Chapter 1

Introduction to the Internet of Things

1.1. Introduction

The Internet of Things (IoT) is somehow a leading path to a smart world with ubiquitous computing and networking. It aims to make different tasks easier for users and provide other tasks, such as easy monitoring of different phenomena surrounding us. With ubiquitous computing, computing will be embedded everywhere and programmed to act automatically with no manual triggering; it will be omnipresent.

In the IoT, environmental and daily life items, also named "things", "objects", or "machines" are enhanced with computing and communication technology and join the communication framework. In this framework, wireless and wired technologies already provide the communication capabilities and interactions, meeting a variety of services based on person-to-person, person-to-machine, machine-to-person, machine-to-machine interactions and so on. These connected machines or objects/things will be new Internet or network users and will generate data traffic in the current or emerging Internet.

Chapter written by Hakima CHAOUCHI.

The Internet of Things: Connecting Objects to the Web Edited by Hakima Chaouchi

Connecting objects might be wireless, as with the radio frequency identification (RFID), or sensor radio technologies that offers, respectively, identification of items and sensing of the environment. Connection may be wired, as with power line communication (PLC). PLC offers data transport over electrical media and has pioneered the in-home networking connectivity of electronic consumer devices that we also name "objects" such as smart fridges, smart TVs, smart heaters, etc.

IoT-based services will provide more automation of various tasks around people and connected objects in order to build a smart world not only in manufacturing industries but also in the office, at home and everywhere. Most of these services will also rely on the easy location and tracking of connected objects. Other services – object-to-object-oriented services – will emerge for instance in the context of the green planet goal. This is where specific applications will monitor the environment and automatically react, for example, to minimize energy wastage or avoid natural disasters.

In the IoT, identifying, sensing and automatically deciding and actuating will be the main new functionalities that will enable ubiquitous computing and networking. Therefore, sensor and RFID, among other technologies, will be increasingly deployed and will thus allow integration of the real world environment in the networked services. In fact, billions of RFID tags and sensors are expected to connect billions of items/objects/things to the network in the coming years. Scalable identification, naming and addressing space and structure, scalable name resolution, scalable and secure data transfer are all of major concern. Other enabling technologies for this real-world networked service include nanotechnology, automatic processing and robotics, and probably newly-emerging technologies enabling the envisioned smart world to become real.

IoT will connect heterogenous devices and will be very dense, connecting billions of objects. An Internet-, IP- (Internet protocol) or TCP/IP (transport control protocol/Internet protocol) -based model stands at the centre of the IoT. It is one possible INTERNETworking solution to hide the ever-increasing heterogenity of networking technologies and communication systems in the ubiquitous environment envisioned. IP might not, however, support the resource limitation and scalability of the network.

IP or the Internet will certainly support the close-to-market IoT applications, but IoT research development will hopefully also come with a new INTERNETworking communication model and architecture. These will better support the new requirement of the heterogenity of objects, scalability (of billions of objects expected), limited resources of connecting objects and requirements related to new services and applications to be designed over this connected real world. It falls exactly under the post-IP or future Internet era [EUR 08, GEN 10, FIN 10], where several research projects are building a new communication model and architecture that is more adaptive to the requirements of a given network.

IoT is one network with new requirements related to the introduction of these nodes/objects with new technologies in the network. The existing TCP/IP model might be compatible with the emerging post-IP or future Internet model. While seeking the design of the IoT network and services, a rethinking of the basic concepts will emerge related to addressing, routing, scaling, guaranteeing quality of service, security, mobility, etc. These research projects are currently supported by the all-IP network, where the packet-switching TCP/IP model has taken over the classical telecom circuit-switching model. Thanks to convergent efforts, the Internet is already the generalized model in telecommunications to offer different services.

1.2. History of IoT

IoT was originally introduced by the Auto-ID research center at the MIT (Massachusetts Institute) [AUT] where an important effort was made to uniquely identify products. The result was termed EPC (electronic product code), which was then commercialized by EPCglobal. EPCglobal was created to follow the AutoID objectives in the industry, with the EAN.UCC (European Article Numbering – Uniform Code Council), now called GS1, as a partner to commercialize Auto-ID research, mainly the EPC.

A “thing” or “object” is any possible item in the real world that might join the communication chain. As presented by [HOD 01], the initial main objective of the IoT was to combine the communication capabilities characterized by data transmission. This was viewed as the Internet, also known as the network of bits representing the “digital world”. The process of automation was viewed as connecting the real or physical world, named the “network of atoms” characterized by the smallest component, which is the atom, to the digital world, named the “network of bits”, characterized by the smallest component, which is the bit.

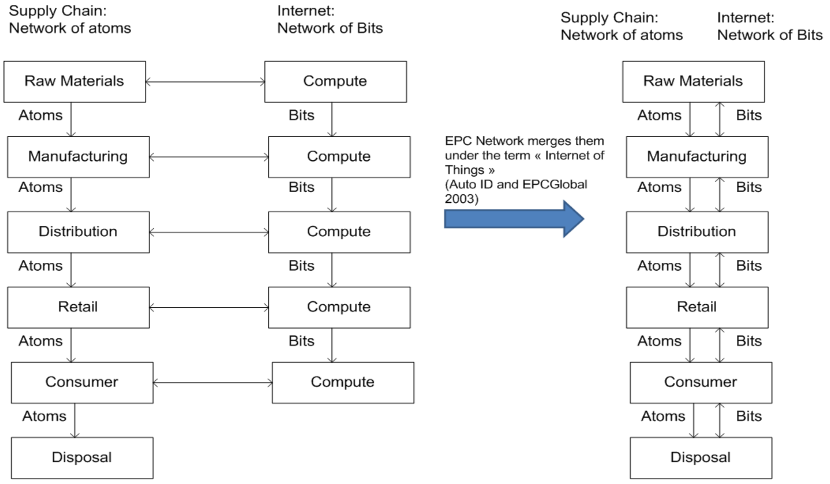

Figure 1.1. *Origin of IoT [HOD 01]*

In 2005, the ITU (International Telecommunication Unit) showed interest in new telecommunication business possibilities that could be built into services around the new connectivity of environment objects to the network.

The ITU produced a comprehensive report on the IoT from technical, economical and ethical views [IoT 05]. It introduced a new axis in the ubiquitous networking path to complete the existing “anywhere” and “anytime” connectivity. It is the “anything” connectivity axes where the thing-to-thing or machine-to-machine interaction is added to complete the existing person-to-person and person-to-machine interaction in the possible connectivity framework. This clearly opens new service opportunities.

Figure 1.2 presents the ITU view of ubiquitous networking, adding the "anything connection" to the connectivity anywhere and anytime.

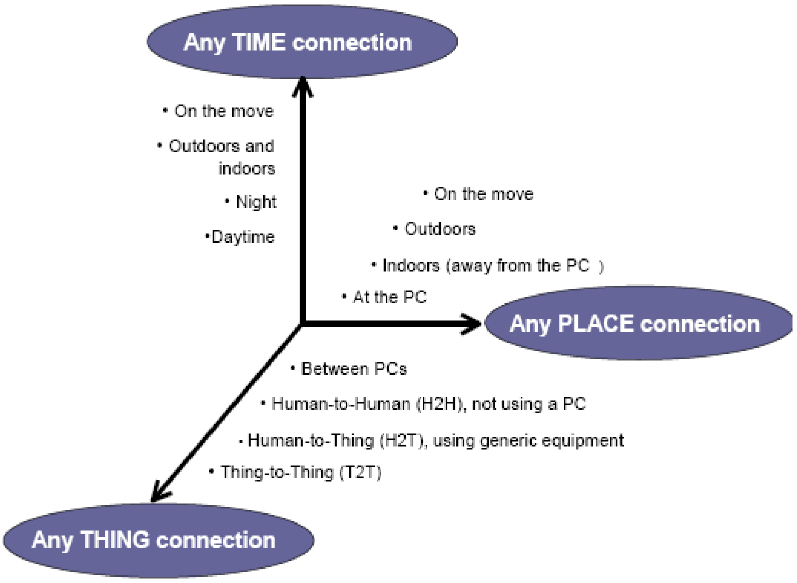

Figure 1.2. *ITU any place, any time and any thing vision [IoT 05]*

By adding the "any thing" connection axis, new sources of information are introduced in the connected network and this enables new services exploiting the newly-introduced information in the network. These services will be designed to offer the expected ubiquitous networking, where the real-world environment might react and adapt to different situations in order to make human life easier and more comfortable. Connecting these new objects will obviously raise many questions such as:

– the connecting technology of the so-called objects;

– the interoperability between objects;

– the communication model of these connected objects;

– the possible interaction with the existing models, such as the Internet;

– the choice of the transport model;

– the addressing, identifying and naming;

– the security and privacy;

– the economic impact and the telecommunication value chain evolution.

In fact, most of the Internet services were designed to satisfy person-to-person interaction, such as email and phone service. The traffic transported through the Internet is currently generated by people; either voice or data. New services were then developed around person-to-machine and machine-to-person interactions, such as video-on-demand or content distribution services. Finally, in order to provide tasks and process automation, new services will be developed around the machine-to-person, machine-to-machine or thing-to-thing and any other possible interactions in the so-called ubiquitous networking, as shown in Figure 1.3.

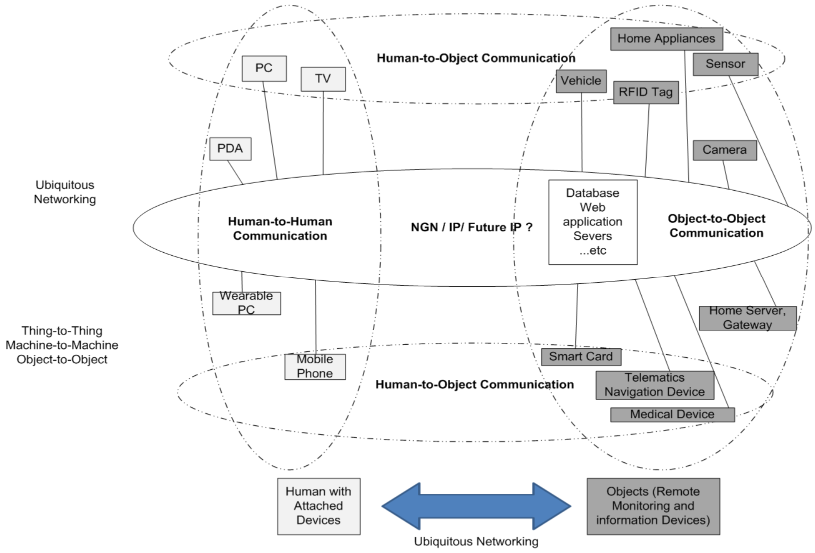
Human-to-Object Communication
PC
TV
PDA
Home Appliances
Sensor
Vehicle
RFID Tag
Camera
Ubiquitous Networking
Human-to-Human Communication
NGN / IP/ Future IP ?
Database Web application Severs ...etc
Object-to-Object Communication
Wearable PC
Home Server, Gateway
Thing-to-Thing Machine-to-Machine Object-to-Object
Mobile Phone
Smart Card
Human-to-Object Communication
Telematics Navigation Device
Medical Device
Human with Attached Devices
Objects (Remote Monitoring and information Devices)
Ubiquitous Networking

Figure 1.3. *Ubiquitous networking [IoT 05]*

IoT will connect objects to offer new services around people and objects; we can also call it the "Network of Things/Objects". IoT might suggest that the Internet model will have to be adapted to support the connectivity and traffic transport of new services based upon the connected objects. It is also worth mentioning that "Web of Objects" is another term used to refer to the IoT. As the Web is the main service accessibility to current Internet-connected nodes, similarly IoT is seen as the main service accessibility to the networked and connected objects. Also, in IoT, the naming resolution of identifiers to Web addresses is needed to handle the correspondence of identifiers introduced by RFID technology and ONS (object name service) has been introduced for that – as a similar service to the internet DNS (domain name service). "Web of Objects" has more meaning from the application viewpoint, without indirectly implying the extension of the Internet communication model to these new connected objects, as "IoT" might suggest.

1.3. About objects/things in the IoT

What exactly is a connecting or connected object or a thing? In close-to-market IoT applications, RFID tags and sensors are connecting inanimate objects and are building the actual things enabling the first IoT services.

Following the American Auto ID research center description of the IoT and the European CASAGRAS research project terminology [CAS 08], "things" or "objects" are described as a set of atoms. The atom is the smallest object in the IoT; as could be seen by nanotechnology, which is one of the enabling technologies of the IoT. A network of atoms combined with a network of bits falls into what is named the IoT. It will gather a set of objects connected to the network to help in the execution of new services enabling the smart world. So with the atom, being the smallest possible object, it is possible to classify objects based on their size and complexity, their moveable aspect and whether they are animate or inanimate, as shown in Figure 1.4 [CAS 08].

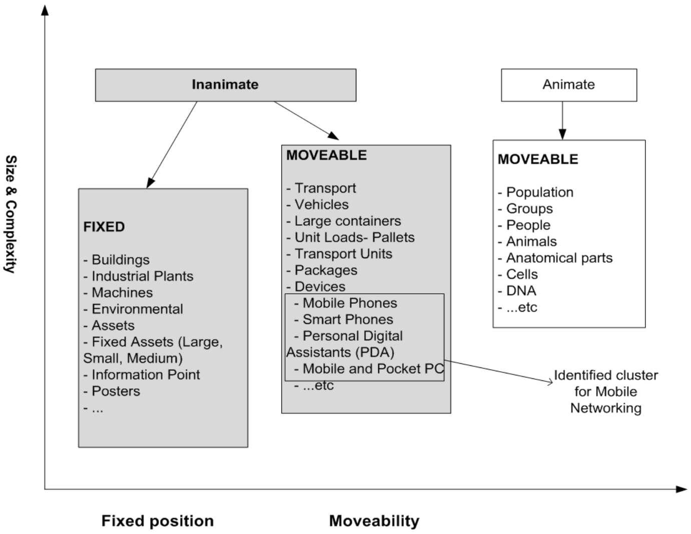

Figure 1.4. *Objects classification [CAS 08]*

In this terminology, classic devices such as PCs and mobile phones are already connected objects using wired or wireless communication. IoT will extend the connectivity and interworking of these currently existing objects with new objects connected through radio sensing or identifying technologies, such as sensor or RFID networks, allowing the development of new services involving information from the environment. This information could be either a simple identifier, as with RFID, or captured information, as with sensors. In other terminologies, common networking devices such as PCs, laptops and mobile phones are not considered to be objects.

Only small devices, such as sensors, actuators and RFID added to objects are considered as connected things or objects. Also, machines identified in home networking (connected consumer electronic devices, such as smart TVs, fridges, lights, etc.) are also connected objects. In this book, by “thing” or “object” we refer to daily life and surrounding items connected using radio connectivity, such as sensors, RFIDs or wired communication such as PLC. These technologies are enabling the development of new services, orchestrating real-world information via the connected objects.

Different technologies can be used to interconnect objects. Note that connecting objects, such as consumer electronics, e.g. a smart fridge or a smart heater, has started with home networking where consumer appliances are connected through wired technology, such as PLC, allowing communication through the power line. A number of standardization and industry organizations are addressing different issues of the home networking puzzle.

Current home networking applications do not suffer from any resource limitations. The connected objects (smart fridge, smart TV, etc.) can easily deploy an existing communication model, such as the TCP/IP model, to allow data transmission. They are affected more by interoperability problems. This is different from the issues of new applications of IoT, which rely on sensors and RFIDs where the resources of the connected objects via radio are limited by energy, memory and processing capability.

Another concern is how to support the connectivity of heterogenous objects, when a huge number of these objects/things will be connected by tags or sensors. Sensor networks have been used in industrial process control. They have allowed automation of the sense and actuate processes in order to perform automatic control, maintenance and data collection operations. A large number of potential environment monitoring applications for RFID and sensor networks are still to come. In home networking, new applications using sensor and RFID technologies will allow the automatic control of certain processes, hence minimizing human intervention.

1.4. The identifier in the IoT

IP addresses identify nodes in the Internet and serve as locators for routing. IPv6 allows larger address space than IPv4. In the IoT a large identification space will be needed to cover the identification of the tremendous number of connected objects. A specific semantic of these identifiers will follow the application’s need. In the IoT, where objects are addressed via identifiers stored into tags and interrogated by networked readers, the question of unifying and standardizing the identifier’s size and structure is critical in order to allow large deployment of services relying on these new connected objects. Since RFID technology is naturally used for identification, the standardization of the identifier stored in the RFID is the current IoT concern. The same question is raised for any addressing schemes used in the network of objects. In the IP based case, the problem will be more about the semantics of the identifier, scalability of the addressing space and memory size limitation of the devices addressed by the chosen address/identifier space.

The term "identifier" is similar to the term "name". A name does not change with location, in contrast to an "address", which is intended to be used to refer to the location of a thing. IP addresses are used to route packets between end-systems. Emerging IoT service providers expect to rely on a convenient identifier space for the envisioned service, knowing that anything can be assigned an identifier – a physical object, person, place or logical object. A wide variety of services and applications can be envisaged once it becomes possible to provide information associated with a tag identifier in different forms (text, audio or image). For example, in a museum, an identifier on a tag attached to a painting could be used to find further information on the painting and the artist. In a grocery store, an identifier on a food package could be used to check that the food is safe to eat and not a member of a sample that has been found to be contaminated in some way. Other areas in which identifier-triggered information access could be valuable are in:

– medicine/pharmaceuticals;

– agriculture;

– libraries;

– the retail trade;

– the tourist industry;

– logistics; and

– supply chain management [MAI 10].

So, the major issue to start with to maximize success is the standardization in order to ensure interoperability of the connected objects and nodes in the IoT. As will be presented in Chapter 7 of this book, this problem is well known in the communication field, but it is worse in the IoT as billions of objects are expected to be connected. It is therefore important to standardize the object identifier since the objects in the network will be addressed by a unique identifier similar to IP the addresses of connected nodes in the Internet.

EPCglobal first standardized the EPC identifier, followed by the International Standardization Organization (ISO). In addition to ISO and EPCglobal, the ubiquitous ID Center (uIDcenter) has defined a generic identifier called "ucode", which is not only intended to identify physical objects but also extended to places and digital information. ISO has addressed the issue of standardized identifiers by considering proprietary proposals, such as EPCglobal and uIDcenter, but it also offers the chance to define other identifiers that conform to ISO recommendations.

For example, if we use IP address space for identification, and if a device/thing has enough memory, we can consider IPv6 address space to be used as an identifier space of objects, since IPv6 address space is supposed to be large enough to offer up to 223 addresses in a square meter. Unfortunately, defining an identifier is not only about the scalability of the identifier space but is also about the structure and meaning/semantic of the identifier. It is important that an identifier only plays the role of identification, so that even if the objects identified are mobile, the identifier remains the same. In the IP communication model, IP addresses play two roles: from a network point of view, they act as a locator for routing and from an application point of view they identify hosts for the duration of a communication session. This dual role is seen to be problematic due to increasing demands for mobility and the multi-homing of end-systems.

For this reason the Internet Research Task Force (IRTF) and the Internet Engineering Task Force (IETF) have developed the host identity protocol (HIP), which defines host identifiers that can perform the identifier role of the IP address. This leaves the IP address to act solely as a locator for routing. These host identifiers of HIP protocol could potentially be used as another type of identifier in the IoT under the condition that they respect the ISO standard and are capable of carrying the semantic of the identifier needed by the intended IoT application. For instance, an EPCglobal identifier contains information on the product itself, the manufacturer, etc. The IPv6 address informs us about the network prefix and the address of the node. This does not contain the semantic expected by the new identifiers. A mapping between IP addresses and the things' identifiers will be possible if an IP network is used to interconnect these identified and connected objects to the Internet.

As mentioned earlier, identifying, addressing and naming the objects in the IoT service is very important. As for IP-based devices, IP addressing and naming are used to enable the routing and network resource location in the network. Address resolution protocol and name resolution using the IP domain name service (DNS) are used in IP networks to offer different services, such as the World Wide Web, email, file transfer, voice over IP, etc. Some existing IP services, such as DNS, are considered in handling the identifier resolution to a name in certain IoT services. These services include product tracking, where a product's electronic identifier will call the webpage of the manufacturer and the history of this product's manufacturing and shipping. This service is named by the EPCglobal ONS.

In order to use ONS for all the emerging IoT services orchestrating identifiers, certain problems, such as the scalability of this naming service, also has to be addressed since we are expecting billions of objects to be tagged with identifiers. Other non-technical issues related to ONS, such as the governance of this ONS, are also important. As for the DNS root, which is hosted in the United States, the ONS system will also have an ONS root, which Europe would like to host [BEN 09]. Using the DNS approach in certain IoT services has led to World Object Web, the application running over the network or web of objects, similar to the World Wide Web running over the network of IP nodes; the Internet. Figure 1.4 shows an example of ONS usage to retrieve a manufacturer's webpage.

An example of ONS usage for IoT applications other than product tracking was presented in the IoT conference in 2008 [IoT 08]. It was about helping blind person in automatic reading a book tagged with an RFID where he or she can put it on a reader connected to a computer.

As soon as the reader gets the identifier of the tagged book, a webpage appears in the screen and starts reading the book. This is the application developed and running on the Internet side. Most of the current RFID-based applications will be developed around this touch-a-tag-and-trigger-an-application, relying on the resolution of the RFID object identifier through the ONS [FLO 08].

1.5. Enabling technologies of IoT

As stated by the ITU report [IoT 05], the full-scale commercialization of many of the technologies related to IoT may require some time yet to come to fruition. Early developments have already led to a lot of innovative applications that are likely to become ubiquitous in everyday life: in the home, at work, on the farm, in the hospital, at the shop, on the road, and even inside the body.

Item-based tagging and identification will take anytime and anywhere communications to the next level in networking: "anything communications". Empowering things to detect and monitor their environment through sensors will enable the network to sense, react and respond to external stimuli. Embedded intelligence at the edges of the network will further increase the network's ability to respond [IoT 05].

IoT services will bring new functionalities in the network that allows real environment information to be processed by some IoT applications. These functionalities will, among others, be identifying, sensing and actuating in addition to the communication or information transport capability.

An increasing number of technologies will be connected to the existing and future network in order to interact with the real world, as shown in the Figure 1.5 to allow different applications around the user of IoT services. Other applications will involve more object-to-object communication for different types of IoT services more closely related to the real-world environment.

The main IoT enabling technologies will first be the electronic identification technology such as RFID and sensing and actuating technology such as sensors/actuators. Communication technologies from object-to-object and from the network of objects to the existing networks, such as wired and wireless communication networks and other technologies such as nanotechnology, smart technologies, robotics, location, etc. will also enable different IoT services.

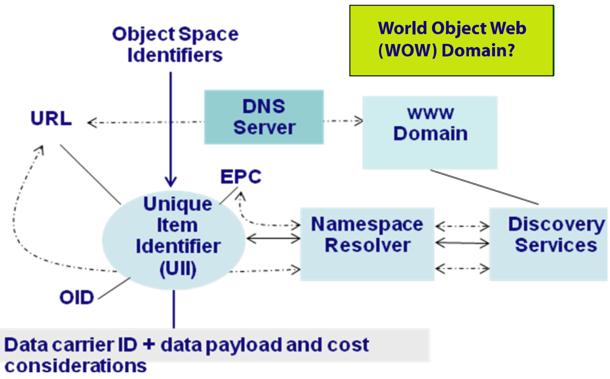
Object Space Identifiers
World Object Web (WOW) Domain?
URL
DNS Server
www Domain
EPC
Unique Item Identifier (UII)
Namespace Resolver
Discovery Services
OID
Data carrier ID + data payload and cost considerations

Figure 1.5. *ONS architecture [CAS 08]*

Wireless-based IoT services have become more popular since RFID and sensors have been able to provide information through the radio interface. Wired communication between objects will mainly be the PLC, since the home electronic appliances considered to be objects will take advantage of the electrical communication to also send information. When home networking application started at the same time as PLC development, these applications were named “home networking applications”. With the introduction of wireless RFID and sensors, new applications can be developed in home networking but also everywhere involving real-world objects. This is when the term IoT is better to cover all of these existing and emerging services and applications interacting with the real world. In this book, we describe RFID technology (Chapter 2) and sensor technology (Chapter 3) since they enable the object or thing to be connected to the network and offer the possibility to develop new services based on wireless communication. This book includes a chapter on PLC technology

(Chapter 4) as this provides a natural connection to other types of objects, such as home electronic appliances, and show other applications of IoT in home networking using wired links, such as PLC. These are actually new applications compared to the classical applications that we get through computers or telephones using the classical technologies, such as fixed or mobile communication. Other communication technologies – such as Ethernet, wireless and mobile communication technologies – are connecting devices such as computers or telephones (fixed or mobiles) but we prefer to not consider these devices as objects or things since they are not used specifically to develop new IoT services. These technologies are forming the support network to transport IoT service information, such as identifier and sensing information. The information will be processed in the application running somewhere in the mobile or fixed network to which the network of objects is connected.

1.5.1. *Identification technology*

Identification technology was initially achieved with simple barcodes that uniquely identify items for tracking. Barcodes evolved to 2D barcodes in order to contain more information or more identifiers in the same 2D space. Finally, electronic bar-coding with the introduction of RFID will allow us to store the identifier in the memory of the RFID tag. In the IoT, RFID technology is considered as one of the enabling technologies for building new services over the network, presented in Chapter 2 of this book. RFID technology will identify, track the location and provide a specific IoT application to the object. It mainly answers the question "What, which, where?", while the sensor answers the question "How?" [IoT 05]. RFID systems consist of four main components:

– a transponder or a *tag* to carry data:

- tags can be passive, semi-passive or active, based on their power source and the way they are used, as shown in Table 1.1;

– microwave *antenna* or coil and a *microchip data* located on the object to be identified;

– an interrogator or *reader*. Compared with tags, readers are larger, more expensive and power-hungry:

- that can be read-only, read/write or read/write/re-write, depending on how their data is encoded;

– *middleware*, which forwards the data to another system, such as a database, a personal computer or robot control system, depending on the application.

Passive RFID	– No need for embedded power – Tracking inventory – Unique identification number – More publicized (Wal-Mart, Metro, Department of Defense, etc.) – *Sensitive to interference* (metal, noise, etc.)
Semi-passive RFID	– Powers the microchip of the tag – Less sensitive to interference than passive tag (metal)
Active RFID	– Embedded power: communicate over greater distance – Unique identifier – Other devices (e.g. sensor) – Better than passive tags *in the presence of metal*
Semi-active RFID	– Power the transmitter part – Better than passive and semi-passive in a *noisy environment*

Table 1.1. *RFID tag technologies [YAN 08]*

Different applications are possible with RFID technology, as presented in Chapter 5; such item tracking of products in retail chains and tracking animals.

The RFID communication system can cover long distances, such as in an animal tracking application where the reading distance is several kilometers.

Near field communication (NFC) is a short-range wireless technology that enables easy and convenient interaction between devices. NFC will use the RFID communication system but limit the reading range to few centimeters. This can be used for applications requiring a secure RFID reading process. It is also an extension of proximity-card technology (contactless ISO 14443). It combines the interface of a smartcard and a reader in one device. NFC technology enables RFID reader-only, tag-only, and smart-card-only solutions. It is optimized for service discovery and initiation where a middleware on the network side is defined, such as the Nokia Field Force Solution architecture.

Mobile devices with enabled NFC technology are already on the market and offer access to different applications, such as mobile ticketing in public transport, mobile payment, smart poster, electronic tickets, electronic money, etc. This is seen as the chance for mobile network operators to be the interface to access different IoT services via NFC-enabled mobile phones.

Different IoT applications are now available, for example the NFC interface in some mobile phones enables us to read RFID tags and triggers certain applications or services, such as automatic payment via the mobile phone [TOU]. More applications and services will emerge taking advantage of the RFID technology and more research effort is currently ongoing in the area of RFID. For instance, in [PAP 09] the authors introduce the possibility of using RFID technology to improve the wireless indoor positioning. In [PAP 10], the authors propose to improve IP mobility by boosting movement detection of the mobile node using RFID technology. Chapter 5 provides more examples of RFID opportunities and research issues.

1.5.2. *Sensing and actuating technology*

As mentioned earlier, an RFID mainly answers the question “what, which, where?” while the sensor answers “how?”

A sensor is an electronic device that detects senses or measures physical stimuli from the real-world environment and converts signals from stimuli into analog or digital form. Some sensors also provide actuation functionality; these are named sensors/actuators.

Sensors can be classified according to the parameters they measure [IoT 05]:

– mechanical (e.g. position, force, pressure, etc.);

– thermal (e.g. temperature, heat flow);

– electrostatic or magnetic fields;

– radiation intensity (e.g. electromagnetic, nuclear);

– chemical (e.g. humidity, ion, gas concentration);

– biological (e.g. toxicity, presence of biological organisms), etc.;

– military – enemy tracking or battlefield surveillance.

Many scientific and research groups are working to develop more efficient and feasible sensor networks. The main technical constraints are:

– power, size, memory and storage capacity;

– trade-off between power and size;

– interference, communication model;

– the environment where the sensors are deployed (underwater, land field, etc.).

Many applications of sensors, as described in Chapter 3, can be envisioned in different domains; military environment, healthcare, construction, commercial applications, remote monitoring of the temperature of products, home applications such as the smart home, and so on. Chapter 3 provides an overview of sensor technology.

1.5.3. *Other technologies*

Emerging technologies will bring more possibilities to develop new IoT applications involving the user less and becoming more object-centric or autonomous. Here are few of them that we can mention:

– smart technologies: thinking and deciding technologies based on sensing and received information building the autonomous communication;

– process automation and robotics: executing the actuation and building the autonomous communication;

– nanotechnology: the atom is the object, the smallest object in IoT.

More possible IoT services will be based on new types of material, feeling cloths, adapting wall painting, etc. pushing ubiquitous networking many daily life objects [IoT 05].

1.5.4. *Connected objects' communication*

1.5.4.1. *Object-to-object*

In object-to-object communication, the interoperability is very important and building the network of objects with end-to-end communication is challenging. For instance, RFID reader to RFID tags will use a standardized ISO communication model named ISO 18000, where serial communication is used at several kilobits per second and in some technologies up to a megabit per second. Here it is a point-to-point communication.

In sensor-to-sensor communication, different wireless technologies are possible and the IEEE 802.15.4 or Zeegbee is one of the wireless technologies promoted for building wireless sensor networks.

In a home networking and wired scenario, objects might communicate with other objects using the PLC.

Using the IP model in the emerging network of objects, communication might be possible under certain conditions related to the resources of the nodes, the addressing, naming and identification of the nodes, the size of the network and the density of the nodes, etc.

At the moment, the IP model is possible as a network hosting IoT application functionalities and using special gateways to connect the objects or network of objects to the Internet.

1.5.4.2. *Object or network of objects to other networks*

The first generation of IoT services that are close to the market will rely on these new objects being connected to the network via technologies, such as RFID (NFC for secure short-range reading applications) and sensors to introduce real-world information into the network. This information will be processed by these new applications. In this case, most of the interconnection effort will be at the gateway point attaching the objects to the network, as shown in Figure 1.6.

This gateway can be connected either by a wired or wireless/mobile communication system. Other technologies that are already used for different applications may be possible technologies for new IoT services to connect the object to the network. Examples include smart cards for automatic payment, location technologies (real time location system, global positioning system or GPS, etc.). Such technologies enable location-based services and tracking, barcode (2D) for item tracking, etc.

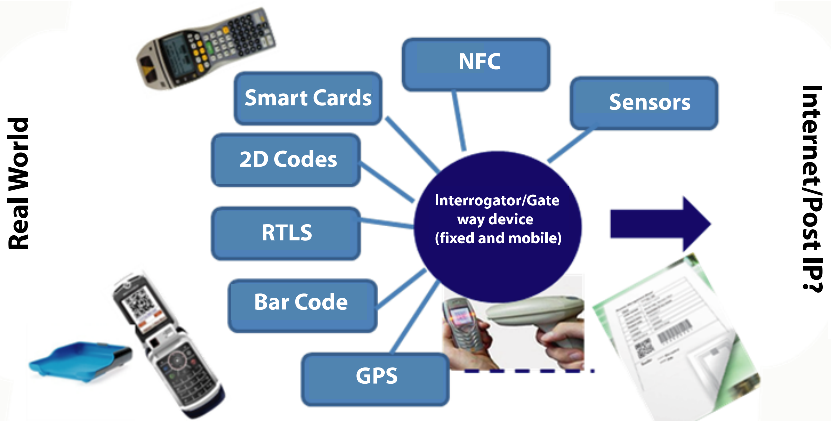

Figure 1.6. *Example of current edge technologies for IoT services [CAS 08]*

1.6. About the Internet in IoT

Connecting objects with different technologies and different communication models raises the question of end-to-end communication between heterogenous systems. IP has in the past answered this question when it interconnected heterogenous networks with different physical and link layers, transporting different types of traffic through the network/IP layer by introducing the new addressing space; the IP addressing and routing schema that allows us to reach any node connected to the IP network as long as it has a routable IP address. In the IoT there are more issues than heterogenity in connecting the new objects and interconnecting the network of objects to the existing network. For this reason, we need to:

– design or adapt an appropriate communication model to set up the network of objects;

– design or adapt the connectivity of this network of objects to the current Internet where some of the IoT functionalities will be hosted, such as information databases, applications, actuation commands, etc.

For the communication model to set up the network of objects, several issues need to be considered. An important issue is the available resources offered by objects, such as battery, memory and processing capability. For instance, tiny objects such as sensors or RFIDs have limited resources. However, other objects in home networking applications, such as a smart TV or smart fridge, might have enough resources. Usually when there are enough resources, the IP addressing and routing model could be considered as the communication model for setting up a network of objects, as long as it respects the application traffic requirement.

Another issue is the heterogenity of the connecting objects. Again, the IP model could be considered to handle the connectivity of heterogenous nodes and networks, but this will only be possible if there are enough resources. Tiny objects, such as sensors, RFID, etc. clearly show the limitations of the current IP model, especially with energy consumption. A new adaptation of this model has therefore already been devised in the IETF where the IP model might be used to connect some objects in the IoT, such as sensors under certain parameters. In fact, the IETF 6LoWPAN working group has produced an IPv6-based model to satisfy the sensor environment requirement over IEEE 802.15.4 [IET 08]. ROLL working group has looked at how to adapt the routing process to these new environments and come up with the RPL (remote program load) protocol [IET 08b]. The IP for Smart Objects (IPSO) Alliance, which is a group of more than 100 industrials, is also looking at the adaptation of IP to these smart and tiny devices [IPS].

Note that sensor networks are gaining increasing attention from industry since they can help in building new services and applications in different domains, such as health, agriculture and transport, in anyplace, therefore creating new revenues. It is the same with RFID technology. Before developing more applications and considering more and more objects, however, it is necessary to avoid problems such as scalability, complexity and heterogenity in communication. Internet (current/future) model is considered to be a possible communication framework for the emerging IoT-based services, at least in the short and medium term. To be more generic, we should consider the word Internet in the "IoT" as INTERNETworking of objects, meaning:

– transport capability;

– heterogenity management;

– easy object network management;

– easy services development; and

– deployment capability.

This could be realized by an adapted version of the IP model or a totally new communication model, which is expected by the Future Internet/Network worldwide initiative [EUR 08, FIN 10].

The interconnection of the network of objects to other networks, such as existing Internet, will depend on the purpose of the interconnection. We know that IoT applications will orchestrate functionalities from the current Internet network to allow the transport of traffic generated on IoT nodes and also allow the local and remote service access. Another functionality is related to the management of the network of objects with simple and known tools locally or remotely. Consequently, a network of objects using the IP model or any other communication model within an objects network has to be connected to the Internet through some specific gateways, as shown in Figure 1.12. This allows communication between the network of objects and the worldwide Internet and enables us to benefit from existing tools, data transport and management. The gateway will be close to the tag reading or the sensor to handle the transport of this information on the IP side. For instance, some commands can be sent from an Internet node towards the network of objects. In this case, the Internet model should be adapted to support the properties of this new traffic coming from, and going to, this network of objects.

In order to understand the new traffic properties, it is important to look at the functionalities required by the IoT service. These emerging services intend to introduce information from the real-world environment in the network to be processed and then automate some tasks in the real world; identifying, sensing and actuating are the major building blocks of an IoT-based service. All these functionalities will generate traffic that needs to be transported from one point to another on the network. For instance, the *identifying* process will generate the identifier information using current identifier technology; the RFID will be used by the application service located in the network. The RFID reader can be directly connected to the network or multi-hop away from it.

When using sensors, *sensing* information is generated by the sensor and has to be transported to the application process through other sensors; multi-hop transport model or one hop away from the node running the application. The *actuation* process might be triggered locally or remotely through a network and will need efficient network transport to satisfy the traffic requirement of the actuation service. In any case, there is a need for efficient information transfer taking into account the limited resources of current object technologies, such as RFID tags and wireless sensors.

The first proposed architecture by the ITU is shown in Figure 1.6 where the IP network is selected to transport the identification or sensing information at the edge of the Internet. It shows a need for an interface for the transport and service planes of the Internet or NGN (next generation network). The IP network will not be the only possibility for supporting the transport of information generated by these new IoT-based services. This is a short- and medium-term view of the IoT applications that are close to the market. A future network model might emerge to handle the new requirement of the IoT services and traffic transport based on these tiny devices suffering from lack of energy, memory and processing resources. More adaptation and autonomic behavior will be included in the new communication model.

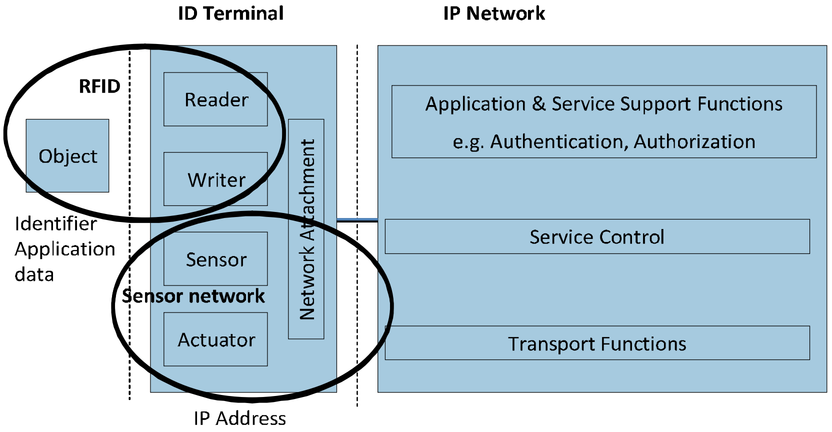

Figure 1.7. *ITU IoT reference model [IoT 05]*

As mentioned by the ITU in Figure 1.6, the industry's is considering IP and NGNs in the short and medium term as the network support for IoT services. This is seen as a natural step forward to the convergence process in telecommunications seeking the all IP model. Based on this fact, certain IoT services might be deployed very quickly as soon as security-related issues are solved, such as privacy related to RFID deployment. These close-to-market services are using the Internet to run the application that orchestrates the objects connected to the existing network nodes. In this context, the user interface to these new services will either be related to fixed or mobile networks. The actuation process might be triggered locally if it is programmed to do so, or remotely through a given network based on a certain terminal. For instance, actuation may be through a mobile phone connected to the emerging 4G network or any other wireless or mobile network. This has attracted particular interest from mobile network operators and mobile device manufacturers designing smart phones with RFID reader capability. In fact, emerging mobile phones could be used to trigger some IoT services remotely, and also interact locally through a new reading interface with the objects added to the real environment.

Following the industry approach where the convergence to all IP continues with the new IoT services, it is important to remind readers of the convergence path to all IP. As summarized in Figure 1.7, the convergence in telecommunications can be seen from different angles. The value chain participants; initially telecommunications, Internet and broadcasting operators offer specific voice, data, and media services respectively. The convergence will cause these specific operators to offer all three services at the same time on the same network. In fact, the convergence in telecommunications will end in the design of a container, named an IP packet, to transport different information (voice, data and media) in the same network, today known as the IP network. This transported information has specific properties satisfied by the corresponding network before convergence and by the IP network after convergence. This is because IP with quality of service architecture can offer these multiple services in the same packet-switched network.

Consequently, the convergence also impacts the corresponding communication, information and entertainment markets. Finally, convergence impacts the design of devices or interfaces to the corresponding services – terminal (telephone), computer, and home consumer electronic appliances (e.g. TV). It will push the industries to design an all-in-one device to access all these services, no matter which physical network we are connected to, fixed or mobile.

This also has an impact on service management from the network side. The convergence in telecommunications came with a service-oriented approach, where a service abstraction layer is introduced and access to a service has to be transparent from the physical transport of the information generated by this service. IP multimedia subsystem (IMS) and fixed mobile convergence is a good example of a service abstraction layer. It is possible to get a service (e.g. telephony) no matter which physical network the user is connected to thanks to SIP (session initiation protocol) signaling that introduces a new user identifier to be mapped with the location of the user at anytime and anywhere.

All IP, which is one concrete answer to the need to converge in telecommunications, started with the need to optimize network resources of a fixed telephony network based on a circuit switching model. Initially, there were specific and dedicated networks with specific nodes and linking technologies to offer one specific service. In fact, the first network designed was only meant to be used for telephony. It is the fixed telecommunication network. The data transport network came mainly with the Internet network and finally the television application was deployed in another specific network, the TV broadcast network. Designing a specific network for a specific service is definitely not optimizing resource usage. Using an end-to-end physical circuit for only one communication, even if there is no voice transported, is not optimizing resource utilization.

One of the major revolutions in networking is the move from circuit switched networking to packet switched networking, also known as the IP network, Internet, TCP/IP network, data network or packet network. IP being the *de facto* protocol for interconnecting heterogenous networks, with an additional set of other protocols for control and management, makes it the convergence vector in the evolving telecommunication systems. IP was threatened at different times, first by ATM, a packet-switching network that was too complex and expensive, then switched Ethernet but was not scalable. IP won due to its simplicity, lower investment requirements, scalability and ability to carry different services relying on the virtual circuit switching over packet-switching network. Convergence to what is called all IP can then be seen at different layers: the transport, management, control and application development. This has enabled all IP to maximize the revenues of the telecom companies in the value chain.

The value chain is also impacted in this convergence path, as shown in Figure 1.8. It was initially linear, where each industry in the value chain has its own development and market. Following convergence the value chain is non-linear and most of the industries are moving towards this user-centric approach, where it is all about designing new services to be transported by this unique and stable network: the all IP.

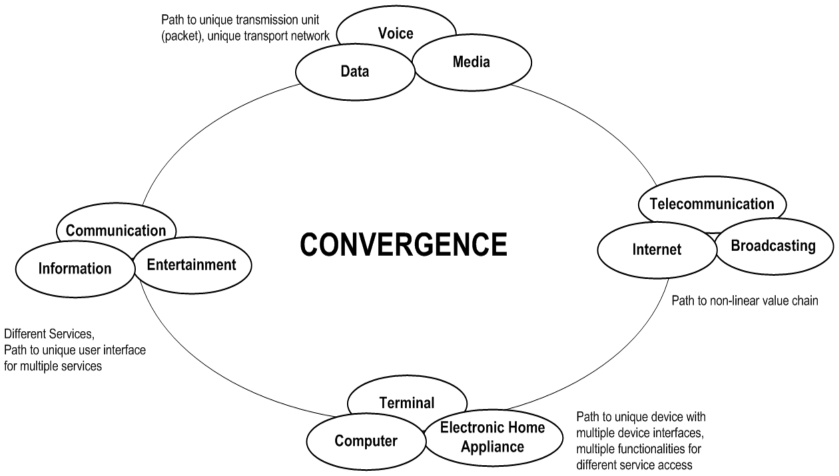
Path to unique transmission unit (packet), unique transport network
Voice
Data
Media
Telecommunication
Internet
Broadcasting
Path to non-linear value chain
CONVERGENCE
Communication
Information
Entertainment
Different Services, Path to unique user interface for multiple services
Terminal
Computer
Electronic Home Appliance
Path to unique device with multiple device interfaces, multiple functionalities for different service access

Figure 1.8. *Convergence in telecommunications [CHA 09]*

New services will emerge with the IoT and will also impact the value chain where some services will be object-centric, meaning that the interaction of these new services will be based from object-to-object with no human interaction. The traffic generated by these object-to-object-oriented services will need to match a certain business model with new participants.

The path to convergence continues with the IoT, and raises the question of whether IP will be fully adopted to support IoT services, or if it will only be partially used. As shown in Figure 1.9, IoT will impact the convergence in telecommunications at different angles.

Adding IoT services to the network will first impact the value chain, since new actors will be introduced in the telecommunication chain. For instance the actor of product identification since RFID technology is part of the IoT enabling technologies. As shown in Figure 1.10, sensing and actuating designers, automation process developers will join the existing telecom value chain with wired and wireless communication providers in order to develop IoT services.

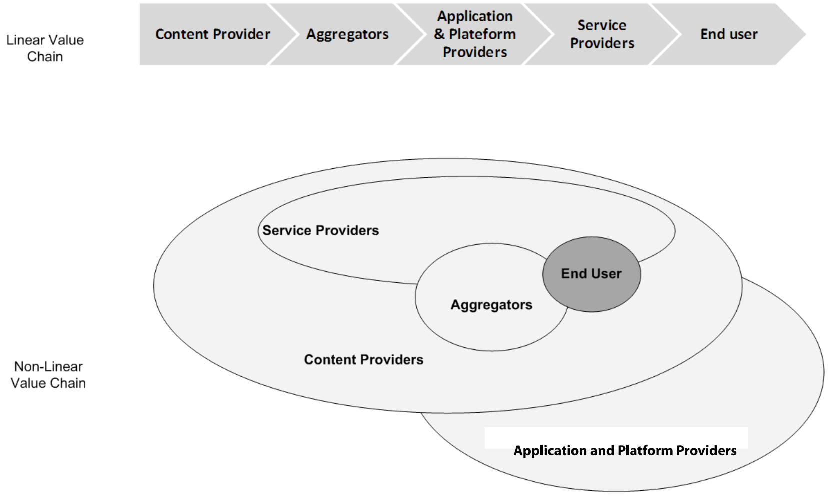

Figure 1.9. *Telecom value chain evolution [CHA 09]*

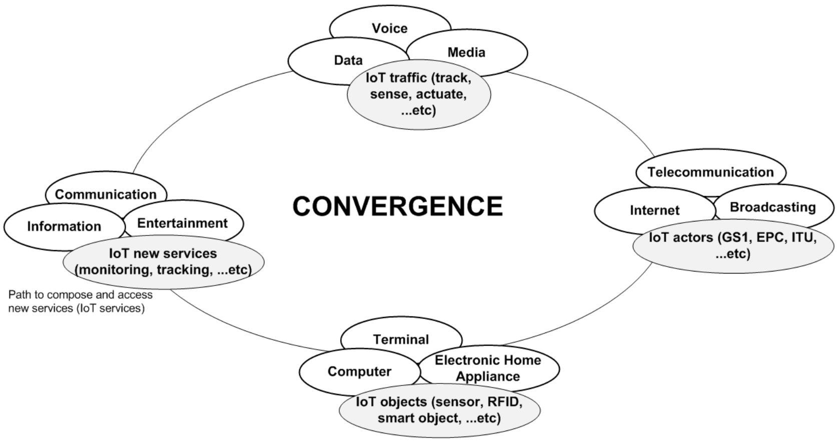
Voice
Data
Media
IoT traffic (track, sense, actuate, ...etc)
CONVERGENCE
Communication
Information
Entertainment
IoT new services (monitoring, tracking, ...etc)
Path to compose and access new services (IoT services)
Telecommunication
Internet
Broadcasting
IoT actors (GS1, EPC, ITU, ...etc)
Terminal
Computer
Electronic Home Appliance
IoT objects (sensor, RFID, smart object, ...etc)

Figure 1.10. *IoT in the convergence path [CHA 09]*

By introducing IoT in the convergence path, it will impact the selection of the information container, which will transport information generated in the converged network the IoT. Knowing that IoT services will introduce mainly new functionalities – identifying, sensing and actuating – we need to ask two questions about keeping IP as the convergence vector. First, what is interesting from IP that can be used in the IoT? The Internet model might be considered immediately in connecting the objects (with enough resources) because it is capable of:

– naming and addressing;

– routing;

– scalability;

– easy deployment and management;

– easy application development;

– easy naming, addressing, name and address resolution;

– etc [IPS].

Second, what are the limitations in using IP for IoT services? In the current object technologies, there are the following object resource limitations: battery, memory and processing. Also, IP has to support the traffic properties of the functionalities introduced, mainly identifying, sensing and actuating.

In Figure 1.9, we add “IoT information” next to “voice, data, media”. Knowing that IoT-generated information may be an identifier, a sensing information, an actuation order, etc., this type of information may have different QoS properties. There is therefore a need to study the traffic model of this new type of information and analyze whether IP as it is today can transport this information by respecting the traffic properties. For instance, a remote actuation might have higher priority than existing voice traffic due to the urgent character of a given IoT application.

For delay-tolerant IoT applications, the question will be more about the overhead of the IP model compared to the IoT-generated data. It is therefore important to know whether the IP model can be used from end-to-end, meaning addressing the objects using IP and then benefiting from the IP traffic forwarding, or only use IP model for the gateway connecting the network of objects to the Internet, as suggested in Figure 1.11.

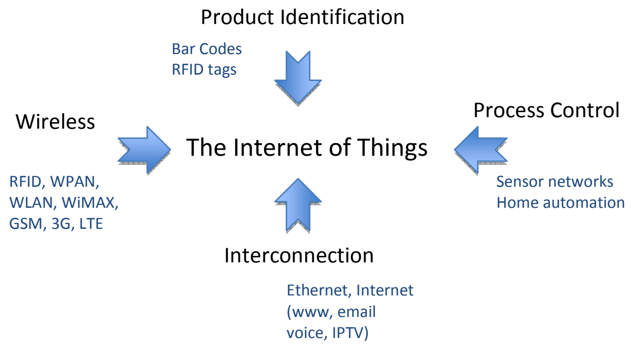

Figure 1.11. *New participants in the IoT value chain [MAI 10]*

Adding IoT services in the big picture of convergence will impact the device design. The design will need contain the interfaces to access the IoT service and will join the all IP in a one-device approach, most probably mobile smart device (cell phone). Cell phone operators are very interested in these newly emerging IoT services.

Following the convergence path in Figure 1.9, from the service access point of view, we might follow the service-oriented approach where IoT services should be independent from the network transport part. This means where the transport network changes, the service will always be accessible, as in the IP-multimedia subsystem (IMS) approach.

This might sound like a new step in the convergence of networks to the all-IP convergence, where a service-oriented approach is followed in order to get a service, no matter what the network transport. It is important to remove responsibility for IoT services development from the transport network, so they are independent. This means that services will be independent whether the network is fixed or mobile, IP-, post-IP-or future network-based. It is important to ensure that the IoT services developed are capable of being applied over any transport network and that the services are offered service no matter which transport network is used by the network of objects. Our view of the IoT service-oriented approach is shown in Figure 1.11.

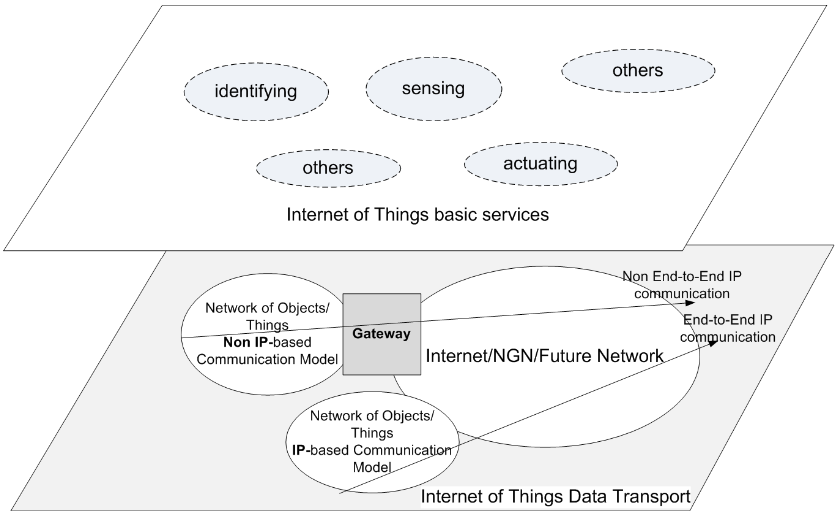
identifying
sensing
others
others
actuating
Internet of Things basic services
Non End-to-End IP communication
End-to-End IP communication
Network of Objects/ Things Non IP-based Communication Model
Gateway
Internet/NGN/Future Network
Network of Objects/ Things IP-based Communication Model
Internet of Things Data Transport

Figure 1.12. *IoT abstract view*

Finally, the path to this convergence will certainly start by considering IP or an adapted version of IP to handle the first generation of IoT services that are still user-centric. The massive deployment of these IoT services in the short and medium term will mainly be allowed by society’s acceptance of the new technologies, such as RFID with privacy issues. This will enable technologies that attract IoT services with promising new revenues to enter the user-centric value chain.

In the long term, a new communication model will probably emerge following the post-IP and future internet/network developments. The next generation of IoT services will then be naturally deployed, being user-centric but mostly object-centric. Network scalability need will to increase to incorporate the billions of objects connected and orchestrated by IoT applications. Research is focusing more on trying to improve society's lifestyle by adding more task automation and respecting the real-world environment by deploying services to monitor or act to reduce damage to the planet.

1.7. Bibliography

[AUT] AUTO-ID LABS, "Architecting the Internet of Things", available at: http://www.autoidlabs.org/, accessed February 19, 2010.

[BEN 09] BENHAMOU B., "Internet of Things. Technological, economical and political challenges", *Revue ESPRIT*, pp. 1-14, 2009.

[CAS 08] CASAGRAS project *Interim report. September 2008*, EU Framework 7 project, 2008. (Available at: http://www.rfidglobal.eu/userfiles/documents/CASAGRAS%20Report.pdf, accessed February 19, 2010.)

[CHA 09] CHAOUCHI H., "Internet of Things, the path to convergence continues", *Invited Paper at Special Session on Internet of Things Co-hosted with the International Conference IFIP WMNC 2009*, Gdansk, 2009.

[EUR 08] EURESCOM, "European future internet portal", Eurescom GmbH, 2008. (Available at: http://www.future-internet.eu/, accessed February 19, 2010.)

[FIN 10] NATIONAL SCIENCE FOUNDATION, "FIND – NSF NeTS FIND Initiative", University of Minnesota, 2010. (Available at: http://www.nets-find.net/, accessed February 19, 2010.)

[FLO 08] FLOERKEMEIER C., *et al*. "The Internet of Things", *Proceedings of the First International Conference*, LNCS 4952, IoT 2008, Zurich, March 2008, pp. 1-377, 2008.

[GEN 10] GENI, "Exploring networks of the future", BBN Technologies, 2010. (Available at: http://www.geni.net/, accessed February 19, 2010.)

[HOD 01] HODGES S., *Auto-ID: Merging Atoms with Bits Around the Globe*, Institute for Manufacturing, 2001. (Available at: http://www.ifm.eng.cam.ac.uk/automation/ presentations, accessed February 19, 2010.)

[IET 08] INTERNET ENGINEERING TASK FORCE (IETF), "6lowpan status pages", 1 September 2008. (Available at: http://tools.ietf.org/wg/6lowpan/, accessed February 19, 2010.)

[IET 08b] INTERNET ENGINEERING TASK FORCE (IETF), "Roll status page", 15 February 2008. (Available at: http://tools.ietf.org/wg/roll/, accessed February 19, 2010.)

[IoT 05] ITU, *The Internet of Things*, ITU Strategy and Policy Unit (SPU), November 2005.

[IoT 08] INTERNET OF THINGS, "International Conference for Industry and Academia" (website), ETH Zurich 2008. (Available at: http://www.iot2008.org/.)

[IPS] IPSO ALLIANCE, "IPSO Alliance: promoting the use of IP for smart objects", 2009. (Available at: http://www.ipso-alliance.org, accessed February 19, 2010.)

[ISO] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. http://www.iso.org (accessed February 19, 2010).

[PAP 09] PAPAPOSTOLOU A., CHAOUCHI H., "Exploiting multi-modality and diversity for localization enhancement: WiFi & RFID usecase", *IEEE PIMRC*, Tokyo, Japan, 2009.

[PAP 10] PAPAPOSTOLOU A., CHAOUCHI H., "RFIC consideration for IP mobility improvement", *Wireless Communications & Networking Conference*, Sydney, Australia, April 18-21, 2010.

[TOU] TOUCHATAG, website, available at: http://www.touchatag.com, accessed February 19, 2010.

[YAN 08] YAN L., *et al.*, *The Internet of Things, From RFID to the Next Generation Pervasive Networked Systems*, Auerbach Publications, 2008.