principle enable the decomposition of complex, monolithic systems into *applications consisting of an ecosystem of simpler components*.
- There is NOT a commonly accepted middleware architecture.
- In the figure we represent a stack which includes functions commonly defined by IoT middleware solutions.

Service composition

- It provides the functionality for the composition of single services offered by networked objects to build specific applications.
- There is no notion of devices: services are the only assets visible at this level.
- A repository/directory is needed of all currently connected service instances.
- The logic for the creation and management of complex services can be expressed in terms of workflows, by using workflow languages.
  - Examples: Business Process Execution Language (BPEL) and Jolie,
- Workflow languages define business processes that interact by means of Web Services. These are defined through the Web Service Description Language (WSDL).
- Workflows can be nested $\rightarrow$ It is possible to call a workflow from inside another one.

Service management

- It provides the functions available for each object and allow their management in the IoT.
- Examples include *object dynamic discovery*, *status monitoring*, *service configuration*.
  - This layer might enable the remote deployment of new services during run-time.
- A service repository is built at this layers to catalogue the services available in the specific object.
- Upper layers can compose services offered by this layer in more complex services.

Object abstraction

- It provides a common language and procedure in order to harmonize access to different devices.
- It consists of two sub-layers:
  - **Interface sub-layer**: It provides a web interface exposing methods available through a standard web service interface.
    Furthermore, it is responsible for the management of incoming/outgoing messages for communications with the external world.
  - **Communication sub-layers**: It implements the logic of the web service methods and translates such methods in device-specific commands to communicate with the real-world objects.
- Possible deployment of the *Object Abstraction* functionality:
  - **Embed web servers in the objects**: This is possible thanks to light TCP/IP stacks such as TinyTCP or mIP.
  - **Proxy-based web servers**: Functionality are run on a proxy server which communicate with the real world object through specific (even *proprietary* sockets).

Trust, privacy and security management

- **Trust, security, and privacy** are major issues in the IoT (*see below*) $\longrightarrow$ $\longrightarrow$ the middleware **must** include appropriate functions.
- Management operations can be run:
  - At a **specific layer**: there is a dedicated layer in the middleware stack.
  - At all layers of the middleware stack.
    This is what is done usually.

Existing middlewares for the IoT

- **Fosstrack**[14]: It is an open-source middleware implements EPC Network interfaces. Its major services are:
  - Data dissemination, data aggregation, data filtering, writing to tag, trigger reader from external sensors, fault and configuration management, data interpretation, sharing of RFID triggered business events, lookup and directory service, tag identifier management, and privacy management.
- **RFID Ecosystem**[15]: It implements three major functions:
  - Tag management: It allows the user to associate each tag to an object.
  - Place management: It supports the creation and editing of location information associated to RFID readers (assumed static, mostly).
  - Scenic management: It combines events collected by readers and related applications.
- **e-Sense**[16]: It focuses on ambient intelligence obtained through WSNs. It defines logical subsystems – application, management, middleware, and connectivity subsystems – which run on three types of nodes – gateway, full function sensor nodes and (a reduced stack) in a reduced function sensor node.

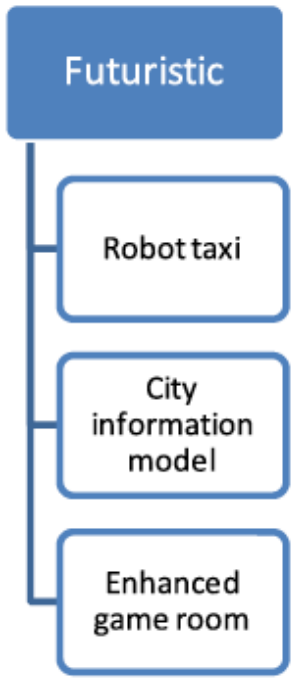
[14] `http://www.fosstrack.org`

[15] E. Welbourne, et al., "Building the Internet of Things Using RFID: The RFID Ecosystem Experience", *IEEE Internet Computing*, 2009.

[16] `http://www.ist-e-sense.org`

Futuristic applications

- For these applications some of the required technologies do not exist yet or their implementation is still too complex.
- The following examples have been taken by the SENSEI Project[a]:
  - Robot taxi: Robot taxis swarm together, moving in flocks, providing service where it is needed in a timely and efficient manner. It requires sensors as well as actors (drive the car) and communications with the infrastructure.
  - City information model: The status of each buildings and urban fabrics are continuously monitored by the city government operates and made available to third parties via appropriate APIs. This enables the sharing energy in the most cost-effective and resource-efficient fashion.
  - Enhanced game room: The game room and the players are equipped with devices to sense location, movements, etc. Information is used to measure excitement and energy levels of players to control game activity accordingly. Objects are placed in the room and players interact with them.



[a] SENSEI FP7 Project, Scenario Portfolio, *User and Context Requirements, Deliverable 1.1*, <http://www.sensei-project.eu/>

5. Open Issues

Standardization

There is a large body of standardization activities in the area:

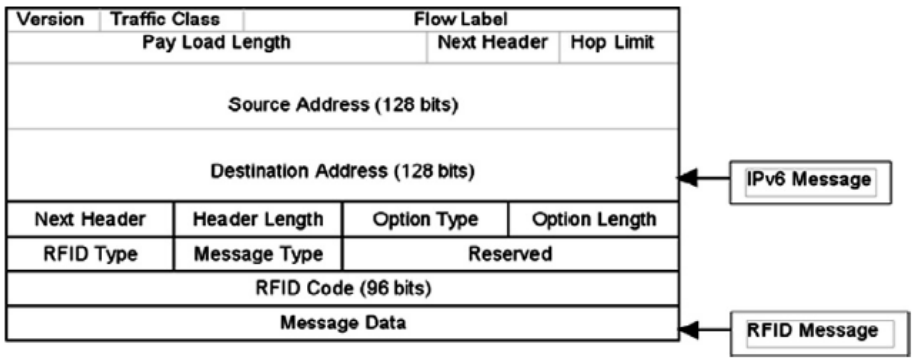
Standard	Objective	Status	Comm. range (m)	Data rate (kbps)	Unitary cost ($)
Standardization activities discussed in this section					
EPCglobal	Integration of RFID technology into the electronic product code (EPC) framework, which allows for sharing of information related to products	Advanced	~1	$\sim 10^2$	~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	$\sim 10^2$	~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	$\sim 10^2$	~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	$\sim 10^{-2}$	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	$\sim 10^2$	~1
ZigBee	Enabling reliable, cost-effective, low-power, wirelessly networked, monitoring and control products	Advanced	10–100	$\sim 10^2$	~1

However, they are not integrated in a comprehensive framework.

Addressing

- IPv4 address space is exhausted *to* use IPv6 (128 bits and thus, 10^{38} possible addresses: enough for all objects worth to be addressed).
- 6LOWPAN allows integration of IEEE 802.15.4 nodes in IPv6 networks $\rightarrow$ no problems for sensor networks.
- What about RFIDs (64-96 bit identifier according to *EPCGlobal*)?
  - In case the tag identifier is 64 bit long, the IPv6 address consists of:
    - ⋆ **Network prefix** (64 bits): the address of the gateway between the RFID system and the Internet.
    - ⋆ **Interface identifier** (64 bits): the RFID tag identifier.

    IP packets should be prepared accordingly. The *gateway* will forward messages directed to an RFID tag to the appropriate reader.
  - *What if the RFID identifier is 96 bit long?* An agent is responsible of the mapping between the RFID tag identifier into 64 bit regardless of its length. Then, the above approach is used.
  - A different approach could be applied using the IP options:



Mobility management

- Mobility management could be based on Mobile IP which is standard in IPv6 and has good **scalability** properties:
  - Each node has a home address that is consistent with its home network.
  - When it is in a foreign network it has a foreign address, while a home agent (a router in the home network) intercepts messages towards the node and forwards them to the foreign address.
- Scalability could be further improved by exploiting group mobility – the fact that things move in groups[17]. This could be used to achieve more accurate location information about nodes.
- However,
  - 6LOWPAN does not implement MobileIPv6
  - The addressing schemes for RFIDs we have discussed do not support mobility.

[17] L. Galluccio, et al., "On the Potentials of Object Group Localization in the Internet of Things", *IEEE WoWMoM 2011*, 2011.

Naming

- In the Internet the address of a node is obtained by querying a Domain Name Server (it translates a logical name into an IP address).
- Analogously, in the IoT an Object Name Server (ONS) is needed to associate a reference to a description of the object (e.g., an URL) and the RFID tag identifier:
- The service that returns the RFID tag identifier of an object with specific characteristics is not straightforward. It is called Object Code Mapping Service (OCMS).
- Solutions for OCMS have been proposed based on a *peer-to-peer* approach[18], *however, their effectiveness in real IoT scenarios has not be demonstrated, yet!*

[18] V. Krylov, et al., "EPC Object Code Mapping Service Software Architecture: Web Approach", *MERA Networks Publications*, 2008.

Transport protocol

- Most IoT applications require reliability → **Use TCP**!
- However,
  - *TCP implements a connection setup*. Most IoT applications exchange a small amount of data → Connection setup introduce too much of overhead.
  - *TCP implements congestion control*. IoT involves
    - ⋆ wireless communications → TCP performance decrease.
    - ⋆ exchange of small amount of data → congestion control is not effective.
  - *TCP receiver buffers data to support ordered data delivery*. Most of the IoT nodes will be battery-less, management of receiver buffer might be too costly.
- **Alternatives to TCP are required!**
- Note that most of IoT applications will be based on web service → HTTP over UDP has been proposed. However,
  - Reliability must be supported at the application layer: it does not solve the problem of data buffering.
  - Congestion control is needed (and not performed if UDP is applied) → network congestion!

Traffic characterization and QoS support

- Characteristics of traffic generated by sensor networks strongly depends on the specific application scenario[19].
  - It was not a problem because traffic was confined to the sensor network.
- Deployment of large scale distributed RFID systems is at the beginning: traffic characteristics have not been studied so far.
- $\longrightarrow$ **IoT traffic is completely unknown!**
- Furthermore, appropriate solutions are required to identify QoS requirements and design schemes for QoS support.

[19] *For example see:* I. Demirkol, et al., "Wireless Sensor Networks for Intrusion Detection: Packet Traffic Modeling", *IEEE Communication Letters*, 2006.

Security

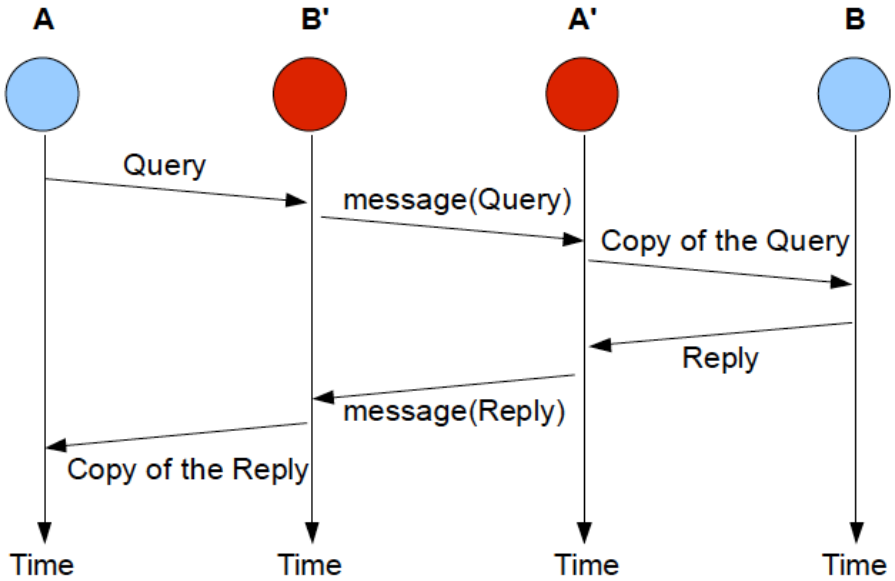
IoT is extremely vulnerable to attacks for the following reasons:

- IoT components spend most of their time **unattended** $\longrightarrow$ it is easy to physically attack them.
- IoT communications are **wireless** $\longrightarrow$ eavesdropping is very simple.
- IoT components are **limited** in terms of both energy and computing capabilities $\longrightarrow$ they cannot implement complex schemes supporting security.

Man-in-the-middle attack

- **Objective**: At the end a reader A believes that the tag B is in its proximity.
- The attacker deploys two nodes:
  - The leach (say A') near B.
  - The ghost (say B') near A.
- The ghost, B', forwards the signal generated by A to the leach, A'.
- A' sends towards the target tag B.
- A' sends the reflection generated by B to the ghost B'.
- B' sends the reflected message to A.

Example



Note that A' and B' are not aware of the meaning of the signals they transmit/receive.

Solutions to the man-in-the-middle attack

Proposed solutions

1. Authenticating gestures:
   - People execute certain sequences of gestures when RFID tags must be recognized.
   - A tag (mounting MEMS) transmits only if such sequence is recognized.
     - Application-specific & RFID tag cost increases
2. Bounding reader-tag distance:
   - Readers authenticate the tag only if the delay is below a threshold.
     - Attention to interactions with MAC.
3. Hiding signals:
   - The reader transmits pseudonoise (not of a tone) $\longrightarrow$ the reply by the tag is noise-like.
     - Energy inefficient.

Our solution

- The reader transmits the signal $c^*(t)$ which is given by:

$$c^*(t) = c(t) + c^{(\text{Modulated})}(t) \quad (1)$$

  where $c(t)$ is the tone generated according to the standard **and** $c^{(\text{Modulated})}(t)$ is obtained modulating $c(t)$ with a random sequence of bits in standard way.
- The reader demodulates the signal transmitted by tags accordingly.
- The delay introduced by the exchange between the ghost and the leach deteriorates demodulation performance at n_{False}.

Privacy

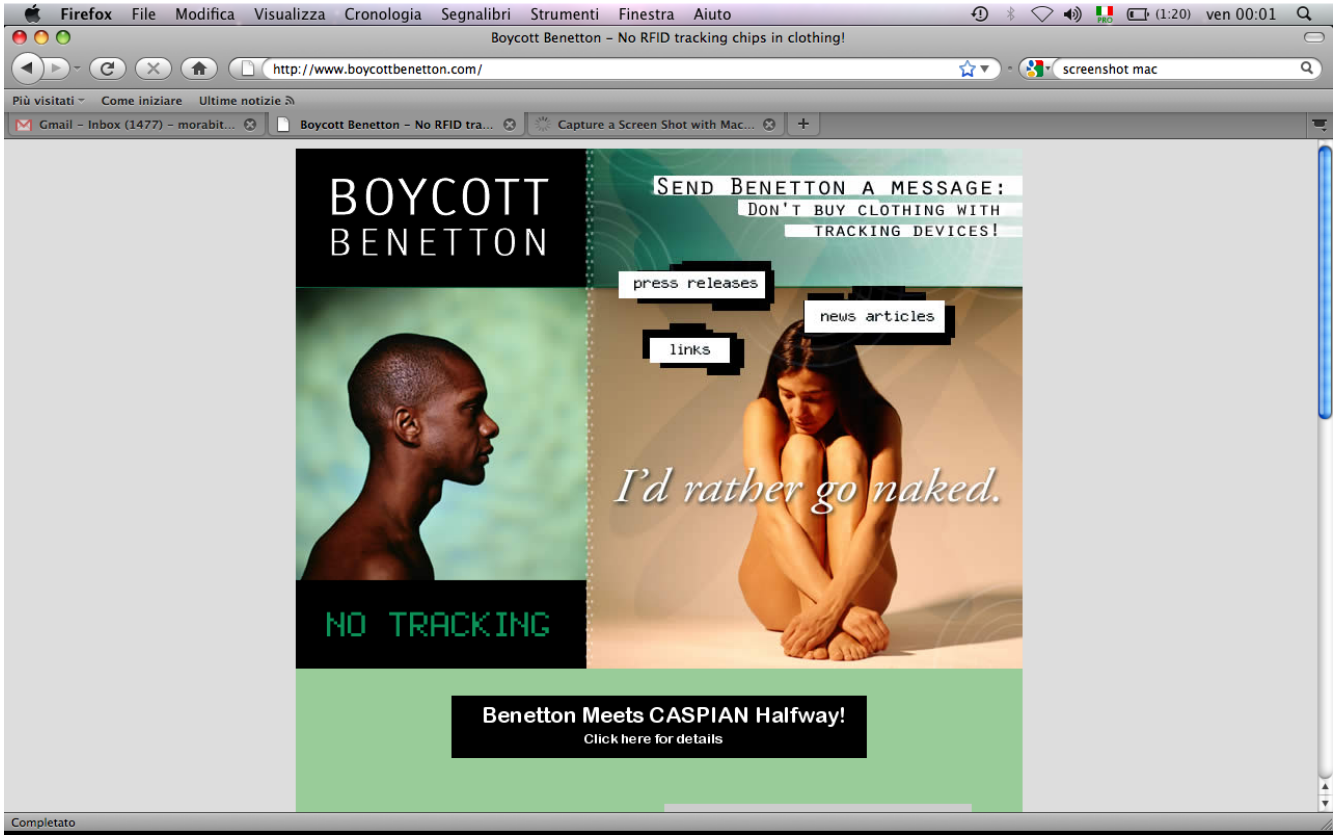


Figure: Boycott Benetton: a spontaneous group of people opposing the deployment of RFID tags in the new line of Benetton clothes.

Privacy issues

- In IoT privacy of non IoT users is menaced as well (differently from the case of traditional Internet).
- Countless number of occasions for personal data to be collected $\longrightarrow$ It is **impossible to control the disclosure of personal information**.
  - **Solutions in WSN domain**: reduce the ability of WSN to collect data at a detail which could compromise privacy[20].
  - **Solutions in RFID domain**: To avoid unauthorized readings of RFID tags a system is deployed that creates collisions with such RFID tags[21].
- Cost of information storage is approaching 10^{-9} euro per byte $\longrightarrow$ information will be retained indefinitely $\longrightarrow$ **denial of digital forgetting**.

[20] J. Wickramasuriya, et al., Privacy protecting data collection in media spaces, *ACM Int. Conf. on Multimedia*, 2004.

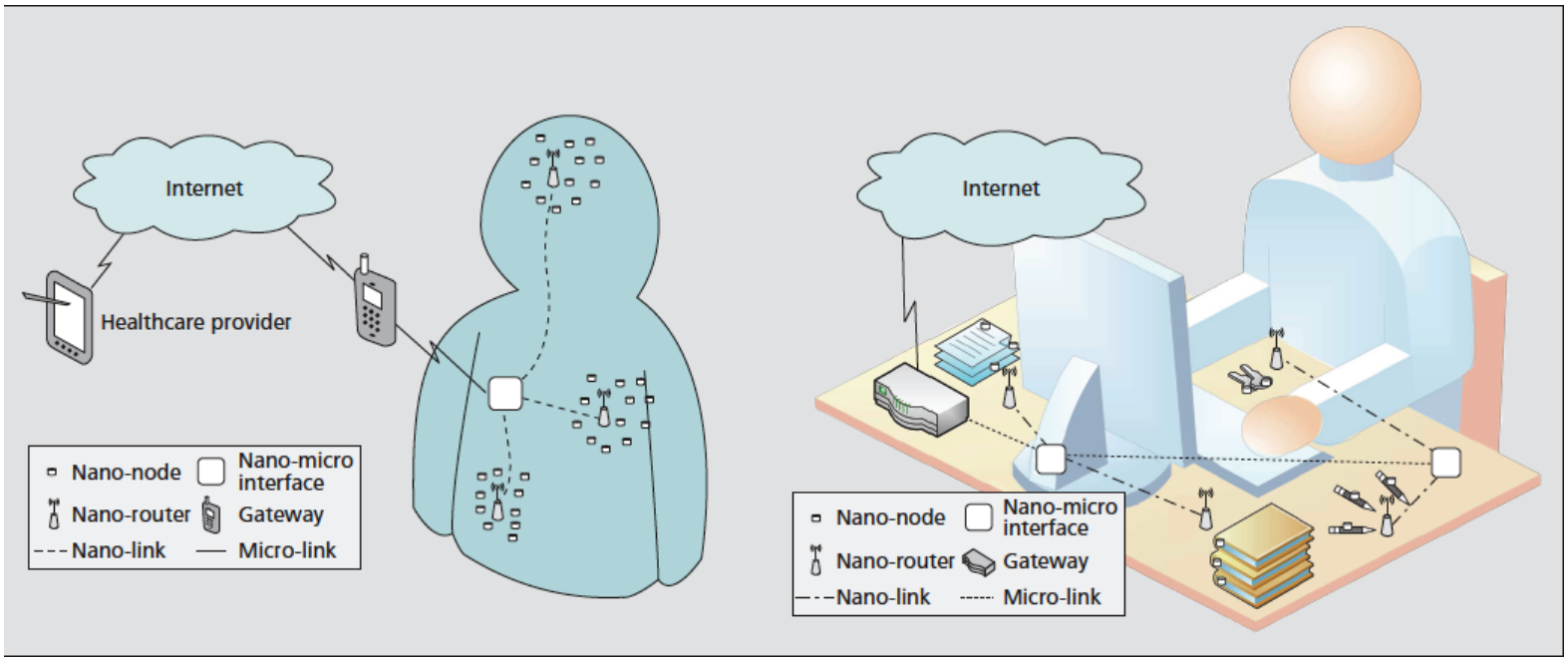
[21] O. Savry et al., Security and privacy protection of contactless devices. *TIWDC 2009*. September 2009.ssss

Summary

Open issue	Brief description of the cause
Standards	There are several standardization efforts but they are not integrated in a comprehensive framework
Mobility support	There are several proposals for object addressing but none for mobility support in the IoT scenario, where scalability and adaptability to heterogeneous technologies represent crucial problems
Naming	Object Name Servers (ONS) 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
Authentication	Authentication is difficult in the IoT as it requires appropriate authentication infrastructures that will not be available in IoT scenarios. Furthermore, things have scarce resources when compared to current communication and computing devices. Also man-in-the-middle attack is a serious problem
Data integrity	This is usually ensured by protecting data with passwords. However, the password lengths supported by IoT technologies are in most cases too short to provide strong levels of protection
Privacy	A lot of private information about a person can be collected without the person being aware. Control on the diffusion of all such information is impossible with current techniques
Digital forgetting	All the information collected about a person by the IoT may be retained indefinitely as the cost of storage decreases. Also data mining techniques can be used to easily retrieve any information even after several years

6. Interesting activities

Internet of Nanothings



- Integrating nanomachine in the IoT $\rightarrow$ the Internet of Nanothings [22].
- A lot of research problems spanning all layers of the protocol stack.

[22] I. F. Akyildiz et al., "The Internet of Nanothings", *IEEE Wireless Communications*, December 2010.

Novel types of communication nodes

- New types of communication nodes are being introduced
  - E.g., transmitting only nodes,

Example (Energy Harvesting Active Networked Tag – EnHANT)

- **Network**: EnHANT actively communicate with each others (WISP did not!).
- **Operate at ultra-low-power**: They spend a few nano-Joules or less on every communicated bit.
- **Harvest environmental energy**: Collect and store energy from source such as light, motion and temperature.
- **Adapt to energy availability**: Communications and networking algorithms adapt to energy and harvesting contraint.
- **Transmit over short range**: Communicate only when in close proximity (1–10 meters) to one another.
- **Are thin, flexible and small**: They measure a few square centimeters – at most.

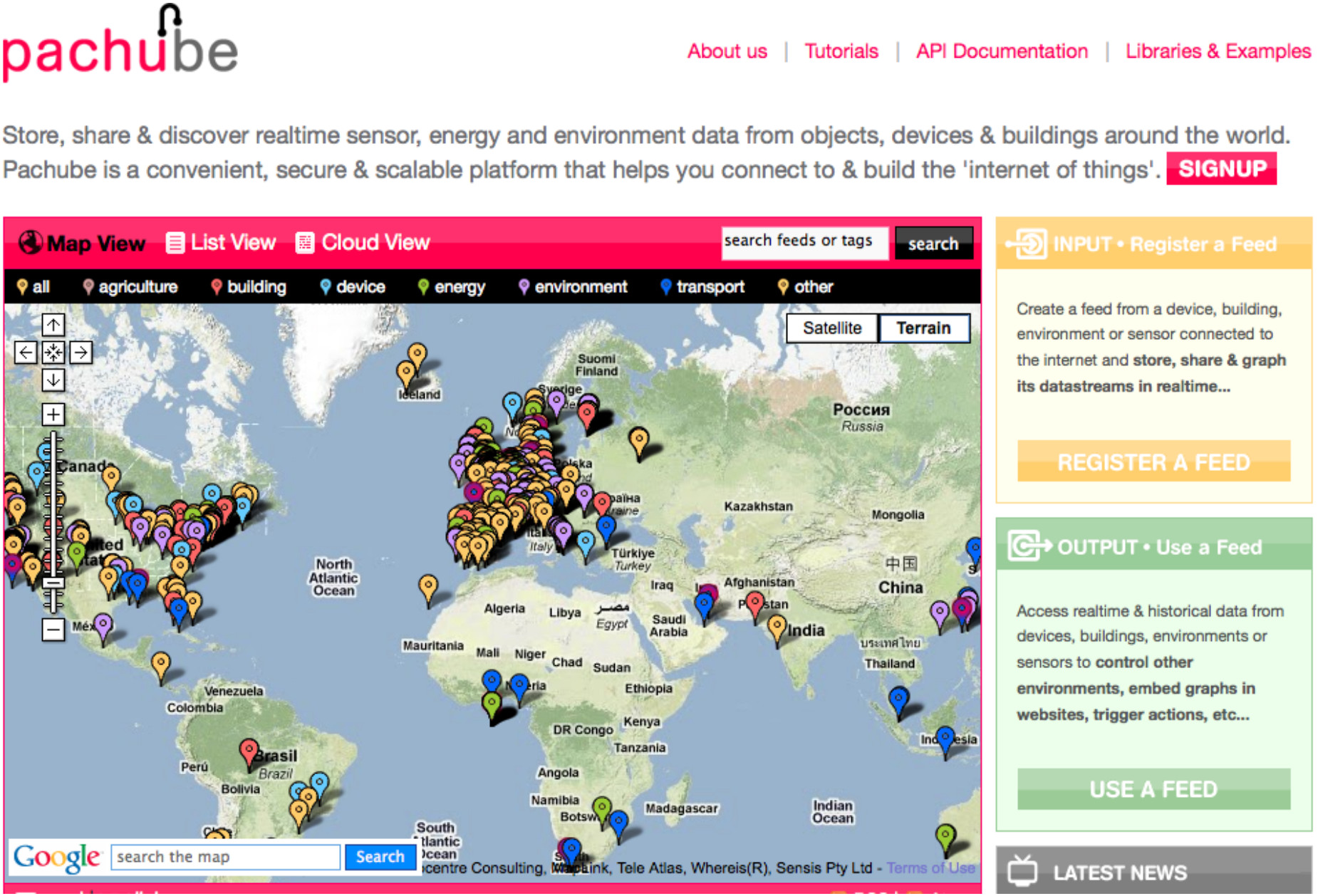


Figure: Collection of sensors sharing measured data.

7. Conclusions

Three pieces of good news

1. Growing interest in the industrial and academic research community
2. Large investments (in Italy and Europe within the framework of the Future Internet)
3. A lot of open research issues (and only a few publications to date)