Abstract – The Internet of things can be defined as to make the “things” belong to the Internet. However, many wonder if the current Internet can support such a challenge. For this and other reasons, hundreds of worldwide initiatives to redesign the Internet are underway. This article discusses the perspectives, challenges and opportunities behind a future Internet that fully supports the “things”, as well as how the “things” can help in the design of a more synergistic future Internet.

Keywords – Internet of things, smart things, future Internet, software-defined networking, service-centrism, information-centrism, ID/Loc splitting, security, privacy, trust.

I. INTRODUCTION

The Internet of things (IoT) refers to uniquely addressable objects and their virtual representations in an Internet-like structure [18][19][20]. We can say that it is an extension of Internet with uniquely addressable objects becoming a part of existing Internet. The objects forming the IoT will have distinct characteristics about them. They may hold self-identifying information; they may even transmit the processed information or anything that may be considered important with respect to the object with which they are associated.

There is a lot of pervasive presence in the human environment of things or objects, such as radio-frequency identification (RFID) tags, sensors, actuators, mobile phones, smart embedded devices, etc. – which, through unique addressing schemes, are able to effectively communicate and interact with each other and work together to reach a common goal of making the system easier to operate and utilize. The objects that will be connected will be adaptive, intelligent, and responsive.

The IoT will be altogether a new environment in which the current Internet will be smartly supported by all together new range of smart embedded devices. The IoT will be characterized by an environment rich in RFID, ipv6, near field communication (NFC), barcodes, quick response (QR) codes, smartphone apps, GPS, and other smart devices.

The networked objects will sense the environment with help of the sensors and will communicate among themselves directly or with the help of the Internet. The amount of knowledge comprised with redundant information will certainly be analyzed and assessed by the analytic software and intelligent decisions will be the final outcome.

In this scenario, what could be the number of networked objects we could expect on the Internet? Estimatives go from billions to trillions [2][21][22]. These estimates will certainly make you wonder if the current Internet can support such tremendous increase in the number of connected devices and networks. These and other challenges have motivated the networking community to question whether it is time to redesign the Internet considering the current state-of-the-art on information and communication technologies (ICT). Thus, worldwide, hundreds of initiatives are proposing to reengineer the Internet under the banner of the so-called future Internet (FI) research [5][21].

Figure 1: Future Internet: A “smart things” evolutionary perspective.

Considering an evolutionary point of view, the future Internet will comprise of existing Internet and smart embedded objects which will be the basis of the Internet of things. The IoT will be a distinct part of the FI. It will be seamlessly integrated in to the existing Internet infrastructure which will help the service oriented
architecture of the Internet to utilize the services available through the system. However, as computing and communication resources become more and more ubiquitous, the smart things will increasingly become integral part of the FI, augmenting the overlapping area of the IoT and Internet spheres in Figure 1.

In an evolutionary perspective, the FI will face the challenge of the integration of smart embedded devices in to the ever expanding Internet. Protocols using 6lowpan are improving. Since there are bandwidth limitations, the users which are using ipv6 will certainly face connectivity and timing issues. To resolve this more efficient compressing algorithm are being developed to be used in the seamless integration in to the system.

In a revolutionary perspective, most of the challenges are at the design level. IoT and FI relationships need to be clearly determined. More synergistic designs are required to take advantage of efforts, reducing unnecessary overlapping and producing more efficient and flexible architectures. This paper provides a first glance discussion on the relationships between the IoT and FI considering a full convergence point of view.

The remaining of this paper is organized as follows. Section II covers the IoT requirements and perspectives regarding capacity, ubiquity, and scalability issues. Section III focuses on the role of IoT considering a more deep integration between the real and virtual worlds. Section IV concerns on how to expose IoT resources to software and how to orchestrate IoT related services and applications. Section V addresses the relationship between IoT and software-defined networking. Management and human intervention aspects are discussed on section VI. Section VII covers the relationships between IoT and the information-centric paradigm for FI design. Section VIII focuses on naming, identification, mobility, and multihoming support. Section IX concerns to the security, privacy, and trust aspects. Finally, the Section X does some final remarks.

II. CAPACITY, UBIQUITY, AND SCALABILITY

The accelerated evolution of computing and communications capacities [1], i.e. memory, processing, storage, transmission rate, etc., allows the implementation of small devices capable of sensing the real world and transmitting the obtained data to services and applications on the Internet. As the cost of technologies fall, more and more capacity becomes available, making the use of networked sensing and actuating devices more and more viable. One can expect that the number of devices will increase faster and faster in the next decades [2]. As a result, sensing and actuating capabilities can become ubiquitous, allowing unprecedented scenarios of interaction between the real and the virtual worlds [3].

Although it is expected that this scenario will bring huge benefits for our information society, the challenges behind it are equally big [3]. A significant increase in the number of internet-enabled devices (IEDs) can create relevant challenges to the scalability of the current TCP/IP stack [2][3], including the support for naming, addressing, identification, location, mobility, routing, etc. The Internet lacks on the support for unique identification and transparency. IP addresses are used no only to locate devices on the network, but also to identify them [2][4]. Since the devices’ addresses behind a network address translation (NAT) are opaque [5], the IDs are not valid outside an autonomous system. This severely limits the transparency on the network. The scalability of the current domain naming system (DNS) is also affected by a huge increase in the number of device networks. Several other aspects on the current Internet are affected by this evolution scenario [2][3].

New network architectures need to overcome the current Internet limitations by rethinking such limiting aspects. They need to take advantage of the expected ubiquity of computing and communication resources to improve the connectivity and robustness of wireless sensor and actuator networks (WSANs). Devices need to be persistently identified to allow perennial traceability to existent sensing and actuating resources [3]. The challenge is to identify perennially and uniquely the devices that are collecting real world information or actuating over the real world. Also, device locators need to be decoupled from identifiers to allow mobility without loss of identity [4]. This and other proposals to improve IoT scalability will be discussed on the following sections.

III. REAL-VIRTUAL WORLDS INTEGRATION

The perspective behind the IoT is that the real world will be increasingly integrated with the virtual one [3]. Right now, the world is in process of making new smart embedded devices. Embedded devices are still emerging. This will create a flood of real world information, considerably enriching our applications, making them more aware of what happens in the real world, in real time, everywhere. Smart applications are being thought of as the process of making the system more popular as per the system point of views. One can expect the popularization of new applications that take advantage of this situational information, like augment reality, ambient intelligence, social appliances, networked cars, and many others. Also, there are the applications to control or act over the real world. Decisions made on the virtual side can be reflected on the real environment. This will help us to save energy, to better use our environmental resources.

To transform this huge amount of raw data on knowledge is one of the biggest challenges behind the IoT. There is an entire cycle of raw data processing up to the generation of a knowledge database. Possible data processing includes statistics generation, data aggregation, filtering, correlation, contextualization, and exposition. Depending on the service or application, time sensitivity is also an issue.

Generally speaking, the information and knowledge obtained from the sensorial network will be further used to feed other processes, like decision making or actuating. Therefore, complex hierarchical feedback control loops can
be investigated. A contract revocation? These are open problems that need to be investigated.

IV. RESOURCES EXPOSITION AND SERVICE CENTRISM

Not only the collected IoT data need to be exposed to the software environment, but also the existent IoT resources, i.e. sensors, actuators, or even entire networks. In other words, IoT resources need to be exposed to software orchestration frameworks, allowing the dynamic and integrated composition of devices, networks, services, and applications [6]. Entire services’ life-cycles can be orchestrated involving such exposed resources. First, services and applications can search for available IoT devices. Second, dynamic usage contracts can be negotiated and established. The quality of the sensing and actuating functionalities can be monitored and evaluated. Dynamic contracts with sensors and actuators that do not perform as expected can be revoked. Devices can compete each other to provide better services to virtual entities. The reputation of networked objects can be estimated according to previous established contracts.

Nonetheless, IoT capabilities can be seen as a service that is exposed to other software via orchestration frameworks and contracted on demand. This view approximates the IoT to the so-called Internet of services (IoS) [7][8], which is a branch of the FI research. In this context, a first challenge is how to design a service oriented IoT? A second one is how to enable the joint orchestration of non-IoT and IoT substrate resources and services. The convergence, the search for synergies, and the elimination of redundant aspects in these two proposals strengthens both and more efficiently addresses the challenges behind the design of a new Internet.

The IoT resources need to be very precisely exposed. Thus, devices’ descriptors can be elaborated and divuligated to possible partners. The publish/subscribe paradigm fits very well on this task [9]. However, one can not expect that small sensors and actuators are able to neither expose their capabilities, nor establish dynamic contracts. It is well known that energy and other factors limit the IEDs’ functionalities. Therefore, proxies can be used to represent simple networked objects that do not support such functionalities.

Another very important challenge for FI architectures is the consistent management of exposed resources’ life-cycle. In this context, some questions are: How to manage the life-cycle of exposed resources? How to share IoT resources among several orchestration frameworks? How to describe the device capabilities? How to format the contracts? How to provide the adequate search mechanisms? Which circumstances can cause a contract revocation? These are open problems that need to be investigated.

V. SOFTWARE-DEFINED NETWORKING

Software-defined networking (SDN) means to design networks from a software engineering perspective [10]. It means to look for the right abstractions when designing new network architectures. OpenFlow is a first realization of this idea [11]. Network control is performed based on a centralized view of the network. However, it is important to note that the SDN paradigm is more broad than the OpenFlow implementation. The research for the right abstractions for the SDN is still in the beginning.

In this scenario, the convergence between the IoT and the SDN is an emerging research area. A priori, the relationship between the two technologies appear to be bilateral. The SDN paradigm could be applied to the IoT design. This is already happening for wireless networks and WSANs, where OpenFlow is used to program/configure network nodes [23]. Software-defined and software-controlled WSANs were just emerged as a research topic. An interesting issue is how the well-known limitations of WSANs will shape the application of the SDN paradigm on this networks.

In the opposite direction, the IoT can be used to collect real-world information that is relevant for networking control, as well as to reflect software decisions on network hardware. An open subject is how to design networking control and management systems that take advantage of the IoT. An additional challenge is to ensure the correctness and temporal coherence of the controls sent by software to the actuators.

VI. MANAGEMENT AND AUTONOMICITY

The expectation behind the IoT is that it will manage itself or at least reduce considerably the degree of the human intervention required [3]. We can not expect that the IoT will be managed in the same way as the telecom operator’s networks today. First, because the quantity of networked devices will be orders of magnitude greater. The traditional management model would have a very high cost if applied for the IoT scenario. Second, hundreds or even thousands of devices will be under the ownership of non-technical people, in their houses, cars, clothes, etc. Third, IoT management requirements have several important differences when compared to traditional networks [12]. Therefore, to manage such devices is a different problem when compared with traditional Internet or telephony management. Fortunately, the restrictions imposed on the IoT devices (e.g. energy, computing power, faults, limited reach, etc.) are well understood right now and have influenced the creation of evolving management approaches less dependent on human interference [14].

The IoT viability depends on the scalability, generality, autonomicity, and comprehensiveness of its management. Moreover, when we look for more deep synergies, the FI management may itself depend on the IoT, since sensing and actuating are desirable functionalities for any ICT.
equipment management. Thus, while the IoT works like a sensorial nervous system for the FI, providing the required data to establish adequate real-world awareness, it also demands the management of its “army” of devices. Therefore, there is a two-way relationship between the substrate resources management and the sensing and actuating capabilities of the IoT. An open challenge is how to combine both requirements in an elegant design, without unnecessary overlappings.

Among the proposals to reduce human interference on ICT, there is the so-called autonomic technology, or self-* [13]. The asterisk is the name of the function that is performed autonomically, e.g. self-organization, self-configuration, self-optimizing, self-healing, etc. The goal would be to create a self-management solution or an autonomic “pilot” for the IoT.

The implementation of the self-* properties is typically based on an autonomic element that performs an autonomic cycle. According to Kephart and Chess [13], this cycle consists on the following phases: monitoring, analyzing, planning, execution, and knowledge. The monitoring phase relies on sensors that collect the relevant data at a managed entity, while the execution phase depends on effectors that execute the planned actions. The analyzing phase aims at contextualizing the monitored data to create the required awareness regarding the managed entity. At the planning phase, actuating plans are generated and evaluated based on the analyzed data and other inputs, like politics, rules, goals, etc. The execution phase aims at executing the elaborated plans. And, in a knowledge phase, fitness and learning takes place based on the history of the actions done. In this context, the IoT role on future networks:

- Merges with the necessary functionalities to implement a self-management approach. Observe that many of the IoT roles overlap with the functionalities advocated by the autonomic cycle. Thus, the autonomic technology appears to be a natural candidate for the IoT management [14].

- Provides the contextualized real-world information necessary to feed the autonomic cycle of other FI architectural components. For example, assume a virtual network admission control service that decides whether a new virtual network can be established or not over some real-world substrate. The autonomic cycle of this service could rely in a set of contracted sensors that measure the available capacity on the physical infrastructure. If a new virtual network is accepted, the admission installation can be done by effectors at the real-world equipment, e.g. optical switch control or electromechanical antenna positioning. Thus, the IoT appears to be a natural candidate to implement some of the phases of the autonomic cycle for FI components.

VII. INFORMATION-CENTRISM

The IoS approach considers that behind a certain level of abstraction, everything in a new Internet can be considered a service, e.g. infrastructure, frameworks, operating systems, databases, etc. On the contrary, the information-centric design considers the information as the main ingredient of the FI [15]. The argument is the same, i.e. everything can be considered as information over a certain level of abstraction. This approach is also know as information centric networking (ICN). Let’s call this branch of the FI design as Internet of information (IoI). As previously discussed, the IoT and IoS also present a two-way relationship, where the IoT can be seen as a service on the IoS approach and the IoS depends on the contextualized information provided by the IoT, as well as on its actuating capability. Thus, what is the relationship between the IoT and the IoI?

Node-centrism is perhaps the most common approach for designing WSANs. A possible explanation is that for many years the main design challenges were related to the energy and other environmental pre-requirements. The idea of putting sensing and actuating nodes on the Internet made other design aspects emerge, such as the ones addressed on this paper. Additionally, there are the information-centric aspects, e.g. information representation, naming, identification, addressing, search, locating, traceability, distribution, privacy, security, integrity, and management. Thus this paper defends that the IoT can take great advantage of the precepts behind the IoI. Self-certifying names (SCNs) can be used to name data and/or information in a persistent and verifiable way¹. The integrity of sensing and actuating data can be checked based on such names. Also, IoT information can be described and represented by information objects, which contain digital signatures, checksums, metadata, access rights, formats, ontology, etc. The persistent identification of data chunks or coded information is another requirement advocated by the IoI. Information identifiers need to be decoupled from addresses and locators. Therefore, IoT information could be moved or copied without loosing its identity. Search and discovery of IoT information can be performed based on persistent names and/or identifiers. Also, information coherence, provenance, and traceability become persistent. Finally, data and information are secured per se [16] – they do not depend anymore only on secured connections.

In the opposite direction, the IoT can enrich the IoI with the information measured in the real world, as well as allow actuating over it. The benefits for the IoI are similar to those resulting from the convergence of the IoS and the IoT. Thus, the application of the information-centric paradigm on the context of the IoT is an unexplored research area. Some open challenges are: How to name data chunks and information sensed on the IoT? How to create identifier for them? How to resolve identifiers to locators? How to create the metadata for the measured data? How to distribute the data to one or more interested destinations? How to support ID-based mobility? How to enable search and discovery of

¹ SCNs contain the result of a cryptographic hash function over the binary pattern of the data.
sensorial information? How to deal with the privacy of the IoT information? Or more generally speaking, how to apply the state-of-the-art on information-centric design to the IoT scope?

VIII. NAMING, IDENTIFICATION, MOBILITY, AND MULTIHOMING

People like to assign legible names to devices, networks, services, and even for information. In addition to the legible names, SCNs can be calculated based on the binary patterns of digital entities and information. On the other hand, identifiers are symbols that uniquely identify an entity or a content in a certain scope. SCNs can be identifiers if they are unique in some scope. The dynamic resolution of an identifier in other identifiers allows the architecture to model the relationships among devices and their sensorial data. As a data moves it changes its address and location, but its identifier remains the same within the same scope. The same occurs to a node that moves in some network. Therefore, the separation of identifiers and locators in the IoT is very desirable. More research needs to be done on the dynamic resolution problem.

Also, standardization bodies need to verify the suitability of the contemporary approaches for device identification on the FI. The research on mechanisms to generate persistent and unique identifiers to other entities in the IoT is also an issue, including networks, services, virtual entities, etc. Other challenges are: How to ensure that there is no collision? Or at least, how to minimize collisions probability? How to check the veracity and uniqueness of a given identifier? How to map an identifier to a locator in a large population of IoT devices? Is it possible to use the IDs as addresses to forward or route information? Or more generally, how to design an ID-based IoT?

Finally, there is the multihoming support for IoT resources. The current Internet provides a limited support for multihoming. New architectures need to support simultaneous connectivity and multipath routing. The ubiquitous connectivity needs to be explored in design, as well as new routing approaches. Service redundancy is also a prerequisite.

IX. SECURITY, PRIVACY, AND TRUST

The data gathered from IoT sensors or tags can carry sensible information for client’s privacy. For example, consider a personal area health monitoring system that periodically transfers to a hospital the state of a certain patient. The data collected by this system are property of the patient being monitored, which authorizes the hospital and its medical staff to access and analyze it. An unauthorized access to this data consists of a breaking on the security and privacy of this patient. However, consider that the communication to the authorized hospital is lost and another medical staff needs to access the data due to a supposed emergency. This situation can become much worse if the patient is unconscious and can not authorize the new medical team. This scenario illustrates how complex can be the security and privacy problem in the IoT. An approach to deal with this situation (and many others on the FI) could be the establishment of a trust network of hospitals. Instead of individually authorizing every possible hospital in a country, the patient authorizes the trust network. Thus, in case of emergency access can be granted to other hospital in the trust network.

Trust networks are in essence a collaboration contract between trustable peers. They can be established among nodes in a WSAN in order to authenticate forwarding, routing, or even aggregation of data [17]. They can also help on the selection of a node cluster’s leader. Observe how close this idea is to the dynamic contract establishment idea on the IoT. Therefore, the management of trust networks requires a complex contract life-cycle management. Also, entities reputation need to be estimated in order to decline or not their participation in some network. Moreover, the establishment of comprehensive trust networks that spread over the IoT and other FI components is a new research frontier.

X. FINAL REMARKS

The Internet of things is a fundamental ingredient of the future Internet, since it provides the sensorial and actuating capabilities required to greatly enhance the interaction between the real and virtual worlds. Not only it collects the real world data that feeds the entire FI, but also it offers the actuating devices that can make virtual world decisions real. The continued reduction in the cost of computing and communication capabilities indicates that the IoT will become ubiquitous, allowing the FI to achieve increasing levels of environmental awareness, as well as making our environment more intelligent and sustainable. Such capabilities feed significant bilateral relationships with other FI ingredients, such as: information- and service-centric approaches, software-defined networking, self-management, naming, identification, mobility, multihoming, security, privacy, and trust. Therefore, this paper argues that the FI research should better exploit the synergies between these proposals and the IoT, eliminating unnecessary overlappings and cohesively integrating them towards the design of a cohesive new Internet.

REFERENCES

[6] M. Presser, P. Barnaghi, M. Euirch, C. Villalonga, The sensei project: integrating the physical world with the digital world of the


