Ad Hoc Networks 10 (2012) 1497–1516

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

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

Survey Paper

Internet of things: Vision, applications and research challenges

Daniele Miorandi [a,*], Sabrina Sicari [b], Francesco De Pellegrini [a], Imrich Chlamtac [a]

[a] CREATE-NET, via Alla Cascata 56/D, IT-38123 Povo, Trento, Italy
[b] Dipartimento di Informatica e Comunicazione, Università degli Studi dell' Insubria, via Mazzini, 5, IT-21100 Varese, Italy

ARTICLE INFO

Article history:
Received 17 February 2012
Accepted 25 February 2012
Available online 21 April 2012

Keywords:
Internet-of-Things
Web
Smart objects
RFID
Sensors
Actuators
Interoperability
Security

ABSTRACT

The term "Internet-of-Things" is used as an umbrella keyword for covering various aspects related to the extension of the Internet and the Web into the physical realm, by means of the widespread deployment of spatially distributed devices with embedded identification, sensing and/or actuation capabilities. Internet-of-Things envisions a future in which digital and physical entities can be linked, by means of appropriate information and communication technologies, to enable a whole new class of applications and services. In this article, we present a survey of technologies, applications and research challenges for Internet-of-Things.

1. Introduction

Nowadays, around two billions people around the world use the Internet for browsing the Web, sending and receiving emails, accessing multimedia content and services, playing games, using social networking applications and many other tasks. While more and more people will gain access to such a global information and communication infrastructure, another big leap forward is coming, related to the use of the Internet as a global platform for letting machines and smart objects communicate, dialogue, compute and coordinate.

It is predictable that, within the next decade, the Internet will exist as a seamless fabric of classic networks and networked objects. Content and services will be all around us, always available, paving the way to new applications, enabling new ways of working; new ways of interacting; new ways of entertainment; new ways of living.

In such a perspective, the conventional concept of the Internet as an infrastructure network reaching out to end-users' terminals will fade, leaving space to a notion of interconnected "smart" objects forming pervasive computing environments [1]. The Internet infrastructure will not disappear. On the contrary, it will retain its vital role as global backbone for worldwide information sharing and diffusion, interconnecting physical objects with computing/communication capabilities across a wide range of services and technologies.

This innovation will be enabled by the embedding of electronics into everyday physical objects, making them "smart" and letting them seamlessly integrate within the global resulting cyberphysical infrastructure. This will give rise to new opportunities for the Information and Communication Technologies (ICT) sector, paving the way to new services and applications able to leverage the interconnection of physical and virtual realms.

Within such perspective, the term "Internet-of-Things" (IoT) is broadly used to refer to both: (i) the resulting global network interconnecting smart objects by means of extended Internet technologies, (ii) the set of supporting technologies necessary to realize such a vision (including,

* Corresponding author. Tel.: +39 0461 40 84 00; fax: +39 0461 42 11 57.
E-mail addresses: daniele.miorandi@create-net.org (D. Miorandi), sabrina.sicari@uninsubria.it (S. Sicari), francesco.depellegrini@create-net.org (F. De Pellegrini), imrich.chlamtac@create-net.org (I. Chlamtac).

1570-8705/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2012.02.016

e.g., RFIDs, sensor/actuators, machine-to-machine communication devices, etc.) and (iii) the ensemble of applications and services leveraging such technologies to open new business and market opportunities [2,3].

In this survey article, we aim at providing a holistic perspective on the Internet-of-Things concept and development, including a critical revision of application fields, enabling technologies and research challenges. As a matter of fact, the research community active on IoT-related themes is still highly fragmented, and, to a large extent, focused around single application domains or single technologies. Further, the involvement of the networking and communications scientific communities is still limited, despite the high potential impact of their contributions on the development of the field [2,4]. We do believe that this fragmentation is potentially harmful for the development and successful adoption of IoT technologies. We therefore hope this survey can help in bridging existing communities, fostering cross-collaborations and ensuring that IoT-related challenges are tackled within a system-level perspective, ensuring that the research activities can then be turned into successful innovation and industry exploitation.

The remainder of this article is organized as follows. In Section 2 we introduce the IoT vision and define the main related concepts. In Section 3 we analyze the relevant research and technology contexts, including related fields and their potential contribution towards the realization of the IoT vision. In Section 4 we present the main research challenges ahead of us in the IoT landscape. In Section 5 we discuss the security challenges introduced by IoT technologies and applications. An analysis of the potential application fields and impact areas is reported in Section 6. A survey of IoT related-on-going initiatives is presented in Section 7. Section 8 concludes the survey with a number of remarks on potential approaches to tackle the challenges identified.

2. Vision and concept

The Internet-of-Things is emerging as one of the major trends shaping the development of technologies in the ICT sector at large [3,5,6,2]. The shift from an Internet used for interconnecting end-user devices to an Internet used for interconnecting physical objects that communicate with each other and/or with humans in order to offer a given service encompasses the need to rethink anew some of the conventional approaches customarily used in networking, computing and service provisioning/management.

From a conceptual standpoint, the IoT builds on three pillars, related to the ability of smart objects to: (i) be identifiable (*anything identifies itself*), (ii) to communicate (*anything communicates*) and (iii) to interact (*anything interacts*) – either among themselves, building networks of interconnected objects, or with end-users or other entities in the network. Developing technologies and solutions for enabling such a vision is the main challenge ahead of us.

At the single component level, the IoT will be based on the notion of "smart objects", or, simply, "things", which will complement the existing entities in the Internet domain (hosts, terminals, routers, etc.) [7]. We define smart objects (or things) as entities that:

- Have a physical embodiment and a set of associated physical features (e.g., size, shape, etc.).
- Have a minimal set of communication functionalities, such as the ability to be discovered and to accept incoming messages and reply to them.
- Possess a unique identifier.
- Are associated to at least one name and one address. The name is a human-readable description of the object and can be used for reasoning purposes. The address is a machine-readable string that can be used to communicate to the object.[1]
- Possess some basic computing capabilities. This can range from the ability to match an incoming message to a given footprint (as in passive RFIDs) to the ability of performing rather complex computations, including service discovery and network management tasks.
- May possess means to sense physical phenomena (e.g., temperature, light, electromagnetic radiation level) or to trigger actions having an effect on the physical reality (actuators).

The last point in the definition above is the key one, and differentiates smart objects from entities traditionally considered in networked systems. In particular, the proposed classification includes devices considered in RFID research [8] as well as those considered in wireless sensor networks (WSNs) and sensor/actor networks (SANETs) [9,10].

The inclusion of such entities into a global networked system questions the architectural and algorithmic principles at the basis of the design of the Internet as we know it. In particular, the increased level of heterogeneity, due to the inclusion of devices with only very basic communication and computing capabilities, challenges the assumption that any device presents a full protocol stack, as well as the application of the end-to-end principle in network operations [11]. From the conceptual standpoint, indeed, IoT is about entities acting as providers and/or consumers of data related to the physical world. The focus is on data and information rather than on point-to-point communications. This fact could push towards the adoption of recently proposed content-centric network architectures and principles [12], as will be discussed in the following sections.

From a system-level perspective, the Internet-of-Things can be looked at as a highly dynamic and radically distributed networked system, composed of a very large number of smart objects producing and consuming information. The ability to interface with the physical realm is achieved through the presence of devices able to sense physical phenomena and translate them into a stream of information data (thereby providing information on the current context and/or environment), as well as through the presence of devices able to trigger actions having an impact on the physical realm (through suitable actuators). As scalability is expected to become a major issue due to the extremely

[1] Their association and relation to the identifier will be discussed further later on in this article.

large scale of the resulting system, and considering also the high level of dynamism in the network (as smart objects can move and create ad hoc connections with nearby ones following unpredictable patterns), the quest for inclusion of self-management and autonomic capabilities is expected to become a major driver in the development of a set of enabling solutions [13,14].

From a service-level perspective, the main issue relate to how to integrate (or: compose) the functionalities and/or resources provided by smart objects (in many cases in forms of data streams generated) into services [15–17]. This requires the definition of: (i) architectures and methods for "virtualizing" objects by creating a standardized representation of smart objects in the digital domain, able to hinder the heterogeneity of devices/resources and (ii) methods for seamlessly integrating and composing the resources/services of smart objects into value-added services for end users.

The Internet-of-Things vision provides a large set of opportunities to users, manufacturers and companies. In fact, IoT technologies will find wide applicability in many productive sectors including, e.g., environmental monitoring, health-care, inventory and product management, workplace and home support, security and surveillance (see Section 6 for a more in-depth discussion of relevant application domains).

From a user point of view, the IoT will enable a large amount of new *always responsive services*, which shall answer to users' needs and support them in everyday activities. The arising of IoT will provide a shift in service provisioning, moving from the current vision of *always-on services*, typical of the Web era, to *always-responsive situated services*, built and composed at run-time to respond to a specific need and able to account for the user's context. When a user has specific needs, she will make a request and an ad hoc application, automatically composed and deployed at run-time and tailored to the specific context the user is in, will satisfy them.

While the IoT vision will require substantial advances in a number of ICT fields (see Section 4), its realization is likely going to follow an incremental process, starting from existing technologies and applications. In particular, IoT will likely expand starting from identification technologies such as RFID (Radio Frequency Identification) [8,18], which are already widely used in a number of applications. At the same time, in its development path, IoT will likely build on approaches introduced in a variety of relevant field, such as wireless sensor networks (as a means to collect contextual data [9]) and service-oriented architectures (SoA) as the software architectural approach for expanding Web-based services through IoT capabilities [19].

Summarizing, we can preliminarily identify the following key system-level features that Internet-of-Things needs to support:

- *Devices heterogeneity.* IoT will be characterized by a large heterogeneity in terms of devices taking part in the system, which are expected to present very different capabilities from the computational and communication standpoints. The management of such a high level of heterogeneity shall be supported at both architectural and protocol levels. In particular, this may question the "thin waist" approach at the basis of IP networking.
- *Scalability.* As everyday objects get connected to a global information infrastructure, scalability issues arise at different levels, including: (i) naming and addressing – due to the sheer size of the resulting system, (ii) data communication and networking – due to the high level of interconnection among a large number of entities, (iii) information and knowledge management – due to the possibility of building a digital counterpart to any entity and/or phenomena in the physical realm and (iv) service provisioning and management – due to the massive number of services/service execution options that could be available and the need to handle heterogeneous resources.
- *Ubiquitous data exchange through proximity wireless technologies.* In IoT, a prominent role will be played by wireless communications technologies, which will enable smart objects to become networked. The ubiquitous adoption of the wireless medium for exchanging data may pose issues in terms of spectrum availability, pushing towards the adoption of cognitive/dynamic radio systems [20].
- *Energy-optimized solutions.* For a variety of IoT entities, minimizing the energy to be spent for communication/computing purposes will be a primary constraint. While techniques related to energy harvesting (by means, e.g., of piezolectric materials or micro solar panels) will relieve devices from the constraints imposed by battery operations, energy will always be a scarce resource to be handled with care. Thereby the need to devise solutions that tend to optimize energy usage (even at the expenses of performance) will become more and more attractive.
- *Localization and tracking capabilities.* As entities in IoT can be identified and are provided with short-range wireless communications capabilities, it becomes possible to track the location (and the movement) of smart objects in the physical realm. This is particularly important for application in logistics and product life-cycle management, which are already extensively adopting RFID technologies.
- *Self-organization capabilities.* The complexity and dynamics that many IoT scenarios will likely present calls for distributing intelligence in the system, making smart objects (or a subset thereof) able to autonomously react to a wide range of different situations, in order to minimize human intervention. Following users' requests, nodes in IoT will organize themselves autonomously into transient ad hoc networks, providing the basic means for sharing data and for performing coordinated tasks [21]. This includes ability to perform device and service discovery without requiring an external trigger, to build overlays and to adaptively tune protocols' behavior to adapt to the current context [13].
- *Semantic interoperability and data management.* IoT will be much about exchanging and analyzing massive amounts of data. In order to turn them into useful information and to ensure interoperability among different applications, it is necessary to provide data with

adequate and standardized formats, models and semantic description of their content (meta-data), using well-defined languages and formats. This will enable IoT applications to support automated reasoning, a key feature for enabling the successful adoption of such a technology on a wide scale.

- *Embedded security and privacy-preserving mechanisms.* Due to the tight entanglement with the physical realm, IoT technology should be secure and privacy-preserving by design. This means that security should be considered a key system-level property, and be taken into account in the design of architectures and methods for IoT solutions. This is expected to represent a key requirements for ensuring acceptance by users and the wide adoption of the technology.

3. Research context

As technology progresses, more and more processing power, storage and battery capacity become available at relatively low cost and with limited space requirements. This trend is enabling the development of extremely small-scale electronic devices with identification/communication/computing capabilities, which could be embedded in the environment or in common objects. Such a class of devices could be used, as described in the previous Section, to enable a set of novel applications and services, leveraging direct interactions with the physical realm. The development of such a new class of services will, in turn, require the introduction of novel paradigms and solutions for communications, networking, computing and software engineering. The IoT umbrella concept comprises all these aspects, based on the paradigm of computing and communications anywhere, anytime and by anything.

In this section, we briefly discuss the relevance and potential impact of existing research areas on the development of IoT technologies and applications.

The Internet-of-Things is unlikely to arise as a brand new class of systems. We envision an incremental development path, along which IoT technologies will be progressively employed to extend existing ICT systems/applications, providing additional functionalities related to the ability of interacting with the physical realm. In this sense, we do believe it is worth analyzing which research fields, among the ones subject of investigation in the last years, can be more relevant (in terms of techniques/solutions introduced or lessons learned) in the IoT scenario.

In terms of enabling technologies, a key issue for IoT is the development of appropriate means for identifying smart objects and enabling interactions with the environment. In this sense, key building blocks are expected to be represented by wireless sensor networking technologies [9] and RFID [8,18,22].

As far as wireless sensor nodes and networks are concerned, the ability of sensing the environment and to self-organize into ad hoc networks represent important features from an IoT perspective. At the same time, three main limiting factors need to be overcome in order to foster their widespread adoption. The first one relates to the support of heterogeneous devices. Nodes in a wireless sensor network are customarily expected to possess a set of common characteristics, and to share a number of common features including a full protocol stack. While advances in embedded electronics and software are making such a requirement less and less stringent [23], it still appears to put unnecessary burden on the devices. Solutions able to accommodate heterogeneity in terms of supported features should be introduced to ease incremental deployment. The second factor relates to the need of equipping sensor nodes with a battery. While a number of solutions for increasing energy efficiency – at various layers of the OSI model – has been devised, the need to replace batteries from time to time represents a huge barrier to the widespread development of such technology. A number of promising research lines, related to energy harvesting [24] and passive wireless sensor networks [25] are currently under development. The third issue relates to the dimension of the electronics needed to be embedded in objects to make them part of the IoT world. While recent advances in microelectronics have led to considerable reduction in size, the current state-of-the-art is unlikely to be sufficient to enable the realization of the full IoT vision. In this respect, applications of nanotechnologies, while still in their infancy [26], may represent a promising research direction for extending the scope and applicability of IoT solutions.

Radio frequency identification devices and solutions can nowadays be considered a mainstream communication technology, with a number of massive deployments, in particular in the goods management and logistics sectors. RFID is expected to play a key role as enabling identification technology in IoT. At the same time, its integration with sensing technologies brings alongside a number of challenges and issues [27,28]. RFID applications have been so far mainly thought for use within isolated, vertically integrated, systems, used only for identification and/or tracking of objects embedded with an RFID tag. Their use as part of a larger system, where identification of an object is only a step of the work-flow to be executed to provide a final service, has not been fully explored yet.

IoT shares a number of characteristics with ambient intelligence [29]. In Ambient Intelligence (AmI), environments rich in sensing/computing/actuation capabilities are designed so to respond in an intelligent way to the presence of users, thereby supporting them in carrying out specific tasks. Ambient intelligence builds upon the ubiquitous computing concept, loosely defined as the embedding of computational devices into the environment. Ubiquitous computing provides therefore the distributed infrastructure necessary to enable the development of AmI applications.

AmI shares with IoT a number of aspects. This comprises the inclusion in the system of sensing/computing capabilities embedded in the environment. At the same time, AmI applications have been mainly developed for "closed" environments (e.g., a room, a building), whereby a number of specific functions (known at design time) can be accommodated and supported. Accordingly, one of the main focus of research in AmI has been the development of reasoning techniques for inferring activities of users and devising appropriate response strategies from the embedded devices. IoT expands the AmI concepts to

integrate "open" scenarios, whereby new functions/capabilities/services need to be accommodated at run-time without them having been necessarily considered at design time. This requires IoT solutions to be inherently autonomic, i.e., presenting the self-configuration and self-organization, possibly cognitive, capabilities needed to provide this additional degree of flexibility.

IoT application scenarios require applications to prove adaptable to highly diverse contexts, with different resources available and possibly deployment environments changing over time. A number of approaches have been proposed to overcome devices heterogeneity in related scenarios. In particular, the use of a standard virtual platform in all network devices has been proposed [30,31]. While this approach has the potential to ease the development of software and services for IoT by providing a standard set of supported primitives, at the same time it poses some rather stringent requirements on the hardware capabilities of the devices themselves. Frameworks based on mobile agents have also been proposed, e.g. [32]. Their applicability to IoT environments may however prove difficult due, again, to the expected high level of heterogeneity in the resources available on devices.

All the efforts required in terms of development of IoT architectures, methods for management of resources, distributed communication and computation, represent the baseline for the introduction of innovative services that will improve users' experience and quality of life. As described in the previous section, IoT services will be responsive in nature, being able to anticipate user needs, according to the situation they are in, by means of dynamic resource management schemes and on-the-fly composition of different service components.

This requires applications to be able to understand the context and situation the user is in. Such a theme has been addressed within the ambient intelligence, ambient assisted living and pervasive computing fields, leading to a number of solutions able to leverage contextual information coming from a number of sources. In [33] a contextual information service is introduced, which provides applications with contextual information via a virtual database in an efficient and scalable way. In this direction other solutions have been proposed for providing applications with contextual information in a distributed setting [34–36]. Schilit's active map system [34,35] represents a location-based publish-subscribe system for contextual information dissemination. In such a system, location-tagged contextual information is published to an active map server, which disseminates the information to subscribed applications. Another approach is Easyliving [36], which stores contextual information in a single database, allowing applications to query it in order to retrieve data.

Services in IoT are expected to be able to seamlessly adapt to different situations and contexts. A number of research efforts for building self-adaptive situated services have been undertaken in the last few years [37–42]. However, we are still far from reaching a global understanding of how to develop self-adaptive services presenting the flexibility level required by IoT scenarios. Further, most of the approaches proposed have been conceived to be applied to a single, well-defined specific application field. What is needed to foster the deployment of IoT applications is instead a set of design patterns that can be used to augment end-user applications with self-adaptive properties. This requires methods for discovering, deploying and composing services at run-time in a distributed fashion, supporting autonomicity within all phases of the service life-cycle. While smart objects may be able to run some limited and lightweight services, one key aspect of IoT is the integration with the Internet infrastructure, i.e., the "cloud". This may take the form of appropriate Web-based services and applications, able to leverage data and/or atomic services made available by smart things to provide value-added services to the end user.

As far as frameworks for developing IoT applications are concerned, a major role is expected to be played by approaches based on so-called service-oriented computing (SOC) [43–45]. SOC envisages a possibly distributed architecture, whereby entities are treated in a uniform way and accessed via standard interfaces. A service-oriented architecture (SOA) is essentially a collection of services, which communicate with each other via a set of standardized interaction patterns. The communication can involve either simple message passing or it could involve two or more services coordinating some activity via appropriate protocols. Currently, many SOC deployments make use of Web-based protocols (e.g., `http`) for supporting interoperability across administrative domains and enabling technologies. SOC can be used to manage web services and make them act like a virtual network, adapting applications to the specific users needs. Service-oriented architectures support a given level of heterogeneity and flexibility in the software modules to be deployed and executed [44,43,46]. SOC/SOA in general and Web services in particular cannot be straightforwardly applied to the construction of IoT applications. In particular, such approaches – at least in their current form – may prove too heavyweight for being deployed on resources-constrained devices. Nonetheless, they represent a very powerful approach in terms of abstracting functionality from the specific software implementation as well as for ensuring integration and compatibility of IoT technologies into the bigger Future Internet-Future Web perspective, a key success factor for enabling the IoT vision. In particular, exploiting the potential of solutions based on Web service technology may ease the development of a new flexible, dynamic and open platform of services for Internet-of-Things with a set of self-$*$ methods for the distributed and autonomic management and run-time optimization of the platform itself. Key concept from SOA/SOC, such as late binding and dynamic service composition/orchestration, are expected to be inherited in IoT. At the same time, new methods are necessary to adapt them to the IoT peculiarities, including the definition of specific data models and representation, architectures and methods for virtualizing smart objects and their services/resources, together with the development of new methods for the dynamic and flexible composition of smart objects into the Internet of Services [47,16,17].

4. Research challenges

The key idea behind the Internet-of-Things concept, as outlined in Section 2, resides in the huge potential of embedding computing and communication capabilities into objects of common use. Two additional features should also be properly accounted for:

- *Identification.* Each object should be identifiable. Depending on the specific scenarios, objects may require to be uniquely identified, or to be identified as belonging to a given class (e.g., this object is a pen, regardless of which pen it is). This could be done basically in two ways. The first one is to physically tag one object by means of RFIDs, QR code or similar. In such a way an object can be "read" by means of an appropriate device, returning an identifier that can be looked up in a database for retrieving the set of features (description) associated to it. The second possibility is to provide one object with its own description: if equipped with wireless communication means, it could communicate directly its own identity and relevant features. These two approaches are not mutually exclusive, and can complement each other. RFID-based identification is indeed cheaper in terms of requirements on the electronics to be embedded in objects, but requires the possibility for the "reader" to access a database where information about such an object is stored. The self-description-based approach, on the contrary, relaxes the requirements to access to a global database, but still requires to embed more electronics into everyday objects.
- *Sensing/Actuation.* Objects can interface with the physical environment either passively, i.e., performing sensing operations, or actively, i.e., performing actions. These two dimensions span the two fundamental operations that represent the interface and the coupling between the digital and the physical realms. Sensor/actor networks (SANETs) [10] have represented an active research field over the last decade. However, they have been mostly intended as ad hoc systems, with limited physical extension and designed to carry out typically a single task. On the other hand, the IoT vision requires to extend such a perspective considerably beyond current state-of-art technology. The main difference is that objects themselves could embed means for sensing the local environments and acting on it, without being a priori bound to a single task/application.

We can briefly resume the three main system-level characteristics of the Internet-of-Things as follows:

1. *Anything communicates:* smart things have the ability to wirelessly communicate among themselves, and form ad hoc networks of interconnected objects.
2. *Anything is identified:* smart things are identified with a digital name: relationships among things can be specified in the digital domain whenever physical interconnection cannot be established.
3. *Anything interacts:* smart things can interact with the local environment through sensing and actuation capabilities whenever present.

Based on the aforementioned considerations, in the following we make an attempt to classify the research challenges that need to be addressed in order to turn the Internet-of-Things from a concept into a well engineered, commercially viable technological paradigm.

4.1. Computing, communication and identification technologies

The scenarios envisioned for IoT require the development of advanced techniques able to embed computing, communication and identification capabilities into everyday objects. In the last years, several aspects have been investigated in related fields. The span is wide, ranging from the research on low-cost low-power consumption micro/nano-electronics (for both computing as well as communication purposes), to advancement in near-field communications (RFID-like) for identification purposes.

Low-power communications is a well-established research field within the sensor networking community, as proved by the active research performed in the last decade on power consumption aware medium access protocols [48–52]. The typical approach pursued in such works relates to the match of the RF front-end activation patterns (i.e., sleep periods) to the traffic pattern. The use of such protocols, however, at present does not provide a final answer to the optimization of energy consumption versus scalability issues. These are of paramount importance for IoT scenarios, as battery replacement is a costly process to be avoided as much as possible, especially for large-scale deployments. Furthermore, the basic idea of such protocols is to perform active/sleep duty cycles in order to save the power dispersed in idle listening. The increase in message latency [48] in turn needs to be traded off in order to balance between network lifetime and communication performance.

More recently, advances in the field of nano-scale accumulators as well as energy harvesting techniques appear of prominent interest to limit the need for battery replacements. In particular, it has been showed that it is possible to integrate several sources of energy harvesting into sensors, including piezoelectric, thermoelectric and radio waves recharging devices [53]. A comprehensive take at the technological problem of energy harvesting in real devices is described in [54]. There, techniques for power management with the adaptation of sensor duty cycles are proposed.

The effort to reduce the speed of discarding of IoT devices has another dimension of particular relevance, which relates to the reciprocal interaction between computation and communication. The notion of distributing computation in order to reduce the communication overhead, which is generally termed in-network processing or in-network computing [55], is typically applied to wireless sensor networks that perform local measurements, as it would be the case of field measurements in IoT scenarios.

There, the natural requirement (and also the concern) is to scale to a large number of sensor nodes. In order to increase scalability, following the seminal work of Gupta and Kumar on the scaling of capacity in wireless networks [56], several schemes for distributed estimation based on local communications have been proposed. For example, authors of [57] proved that the best linear unbiased estimation of a deterministic parameter can be computed at every sensor with a distributed algorithm. Similarly, the scheme from [58] produces an estimate of the average value of a random field at each sensor. Average field measurement is performed by the distributed self-clocking scheme described in [59]. Other approaches combine packet forwarding and computation as in [60], which uses a combination of a binary split-tree algorithm coupled to a binary hypothesis testing procedure. A joint MAC/PHY design is proposed in [61], proving an asymptotically optimal MAC for type-based estimation. In literature, the seminal paper exploring the issue is the Gallagher's scheme [62], where, under the assumption of perfectly scheduled communication, the proposed solution would permit the parity check on the binary status of a set of nodes with required communication complexity $O(\log\log n)$. The later work in [63] proved that, in the case of type-threshold functions, such as `AND`, `OR` and `MAJORITY`, computing requires $O(n)$ broadcasts. Recently, the problem has been addressed by the works in [55,64], proving fundamental scaling laws in the case of co-located and multi-hop packet networks. The works [55,64] prove that there exist a strong dependence on the scaling law of the number of messages exchanged and the computed function.

Clearly, scaling issues arise when the need is either to cover large areas with a grid of small-size devices for sensing purposes, or to deploy a very dense one for localized measurements. *Both cases apply indeed to IoT scenarios: how to reconcile scaling laws derived in the context of in-network computing and ad hoc communications with a practically viable IoT architecture represents a major research challenge.*

At present the issues of density of deployed IoT devices are probably less critical, though. This relates to miniaturization of sensing and transmitting devices, a celebrated dimension of the research in sensing technologies which is not meeting the expectations set. Indeed, current technologies are far from the level of integration foreseen in the SmartDust vision [65]. The dimensions of commercial devices such as WASPMote[2] or equivalent ones are typically of the order of 3–5 cm, dictated by the packaging dimension, mostly due to the RF interface dimensions and the volume of batteries. Nevertheless, notable advances have been made with respect to the variety and the integration of sensing devices that are hosted on modern sensing boards: photocells for light measurements, thermistores for temperature probes, microphones, accelerometers and magnetometers represent standard equipment for modern sensor boards.

Localization systems represent a rather old research line, dating back to early 90s, see for example Active Badge of Olivetti Research Ltd. [66] and Georgia Institute of Technology CyberGuide [67]. Along some twenty years of activities, research on localization systems has tackled a number of issues that are certainly relevant in IoT research. One topic addressed involves the surveillance of moving objects within a sensorized area [68], or the robustness of location detection schemes [69] as needed in the case of emergency networks [70]. Also, the recent advancement of ultra-wideband radio frequency technologies stimulated research for very fine-grained location estimation and ranging [71].

Identification and proximity detection schemes that make use of inexpensive RFIDs became recently a promising choice for commercial deployments in the logistics field [72]. The most popular type of RFIDs are passive tags, which do not contain an on-board power source: energy for operation is supplied by the RFID interrogation signal itself. Conversely, active tags have an on-board power source that feeds the on-board receiver and transmitter, allowing for an increased radio range. Semi-active and semi-passive RFIDs differ in that the on-board power source is used to feed the microchip, whereas transmission is either active (semi-active) or performed using back-scattering (semi-passive). Several vendors propose proprietary middleware platforms that have been developed with the aim to support commercial deployments of RFIDs; see for example the SAP Auto-ID Infrastructure [73]. Other platform include the Siemens RFID Middleware, Sun Java System RFID Software or the IBM WebSphere RFID.

Ultimately, the main challenge from the communication/computing perspective that hides behind the IoT concept is the need for an *architecture* supporting *low-power, low-cost and yet fully networked and integrated devices* fully compatible with standard communication technologies.

4.2. Distributed systems technology

This area includes all aspects related to enabling objects to build a network, creating a distributed platform that enable the easy implementation of services on top. This builds on a traditional research line in computer science [74,75], where a distributed system is defined as a system driven by separate components which may be executed either sequentially or in parallel on different, interconnected, nodes. The design of architectures and protocols for distributed systems is a key issue for general networked systems and for IoT in particular. In particular, several issues, involved in the design of IoT as a distributed system, can be identified. The analysis and design of IoT cannot overlook aspects related to networking technologies such as routing protocols, flow control robustness, and synchronization. Problems like leader-election, node counting and averages computation are a core topic in the distributed systems literature [76–78]. Part of such research lines have been already re-discovered and renewed in sensor networks literature, as recalled in the previous section [79,80].

The distributed implementation of routing protocols is one of the fundamental algorithmic building blocks for networked systems [81]. However, as seen above, scalability issues discourage multi-hop communications for environmental data retrieval, i.e., massive and large scale sensor networks do not appear a viable solution for IoT,

[2] http://www.libelium.com/products/waspmote.

at present. Alternative architectures may make use of proximity communications whenever possible in case of large deployments; possible implementations are described in [82,83].

The massive amount of data streaming from the environment to the Internet is a side effect of the IoT type of scenarios: this means a potentially very large amount of information injected into the network. The control of information injected by "objects" and related data filtering techniques is a concern for pervasive scenarios [84]. Distributed flow control, in turn, is a well-studied traditional topic in networking and controls due to the large amount of work on TCP [85]. *Surprisingly, how to control the huge amount of data injected into the network from the environment is a problem so far mostly neglected in the IoT research*. Robustness and fault tolerance will become fundamental topics in IoT scenarios, involving both the impact of communication links failure, nodes software and hardware failures, critical data integrity and general safety aspects. For a general reference on fault tolerance and robustness approaches please refer to [86]. Issues concerning the impact of misbehaving nodes [87] represent also a traditional topic that is of interest for large-scale distributed systems as those foreseen in IoT. *For a large-scale IoT deployment, the presence of myriads of devices in the environment requires to replace/repair/reprogramm faulty, possibly embedded devices and to design a system natively robust to failures of single nodes or groups thereof.*

Synchronization of clocks for tasks, which might undergo failures and restart has also been addressed extensively in the literature [88]. In the IoT scenario, the foreseen large scale enriches the challenges for both for data consistency reasons and protocols functioning purposes.

From the implementation standpoint, a key issue is to ease the inter-working from an application perspective. In practice, what is typically provided is a middleware platform guaranteeing a pre-defined infrastructure for development and execution of distributed applications. Middleware design, in particular, has become a popular research area [89–91]. Middleware communications may involve synchronous, asynchronous, message or request-oriented methods. The IoT domain spans any of those models depending on the specific application targeted.

As mentioned before, a key issue of IoT systems will be the possibility to address objects using unique IDs. The initiative for the definition of a global naming system, ONS [92], is meant to extend the concept of Domain Name Service (DNS) to real-world RFID-tagged objects. Indeed, the ability of distinguishing objects is key in enabling distributed applications. *At present, the possibility to address an object and a network node in a seamless fashion is a quite deep technical issue and requires a global-scale standardization effort, probably wider than ONS. This issue represents also one of the key technical barriers to overcome in order to foster wide adoption of IoT technology.*

4.3. Distributed intelligence

Given a system of smart objects that are interconnected in the digital domain and equipped with suitable interfaces for programming purposes, applications need to coordinate communications and computing in order to leverage the data coming from several information sources.

IoT scenarios will be typically characterized by huge amounts of data made available. A challenging task is to interpret such data and reason about it. This underpins the need to have an actionable representation of IoT data and data streams. This represents a key issue in order to achieve re-usability of components and services, together with interoperabilty among IoT solutions. Advances in data mining and knowledge representation/management will also be required, to satisfactorily address the peculiar features of IoT technologies.

A related research field is that of distributed artificial intelligence, which addresses how autonomous software entities, usually referred to as 'agents', can be made able to interact with the environment and among themselves in such a way to effectively pursue a given global goal [93]. Notice that in this domain a major challenge has to be faced, compared to the traditional design of a distributed system. In fact, consider a simple task that involves the coordination of several autonomous entities: e.g., voting, auctioning, or cluster formation. The design of such applications has to account for the fact that part of the control resides on single agents. Those are the entities that ultimately interact and may choose different strategies depending on a certain utility function. Thus, at system design time, it is possible to leverage the theory of competitive/cooperative games and let agents compete/form coalitions upon their needs [94]. Theoretical foundations for these topics are rooted in game theory and social welfare. Applications to networking problems emerged only recently. A technical description of the issues arising in that context are beyond the scope of this survey: for a standard reference see [95]. *The access to the IoT devices is unlikely to be centrally scheduled; conversely, it will be likely decided based on local interaction of IoT users and devices. This in turn may stimulate a game-theoretical approach to the resulting problem of resource (object) sharing in the IoT.*

IoT may well inherit concepts and lessons learned in pervasive computing, ambient intelligence applications and service-oriented computing [96–99], as detailed in Section 3. Researchers working in the field of human–computer interfaces and user-centric design methodologies, in particular, addressed already several issues concerning the impact of sensorized and pervasive environment on the user experience [100]. *Since IoT will take the reference scenarios one step further in terms of scale and offered features, it will also require the development of suitable, scalable service delivery platforms that permit multiple services to coexist. As mentioned already in the previous sections, in literature there exists indeed a clear gap as concerns reference architecture models able to support the composition of IoT based services.*

Another key set of research challenges relate to security issues. Due to their fundamental role as enablers of IoT applications, they will be separately discussed in the following section.

The taxonomy of the main research areas and related topics relevant to the Internet-of-Things, as described above, is graphically depicted in Fig. 1.

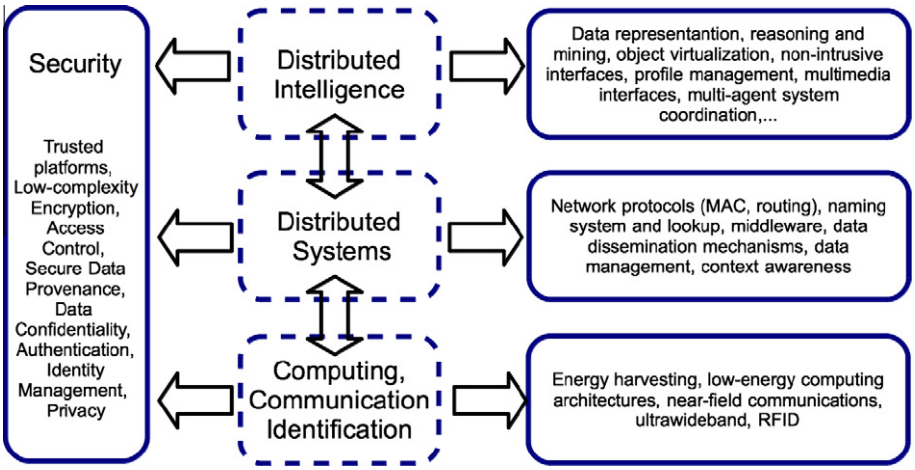

Fig. 1. Taxonomy of research areas relevant to Internet-of-Things.

5. Security

Security represents a critical component for enabling the widespread adoption of IoT technologies and applications. Without guarantees in terms of system-level confidentiality, authenticity and privacy the relevant stakeholders are unlikely to adopt IoT solutions on a large scale. In early-stage IoT deployments (e.g., based on RFIDs only), security solutions have mostly been devised in an ad hoc way. This comes from the fact that such deployments were usually vertically integrated, with all components under the control of a single administrative entity. In the perspective of an *open* IoT eco-system, whereby different actors may be involved in a given application scenario (e.g., one stakeholder owing the physical sensors/actuators, one stakeholder handling the data and processing them, various stakeholders providing different services based on such data to the end-users, etc.), a number of security challenges do arise. In this section, we aim at revising and discussing the major security challenges to be addressed to turn Internet-of-Things technology into a mainstream, widely deployed one. In particular, we identified three key issues requiring innovative approaches: data confidentiality, privacy and trust. In the following, we analyze them one by one. It is worth remarking that, as depicted in Fig. 1, security considerations are orthogonal to the other research areas, and span both the communications/networking, platform/data management and application/service levels.

5.1. Data confidentiality

Data confidentiality represents a fundamental issue in IoT scenarios, indicating the guarantee that only authorized entities can access and modify data. This is particularly relevant in the business context, whereby data may represent an asset to be protected to safeguard competitiveness and market values. In the IoT context not only users, but also authorized objects may access data. This requires addressing two important aspects: first, the definition of an access control mechanism and second, the definition of an object authentication process (with a related identity management system).

As data in IoT applications will be related to the physical realm, ensuring data confidentiality is a primary constraint for many use cases (see Section 6 for further description of potential application scenarios). As a first example, we may consider data provided by bio-sensors on bacterial composition of the product used for guaranteeing the required quality in the food industry. This data is clearly confidential because their uncontrolled spreading could harm company reputation and its competitive advantage over competing companies. As a second example, we may consider an environmental monitoring application, whereby data is used to feed an early warning system against, e.g., the rise of tsunami/earthquakes, etc. In such a setting, data should be accessible only by the relevant civil protection bodies, which can then put in place appropriate risks management strategies. The leakage of such information into the public sphere may give rise to chaotic and panic situations, putting at risk the safety of large groups of people.

Customary solutions for ensuring data confidentiality may not be straightforwardly applied to IoT contexts, due to two major limiting factors. The first one concerns the sheer amount of data generated by such systems, and relates hence to scalability issues. The second one relates to the need of controlling the access to data in an on-line and flexible way, with access rights changing at run-time and being applied to dynamic data streams.

Various access control techniques have been proposed to ensure confidentiality in knowledge management systems.[3] A standard approach, which matches well the features of IoT environments, is represented by Role-Based Access Control (RBAC) [101]. The concept of RBAC has emerged in the past decade as a widely used and highly successful alternative to conventional discretionary and mandatory access controls. In RBAC, users and permissions are

[3] All techniques are based on a strong trust assumption with respect to the system platform that handles the access attributes.

assigned to *roles*. Users acquire permissions indirectly via roles assignment. The main advantage of RBAC, in an IoT perspective, is the fact that access rights can be modified dynamically by changing the role assignments. The IoT context requires the introduction of new forms of RBAC-style solutions, in particular considering that IoT data will likely represent streams to be accessed in real-time, rather than constituting static databases. Data Stream management systems have been increasingly used to support a wide range of real-time applications (battlefield and network monitoring, sensor networks and so on), and represents a suitable solution for the IoT context. In IoT, access control techniques should be integrated with data streams management systems. The scientific literature offers few proposals, which are classified into two main categories: those aiming to ensure authenticity, confidentiality and integrity of data streams during transmission [102,103] and those related to access control [104,105]. An example of the first category is presented in [103], which proposes an extension of the RC4 encryption algorithm to overcome possible decryption failures due to synchronization problems. The proposed encryption scheme has been developed in the Nile [106] stream engine. Another interesting proposal is discussed in [102], where authors address the authenticity problem of outsourced data streams. More precisely, [102] considers a scenario where a data owner constantly outsources its data streams, complemented with additional authentication information, to a service provider. As far as data stream access control is considered, it is only recently that mechanisms to guard against unauthorized access to streaming data have been investigated. The work in [104] proposes a model for extending RBAC to protect data streams from unauthorized access. The basic idea is to apply a newly designed operator at the stream, resulting from the evaluation of a query to filter out output tuples that do not satisfy access control policies. The main drawback of this approach is that the proposed framework is not able to handle certain control policies on views of data from multiple streams, as occurs in IoT. Another relevant work is presented in [105], where the authors propose that the data access policies are defined by the user owning the devices and within the data stream itself. This makes users able to specify how the data streams management system has to access her/his personal data. As such, this solution is more suitable for addressing privacy issues, rather than general access control problems. This approach is also dependent on the adopted stream engine, raising issues in terms of support of heterogeneous stream engines. The most general available solution, to best of our knowledge, is [107], which extends the work of [108,109] by proposing a general framework to protect streaming data that is independent form the target engine. The framework is based on an expressive role-based access control tailored for data streams [108]. It exploits a query rewriting mechanism, which rewrites user queries in such a way that they do not return data tuples that should not be accessed according to the specified access control policies. Furthermore, the framework includes a deployment module that translates the rewritten query in such a way that it can be executed by heterogeneous stream engines, thus overcoming the lack of a standardized stream engine solution. This framework should therefore be considered a good starting point for the development of an holistic solution for IoT scenarios.

In many applications aggregated data obtained from multiple data sources by applying adequate operators, will be used. In the literature there are many works that address security issues of aggregated data in WSN. These works have been classified in hop-by-hop encrypted data aggregation and end-to-end encrypted data aggregation. In the former the data is encrypted by the sensing nodes and decrypted by the aggregator nodes. The aggregator nodes, then, decrypt data coming from the sensing nodes, aggregate data and encrypt the aggregated data again. At last, the *Sink* gets the final encrypted aggregation result and decrypts it. In the end-to-end encrypted data aggregation the intermediate aggregator nodes have not the key and can only do aggregations on the encrypted data.

Different hop-by-hop related works [110–112] assumes that data security is guaranteed by means of some key distribution schemes. For example SEDAN [113] proposes a secure hop-by-hop data aggregation protocol, in which each node can verify immediately the integrity of its two hops neighbors' data and the aggregation of the immediate neighbors by means a management of new type of key, called *two hops pair-wise key*. The performance of SEDAN, evaluated by means of ad hoc simulation, shows that such scheme is able to outperform competitive solutions such as SAWAN [110] in terms of overhead and mean time to detection. All hop-by-hop proposed solutions are vulnerable because the intermediate aggregator nodes are easy to tamper and the sensor readings are decrypted on those aggregators. End-to-end encrypted techniques overcome this weakness of hop-by-hop techniques. Notice that end-to-end secure data aggregation techniques also use a key scheme. Some approaches [114–117] suggest to share a key among all sensing nodes and the *Sink*, the aggregator nodes have not the key because the aggregator nodes handle data without making any encryption/decryption operation. The limitation of such a solution is that the whole network is compromised in case the key is compromised in a sensing nodes.

An alternative approach is represented by the adoption of public-key encryption [118], but in this case the drawback is represented by the related high computational cost.

The aforementioned solutions are all focused on lower layer security issues, i.e., on the adoption of encryption techniques and ad hoc key distribution schemes [119–121]. In the IoT domain, the use of aggregated data requires to address two other fundamental research challenges. The first one is related to the access control of aggregated data/data streams: in case of the aggregation of data with different access attributes a solution is needed to establish the access attributes of the aggregated data. The second, related, one deals with the introduction of appropriate operators for ensuring the impossibility of recovering raw data streams from the aggregated one.

Furthermore, in order to avoid unauthorized access, especially considering the use of wireless communications means at the lower layers, the access control mechanisms should be combined with appropriate data protection techniques. Typical examples are anonymization techniques based on data suppression or randomization

[122,123], or other data cloaking mechanisms, which perturb data following some criteria (e.g., k-anonymity guarantees that every record is indistinguishable from at least $k-1$ other records [124]). Relevant issues to be addressed in this context relate to scalability and energy consumptions of existing solutions, which may not meet the requirements typical of IoT deployments.

Another aspect that should be considered when the problem of confidentiality is faced is that of *identity management*. In fact this issue is critical in IoT scenarios where there is a fusion of digital and physical world. The problem is to find solutions for handling in secure manner the identity of objects/things and the related authorization processes. Although user's identity management is a well-investigated topic in the literature, managing the identity of smart objects raises a number of novel issues to be dealt with.

First, it is necessary to reach an agreement on a well-defined concept of identity, when referred to a smart object. A well characterized definition of identity should indeed drive the development of an object identity management system (IdM), specifying the main operations that the IdM should perform. Looking at the state-of-the-art, a starting point could be represented by the concept of federation [125]. A federation is defined as a set of organizations that establish trust relationships with respect to the identity information maintained. A federated identity management system provides a group of organizations that collaborate with mechanisms for managing and gaining access to identity information of a given entity in the system and other resources across organizational boundaries. Traditionally, identity management systems consider users as entities whose identity has to be managed; in our case we are interested in systems whereby the identity attributes relate to smart objects, and not to users.

IdM systems involve at least two types of actors: identity providers (IdP) and service providers (SP). An IdP manages authentication of entities[4] and of entity-relevant information. A SP offers services to users that satisfy the policy requirements associated with the offered services. It further specifies and enforces the access control policies for the resources it offers. An organization in a federation can act as both an IdP and a SP.

In most IdM systems, IdPs authenticate entities using single-sign-on (SSO) technology. With SSO, conventionally, users can log on with the same user name and password for seamless access to federated services within one or multiple organizations. Federated identity includes not only users' login names, but also user properties, or user identity attributes (user attributes, for short). Thus, authorizations, specified for a given resource, are no longer expressed in terms of user login IDs, but in terms of requirements and conditions against user properties.

In order to apply these concepts to IoT scenarios, we need to assess their suitability to deal with smart objects instead of users. Further, we need to properly account for the distributed nature of IdPs and SPs in IoT applications. We thus need a secure and privacy-preserving mechanism for retrieving the entity attributes from different SPs. The IdM system must provide only the object's information that is needed to satisfy the requesting SPs' access control policies. In this regard, objects should present different accessibility (privacy) levels for various types of information. For example, depending on the specific application considered, an object might agree to share a given type of information, but not all its attributes. Such requirements call for a flexible and selective approach to sharing entity attributes in federated systems. A system could achieve selective release of identity by supporting multiple federated digital identities. In this direction is the proposal of [125] that integrates federated IdM with trust-negotiation techniques. In this way, entities do not have to provide a given attribute more than once to a given federation. Although it represents a promising approach, for both its flexible/distributed nature and its capability to couple identity management with trust, its application to IoT scenarios require proper tailoring and further studies.

Summarizing, the main research challenges for ensuring data confidentiality in an IoT scenario, as reported in Fig. 2, relate to:

- Definition of suitable mechanisms for controlling access to data streams generated by IoT devices.
- Definition of an appropriate query language for enabling applications to retrieve the desired information out of a data stream.
- Definition of a suitable smart objects' identity management system.

5.2. Privacy

Privacy defines the rules under which data referring to individual users may be accessed. The main reasons that makes privacy a fundamental IoT requirement lies in the envisioned IoT application domains and in the technologies used. Health-care applications represent the most outstanding application field, whereby the lack of appropriate mechanisms for ensuring privacy of personal and/or sensitive information has harnessed the adoption of IoT technologies. In addition, in the IoT vision, a prominent role will be played by wireless communication technologies. The ubiquitous adoption of the wireless medium for exchanging data may pose new issue in term of privacy violation. In fact, wireless channel increases the risk of violation due to the remote access capabilities, which potentially expose the system to eavesdropping and masking attacks. Hence privacy represents a real open issue that may limit the development of the IoT.

A number of frameworks have been proposed for accounting for privacy issues in the system design phase, such as Kaos [126], Tropos [127,128], NFR [129,130], GBRAM [131], PRIS [132,133]. The latter approach may represent a viable starting point for the definition of appropriate privacy-preserving mechanisms for IoT. PRIS [132], indeed, represents a requirement engineering methodology, which incorporates privacy requirements into the system design process. PRIS provides a set of concepts to

[4] Traditional IdM systems handle identities of users. As we are interested also in handling identities of smart objects, we use the term 'entity' in the remainder to indicate both users and smart objects, depending on the application context.

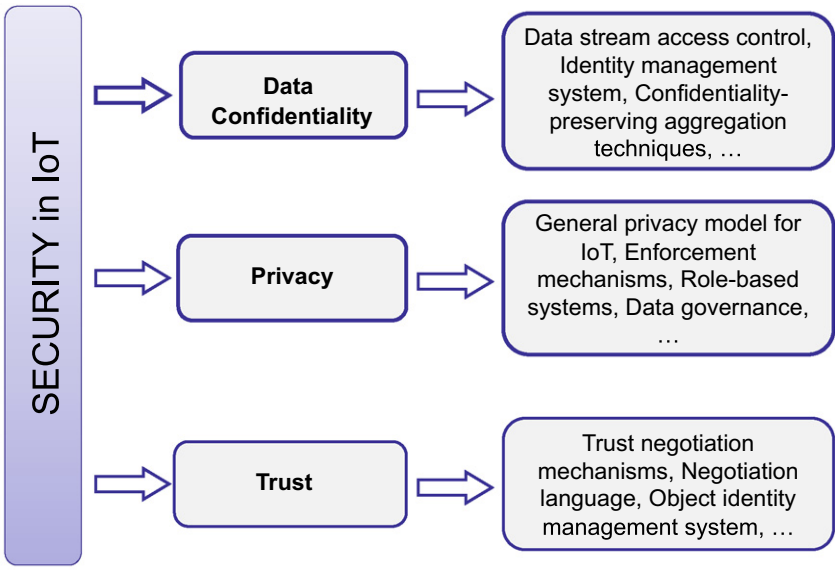

Fig. 2. Graphical representation of security challenges in Internet-of-Things.

model privacy requirements and a set of rules to transform such requirements into implementation techniques. Different is the goal of [133], which defines a general UML conceptual model for representing privacy policies. The model specifies the needed functional modules of an application in order to enforce such policies, introducing all the elements required for the definition of privacy aware systems. As it operates at a very high level of abstraction, it is suitable for application to IoT scenarios, characterized by a high degree of heterogeneity in terms of privacy requirements.

At the same time, the development of concrete approaches for building privacy-preserving mechanisms for IoT applications still presents a number of challenging aspects. The development of concrete implementations would benefit from the definition of a general model, able to represent all IoT fundamental entities and their relationships. Moreover the implementations should include enforcement mechanisms able to cope with the scale and with the dynamic nature of IoT scenarios. In order to satisfy such requirements, solutions also able to enforce a dynamic data stream access control should be provided. Summarizing, the open research challenges in terms of privacy-preserving mechanisms for IoT, as reported in Fig. 2, are given by:

- Definition of a general model for privacy in IoT.
- Development of innovative enforcement techniques, able to support the scale and heterogeneity characterizing IoT scenarios.
- Development of solutions that balance the need of anonymity presented by some applications with the localization and tracking requirements of some other ones. This entails the definition of privacy policies, that specify under which conditions it is possible to identify and localize a smart object. Moreover, it needs to specify when it is possible to access sensitive data.

5.3. Trust

The concept of trust is used in a large number of different contexts and with diverse meanings. Trust is a complex notion about which no consensus exists in the computer and information science literature, although its importance has been widely recognized. Different definitions are possible depending on the adopted perspective. A main problem with many approaches towards trust definition is that they do not lend themselves to the establishment of metrics and evaluation methodologies.

A widely used definition is the one provided by Blaze and Feigenbaum [134], which refers to security policies regulating accesses to resources and credentials that are required to satisfy such policies. Trust negotiation refers to the process of credential exchanges that allows a party requiring a service or a resource from another party to provide the necessary credentials in order to obtain the service or the resource. This definition of trust is very natural for secure knowledge management as systems may have to exchange credentials before sharing knowledge. For this reason, we base our analysis of trust issues in IoT upon it. Trust negotiation relies on peer-to-peer interactions, and consists of the iterative disclosure of digital credentials, representing statements certified by given entities, for verifying properties of their holders in order to establish mutual trust. In such an approach, access resources (data and/or services) is possible only after a successful trust negotiation has been completed. A trust negotiation system typically exploits digital identity information for the purpose of providing a fine-grained access control to protected resources. The ability to meet the trust requirement is indeed strictly related to the identity management and access control issues, as discussed above. At present a limited number of solutions are available [135,136,46,134]. The most popular approaches include KeyNote [134] and TrustBuilder [46], which nonetheless

do not lend themselves to a straightforward application to the IoT domain, due to the high computational requirements they impose. Many open issues have to be addressed in order to develop IoT trust services. First, the definition of globally accepted certification authorities should be addressed, together with a number of requirements that an IoT-compliant certification authority should respect. Furthermore, it is necessary to devise an effective trust negotiation language, able to simplify credential specifications and to express a wide range of protection requirements through the definition of flexible disclosure policies. In addition, the definition of an effective model of trust should account for both the highly distributed nature of the IoT as well as for the requirements (in terms of computational complexity and/or response time) typical of many IoT applications.

In other words, we need to move away from the classical centralized and static approaches underpinning the most widely used trust management solutions, to adopt a fully distributed and dynamic approach that assumes that no trust relationship is defined a priori among the entities in the system. Moreover, a new flexible framework for trust management should be introduced in order to meet the scalability requirements that arise at different levels, including, e.g., naming and addressing information knowledge management and service provisioning.

Anyway, although the complete dynamic and distributed nature of IoT makes to address trustworthiness extremely challenging, we may well consider IoT as an extremely interesting application of trust concepts. In fact in a context in which smart objects themselves take decisions, the first trust relationship has to be established among humans and the objects surrounding them.

The most relevant research challenges in the definition of appropriate trust mechanisms for IoT, as reported in Fig. 2, can be summarized as:

- Introduction of a simple trust negotiation language supporting the semantic interoperability requirements of IoT.
- Definition of a trust negotiation mechanism based on a fine-grained access control of data streams.
- Development of an adequate object identity management system.
- Design of a general and flexible trust management framework able to leverage the aforementioned items.

6. Applications and impact areas

The concept of Internet-of-Things, with its vision of Internet-connected objects of various capabilities and form factors, could boost the role of ICT as innovation enabler in a variety of application markets.

One of the technological pillars of the Internet-of-Things, namely RFID technology, has already been incorporated into a wide array of products. The number of RFID tags sold in 2011 accounted to 2.88 tags (source: www.idtechex.com), with an estimated market value of $ 5.84 billions (source: www.idtechex.com). Adoption of RFID technology in industry slowed down in 2008/2010 as a consequence of the global economic downturn, but this decrease got balanced by the adoption of RFID technology by major governments (e.g., the issuance of RFID-tag-inlaid Resident ID cards by the Ministry of Public Security of China).

The increase in the usage of RFID, paving the way to making Internet-of-Things a reality, is not simply a result of technological push; it is also driven by the market pull, since enterprises are increasingly realizing the commercial benefits of applications that can be realized with Internet-of-Things technologies. The evolution of Internet-of-Things may follow the evolution path of mobile phones [137]. At the end of 2009 there were 5.9 billion mobile phone subscribers (source: ITU), driven by the need to communicate anywhere and at anytime. Now, imagine this connectivity being brought to everyday objects: fridges, cars, cups, keys, etc., as it will be enabled by IoT. A huge market opportunity exists for Internet-of-Things, related to the possibility of networking smart things and of providing applications leveraging said connectivity.

Besides enhancing the competitiveness of various vertical markets, IoT technologies can open up new business opportunities by: (i) bridging vertical markets, giving rise to cross-cutting applications and services, based on the use of a common underlying ICT platform, (ii) enabling the arising and growth of new market segments and applications, made possible by the ability, provided by IoT technologies, to interact with physical objects via digital means and (iii) optimizing business processes by leveraging on advanced analytics techniques applied to IoT data streams.

As an example of the latter point, we could consider the "smart fridge" scenario, whereby items stored in a refrigerator are identified by means of RFID or equivalent technologies and the fridge has embedded computing and networking capability, so that it may understand the quantity and type of items stored and decide whether there is a need to buy new items, etc. At the moment the electronic appliances and the large-scale retail trade represent separate industrial sectors. Without a set of common technical standards and interfaces (at both the device and semantic level) joining the activities of such two sectors, an IoT-enabled device like the smart fridge could not take place. Vice versa, the adoption of IoT technologies can give rise to new business ecosystems, characterized by new actors and value chains. An example could be a brokerage service that, by accounting for what is currently in your fridge, your dietary constraints and tastes, your agenda (in terms of dinners with friends, etc.) negotiates for you the best food at the best rate, etc.

In terms of application fields and market sectors where IoT solutions can provide competitive advantages over current solutions, we identified six ones which we do believe can play a leading role in the adoption of IoT technologies: environmental monitoring; smart cities; smart business/inventory and product management; smart homes/smart building management; health-care and security and surveillance. In the following we briefly discuss the relevance and potential impact of IoT technologies on the competitiveness of players in such markets.

- *Smart Homes/Smart Buildings.* Instrumenting buildings with advanced IoT technologies may help in both reducing the consumption of resources associated to

buildings (electricity, water) as well as in improving the satisfaction level of humans populating it, be it workers for office buildings or tenants for private houses. Impact is both in economic terms (reduced operational expenditures) as well as societal ones (reducing the carbon footprint associated to buildings, which are a key contributors to the global greenhouse gas emissions). In this application, a key role is played by sensors, which are used to both monitor resource consumptions as well as to proactively detect current users' needs. Such a scenario integrates a number of different subsystems, and hence requires a high level of standardisation to ensure interoperability. Ability to reason in a distributed, cooperative way, and to actuate is also necessary in order to ensure that decisions taken on the resources under control (e.g., switch on/off lighting, heating, cooling, etc.) are in line with the users' needs and expectations, which in turn are strictly intertwined to the activities they undertake and/or plan to take.

- *Smart Cities.* The term 'Smart Cities' is used to denote the cyberphisycal eco-system emerging by deploying advanced communication infrastructure and novel services over city-wide scenarios. By means of advanced services, it is indeed possible to optimize the usage of physical city infrastructures (e.g., road networks, power grid, etc.) and quality of life for its citizens. IoT technologies can find a number of diverse application in smart cities scenarios. As a case study, IoT technologies can be used to provide advanced traffic control systems. Through IoT it will be possible to monitor car traffic in big cities or highways and deploy services that offer traffic routing advice to avoid congestion. In this perspective, cars will be understood as representing 'smart objects'. In addition, smart parking devices system, based on RFID and sensor technologies, may allow to monitor available parking spaces and provide drivers with automated parking advice, thus improving mobility in urban area. Moreover, sensors may monitor the flow of vehicular traffic on highways and retrieve aggregate information such as average speed and numbers of cars. Sensors could detect the pollution level of air, retrieving smog information such as the level of carbon dioxide, PM10, etc., and deliver such information to health agencies. Furthermore, sensors could be used in a forensics setting, by detecting violations and by transmitting the relevant data to law enforcement agencies in order to identify the violator, or to store information that will be provided in case of accident for subsequent accident scene analysis.
- *Environmental monitoring.* IoT technology can be suitably applied to environmental monitoring applications. In this case a key role is played by the ability of sensing, in a distributed and self-managing fashion, natural phenomena and processes (e.g., temperature, wind, rainfall, river height), as well as to seamlessly integrate such heterogeneous data into global applications. Real-time information processing, coupled with the ability of a large number of devices to communicate among them, provides a solid platform to detect and monitor anomalies that can lead to endangering human and animal life. The vast deployment of miniaturized devices may enable access to critical areas, whereby the presence of human operators might not represent a viable option (e.g., volcanic areas, oceanic abysses, remote areas), from where sensed information can be communicated to a decision point in order to detect anomalous conditions. In this perspective, IoT technologies can enable the development of a new generation of monitoring and decision support systems, providing enhanced granularity and real-time capabilities over current solutions. Another case in which the sensing ability of IoT devices supports the environmental safety is represented by fire detection. When a suite of sensors detects the possible presence of fire (by means, e.g., of temperature sensors), an alarm is sent directly to the fire department in a short time (exploiting the advanced communication features of IoT platform), along with other parameters that are useful in decision making and support, such as the description of the area subject to the fire, the possible presence of people, of inflammable materials, etc. Clearly, rapid response has the consequence of saving human lives, mitigating the damage to the property or vegetation and in general reducing the level of disaster. Many other scenarios related to civil protection can profit from IoT technologies (tunnel area, earthquake, tsunami, etc.), whereby the ability to access environmental data in real-time over large-scale areas enable the uptake of efficient coordination strategies among rescue teams.
- *Health-care.* IoT technologies can find a number of applications in the health-care sector. On the one hand, they can be used to enhance current assisted living solutions. Patients will carry medical sensors to monitor parameters such as body temperature, blood pressure, breathing activity. Other sensors, either wearable (e.g., accelerometers, gyroscopes) or fixed (proximity) will be used to gather data used to monitor patient activities in their living environments. Information will be locally aggregated and transmitted to remote medical centers, which will be able to perform advanced remote monitoring and will be capable of rapid response actions when needed. The interconnection of such heterogeneous sensors could provide a comprehensive picture of health parameters, thereby triggering an intervention by the medical staff upon detection of conditions that may lead to health deterioration, thus realizing preventive care.

  Another relevant application sector relates to personalized health-care and well-being solutions. The use of wearable sensors, together with suitable applications running on personal computing devices enables people to track their daily activities (steps walked, calories burned, exercises performed, etc.), providing suggestions for enhancing their lifestyle and prevent the onset of health problems.
- *Smart business/Inventory and product management.* RFID technologies are already used in many sectors for inventory management, throughout the supply and delivery chain. This relies on the ability of RFID technologies to identify and provide support for tracking goods. At the moment, however, RFID applications are built in a rather ad hoc fashion, and are only partially integrated into supply management systems.

RFID are customarily used to monitor and manage the movement of products through a supply chain; typically, RFID tags are directly attached to the items (or to the containers that carry them), while readers are placed throughout the facility to be monitored. IoT technologies can provide enhanced flexibility in terms of readers positions, while at the same time enabling seamless interoperability between RFID-based applications used by different actors dealing with the product throughout the various phases of its life-cycle.
In retail applications, IoT technologies can be used to monitor in real-time product availability and maintain accurate stock inventory. They can also play a role in after-market support, whereby users can automatically retrieve all data about the products they bought. Also, identification technologies can help in limiting thefts and in fighting counterfeiting by providing products with a unique identifier including a complete and trustworthy description of the good itself.
Furthermore, sensors and specifically bio-sensor technologies in combination with RFID technology may allow control production processes, final product quality and possible shelf life deterioration of the product, e.g., in the food industry. For example, RFID devices can be used to identify and track the product, while the bio-sensors can monitor parameters such as temperature and bacterial composition in order to guarantee required quality of the final product.

- *Security and surveillance.* Security surveillance has become a necessity for enterprise buildings, shopping malls, factory floors, car parks and many other public places. Homeland security scenarios faces also similar threats, albeit on a different scale. IoT-enabled technologies can be used to greatly enhance the performance of current solutions, providing cheaper and less invasive alternatives to the widespread deployment of cameras while at the same time preserving users' privacy. Ambient sensors can be used to monitor the presence of dangerous chemicals. Sensors monitoring the behaviour of people may be used to assess the presence of people acting in a suspicious way. Efficient early warning systems can therefore be built. Personal identification by means of RFID or similar technologies is also an option. However in many countries user associations are fiercely protesting about the privacy infringement that could result from the widespread adoption of such a technology. When used in conjunction with role-based access control systems, IoT technologies can provide high level of flexibility, being able to cope with access policies (e.g., to different areas of buildings) which may change over time due to logistic changes and/or to changes in role of the user and/or according to contextual information (e.g., some areas not accessible on a given day due to renovation works going on). Also in this market the advantages are in terms of enhanced functionality, better user acceptance through reduction of the use of cameras, reduced operational costs and increased flexibility in a changing environment.

Clearly, the scope of IoT is extremely wide. However, applications that are built on top of IoT may consistently improve the competitiveness of the solutions at hand. IoT adoption is therefore expected to be to strongly driven by the market needs and by the market dynamics. At the same time, ICT industries, standardisation bodies and policy-makers are undertaking a series of initiatives to steer the IoT development process with the objective of maximizing its socio-economic value while minimizing the threats related to privacy and confidentiality of data. In this regard, the following section reviews a number of IoT initiatives and also provides a discussion on standardisation activities.

7. Related on-going initiatives

A number of large-scale initiatives on IoT are active in the US, in Europe, in Japan, China, Korea and other countries. In the following subsection we will briefly report on the most relevant ones.

Besides research initiatives, standardization activities are also of key importance in order to ensure a successful widespread adoption of IoT technologies and services. In Section 7.2 we briefly report on the most relevant ones.

7.1. IoT related projects

The growing interest in IoT technologies and applications is well exemplified by the number of research initiatives arising worldwide around such themes. In the US, the American National Science Foundation (NSF) launched in 2008 a program on Cyber-Physical Systems,[5] aimed at introducing systems able to merge computational and physical resources. The program is meant to cover a wide array of application scenarios, ranging from smart electric grid to smart transportation, from smart medical technologies to smart manufacturing. The 2010 report of the President's Council of Advisors on Science and Technology, "Designing a digital future: federally funded research and development in networking and information technology"[6] encourages further investments in Cyber-Physical System, due to their high potential impact on a number of critical industrial sectors.

The European Commission has been pushing initiatives related to IoT since 2005 [5], and has recently launched, in the framework of the 7th Framework Programme, an initiative on "Internet-Connected Objects". The focus is on adoption of IoT technologies and services in enterprise environments, with the aim of increasing the competitiveness of European industry through adoption of IoT-enabled solutions[7] http://www.rfid-in-action.eu/cerp. Activities in such field led to the definition of a strategic research agenda, including a description of European strategies in this sector [6].

Within the initiatives which have taken place at the European level, four large-scale ones are worth mentioning. The HYDRA project[8] developed a middleware based on a service-oriented architecture, transparent to the under-

[5] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286.
[6] http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf.
[7] http://cordis.europa.eu/fp7/ict/programme/challenge1_en.html.
[8] http://www.hydramiddleware.eu.

lying communication, supporting distributed as well as centralized architectures, security and trust models. This project was meant to provide a middleware solution allowing the developers to incorporate heterogeneous physical devices into their applications by offering easy to use Web service interfaces for controlling the physical devices. Support was provided for a number of underlying communication technologies, including Bluetooth, RF, ZigBee, RFID, WiFi, etc. The Hydra middleware included methods for performing effectively device and service discovery, for supporting peer-to-peer interaction models and efficient diagnostics tools. Solutions for distributed security and social trusts were also devised and prototyped.

The RUNES project[9] was meant to create a large-scale, widely distributed, heterogeneous networked embedded systems which provide a flexible and adaptable ICT tool to leverage environmental data. The main target of RUNES is a fully operational middleware enabling the potential for the introduction of a new class of networked embedded systems. In RUNES, one of the target challenges was to achieve the required level of self-organization to suit a dynamic environment, while ensuring that proper interfaces were provided to programmers in order to ease the development of applications and services. This was meant to allow for a significant cut in the cost of new application development and a much faster time to market.

The IoT-A project[10] aims at introducing an architectural reference model for the interoperability of Internet-of-Things, together with a set of mechanisms for its efficient integration into the service layer of the Future Internet. The project is a large-scale one, involving a number of relevant stakeholders and addressing a number of application domains. Particular attention is paid to resolution schemes, whereby innovative approaches are proposed to ensure scalable look-up and discovery of smart objects and associated resources.

The iCORE project[11] aims at empowering the IoT with cognitive technologies and is focused around the concept of virtual objects (VOs), intended as semantically enriched virtual representation of the capabilities/resources provided by real-world objects fostering their re-usability and supporting their aggregation into more composite services (composite virtual objects – CVOs). VOs provide a unified representation, thereby hiding any underlying technological heterogeneity and providing a standardized way of accessing objects' capabilities and resources. One key element in the iCORE project is the use of advanced cognitive techniques for managing and composing VOs to improve IoT applications and better match user/stakeholder requirements. Four use cases are put forward for validation purposes: ambient assisted living, smart office, smart transportation and supply chain management.

IoT-centric programs are active also in Japan, under the umbrella of the UNS initiative (Ubiquitous Networked Society, part of the wider "e-Japan" strategy[12]), which focuses on the ubiquitous presence of sensors and RFIDs in order to enable pervasive services, with target applications ranging from smart home environments to supply chain management.

While the widespread diffusion of research initiatives denotes the vitality of the field and the potential of IoT applications, it brings alongside a risk of fragmentation and of lack of adoption of adequate standards. IoT would require, as the technology gets mature and makes its way into the real world, a careful standardization process, in order to ensure interoperability among devices and applications coming from different countries, building the foundations the real arising of an "Internet" of things.

7.2. Standardization activities

A number of standardization activities with focus on tag-based technologies has been active in the last years. These standardization activities are confined mostly within the sensing/RFID domain. In particular, the RF-layer and the NFCIP (Near Field Communication Interface and Protocol) are already standardized by various bodies (ISO 18092, 21481, 22536 and 23917; ECMA 340, 352, 356 and 365; ETSI TS 102 190). Also, ECMA 340/352 and ISO 18092/21481 describe the Near Field Communication Interface and Protocol (NFCIP-1 and -2). Test methods for interfaces and protocols are described in ECMA 356/362 and in ISO 22536/23917. In parallel, also the Global System for Mobile Communications Association (GMSA) established a NFC working group in 2006 and already derived guidelines for NFC services to be supported by cellular phones technologies. The reason for the interest of the GSMA is that cellular technology is perceived as a potential enabler for the diffusion of a large number of services based on the use of embedded NFC devices (e.g., micro-payments).

A key issue in IoT relate to the naming systems. As most IoT applications would require unique identifiers, a global coordination of the naming scheme to be used is needed. In the RFID field, the most widely adopted solution is the Electronic Product Code (EPC). Specification of EPC identifiers constitute an open, freely accessible standard, issued by EPCglobal Inc., and based upon the work carried out in the last decade at the MIT Auto-ID Center. Object Naming Service (ONS) represents a mechanism for discovering information about a given object starting from its EPC [92].

In terms of communications among smart objects, we should distinguish between two aspects. At the lower layers (PHY and MAC), IEEE is running the 802.15 Working Group on wireless personal area networks. This includes a number of task groups, which led to the definition of the 802.15.4 specifications, which are at the basis of the ZigBee technology. Lately, attention has also been devoted to optical wireless communications, within the 802.15.7 Task Group. In terms of upper layers, ETSI has launched in 2008 a technical committee on Machine-to-Machine (M2M) communications, which is however mostly focused on the telecommunications perspective.[13]

It is important to remark that there is a clear lack of standardization activities related to the data models, ontologies and data format (s) to be used in IoT applications and

[9] http://www.ist-runes.org/.
[10] http://www.iot-a.eu/.
[11] http://www.iot-icore.eu/.
[12] http://www.kantei.go.jp/foreign/it/network/0122full_e.html.
[13] http://www.etsi.org/Website/Technologies/M2M.aspx.

in terms of service-level interfaces and protocols. Such issues are expected to play a key role for enabling semantic interoperability and thus the mushrooming of IoT-based services and applications. A working group on "Semantic Sensor Network" was active at W3C from 2009 to 2011; the final report could be found here: http://www.w3.org/2005/Incubator/ssn/XGR-ssn-20110628/. The lack of a shared approach towards such issues could represent a barrier for the development of an open IoT architecture, thereby harnessing the disruptive innovation potential of such technology.

8. Conclusions

The Internet-of-Things may represent the next big leap ahead in the ICT sector. The possibility of seamlessly merging the real and the virtual world, through the massive deployment of embedded devices, opens up new exciting directions for both research and business.

In this survey article, we provided an overview of the key issues related to the development of IoT technologies and services. A number of research challenges has been identified, which are expected to become major research trends in the next years. The most relevant application fields have been presented, and a number of use cases identified.

We do hope that this survey will be useful for researchers and practitioners in the field, helping them to understand the huge potential of IoT and what are the major issues to be tackled, devising innovative technical solutions able to turn IoT from a research vision into reality.

Acknowledgments

The work of D. Miorandi and F. De Pellegrini was supported by the EC within the framework of the BIONETS Project IST-FET-SAC-FP6-027748, www.bionets.eu. The authors would like to acknowledge Dr. V. Osmani and Dr. G. Russello for the comments provided while preparing this work. The authors also acknowledge the iCore Consortium for the feedback and suggestions provided on an early version of the article.

References

[1] M. Weiser, The computer for the 21st century, Sci. Am. (1991) 94–100.
[2] L. Atzori, A. Iera, G. Morabito, The Internet of Things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.
[3] The Internet of Things, ITU Internet Reports, 2005. <http://www.itu.int/internetofthings/>.
[4] M. Zorzi, A. Gluhak, S. Lange, A. Bassi, From today's INTRAnet of things to a future INTERnet of things: a wireless- and mobility-related view, IEEE Wireless Commun. 17 (6) (2010) 44–51 .
[5] J. Buckley, From RFID to the Internet of things: pervasive networked systems, Final Report on the Conference organised by DG Information Society and Media, Networks and Communication Technologies Directorate, March 2006. <ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/au_conf670306_buckley_en.pdf>.
[6] Internet of Things: Strategic Research Agenda, September 2009. <http://ec.europa.eu/information_society/policy/rfid/documents/in_cerp.pdf>.
[7] G. Kortuem, F. Kawsar, V. Sundramoorthy, D. Fitton, Smart objects as building blocks for the internet of things, IEEE Internet Comput. 14 (2010) 44–51.
[8] G. Roussos, V. Kostakos, RFID in pervasive computing: state-of-the-art and outlook, Pervasive Mob. Comput. 5 (2009) 110–131. http://dx.doi.org/10.1016/j.pmcj.2008.11.004.
[9] I. Akyilidiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor network: a survey, Comput. Netw. 38 (4) (2002) 393–422.
[10] I.F. Akyildiz, I.H. Kasimoglu, Wireless sensor and actor networks: research challenges, Ad Hoc Netw. J. 2 (2004) 351–367.
[11] J. Saltzer, D. Reed, D. Clark, End-to-end arguments in system design, ACM Trans. Comput. Syst. 2 (1984) 277–288.
[12] V. Jacobson, D.K. Smetters, J.D. Thornton, M.F. Plasee, N. Briggs, R. Braynard, Networking named content, in: Proceedings of ACM CoNEXT, Rome, Italy, 2009, pp. 1–12.
[13] S. Dobson, S.G. Denazis, A. Fernández, D. Gaïti, E. Gelenbe, F. Massacci, P. Nixon, F. Saffre, N. Schmidt, F. Zambonelli, A survey of autonomic communications, TAAS 1 (2) (2006) 223–259. http://doi.acm.org/10.1145/1186778.1186782.
[14] W. Elmenreich, R. D'Souza, C. Bettstetter, H. de Meer, A survey of models and design methods for self-organizing networked systems, in: IWSOS, 2009, pp. 37–49.
[15] D. Guinard, V. Trifa, F. Mattern, E. Wilde, From the Internet of Things to the Web of Things: Resource Oriented Architecture and Best Practices, Springer, New York, Dordrecht, Heidelberg, London, 2011 (Chapter 5).
[16] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, D. Savio, Interacting with the SOA-based Internet of Things: discovery, query, selection, and on-demand provisioning of Web services, IEEE Trans. Serv. Comput. 3 (3) (2010) 223–235.
[17] L. Chen, M. Tseng, X. Lian, Development of foundation models for Internet of Things, Front. Comput. Sci. China 4 (2010) 376–385.
[18] F. Michahelles, F. Thiesse, A. Schmidt, J.R. Williams, Pervasive RFID and near field communication technology, IEEE Pervasive Comput. 6 (3) (2007) 94–96.
[19] C. Ghezzi, F. Pacifici, Evolution of software composition mechanisms: a survey, in: D. Lucia, F. Ferrucci, G. Tortora, M. Tucci (Eds.), Emerging Methods, Technologies, and Process Management in Software Engineering, J. Wiley and Sons, New York, 2008, pp. 3–19.
[20] S. Haykin, Cognitive radio: brain-empowered wireless communications, IEEE J. Sel. Areas Commun. 23 (2005) 201–220.
[21] I. Chlamtac, M. Conti, J.J.-N. Liu, Mobile ad hoc networking: imperatives and challenges, Ad Hoc Netw. 1 (1) (2003) 13–64.
[22] M. Murphy, J. Butler, Proactive computing: RFID & sensor networks, Final Report on the Conference organised by DG Information Society and Media, Networks and Communication Technologies Directorate, March 2006. <ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/au_conf670306_murphy_en.pdf>.
[23] M. Durvy, J. Abeillé, P. Wetterwald, C. O'Flynn, B. Leverett, E. Gnoske, M. Vidales, G. Mulligan, N. Tsiftes, N. Finne, A. Dunkels, Making sensor networks ipv6 ready, in: Proceedings of the Sixth ACM Conference on Networked Embedded Sensor Systems (ACM SenSys 2008), poster session, Raleigh, North Carolina, USA, 2008, pp. 421–422.
[24] V. Raghunathan, S. Ganeriwal, M. Srivastava, Emerging techniques for long lived wireless sensor networks, IEEE Commun. Mag. 44 (2006) 108–114.
[25] O.B. Akan, M.T. Isik, B. Baykal, Wireless passive sensor networks, IEEE Commun. Mag. 47 (2009) 92–99.
[26] I. Akyilidiz, F. Brunetti, C. Blazquez, Nanonetworking: a new communication paradigm, Comput. Netw. 52 (12) (2008) 2260–2279.
[27] H. Liu, M. Bolic, A. Nayak, I. Stojmenovic, Taxonomy and challenges of the integration of RFID and wireless sensor networks, IEEE Netw. 22 (2008) 26–35.
[28] L. Zhang, Z. Wang, Integration of RFID into wireless sensor networks: architectures, opportunities and challenging problems, in: Proceedings of GCCW, 2006, pp. 463–469.
[29] E. Aarts, R. Wichert, Ambient intelligence, in: H.-J. Bullinger (Ed.), Technology Guide, Springer, Berlin, Heidelberg, 2009, pp. 244–249.
[30] J. Gosling, B. Joy, G. Steele, The Java Language Specification, Addison-Wesley, 1996.
[31] R. Grimm, T. Anderson, B. Bershad, D. Wetherall, A system architecture for pervasive computing, in: Proceedings of the 9th ACM SIGOPS European Workshop, Kolding, Denmark, 2000, pp. 177–182.
[32] J.P. Sousa, D. Garlan, Aura: an architectural framework for user mobility in ubiquitous computing environments, in: Proceedings of the 3rd Working IEEE/IFIP Conference on Software Architecture, Kluwer Academic Publishers, Madison, Wisconsin, 2002, pp. 29–43.

[33] G. Judd, P. Steenkiste, Providing contextual information to pervasive computing applications, in: Proceedings of the IEEE International Conference on Pervasive Computing (PERCOM'03), Dallas, 2003, pp. 29–43.
[34] B. Schilit, M. Theime, Disseminating active map information to mobile hosts, IEEE Netw. 8 (1994) 22–32.
[35] B. Schilit, N. Adams, R. Want, Context-aware computing applications, in: Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, Santa Cruz, CA, 1994, pp. 85–90.
[36] B. Brumitt, S. Shafer, Topological world modeling using semantic spaces, in: Proceedings of Workshop on Location Modeling for Ubiquitous Computing, Atlanta, GA, 2001, pp. 55–62.
[37] M. Baldauf, S. Dustdar, F. Rosenberg, A survey on context-aware systems, Int. J. Ad Hoc Ubiquitous Comput. 2 (4) (2007) 263–277.
[38] P. Oreizy, M. Gorlick, R. Taylor, D. Heimbigner, G. Johnson, N. Medvidovic, A. Quilici, D. Rosenblum, A. Wolf, An architecture-based approach to self-adaptive software, IEEE Intell. Syst. 14 (1999) 54–62.
[39] J. Coutaz, C. J, S. Dobson, D. Garlan, Context is key, Commun. ACM 48 (2005) 49–53.
[40] A. Krause, A. Smailagic, D.P. Siewiorek, Context-aware mobile computing: learning context dependent personal preferences from wearable sensor array, IEEE Trans. Mob. Comput. 5 (2006) 113–127.
[41] A.K. Clear, R. Shannon, T. Holland, A. Quigley, S. Dobson, P.Nixon, SITUVIS: a visual tool for modelling a users behavior patterns in a pervasive environment, in: Proceedings of the Seventh International Conference on Pervasive Computing, Nara, Japan, 2009, pp. 327–341.
[42] S. Loke, Representing and reasoning with situations for context-aware pervasive computing:a logic programming perspective, The Knowl. Eng. Rev. 19 (2004) 213–233.
[43] V. Andrikopoulos, S. Benbernou, M.P. Papazoglou, Managing the evolution of service specifications, in: Proceedings of 20th International Conference on the Advanced Information Systems Engineering, CAiSE 2008, Montpellier, France, 2008, pp. 359–374.
[44] M.P. Papazoglou, W. van den Heuvel, Service oriented architectures: approaches, technologies and research issues, VLDB J. 16 (2007) 389–415.
[45] M. Papazoglou, Foresight & research priorities for service oriented computing, in: Proceedings of the 11th International Conference on Enterprise Information Systems, Milan, Italy, 2009, pp. 5–6.
[46] T. Yu, M. Winslett, A unified scheme for resource protection in automated trust negotiation, in: Proceedings of IEEE International Symposium Security and Privacy, Colorado Springs, 2003, pp. 110–122.
[47] Perci (pervasive service interaction). <http://www.hcilab.org/projects/perci/index.html>.
[48] W. Ye, J. Heidemann, D. Estrin, An energy-efficient MAC protocol for wireless sensor networks, in: Proceedings of IEEE INFOCOM, vol. 3, 2002, pp. 1567–1576.
[49] J. Polastre, J. Hill, D. Culler, Versatile low power media access for wireless sensor networks, in: Proceedings of ACM SenSys, Baltimore, MD, USA, 2004, pp. 95–107.
[50] G. Lu, B. Krishnamachari, C. Raghavendra, An adaptive energy-efficient and low-latency MAC for data gathering in sensor networks, in: Proceedings of International Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (WMAN), Santa Fe, NM, 2004, p. 224.
[51] C. Enz, A. El-Hoiydi, J.-D. Decotignie, V. Peiris, WiseNET: an ultralow-power wireless sensor network solution, IEEE Comput. 37 (8) (2004) 62–70.
[52] C. Schurgers, V. Tsiatsis, S. Ganeriwal, M. Srivastava, Optimizing sensor networks in the energy-latency-density design space, IEEE Trans. Mob. Comput. 1 (1) (2002) 70–80.
[53] G. Merrett, N. White, N. Harris, B. Al-Hashimi, Energy-aware simulation for wireless sensor networks, in: Proceedings of IEEE SECON, Rome, Italy, 2009, pp. 64–71.
[54] A. Kansal, J. Hsu, S. Zahedi, M.B. Srivastava, Power management in energy harvesting sensor networks, ACM Trans. Embed. Comput. Syst. 6 (4) (2007) 32.
[55] A. Giridhar, P.R. Kumar, Computing and communicating functions over sensor networks, IEEE JSAC 23 (4) (2005) 755–764.
[56] P. Gupta, P.R. Kumar, The capacity of wireless networks, IEEE Trans. Inform. Theory 46 (2) (2000) 388–404.
[57] A.R.I. Schizas, G.B. Giannakis, Distributed estimation with ad hoc wireless sensor networks, in: Proceedings of EURASIP EUSIPCO, Florence, 2006.
[58] D.S. Scherber, H. Papadopoulos, Distributed computing of averages over ad-hoc networks, IEEE JSAC 23 (4) (2005) 755–764.
[59] S. Barbarossa, G. Scutari, A. Swami, Distributed detection and estimation in decentralized sensor networks: and overview, in: Proceedings of EURASIP EUSIPCO, Florence, 2006.
[60] M.Z.H.Y.E. Bottega, P. Popowsky, R. Prasad, Hypothesis testing over a random access channel in wireless sensor networks, in: Proceedings of EURASIP EUSIPCO, Florence, Italy, 2006.
[61] G. Mergen, L. Tong, Type based estimation over multiaccess channels, IEEE Trans. Signal Process. 54 (2) (2006) 613–626.
[62] R. Gallagher, Finding parity in a simple broadcast network, IEEE Trans. Inform. Theory 34 (2) (1988) 176–179.
[63] E. Kushilevitz, Y. Mansour, Computation in noisy radio networks, in: Proceedings of ACM-SIAM Symposium on Discrete Algorithms, San Francisco, USA, 1998, pp. 236–243.
[64] A. Giridhar, P.R. Kumar, Towards a theory of in-network computation in wireless sensor networks, IEEE Commun. Mag. 44 (4) (2006) 98–107.
[65] B. Warneke, M. Last, B. Liebowitz, K.S.J. Pister, Smart dust: communicating with a cubic-millimeter computer, Computer 34 (1) (2001) 44–51.
[66] A. Harter, A. Hopper, A distributed location system for the active office, IEEE Netw. 8 (1) (1994) 62–70.
[67] G.D. Abowd, C.G. Atkeson, J. Hong, S. Long, R. Kooper, M. Pinkerton, Cyberguide: a mobile context-aware tour guide, Wireless Netw. 3 (1997) 421–433.
[68] P. Vicaire, T. He, T. Yan, Q. Cao, G. Zhou, L. Gu, L. Luo, R. Stoleru, J.A. Stankovic, T. Abdelzaher, Achieving long-term surveillance in vigilne, ACM Trans. Sens. Netw. 5 (2009) 1–39.
[69] D. Moore, J. Leonard, D. Rus, S. Teller, Robust distributed network localization with noisy range measurements, in: Proceedings of SenSys '04, Baltimore, USA, 2004, pp. 50–61.
[70] S. Ray, R. Ungrangsi, F.D. Pellegrini, A. Trachtenberg, D. Starobinski, Robust location detection in emergency sensor networks, in: Proceedings of INFOCOM, S. Francisco, CA, 2003, pp. 1044–1053.
[71] S. Gezici, Z. Tian, G.B. Giannakis, H. Kobayashi, A.F. Molisch, H.V. Poor, Z. Sahinoglu, Localization via ultra-wideband radios, IEEE Signal Process. Mag. 22 (2005) 70–84.
[72] C. Decker et al., Cost–benefit model for smart items in the supply chain, in: Proceedings of IOT Conference, Zurich, Switzerland, 2008, pp. 155–172.
[73] C. Bornhövd, T. Lin, S. Haller, J. Schaper, Integrating automatic data acquisition with business processes experiences with sap's auto-id infrastructure, in: VLDB '04: Proceedings of the Thirtieth International Conference on Very Large Data Bases, VLDB Endowment, 2004, pp. 1182–1188.
[74] A.S. Tanenbaum, M.V. Steen, Distributed Systems: Principles and Paradigms, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2001.
[75] J.N. Tsitsiklis, Problems in decentralized decision making and computation, Ph.D. thesis, Massachusetts Institute of Technology, 1984.
[76] M. Jelasity, A. Montresor, O. Babaoglu, Gossip-based aggregation in large dynamic networks, ACM Trans. Comput. Syst. 23 (1) (2005) 219–252.
[77] D. Kempe, A. Dobra, J. Gehrke, Gossip-based computation of aggregate information, in: Proceedings of FOCS, IEEE, Cambridge, MA, USA, 2003, pp. 482–491.
[78] J. Garay, Y. Moses, Fully polynomial byzantine agreement for $n > 3t$ processors in $t + 1$ rounds, SIAM J. Comput. 27 (1) (1998) 247–290.
[79] D. Spanos, R. Olfati-Saber, R.M. Murray, Distributed sensor fusion using dynamic consensus, in: Proceedings of IFAC'05, Prague, 2005, p. 99.
[80] L. Xiao, S. Boyd, S. Lall, A scheme for asynchronous distributed sensor fusion based on average consensus, in: Proceedings of IPSN'05, Los Angeles, USA, 2005, p. 99.
[81] T.H. Cormen, C.E. Leiserson, R.L. Rivest, C. Stein, Introduction to Algorithms, MIT Press, 2001.
[82] R.C. Shah, S. Roy, S. Jain, W. Brunette, Data mules: modeling a three-tier architecture for sparse sensor networks, in: Proceedings of IEEE International Workshop on Sensor Networks Protocols and Applications, 2003, pp. 30–41.
[83] F. De Pellegrini, C. Moiso, D. Miorandi, I. Chlamtac, R-P2P: a data centric dtn middleware with interconnected throwboxes, in: Proceedings of Autonomics, Turin, Italy, 2008, pp. 11–20.
[84] I. Carreras, I. Chlamtac, F. De Pellegrini, D. Miorandi, BIONETS: bio-inspired networking for pervasive communication environments, IEEE Trans. Veh. Technol. 56 (1) (2007) 218–229.

[85] J. Padhye, V. Firoiu, D. Towsley, J. Kurose, Modeling TCP throughput: a simple model and its empirical validation, in: Proceedings of ACM SIGCOMM, Vancouver, CA, 1998, pp. 303–314.
[86] I. Koren, C.M. Krishna, Fault Tolerant Systems, Morgan Kaufman Publishers Inc., San Francisco, CA, USA, 2007.
[87] R.S. Leslie Lamport, M. Pease, The byzantine generals problem, ACM Trans. Program. Lang. Syst. 4 (3) (1982) 382–401.
[88] S. Dolev, Self-stabilization, MIT Press, Cambridge, MA, USA, 2000.
[89] W. Masri, Z. Mammeri, Middleware for wireless sensor networks: a comparative analysis, in: Proceedings of IFIP International Network and Parallel Computing Workshops (NPC), China, 2007, pp. 349–356.
[90] J. Charles, Middleware moves to the forefront, Computer 32 (5) (1999) 17–19.
[91] N. Ibrahim, Orthogonal classification of middleware technologies, in: Proceedings of UBICOMM '09, Sliema, Malta, 2009, pp. 46–51.
[92] Object Naming Service (ONS) Standard. <http://www.epcglobalinc.org/standards/ons/ons101-standard-20080529.pdf>.
[93] G. Weiss, Multiagent Systems. A Modern Approach to Distributed Modern Approach to Artificial Intelligence, MIT Press, Cambridge, MA, USA, 1999.
[94] T.W. Sandholm, V.R. Lesser, Coalitions among computationally bounded agents, Artif. Intell. 1 (94) (1997) 99–137.
[95] D. Fudenberg, J. Tirole, Game Theory, MIT Press, 1991.
[96] D. Estrin, D. Culler, K. Pister, G. Sukhatme, Connecting the physical world with pervasive networks, IEEE Pervasive Comput. 1 (1) (2002) 59–69.
[97] W. Weber, J. Rabaaey, E. Aarts (Eds.), Ambient Intelligence, Springer-Verlag, Berlin, 2005.
[98] E. Zelkha, B. Epstein, From devices to ambient intelligence, in: Digital Living Room Conference, Laguna Niguel, California, 1998.
[99] M. Berger, F. Fuchs, M. Pirker, Ambient intelligence – from personal assistance to intelligent megacities, in: Proceedings of Conference on Advances in Ambient Intelligence, 2007, pp. 21–35.
[100] M. Kranz, P. Holleis, A. Schmidt, Embedded interaction: interacting with the internet of things, IEEE Internet Comput. 14 (2010) 46–53.
[101] R. Sandhu, E. Coyne, H. Feinstein, C. Youman, Role-based access control models, IEEE Comput. 29 (2) (1996) 38–47.
[102] S. Papadopoulos, Y. Yang, D. Papadias, CADS: continuous authentication on data streams, in: Proceedings of the 33rd International Conference on Very Large Data Base (VLDB'07), Morgan Kaufmann Publishers Inc., Vienna, Austria, 2007, pp. 135–146.
[103] M. Ali, M. ElTabakh, C. Nita-Rotaru, Ft-Rc4: A Robust Security Mechanism for Data Stream Systems, Purdue University, Technical Report, TR-05-024.
[104] W. Lindner, J. Meier, Securing the borealis data stream engine, in: Proceedings of the International Database Engineering and Application Symposium (IDEAS'06), Delhi, India, 2006, pp. 137–147.
[105] R. Nehme, E. Rundesteiner, E. Bertino, A security punctuation framework for enforcing access control on streaming data, in: Proceedings of the 24th International Conference on Data Engineering (ICDE'08), Cancun, Mexico, 2008, pp. 406–415.
[106] M. Hammad, M. Franklin, W. Aref, A. Elmagarmid, Scheduling the shared window joins over data streams, in: Proceedings of the 29th International Conference on Very Large Data Base (VLDB'03), Morgan Kaufman Publishers Inc., Berlin, Germany, 2003, pp. 297–308.
[107] B. Carminati, E. Ferrari, K. Tan, J. Cao, A framework to enforce access control over data streams, ACM Trans. Inform. Syst. Sec. (TISSEC) 13 (3) (2008) 1–31.
[108] B. Carminati, E. Ferrari, K. Tan, Enforcing access control policies on data streams, in: Proceedings of the 12th ACM Symposium on Access Control Models and Technologies (SACMAT'07), Sophia Antipolis, France, 2007, pp. 21–30.
[109] B. Carminati, E. Ferrari, K. Tan, Specifying access control policies on data streams, in: Proceedings of the 12th International Conference on Database System for Advanced Applications, Lecture Notes in Computer Science, Springer, Bangkok, Thailand, 2007, pp. 410–421.
[110] L. Hu, D. Evans, Secure data aggregation in wireless sensor networks, in: Proceedings of IEEE WSAAN, Orlando, Florida, USA, 2003, pp. 93–105.
[111] A. Mahimkar, T. Rappaport, SECUREDAV: a secure data aggregation and verification protocol for sensor networks, in: Proceedings of IEEE Globecom, Dallas, Texas, USA, 2004, pp. 2175–2179.
[112] B. Przydatek, D. Song, A. Perrig, SIA: secure information aggregation in sensor networks, in: Proceedings of ACM SenSys, Los Angeles, California, USA, 2003, pp. 255–265.
[113] M. Bagaa, N. Lasla, A. Ouadjaout, Y. Challal, SEDAN: secure and efficient protocol for data aggregation in wireless sensor networks, in: Proceedings of IEEE LCN, Dublin, Ireland, 2007, pp. 1053–1060.
[114] C. Castelluccia, E. Mykletun, G. Tsudik, Efficient aggregation of encrypted data in wireless sensor networks, in: Proceedings of MobiQuitous, San Diego, CA, USA, 2005, pp. 109–117.
[115] J. Girao, D. Westhoff, M. Schneider, CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks, in: Proceedings of IEEE ICC, Seoul, Korea, 2005, pp. 3044–3049.
[116] R. Riggio, S. Sicari, Secure aggregation in hybrid mesh/sensor networks, in: Proceedings of SASN, Saint Petersburg, Russia, 2009, pp. 1–6.
[117] A. Coen-Porisini, S. Sicari, SeDAP: Secure data aggregation protocol in privacy aware wireless sensor networks, in: Springer Proceedings of the 2nd International Conference on Sensor Systems and Software, Miami, Florida, USA, 2010.
[118] E. Mykletun, J. Girao, D. Westhoff, Public key based cryptoschemes for data concealment in wireless sensor networks, in: Proceedings of IEEE ICC, Istanbul, Turkey, 2006, pp. 2288–2295.
[119] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, in: Proceedings of ACM CCS, Washington, DC, USA, 2002, pp. 41–47.
[120] R.D. Pietro, A. Mei, L.V. Mancini, Random key assignment for secure wireless sensor networks, in: Proceedings of ACM SASN, Fairfax, VA, USA, 2003, pp. 62–71.
[121] R.D. Pietro, C. Soriente, A. Spognardi, G. Tsudik, Collaborative authentication in unattended WSNs, in: Proceedings of ACN WiSec, Zurich, Switzerland, 2009, pp. 237–244.
[122] T. Mielikinen, Privacy problems with anonymized transaction databases, in: Proceedings of international Conference on Discovery Science (DS 2004), Lecture Notes in Computer Science, vol. 3245, Springer, 2004.
[123] A. Narayanan, V. Shmatikov, Obfuscated databases and group privacy, in: Proceedings of ACM International Conference on Computer and Communications Security (CCS), ACM Press, New York, USA, 2005, pp. 102–111.
[124] P. Samarati, L. Sweeney, Protecting privacy when disclosing information: *k*-anonymity and its enforcement through generalization and suppression, Technical Report SRI-CSL-98-04, Computer Science Laboratory, SRI International.
[125] A. Bhargavspantzel, A. Squicciarini, E. Bertino, Trust negotiation in identity management, IEEE Secur. Priv. (2007) 55–63.
[126] A.V. Lamsweerde, E. Handling, Obstacles in goal-oriented requirement engineering, IEEE Trans. Softw. Eng. 26 (2000) 978–1005.
[127] L. Liu, E. Yu, J. Mylopoulos, Analyzing security requirements as relationships among strategic actors, in: Proceedings of International Symposium on Requirements Engineering for Information Security (SREIS), Raleigh, North Carolina, USA, 2002.
[128] H. Mouratidis, P. Giorgini, G.A. Mason, Integrating security and systems engineering: towards the modelling of secure information system, in: Proceedings of International Conference on Advanced Information System Engineering (CAiSE), Lecture Notes in Computer Science, vol. 2681, Springer, 2003, pp. 63–78.
[129] L. Chung, Dealing with security requirements during the development of information system, in: Proceedings of International Conference on Advanced Information System Engineering (CAiSE), vol. Klagenfurt/Velden, Austria, Lecture Notes in Computer Science, Springer, Paris, France, 1993, pp. 234–251.
[130] J. Mylopolulos, L. Chung, B. Nixon, Representing and using non functional requirements: a process oriented approach, IEEE Trans. Softw. Eng. 18 (1998) 483–497.
[131] A. Anton, Goal-based requirements analysis, in: Proceedings of IEEE International Conference on Requirements Engineering (ICRE 96), Colorado Springs, 1996, pp. 136–144.
[132] E. Kavakli, C. Kalloniatis, P. Loucopoulos, S. Gritzalis, Addressing privacy requirements in system design: the pris method, J. Requirements Eng. 13 (3) (2008) 241–255.
[133] A. Coen-Porisini, P. Colombo, S. Sicari, Privacy aware systems: from models to patterns, in: Software Engineering for Secure Systems: Industrial and Research Perspectives, IGI Global, 2010.
[134] M. Blaze, J. Feigenbaum, J. Lacy, Decentralized trust management, in: Proceedings of IEEE International Symposium Security and Privacy, Colorado Springs, 1996, pp. 164–173.
[135] K. Ren, T. Li, Z. Wan, F. Bao, R. Deng, K. Kim, Highly realible trust establishment scheme in ad hoc networks, Comput. Netw. 45 (6) (2004) 687–699.

[136] Z. Liang, W. Shi, Enforcing cooperative resource sharing in untrusted peer to peer environment, ACM J. Mobile Netw. Appl. 10 (6) (2005) 771–783.
[137] Y.-B. Lin, I. Chlamtac, Wireless and Mobile Network Architectures, John Wiley & Sons, Inc., New York, NY, USA, 2000.

Daniele Miorandi is the head of the iNSPIRE Area at CREATE-NET, Italy. He received a PhD in Communications Engineering from Univ. of Padova, Italy, in 2005, and a Laurea degree (summa cum lauda) in Communications Engineering from Univ. of Padova, Italy, in 2001. He joined CREATE-NET in Jan. 2005, where he is leading the iNSPIRE (Networking and Security Solutions for Pervasive Computing Systems: Research & Experimentation). His research interests include bio-inspired approaches to networking and service provisioning in large-scale computing systems, modeling and performance evaluation of wireless networks, prototyping of wireless mesh solutions. Dr. Miorandi has co-authored more than 100 papers in internationally refereed journals and conferences. He serves on the Steering Committee of various international events (WiOpt, Autonomics, ValueTools), for some of which he was a co-founder (Autonomics and ValueTools). He also serves on the TPC of leading conferences in the networking field, including, e.g., IEEE INFOCOM, IEEE ICC, IEEE Globecom. He is a member of IEEE, ACM and ICST.

Sabrina Sicari was born on September 18, 1977 in Catania, Sicily, Italy. She received her laurea degree in Electronical Engineering,110/110 cum laude, from University of Catania, Catania, Italy, in 2002. In March 2006 she got her Ph.D. in Computer and Telecommunications Engineering at the same university. From September 2004 to March 2006 she has been a Visiting Scholar at Dipartimento di Elettronica e Informatica, Politecnico di Milano, Italy. Since May 2006 she works at Dipartimento di Informatica e Comunicazione, Universit degli Studi dell'Insubria in software engineering group (head Prof. Alberto Coen-Porisini). Dr. Sicari is an IEEE member. She is reviewer of Pervasive and Mobile Computing (Elsevier), IEEE Transactions on Vehicular Technology, ACM-Monet, International Journal of Computer Applications in Technology (IJCAT), IEEE ICC'09, IEEE ICC'10, IEEE ISIE'10, S-Cube'09, WiOpt'09, Mobility'11, ICDT 2012,and TPC member of Q2SWinet 2011, Q2SWinet 2010, Q2SWinet 2009, IEEE Globecom'11, IEEE Globecom'10, IEEE ICC'11, GIIS'11, IWCMC '11, the international workshop SESENA 2010 (co-located with ICSE'10), S-cube'10. Dr. Sicari has been the general co-chair of S-Cube 2009. She has been a Steering Committee member of S-Cube 2010 and guest editor for the ACM Monet Special Issue, named "Sensor, system and Software". Dr. Sicari is an Editor for Computer Networks (Elsevier) journal since 2008. She is a Steering Commitee member of S-Cube 2012. She is a TPC member of the international conference IWCMC 2012, SENSORNETS 2012, S-Cube 2012, ICDT 2012, Mobility 2012, SNDS 2012, Q2SWinet 2012

Francesco De Pellegrini received the Laurea degree in 2000 and the Ph.D. degree in 2004, both in Telecommunication Engineering, from the University of Padova. During year 2001/2002 he spent one year at Boston University as a visiting scholar. He is currently a senior researcher and Deputy Area Head of the iNspire group at CREATE-NET. His research interests are location detection, multirate systems, routing, wireless mesh networks, VoIP, Ad Hoc and Delay Tolerant Networks. F. De Pellegrini has been a TPC member of IEEE Infocom and a reviewer for several international networking conferences and journals. Francesco serves in the Steering Programm Commitee of Mobiquitous and Complex Conferences. Francesco was the Vice-chair for the first edition of Robocomm.

Imrich Chlamtac is the President of CREATE-NET and the Bruno Kessler Professor at the University of Trento, Italy and has held various honorary and chaired professorships in USA and Europe including the Distinguished Chair in Telecommunications Professorship at the University of Texas at Dallas, Sackler Professorship at Tel Aviv University and University Professorship at the Tech- nical University of Budapest. In the past he was with Technion and UMass, Amherst, DEC Research. Dr. Imrich Chlamtac has made significant contribution to various networking technologies as scientist, educator and entrepreneur. Dr. Chlamtac is the recipient of multiple awards and recognitions including Fellow of the IEEE, Fellow of the ACM, Fulbright Scholar, the ACM Award for Outstanding Contributions to Research on Mobility and the IEEE Award for Outstanding Technical Contributions to Wireless Personal Communications. Dr. Chlamtac published close to four hundred refereed journal, book, and conference articles and is listed among ISIs Highly Cited Researchers in Computer Science. Dr. Chlamtac is the co-author of four books, including the first book on Local Area Networks (1980) and the Amazon.com best seller and IEEE Editor's Choice Wireless and Mobile Network Architectures, published by John Wiley and Sons (2000). Dr. Chlamtac has widely contributed to the scientific community as founder and Chair of ACM Sigmobile, founder and steering committee chair of some of the lead conferences in net-working, including ACM Mobicom, IEEE/SPIE/ACM OptiComm, CreateNet Mobiquitous, CreateNet WiOpt, IEEE/CreateNet Broadnet, IEEE/CreateNet Tridentcom and IEEE/CreateNet Securecomm conferences. Dr. Chlamtac also serves as the founding Editor in Chief of the ACM/URSI/Springer Wireless Networks (WINET), the ACM/Springer Journal on Special Topics in Mobile Networks and Applications (MONET).