From the Internet of things to the Internet of physical world

Nathalie Mitton, David Simplot-Ryl

From the Internet of things to the Internet of physical world

Nathalie Mitton and David Simplot-Ryl
INRIA Lille -Nord Europe, Univ. Lille 1, CNRS
firstname.lastname@inria.fr

Abstract:

Nowadays, we daily meet new wireless technologies. This is often achieved through the use of RFID (Radio Frequency Identification) tags and wireless sensors. Our environment and surrounding objects become communicating. New applications thus arise in domains such as logistic, health, rescue and environment preservation. Embedding such devices in various industrial goods could lead to a world in which objects communicate and interact with other objects and with people, i.e the so called “Internet of things”. This article describes the various types of RFID tags, and the hot topic for research and some examples of applications are given.

Résumé :

De nos jours, on est confronté de manière banale à des technologies de communication sans fil. C’est souvent le fait de RFID (systèmes d’identification de radio fréquence) et de capteurs sans fils. Notre environnement et les objets qui nous entourent deviennent communicants. De nouvelles applications émergent dans des domaines aussi variés que la logistique, la santé, les sauvetages, la préservation de l’environnement. L’incorporation de tels dispositifs dans des produits industriels pourrait conduire à un monde dans lequel les objets communiquent et interagissent entre eux et avec les humains, c'est-à-dire « l’Internet des objets ». Cet article décrit les différents types de RFID et les sujets brulant de recherche et des exemples d’applications sont donnés.

1 Introduction

Nowadays, we daily meet new wireless, contactless technologies. These latter ones are being invading our everyday life in a natural way. Our environment and surrounding objects become communicating. New applications thus arise in every discipline ranging from logistic and traceability applications to rescue and preventive operations going through health, biology areas, etc.... This is achieved through the use of RFID (Radio Frequency Identification) tags and wireless sensors.

Basic principles of RFID (Radio Frequency IDentification) consist in identifying an object through wireless medium (radiofrequency). A reader queries a tag (basically who is there?) and the tag answers with its identifier. RFID has been mainly declined in two wide areas: passive tags and active tags which aim at different purposes. For each category, advances in technology allow more and more applications and possibilities every day. The tag does not answer its identifier only but can embed additional data. They offer the opportunity to build the *Internet of things*.

The Internet of things paradigm [5] aims to bring intelligent interconnection of objects in the physical world through information sensing devices, such as RFID tags and communicating sensors connected to the global network by using network protocols and information systems. The objects can communicate and interact with other objects and with people. The Internet of things gives a lot of opportunities for new applications which are expected to address many challenges in today’s societies like healthcare monitoring systems, intelligent transportation systems, and smart recycling systems. To make these applications a reality, significant research needs to be conducted which has motivated a voluminous amount of activities in this hot field.

This article is organized as follows. Section 2 describes the different kinds of RFID tags. Section 3 details passive RFID tags functions and uses, while Section 4 describes active tags.

2 Classification of RFID

There exist several kinds of RFID technologies that are classified into 5 categories, as depicted by Figure 1. Functionalities of lower classes are included in higher ones.

- **Class 1:** This class gathers the simpler and cheaper tags. These RFID tags are passive tags which can only be read. That means that they embed no energy source and are encoded only once. The information they hold will never be changed.

- **Class 2:** This second category gathers passive tags which can be read and written. They embed no energy source but the information they embed may be modified by a reader if needed.

- **Class 3**: Category 3 gathers a special kind of RFID tags that are referred as semi-active. They are so called because they embed a battery that can be used only to write data in the tag. Indeed, passive tags are supplied in energy only when they are in the field of a reader. The further the reader, the less energy received by tags. As shown on Figure 2, this impacts the functionalities the reader can use on tags with regards to the distance between the reader and the tag. If the tag is located in the area 2 of Figure 2, i.e. it can be read but not written, the tag can use its own battery to complete the missing energy needed to write in it.

- **Class 4:** RFID of class 4 are active tags. They embed a battery that they can used to send data to another active tag or a reader. They do not need to be powered by the reader communication field to be read. Yet, a set of active tags can be seen as a wireless sensor network in which every entity is able to communicate with each other. The challenge that appears here is to save energy when communicating to prolong the tag lifetime.

- **Class 5**: This last class gathers smart devices that are the readers. These readers must be used to retrieve data hold by tags from classes 1, 2 and 3.

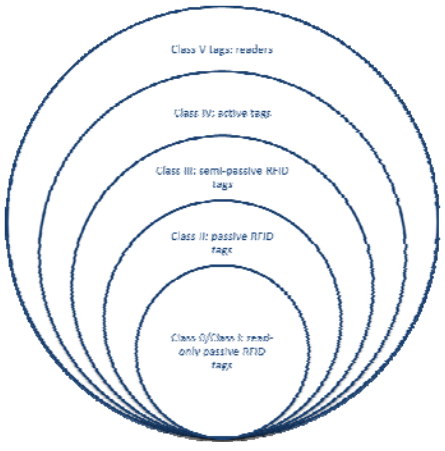


Figure 1: RFID classification

Obviously, the upper class tag the more functionalities it offers but the more expensive. Tags from categories from 1 to 3 are mainly used for the same applications since they need to be powered by a reader. We will have a closer look at these passive and semi-passive tags in Section 3. Active tags (class 4) are the most expensive ones but answers different needs as we will see in Section 4.

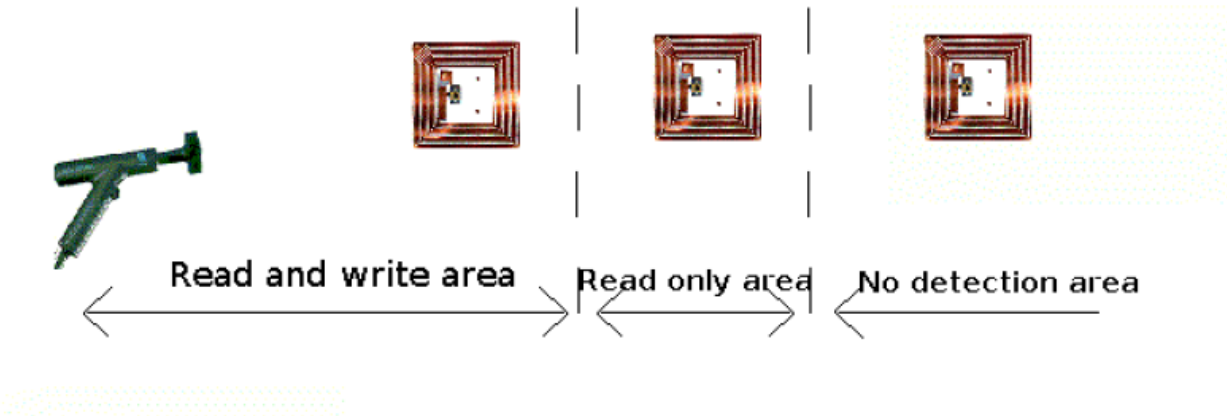


Figure 2: Reading and writing areas. A tag close to the reader receives enough energy to be both read and written. If it gets further from the reader, it can be read but the electromagnetic field is not strong enough to provide enough power to enable the writing. At last, when it gets again further, it exits the reader field and can neither be read nor written.

3 Passive RFID

3.1 History

RFID technology concepts exist for a long time since they appeared in 1940's to identify aircrafts during the war. They then have been widely used by militaries during the cold war to protect and watch sensitive places such as nuclear plants. The technology was transferred to the civil area in 1980. First applications in Europe were for tracking and identifying cattle. RFID, as we know it today, appeared in 1990's when IBM integrated all components on a chip. First applications were for electronic goods surveillance to prevent from robberies in shops. It then experienced a boom these latter years when chips could embed larger quantity of data which enables new applications such as traceability. This great interest led to the need for standards since companies needed system interoperability. This is why EPC Global[10] has been created in 2003 to develop and define standard for RFID tags and middleware's.

3.2 Architecture and principles

Passive tags need to be powered by the electromagnetic field of the reader to deliver the data hey hold. They are composed of a chip and an antenna. The antenna has a double role. It first allows the tag to send and receive data. Second, when in the electromagnetic field of the reader, the antenna generates an electric current which powers the chip, which is thus able to communicate its data. To do so, it opens and closes the antenna, which makes the wave emitted by the reader bounce in a different way and thus it can generate 0 and 1.

3.3 Frequencies and applications

Three main frequencies are used in passive RFID. Each frequency range corresponds to a special RFID behavior and thus matches specific applications.

- Low Frequencies (below150kHz): these frequencies are mainly used for niche applications. Such a frequency allows to better deal with metal and liquid environments. They are used for instance in the vet area. Animals are tagged with such tags.

- High Frequency (HF) -13, 56 MHz: this is one of the most widely used for RFID technology. HF passive tags can be read up to1m in every direction (omnidirectional antenna). It better fits

applications such as shelf inventory and stock management. We now can find it incorporated in skipasses in many ski resorts or in metro tickets in cities like Brussels, Shanghai or Beijing. It is also used for more secured operations since it needs tag proximity, such as passport identification. This frequency has also been declined in NFC technology. Examples of such tags are shown in Figure 3(a).

- Ultra High Frequency (UHF) - 900MHz: this is also a widely used frequency for which EPC standards have been written [10]. UHF RFID tags can be read up to 10 m in a very directional way. This feature makes them very suitable for traceability and logistic applications in pallets tracking in warehouses or luggage sorting in airports such as in Hong-Kong or Lisbon. An example of such a tag is shown on Figure 3(b).

3.4 Advantages and drawbacks

Passive RFID technologies present many advantages. Indeed, RFID can be seen as “electronic bar codes” which do not need objects to be handled one by one. In addition, no direct sight is necessary. More and more information can be stored in tags. Tag reading is quick (a reader can read up to 250 tags per second) [19]. Thanks to technology advances, up to 2kbytes can be stored in a tag with possible data protection by password (the tag will provide its information to the reader if and only if this latter one sends the correct password).

a) HF tag b)UHF tag

Figure 3: Some examples of passive RFID tags (© INRIA / Photo Kaksonen)

Nevertheless, due to their inherent way of functioning, passive RFID suffer from drawbacks. Indeed, electromagnetic fields are disturbed by liquids or metal. This disturbance is more or less strong depending of reader frequency. For instance, low frequencies are very slightly impacted by liquids. This is why low frequency RFID are used for tagging animals (body is mainly composed of water). But this is not the case for HF and UHF technologies, which are the ones which best fit most of applications.

3.5 Challenges

Research for RFID encompasses both hardware and software. For hardware, researches focuses on way to miniaturize tags and how to store more and more data at the same cost and/or the same chip size.

For software, research deals with several issues [7]. About tags themselves, it focuses on the way to query tags while avoiding collisions (i) when two tags in the field of the same reader answer at the same time, (ii) when two reader fields overlap: the tags laying in the overlapping area become dumb. Much work has been done in the former case [3,19,2,13,18,12,14]. Better solutions [18,19] are implemented in the EPC Gen2 [20] and allow to read up to 250 tags per second. In the latter case, only

marginal research has been done.

Another major issue is security and privacy. Indeed, even if data may be protected by a password, this is not always the case. Thus, if each good is equipped with a RFID tag, it can possibly be read anywhere, compromising the privacy of its owner. This is a current important issue that national privacy councils are discussing. Current laws require that the tag is destroyed when exiting a shop except if the customer explicitly asks for keeping it.

At last, another challenge concerns the middleware design. As it has been mentioned, EPC Global is a pretty young organization and standards have not been defined yet for every part of the middleware (so far, only UHF tags have been fully addressed). In addition, several bricks already defined such as the ONS[11] suffer from political and scalability issues and need to be re-visited.

3.6 The RFID in the next years

RFID technology improves day and day. A single RFID tag still remains too expensive (˜10 Euro cents per unit) which limits its use for very large scales applications. Nevertheless, the trade industry is about to label every product for logistics and traceability purposes as soon as the tag cost is lower than˜5 Euro cents per unit. Indeed, using the RFID instead of the bar code improves the quality of inventory report while dividing by 10 the time needed to draw it. This cost will be reached soon with scale effect and thanks to research, like for instance imprinted antenna systems which reduce both cost and ecological impact.

4 Active RFID

Unlike passive ones, active RFID tags are autonomous. They embed their own battery and can use it to send and receive data from peers. They are usually coupled with a sensor (temperature, humidity, etc) and send the sensed data to a central entity. The concept of active RFID (chip with microprocessor and memory, sensor, antenna) thus meets the one of wireless sensor networks. In such networks, sensors communicate between each other through a wireless medium. RFID are spread over an area to cover (a forest, a volcano, a car park, etc) and regularly send their data to a special entity called sink, which gathers every data retrieved by sensors to process them.

4.1 Principles

Sensors are autonomous and able to self-organize and adapt to their environment. The rationale for their use is that they are small, low cost communicating objects that can be dropped in a random way over an area. Individual sensors thus need to self-organize in order to “know” where to send the data they collect. Indeed, since they have a limited energy storage (battery has a finite lifetime and this is not conceivable to change manually battery of each sensor), they can communicate only on small range so that data should travel from sensor to sensor till reaching the sink. Each RFID thus should firstly detect its ’neighbors’,i.e. the other ones which are in communication range and then decide to which one send or forward data. RFID can use various frequencies to communicate ranging from 900 MHz to 2.4 GHz.

4.2 Applications

A wireless sensor network can be used for various purposes and uses. With the advances hardware development, more and more networks applications become feasible.

A first type of application is the one which aim to survey a geographic area. For instance, temperature sensors may be deployed over a forest (by a plane) for fire prevention. When sensors detect a too high temperature they send this information to firemen, who can intervene quickly. Similarly, seismic sensors can be deployed on a volcano and monitor its seismic activity to detect its wake-up. Generally speaking, sensor networks may be useful for many similar applications related to environment surveillance[1] .

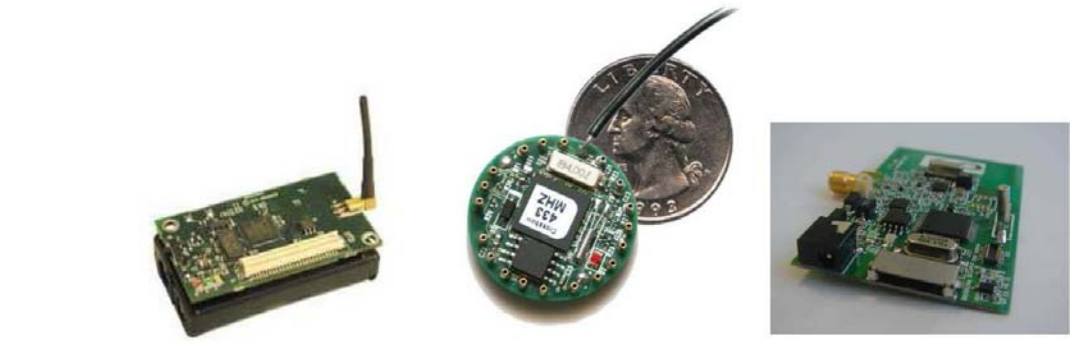
[1] http://www.sti.nasa.gov/tto/Spinoff2008/ct_5.html

Wireless sensor networks are also used for rescue applications. For instance, sensors can be deployed in an underground car park for instance. In case of fire in such an environment, firemen encounter difficulties to locate the fire hearth while temperature sensors can guide them. Sensors can also be embedded in building walls. If the building collapses, the sensors may guide the firemen to trapped people which are detected as heat sources.

Wireless sensor networks can also be deployed to understand and/or track. Wireless sensor networks are for instance used by ethologists who wish to study animal behavior [15]. Animals which are equipped with sensors can be observed remotely. Other studies use wireless sensor networks to understand how infectious diseases propagate [8].

Most recent years have witnessed the apparition of actuators that come to complete sensor. Indeed, actuators can be seen as more powerful than sensors since they can act on their environment. For instance, while sensors detect a fire, actuators can action watering to switch it off. This opens new applications relative for instance to home monitoring and smart building. The building becomes “alive” as each sensor it contains communicates with the others to offer the better services to its occupants. At last, actuators may move like a little robot and can drop off plain sensors. Actuators can then extend the networks they belong to, interacting with it and explore new territories hostile to human being.

Wireless sensor networks present a lot of advantages since they can be useful for many applications. Nevertheless, today, they still present two drawbacks : first their cost a little too high and their environmental impact.



(a) Mica Z -Credit: web.sensor-IC (b) Mica Z -Credit: crossbow (c) WSN430-Credit : INRIA

Figure 4: Some example of sensors.

4.3 Challenges

Research in wireless sensor and actuator networks is related to various topics. First, on hardware, research focuses on the way to miniaturize the sensors at low cost and to design battery with more autonomy and with a minimum impact on the environment. Then, on software, many tracks are followed. Most of them investigate the way to provide efficient algorithms for messages routing from each sensor to one or several sinks or to organize the network over large scales, taking in consideration the nature of the environment (sensors may move if attached to animals for instance) and inherent features of sensors [6,16]. Indeed, sensors are tiny devices with little resources in terms

of energy, computation and memory. Thus, any algorithm designed for such networks requires little memory space for data, small-size code, no complex computing and to use as little energy as possible.

Another research direction focuses on medium access algorithm (MAC) to allow multiple accesses with a minimum of collisions. Most of the outcomes rely on a CSMA (Carrier-Sense Multiple access) with various waiting time managements. More spread algorithms are known as IEEE 802.11[17], IEEE802.15.4 [21] (used in the ZigBee stack) or XMAC[4]. The last research direction is the best way to schedule sensor activity in order to power off some of them, if the area they cover is already covered by some others [9].

Thus, research in the field of wireless sensor networks covers a wide front. The apparition of actuators and the opportunity of using controlled mobility open a new field of research. How to use efficiently this mobility, still considering the limited resources of devices and the requirement to keep the network connected.

Experiments with such networks at large scales are still a challenge. Indeed, hardware and space are needed to deploy sensors. In addition, the code to be launched on sensors needs to be loaded on each sensor individually. To overcome this drawback, some experimenting platforms are appearing like SensLAB[1]. It allows running any experimentation on wireless sensor networks. The interest sparked off by SensLAB shows the craze of people from different disciplines and the need for such tools.

Another important research field is security. How to ensure that malicious nodes will not impact the whole network? And how to ensure that if a node is stolen, the data it contains will not be retrieved by anyone? Many proposals have been made so far inspired by what is done for of smart cards and self healing techniques but the topic remains wide.

5 Conclusions

In this paper, we have presented the research challenges opened by the Internet of Things which was invented for passive RFID tags. Technological advances allow the production of self-powered small devices, equipped with sensing and communicating capabilities. These are known as communicating sensors and they give the opportunity to move from the Internet of Things to Physical World. Indeed, wireless sensor networks appear as efficient tools which are helpful in many sectors. Therefore, they are called to develop and thrive. These research areas are still very active and we note that activity is increasing in the interdisciplinary domain of sensor and actuator networks (SANET) and in particular in the combination of sensor networks and mobile robot fleet.

References

[1] ANR. Very large scale open wireless sensor network testbed. http://www.senslab.info/.

[2] S. Birari and S. Iyer. Pulse : A mac protocol for RFID networks. In Inter. workshop on RFID and Ubiquitous Sensor Networks (USN), Japan, 2005.

[3] M. Bolic, M. Latteux, and D. Simplot-Ryl. Framed aloha based anti-collision protocol for rfid tags. In Proc. SenseID, Australia, 2007.

[4] M. Buettner, G. V. Yee, E. Anderson, and R. Han. X-mac: a short preamble mac protocol for duty-cycled wireless sensor networks. In Proceedings of the 4th international conference on Embedded networked sensor systems, SenSys '06, pages 307–320, New York, NY, USA, 2006. ACM.

[5] H. Chaouchi. Internet of Things. Connecting Objects. Wiley and Sons, January 2010.

[6] E. Elhafsi, N. Mitton, and D. Simplot-Ryl. End-to-end energy efficient geographic path discovery withguaranteeddelivery in adhoc and sensor networks.In Proc. 19th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'08), Cannes, France, 09 2008.

[7] D. Engels and S. Sarma. The reader collision problem. Proc. of IEEE Inter. Conference on Systems, Man and Cybernetics, 2002.

[8] FP6. Mastering hospital antimicrobial resistance. https://www.mosar-sic.org/mosar/ en-GB/, 2007.

[9] A. Gallais and J. Carle. Performance evaluation and enhancement of surface coverage relay protocol. In In Proc. IFIP Networking'08, Singapore, 2008.

[10] EPC Global. Electronic product code global. http://www.epcglobalinc.org.

[11] EPC Global. ONS standards. http://www.epcglobalinc.org/standards/ons, 2008.

[12] J. Ho, D.W. Engels, and S.E. Sarma. Hiq: a hierarchical Q-learning algorithm to solve the reader collision problem. In Inter. Symposium on Applications and the Internet Workshops (SAINT), USA, 2006.

[13] K.-I.Hwang,K.T.Kim,andD.-S.Eom.Dica:Distributed tag accesswith collision-avoidance among mobile RFID readers. In Embedded and Ubiquitous Computing Workshops, Korea, 2006.

[14] S.JainandS.R.Das.CollisionavoidanceinadenseRFID network.In Proc. of the third ACM international workshop on Wireless network testbeds, experimental evaluation and characterization WiNTECH, pages 49–56, San Francisco, USA, 2006.

[15] N-H Liu, C-A Wu, and S-J Hsieh. Long-term animal observation by wireless sensor networks with sound recognition. In Lecture Notes in Computer Science, editor, Wireless Algorithms, Systems, and Applications, volume 5682/2009, pages 1–11, 2009.

[16] N. Mitton, T. Razafindralambo, D. Simplot-Ryl, and I. Stojmenovic. Hector is an energy efficient tree-based optimized routing protocol for wireless networks. In Proc. Int. Conf. on Mobile Ad-hoc and Sensor Networks (MSN 2008), Wuhan, China, December 2008.

[17] IEEE 802.11 Wireless local area networks. Ieee 802.11. http://www.ieee802. org/11/, 1997.

[18] S. Piramuthu. Anticollision algorithm for RFID tags. In Proc. of National Conference on Mobile and Pervasive Computing CoMPC, Chennai, 2008.

[19] D. Simplot-Ryl, I. Stojmenovic, A. Micic, and A. Nayak. A hybrid randomized protocol for RFID tag identification. Sensor Review, 26(2):147–154, 2006.

[20] EPCglobal Standard specification. EPC TM radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz -960 MHz version 1.2.0, 2007.

[21] IEEE 802.15 WPAN Task Group 4 (TG4). Ieee 802.15.4. http://www.ieee802.org/15/ pub/TG4.html, 2006.