Chapter 16: The Internet of Things: A survey

Department of Computer Science
And Information Engineering
National Taipei University

Outline

- Introduction
- One paradigm, many vision
- Enabling technologies
  - Identification, sensing and communication technologies
  - Middleware
- Applications
- Open issues
- Conclusions

Introduction

- The Internet of Things (IoT) is the basic idea of this concept is the pervasive presence around us of a variety of things or objects – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals .
- From the point of view of a private user, the most obvious effects of the IoT introduction will be visible in both working and domestic fields. In this context, domotics, assisted living, e-health, enhanced learning are only a few examples of possible application.
- Similarly, from the perspective of business users, the most apparent consequences will be equally visible in fields such as, automation and industrial manufacturing, logistics, business/process management, intelligent transportation of people and goods.

Cont.

- Also, the IoT idea poses several new problems concerning the networking aspects. In fact, the things composing the IoT will be characterized by low resources in terms of both computation and energy capacity

- Accordingly, the proposed solutions need to pay special attention to resource efficiency besides the obvious scalability problems.

One paradigm, many visions

- The reason of today apparent fuzziness around this term is a consequence of the name ‘‘Internet of Things” itself, which syntactically is composed of two terms. The first one pushes towards a network oriented vision of IoT, while the second one moves the focus on generic ‘‘objects” to be integrated into a common framework.
- Differences, sometimes substantial, in the IoT visions raise from the fact that stakeholders, business alliances, research and standardization bodies start approaching the issue from either an ‘‘Internet oriented” or a ‘‘Things oriented” perspective, depending on their specific interests, finalities and backgrounds.
- The object unique addressing and the representation and storing of the exchanged information become the most challenging issues, bringing directly to a third, ‘‘Semantic oriented”, perspective of IoT.

Cont.

- In Fig. 1 from such an illustration, it clearly appears that the IoT paradigm shall be the result of the convergence of the three main visions addressed above.

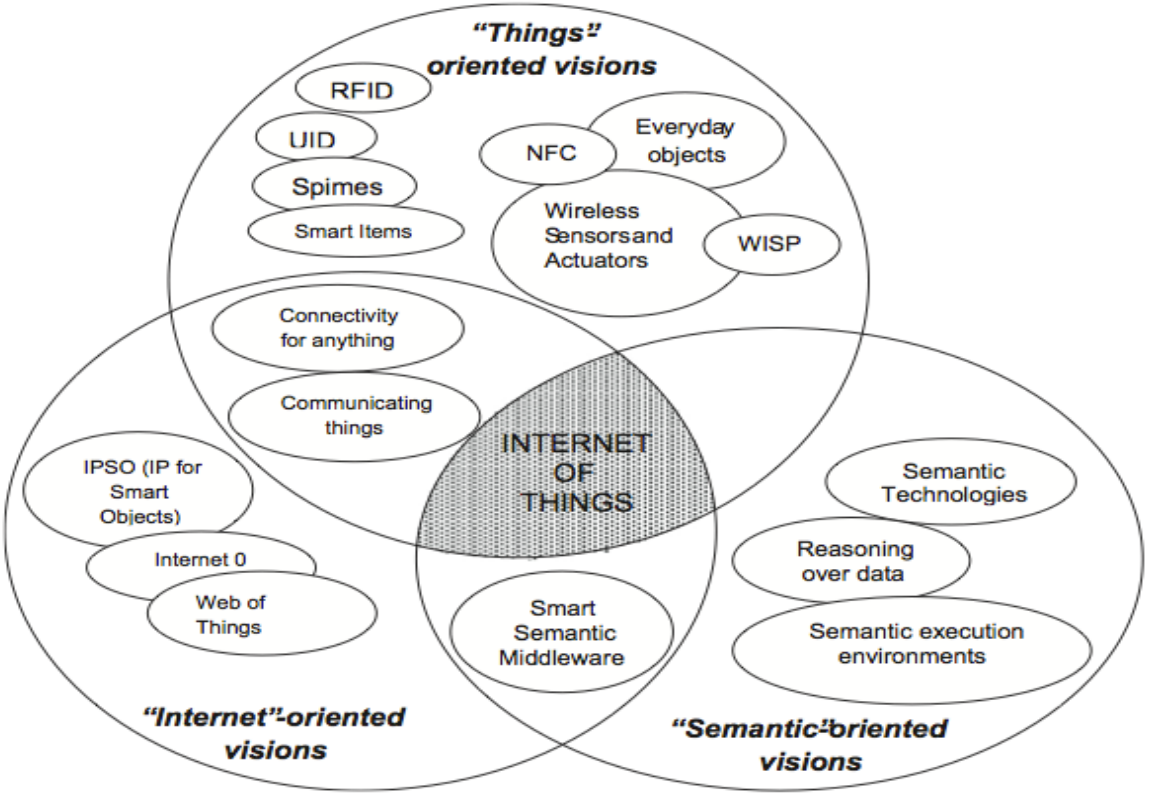


Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

Cont.

- A world-wide network of academic research laboratories in the field of networked RFID and emerging sensing technologies Their focus has primarily been on the development of the Electronic Product CodeTM (EPC) to support the spread use of RFID in world-wide modern trading networks, and to create the industry-driven global standards for the EPCglobal NetworkTM

- In a broader sense, IoT cannot be just a global EPC system in which the only objects are RFIDs; they are just a part of the full story!

Cont.

- RFID still stands at the forefront of the technologies driving the vision. This a consequence of the RFID maturity, low cost, and strong support from the business community.
- However, they state that a wide portfolio of device, network, and service technologies will eventually build up the IoT.
- According to the IPSO vision, the IP stack is a light protocol that already connects a huge amount of communicating devices and runs on tiny and battery operated embedded devices.
- Therefore, issues related to how to represent, store, interconnect, search, and organize information generated by the IoT will become very challenging.

Identification, sensing and communication technologies

- In this context, key components of the IoT will be RFID systems, which are composed of one or more reader(s) and several RFID tags. Tags are characterized by a unique identifier and are applied to objects.
- Accordingly, RFID systems can be used to monitor objects in real-time, without the need of being in line-of-sight; this allows for mapping the real world into the virtual world.
- Therefore, they can be used in an incredibly wide range of application scenarios, spanning from logistics to e-health and security.

- Usually, RFID tags are passive, i.e., they do not have onboard power supplies and harvest the energy required for transmitting their ID from the query signal transmitted by a RFID reader in the proximity.

Cont.

- Nevertheless, there are also RFID tags getting power supply by batteries. In this case we can distinguish semi-passive from active RFID tags. In semi-passive RFIDs batteries power the microchip while receiving the signal from the reader.
- Differently, in active RFIDs the battery powers the transmission of the signal as well. Obviously the radio coverage is the highest for active tags even if this is achieved at the expenses of higher production costs.
- Sensor networks will also play a crucial role in the IoT. In fact, they can cooperate with RFID systems to better track the status of things, i.e., their location, temperature, movements, etc.

Cont.

- Today, most of commercial wireless sensor network solutions are based on the IEEE 802.15.4 standard, which defines the physical and MAC layers for low-power, low bit rate communications in wireless personal area networks.This is a difficult task for several reasons, the most important are given below:
  - Sensor networks may consist of a very large number of nodes. This would result in obvious problems as today there is a scarce availability of IP addresses.
  - The largest physical layer packet in IEEE 802.15.4 has 127 bytes; the resulting maximum frame size at the media access control layer is 102 octets, which may further decrease based on the link layer security algorithm utilized. Such sizes are too small when compared to typical IP packet sizes.
  - In many scenarios sensor nodes spend a large part of their time in a sleep mode to save energy and cannot communicate during these periods. This is absolutely anomalous for IP networks.

Cont.

- Table 1 compares the characteristics of RFID systems (RFID), wireless sensor networks (WSN), and RFID sensor networks (RSN) . Observe that the major advantages of:
  - RFID systems are the very small size and the very low cost. Furthermore, their lifetime is not limited by the battery duration
  - wireless sensor networks are the high radio coverage and the communication paradigm, which does not require the presence of a reader
  - RFID sensor network are the possibility of supporting sensing, computing, and communication capabilities in a passive system.

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

Middleware

- As it is happening in other contexts, the middleware architectures proposed in the last years for the IoT often follow the Service Oriented Architecture (SOA) approach. The adoption of the SOA principles allows for decomposing complex and monolithic systems into applications consisting of an ecosystem of simpler and well-defined components.
- A SOA approach also allows for software and hardware reusing, because it does not impose a specific technology for the service implementation

Cont.

- Applications
  - Applications are on the top of the architecture, exporting all the system's functionalities to the final user. Indeed, this layer is not considered to be part of the middleware but exploits all the functionalities of the middleware layer.

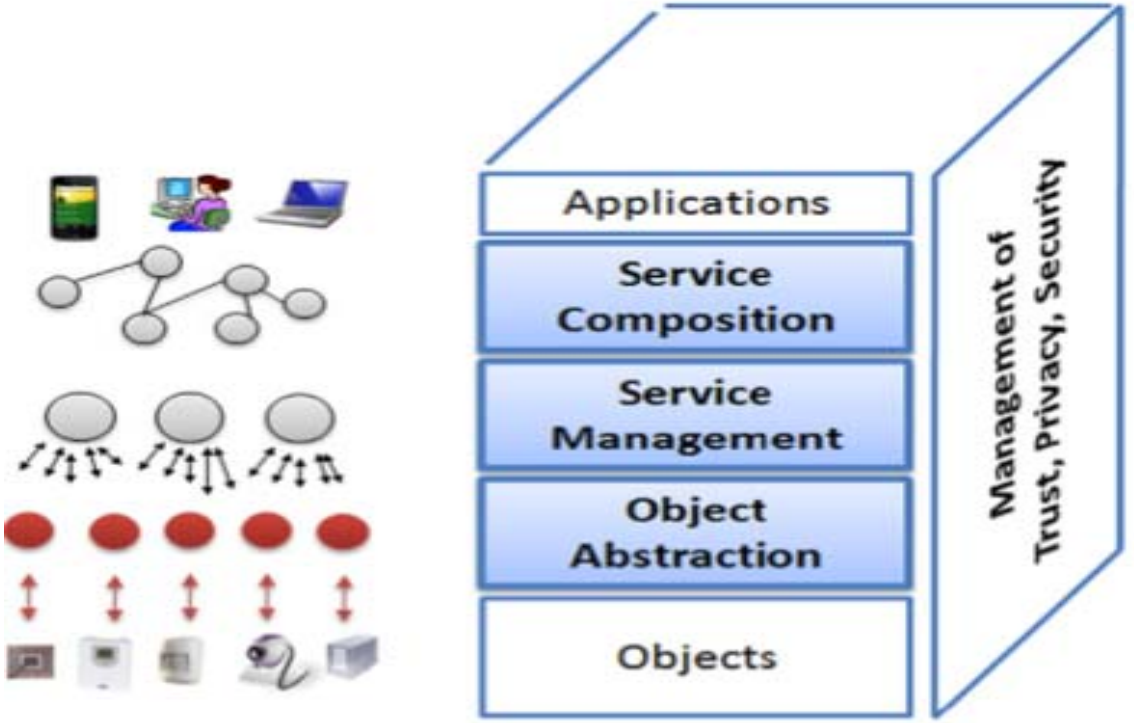


Fig. 2. SOA-based architecture for the IoT middleware.

Cont.

- Service composition
  - This is a common layer on top of a SOA-based middleware architecture. It provides the functionalities for the composition of single services offered by networked objects to build specific applications.

- 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.
  - A basic set of services encompasses: object dynamic discovery, status monitoring, and service configuration.
  - This layer might enable the remote deployment of new services during run-time, in order to satisfy application needs. A service repository is built at this layer so as to know which is the catalogue of services that are associated to each object in the network.

Cont.

- Object abstraction
  - The IoT relies on a vast and heterogeneous set of objects, each one providing specific functions accessible through its own dialect. There is thus the need for an abstraction layer capable of harmonizing the access to the different devices with a common language and procedure.
  - However, more often this wrapping function is provided through a proxy, which is then responsible to open a communication socket with the device's console and send all the commands to it by using different communication languages. It can reduce the complexity of the operations required by the end-device.

- Trust, privacy and security management
  - The middleware must then include functions related to the management of the trust, privacy and security of all the exchanged data.
  - The related functions may be either built on one specific layer of the previous ones distributed through the entire stack, in a manner that does not affect system performance or introduce excessive overheads.

Applications

- Many are the domains and the environments in which new applications would likely improve the quality of our lives: at home, while travelling, when sick, at work, when jogging and at the gym.

- Where a very wide range of applications can be deployed. These can be grouped into the following domains:
  - Transportation and logistics domain.
  - Healthcare domain.
  - Smart environment (home, office, plant) domain.
  - Personal and social domain.

- Among the possible applications, we may distinguish between those either directly applicable or closer to our current living habitudes and those futuristic, which we can only fancy of at the moment, since the technologies and/or our societies are not ready for their deployment

Transportation and logistics domain

- Advanced cars, trains, buses as well as bicycles along with roads and /or rails are becoming more instrumented with sensors, actuators, and processing power. Below, the main applications in the transportation and logistics domain are described.

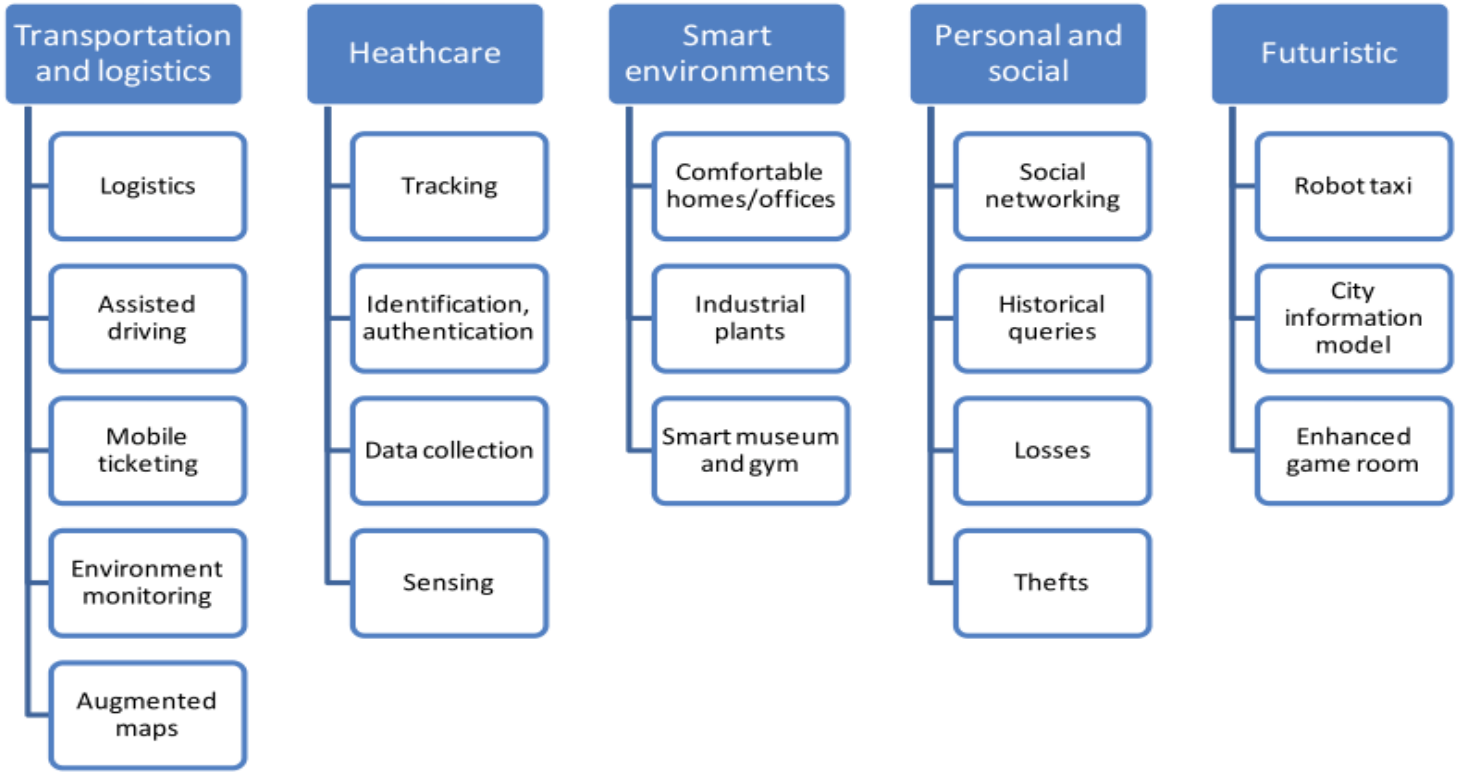


Fig. 3. Applications domains and relevant major scenarios.

Cont.

- Logistics
  - It is also possible to obtain products related information, promptly, timely, and accurately so that enterprises or even the whole supply chain can respond to intricate and changeable markets in the shortest time.
- Assisted driving
  - Cars, trains, and buses along with the roads and the rails equipped with sensors, actuators and processing power may provide important information to the driver and/or passengers of a car to allow better navigation and safety.
- Mobile ticketing
  - Posters or panels providing information about transportation services can be equipped with an NFC tag, a visual marker, and a numeric identifier.
- Monitoring environmental parameters
  - During the transportation the conservation status need to be monitored to avoid uncertainty in quality levels for distribution decisions.
- Augmented maps
  - Touristic maps can be equipped with tags that allow NFC-equipped phones to browse it and automatically call web services providing information

Healthcare domain

■ Many are the benefits provided by the IoT technologies to the healthcare domain and the resulting applications can be grouped mostly into: tracking of objects and people , identification and authentication of people, automatic data collection and sensing.

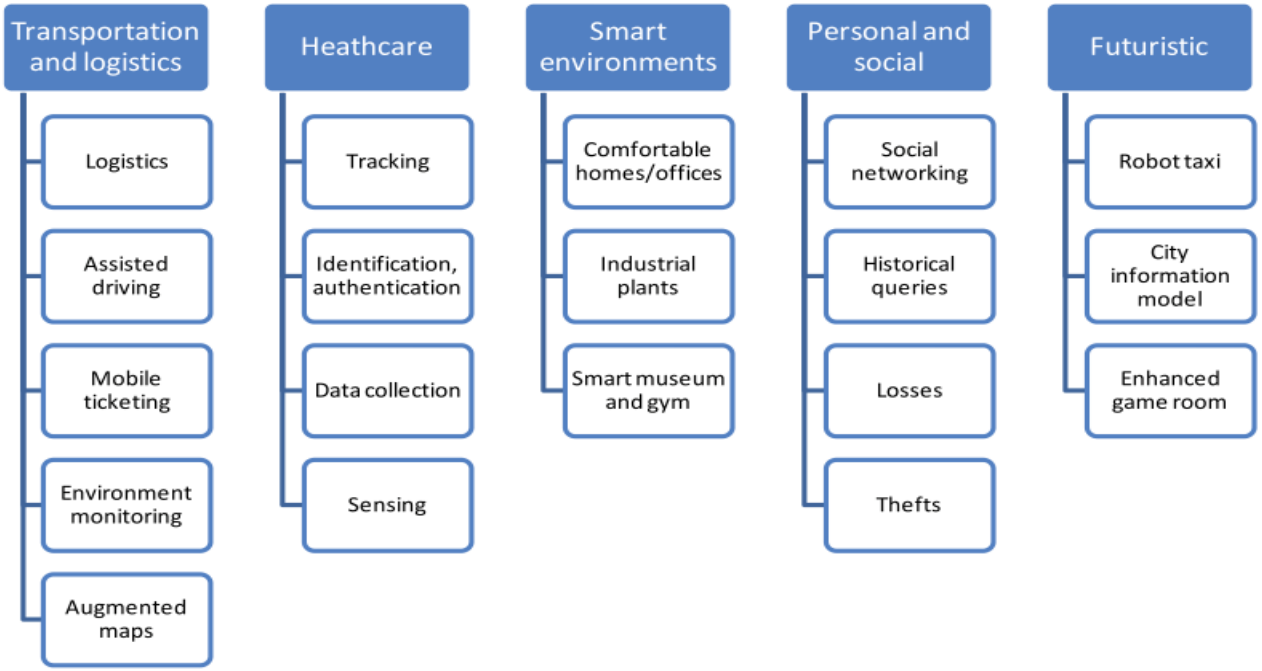


Fig. 3. Applications domains and relevant major scenarios.

Cont.

- Tracking
  - Tracking is the function aimed at the identification of a person or object in motion. This includes both real-time position tracking, such as the case of patient-flow monitoring to improve workflow in hospitals
- Identification and authentication
  - It includes patient identification to reduce incidents harmful to patients, comprehensive and current electronic medical record maintenance, and infant identification in hospitals to prevent mismatching.
- Data collection
  - Automatic data collection and transfer is mostly aimed at reducing form processing time, process automation, automated care and procedure auditing, and medical inventory management.
- Sensing
  - Sensor devices enable function centered on patients, and in particular on diagnosing patient conditions, providing real-time information on patient health indicators.

Smart environments domain

- A smart environment is that making its ‘‘employment” easy and comfortable thanks to the intelligence of contained objects, be it an office, a home, an industrial plant, or a leisure environment.

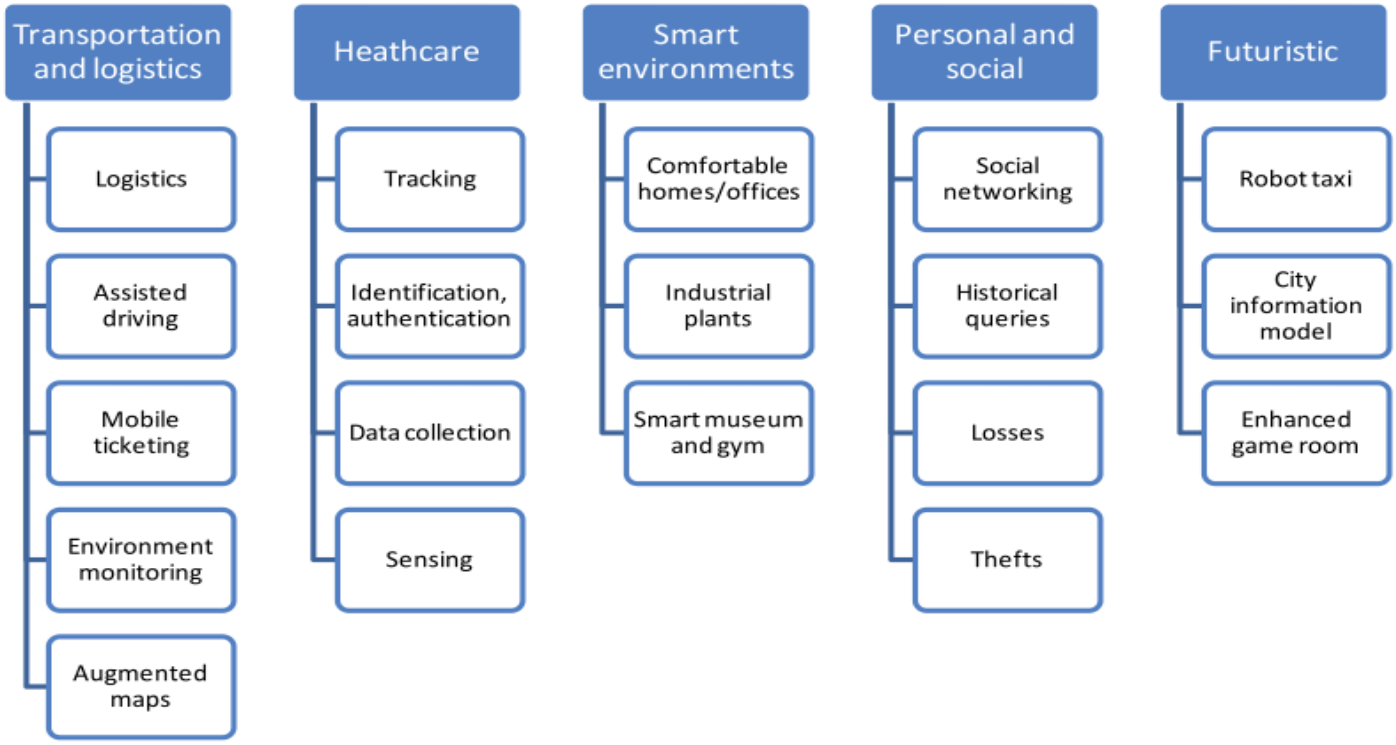


Fig. 3. Applications domains and relevant major scenarios.

Cont.

- Comfortable homes and offices
  - Sensors and actuators distributed in houses and offices can make our life more comfortable in several aspects: rooms heating can be adapted to our preferences and to the weather; the room lighting can change according to the time of the day
- Industrial plants
  - Smart environments also help in improving the automation in industrial plants with a massive deployment of RFID tags associated to the production parts.

    The plant manager also immediately sees the status of the so called Enterprise Resource Planning (ERP) orders, the production progress, the device status.
- Smart museum and gym
  - In the gym, the personal trainer can upload the exercise profile into the training machine for each trainee, who is then automatically recognized by the machine through the RFID tag.
  - In the museum, for instance, expositions in the building may evoke various historical periods (Egyptian period or ice age) with widely diverging climate conditions.

Personal and social domain

- The applications falling in this domain are those that enable the user to interact with other people to maintain and build social relationships.
- Indeed, things may automatically trigger the transmission of messages to friends to allow them to know what we are doing or what we have done in the past, such as moving from/to our house/office, travelling, meeting some common mates or playing soccer

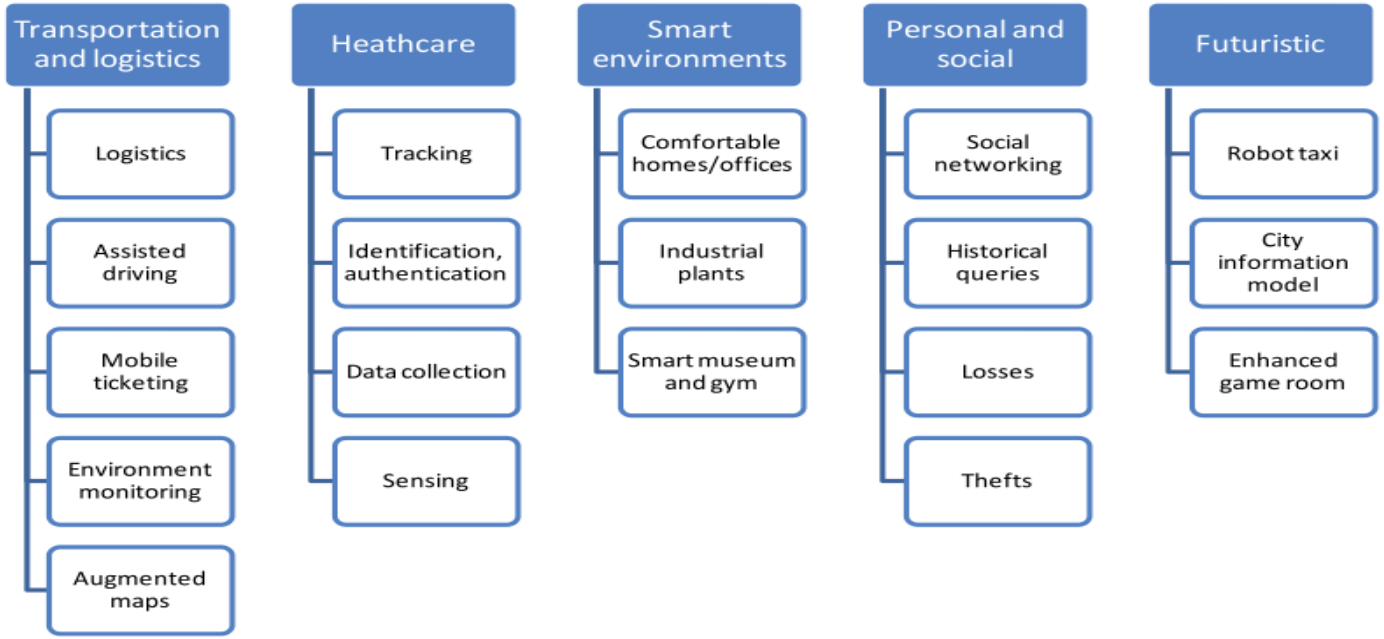


Fig. 3. Applications domains and relevant major scenarios.

Cont.

- Social networking
  - This application is related to the automatic update of information about our social activities in social networking web portals, such as Twitter and Plazes.
- Historical queries
  - A digital diary application can be built that records and displays events for example in a Google Calendar for later perusal. This way, users can look back over their diaries to see how and with whom they've spent their time.
- Losses
  - The simplest web-based RFID application is a search engine for things that lets users view the last recorded location for their tagged objects or search for a particular object's location.
- Thefts
  - An application similar to the previous one may allow the user to know if some objects are moved from a restricted area, which would indicate that the object is being stolen.

Futuristic applications domain

- The applications described in the previous sections are realistic as they either have been already deployed or can be implemented in a short/medium period since the required technologies are already available.

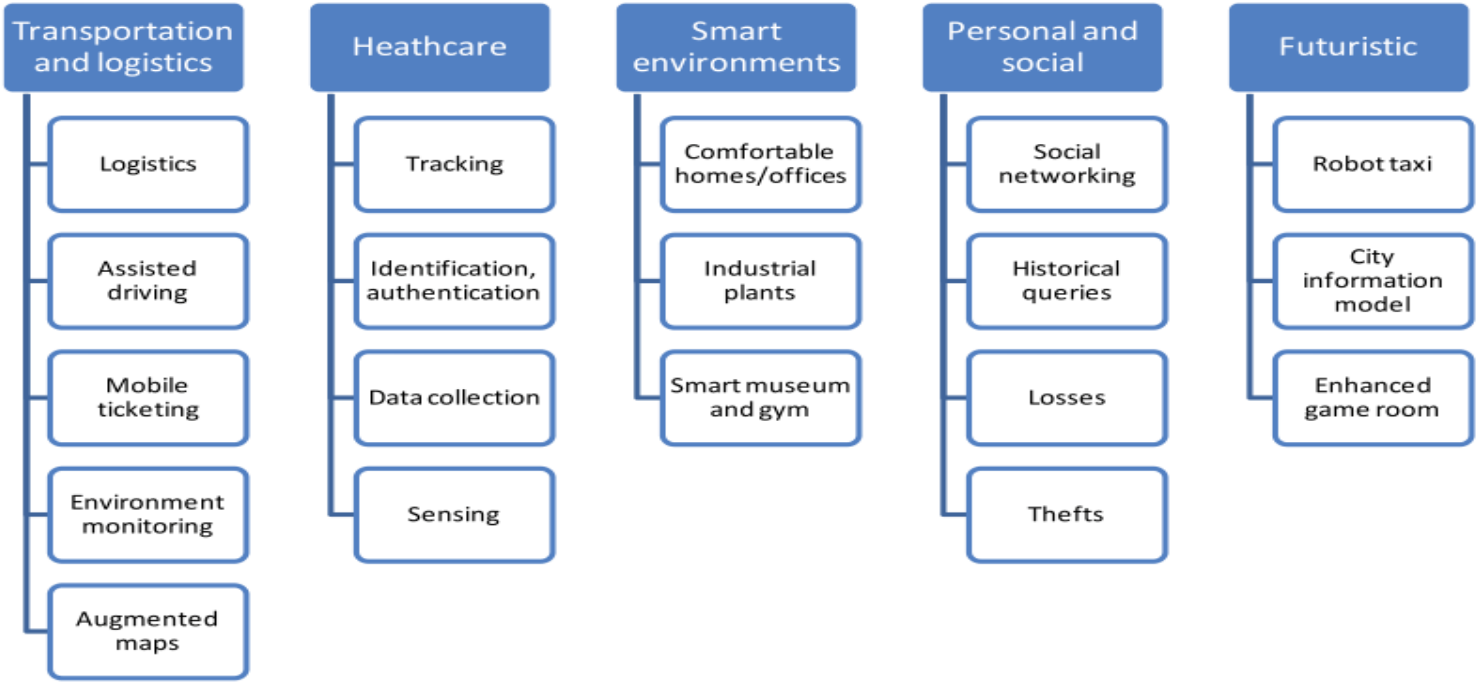


Fig. 3. Applications domains and relevant major scenarios.

Cont.

- Robot taxi
  - The user's location is automatically tracked via GPS and enables users to request a taxi to be at a certain location at a particular time by just pointing it out on a detailed map.
- City information model
  - The idea of a City Information Model (CIM) is based on the concept that the status and performance of each buildings and urban fabrics – such as pedestrian walkways, cycle paths and heavier infrastructure like sewers, rail lines, and bus corridors – are continuously monitored by the city government operates and made available to third parties via a series of APIs, even though some information is confidential.
- Enhanced game room
  - The enhanced game room as well as the players are equipped with a variety of devices to sense location, movement, acceleration, humidity, temperature, noise, voice, visual information, heart rate and blood pressure. Their controller recognizes RFID tags on objects in the room. As the game progresses, the system gradually makes it more difficult.

Open issues

- In this section, we firstly review the standardization activities that are being carried out on different IoT-related technologies.

- More specifically, we focus on addressing and networking issues, whereas we describe the problems related to security and privacy.

Standardization activity

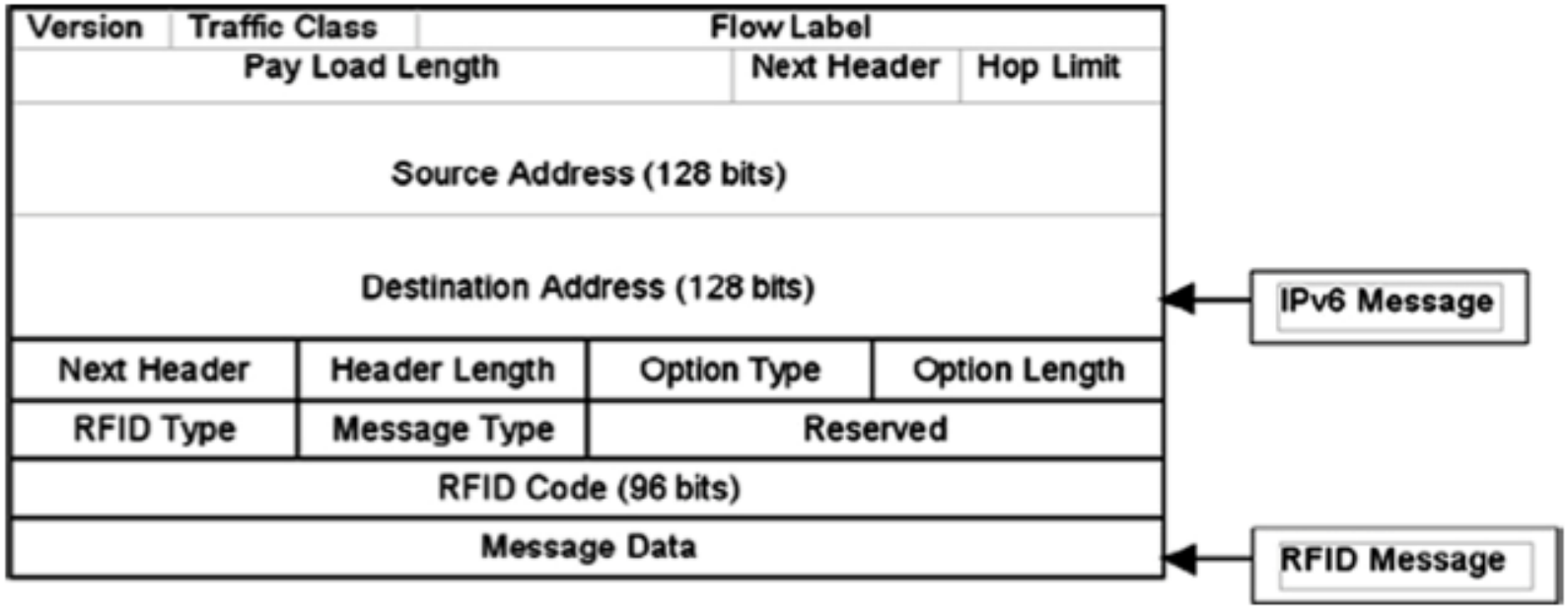
- RFID frequency and readers-tags communication protocols, data formats placed on tags and labels. The major standardization bodies dealing with RFID systems are EPCglobal, ETSI, and ISO.
- More specifically, EPCglobal is a subsidiary of the global not-for-profit standards organization GS1. It mainly aims at supporting the global adoption of a unique identifier for each tag, which is called Electronic Product Code (EPC), and related industry-driven standards.
- In fact ETSI (the European Telecommunications Standards Institute) the Machine-to-Machine (M2M) Technical Committee was launched, to the purpose of conducting standardization activities relevant to M2M systems and sensor networks
- According to it, the integration of different things into wider networks, either mobile or fixed, will allow their interconnection with the Future Internet

Addressing and networking issues

- 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. Therefore, it is clear that other addressing policies should be used other than that utilized by IPv4.
- IPv6 addressing has been proposed for low-power wireless communication nodes .However, since RFID tags use 64–96 bit identifiers, as standardized by EPCglobal, solutions are required for enabling the addressing of RFID tags into IPv6 networks.
- Recently, integration of RFID tags into IPv6 networks has been investigated and methodologies to integrate RFID identifiers and IPv6 addresses have been proposed.
- A new IPv6 packet will be created. Its payload will contain the message generated by the tag, whereas its source address will be created by concatenating the gateway ID and the RFID tag identifier.

Cont.

- Where the RFID message and headers are included into the IPv6 packet payload as shown in Fig



Cont.

- In the traditional Internet, the protocol utilized at the transport layer for reliable communications is the Transmission Control Protocol (TCP). It is obvious that TCP is inadequate for the IoT, due to the following reasons:
  - Connection setup:
    - TCP is connection oriented with a connection setup procedure This is unnecessary, given that most of the communications within the IoT will involve the exchange of a small amount of data and, therefore, the setup phase would last for a considerable portion of the session time.
  - Congestion control:
    - if the amount of data to be exchanged in a single session is very small, TCP congestion control is useless, given that the whole TCP session will be concluded with the transmission of the first segment and the consequent reception of the corresponding acknowledgement.
  - Data buffering:
    - TCP requires data to be stored in a memory buffer both at the source and at the destination. In fact, at the source data should be buffered so that it can be retransmitted in case it is lost.

Security

- Public concerns are indeed likely to focus on a certain number of security and privacy issues
- The IoT is extremely vulnerable to attacks for several reasons. First, often its components spend most of the time unattended; and thus, it is easy to physically attack them. Second, most of the communications are wireless, which makes eavesdropping extremely simple.
- More specifically, the major problems related to security concern authentication and data integrity. 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 last few years, some solutions have been proposed for RFID systems, however, they all have serious problems

Cont.

- Finally, none of the existing solutions can help in solving the proxy attack problem, also known as the man-in-the-middle attack. Consider the case in which a node is utilized to identify something or someone and, accordingly, provides access to a certain service or a certain area

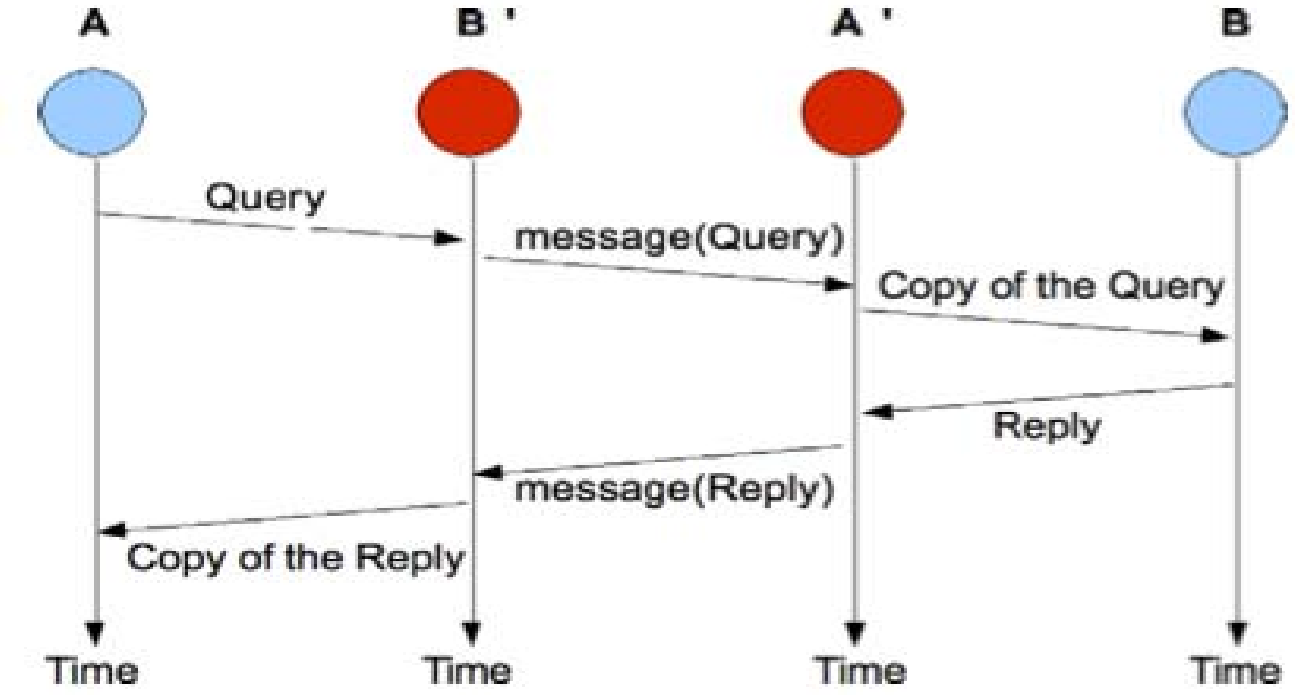


Fig. 5. Man in the middle attack.

Cont.

- Finally, please note that that all the solutions proposed to support security use some cryptographic methodologies. Typical cryptographic algorithms spend large amount of resources in terms of energy and bandwidth both at the source and the destination. Such solutions cannot be applied to the IoT, given that they will include elements that are seriously constrained in terms of energy, communications, and computation capabilities.

Privacy

- The concept of privacy is deeply rooted into our civilizations.People concerns about privacy are indeed well justified ,In fact, the ways in which data collection, mining, and provisioning will be accomplished in the IoT .Therefore, for human individuals it will be impossible to personally control the disclosure of their personal information.
- Accordingly, 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.
- Furthermore, the personal data collected should be used only in the aim of supporting authorized services by authorized service providers.
- For example, consider the application scenario regarding Comfortable homes and offices described, and focus on the case of a building where several offices are located.

Cont.

- In this case, some sensing capabilities will be deployed in the environment to track position of people and control the lighting or heating accordingly appropriate to protect privacy should be applied guaranteeing that:
  - the tracking system does not collect information about the position and movements of individual users but only considers aggregate users;
  - people are informed of the scope and the way in which their movements are tracked by the system
  - data collected by the tracking system should be processed for the purposes of controlling the lighting and heating and then deleted by the storage system.

Cont.

- To handle the data collection process appropriate solutions are needed in all the different subsystems interacting with human beings in the IoT.
- The problem becomes impossible to be solved in the case of sensor networks. In fact, individuals entering in an area where a sensor network is deployed cannot control what information is being collected about themselves. In this case, images of people can be blurred in order to protect their privacy.
- To fix this problem, there is a new family of solutions in which the signal transmitted by the reader has the form of a pseudo-noise. Such noisy signal is modulated by the RFID tags and therefore, its transmission cannot be detected by malicious readers.

Conclusions

- The IoT has the potential to add a new dimension to this process by enabling communications with and among smart objects, thus leading to the vision of ‘‘anytime, anywhere , anything” communications.
- In this perspective, the current trend, which we have highlighted , of assigning an IPv6 address to each IoT element so as to make it possible to reach them from any other node of the network, looks more suitable for the traditional Internet paradigm.
- Another interesting paradigm which is an evolution of the Web 2.0. It is aimed at integrating web and sensing technologies together so as to enrich the content provided to users. This is obtained by taking into account the information about the user context collected by the deployed in the user terminals.

Homework #16

1. Compares the characteristics of RFID systems (RFID), wireless sensor networks (WSN), and RFID sensor networks (RSN) .

2. Description the man-in-the-middle attack.