RFID & IoT: a Synergic Pair
Issue 8 • March 2015

Topics
1. Introduction
2. RFID and IoT in Numbers
3. Pioneering Papers on RFID &plus; IoT
4. Overview
   - New paradigms of energy harvesting for RFID communication and sensing
   - RFID for Smart Spaces
   - Industrial opportunities for RFID-IoT
   - Business models for RFID-IoT
   - Evaluation of IoT infrastructures
5. RFID as the Last-meter Sensor Nodes of IoT
   - Battery-assisted wireless sensor nodes
   - Fully passive sensor nodes with onboard electronics
   - Antenna as a chemical to electromagnetic signal transducer
   - Chip-free tags, the RF analog to barcodes
6. RFID Localization Networks
   - Algorithms for Indoor Localization
   - Ontology for automatic geo-mapping of Things
7. RFID &mdash; IoT for Healthcare
   - Enabling Virtual Worlds for Healthcare
   - IoT and medical implanted devices
8. Organizing and Securing RFID-generated Data
   - RFID in the cloud
   - How secure is RFID authentication for IoT ?
9. Conclusion: Economic and Ethic Impacts
10. References

- Pioneering papers on RFID + IoT
- Overview
- RFID as sensor nodes of IoT
- RFID Localization Networks
- RFID for IoT Healthcare
- Networks and Security of RFID-IoT
- Economic and Ethic impact

Editors

**Associate Editors**

Sara Amendola  
University of Roma Tor Vergata, Italy

Maria Cristina Caccami  
University of Roma Tor Vergata, Italy

Alberto Caponi  
University of Roma Tor Vergata, Italy

Luca Catarinucci  
University of Salento, Lecce, Italy

Valeria Cardellini  
University of Roma Tor Vergata, Italy

Emidio Di Giampaolo  
University of L’Aquila, Italy

Sabina Manzari  
RADIOSENSE srl, The Last meters of Internet of Things, Roma, Italy

Francesco Martinelli  
University of Roma Tor Vergata, Italy

Stefano Milici  
University of Roma Tor Vergata, Italy

Cecilia Occhiuzzi  
RADIOSENSE srl, The Last meters of Internet of Things, Roma, Italy

**Editor in Chief**

Gaetano Marrocco  
University of Roma Tor Vergata, Italy
1. Introduction

by Gaetano Marrocco

Internet Of Things (IoT) is driven by a combination of sensors and actuators, connectivity, people and processes. The interactions among these entities are creating new types of applications and services.

IoT will provide a dynamic global network infrastructure with self-configuring capabilities where physical and virtual "Things" have both unique identities and physical attributes and are integrated into the information network in a fully transparent way for a final user.

In the framework of Internet of things, an entity can be a farm animal with a biochip transponder for identification and tracking, an historical monument protected by a structural-health monitoring-network, a person with an implanted smart prosthesis, a car with built-in sensors or any other natural or man-made object which can be provided with an IP address and with the capability to exchange data over a network. So far, the Internet of Things has been mostly associated with machine-to-machine (M2M) communication in manufacturing and power, oil and gas utilities, but many other implementations are currently being investigated and even experimented.

Although the IoT concept appeared after 1998, the basic ideas are older and have been in development for decades. One of the first examples is an internet-connected Coke machine at Carnegie Mellon University in the early 1980s. In 1991, Mark Wiser of Palo Alto Research Center (PARC) talked about Embodied Virtuality in its famous writing The Computer of the 21th Century, i.e. the process of drawing computers out of electronics shells, so that the virtuality of computer-readable data is brought into the physical world. In more recent times, CISCO and NASA started the program Planetary Skin, with the purpose to deploy a global nervous system, which integrates land-sensors, sea-sensors, air-sensors and Space-sensors, to help the public and private sectors to make decisions and prevent and adapt to climate changes. In a much smaller scale, some researchers introduced the concept of Internet of Nano-things (Akyildiz, Jornet, 2010) where microscopic objects inside our working desktop or even inside our body, wirelessly or chemically exchange information thus contributing to a macroscopic goal.

The continuous migration of Internet toward the material world is now going beyond the current wired cloud infrastructures, wherein most of the interconnection and profiling services are generated. An augmented version of Internet comprises a mobile access layer which provides a suitable interface between the core of the network and wireless sensors distributed all around, in the short range. The mobile access will be made possible by fixed nodes as well as by mobile nodes such as hand-held devices and scanner-equipped drones and robots (Fig. 1).

![A pictorial representation of the Internet of Things](Fig. 1)
to large scale-decisions concerning Environments, Precision Agriculture, E-Health and sustainable progress in general (Smart Community and Smart-Cities). The pervasive interconnection with Things will require deploying a multitude of RFID tags and sensors, and conceiving new functionalities concerning the habitat control, the disaster relief, the mobile healthcare, the monitoring of industrial processes, the security surveillance and the realization of augmented spaces in general.

An interconnected object possesses one or more of the following capabilities:

- Identification
- Localization
- Self-diagnosis
- Sensing
- Actuation (of remotely-given commands)
- Local computation and data analysis.

Radiofrequency Identification (RFID) is one of the key-enabling technologies of IoT since it not only permits to link a digital code to an object in a wireless modality, but also to capture its physical status and to provide geo-referenced information. RFID tags can be equipped with a large variety of sensors according to several integration modes, exploiting a broad range of possible functionalities and costs. Active RFID tags, which make use of independent batteries, a microcontroller and dedicated electronics, ensure long operating ranges, high data rate, and the greatest versatility in terms of sensor interconnection. Main drawbacks of this solution are high costs, limited lifetime and not-negligible weight and size. Conversely, passive RFID tags are completely battery-free and can be printed on or permanently embedded into tagged objects for structural, medical or product monitoring, thus becoming a seamless attribute of the objects themselves. The major limitations of this class of systems are the need of proximity to a reading device and a rather reduced set of functionalities.

The implementation of RFID technology in the framework of Internet of Things deserves to be considered with the largest scope, ranging from the acquisition of an elementary status of an object, for instance its presence/absence within a given region (localization), up to the multidimensional description of the chemical-physical and relational parameters of a Thing with respect to the nearby environment and to other Things. Here the term "Thing" is indicated with capital letter to highlight the fact that the usual tagging of an object is augmented by the physical interaction between the objects and the RFID tag itself to produce a richer informative content. In this vision any object becomes a completely new kind of entity, partly material and partly digital, that which continuously produces information all along its lifetime. Bruce Sterling, (Shaping Things, 2005) refers to this concept with the evocative term "Spime" (Space + Time), pointing out the idea of material objects correlated with evolving information. RFID is hence a mean to transform an object into a Spime in the IoT domain.

2. RFID and IoT in Numbers

by Maria Cristina Caccami and Gaetano Marrocco

The scientific production about the inter-correlated topics of IoT and RFID is still in an embryonic state but it has been growing in the last decade with a great variety of colors and delineations.

A search on Google Scholar for these two keys:

RFID + Internet of Things

returned more than 16000 entries (excluding patents).

The current situation on IEEE Explore is rather different and a considerably smaller set of papers is found for the same combined keys.

To better understand, three different kinds of filters have been applied to configure the search:

a) full text (including metadata)

b) metadata only (e.g. title, abstract and keywords)

c) title only

Results are shown in Table 1 together with the number of papers returned by making two separate queries for the two keys ("RFID", "Internet of Things"). The keys RFID + Internet of Things were at least mentioned inside the papers no less than 2500 times up to December 2014 (distributed in Conferences and Journals as in Table 2), no matter with what emphasis, hence indicating an at least "generic" interest for this two hot topics since 2003. A smaller set of 458 papers referred the keywords into the title or abstract (metadata filter) and only 43 of them hosted RFID+IoT in the title. If we consider the much relevant number of papers concerning RFID and IoT separately (Fig. 1), we may conclude that the role of RFID technology in the IoT architecture is not so clear and not so clearly assessed for most of scientists and engineers who make research and/or development on RFID matters.
Table 1: Statistics on IEEE Explore for papers including the RFID and Internet of Things keywords up to December 2014.

<table>
<thead>
<tr>
<th></th>
<th>Full text</th>
<th>Metadata</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID</td>
<td>30895</td>
<td>11362</td>
<td>1120</td>
</tr>
<tr>
<td>IoT</td>
<td>8700</td>
<td>4092</td>
<td>1576</td>
</tr>
<tr>
<td>RFID+Internet of Things</td>
<td>2536</td>
<td>458</td>
<td>43</td>
</tr>
</tbody>
</table>

Table 2: Distribution of papers into Journals and Conferences and year (in brackets) of the publication of the first paper.

<table>
<thead>
<tr>
<th></th>
<th>Conferences</th>
<th>Journal &amp; Magazines</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata Only</td>
<td>413 (2003)</td>
<td>45 (2008)</td>
<td>-</td>
</tr>
<tr>
<td>Title</td>
<td>38 (2007)</td>
<td>3 (2009)</td>
<td>-</td>
</tr>
</tbody>
</table>

Fig. 2: Number of papers returned by IEEE EXPLORE for three independent queries applied on Metadata (title, abstract and keywords) only (updated at December 2014)

The occurrence of papers per year (Fig. 3) reveals a sharp increase of the interest of the scientific community in 2010, with a peak in 2012. Most of the entries are contributions to conferences while in the last 2 years, in spite of a reduction of conference papers (at least in the IEEE eco-system) the number of more structured papers appearing over Transactions, Journal and Magazines is becoming remarkable even if still far from providing a well assessed base of knowledge. In particular, in 2014, 156 papers included a reference to RFID+IoT somewhere and 22 papers addressed such binomial with great emphasis.
Fig. 3 Bar plot of the papers per year presenting the combination of the two search keys "RFID" and "Internet of Things" as returned by IEEE-Explore when the search is limited to a) full text and b) metadata only.

Fig. 4 finally shows the diagram of the citations per year of papers having the couplet RFID and Internet of Things in the full text, as provided by SCOPUS. The trend was continuously increasing since 2003 and the peak was registered in 2013 with an appreciable 1000 citations.
The conference papers of the past two years and the journal papers in the period 2008–2014 which include the RFID+IoT keys into title/abstract/keywords can be classified according to the following set of topics (Tab. 3).

**Table 3: A possible classification of RFID-IoT papers**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Overviews</td>
<td>20</td>
<td>18</td>
</tr>
<tr>
<td>Localization &amp; Labeling</td>
<td>23</td>
<td>7</td>
</tr>
<tr>
<td>Sensing</td>
<td>16</td>
<td>7</td>
</tr>
<tr>
<td>Healthcare</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Networks and Security</td>
<td>60</td>
<td>13</td>
</tr>
<tr>
<td>Economic and Ethics impacts</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Other</td>
<td>9</td>
<td>136</td>
</tr>
</tbody>
</table>

A relevant percentage of papers published so far concerned overviews and scenarios as well as computer-science issues. Privacy & Security is currently one of the hottest topics in the IoT arena due to the expected increase of interconnected devices virtually exposed to cyber-attacks. Moreover there is a remarkable interest for the localization topic which is strategic to provide context-aware services.

The recurring keywords for each class are listed in Table 4 and may provide a useful starting point to further probe these rich IoT-RFID macro-topics.

**Table 4: Recurring hot-words of latest RFID-IoT papers**

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>KEYWORDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overviews</td>
<td>future scenarios, new architectures, context-aware systems, standards, modeling and optimization, participative marketing, augmented reality, energy harvesting, ubiquity, near field communication, smart surfaces, chipless technology</td>
</tr>
<tr>
<td>Localization &amp; Labeling</td>
<td>object tracking, context awareness, cooperative/collaborative/distributed localization, vehicle mounting, IoT tracking, intelligent parking, intelligent inventory, ontologies</td>
</tr>
<tr>
<td>Sensing</td>
<td>cognitive intelligence, ambient sensing, heterogeneous wireless sensor network, pervasive electromagnetics, antennas, inkjet print, chemical-loaded sensors, structural health monitoring</td>
</tr>
<tr>
<td>Healthcare</td>
<td>E-health, implantable devices, intelligent packaging, smart spaces, virtual worlds, healthcare logistics</td>
</tr>
<tr>
<td>Networks and Security</td>
<td>E-health, implantable devices, intelligent packaging, smart spaces, virtual worlds, healthcare logistics</td>
</tr>
<tr>
<td>Economic and Ethic impact</td>
<td>E-business, ethical implications, long-term impact, return on asset (ROA)</td>
</tr>
</tbody>
</table>

This preliminary bibliographic analysis revealed that the interest for RFID applications in IoT is certainly increasing but most of publications appeared outside the IEEE eco-system. Moreover these two technologies are not yet perceived as much correlated.

In the next sections, some selected papers are reviewed for each classification topic, starting from the very early papers listed by IEEE Explore.

### 3. Pioneering Papers on RFID &plus; IoT

By Gaetano Marrocco

The first two papers on RFID-IoT as reported by IEEE Explore appeared in 2003 and they both anticipated the central role of RFID tag in the newborn IoT architecture, concerning both the interaction of Things as well as a new way to distribute and access information.
4. Overview

By Gaetano Marrocco

There are several overview papers published in the last few years concerning the various shades of RFID and IoT topics and they offer an excellent starting point for entering into the realm of interconnected objects.

The five selected papers address the current and the future implementation of energy harvesting (section 4.1), bodycentric and ambient sensors (section 4.2), the potential new services and opportunities for industrial applications (section 4.3), the possible business models (section 4.4) and the way a complete IoT infrastructure could be quantitatively validated before use (section 4.5).

4A. New paradigms of energy harvesting for RFID communication and sensing

Power autonomy is the enabling attribute for the physical layer of IoT. While current RFID devices use the power coming from a reader placed at a close distance to perform backscattering modulations and hence to establish short range links, new sensing and communication means are being explored concerning how to harvesting, storing and modulating free-power from TV broadcast and cellular communications transmitters.
The survey in [Gollakota et al, 2014] discusses the “emergence” of RF-powered computers, including not only the augmented RFID systems with sensor capability, but also the data interchange between fully passive devices immersed into a free wireless field (TV, cellular) by applying the concept of ambient backscattering which may be reasonably considered as the further step of RFID toward ubiquity.

4B. RFID for Smart Spaces

Internet of Things may boost the traditional medical models toward the Participatory Medicine involving sensors (environmental, wearable, and implanted) spread inside domestic environments with the purpose to unobtrusively monitor the user’s health and to activate remote assistance.

The paper [Amendola, et al, 2014] gives a survey on the state-of-the-art of RFID for application to bodycentric systems and for gathering information (temperature, humidity, and other gases) about the user’s living environment. Many available options are described, from the physical up to the application level with some examples of RFID systems able to collect and process multichannel data about the human behavior in compliance with the power exposure and sanitary regulations.

4C. Industrial opportunities for RFID-IoT

IoT provides a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of RFID, and of wireless, mobile, and sensor devices.

The survey [Li et al, 2014] provides a deep scan of existing papers in the main scientific catalogs with regard to both current and foreseen industrial applications of RFID-IoT which are organized into the following areas: healthcare services, supply chain, safer mining production, transportation and logistics, and firefighting.

4D. Business models for RFID-IoT

Incremental innovations may see RFID being sold as a service (much like photocopiers are maintained today) rather than as a suite of technologies within a system which are sold as individual or bundled packaged components.

The overview [Michael et al, 2010] outlines the vision for such a Product Service System (PSS), the kinds of smart applications we are likely to see in the future as a result, and the importance of data management capabilities in planetary-scale systems.

Following the PSS business model, the usage of automatic identification services is sold to the end-users while the RFID-solution providers retain the ownership of RFID devices, software, and networks. End-users do not have to invest in acquiring RFID hardware devices, which are not charged by ownership, but only pay for their usage. RFID manufacturers share and reduce technical risks and total costs with end users by retaining the ownership and by providing upgrades of their devices. In addition, RFID solution providers are responsible for technical support for RFID systems throughout the implementation process.

4E. Evaluation of IoT infrastructures


An efficient implementation of an heterogeneous network including RFID nodes and other different motes, requires a preliminary assessment into test beds able to reproduce the relevant response of the overall IoT applications by including both physical layers (say Electromagnetic propagation, communication and protocols) and the application layers. The bottleneck is the huge reliance of IoT systems on real-world processes which are often the result of interactions among complex systems of systems and are extremely difficult to be accurately modeled.

The paper provides a taxonomy of the IoT experimental facilities available worldwide as laboratory test-bed and even at a city-scale level and suggests ways to arrange a complete test bed integrating many types of IoT devices such as actuators, RFID readers, tags, NFC-enabled mobile phones (used as participatory and opportunistic sensing platforms) as well as heterogeneous gateway platforms.

5. RFID as the Last-meter Sensor Nodes of IoT

The sensor is maybe one of the main applications of RFID to Internet of Things. At least four different architectures have been proposed so far for RFID sensing. In the first case summarized in section 5.1, the tag hosts complex on-board electronics and an analog to digital conversion is implemented on the tag itself so that the data collected by the sensor is transmitted to the reader in a digital format. The intelligence is hence located inside the tag itself. This kind of sensor node, which is usually battery-assisted, is more expensive than other options but much more accurate and flexible since it may include multiple sensors and provides a read range up to 10–15 meters. Possible applications are to the interconnection of environments or of devices inside critical infrastructures.

In the second class discussed in section 5.2, similar functionalities as the previous ones are obtained by a battery-less sensor node but the read distance is reduced down to a couple of meters, so that a feasible interrogation generally requires an agent moving close to the tag.
In third class shown in section 5.3, the electronics of the sensor consists just of the standard RFID microchip transponder. The antenna of the tag works as a chemical/mechanical to electromagnetic signals transducer and the intelligence to extract meaningful sensing information is mostly concentrated at the reader side. In other words the sensing information is derived from the fluctuation of the backscattered signals coming from the tag. This class of devices provides approximate and qualitative data with a very low-cost and therefore they could be suitable to interconnect even single items.

Finally, there is the emerging research on sensor nodes completely free of electronics (section 5.4), the useful labeling and sensing information is extracted through the broadband processing of the un-modulated radar signature of the tagged objects. These devices are referred to as chip-less tags or even RF tags, their cost is expected to be comparable with that of barcodes but production and real applicability are still in question.

5A. Battery-assisted wireless sensor nodes

by Sabina Manzari

A possible approach to design RFID sensor nodes for the IoT considers multi-functional battery-assisted devices which are optimized to last years. The paper [De Donno, et al, 2014] describes the design, the characterization and the test of a long-range, fully Gen2-compliant and programmable RFID tag equipped with three different sensors for temperature, light, and acceleration detection. The working principle of the device relies on a novel approach that exploits a new-generation RFID chip with a dual communication interface: a wired I2C interface managed by a microcontroller and a wireless UHF interface directly accessible by conventional RFID Gen2 readers. The RFID sensor comprises a compact dipole-like RFID and low-cost commercial discrete components on an FR4 substrate and it operates in battery-assisted passive (BAP) mode. The sensor readings are written via the I2C bus into the password-protected user memory of the RFID Gen2 chip leaving the EPC memory totally reserved for product identification. Unlike other recently developed RFID devices, which need specific settings for the reader, this solution is fully compliant with RFID standards and regulations.

The authors carried out a series of experiments to estimate the power consumption, the communication performance and the sensing features of the device. Thanks to the implementation of a wear-leveling algorithm, the memory usage provides up to 3 years of lifetime when the sensor is programmed to sample temperature, light, and acceleration every 30 seconds. The RFID-based sensor data are correctly transmitted up to a distance of approximately 22 m from the interrogator, which is the longest read range ever reported for similar devices. The high level performance in terms of communication, power consumption, and sensing capabilities of the proposed device could enable a broad range of IoT applications where everyday networked objects with sensing and computing capabilities interact with each other to create smart environments.

5B. Fully passive sensor nodes with onboard electronics

by Luca Catarinucci
The paper [Roy et al., 2010] introduces the main brick to build a possible IoT-like application in the framework of the RFID-based sensor networks. It is maybe the first example of augmented UHF RFID Tag in the literature. The wireless identification and sensing platform (WISP) was introduced by the same authors in 2005 and gradually refined over time. The version of WISP discussed in the paper is provided with some sensors and with a fully programmable low-power microcontroller unit (MCU) on which the EPC Gen 2 protocol is implemented via software. The MCU and the sensors are powered by means of an energy harvesting circuit tuned to the UHF RFID bandwidth at the purpose to take advantage from the signal emitted by the interrogating RFID reader.

A Software-Defined RFID reader is moreover implemented and exploited in place of a commercial one in order to fully master the communication between WISPs devices and the RFID infrastructure. The joint use of the two categories of devices represents a solid base from which the implementation of RFID-based Sensor Networks may actually begin.

5C. Antenna as a chemical to electromagnetic signal transducer

By Cristina Caccami

The paper [Manzari, et al., 2013] introduces a simple, highly sensitive and tunable miniaturized layout suitable to be used as gas sensor. The sensing function is played by the antenna itself which is coated by a layer of specialized chemically interactive material (CIM) whose dielectric properties are influenced by the absorption of volatile compounds. The sensitive chemical material is the Pedot:PSS, a COTS conductive organic polymer already proposed as RFID humidity sensor by the same authors and here applied to detect different gases like ethanol. Through an experimental campaign, the authors demonstrated that just a single polymer drop of Pedot:PSS, deposited very close to the microchip, ensures a remarkable dynamic range for the turn-on power during the exposure to gases. Moreover, when the radio-sensor is exposed to different percentages of humidity and ethanol and then let recover, the chemical effects are fully reversible and proportional to the various concentrations of the gases. The proposed tag can be also doped with different sensitive chemical materials with the purpose to obtain an array of wireless passive sensors for the multivariate analysis of volatile compounds. Possible applications are the control over the quality of bio-medical environments, precise agriculture, industrial processes, foods and the human wellness in general.

5D. Chip-free tags, the RF analog to barcodes

By Luca Catarinucci
The pervasive adoption of the RFID technology would be still possible if tags were made further cheaper, better recyclable and more robust, reliable, and secure. A possible solution, not exempt from technological challenges, is certainly the one based on chipless tags and on specific RFID readers capable to read them. The ambitious goal of such systems is storing and transmitting the ID code without the use of any chip.

This variant of the RFID technology is the so-called “chipless RFID”. The paper [Tedjini et al, 2013] provides an overview on the chipless RFID technology from the point of view of the RF engineer. The paper starts with the captivating first ever example of chipless RFID tag, designed by Léon Theremin in 1945 and used by the Soviet Union during World War II to fraudulently listen to the conversations of the U.S ambassador in Moscow. Then the three different approaches commonly exploited to design chipless tags are discussed in detail. The first one establishes a direct link between the electromagnetic signature of the tag and the information to be stored. The second uses a compact and simple RF processing circuit to encode information into the tag. The third one is based on the optimization and on the exploitation of the electromagnetic signature of the tag to combine the two previous techniques. In all cases, the idea is to apply the radar principles and signal processing tools to extract digital information from the engineered electromagnetic signature of the structure. However, since there is no chip embedded within the tag, all the sensing intelligence is transferred to the reader, which consequently becomes more complex than the conventional RFID scanners. Several possible reader architectures operating either in frequency domain or in time domain have been investigated so far. Frequency domain readers are much easier to develop, but they contravene the RF emission regulations. A relevant research effort is hence dedicated to time-domain scanners that can also exploit UWB signals.

6. RFID Localization Networks

One of the main application domains of IoT is in the smart home (SH) systems which are intended to assist users with daily activities within their home by applying ubiquitous computing.

The technology of Radio Frequency Identification plays a dual role in this context: it is an effective tool to uniquely identify objects and people and to collect and store environmental data, but it can also be applied to address and solve localization issues.

The use of sensors to gather information about operating conditions fosters the integration of complex platforms that will enable a proactive managing of the building as well as of daily activities by handling heterogeneous context-aware data (e.g. optimization of energy consumption, healthcare monitoring, entertainment, etc.).

Physical localization assumes therefore a big role in the context of smart home systems which require a real-world search for things, but also for inferring knowledge about people's behavior.

Classic localization procedures shown in section 6.1, suitable to estimate trajectories, may be merged with the conceptual tool of Ontologies, section 5.2, with the purpose of extracting more aggregated and user-oriented information.

6A. Algorithms for Indoor Localization

By Francesco Martinelli
In several localization setups, tagged objects can be detected by means of a certain number of readers located in known positions of the environment. Several methods have been proposed so far with the goal to solve the problem of localizing tagged objects. Remarkable techniques are those based on the Angle of Arrival (AOA), propagation delay (either using Time of Arrival (TOA) or Time Difference of Arrival (TDOA)) and Received Signal Strength Indicator (RSSI). All these approaches raise specific problems which limit the achievable accuracy of localization.

Another technique, which is becoming increasingly important for determining the position of a tag, relies on the processing of the phase of the RFID signal: phase information can be used to retrieve the distance from the reader to the tag [Ma, et al. 2014]. The phase-based localization often provides better accuracy, robustness and sensitivity with respect to other RFID-based approaches.

While developing their phase-based localization method, the authors tackle a very important problem that afflicts all the aforementioned procedures: the deterioration of the localization accuracy in non-line-of-sight (NLOS) environments, which is the usual scenario in several applications. They propose an approach based on the key observation that the NLOS range of measurement is always positively biased. Taking advantage of this fact, the authors developed a new RFID indoor localization algorithm using convex optimization and an iterative procedure that progressively improves the estimate of the tag position. Compared to other approaches, this algorithm sensibly shows a better performance especially under severe NLOS conditions.

6B. Ontology for automatic geo-mapping of Things
by Emidio Di Giampaolo
A possible Home Localization System for Misplaced objects (HLSM) is based on the application of ontologies [Huynh et al, 2014] and it is suited for integration with a Smart Home platform to localize lost or misplaced objects inside the home.

The HLSM consists of a central server connected to fixed RFID readers deployed in the environment and to mobile RFID readers. Fixed RFID readers are used as high-level navigation landmarks (HLNLs) placed at the entry doors of a room. A number of passive RFID tags are fixed on each piece of furniture and are used as detailed navigation landmarks (DTNLs) (i.e. reference points). The HLNLs help identify in which room the tagged object could possibly be, while the DTNLs help narrow the uncertainty on the part of the room where the object is located. The proximity of the lost object to DTNLs is based on the measurement of the RSSI of signals received by the mobile reader.

The main novelty is the software architecture of HLSM based on ontology. The central server consists of a Web server, an application server, and an ontology database. Mobile RFID readers communicate with the Web server and the fixed RFID readers communicate with the application server. The application server and the Web server query the ontology database using SPARQL protocol, an RDF (Resource Description Framework) query language in semantic Web environments. Information stored as ontology permits to apply reasoning to the search and to ease its integration with the entire system. It also ensures adaptability with the emerging semantic Web. Most of the functionalities are done on the Web server. Mobile readers, which are integrated into smart phones/tablets, are mainly used to read the RFID tags, to send the information to the Web server and to receive the result as HTML pages.

The location of the lost object is not given in terms of coordinates, since it would be hard for the user to interpret where it is in the room, but as nearness to well known reference objects (e.g. "glasses are at the kitchen table") which is much more comprehensive.

The system has been experimented in the real life showing a successful localization rate of 87.5%.

7. RFID &mdash; IoT for Healthcare

Possible applications of RFID-IoT to Healthcare concern the logistics of the caregiving environments and the patient-centric diagnostic and care.

A networked infrastructure, which enables an augmented tracking of equipment, of personnel and patients inside a hospital, may improve the optimization of spaces and the maintenance of diagnostic and therapeutic devices (section 7.1).

On the other side, bodycentric sensors, both wearable and implantable, will open a new frontier in ubiquitous monitoring and diagnostic of patients even outside hospitals. However, a critical issue to be investigated and assessed is the Electromagnetic interaction of RFID sources with the human body and in particular with vital implantable devices (section 7.2).
7A. Enabling Virtual Worlds for Healthcare

By Sara Amendola

Fig. 12 Left) 3D futuristic hospital as built in Second Life. Right) RFID virtual system embedded into the model of smart hospital.

A healthcare infrastructure, like a hospital, may greatly benefit from the network-oriented use of RFID devices not only to track assets and personnel, but also for a continuous monitoring of patients.

The preliminary evaluation of an IoT network and the training of the personnel may be simplified by the help of a simulated model of the environment also accounting for the physical and logical interactions about things.

The University of Arkansas [Thompson and Hangstrom, 2008] conducted a pioneering experiment, mostly supported by students, with the purpose to understand how 3D virtual worlds and RFID middleware may be cooperatively exploited in a pervasive scenario.

A free Internet virtual environment (www.secondlife.com) was selected as test-bed platform for modeling and analyzing the role of ubiquitous computing in healthcare settings. This project, called "Everything is Alive", was aimed at building a virtual futuristic hospital provided with tracking systems, smart networked equipment and workflow automation. This world is populated by avatar-bots mimicking doctors, nurses and patients. The RFID technology appeared as the natural tool to support different aspects of healthcare logistics, ranging from the physical assets to the inventory of drugs and furnishing, and the corresponding logical records that describe them in IT databases. Virtual RFID readers are included into the 3D environment and both objects and avatars are virtually tagged so that they can be univocally detected whenever they enter a certain reader's field. Data collected by RFID tags are continuously transmitted to an external relational database which feeds a location-aware system for tracking all items in the hospital supply chain. This architectural framework could be successfully used to test the performance of large RFID infrastructure before full-scale deployment, to compare different hospital configurations by means of low-cost simulation and also to train personnel.

The project included many simplified assumptions, especially from the point of view of electromagnetic modeling. Indeed the current RFID virtual system did not account for metals and liquids, which may interfere with the radiation of the readers and of the tags, nor of many capabilities of real EPCglobal-compliant readers. Nevertheless, the study gave an appreciable effort to merge cross disciplines such as Informatics and Electromagnetics with the purpose to develop a valuable platform able to simulate the coming "smart world" where computing is pervasive and people and devices are seamlessly interconnected.

7B. IoT and medical implanted devices

By Stefano Milici
Although the IoT paradigm may provide great advantages in healthcare to patients, care givers, and medical institutions, the impact on public health and safety has to be taken into account seriously. Indeed, the increasing number of radiofrequency emitters, which are densely distributed into daily environments, could cause interferences on pacemakers, defibrillators and other implantable devices. Several studies already addressed the electromagnetic interferences and some of them have recognized RFID systems as possible source of significant clinical interferences because of the generally higher radiated power with respect to other wireless devices (WIFI, BT). An example is reported in [Stachel et al, 2013] concerning the electromagnetic interferences on implantable cardiac rhythm management devices caused by RFID interrogators.

First of all, an effort is required to emulate a real-world condition without involving the real patients. In order to fully characterize the electromagnetic interactions, three different types of human simulators were developed and the emitters were tested on a wide range of RFID frequencies (LF, HF and UHF). The lower-frequency carriers (LF, HF) were shown to cause greater rates of interference, whereas there was no relevant occurrence of interference recorded for UHF signals at all. In addition, they propose an innovative method to reduce interferences by more than 50% by using a ramped amplitude modulation on the transmitting signals.

The outcomes of the study reveal that the RFID signals might in principle cause the failure of the considered implanted device, but the risk looks negligible for UHF systems, and this is a good result since UHF RFID is expected to play a key role in the implementation of IoT networks. As we approach a pervasive IoT, we have also to properly handle potential EMI threats just "by design" or at least to consider proper mitigation procedures for already installed infrastructures.

8. Organizing and Securing RFID-generated Data

RFID devices are formidable generators of data and accordingly of network traffic. An efficient and secure management of such an information stream, accounting also for possible sources of uncertainties and failures, has to be addressed in a vision of networked RFID. The two selected papers address the efficient representation of RFID events (trajectories) in a Cloud architecture in section 8.1 and the authentication requirements and algorithms to achieve secure transactions in section 8.2.

8A. RFID in the cloud

By Valeria Cardellini
With the rapid development of Radio Frequency Identification, sensor and wireless technologies, many organizations are planning to use distributed RFID-enabled traceability systems. As a consequence, a large amount of trajectory data of moving objects is becoming available and procedures for mining useful information from trajectory data are receiving an ever-increasing attention. Since RFID data usually contain a considerable degree of uncertainty caused by various factors, such as hardware flaws, transmission faults and environment instability, objects’ trajectories become incomplete. Efficient approaches, which handle uncertainty in distributed RFID-enabled traceability systems, are hence required to prevent such uncertainty from causing a negative impact on business decisions.

The paper [Wu et al 2014] provides a good review of the state-of-the-art research on uncertainties in RFID-based systems and proposes an efficient trajectory-clustering algorithm with the capability to recover missing RFID readings. The algorithm employs a novel similarity measurement model, which is specifically designed for RFID trajectories, and takes into account variants in both time and space dimensions. The clustering algorithm is a hierarchical one; as a first phase, it clusters the points in a two-dimensional space; then, each cluster in this plane is expanded according to the third dimension, represented by the location. Since the algorithm for the hierarchical clustering of RFID trajectories does not handle the missing readings, the authors propose a second algorithm which performs a merging operation of two sets of trajectories into one set. The authors also discuss the implementation of the clustering algorithm by providing a solution based on Google MapReduce framework. Such solution exploits the intrinsic parallelism of the proposed algorithm and, as expected, turns out to be convenient when the saving in processing time compensates the communication cost paid to transfer the data to the Cloud nodes. The paper gives an interesting example of the fruitful convergence between Internet of Things and Cloud Computing, which can provide the users with the illusion of having infinite resources to efficiently process large amount of data trajectories.

The performance of the proposed approach is analyzed using synthetic and offline data and the experiments demonstrate the scalability and efficiency of the proposed algorithm with respect to existing methods. We observe that it would be beneficial for the research community to have public datasets of RFID trajectories available for performance comparison.

8B. How secure is RFID authentication for IoT?

By Alberto Caponi
Connected medical devices are transforming the way health organizations deliver care and monitor patient's health, both inside the provider facilities as well as in individual homes. Indeed, the IoT technologies are spreading in many health-care applications making monitoring, diagnostics and treatment more personalized, timely and convenient, while also lowering costs. An IoT network could eventually comprise many heterogeneous devices and different applications, including sensors, actuators, micro-controllers, mobile-communication devices and more. Radio-frequency identification is one of the most important technologies used in the IoT as it enables wireless communication with objects, their automatic identification and tracking or even the storage of sensitive data. In such heterogeneous and dynamically-changing networks (which mostly comprise sensors having low computational performances), it is of primary importance to properly handle security issues such as authentication of devices and users and to quantify the impact of cryptographic schemes on these systems.

The paper [He and Zeadally, 2014], carefully discusses the security requirements of RFID authentication, presenting a review of RFID authentication schemes based on Elliptic Curve Cryptography (ECC) in terms of performance and security. None of the reviewed schemes currently provide a suitable security model for RFID systems that demonstrated to be provably secure. Although most of them are still vulnerable to different types of malicious attacks, the authors identified three recently proposed ECC-based authentication schemes that are compliant with all the security requirements at an acceptable computation and communication cost so that to be suitable for IoT applications currently deployed in the health-care environment.

9. Conclusion: Economic and Ethic Impacts

IoT is a technology that may deeply permeate the daily-life of individuals at both the macro and the micro scales, affecting the Economy as well as the Privacy and Ethic dimensions.

From the beginning of its history, one of the mostly used and (ab)-used adjectives commonly associated to RFID systems is "low-cost". Especially in Academic papers, innovative and high performance RFID tags and applications are often praised as extremely cheap solutions, thanks to the absence of batteries and sophisticated electronics and to the easiness of their fabrications, installation and maintenance. Anyway, when technicians approach the real world and try to persuade businessmen and managers about the benefits of RFID investments, all the enthusiastic perspectives start vacillating under the high and unexpected start up costs. The envisaged improvements in terms of company organization, warehouse management and processes have to deal with the current costs of readers, labels, software and network design as well as with the unpleasant feeling that RFID technology is far to be a miraculous cure or a magic wand (section 9.1).

Focusing on the private and emotional dimensions, beside the technology enthusiasts, trans-humanists and people longing to have RFID tags implanted inside their body to express an augmented interaction with things and environments, there is also a minority fringe of a-priori skeptics who consider this new paradigm as something to be forbidden since it is expected to spy on people or collect personal data. Human
being may be monitored and their privacy may be infringed. Hence RFID and IoT technology in general should be prohibited. Colorful images and metaphors like the Mark of the Beast could be relegated to the expression of fanatics but include, in their inside, some still unsolved questions concerning Ethics which refers to a sphere that is complementary to technology, shown in section 9.2.

9A. Long-term economic impact
by Cecilia Occhiuzzi

An interesting analysis on the long-term effects of RFID initiatives has been recently presented in [Chen et al 2014]. In that paper, more than seventy US and non-US companies, with announced RFID investments over the years 1997–2009, have been analyzed in terms of ROA (return of assets), one of the most accepted metrics to quantify the competitive advantage. A list of similar non-RFID adopters has been considered as benchmark over a three years period.

The results are surprising. Contrary to other similar studies, the main conclusion is that there is no sensible difference in term of financial performance between RFID adopters and non-adopters, which may indicate that RFID may not be a critical driver of company’s revenue, at least in the first three years after the investment.

Among all the possible explanations proposed by the authors The authors proposed a number of possible explanations relating that relate the ROA to other factors such as the company’s country, type, financial health and growth potential. One is particularly interesting and underlines evidence is the necessity for RFID technology to be an enabler of opportunities and not only a simple value-creator.

Especially in the IoT perspective, it is necessary to overcome the traditional RFID "logistic" concept in order to move toward more innovative and challenging paradigms. RFID "heavy and expensive" architecture must be considered as a multi-purpose platform able to contemporarily make possible different and independent applications ranging from tracking to sensing, from labeling to secure protection, from access control to living assistance, without additional costs or design efforts. The offer of additional capabilities, besides labeling, will automatically foster its acceptance to a higher level, where the benchmark is not the simple barcode but any other (even if not yet revealed) multi-potent technological device able to offer similar functionalities.

9B. The religious and ethical dimension of RFID and IoT
by Gaetano Marrocco

Researchers of non-technological fields have very recently started a serious discussion [Schmidt and Kessler, 2013] about the Ethic implication of RFID and Internet of Things from the particular perspective of Jewish and Christian theology. This contribution, which looks apparently neutral for an engineer reader, can be appreciated for the will of not to provide a final answer like total prohibition or total free use, while instead to set up a methodology for a long-term analysis.

Ethics are reflections on our behavior and on its moral implications. Teachings from sacred writings produced the well-accepted concepts in many cultures that a leading person may not use his/her power for their own purposes and to the disadvantage of his/her subordinates. All human beings have the same dignity and deserve the same respect. It can be seen as a general norm of inter-human relations. It concerns every human beings private or individual right, including the right to privacy. Of course technology could provide secure encryption of wireless data transmission but profiling would still be possible by persons who are in charge the access to the encrypted data to carry on their job. So who could guarantee that the intended receiver works with this data in a responsible way? Technical means are not sufficient to solve all our data protection and privacy problems.

From a complementary point of view, the development of this new technology requires the development of new laws. But, laws cannot totally prevent technology misuses if the expectation of high profit may encourage people to neglect laws and take the risk of a punishment.

This shows that legal and juridical means are limited.

The authors hence conclude that the need of responsible ethical behavior is rather difficult to enforce and even difficult to measure since it can be only requested on a volunteer basis.

Many applications of RFID and IoT are not related to human beings and inter-human relations since they are pure technical or economical applications. They are useful to improve human activities and in the long run will increase human welfare. All these uses of RFID should not be hindered.

10. References

10A. Pioneering papers on RFID + IoT

Qiu, R.; Zhijun Zhang 2003
Design of enterprise Web servers in support of instant information retrievals

R. Dettmer
What’s in a name [Internet Domain Name System]
IEE Review,

10B. Overview

3 S. Gollakota; M. S. Reynolds; J. R. Smith; D. J. Wetherall 2014
The Emergence of RF-Powered Computing
Computer, 2014

4 S. Amendola; R. Lodato; S. Manzari; C. Occhiuzzi; G. Marrocco 2014
RFID Technology for IoT-Based Personal Healthcare in Smart Spaces
IEEE Internet of Things Journal, 2014

5 Li Da Xu; Wu He; Shancang Li 2014
Internet of Things in Industries: A Survey
IEEE Transaction on Industrial Informatics, 2014

6 K. Michael; G. Roussos; G. Q. Huang; A. Chattopadhyay; R. Gadh 2010
Planetary-Scale RFID Services in an Age of Ubervillance
IEEE, B. S. Prabhu, and Peter Chu, Proceedings of the IEEE, 2010

7 A. Gluhak; S. Krco; M. Nati; D. Pfisterer; N. Mitton; T. Razafindralambo 2011
A Survey on Facilities for Experimental Internet of Things Research
IEEE Communication Magazine, 2011

10C. RFID as sensor nodes of IoT

8 D. De Donno; L. Catarinucci; L. Tarricone 2014
A Battery-Assisted Sensor-Enhanced RFID Tag Enabling Heterogeneous Wireless Sensor Networks

9 S. Roy; V, Jandhyala; J. R. Smith; D.J. Wetherall; B.P. Otis; R. Chakraborty; M. Buettner; D.J. Yeager; You-Chang Ko; A.P. Sample 2010
RFID: From Supply Chains to Sensor Nets
Proceedings of the IEEE, 2010

10 S. Manzari; A. Catin; C. Di Natale; G. Marrocco 2013
Ambient Sensing by Chemical-loaded UHF-RFIDs
Proceedings from the 7th European Conference on Antennas and Propagation (EUCAP 2013), 2013

11 S. Tedjini; N. Karmakar; E. Perret; A Vena; R. Koswatta; R. E-Azim 2013
Hold the Chips: Chipless Technology, an Alternative Technique for RFID
IEEE Microwave Magazine, 2013

10D. RFID Localization Networks

12 Yongtao Ma; Liujii Zhou; Kaihua Liu; Jinlong Wang 2014
Iterative Phase Reconstruction and Weighted Localization Algorithm for Indoor RFID-Based Localization in NLOS Environment

13 Son Huynh; Parry, D.; Fong, A.C.M.; Jie Tang 2014
Novel RFID and ontology based home localization system for misplaced objects
10E. RFID for IoT Healthcare

14 C. W. Thompson; F. Hangstrom 2008
Modeling Healthcare Logistics in a Virtual World
IEEE Internet Computing, 2008

15 J. R. Stachel; E. Sejdic; A. Ogirala; M.H. Mickel
The impact of the internet of Things on implanted medical devices including pacemakers, and ICDs
IEEE int. Conference on Instrumentation and Measurement Tech.(I2MTC),

10F. Networks and Security of RFID-IoT

16 Yanbo Wu; Hong Shen; Quan Z. Sheng 2014
A Cloud-friendly RFID Trajectory Clustering Algorithm in Uncertain Environments
IEEE Transactions on Parallel and Distributed Systems, accepted for publication, 2014

17 D. He; S. Zeadally 2014
An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography
IEEE Internet of Things Journal, 2014

10G. Economic and Ethic impact

18 Chen Xi; Shanshan Liu; I. Bose 2014
Measuring the long term impact on firm performance using ROA: an empirical study of RFID adoption
Int. Conf. Service Systems and Service Management (IXSSSM) 2014, 2014

19 E. W. Schmidt; V. Kessler 2013
Ethical Implications of RFID and Internet of Things seen from a Christian Perspective
Proceedings of 2013 European Conference on Smart Objects, Systems and Technologies (SmartSysTech), 2013