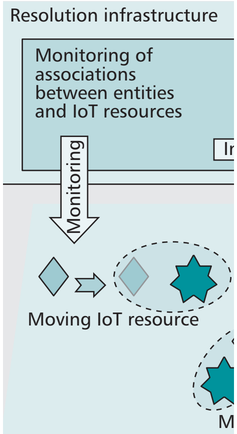
THE INTERNET OF THINGS

FROM TODAY'S INTRANET OF THINGS TO A FUTURE INTERNET OF THINGS: A WIRELESS- AND MOBILITY-RELATED VIEW

MICHELE ZORZI, UNIVERSITY OF PADOVA
ALEXANDER GLUHAK, UNIVERSITY OF SURREY
SEBASTIAN LANGE, VDI/VDE INNOVATION + TECHNIK GMBH
ALESSANDRO BASSI, HITACHI EUROPE, LTD.


Resolution infrastructure
Monitoring of associations between entities and IoT resources
Ir
Monitoring
Moving IoT resource
M

The authors present the current status of the Internet of Things, and discuss how the current situation of many "Intranets" of Things should evolve into a much more integrated and heterogeneous system.

ABSTRACT

In this article, we present the current status of the Internet of Things, and discuss how the current situation of many "Intranets" of Things should evolve into a much more integrated and heterogeneous system. We also summarize what in our opinion are the main wireless- and mobility-related technical challenges that lie ahead, and outline some initial ideas on how such challenges can be addressed in order to facilitate the IoT's development and acceptance in the next few years. We also describe a case study on the IoT protocol architecture.

INTRODUCTION

The Internet of Things (IoT) arena as of today resembles the "Wild West" of a couple of centuries ago. It is a vast, mostly unexplored territory, without clear borders, where all current technologies can play a role, and where ad hoc solutions are often the norm. Governance is very limited and contradictory, and attacks, both from consumer associations scared of a "big brother like" control and from business executives scared of new and radically different business models, can seriously hamper its development.

But, as the Wild West, the mirage of the seemingly unlimited capabilities offered by the "web of things" is driving more and more research and development solutions in this area. IoT is seen as a pillar of the Future Internet [1], and recent advances in battery life, miniaturization, energy harvesting, transmission protocols, and hardware costs are bringing its vision closer and closer to reality.

The IoT vision [2, 3] of pervasively connecting smart things will provide a unique chance to enable a rich set of evolutionary as well as revolutionary applications and services (see [4] for some interesting examples). For the first time it will be possible to interact with the environment around us, and to receive information on its status that was previously not available by simply looking at things. Moreover, it will be possible not only to actively interconnect things in the physical world, but also to enable them to exchange and make use of their information (in the "digital" world).

Given the current fragmentation of efforts in this area, which prevents a synergistic integration process, we believe that there is a clear need to develop a reference architectural model that will allow interoperability between different systems. The TCP/IP protocol suite, by now universally used in the Internet, emerged from a pool of many different protocols rather than "being created" following a clean-slate approach. Similarly, instead of designing "the" IoT from scratch, we believe that a better approach will be to integrate existing efforts and current technologies into a unified, ubiquitously applicable architecture, to design open and flexible interfaces and, where missing, to develop the necessary bridges to connect different technologies from the hardware to the service layer. We firmly believe that only such a foundational work will jump start the Internet of Things era, whose impact on our lives can be expected to be even more dramatic than what the Internet has brought about.

With respect to the technological roadblocks (the focus of this article), we see an immediate need for action in three different areas:

1. An architectural reference model for the interoperability of IoT systems, outlining principles and guidelines for the design of its protocols, interfaces, and algorithms
2. Mechanisms for the efficient integration of this architecture into the service layer of the Future Internet networking infrastructure
3. A Novel resolution infrastructure, allowing scalable lookup and discovery of IoT resources, entities of the real world, and their associations

1536-1284/10/$25.00 © 2010 IEEE

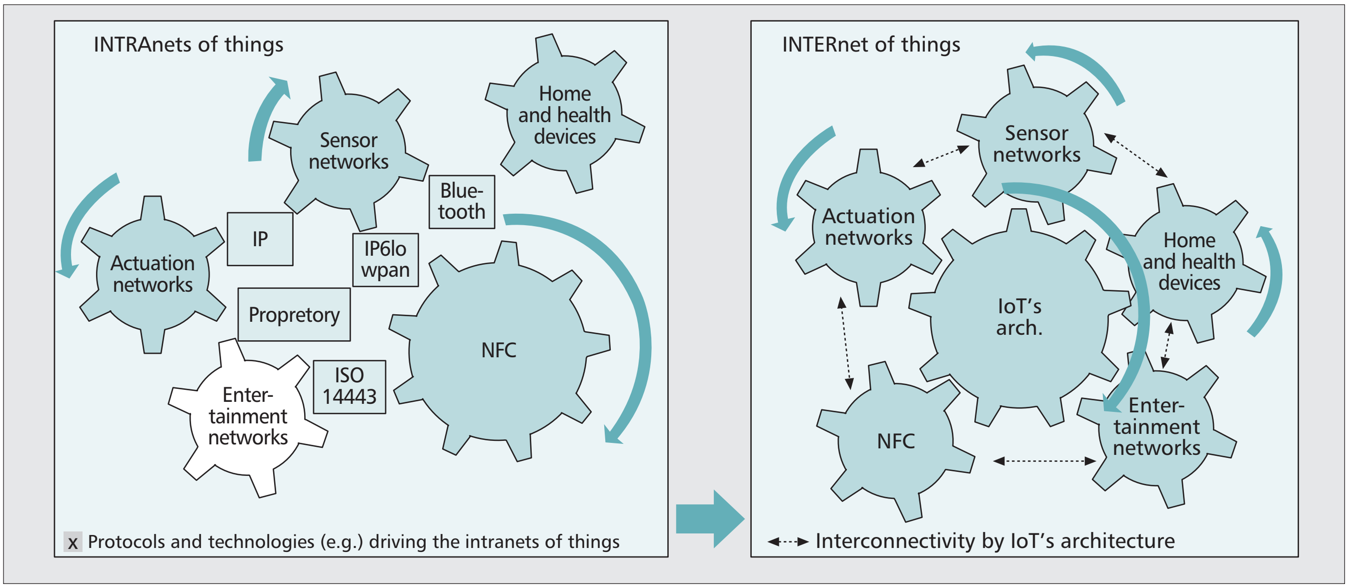


Figure 1. *From the current "Intranets of Things" to the "Internet of Things."*

This architectural framework will make it possible to overcome the current fragmentation and limitation of solutions, where many "Intranets" of Things exist, towards a true "Internet" of Things, where all devices will be part of a globally integrated system. (A pictorial view of this concept is provided in Fig. 1.) In this article, we will discuss some of the main technical challenges related to wireless communications and mobility in an IoT context, and outline some initial ideas towards possible solutions.

Related Work

The term "Internet of Things" was coined more than 10 years ago by the Auto-Id Labs in the US (http://www.autoidlabs.org/), where in parallel the concepts of "ambient intelligence" and "ubiquitous computing" were also being developed. Since then, there have been some considerable developments, in both academia and industry, in the US as well as in Europe and Asia. Such developments have primarily been dedicated to applying RFID technology to the logistics value chain [5]. Beyond this, sensor networks have been applied in numerous industrial environments for process monitoring [6]. The first trials to establish IoT-like applications for end users in public have been set up in so called "future stores" in Germany, Switzerland and Japan. Despite these early efforts, some of the more visionary aspects of the IoT concept have only been studied in laboratory scale use cases, and many more are still waiting to be developed and invented.

The Internet of Things theme can be seen as a concept originating from converging topics that find their origin in a number of different research streams [2]. Its cornerstone is undoubtedly the RFID technology. Radio Frequency Identifiers (RFIDs) were first introduced to overcome the limitations of the barcode technology and primarily focus on tagging objects by attaching an individual identifier to them [7]. While the original idea was to tag items for retail and logistics, it is foreseen that the application of RFID tags to any object around us will open up the possibility to develop a huge number of disruptive services. Although some privacy concerns have been raised, RFIDs have become part of our everyday life. Despite the recent improvements in RFID technology (e.g., in terms of miniaturization), further developments need to be realized, especially in the areas of energy harvesting and batteries, integration into materials, and cost. Furthermore, integration of RFIDs in other devices such as mobile phones and sensors, which is seen as a major step towards the development of IoT, is not yet widespread.

With respect to numbering and identification issues, organizations such as EPC Global (www.epcglobalinc.org), the IP for Smart Objects Alliance (www.ipso-alliance.org) and the Ubiquitous ID Center (www.uidcenter.org) currently aim at promoting standards, in order to make RFID interoperable and ubiquitously applicable. While these efforts are certainly important and worthwhile, there are some concerns about their impact on how the field will evolve and their vulnerability to possibly unfair practices [8].

Sensor networks, that are considered another pillar of the IoT, experienced a similar development in the recent past. A lot of research has been done in the last couple of decades, not only in the area of networking protocols, including MAC and routing, but also in micro and nano technologies, as well as on higher-layer issues, such as middleware, security and applications [9]. In particular, technological advances allow to have extremely sensitive, extremely precise, and extremely small sensors, combining different sensing techniques to minimize reading errors and calibration issues. Sensor networks and RFID research are slowly growing together [10] as sensor nodes are becoming smaller and more highly integrated and RFID tags are equipped with more computing power and storage capacity than required by just an identification code. In the future we may expect that smart functional

One of the key requirements for the IoT paradigm to be successful is its ability to integrate many types of devices, technologies, and services. At the device level, this includes very diverse features.

components such as tags and sensors will be inherently integrated into the environment, so that their presence will be pervasive but invisible.

In the wireless communication area, it is possible to identify several parallel developments. Efforts such as ZigBee, Bluetooth, Wi-Fi, NFC, all with their own specific characteristics and application domains, have reached a significant maturity and market size. However, the fragmentation of these protocols may again hamper objects interoperability and can slow down the development of a unified reference model for the IoT.

Today, while single applications are getting more and more common, the necessity of a unified approach for the IoT is still a topic promoted and developed by a fairly small group of enthusiasts from academia, industry and public institutions. In order to promote IoT as a publicly accepted and implemented paradigm, and to guarantee a sustainable development of the related technologies and products, standardization will be crucial as it will guarantee that the unavoidable evolution towards smart communicating objects will lead to a unified and integrated system of heterogeneous devices (the "Internet" of Things), as opposed to separate vertical "silos" solutions which, though possibly highly optimized, cannot have a global scope (the "intranets" of things). Some initial effort in this area has been made, notably within ETSI [11]; however, in order to achieve the necessary scale, different areas (such as for example naming resolution and the definition of common interfaces for different device technologies) need to undergo a substantial standardization effort as well.

The key challenge in the years to come will therefore involve both significant conceptual innovation to solve the many open problems and an effort to bring these concepts to real-life systems and applications.

Key Technical Issues

Given the complexity of the IoT paradigm, the list of challenges to be addressed is potentially very long. In the paragraphs below we will concentrate on the major technical roadblocks related to wireless communication and mobility. A discussion on more general issues can be found in [2].

Heterogeneity

One of the key requirements for the IoT paradigm to be successful is its ability to integrate many types of devices, technologies, and services. At the device level, this includes very diverse features in terms of data communication capabilities (e.g., data-rates and/or reliability), computational and storage power, availability of energy, flexibility in handling different technologies, mobility, etc. As to services, the system should ideally be open to supporting a huge variety of different applications whose characteristics and requirements may be extremely diverse, in terms of bandwidth, latency, reliability, etc. These heterogeneity traits of the overall system make the design of a unifying framework and of the communication protocols a very challenging task, especially with reference to wireless communications devices with vastly different levels of capabilities and performance, and will involve an inevitable performance degradation compared to a highly optimized vertical design.

Connectivity

Another key area of investigation relates to how to provide communications capabilities to the various devices involved, that in many cases will be wireless. Issues such as communications energy consumption, antenna design, interoperability of different technologies (e.g., via cognitive radio capabilities), adaptive techniques for a dynamic environment in the face of possibly heavily constrained resources, etc. will have to be addressed. It will be important to understand what needs to be connected so as to provide the necessary communications capabilities, while avoiding that a system that is too connected becomes hard to manage (e.g., due to excessive interference). In a more futuristic scenario, alternative means of communications may also be considered, including for example communications through organic matter.

Scale

If all things need to be part of this system, another major challenge is related to the sheer numbers involved. It is well known that in the presence of many nodes, which cannot be a priori expected to be tightly coordinated, the performance of most communications schemes will suffer, assuming they can work at all. In a wireless context, such problems are further exacerbated, e.g., due to the difficulty of having a coherent and stable view of the topology because of the channel- and mobility-related dynamics, as well as the inherent unreliability of the medium, which in dense multi-hop environments may become a serious bottleneck. Communications protocols will therefore pose several challenges. Management of the network becomes very difficult in a large distributed environment, and solutions to dominate the complexity need to be found. Despite the huge literature on these topics, such extreme situations have not been adequately studied, and the behavior of the overall system in terms of data handling performance, stability, fairness, reliability, etc. will need to be revisited. The challenges related to other aspects (e.g., heterogeneity or addressing) will also be exacerbated by the very large number of devices involved.

Naming, Addressing and Identification

Identifying an object is one of the primary pillars of the IoT. A key problem is how to split Location and Identification of a device. Although workarounds exist for IPv4, and some mechanisms were introduced in IPv6 to support Internet mobility, the heterogeneity of existing identification mechanisms and their co-existence and efficient use across different systems make this problem wider and more complex to solve for RFIDs. While the RFID world has been initially dominated by the use of EPC for identification, uID [12] has recently gained popularity as a more flexible alternative. Future identification schemes will have to embrace various entities of the real world such as places or living beings, making the world-wide convergence to a single scheme highly unlikely (not to mention the political considerations concerning governance). Suitable solutions therefore must be able to inter-relate heterogeneous schemes, considering also heterogeneous location/ID splitting techniques, across different system boundaries.

PRIVACY & SECURITY

One major social concern related to pervasive systems that have learning and reasoning capabilities and can collect and store data about the environment is the way such data may be used (or abused). In addition, in applications where the system is called to act on the physical reality, tampering with the system by a malicious intruder may result in severe consequences in terms of performance, operational disruption, theft, or even safety hazards. In a wireless IoT context, besides the obvious weakness of the radio channel with regard to eavesdropping, the heavily constrained nature of the devices and the limited bandwidth available make it very challenging to provide effective security mechanisms via simple algorithms with limited room for message exchanges. We observe that these privacy and security issues are not unique to this environment but need to be addressed in a variety of systems, so that some concepts that already exist or are being developed in different contexts can likely be reused.

SELF-MANAGEMENT CAPABILITIES

In order to support the expected scale of the IoT, devices will need to self-manage without external intervention. Orchestration and management mechanisms as well as information models will have to be defined taking into account this scale of deployment. The success of the Internet lies in its minimalistic best-effort service approach. When trying to apply a similarly simple approach to the IoT architecture, we have to face the exponential growth in complexity that the connection of billions of heterogeneous devices will bring, which will call for context awareness, self-organization, self-management, self-optimization, self-healing and self-protection capabilities. In a wireless context, the increased topology dynamics and likelihood of faults due to channel fluctuations and possible device mobility, as well as the loss of signaling and control messages, make these issues all the more challenging and call for schemes where robustness may be more important than efficiency.

ENERGY MANAGEMENT

Energy in all its phases (harvesting, conservation and consumption) is a major issue, not only in the IoT area, but more in general for the society at large. The development of novel solutions that maximize energy efficiency is paramount. In this respect, current technology is inadequate, and existing processing power and energy capacity are too low to cope with future needs. The development of new and more efficient and compact energy storage sources such as batteries, fuel cells, and printed/polymer batteries, together with new energy generation devices coupling energy transmission methods or energy harvesting using energy conversion, as well as extremely low-power circuitry and energy efficient architectures and protocol suites, will be the key factors for the roll out of autonomous wireless smart systems.

TOWARDS A SOLUTION

There is little doubt that comprehensive research efforts in a variety of areas are required, in order to come up with the necessary architectural foundations for the IoT. As a focused contribution to the general discussion on how the key technical IoT challenges are to be addressed, in this section we concentrate on three wireless-related issues, and provide a case-study IoT architecture implementation as a concrete example.

COMMUNICATIONS AND NETWORKING IN DENSE ENVIRONMENTS

Effective communications and networking in a large and dense heterogeneous environment need protocols at the lower layers that support co-existence of diverse wireless interfaces, such as intelligent (or cognitive) management of interference and distributed management of channel allocation/medium access. Communication protocols exploiting the locality in order to deal with scale are a promising approach, as in the IoT many interactions are expected to take place locally between physically co-located devices, and do not require support for global end-to-end interactions, as in the "traditional" Internet. Where needed, end-to-end interactions can be resolved by smart ways of aggregation, e.g., by allowing nested aggregation of objects and associated IoT resources to deal with scale, exploiting physical proximity and inter-relationships between objects (for example, objects placed in a container) for the use of addressing or for discovery.

Issues such as medium access control, routing, error control, and Quality-of-Service will need to be explicitly incorporated in the design. Such issues are made significantly more difficult than in traditional (wireless) networks by the heterogeneity and density of the deployment. Given the potentially high level of dynamics in the system and the limited bandwidth, energy, storage and communications capabilities of most of the devices involved, the need to maintain and process state should be kept to a minimum. Also, robust schemes which provide the capability to survive bad channel conditions or temporary (or even prolonged) lack of connectivity will be of paramount importance in this context. In our opinion, the following components will play a key role in developing a solution with the above features, towards a protocol suite able to support IoT systems:

- Random access and geographic routing: random access is inherently distributed, and suitable in an environment where knowledge of the topology is not always available or accurate; it can also be effectively coupled, via cross-layer optimization, with geographic routing, which is stateless and can be made very efficient in dense topologies. In addition, we could also try to

Issues such as medium access control, routing, error control, and Quality-of-Service will need to be explicitly incorporated in the design. Such issues are made significantly more difficult than in traditional (wireless) networks by the heterogeneity and density of the deployment.

One of the main factors that contributed to the success of the current Internet architecture is the centrality of the IP. As the variety of technologies and services that belong to the IoT is even wider, we believe that building an architecture that is centered on a similar concept will be essential for its success.

leverage on the presence of devices with different capabilities, moving away from the "flat" design concept typical of ad hoc networks, towards a more efficient structure in which nodes take on roles according to their own capabilities and where more capable nodes may give resource-poor devices access to advanced features (e.g., computing or storage). This approach will open up several research challenges that do not currently have a definitive solution.

- Network coding and random data combination: network coding has been shown to provide an effective means for efficient reliable data dissemination and to require little coordination among nodes; random data combination is a lightweight, yet effective, mechanism to provide adequate reliability and error control with little overhead. Recent results have shown how these paradigms can greatly improve the performance of dissemination in homogeneous networks, but extension of these techniques to highly heterogeneous scenarios has not yet been addressed. Finally, for densely deployed nodes with very limited individual capabilities it makes sense to look into distributed processing paradigms for decoding.
- Clustering and cooperation: leveraging on the presence of more capable nodes to help others in reliably delivering their data is a good approach in a heterogeneous environment; an interesting open research problem in this context is how to place a number of such nodes in an environment so as to improve the overall network performance. Cooperation strategies, ranging from PHY cooperation to improve the quality of wireless links to opportunistic strategies at the MAC and routing layers, have been shown to provide significantly better performance in dynamic wireless networking contexts; we may expect that this approach will be even more important in an IoT scenario, where heterogeneity and scale are key factors. The challenge in this case is how to provide simple yet effective and robust distributed schemes.
- Disruption-tolerant paradigms: techniques to provide networking capabilities even in the absence of stable connectivity will play an important role in environments where continuous wireless coverage cannot be guaranteed and where there may be a significant degree of randomness in the communications relationships among wireless nodes. Mechanisms to reveal the presence of other nodes and to decide whether to exchange data will need to be developed, in view of the fact that some nodes cannot afford to continuously transmit/listen but rather need to judiciously manage their own energy. Scenarios where mobile users (e.g., a person carrying a cell phone) can be used for data ferrying and/or to provide information about, e.g., the network topology, seem very promising.

A New Narrow Waist Below the Service Layer

One of the main factors that contributed to the success of the current Internet architecture is the centrality of the Internet Protocol (IP), which can be seen as a narrow waist between connected devices on one side and applications and services on the other. This architectural choice permits a wide range of different communication implementations below, and a wide variety of transport and application protocols above, allowing a highly diversified range of services and technologies to inter-operate. As the variety of technologies and services that belong to the IoT is even wider, we believe that building an architecture that is centered on a similar concept will be essential for its success, allowing heterogeneous technologies to thrive underneath and applications and services to flourish above.

However, the complexity of the IoT and the heterogeneity of devices and technologies pose a much greater challenge than in the traditional Internet. The quest for the proper hourglass model for the IoT is just in its infancy. One point of view, currently supported by some researchers, is to have a narrow waist above the network layer and just below the service layer. By doing so, the capabilities of the underlying IoT technologies could be exposed as a universal building block. Standardized interfaces could provide consistent service primitives for applications and services. While we can concede that this is a useful starting point for a discussion, we strongly believe that this issue needs to be investigated more deeply, before a final conclusion can be drawn as to where the "next" narrow waist will be, and how it will look like. The use of different wireless protocol stacks for different applications and environments makes the choice of the "next" narrow waist extremely complex. The convergence between different communication mechanisms into a coherent and interoperable fabric might pass through the extension of some of the existing protocols, together with the creation of bridge routers, hosted in base stations.

As a first step towards drafting a convergent architecture for the wireless protocols in the IoT area, we identify three main issues . We believe that the development of Machine to Machine interfaces (M2M API) will enable proactive communication of devices, transparent to the user. M2M APIs should be drawn up for all devices of the identified application areas. Important efforts have been made in this area, and groups such as the ETSI M2M Working Group are developing interesting solutions. Furthermore, we think that a uniform protocol view, compatible with the current IP suite, will provide protocols at different levels and will be the basis of device interoperability. The development of interfaces, bridges and inter-protocol routers will allow all devices, generally developed with a precise service in mind, to embrace a greater variety of applications. Last but not least, a thorough analysis of the effects of the IoT at the network level will be needed, paying particular attention to the *terabyte torrent* generated by billions of interconnected devices and how it can be handled via wireless communications.

Linking Physical Entities and Devices of the Internet of Things

The IoT is expected to provide a resource fabric interfacing the physical world by means of a ubiquitously deployed substrate of embedded networked devices. These resources provided by the IoT include sensors, actuators, RFID tags and readers, NFC enabled devices, etc. Some of these devices will have the ability to interact with or record information/events concerning the real world and the entities contained within. Real world entities can have living embodiments such as persons and animals or be objects such as buildings, cars, tools, production material or other organic and inorganic matter.

Business services, end user applications or enabling middleware services can exploit the information and interaction capabilities of the IoT with respect to real world entities only if the necessary set of available IoT devices can be determined. This includes finding the relevant entities and the corresponding IoT devices that provide information about these entities or allow interactions with them. Most of the existing research has been based on the assumption that there is a static association between the resources of the IoT and surrounding real world entities, or that associations can be inferred by globally available location information. In real life the environment is much more heterogeneous and dynamic as IoT devices and real world entities may be mobile with respect to each other, IoT resource availability and communication capabilities may vary throughout an environment and in time, and knowledge of locality may be incomplete. Such an environment makes the resolution of available IoT devices that are concerned with real world entities a challenging task, particularly on a global scale.

We envision the development of a new resolution infrastructure that enables an efficient linking of real world entities with relevant devices of the IoT. The provided functionality consists of three different aspects which are visualized in Fig. 2, namely:

1. Discovery of the relevant entities, e.g., based on identifier, location, type, provider, topic, or a combination thereof
2. Lookup of IoT devices that can provide information about the entities or allow interactions with them
3. Monitoring IoT devices and entities and keeping the dynamic links between them up-to-date

At the same time the developed resolution infrastructure has to ensure that only authorized services and applications can discover available devices of the IoT concerning real world entities. A particular challenge hereby is the handling of heterogeneous identification schemes that will unavoidably exist in the Internet of Things. As mentioned, earlier IoT devices can be identified by different identification schemes or communication level identifiers. Similar heterogeneity can be expected from the assignment of identities to real world entities. The resolution infrastructure will be able to cope with this heterogeneity, allowing a controlled inter-linking of those based on the privacy and security contexts of the IoT devices and their respective real world entities.

Architecture and Protocols for the Internet of Things: A Case Study [13]

The future Internet will strive to yield novel means of interaction with services, other users, and the environment. Wireless Sensor Networks (WSNs) represent a reasonably cheap sensory extension to Internet-connected devices; moreover, their computational capabilities allow for further (though possibly limited) flexibility of use and functional expansion. Any kind of next-generation Internet enabled portable device will set up advanced interactions with the “things” making up the new IoT, resulting in a pervasive infrastructure of fixed and mobile heterogeneous nodes, seamlessly providing, exploiting or sharing context based services and applications. In particular, capturing the context around the devices will constitute a key component, making such operations as “Googling” the physical reality possible and common. By integrating any object into the IP infrastructure, making it possible to natively address and connect it, 6LoWPAN [14] is an important enabling technology to support the cited IoT interaction paradigm, while still running everything over the widespread Internet infrastructure. The use of Web services is a key ingredient of this migration, and allows the transparent integration of specialized systems (such as a WSN) with any system built with standard components, thereby greatly accelerating the penetration of the IoT paradigm. As an example, TinyREST is an efficient implementation of Web services in WSNs, that accounts for the specific resource requirements of sensor nodes.

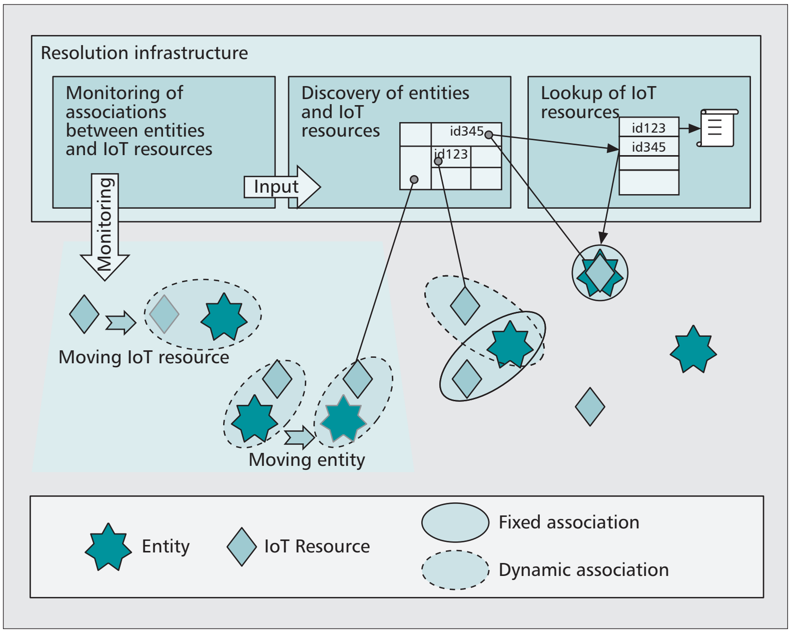
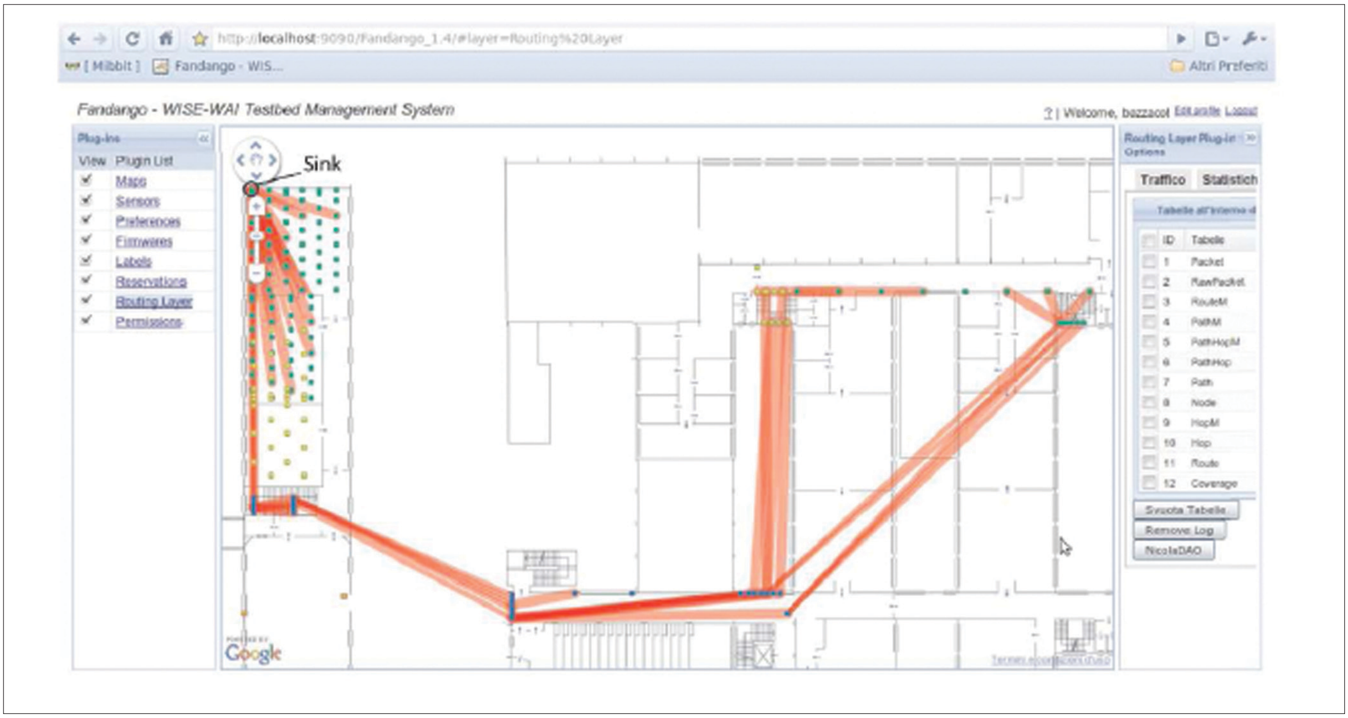


Figure 2. *A new resolution infrastructure for linking physical entities and devices in the IoT.*

We recently put this vision into practice [13], by channeling experience in the field of wireless sensor networking towards the realization of a scalable and easily extendable network structure, which includes different classes of nodes running compatible code but providing different functions and carrying out different tasks. The network spans several floors in three buildings at the University of Padova, and includes high- as well as low-density areas (Fig. 3). The focus is not only on the setup and installation of the network (although this is by itself interesting and



□	ID	Tabelle
□	1	Packet
□	2	RawPacket
□	3	RouteM
□	4	PathM
□	5	PathHopM
□	6	PathHop
□	7	Path
□	8	Node
□	9	HopM
□	10	Hop
□	11	Route
□	12	Coverage

Figure 3. *Topology of a portion of the testbed at the University of Padova, shown through a Google Maps-based application [15].*

challenging), but rather on its use, development and structure optimization. To this end, all nodes are IPv6-compatible, which makes them directly addressable from any Internet-capable device. The nodes support diverse services, from environmental parameter monitoring to localization, and are in turn supported by lower-level functionalities allowing, e.g., to switch the application being run on the node, to change the class/role of a node, to spread software changes and updates over the air, or to perform low-level resets in case of malfunctions. Offering services through our network provides an opportunity to realize part of the IoT vision and continue research efforts in the field. In addition, it concretely demonstrates the advantages of the IoT in the everyday management of a campus environment.

Experience with such a large network testbed, in which the above protocol suite has been fully implemented and tested, has shown that the IoT architecture based on Web services and IPv6/6LoWPAN is a powerful paradigm with the potential of allowing a rapid penetration of IoT concepts in practical systems. Details of the implementation and additional discussion can be found in [13], whereas some experimental results related to the use of such architecture in a smart monitoring and smart grid scenario can be found in [15].

Conclusions

In this article we have provided a brief description of the current state of the art of the Internet of Things, with special focus on concepts and technologies related to mobility and wireless communications and networking. Although the IoT concept has been around for several years now, there are still many major technical issues that have not been solved, including heterogeneity, scalability, security, connectivity, energy, management, naming and identification. The complexity of these technical issues, especially in view of the resource-constrained nature of many IoT components and of the use of wireless communications, calls for a unified architectural view able to address them in a coherent fashion. After pointing out several of the main issues, we have provided some initial ideas to address some of them. We have also briefly described a recent case study where an architecture and protocol suite for IoT has been implemented. These contributions, far from representing complete and definitive answers, are nevertheless a useful starting point for a deeper discussion that will keep researchers busy for the next decade.

A major research effort, IoT-A (Internet of Things — Architecture, www.iot-a.eu), which represents the flagship project in the IoT area within the European Commission's FP7, and which includes the authors among its key participants, has started in September 2010 and will be running for three years.

Acknowledgment

This work has been partially supported by the European Commission under the IoT-A project in FP7 (Grant Agreement no. 257521). The authors would also like to thank the partners of the IoT-A consortium, whose discussions have inspired some of the ideas presented in this article.

References

[1] X-ETP Group, Future Internet Strategic Research Agenda, Feb. 2010.

[2] L. Atzori, A. Iera, and G. Morabito, *The Internet of Things: A Survey*, Elsevier Computer Networks, 2010.

[3] ITU Internet Reports, The Internet of Things (Ed. 2005), Nov. 2005.

[4] SENSEI FP7 Project, Scenario Portfolio, User and Context Requirements, Deliverable 1.1, Available at http://www.sensei-project.eu/.

[5] E. Welbourne *et al.*, "Building the Internet of Things Using RFID: The RFID Ecosystem Experience," *IEEE Internet Computing*, vol. 13, no. 3, May–June 2009, pp. 48–55.

[6] A. Dada and F. Thiesse, "Sensor Applications in the Supply Chain: The Example of Quality-Based Issuing of Perishables," *Proc. Internet of Things 2008*, Zurich, Switzerland, May 2008.

[7] K. Finkenzeller, *RFID Handbook, 3rd Ed.*, Wiley, 2010, ISBN: 978-0-470-69506-7.

[8] D. Kofman, EPC Global Standards: An Opportunity or A Threat for Europe, The Internet of the Future, Bled 2008.

[9] B. Krishnamachari, *Networking Wireless Sensors*, Cambridge University Press, Jan. 2006, ISBN: 978-0-5218-3847-4

[10] C. Floerkemeier, R. Bhattacharyya, and S. Sarma, "Beyond the ID in RFID," *Proc. TIWDC 2009*, Pula, Italy, Sept. 2009.

[11] ETSI Machine to Machine Standardization Technical Committee, www.etsi.org/Website/Technologies/M2M.aspx.

[12] K. Sakamura, "Challenges in the Age of Ubiquitous Computing: A Case Study of T-Engine — An Open Development Platform for Embedded Systems," *Proc. ICSE'06*, Shanghai, China, May 2006.

[13] A. P. Castellani *et al.*, "Architecture and Protocols for the Internet of Things: A Case Study," *Proc. 1st IEEE Int'l. Wksp. Web of Things (WoT 2010 at IEEE PERCOM)*, pp. 678–83.

[14] Z. Shelby and C. Borman, *6LoWPAN: The Wireless Embedded Internet*, Wiley, 2009, ISBN: 978-0-470-74799-5.

[15] N. Bressan *et al.*, "The Deployment of A Smart Monitoring System Using Wireless Sensor Network and Actuator Networks," *Proc. IEEE SmartGridComm*, Gaithersburg, MD, Oct. 4–6, 2010.

Biographies

MICHELE ZORZI [F'07] (zorzi@dei.unipd.it) received his Laurea and Ph.D. degrees in electrical engineering from the University of Padova, in 1990 and 1994, respectively. During the academic year 1992-1993, he was on leave at the University of California, San Diego (UCSD), attending graduate courses and doing research on multiple access in mobile radio networks. In 1993 he joined the faculty of the Dipartimento di Elettronica e Informazione, Politecnico di Milano, Italy. After spending three years with the Center for Wireless Communications at UCSD, in 1998 he joined the School of Engineering of the University of Ferrara, Italy, and in 2003 joined the Department of Information Engineering of the University of Padova, Italy, where he is currently a professor. His present research interests include performance evaluation in mobile communications systems, random access in mobile radio networks, ad hoc and sensor networks, energy constrained communications protocols, cognitive radios and networks, and underwater acoustic communications and networking. He was Editor-in-Chief of the IEEE Wireless Communications Magazine from 2003 to 2005, is currently Editor-In-Chief of the IEEE Transactions on Communications, and serves on the Editorial Board of the Wiley Journal of Wireless Communications and Mobile Computing. He was also a guest editor for special issues in IEEE Personal Communications (Energy Management in Personal Communications Systems) and IEEE Journal on Selected Areas in Communications (Multimedia Network Radios, Underwater Wireless Communication Networks). He is currently serving as a voting member of the ComSoc Board of Governors.

ALEX GLUHAK (A.Gluhak@surrey.ac.uk) is a senior researcher at the Centre for Communication System Research (CCSR) at the University of Surrey, UK, where he is coordinating Internet of Things related research activities. He is technical manager of the ICT-FP7 SENSEI project, a European project with 20 partners, investigating the integration of the physical world into the Future Internet. He has held research positions with CSSR and later the Ericsson Ireland Research Centre, while contributing actively to several large European research projects, such as e-SENSE, SENSEI and recently SmartSantander and IoT-A. His main research interests are next generation network architectures and experimental facilities - in particular integration of the Internet of Things into Internet service layers, service-oriented sensor networks and scalable context information infrastructures for next generation networks. He has been visiting researcher at NICT Japan, in 2005 and University of California Irvine, US in 2002.

SEBASTIAN LANGE (slange@vdivde-it.de) holds a degree in physics from the University of Heidelberg, Germany. After his Ph.D. at the European Molecular Biology Laboratory in Heidelberg, Germany he has been working as management consultant for the Consulting Company Droege & Comp./Arideon with a focus on business-process and knowledge management. He has been working with VDI/VDE-IT since 2006 and is currently Senior Consultant in the Department Innovation Europe. He helped to establish the European Technology Platform on Smart Systems Integration where he is currently responsible for the management of the ETPs Office as deputy secretary general and holds conceptual and advisory functions. He has been involved in the management of several EU FP projects and has been strongly committed to establishing and evolving the topic of IoT on a European level in the recent years.

ALESSANDRO BASSI (abassi@eecs.utk.edu) graduated from the University of Milan in 1994, with soft computing and software engineering as majors. He joined Amadeus in 1997, and moved to the University of Tennessee in 2000, where he was involved in the seminal work of the Internet Backplane Protocol. He then held a Research Visitor position at the ENS in Lyon, France, where he developed the relationship between storage and active networking. After working for RIPE NCC, in November 2004 he joined Hitachi. He was the deputy project coordinator of the FP5 6QM project, and the project coordinator of the FP7 "Autonomic Internet" project. He also participated to several other EU projects and initiatives. Since 2007, his research interests are focused on RFID technology and the Internet of Things. He is the chair of the Internet of Things WG of the European Technology Platform EPoSS. He is an expert for ENISA on possible threats from IoT technology adoption, and he is the Technical Coordinator of the IP FP7 project "Internet-of-Things Architecture" (IoT-A).