Computer Networks xxx (2010) xxx–xxx

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

The Internet of Things: A survey

Luigi Atzori [a], Antonio Iera [b], Giacomo Morabito [c,*]

[a] DIEE, University of Cagliari, Italy
[b] University "Mediterranea" of Reggio Calabria, Italy
[c] University of Catania, Italy

ARTICLE INFO

Article history:
Received 10 December 2009
Received in revised form 27 April 2010
Accepted 14 May 2010
Available online xxxx
Responsible Editor: E. Ekici

Keywords:
Internet of Things
Pervasive computing
RFID systems

ABSTRACT

This paper addresses the Internet of Things. Main enabling factor of this promising paradigm is the integration of several technologies and communications solutions. Identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols (shared with the Next Generation Internet), and distributed intelligence for smart objects are just the most relevant. As one can easily imagine, any serious contribution to the advance of the Internet of Things must necessarily be the result of synergetic activities conducted in different fields of knowledge, such as telecommunications, informatics, electronics and social science. In such a complex scenario, this survey is directed to those who want to approach this complex discipline and contribute to its development. Different visions of this Internet of Things paradigm are reported and enabling technologies reviewed. What emerges is that still major issues shall be faced by the research community. The most relevant among them are addressed in details.

1. Introduction

The *Internet of Things* (*IoT*) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. 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 [1].

Unquestionably, the main strength of the IoT idea is the high impact it will have on several aspects of everyday-life and behavior of potential users. 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 scenarios in which the new paradigm will play a leading role in the near future. 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.

By starting from the considerations above, it should not be surprising that IoT is included by the US National Intelligence Council in the list of six "Disruptive Civil Technologies" with potential impacts on US national power [2]. NIC foresees that "by 2025 Internet nodes may reside in everyday things – food packages, furniture, paper documents, and more". It highlights future opportunities that will arise, starting from the idea that "popular demand combined with technology advances could drive widespread diffusion of an Internet of Things (IoT) that could, like the present Internet, contribute invaluably to economic development". The possible threats deriving from a widespread adoption of such a technology are also stressed. Indeed, it is emphasized that "to the extent that everyday objects become information security risks, the IoT could distribute those risks far more widely than the Internet has to date".

Q1 * Corresponding author. Tel.: +39 095 7382355; fax: +39 095 7382397.
E-mail addresses: l.atzori@diee.unica.it (L. Atzori), antonio.iera@unirc.it (A. Iera), giacomo.morabito@diit.unict.it (G. Morabito).

1389-1286/$ - see front matter © 2010 Published by Elsevier B.V.
doi:10.1016/j.comnet.2010.05.010

Actually, many challenging issues still need to be addressed and both technological as well as social knots have to be untied before the IoT idea being widely accepted. Central issues are making a full interoperability of interconnected devices possible, providing them with an always higher *degree of smartness* by enabling their adaptation and autonomous behavior, while guaranteeing trust, privacy, and security. 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.

Several industrial, standardization and research bodies are currently involved in the activity of development of solutions to fulfill the highlighted technological requirements. This survey gives a picture of the current state of the art on the IoT. More specifically, it:

- provides the readers with a description of the different visions of the Internet of Things paradigm coming from different scientific communities;
- reviews the enabling technologies and illustrates which are the major benefits of spread of this paradigm in everyday-life;
- offers an analysis of the major research issues the scientific community still has to face.

The main objective is to give the reader the opportunity of understanding what has been done (protocols, algorithms, proposed solutions) and what still remains to be addressed, as well as which are the enabling factors of this evolutionary process and what are its weaknesses and risk factors.

The remainder of the paper is organized as follows. In Section 2, we introduce and compare the different visions of the IoT paradigm, which are available from the literature. The IoT main enabling technologies are the subject of Section 3, while the description of the principal applications, which in the future will benefit from the full deployment of the IoT idea, are addressed in Section 4. Section 5 gives a glance at the open issues on which research should focus more, by stressing topics such as addressing, networking, security, privacy, and standardization efforts. Conclusions and future research hints are given in Section 6.

2. One paradigm, many visions

Manifold definitions of *Internet of Things* traceable within the research community testify to the strong interest in the IoT issue and to the vivacity of the debates on it. By browsing the literature, an interested reader might experience a real difficulty in understanding what IoT really means, which basic ideas stand behind this concept, and which social, economical and technical implications the full deployment of IoT will have.

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.

It shall not be forgotten, anyway, that the words "Internet" and "Things", when put together, assume a meaning which introduces a disruptive level of innovation into today ICT world. In fact, "Internet of Things" semantically means "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [3]. This implies a huge number of (heterogeneous) objects involved in the process.

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.

In Fig. 1, the main concepts, technologies and standards are highlighted and classified with reference to the IoT vision/s they contribute to characterize best. 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.

The very first definition of IoT derives from a "Things oriented" perspective; the considered things were very simple items: Radio-Frequency IDentification (RFID) tags. The terms "Internet of Things" is, in fact, attributed to The Auto-ID Labs [4], a world-wide network of academic research laboratories in the field of networked RFID and emerging sensing technologies. These institutions, since their establishment, have been targeted to architect the IoT, together with EPCglobal [5]. Their focus has primarily been on the development of the Electronic Product Code™ (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 Network™. These standards are mainly designed to improve object visibility (i.e. the traceability of an object and the awareness of its status, current location, etc.). This is undoubtedly a key component of the path to the full deployment of the IoT vision; but it is not the only one.

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! And the same holds for the alternative Unique/Universal/Ubiquitous IDentifier (uID) architecture [6], whose main idea is still the development of (middleware based) solutions for a global visibility of objects in an IoT vision. It is the authors' opinion that, starting from RFID centric solutions may be positive as the main aspects stressed by RFID technology, namely item traceability and addressability, shall definitely be addressed also by the IoT. Notwithstanding, alternative, and somehow more complete, IoT visions recognize that the term IoT implies a much wider vision than the idea of a mere objects identification.

Please cite this article in press as: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.05.010

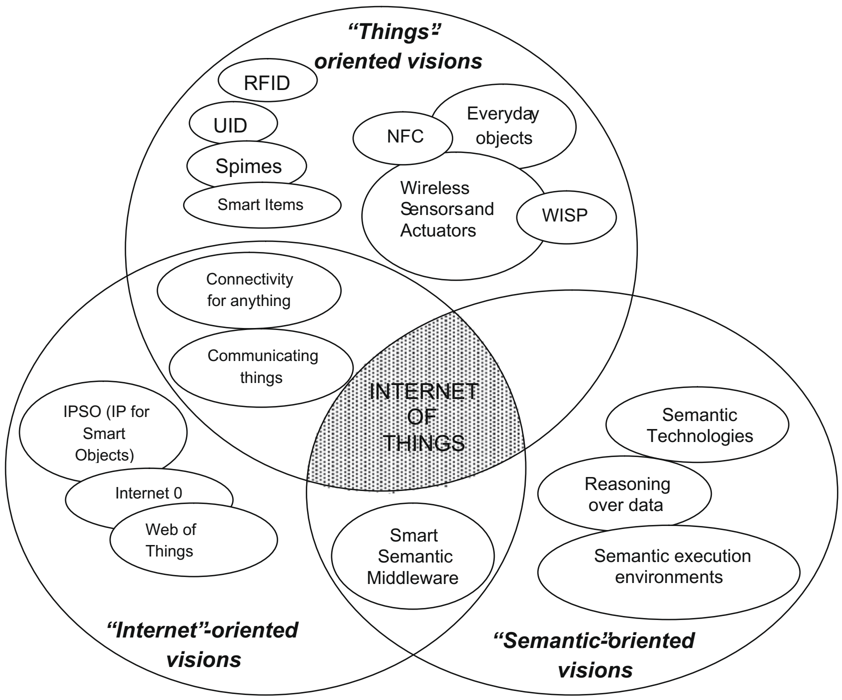

Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

According to the authors of [7], 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. Near Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN) together with RFID are recognized as "the atomic components that will link the real world with the digital world". It is also worth recalling that major projects are being carried out with the aim of developing relevant platforms, such as the WISP (Wireless Identification and Sensing Platforms) project.

The one in [7] is not the only "Things oriented" vision clearly speaking of something going beyond RFID. Another one has been proposed by the United Nations, which, during the 2005 Tunis meeting, predicted the advent of IoT. A UN Report states that a new era of ubiquity is coming where humans may become the minority as generators and receivers of traffic and changes brought about by the Internet will be dwarfed by those prompted by the networking of everyday objects [8].

Similarly, other relevant institutions have stressed the concept that IoT has primarily to be focused on the "Things" and that the road to its full deployment has to start from the augmentation in the Things' intelligence. This is why a concept that emerged aside IoT is the *spime*, defined as an object that can be tracked through space and time throughout its lifetime and that will be sustainable, enhanceable, and uniquely identifiable [9]. Although quite *theoretical*, the *spime* definition finds some real-world implementations in so called *Smart Items*. These are a sort of sensors not only equipped with usual wireless communication, memory, and elaboration capabilities, but also with new potentials. Autonomous and proactive behavior, context awareness, collaborative communications and elaboration are just some required capabilities.

The definitions above paved the way to the ITU vision of the IoT, according to which: "from anytime, anyplace connectivity for anyone, we will now have connectivity for *anything*" [10]. A similar vision is available from documents and communications of the European Commission, in which the most recurrent definition of 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" [3].

An IoT vision statement, which goes well beyond a mere "RFID centric" approach, is also proposed by the consortium CASAGRAS [11]. Its members focus on "a world where things can automatically communicate to computers and each other providing services to the benefit of the human kind". CASAGRAS consortium (i) proposes a vision of IoT as a global infrastructure which connects both virtual and physical generic objects and (ii) highlights the importance of including existing and evolving Internet and network developments in this vision. In this sense, IoT becomes the natural enabling architecture for the deployment of independent federated services and applications, characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.

This definition plays the role of *trait d'union* between what we referred to as a "Things oriented" vision and an "Internet oriented" vision.

Please cite this article in press as: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.05.010

Within the latter category falls the IoT vision of the IPSO (IP for Smart Objects) Alliance [11], a forum formed in September 2008 by 25 founding companies to promote the Internet Protocol as the network technology for connecting Smart Objects around the world. 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. This guarantees that IP has all the qualities to make IoT a reality. By reading IPSO whitepapers, it seems that through a wise IP adaptation and by incorporating IEEE 802.15.4 into the IP architecture, in the view of 6LoWPAN [12], the full deployment of the IoT paradigm will be automatically enabled.

Internet Ø [13] follows a similar approach of reducing the complexity of the IP stack to achieve a protocol designed to route "IP over anything". In some forums this is looked at as the wisest way to move from the Internet of Devices to the Internet of Things. According to both the IPSO and Internet Ø approaches, the IoT will be deployed by means of a sort of *simplification* of the current IP to adapt it to any object and make those objects addressable and reachable from any location.

As said before, it is worth noticing that "Semantic oriented" IoT visions are available in the literature [14–17]. The idea behind them is that the number of items involved in the Future Internet is destined to become extremely high. Therefore, issues related to how to represent, store, interconnect, search, and organize information generated by the IoT will become very challenging. In this context, semantic technologies could play a key role. In fact, these can exploit appropriate modeling solutions for things description, reasoning over data generated by IoT, semantic execution environments and architectures that accommodate IoT requirements and scalable storing and communication infrastructure [14].

A further vision correlated with the IoT is the so called "Web of Things" [18], according to which Web standards are re-used to connect and integrate into the Web everyday-life objects that contain an embedded device or computer.

3. Enabling technologies

Actualization of the IoT concept into the real world is possible through the integration of several enabling technologies. In this section we discuss the most relevant ones. Note that it is not our purpose to provide a comprehensive survey of each technology. Our major aim is to provide a picture of the role they will likely play in the IoT. Interested readers will find references to technical publications for each specific technology.

3.1. Identification, sensing and communication technologies

"Anytime, anywhere, anymedia" has been for a long time the vision pushing forward the advances in communication technologies. In this context, wireless technologies have played a key role and today the ratio between radios and humans is nearing the 1 to 1 value [19].

However, the reduction in terms of size, weight, energy consumption, and cost of the radio can take us to a new era where the above ratio increases of orders of magnitude. This will allow us to integrate radios in almost all objects and thus, to add the world "anything" to the above vision, which leads to the IoT concept.

In this context, key components of the IoT will be RFID systems [20], 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 (even persons or animals). Readers trigger the tag transmission by generating an appropriate signal, which represents a query for the possible presence of tags in the surrounding area and for the reception of their IDs. 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.

From a physical point of view a RFID tag is a small microchip[1] attached to an antenna (that is used for both receiving the reader signal and transmitting the tag ID) in a package which usually is similar to an adhesive sticker [21]. Dimensions can be very low: Hitachi has developed a tag with dimensions 0.4 mm × 0.4 mm × 0.15 mm.

Usually, RFID tags are *passive*, i.e., they do not have on-board power supplies and harvest the energy required for transmitting their ID from the query signal transmitted by a RFID reader in the proximity. In fact, this signal generates a current into the tag antenna by induction and such a current is utilized to supply the microchip which will transmit the tag ID. Usually, the gain (power of the signal received by the reader divided by the power of the signal transmitted by the same reader) characterizing such systems is very low. However, thanks to the highly directive antennas utilized by the readers, tags ID can be correctly received within a radio range that can be as long as a few meters. Transmission may occur in several frequency bands spanning from low frequencies (LF) at 124–135 kHz up to ultra high frequencies (UHF) at 860–960 MHz that have the longest range.

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 (the radio is powered with the energy harvested by the reader signal). 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. As such, they can augment the awareness of a certain environment and, thus, act as a further bridge between physical and digital world. Usage of sensor net-

[1] New RFID tags, named *chipless tags*, are under study which do not use microchips so as to decrease production cost [Ted09]. Q2

works has been proposed in several application scenarios, such as environmental monitoring, e-health, intelligent transportation systems, military, and industrial plant monitoring.

Sensor networks consist of a certain number (which can be very high) of sensing nodes communicating in a wireless multi-hop fashion. Usually nodes report the results of their sensing to a small number (in most cases, only one) of special nodes called *sinks*. A large scientific literature has been produced on sensor networks in the recent past, addressing several problems at all layers of the protocol stack [22]. Design objectives of the proposed solutions are energy efficiency (which is the scarcest resource in most of the scenarios involving sensor networks), scalability (the number of nodes can be very high), reliability (the network may be used to report urgent alarm events), and robustness (sensor nodes are likely to be subject to failures for several reasons).

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 (WPAN) [23]. IEEE 802.15.4 does not include specifications on the higher layers of the protocol stack, which is necessary for the seamless integration of sensor nodes into the Internet. 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.

Integration of sensing technologies into passive RFID tags would enable a lot of completely new applications into the IoT context, especially into the e-health area [24]. Recently, several solutions have been proposed in this direction. As an example, the WISP project is being carried out at Intel Labs to develop *wireless identification and sensing platforms* (WISP) [25]. WISPs are powered and read by standard RFID readers, harvesting the power from the reader's querying signal. WISPs have been used to measure quantities in a certain environment, such as light, temperature, acceleration, strain, and liquid level.

Sensing RFID systems will allow to build RFID sensor networks [26], which consist of small, RFID-based sensing and computing devices, and RFID readers, which are the sinks of the data generated by the sensing RFID tags and provide the power for the network operation.

Table 1 compares the characteristics of RFID systems (RFID), wireless sensor networks (WSN), and RFID sensor networks (RSN) [26]. 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 (communication is peer-to-peer whereas, it is asymmetric for the other types of systems);
- RFID sensor network are the possibility of supporting sensing, computing, and communication capabilities in a passive system.

3.2. Middleware

The middleware is a software layer or a set of sub-layers interposed between the technological and the application levels. Its feature of hiding the details of different technologies is fundamental to exempt the programmer from issues that are not directly pertinent to her/his focus, which is the development of the specific application enabled by the IoT infrastructures. The middleware is gaining more and more importance in the last years due to its major role in simplifying the development of new services and the integration of legacy technologies into new ones. This excepts the programmer from the exact knowledge of the variegate set of technologies adopted by the lower layers.

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. The use of common interfaces and standard protocols gives a horizontal view of an enterprise system. Thus, the development of business processes enabled by the SOA is the result of the process of designing workflows of coordinated services, which eventually are associated with objects actions. This facilitates the interaction among the parts of an enterprise and allows for reducing the time necessary to adapt itself to the changes imposed by the market evolution [27]. A SOA approach also allows for software and hardware reusing, be-

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

Please cite this article in press as: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.05.010

cause it does not impose a specific technology for the service implementation [28].

Advantages of the SOA approach are recognized in most studies on middleware solutions for IoT. While a commonly accepted layered architecture is missing, the proposed solutions face essentially the same problems of abstracting the devices functionalities and communications capabilities, providing a common set of services and an environment for service composition. These common objectives lead to the definition of the middleware sketch shown in Fig. 2. It tries to encompass all the functionalities addressed in past works dealing with IoT middleware issues. It is quite similar to the scheme proposed in [29], which addresses the middleware issues with a complete and integrated architectural approach. It relies on the following layers.

3.2.1. 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. Through the use of standard web service protocols and service composition technologies, applications can realize a perfect integration between distributed systems and applications.

3.2.2. 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. On this layer there is no notion of devices and the only visible assets are services. An important insight into the service landscape is to have a repository of all currently connected service instances, which are executed in run-time to build composed services. The logic behind the creation and the management of complex services, can be expressed in terms of workflows of business processes, using workflow languages. In this context, a frequent choice is to adopt standard languages such as the Business Process Execution Language (BPEL) and Jolie [29,30]. Workflow languages define business processes that interact with external entities through Web Service operations, defined by using the Web Service Definition Language (WSDL) [31]. Workflows can be nested, so it is possible to call a workflow from inside another one. The creation of complex processes can be represented as a sequence of coordinated actions performed by single components.

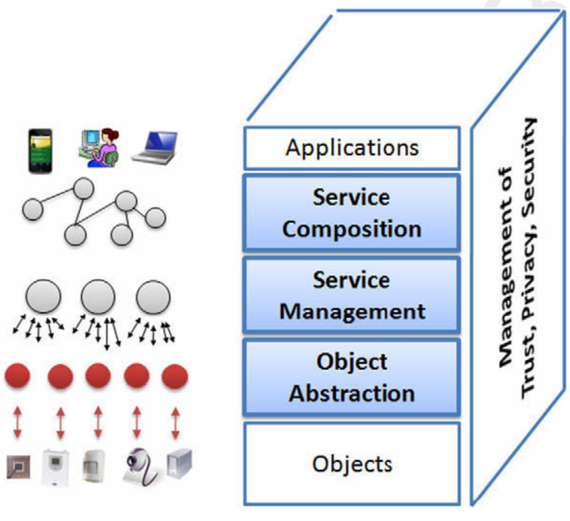

Fig. 2. SOA-based architecture for the IoT middleware.

3.2.3. 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. At this layer, some middleware proposals include an expanded set of functionalities related to the QoS management and lock management, as well as some semantic functions (e.g., police and context management) [32]. 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. The upper layer can then compose complex services by joining services provided at this layer.

3.2.4. 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. Accordingly, unless a device offers discoverable web services on an IP network, there is the need to introduce a wrapping layer, consisting of two main sub-layers: the interface and the communication sub-layers. The first one provides a web interface exposing the methods available through a standard web service interface and is responsible for the management of all the incoming/outcoming messaging operations involved in the communication with the external world. The second sub-layer implements the logic behind the web service methods and translates these methods into a set of device-specific commands to communicate with the real-world objects.

Some works proposed the embedding of TCP/IP stacks in the devices, such as the TinyTCP, the mIP and the IwIP (see [33] and references herein), which provide a socket like interface for embedded applications. Embedded web servers can then be integrated in the objects, performing the function of this object abstraction layer. 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 is then responsible to make the conversion into a standard web service language and, sometimes, elaborate the request to reduce the complexity of the operations required by the end-device [30].

Please cite this article in press as: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.05.010

3.2.5. Trust, privacy and security management

The deployment of automatic communication of objects in our lives represents a danger for our future. Indeed, unseen by users, embedded RFID tags in our personal devices, clothes, and groceries can unknowingly be triggered to reply with their ID and other information. This potentially enables a surveillance mechanism that would pervade large parts of our lives. 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 or (it happens more often) distributed through the entire stack, from the object abstraction to the service composition, in a manner that does not affect system performance or introduce excessive overheads.

While most of the proposed middleware solutions make use of the SOA approach, some others have followed a different way, especially if developed for a specific scenario (target application, specific set of objects or limited geographical scenario). One remarkable project is the Fosstrak one, which is specifically focused on the management of RFID related applications [34]. It is an open source RFID infrastructure that implements the interfaces defined in the EPC Network specifications. It provides the following services related to RFID management: data dissemination, data aggregation, data filtering, writing to a tag, trigger RFID 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 [35]. All these functions are made available to the application layer to ease the deployment of RFID-related services. In [36], the authors present another RFID-related middleware which relies on three functionalities: the tag, the place, and the scenic managers. The first allows the user to associate each tag to an object; the second supports creating and editing location information associated to RFID antennas; the third one is used to combine the events collected by the antennas and the developed related applications.

Another architecture that does not follow the SOA approach is proposed in the e-SENSE project, which focuses on issues related to capturing ambient intelligence through wireless sensor networks. The proposed architecture is divided into four logical subsystems, namely the application, management, middleware, and connectivity subsystems. Each subsystem comprises various protocol and control entities, which offer a wide range of services and functions at service access points to other subsystems [37]. This entire stack is implemented in a full function sensor node and in a gateway node; while a reduced-function sensor node has fewer functions. In the e-SENSE vision the middleware subsystem has the only purpose to develop and handle an infrastructure where information sensed by nodes is processed in a distributed fashion and, if necessary, the result is transmitted to an actuating node and/or to the fixed infrastructure by means of a gateway. The other functions that we have assigned to the middleware shown in Fig. 2 are attributed to other components and layers. The project UbiSec&Sens was also aimed at defining a comprehensive architecture for medium and large scale wireless sensor networks, with a particular attention to the security issues so as to provide a trusted and secure environment for all applications [38]. The middleware layer in this architecture mostly focuses on: (i) the secure long-term logging of the collected environmental data over time and over some regions (TinyPEDS), (ii) functions that provides the nodes in the network with the abstraction of shared memory (TinyDSM), (iii) the implementation of distributed information storage and collection (DISC) protocol for wireless sensor networks.

4. Applications

Potentialities offered by the IoT make possible the development of a huge number of applications, of which only a very small part is currently available to our society. 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, just to cite a few. These environments are now equipped with objects with only primitive intelligence, most of times without any communication capabilities. Giving these objects the possibility to communicate with each other and to elaborate the information perceived from the surroundings imply having different environments 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 (see Fig. 3). In the following subsections we provide a review of the short-medium term applications for each of these categories and a range of futuristic applications.

4.1. 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. Roads themselves and transported goods are also equipped with tags and sensors that send important information to traffic control sites and transportation vehicles to better route the traffic, help in the management of the depots, provide the tourist with appropriate transportation information, and monitor the status of the transported goods. Below, the main applications in the transportation and logistics domain are described.

4.1.1. Logistics

Real-time information processing technology based on RFID and NFC can realize real-time monitoring of almost every link of the supply chain, ranging from commodity design, raw material purchasing, production, transportation,

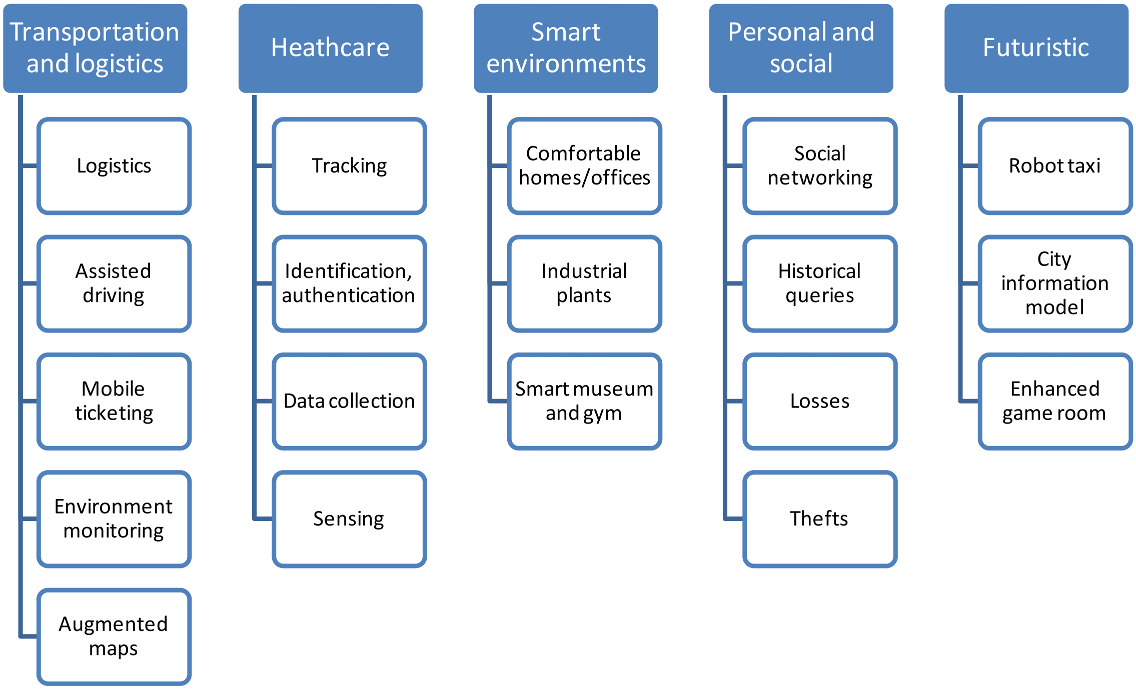

Fig. 3. Applications domains and relevant major scenarios.

storage, distribution and sale of semi-products and products, returns' processing and after-sales service..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. The application result is that the reaction time of traditional enterprises is 120 days from requirements of customers to the supply of commodity while advanced companies that make use of these technologies (such as Wal-mart and Metro) only needs few days and can basically work with zero safety stock [39,40]. Additionally, real-time access to the ERP program helps the shop assistants to better inform customers about availability of products and give them more product information in general [41].

4.1.2. 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. Collision avoidance systems and monitoring of transportation of hazardous materials are two typical example functions. Governmental authorities would also benefit from more accurate information about road traffic patterns for planning purposes. Whereas the private transportation traffic could better find the right path with appropriate information about the jam and incidents. Enterprises, such as freight companies, would be able to perform more effective route optimization which allows energy savings. Information about the movement of the vehicles transporting goods together with information about the type and status of the goods can integrated to provide important information about the delivery time, delivery delays, and faults. This information can be also combined with the status of the warehouses in order to automate the refilling of the magazines.

4.1.3. Mobile ticketing

Posters or panels providing information (description, costs, schedule) about transportation services can be equipped with an NFC tag, a visual marker and a numeric identifier. The user can then get information about several categories of options from the web by either hovering his mobile phone over the NFC tag, or pointing the mobile phone to the visual markers. The mobile phone automatically gets information from the associated web services (stations, numbers of passengers, costs, available seats and type of services) and allows the user to buy the related tickets [42].

4.1.4. Monitoring environmental parameters

Perishable goods such as fruits, fresh-cut produce, meat, and dairy products are vital parts of our nutrition. From the production to the consumption sites thousands of kilometers or even more are covered and during the transportation the conservation status (temperature, humidity, shock) need to be monitored to avoid uncertainty in quality levels for distribution decisions. Pervasive computing and sensor technologies offer great potential for improving the efficiency of the food supply chain [43,44].

Please cite this article in press as: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.05.010

4.1.5. Augmented maps

Touristic maps can be equipped with tags that allow NFC-equipped phones to browse it and automatically call web services providing information about hotels, restaurants, monuments and events related to the area of interest for the user [45]. There is a collection of Physical Mobile Interaction (PMI) techniques that can be employed to augment the information of the map:

- hovering within read range of a tag so that additional information regarding the marker is displayed on the phone screen;
- single selection/de-selection of tags by pressing a specific key when the tag is hovered;
- multi-selection/de-selection of different tags;
- polygon drawing by selecting the tags in a polygon that delimits an area of interest;
- picking-and-dropping, so that selected markers that have been 'picked up' using the phone can be dropped in the itinerary of interest;
- context menu displaying when a marker is hovered [46].

4.2. 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 (staff and patients); identification and authentication of people; automatic data collection and sensing [47].

4.2.1. 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, and tracking of motion through choke points, such as access to designated areas. In relation to assets, tracking is most frequently applied to continuous inventory location tracking (for example for maintenance, availability when needed and monitoring of use), and materials tracking to prevent left-ins during surgery, such as specimen and blood products.

4.2.2. Identification and authentication

It includes patient identification to reduce incidents harmful to patients (such as wrong drug/dose/time/procedure), comprehensive and current electronic medical record maintenance (both in the in- and out-patient settings), and infant identification in hospitals to prevent mismatching. In relation to staff, identification and authentication is most frequently used to grant access and to improve employee morale by addressing patient safety issues. In relation to assets, identification and authentication is predominantly used to meet the requirements of security procedures, to avoid thefts or losses of important instruments and products.

4.2.3. Data collection

Automatic data collection and transfer is mostly aimed at reducing form processing time, process automation (including data entry and collection errors), automated care and procedure auditing, and medical inventory management. This function also relates to integrating RFID technology with other health information and clinical application technologies within a facility and with potential expansions of such networks across providers and locations.

4.2.4. Sensing

Sensor devices enable function centered on patients, and in particular on diagnosing patient conditions, providing real-time information on patient health indicators. Application domains include different telemedicine solutions, monitoring patient compliance with medication regiment prescriptions, and alerting for patient well-being. In this capacity, sensors can be applied both in in-patient and out-patient care. Heterogeneous wireless access-based remote patient monitoring systems can be deployed to reach the patient everywhere, with multiple wireless technologies integrated to support continuous bio-signal monitoring in presence of patient mobility [48].

4.3. 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.

4.3.1. 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; domestic incidents can be avoided with appropriate monitoring and alarm systems; and energy can be saved by automatically switching off the electrical equipments when not needed. For instance, we may think of energy providers that use dynamically changing energy prices to influence the overall energy consumption in a way that smoothes load peaks. An automation logic may optimize the power consumption costs throughout the day by observing when the prices, which are provided by an external web service and are set according to the current energy production and consumption, are cheap and by considering the specific requirements of each appliances at home (battery charger, refrigerator, ovens) [30].

4.3.2. 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. In a generic scenario, as production parts reach the processing point, the tag is read by the RFID reader. An event is generated by the reader with all the necessary data, such as the RFID number, and stored on the network. The machine/robot gets notified by this event (as it has subscribed to the service) and picks up the production part. By matching data from the enterprise system and the RFID tag, it knows how to further process the part. In parallel, a wireless sensor mounted on the machine monitors the vibration and if it exceeds a specific threshold an event is raised to immediately stop the process (quality control). Once such an emergency event is propagated, devices that consume it react accordingly. The robot receives the emergency shutdown event and immediately stops its operation. The plant manager also immediately sees the status of the so called Enterprise Resource Planning (ERP) orders, the production progress, the device status, as well as a global view on all the elements and the possible side effects of a production line delay due to shop-floor device malfunctions [29].

4.3.3. Smart museum and gym

As to smart leisure environments, the museum and the gym are two representative examples where the IoT technologies can help in exploiting their facilities at the best. In the museum, for instance, expositions in the building may evoke various historical periods (Egyptian period or ice age) with widely diverging climate conditions. The building adjusts locally to these conditions while also taking into account outdoor conditions. 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. Health parameters are monitored during the whole training session and the reported values are checked to see if the trainee is overtraining or if she/he is too relaxed when doing the exercises.

4.4. 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 [36]. The following are the major applications.

4.4.1. 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. We may think of RFIDs that generate events about people and places to give users real-time updates in their social networks, which are then gathered and uploaded in social networking websites. Application user interfaces display a feed of events that their friends have preliminarily defined and the users can control their friend lists as well as what events are disclosed to which friends.

4.4.2. Historical queries

Historical queries about objects and events data let users study trends in their activities over time. This can be extremely useful for applications that support long-term activities such as business projects and collaborations. 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. Historical trends plots can also be automatically generated using the Google Charts API to display where, how, and with whom or what they have spent their time over some arbitrary period.

4.4.3. Losses

A search engine for things is a tool that helps in finding objects that we don't remember where have been left. 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. A more proactive extension of this application leverages user-defined events to notify users when the last recorded object location matches some conditions.

4.4.4. Thefts

An application similar to the previous one may allow the user to know if some objects are moved from a restricted area (the owner house or office), which would indicate that the object is being stolen. In this case, the event has to be notified immediately to the owner and/or to the security guards. For example, the application can send an SMS to the users when the stolen objects leave the building without any authorization (such as a laptop, a wallet or an ornament).

4.5. Futuristic applications domain Q3

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. Apart from these, we may envision many other applications, which we herein define *futuristic* since these rely on some (communications, sensing, material and/or industrial processes) technologies that either are still to come or whose implementation is still too complex. These applications are even more interesting in terms of required research and potential impact. An interesting analysis of this kind of applications is provided by SENSEI FP7 Project [49] from which we have taken the three most appealing applications.

4.5.1. Robot taxi

In future cities, robot taxis swarm together, moving in flocks, providing service where it is needed in a timely and efficient manner. The robot taxis respond to real-time traffic movements of the city, and are calibrated to reduce congestion at bottlenecks in the city and to service pick-up areas that are most frequently used. With or without a human driver, they weave in and out of traffic at optimum speeds, avoiding accidents through proximity sensors, which repel them magnetically from other objects on the road. They can be hailed from the side of the street by pointing a mobile phone at them or by using hand gestures. 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. On the rare occasions they are not in use, the taxis head for 'pit-stops' where they automatically stack themselves into tight bays which are instrumented with sensors where actuators set off recharging batteries, perform simple maintenance tasks and clean the cars. The pit-stops communicate with each other to ensure no over or under-utilization [49].

4.5.2. 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. Accordingly, nothing can be built legally unless it is compatible with CIM. The facilities management services communicate with each other and the CIM, sharing energy in the most cost-effective and resource-efficient fashion. They automatically trade surplus energy with each other and prices are calculated to match supply and demand. In this sense, planning and design is an ongoing social process, in which the performance of each item is being reported in real-time and compared with others. Population changes can be inferred, as can movement patterns, environmental performance, as well as the overall efficiency of products and buildings.

4.5.3. 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. The room uses this information to measure excitement and energy levels so that to control the game activity according to status of the player. Various objects are also placed throughout the room and the point of the game is to crawl and jump from one to the other without touching the floor. Points are awarded for long jumps and difficult places to reach. The game also puts a target on the wall-mounted screen. Whoever reaches that target first, wins. As the players work their way around the room, the game keeps track of their achievements. Their controller recognizes RFID tags on objects in the room. To score, they have to touch the object with it. As the game progresses, the system gradually makes it more difficult. At first the objects they have to reach are nearby and easy to reach. At some point it gets too difficult and both players must touch the floor with their feet. Then the game makes a loud noise to indicate that this was wrong. The room now notices that one player is a bit taller and faster than the other so it starts putting the objects a bit closer to him, so that he can keep up. The game then adapts the difficulty level and the target according to the achievements of the players so that to keep high the excitement level perceived by the console through the sensing devices.

5. Open issues

Although the enabling technologies described in Section 3 make the IoT concept feasible, a large research effort is still required. In this section, we firstly review the standardization activities that are being carried out on different IoT-related technologies (Section 5.1). Secondly, we show the most important research issues that need to be addressed to meet the requirements characterizing IoT scenarios. More specifically, in Section 5.2 we focus on addressing and networking issues, whereas in Section 5.3 we describe the problems related to security and privacy.

In Table 2 we summarize the open research issues, the causes for which they are specifically crucial for IoT scenarios and the sections when such issues will be discussed in detail.

5.1. Standardization activity

Several contributions to the full deployment and standardization of the IoT paradigm are coming from the scientific community. Among them, the most relevant are

Table 2
Open research issues.

Open issue	Brief description of the cause	Details in
Standards	There are several standardization efforts but they are not integrated in a comprehensive framework	Section 5.1
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	Section 5.2
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*	Section 5.2
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*	Section 5.2
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	Section 5.2
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	Section 5.3
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	Section 5.3
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	Section 5.3
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	Section 5.3

Please cite this article in press as: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.05.010

provided by the different sections of the Auto-ID Lab scattered all over the world [50,51,34], by the European Commission [52] and European Standards Organisations (ETSI, CEN, CENELEC, etc.), by their international counterparts (ISO, ITU), and by other standards bodies and consortia (IETF, EPCglobal, etc.). Inputs are particularly expected from the Machine-to-Machine Workgroup of the European Telecommunications Standards Institute (ETSI) and from some Internet Engineering Task Force (IETF) Working Groups. 6LoWPAN [53], aiming at making the IPv6 protocol compatible with low capacity devices, and ROLL [54], more interested in the routing issue for Internet of the Future scenarios, are the best candidates.

In Table 3 we summarize the fundamental characteristics of the main standards of interest in terms of objectives of the standard, status of the standardization process, communication range, data rate, and cost of devices. In the table we highlight the standards that are discussed in detail in this section.

With regards to the RFID technology, it is currently slowed down by fragmented efforts towards standardization, which is focusing on a couple of principal areas: RFID frequency and readers-tags (tags-reader) 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. The production of a recommendation for the "EPCglobal Architecture Framework" is a EPCglobal objective, shared with a community of experts and several organizations, including Auto-ID Labs, GS1 Global Office, GS1 Member Organizations, government agencies, and non-governmental organizations (NGOs). Interesting results are already available [5].

As for the European Commission efforts, the event that might have the strongest influence on the future RFID standardization process is undoubtedly the official constitution of the so called "Informal working group on the implementation of the RFID". This is composed of stakeholders (industry, operators, European standard organisations, civil society organisations, data protection authorities, etc.) required "to be familiar with RFID in general, the Data Protection Directive and the RFID Recommendation".

One of these stakeholders, CEN (European Committee for Standardization) [55], although does not conduct any activity specifically related to the IoT, is interested in RFID evolution towards IoT. Among its Working Groups (WGs), the most relevant to the IoT are WG 1-4 BARCODES, WG 5 RFID, and the Global RFID Interoperability Forum for Standards (GRIFS). This latter is a two-year-project coordinated by GS1, ETSI, and CEN and aimed at defining standards related to physical objects (readers, tags, sensors), communications infrastructures, spectrum for RFID use, privacy and security issues affecting RFID [56].

Differently from these projects, ISO [57] focuses on technical issues such as the frequencies utilized, the modulation schemes, and the anti-collision protocol.

With regards to the IoT paradigm at large, a very interesting standardization effort is now starting in ETSI [58] (the European Telecommunications Standards Institute, which produces globally-applicable ICT related standards). Within ETSI, in fact, the Machine-to-Machine (M2M) Technical Committee was launched, to the purpose of conducting standardization activities relevant to M2M systems and sensor networks (in the view of the IoT). M2M is a real leading paradigm towards IoT, but there is very little standardization for it, while the multiplicity of the solutions on the market use standard Internet, Cellular, and Web technologies. Therefore, the goals of the ETSI M2M committee include: the development and the maintenance of an end-to-end architecture for M2M (with end-to-end IP philosophy behind it), strengthening the standardization efforts on M2M, including sensor network integration, naming, addressing, location, QoS, security, charging, management, application, and hardware interfaces [59].

As for the Internet Engineering Task Force (IETF) activities related to the IoT, we can say that recently the *IPv6*

Table 3
Characteristics of the most relevant standardization activities.

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

over Low-Power Wireless Personal Area Networks (6LOWPAN) IETF group was born [53]. 6LOWPAN is defining a set of protocols that can be used to integrate sensor nodes into IPv6 networks. Core protocols composing the 6LOWPAN architecture have been already specified and some commercial products have been already released that implement this protocol suite. The 6LOWPAN working group is currently moving four Internet-Drafts towards last call in the standards track (Improved Header Compression, 6LoWPAN Neighbour Discovery) and informational track (Use Cases, Routing Requirements) [60].

A further relevant IETF Working Group is named *Routing Over Low power and Lossy networks* (ROLL). It has recently produced the RPL (pronounced "ripple") routing protocol draft. This will be the basis for routing over low-power and lossy networks including 6LoWPAN, which still needs lots of contributions to reach a full solution.

We clearly understand, from what is described above, that an emerging idea is to consider the IoT standardisation as an integral part of the Future Internet definition and standardisation process. This assertion was recently made by the cluster of European R&D projects on the IoT (CERP-IoT). According to it, the integration of different *things* into wider networks, either mobile or fixed, will allow their interconnection with the Future Internet [61].

What is worth pointing out in the cited standardization areas is the tight collaboration between standardization Institutions and other world-wide Interest Groups and Alliances. It seems that the whole industry is willing to cooperate on achieving the IoT. IPSO, but also the ZigBee Alliance, the IETF and the IEEE work in the same direction of IP standards integration [61].

5.2. Addressing and networking issues

The IoT will include an incredibly high number of nodes, each of which will produce content that should be retrievable by any authorized user regardless of her/his position. This requires effective addressing policies. Currently, the IPv4 protocol identifies each node through a 4-byte address. It is well known that the number of available IPv4 addresses is decreasing rapidly and will soon reach zero. Therefore, it is clear that other addressing policies should be used other than that utilized by IPv4.

In this context, as we already said in Section 5.1, IPv6 addressing has been proposed for low-power wireless communication nodes within the 6LOWPAN context. IPv6 addresses are expressed by means of 128 bits and therefore, it is possible to define 10^{38} addresses, which should be enough to identify any object which is worth to be addressed. Accordingly, we may think to assign an IPv6 address to all the *things* included in the network. However, since RFID tags use 64–96 bits 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 [62] and methodologies to integrate RFID identifiers and IPv6 addresses have been proposed. For example, in [63] authors propose to use the 64 bits of the interface identifier of the IPv6 address to report the RFID tag identifier, whereas the other 64 bits of the network prefix are used to address the gateway between the RFID system and the Internet.

Accordingly, the gateway will handle messages generated by RFID tags that must leave the RFID system and enter the Internet as follows. 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 (which is copied into the network prefix part of the IPv6 address) and the RFID tag identifier (which is copied into the interface identifier part of the IPv6 address). Analogously, the gateway will handle IPv6 packets coming from the Internet and directed towards a certain RFID tag as follows. The specific RFID tag, which represents the destination of the message, will be easily recognized as its identifier is reported into the interface identifier part of the IPv6 address; the specific message (which in most cases represents the request of a certain operation) will be, instead, notified to the relevant RFID reader(s).

This approach, however, cannot be used if the RFID tag identifier is long 96 bits, as allowed by the EPCglobal standard. To solve this problem, in [64] a methodology is proposed that uses an appropriate network element, called *agent*, that maps the RFID identifier (regardless of its length) into a 64 bits field which will be used as the interface ID of the IPv6 address. Obviously, the agent must keep updated a mapping between the IPv6 addresses generated and the RFID tag identifier.

A complete different approach is illustrated in [65], where the RFID message and headers are included into the IPv6 packet payload as shown in Fig. 4.

It is important to note, however, that in all the above cases RFID mobility is not supported. In fact, the common basic assumption is that each RFID can be reached through a given gateway between the network and the RFID system.

It follows that appropriate mechanisms are required to support mobility in the IoT scenarios. In this contexts, the overall system will be composed of a large number of subsystems with extremely different characteristics. In the past, several solutions have been proposed for the mobility management [66]; however, their validity in the IoT scenarios should be proven as they may have problems in terms of scalability and adaptability to be applied in such a heterogeneous environment. To this purpose it is important to note that higher scalability can be achieved by solutions based on the utilization of a home agent (like Mobile IP [67]), rather than by solutions based on *home location registers* (HLR) and *visitor location registers* (VLR), which are widely used in cellular networks. In fact, Mobile IP-like protocols do not use central servers, which are critical from a scalability point of view.

Another issue regards the way in which addresses are obtained. In the traditional Internet any host address is identified by querying appropriate servers called *domain name servers* (DNS). Objective of DNSs is to provide the IP address of a host from a certain input name. In the IoT, communications are likely to occur between (or with) *objects* instead of hosts. Therefore, the concept of *Object Name Service* (ONS) must be introduced, which associates a reference to a description of the specific object and the related RFID tag identifier [68,5]. In fact, the

Please cite this article in press as: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.05.010

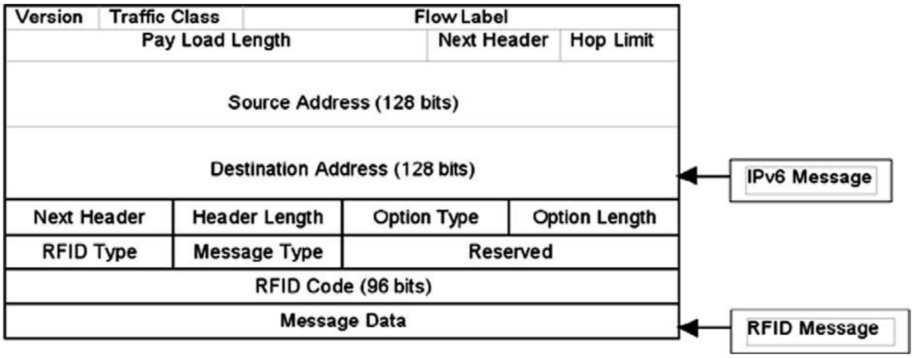

Fig. 4. Encapsulation of RFID message into an IPv6 packet.

tag identifier is mapped into a *Internet Uniform Reference Locator* (URL), which points to relevant information of the object. In the IoT, the ONS should operate in both directions, i.e., should be able to associate the description of the object specified to a given RFID tag identifier, and vice versa. Inverting the function is not easy and requires an appropriate service, which is called *Object Code Mapping Service* (OCMS). Desired characteristics for OCMSs are reported in [69], where a P2P approach is suggested in order to improve scalability. However, note that design and assessment of OCMS in complex operational environments, such as the IoT, is still an open issue.

Also a new conception of the transport layer is required for the IoT. Major goals of the transport layer are to guarantee end-to-end reliability and to perform end-to-end congestion control. In the traditional Internet, the protocol utilized at the transport layer for reliable communications is the *Transmission Control Protocol* (TCP) [70]. It is obvious that TCP is inadequate for the IoT, due to the following reasons:

1. *Connection setup*: TCP is connection oriented and each session begins with a connection setup procedure (the so called *three ways handshake*). 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. Furthermore, the connection setup phase involves data to be processed and transmitted by end-terminals, which in most cases are limited in terms of both energy and communication resources, such as sensor nodes and RFID tags.
2. *Congestion control*: TCP is responsible of performing end-to-end congestion control. In the IoT this may cause performance problems as most of the communications will exploit the wireless medium, which is known to be a challenging environment for TCP [71]. Furthermore, 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.
3. *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. At the destination data should be buffered to provide ordered delivery of data to the application. Management of such buffers may be too costly in terms of required energy for battery-less devices.

As a consequence, TCP cannot be used efficiently for the end-to-end transmission control in the IoT. Up to date, no solutions have been proposed for the IoT and therefore, research contributions are required.

Furthermore, we do not know what will be the characteristics of the traffic exchanged by smart objects in the IoT. Whereas it is fundamental to investigate such characteristics as they should be the basis for the design of the network infrastructures and protocols.

Accordingly, another important research issue concerning the networking aspects is related to traffic characterization. It is well known that traffic characteristics in wireless sensor networks strongly depend on the application scenario (see [72], for example). This was not a problem as the interest was focused on the traffic flow inside the wireless sensor network itself. Complications arise when, according to the IoT paradigm, sensor nodes become part of the overall Internet. In fact, in this scenario, the Internet will be traversed by a large amount of data generated by sensor networks deployed for heterogeneous purposes and thus, with extremely different traffic characteristics. Furthermore, since the deployment of large scale, distributed RFID systems is still at the very beginning, the characteristics of the related traffic flows have not been studied so far, and therefore, the traffic which will traverse the IoT is completely unknown.

On the contrary characterization of the traffic is very important as it is necessary to network providers for planning the expansion of their infrastructures (if needed).

Finally, traffic characterization and modeling together with a list of traffic requirements is needed to devise appropriate solutions for supporting quality of service (QoS). In fact, if some work has been done for supporting QoS in wireless sensor networks [73], the problem is still completely unexplored in RFID systems. Accordingly, a large research effort is needed in the field of QoS support in the IoT. We believe that there will be several analogies with QoS for machine-to-machine communications. Since such types of communications have been already ad-

Please cite this article in press as: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.05.010

dressed in recent years [74], we can apply to the IoT scenarios QoS management schemes proposed for M2M scenarios. Obviously, this should be just a starting point and specific solutions for the IoT should be introduced in the future.

5.3. Security and privacy

People will resist the IoT as long as there is no public confidence that it will not cause serious threats to privacy. All the talking and complains (see [75] for example) following the announcement by the Italian retailer Benetton on the plan to tag a complete line of clothes (around 15 million RFIDs) has been the first, clear confirmation of this mistrust towards the use that will be done of the data collected by the IoT technologies [76].

Public concerns are indeed likely to focus on a certain number of security and privacy issues [21,77].

5.3.1. Security

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. Finally, most of the IoT components are characterized by low capabilities in terms of both energy and computing resources (this is especially the case for passive components) and thus, they cannot implement complex schemes supporting security.

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 IoT such approaches are not feasible given that passive RFID tags cannot exchange too many messages with the authentication servers. The same reasoning applies (in a less restrictive way) to the sensor nodes as well.

In this context, note that several solutions have been proposed for sensor networks in the recent past [78]. However, existing solutions can be applied when sensor nodes are considered as part of a sensor network connected to the rest of the Internet via some nodes playing the roles of gateways. In the IoT scenarios, instead, sensor nodes must be seen as nodes of the Internet, so that it becomes necessary to authenticate them even from nodes not belonging to the same sensor network.

In the last few years, some solutions have been proposed for RFID systems, however, they all have serious problems as described in [21].

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 (consider an electronic passport for example, or some keys based on RFID). The attack depicted in Fig. 5 could be successfully performed.

Consider the case in which A is the node that wants to authenticate other system elements through some RF mechanism and that an attacker wants to stole the identity of the element B (please note that that B can be any IoT element capable of computing and communicating). The attacker will position two transceivers. The first close to A, which we call B' and the second close to B, which we call A'. The basic idea is to make A believe that B' is B, and make B believe that A' is A. To this purpose, node B' will transmit the query signal received by the authenticating node A to the transceiver A'. The transceiver A' will transmit such signal so that B can receive it. Observe, that the signal transmitted by A' is an exact replica of the signal transmitted by A. Accordingly, it is impossible for node B to understand that the signal was not transmitted by A and therefore, it will reply with its identification. Node A' receives such reply and transmits it to node B', that will transmit it to node A. Node A cannot distinguish that such reply was not transmitted by B, and therefore, will identify the transceiver B' as the element B and provide access accordingly. Observe that this can be done regardless of the fact that the signal is encrypted or not.

Data integrity solutions should guarantee that an adversary cannot modify data in the transaction without the system detecting the change. The problem of data integrity has been extensively studied in all traditional computing and communication systems and some preliminary results exist for sensor networks, e.g., [79]. However, new problems arise when RFID systems are integrated in the Internet as they spend most of the time unattended. Data can be modified by adversaries while it is stored in the node or when it traverses the network [80]. To protect data against the first type of attack, memory is protected in most tag technologies and solutions have been proposed for wireless sensor networks as well [81]. For example, both *EPCglobal Class-1 Generation-2* and *ISO/IEC 18000–3* tags protect both read and write operations on their memory with a password. In fact, *EPCglobal Class-1 Generation-2* tags have five areas of memory, each of which can be protected in read or write with a password independently of each others. Whereas, *ISO/18000–3* tags define a pointer to a memory address and protect with a password all memory areas with a lower memory address. To protect data against the second type of attack, messages may be protected according to the *Keyed-Hash Message Authentication Code* (HMAC) scheme [82]. This is based on a common

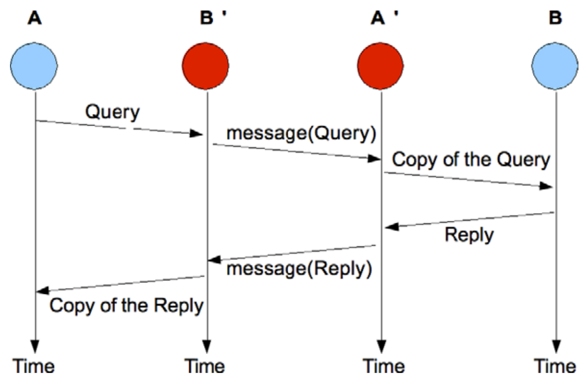

Fig. 5. Man in the middle attack.

Please cite this article in press as: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.05.010

secret key shared between the tag and the destination of the message, which is used in combination with a hash function to provide authentication.

Observe that the above solutions proposed to support data integrity when RFID systems are considered have serious problems. In fact, the password length supported by most tag technologies is too short to provide strong levels of protections. Moreover, even if longer passwords are supported, still their management remains a challenging task, especially when entities belonging to different organizations, as in the case of the IoT, are involved.

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 (like RFID tags and sensor nodes) that are seriously constrained in terms of energy, communications, and computation capabilities. It follows that new solutions are required able to provide a satisfactory level of security regardless of the scarcity of resources. In this context, a few solutions have been proposed for light symmetric key cryptographic schemes (see [83,84] for RFID scenarios and [78] for sensor network scenarios). However, as we already said, key management schemes are still at an early stage (especially in the case of RFID) and require large research efforts.

5.3.2 Privacy

The concept of *privacy* is deeply rooted into our civilizations, is recognized in all legislations of civilized countries and, as we already said, concerns about its protection have proven to be a significant barrier against the diffusion of the technologies involved in the IoT [75]. 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 are completely different from those that we now know and there will be an amazing number of occasions for personal data to be collected. Therefore, for human individuals it will be impossible to personally control the disclosure of their personal information.

Furthermore, the cost of information storage continues to decrease and is now approaching 10^{-9} euro per byte. Accordingly, once information is generated, will most probably be retained indefinitely, which involves denial of digital forgetting in people perspective.

It follows that the IoT really represents an environment in which privacy of individuals is seriously menaced in several ways. Furthermore, while in the traditional Internet problems of privacy arise mostly for Internet users (individuals playing an active role), in the IoT scenarios privacy problems arise even for people not using any IoT service.

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; and, finally, the above data should be stored only until it is strictly needed. For example, consider the application scenario regarding *Comfortable homes and offices* described in Section 4.3, and focus on the case of a building where several offices are located. In this case, some sensing capabilities will be deployed in the environment to track position of people and control the lighting or heating accordingly. If the tracking system is deployed only for increasing comfort of the offices while reducing energy consumption, then, appropriate policies 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 (position and movements of people should not be linkable to their identities);
- people are informed of the scope and the way in which their movements are tracked by the system (taking people informed about possible leaks of their privacy is essential and required by most legislations);
- 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.

To handle the data collection process appropriate solutions are needed in all the different subsystems interacting with human beings in the IoT. For example, in the context of traditional Internet services the W3C group has defined the *Platform for Privacy Preferences* (P3P) [85], which provides a language for the description of the privacy preferences and policies and therefore, allows automatic negotiation of the parameters concerning privacy based on the needs of personal information for running the service and the privacy requirements set by the user. Always in the context of traditional Internet services, through appropriate settings of the applications run on the user terminals, the time instants when personal information are being released can be easily detected and the entity collecting such data can be identified through well established authentication procedures.

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. For example, consider a sensor network composed of cameras deployed in a certain area. The only way an individual can avoid such cameras not to take her/his image is not to enter into the area. In this context, a possible solution that can reduce privacy problems might be to restrict the network's ability to gather data at a detail level that could compromise privacy [86]. For example, a sensor network might anonymize data by reporting only approximate locations of sensed individuals and tradeoff privacy requirements with the level of details required by the application. Another example regarding sensor networks composed of cameras deployed for video surveillance purposes. In this case, images of people can be blurred in order to protect their privacy [87]. If some event occurs, then the image of relevant people can be reconstructed by the law enforcement personnel.

In the case of RFID systems, the problem is twofold. In fact, on the one hand usually RFID tags are passive and reply to readers queries regardless of the desire of their proprietary. On the other hand an attacker can eavesdrop the reply from a tag to another authorized reader. Solutions to the first type of problems proposed so far are based on authentication of authorized readers (which have been discussed above). However, such solutions require tags that are able to perform authentication procedures. This involves higher costs and an authentication infrastructure, which, as we have already said, cannot be deployed in complex systems like those expected in IoT scenarios. Accordingly, solutions have been recently proposed (see [88] for example) that use a new system that, on the basis of preferences set by the user, negotiates privacy on her/his behalf. The privacy decisions taken by the above system can be enforced by creating collisions in the wireless channel with the replies transmitted by the RFID tags, which should not be read [89].

Avoiding eavesdropping by attacker in RFID systems can be accomplished through protecting the communication with encryption as explained above. However, these types of solutions still allow malicious readers to detect the presence of the RFID tags scanned by the authorized reader. 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 [90].

In order to ensure that the personal data collected is used only to support authorized services by authorized providers, solutions have been proposed that usually rely on a system called *privacy broker* [91]. The proxy interacts with the user on the one side and with the services on the other. Accordingly, it guarantees that the provider obtains only the information about the user which is strictly needed. The user can set the preferences of the proxy. When sensor networks and RFID systems are included in the network, then the proxy operates between them and the services. However, note that in this case the individual cannot set and control the policies utilized by the privacy brokers. Moreover, observe that such solutions based on privacy proxies suffer from scalability problems.

Finally, studies are still at the beginning regarding digital forgetting as this has been recognized as an important issue only recently [92]. In fact, as the cost of storage decreases, the amount of data that can be memorized increases dramatically. Accordingly, there is the need to create solutions that periodically delete information that is of no use for the purpose it was generated. Accordingly, the new software tools that will be developed in the future should support such forgetting functionalities. For example, a few experimental solutions have been developed and released for public use in the recent past that allow users to insert and share pictures and other types of files over the Internet with the assurance that such pictures will expire at a certain date and will be deleted afterwards (see drop.io and the Guest Pass features on Flickr for example [93]). Porting of such solutions to the IoT context is not straightforward and requires further research effort.

6. Conclusions

The Internet has changed drastically the way we live, moving interactions between people at a *virtual* level in several contexts spanning from the professional life to social relationships. 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, anymedia, anything" communications.

To this purpose, we observe that the IoT should be considered as part of the overall Internet of the future, which is likely to be dramatically different from the Internet we use today. In fact, it is clear that the current Internet paradigm, which supports and has been built around host-to-host communications, is now a limiting factor for the current use of the Internet. It has become clear that Internet is mostly used for the publishing and retrieving of information (regardless of the host where such information is published or retrieved from) and therefore, information should be the focus of communication and networking solutions. This leads to the concept of data-centric networks, which has been investigated only recently [94]. According to such a concept, data and the related queries are self-addressable and self-routable.

In this perspective, the current trend, which we have highlighted in Section 5.2, 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. Therefore, it is possible that the Internet evolution will require a change in the above trend.

Another interesting paradigm which is emerging in the Internet of the Future context is the so called *Web Squared*, which is an evolution of the Web 2.0. It is aimed at integrating web and sensing technologies [95] 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 sensors (microphone, cameras, GPS, etc.) deployed in the user terminals. In this perspective, observe that Web Squared can be considered as one of the applications running over the IoT, like the Web is today an (important) application running over the Internet.

In this paper, we have surveyed the most important aspects of the IoT with emphasis on what is being done and what are the issues that require further research. Indeed, current technologies make the IoT concept feasible but do not fit well with the scalability and efficiency requirements they will face. We believe that, given the interest shown by industries in the IoT applications, in the next years addressing such issues will be a powerful driving factor for networking and communication research in both industrial and academic laboratories.

References

[1] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010. ISBN: 978-1-4419-1673-0.
[2] National Intelligence Council, Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests Out to 2025 – Conference Report CR 2008-07, April 2008, <http://www.dni.gov/nic/NIC_home.html>.

[3] INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems, in: Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future, Version 1.1, 27 May 2008.
[4] Auto-Id Labs, <http://www.autoidlabs.org/>.
[5] The EPCglobal Architecture Framework, EPCglobal Final Version 1.3, Approved 19 March 2009, <www.epcglobalinc.org>.
[6] K. Sakamura, Challenges in the age of ubiquitous computing: a case study of T-engine – an open development platform for embedded systems, in: Proceedings of ICSE'06, Shanghai, China, May 2006.
[7] 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, <http://www.eurescom.eu/message>.
[8] M. Botterman, for the European Commission Information Society and Media Directorate General, Networked Enterprise & RFID Unit – D4, Internet of Things: An Early Reality of the Future Internet, Report of the Internet of Things Workshop, Prague, Czech Republic, May 2009.
[9] B. Sterling, Shaping Things – Mediawork Pamphlets, The MIT Press, 2005.
[10] ITU Internet Reports, The Internet of Things, November 2005.
[11] A. Dunkels, J.P. Vasseur, IP for Smart Objects, Internet Protocol for Smart Objects (IPSO) Alliance, White Paper #1, September 2008, <http://www.ipso-alliance.org>.
[12] J. Hui, D. Culler, S. Chakrabarti, 6LoWPAN: Incorporating IEEE 802.15.4 Into the IP Architecture – Internet Protocol for Smart Objects (IPSO) Alliance, White Paper #3, January 2009, <http://www.ipso-alliance.org>.
[13] N. Gershenfeld, R. Krikorian, D. Cohen, The internet of things, Scientific American 291 (4) (2004) 76–81.
[14] I. Toma, E. Simperl, Graham Hench, A joint roadmap for semantic technologies and the internet of things, in: Proceedings of the Third STI Roadmapping Workshop, Crete, Greece, June 2009.
[15] A. Katasonov, O. Kaykova, O. Khriyenko, S. Nikitin, V. Terziyan, Smart semantic middleware for the internet of things, in: Proceedings of the Fifth International Conference on Informatics in Control, Automation and Robotics, Funchal, Madeira, Portugal, May 2008.
[16] W. Wahlster, Web 3.0: Semantic Technologies for the Internet of Services and of Things, Lecture at the 2008 Dresden Future Forum, June 2008.
[17] I. Vázquez, Social Devices: Semantic Technology for the Internet of Things, Week@ESI, Zamudio, Spain, June 2009.
[18] D. Guinard, T. Vlad, Towards the web of things: web mashups for embedded devices, in: Proceedings of the International World Wide Web Conference 2009 (WWW 2009), Madrid, Spain, April 2009.
[19] L. Srivastava, Pervasive, ambient, ubiquitous: the magic of radio, in: European Commission Conference "From RFID to the Internet of Things", Bruxelles, Belgium, March 2006.
[20] K. Finkenzeller, RFID Handbook, Wiley, 2003.
[21] A. Jules, RFID security and privacy: a research survey, IEEE Journal on Selected Areas in Communications 24 (2) (2006) 381–394.
[22] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (4) (2002) 393–422.
[23] <http://ieee802.org/15>.
[24] G. Marrocco, C. Occhiuzzi, F. Amato, Sensor-oriented passive RFID, in: Proceedings of TIWDC 2009, Pula, Italy, September 2009.
[25] <http://seattle.intel-research.net/wisp/>.
[26] M. Buettner, B. Greenstein, A. Sample, J.R. Smith, D. Wetherall, Revisiting smart dust with RFID sensor networks, in: Proceedings of ACM HotNets 2008, Calgary, Canada, October 2008.
[27] S. De Deugd, R. Carroll, K. Kelly, B. Millett, J. Ricker, SODA: service oriented device architecture, IEEE Pervasive Computing 5 (3) (2006) 94–96.
[28] J. Pasley, How BPEL and SOA are changing web services development, IEEE Internet Computing 9 (3) (2005) 60–67.
[29] P. Spiess, S. Karnouskos, D. Guinard, D. Savio, O. Baecker, L. Souza, V. Trifa, SOA-based integration of the internet of things in enterprise services, in: Proceedings of IEEE ICWS 2009, Los Angeles, Ca, USA, July 2009.
[30] C. Buckl, S. Sommer, A. Scholz, A. Knoll, A. Kemper, J. Heuer, A. Schmitt, Services to the field: an approach for resource constrained sensor/actor networks, in: Proceedings of WAINA'09, Bradford, United Kingdom, May 2009.
[31] OASIS, Web Services Business Process Execution Language Version 2.0, Working Draft, <http://docs.oasis-open.org/wsbpel/2.0/wsbpelspecificationdraft.pdf>.
[32] Hydra Middleware Project, FP6 European Project, <http://www.hydramiddleware.eu>.
[33] S. Duquennoy, G. Grimaud, J.-J. Vandewalle, The web of things: interconnecting devices with high usability and performance, in: Proceedings of ICESS '09, HangZhou, Zhejiang, China, May 2009.
[34] <http://www.fosstrak.org>.
[35] C. Floerkemeier, C. Roduner, M. Lampe, RFID application development with the Accada middleware platform, IEEE System Journal 1 (2) (2007) 82–94.
[36] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, G. Borriello, Building the internet of things using RFID: the RFID ecosystem experience, IEEE Internet Computing 13 (3) (2009) 48–55.
[37] <http://www.ist-e-sense.org>.
[38] <http://www.ist-ubisecsens.org>.
[39] R. Yuan, L. Shumin, Y. Baogang, Value Chain Oriented RFID System Framework and Enterprise Application, Science Press, Beijing, 2007.
[40] METRO Group Future Store Initiative, <http://www.futurestore.org/>.
[41] S. Karpischek, F. Michahelles, F. Resatsch, E. Fleisch, Mobile sales assistant – an NFC-based product information system for retailers, in: Proceedings of the First International Workshop on Near Field Communications 2009, Hagenberg, Austria, February 2009.
[42] G. Broll, E. Rukzio, M. Paolucci, M. Wagner, A. Schmidt, H. Hussmann, PERCI: pervasive service interaction with the internet of things, IEEE Internet Computing 13 (6) (2009) 74–81.
[43] A. Ilic, T. Staake, E. Fleisch, Using sensor information to reduce the carbon footprint of perishable goods, IEEE Pervasive Computing 8 (1) (2009) 22–29.
[44] A. Dada, F. Thiesse, Sensor applications in the supply chain: the example of quality-based issuing of perishables, in: Proceedings of Internet of Things 2008, Zurich, Switzerland, May 2008.
[45] D. Reilly, M. Welsman-Dinelle, C. Bate, K. Inkpen, Just point and click? Using handhelds to interact with paper maps, in: Proceedings of ACM MobileHCI'05, University of Salzburg, Austria, September 2005.
[46] R. Hardy, E. Rukzio, Touch & interact: touch-based interaction of mobile phones with displays, in: Proceedings of ACM MobileHCI '08, Amsterdam, The Netherlands, September 2008.
[47] A.M. Vilamovska, E. Hattziandreu, R. Schindler, C. Van Oranje, H. De Vries, J. Krapelse, RFID Application in Healthcare – Scoping and Identifying Areas for RFID Deployment in Healthcare Delivery, RAND Europe, February 2009.
[48] D. Niyato, E. Hossain, S. Camorlinga, Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization, IEEE Journal on Selected Areas in Communications 27 (4) (2009) 412–423.
[49] SENSEI FP7 Project, Scenario Portfolio, User and Context Requirements, Deliverable 1.1, <http://www.sensei-project.eu/>.
[50] C. Floerkemeier, R. Bhattacharyya, S. Sarma, Beyond RFID, in: Proceedings of TIWDC 2009, Pula, Italy, September 2009.
[51] J. Sung, T. Sanchez Lopez, D. Kim, The EPC sensor network for RFID and WSN integration infrastructure, in: Proceedings of IEEE PerComW'07, White Plains, NY, USA, March 2007.
[52] Commission of the European Communities, Early Challenges Regarding the "Internet of Things", 2008.
[53] N. Kushalnagar, G. Montenegro, C. Schumacher, IPv6 Over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, IETF RFC 4919, August 2007.
[54] M. Weiser, The computer for the 21st century, ACM Mobile Computing and Communications Review 3 (3) (1999) 3–11.
[55] <http://www.cen.eu>.
[56] A. Nilssen, Security and privacy standardization in internet of things, in: eMatch'09 – Future Internet Workshop, Oslo, Norway, September 2009.
[57] <http://www.iso.org>.
[58] <http://www.etsi.org>.
[59] Z. Shelby, ETSI M2M Standardization, March 16, 2009, <http://zachshelby.org>.
[60] Z. Shelby, News from the 75th IETF, August 3, 2009, <http://zachshelby.org>.
[61] G. Santucci, Internet of the future and internet of things: what is at stake and how are we getting prepared for them? in: eMatch'09 – Future Internet Workshop, Oslo, Norway, September 2009.
[62] Y.-W. Ma, C.-F. Lai, Y.-M. Huang, J.-L. Chen, Mobile RFID with IPv6 for phone services, in: Proceedings of IEEE ISCE 2009, Kyoto, Japan, May 2009.

[63] S.-D. Lee, M.-K. Shin, H.-J. Kim, EPC vs. IPv6 mapping mechanism, in: Proceedings of Ninth International Conference on Advanced Communication Technology, Phoenix Park, South Korea, February 2007.
[64] D.G. Yoo, D.H. Lee, C.H. Seo, S.G. Choi, RFID networking mechanism using address management agent, in: Proceedings of NCM 2008, Gyeongju, South Korea, September 2008.
[65] <http://ipv6.com/articles/applications/Using-RFID-and-IPv6.htm>.
[66] I.F. Akyildiz, J. Xie, S. Mohanty, A survey on mobility management in next generation All-IP based wireless systems, IEEE Wireless Communications Magazine 11 (4) (2004) 16–28.
[67] C. Perkins, IP Mobility Support for IPv4, IETF RFC 3344, August 2002.
[68] M. Mealling, Auto-ID Object Name Service (ONS) v1.0, Auto-ID Center Working Draft, August 2003.
[69] V. Krylov, A. Logvinov, D. Ponomarev, EPC Object Code Mapping Service Software Architecture: Web Approach, MERA Networks Publications, 2008.
[70] V. Cerf, Y. Dalal, C. Sunshine, Specification of Internet Transmission Control Program, IETF RFC 675, December 1974.
[71] T. V Lakshman, U. Madhow, The performance of TCP/IP for networks with high bandwidth-delay products and random loss, IEEE/ACM Transactions on Networking 5 (3) (1997) 336–350.
[72] I. Demirkol, F. Alagoz, H. Deliç, C. Ersoy, Wireless sensor networks for intrusion detection: packet traffic modeling, IEEE Communication Letters 10 (1) (2006) 22–24.
[73] D. Chen, P.K. Varshney, QoS support in wireless sensor networks: a survey, in: Proceedings of International Conference on Wireless Networks 2004, Las Vegas, NE, USA, June 2004.
[74] T. Van Landegem, H. Viswanathan, Anywhere, Anytime, Immersive Communications, Enriching Communications, vol. 2, No. 1, 2008, <http://www2.alcatel-lucent.com/enrich/en/previous-editions/>.
[75] <http://www.boycottbenetton.com/>.
[76] Benetton to tag 15 million items, RFID Journal (March) (2003), <http://www.rfidjournal.com/article/articleview/344/1/1/>.
[77] J. Bukley, From RFID to the internet of things: final report, in: European Commission Conference "From RFID to the Internet of Things", Brussels, Belgium, March 2006.
[78] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, in: Proceedings of the Ninth ACM Conference on Computer and Communications Security, Washington, DC, USA, November 2002.
[79] R. Acharya, K. Asha, Data integrity and intrusion detection in wireless sensor networks, in: Proceedings of IEEE ICON 2008, New Delhi, India, December 2008.
[80] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, T. Phillips, Guidelines for Securing Radio Frequency Identification (RFID) Systems, NIST Special Publication 800-98, April 2007.
[81] R. Kumar, E. Kohler, M. Srivastava, Harbor: software-based memory protection for sensor nodes, in: Proceedings of IPSN 2007, Cambridge, MA, USA, April 2007.
[82] H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed-Hashing for Message Authentication, IETF RFC 2104, February 1997.
[83] M. Feldhofer, S. Dominikus, J. Wolkerstorfer, Strong authentication for RFID systems using AES algorithm, in: Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Cambridge, MA, USA, August 2004.
[84] B. Calmels, S. Canard, M. Girault, H. Sibert, Low-cost cryptography for privacy in RFID systems, in: Proceedings of IFIP CARIDS 2006, Terragona, Spain, April 2006.
[85] L. Cranor, et al., The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, W3C Working Group Note, November 2006.
[86] H. Chan, A. Perrig, Security and privacy in sensor networks, IEEE Computer 36 (10) (2003) 103–105.
[87] J. Wickramasuriya, M. Datt, S. Mehrotra, N. Venkatasubramanian, Privacy protecting data collection in media spaces, in: Proceedings of ACM International Conference on Multimedia 2004, New York, NY, USA, October 2004.
[88] C.M. Medaglia, A. Serbanati, An overview of privacy and security issues in the internet of things, in: Proceedings of TIWDC 2009, Pula, Italy, September 2009.
[89] O. Savry, F. Vacherand, Security and privacy protection of contactless devices, in: Proceedings of TIWDC 2009, Pula, Italy, September 2009.
[90] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, J. Reverdy, RFID noisy reader: how to prevent from eavesdropping on the communication? in: Proceedings of Workshop on Cryptographic Hardware and Embedded Systems 2007, Vienna, Austria, September 2007.
[91] G.V. Lioudakis, E.A. Koutsoloukas, N. Dellas, S. Kapellaki, G.N. Prezerakos, D.I. Kaklamani, I.S. Venieris, A proxy for privacy: the discreet box, in: EUROCON 2007, Warsaw, Poland, September 2007.
[92] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, 2009.
[93] C. Thompson, 25 Ideas for 2010: Digital Forgetting, Wired UK, November 2009.
[94] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K.H. Kim, S. Shenker, I. Stoica, A data-oriented (and beyond) network architecture, in: Proceedings of ACM SIGCOMM'07, Kyoto, Japan, August 2007.
[95] T. O'Reilly, J. Pahlka, The 'Web Squared' Era, Forbes, September 2009.

Luigi Atzori is assistant professor at the University of Cagliari (Italy) since 2000. His main research topics of interest are in multimedia networking: error recovery and concealment, IP Telephony, video streaming, network QoS management. He has published more than 80 journal articles and refereed conference papers. He has been awarded a Fulbright Scholarship (11/2003–05/2004) to work on video at the University of Arizona. He is editor for the ACM/Springer Wireless Networks Journal and is involved in the organization of several International Conferences on Multimedia Networking.

Antonio Iera is a Full Professor of Telecommunications at the University "Mediterranea" of Reggio Calabria, Italy. He graduated in Computer Engineering at the University of Calabria in 1991; then he received a Master Diploma in Information Technology from CEFRIEL/Politecnico di Milano and a Ph.D. degree from the University of Calabria. From 1994 to 1995 he has been with Siemens AG in Munich, Germany to participate to the RACE II ATDMA (Advanced TDMA Mobile Access) project under a CEC Fellowship Contract. Since 1997 he has been with the University Mediterranea, Reggio Calabria, where he currently holds the positions of scientific coordinator of the local Research Units of the National Group of Telecommunications and Information Theory (GTTI) and of the National Inter-University Consortium for Telecommunications (CNIT), Director of the ARTS – Laboratory for Advanced Research into Telecommunication Systems, and Head of the Department DIMET. His research interests include: new generation mobile and wireless systems, broadband satellite systems, Internet of Things. Elevated to the IEEE Senior Member status in 2007.

Giacomo Morabito was born in Messina, Sicily (Italy) on March 16, 1972. He received the laurea degree in Electrical Engineering and the Ph.D. in Electrical, Computer and Telecommunications Engineering from the Istituto di Informatica e Telecomunicazioni, University of Catania, Catania (Italy), in 1996 and 2000, respectively. From November 1999 to April 2001, he was with the Broadband and Wireless Networking Laboratory of the Georgia Institute of Technology as a Research Engineer. Since April 2001 he is with the Dipartimento di Ingegneria Informatica e delleTelecomunicazioni of the University of Catania where he is currently Associate Professor. His research interests focus on analysis and solutions for wireless networks.