Towards the Internet of Things: An Introduction to RFID Technology

Miguel L. Pardal and José Alves Marques

Department of Computer Science and Engineering, Instituto Superior Técnico
Technical University of Lisbon, Av. Rovisco Pais 1, 1049-001 Lisboa, Portugal

Abstract. *Radio frequency identification* (RFID) is an automatic identification technology making its way to *supply chains* in Retail, Pharmaceutical, and other industries.

RFID extends the reach of supply chain information systems in such a way that it will soon be possible and economically feasible to tag valuable physical objects and then to track and trace them, enabling many novel and useful applications.

This paper provides an introduction to RFID for practitioners with a computer science background.

1 Introduction

Radio frequency identification (RFID) [1] is a technology that can be used to tag physical goods, allowing them to be detected and identified automatically. The captured data can be used by information systems to keep their internal data representations more accurate and up-to-date, thereby improving their business function.

RFID is already being used in industries such as [2]: Warehousing; Maintenance; Pharmaceuticals; Medical Devices; Agriculture; Food; Retailing; Defense.

The basic functionality of an RFID system is *asset management*. The fundamental use cases are: identification, alerting, monitoring, authentication. The improved asset visibility can help prevent losses due to spoiling of perishables, theft, and counterfeiting.

If all the benefits of RFID are to materialize, the technology must first be properly understood. In the following sections, this paper describes the working principles of RFID with references for further study.

2 RFID Technology

2.1 Readers and Transponders

RFID communication occurs between readers and transponders (tags). First the reader sends commands, then the tag responds. Figure 1 shows an example of a RFID reader with 2 antennas. Figure 2 shows a tag.

L. Pardal M. and Alves Marques J.
Towards the Internet of Things: An Introduction to RFID Technology.
DOI: 10.5220/0003026100300039
In *Proceedings of the 4th International Workshop on RFID Technology - Concepts, Applications, Challenges (ICEIS 2010)*, page
ISBN: 978-989-8425-11-9

Fig. 1. RFID Antennas and Reader (image courtesy of Alien Technologies).

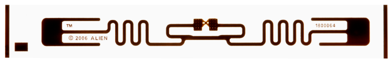

Fig. 2. UHF RFID Tag (image courtesy of Alien Technologies).

2.2 Tag Components

A tag is composed by: Integrated circuit (IC); Antenna; Connection between the IC and the antenna; Substrate on which the antenna resides. Figure 3 shows the different components for a tag manufactured by Rafsec[1].

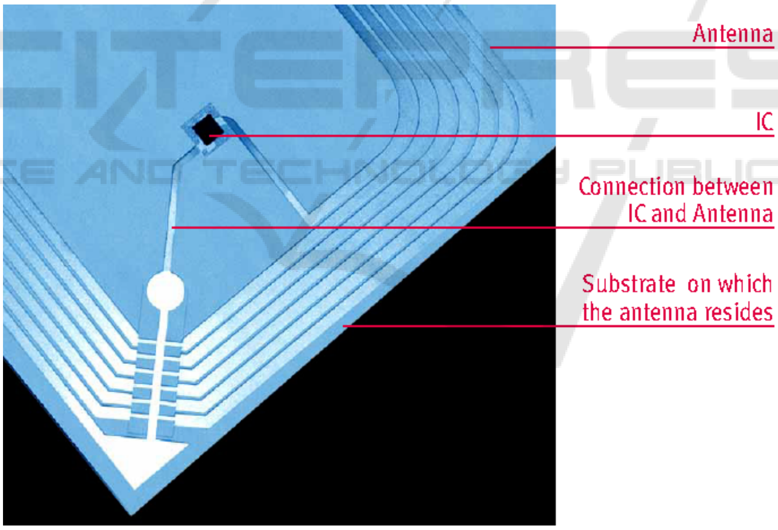
Antenna
IC
Connection between IC and Antenna
Substrate on which the antenna resides

Fig. 3. Tag components (image courtesy of Rafsec OY) [3].

A tag can be protected to endure rough environments that other identification technologies, like bar codes [4], can not.

[1] http://www.upmraflatac.com/

2.3 Tag Categories

There are 3 categories of tags:

- *Passive* or *battery-less* - use only power provided by the RFID reader's signal;
- *Semi-passive* or *battery-assisted* - use a battery to boost response signal;
- *Active* or *battery-powered* - have more power available that allows for additional range, processing capabilities, and autonomy.

Tags with a battery can also use it to operate even when no reader is providing power, for example, to collect temperature or other sensor readings.

2.4 Tag Manufacturing Process

A tag is manufactured in the following steps:

1. Manufacture of the IC;
2. Manufacture of the antenna (the conductive element is shaped to a specific configuration);
3. Assembly of the IC to the antenna:
4. Conversion to package: the antenna with the IC is attached, first to substrate, and then to a package.

The conversion process transforms raw inlay tags into usable form factors such as [5]: printable, metal mount, durable, and battery-assisted.

2.5 Tag Cost

Cost is decisive for the adoption of RFID. The tag is one of the fundamental cost components in a RFID system.

There are many different characteristics that impact tag cost [5]: raw inlay, converted labels, specialty labels, specialty adhesives, encapsulation metal, mount design, user memory, battery, and data pre-encoding. These characteristics can drive tag costs ranging from less than USD 0.1 to USD 10. Tag cost is expected to continue falling in the near future [5].

2.6 Operating Principles

The crucial difference of RFID when compared to other radio technologies, like WLAN[2] and Bluetooth[3], is that the transponder relies on the reader for its power. RFID can work on two distinct principles: "inductive coupling in the electromagnetic near-field with load modulation at LF/HF" or "wave coupling in the electromagnetic far-field with backscatter at UHF/MW".

[2] Wireless Local Area Network. IEEE standard 802.11.

[3] IEEE standard 802.15.1.

Near-Field and Far-Field. The *near-field* is an energy storage field, where energy is preserved, moving from capacitor to the circuit. The *far-field* is an energy propagation field, where the electromagnetic waves would propagate forever, were it not for the absorption losses.

Inductive Coupling and Wave Coupling. *Inductive coupling* works on a electrical transformer principle. The transponder talks back to the reader using load modulation i.e. by interfering with the whole system energy. Inductive coupling is good for short read ranges, and has a greater ability to penetrate objects and to operate in metallic environments. The most common frequencies are in the ranges LF (Low Frequency - 30 to 300 kHz) to HF (High Frequency - 3 to 30 MHz).

Inductive coupling is only practical in the near-field. For the far-field, the magnetic field is replaced by the electromagnetic field.

Wave coupling works on a radar principle. The transponder talks back to the reader using interference. Wave coupling allows much greater reading ranges (up to 100 meters), even though the readings are more erratic because of destructive wave interference. The most common frequencies are in the ranges UHF (Ultra-High Frequency - 300 to 3 000 MHz) and MW (Microwaves - 2.5 to 5.8 GHz).

2.7 Collision Avoidance

When a reader transmits, it broadcasts energy, and it activates all transponders in range. The response data is sent by all at the same time, causing signal collisions.

Transponders do not hear the signals from other transponders, they can only listen to the reader's signal.

The reader must be able to prevent collisions. More information on anti-collision protocols (deterministic and stochastic) can be found in section 7.2 of Finkenzeller [1].

2.8 Spectrum Regulations

RFID uses Industrial, Scientific, and Medical (ISM) radio bands [1]. Radio communication services operating within these bands must accept harmful interference, which may be caused by other applications. The available ISM frequencies are different in Europe, Americas, and Asia. The choice of RFID readers and tags has to take these differences into account.

There is a trade-off in tag manufacturing due to these regional differences [5]: tags designed for use in a particular geography will typically outperform a global tag, because tags either have a high performance at a narrow frequency band or lower performance in a wider frequency range.

3 RFID Software

RFID systems can cross geographic regions and trust boundaries. In *small, closed* systems everything can be controlled by the same organization and rules can be dictated centrally. In *large, open* systems there are multiple authorities, but the system still needs rules to function properly. For this reason, standards play a central role in RFID software.

3.1 Standards

GS1 Identifiers. GS1[4] is the standards organization that oversees *bar code* use in the world. It defines a set of *identifiers* that are widely used and very useful for business applications. Two of the most important GS1 identifiers are the GTIN and the GLN.

A *GTIN (Global Trade Item Number)* is used to identify any item upon which there is a need to retrieve predefined information and that may be priced or ordered or invoiced at any point in a supply chain.

A *GLN (Global Location Number)* is used for location: physical, functional or legal entities requiring a permanent identification, such as a company, department, or warehouse.

These identifiers can be extended with serial numbers to create unique identifiers for individual products and locations. The serialized identifiers are called SGTIN and SGLN, respectively.

EPC Standards. EPCglobal Inc.[5] is a subsidiary of GS1. It defines specifications and provides services based on the Electronic Product Code (EPC), a globally unique serial identifier for RFID tags. The specifications encompass hardware, software, and data.

The EPCglobal Architecture Framework [6] is a collection of interrelated standards, represented in figure 4, for the exchange of data and physical objects between companies.

The Application Level Events (ALE) [7] specifies a software interface through which client applications may access filtered, consolidated, real-time EPC data from multiple reader sources. The data is processed using low-complexity rules (e.g. wildcards). The ALE interface also allows applications to read and write RFID tags, interacting with one or more RFID reader devices.

The EPC Information Services (EPCIS) [8] specification is concerned with recording business events. EPCIS is responsible for capturing data coming from ALE, adding business context to it, and creating events that are made available for querying or subscription.

The Object Naming Service (ONS) [9] extends DNS [10] to resolve EPC codes. It receives a product code and returns the network location of data and services about that product, provided by the company that issued the EPC code.

3.2 Software

Floerkemeier [11] presents a thorough list of RFID software requirements and constraints, based on the results of field-tests conducted for the implementation of *Fosstrak*

[4] http://www.gs1.org/

[5] http://www.epcglobalinc.org/

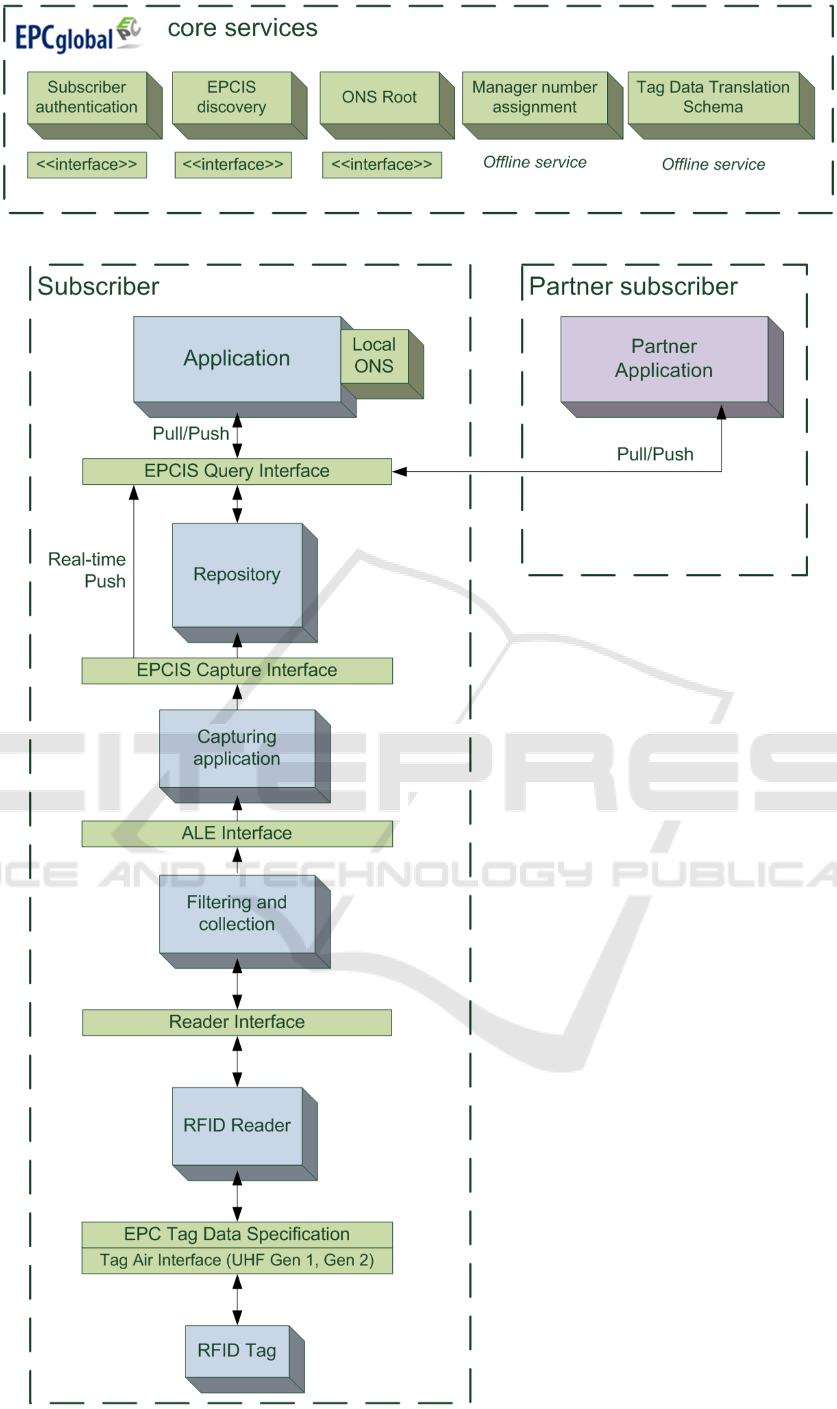

Fig. 4. Overview of the EPC Architecture Framework.

(Free and Open Source Software for track and trace)[6], the first open-source implementation of the EPC framework software. The most important requirements and constraints are summarized next.

Requirements:

- Data dissemination - information captured by a reader is of interest to multiple applications inside and outside the company. There is a need to support asynchronous and synchronous messaging because different applications require different latencies;
- Data aggregation - data may be: *time*-aggregated - e.g. items detected in the last minute, appearing/disappearing items; *space*-aggregated - e.g. items detected by multiple readers at same location; *count*-aggregated - e.g. product type totals;
- Data filtering - data may be filtered into subsets based on tag identity, tag memory, reader antenna, reader identifier, etc;

Constraints:

- Reliability - false negative reads can be caused by interference or absorption by objects. False positives reads can happen when tags are detected outside the typical range of a reader;
- Heterogeneous readers - reading devices with diverse computing and networking capabilities;
- Reader collisions - requires coordination to avoid collisions without missing tags;
- Limited communication - the bandwidth available per channel limits the data rate between readers and tags.

4 Security in RFID

4.1 Threats

Garfinkel [12] presents a taxonomy of RFID threats:

- Threats to company data security: espionage of supply chain flows, denial-of-service via radio jamming, access to competitor's marketing data, widening of trust perimeter;
- Threats to personal privacy: association of a person with a tag (single tag or a set/constellation of tags), exposure of preferences (by carried objects), location tracking, action detection (by object transactions).

Attack Model. Typical computer and network security attack models [13] can be significantly relaxed to accurately reflect real-world threats and real-world tag capabilities. For example, RFID attackers do not have access to a tag at all times, but only for limited time (in the order of minutes and seconds). This makes some brute-force attacks impractical and allows for simpler security mechanisms to be effective.

[6] http://www.fosstrak.org/

4.2 Authentication and Privacy

Juels [13] identified two major RFID security concerns: authentication and privacy.

RFID authentication issues are caused by well-behaving readers harvesting information from misbehaving tags. The security goal is to make sure that the tag is authentic. This goal can be achieved with: password, or yoking (recording tag evidence tracks in a trusted third party). However, tag cloning is hard to prevent because all tags are sensible to reverse-engineering procedures, like timing attacks, and power analysis.

RFID privacy concerns are caused by misbehaving readers harvesting information from well-behaving tags. The security goal is to prevent tag data from being read by someone not authorized to do so. This goal can be achieved through: physical protection (shielded containers or jamming devices), tag killing (to prevent further use), tag sleeping (to suspend use temporarily), or tag renaming (one tag can have a set of aliases).

Advanced Tags. Advanced tags can perform limited symmetric-key cryptographic operations, but have a significantly higher cost. For these tags, *challenge-response* mechanisms are feasible and can be used both for privacy and for authentication purposes.

The big challenge of this approach is the key management, and the computational cost of key search.

There is on-going research on probabilist algorithms to introduce intentional noise in tag to reader communications, to force attackers to spend considerable time in close proximity to target. This is an example of how to leverage the weakened attack model mentioned earlier.

4.3 Infrastructure Security

Fabian [14] makes the point that even if RFID tag security mechanisms are in place, there are many attacks possible on the EPC information infrastructure. Attackers can intercept unprotected ONS, EPCIS, and Discovery service queries. The query contents expose data about product and raw material flows, and other sensitive business information.

The main privacy enhancing strategy is creating *anonymous mixes* i.e. obfuscating the source of queries by bundling together many queries from diverse clients. This makes extracting inside information much more difficult, but not impossible.

5 Conclusions

RFID technology is at a mature stage of development, with increasing adoption in many industries. However, RFID is not a single technology but a suite of technologies. The choice of the “right” tags and readers must be made considering the end-application’s requirements and working environment.

There is a trade-off between tag *cost*, *range* and *functionality*. Current technology allows the choice of 2 of these 3 features [3] [15].

Many improvements have been achieved in the manufacturing of tags and soon cost will no longer be a significant obstacle for most RFID deployments. Passive tags are the least expensive to manufacture and are the best suited for supply chains and other large volume applications.

The most relevant back-end software and standards are described in the EPC framework. However, there is still a need for RFID system design practices that capture business requirements and then translate them into artifacts implemented across all levels of the system: tag, reader, middleware, and applications.

The physical locations have a significant impact on the system design choices. One of the key points is the need for reader coordination because of limited channels and bandwidth. This need is not obvious for practitioners with a computer science background, but it collapses the "all readers read all tags at all times" mindset.

Security is a critical requirement for most applications. Both user concerns and legal regulations have to be taken into account. All existing solutions have trade-offs between tag cost and key management costs, so a careful analysis is required for each end-application to choose a suitable security scheme.

5.1 Looking Ahead: The Internet of things

RFID makes it possible to extend the fundamental abstraction of the World Wide Web - *"everything is a resource, and any resource can link to other resources"* - to the physical world: a tagged object can become the anchor or target of an *hyperlink*.

Eventually every interesting physical object in the world will be connected to the network, opening up the possibility for an Internet of Things (IoT). Fleisch [16] identifies the key traits of the IoT, that will set it apart from the current Internet:

1. It will be machine-centric rather than user-centric;
2. It will connect low-end and low energy consumption devices;
3. It will have trillions (10^{12}) rather then billions (10^{9}) of network nodes;
4. The communication with the low-end devices will be restricted to narrow bandwidth;
5. It will require a lightweight global standard protocol for identification and addressing.

Much research is still needed to make the IoT a reality, but RFID technology will surely be a part of it.

Acknowledgements

The authors acknowledge Prof. Sanjay Sarma, Dr. Christian Floerkemeier, and Rahul Bhattacharyya for their invaluable input for this paper.

The authors also thank Prof. Luís E. T. Rodrigues.

Miguel L. Pardal is supported by a PhD fellowship from the Portuguese Foundation for Science and Technology FCT (SFRH/BD/45289/2008).

References

1. K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 2nd ed. John Wiley & Sons, Ltd, 2003.
2. E. W. Schuster, S. J. Allen, and D. L. Brock, Global RFID: The value of the EPCglobal network for supply chain management. Springer, 2007. [Online]. Available: http://www.amazon.com/Global-RFID-EPCglobal-Network-Management/dp/3540356541
3. S. Sarma, “Towards the 5 cent tag,” MIT Auto-ID Center, Tech. Rep., 11 2001.
4. D. Hunt, A. Puglia, and M. Puglia, RFID: A Guide to Radio Frequency Identification. Wiley, 2007.
5. “RFID tag pricing guide,” ODIN Technologies, Tech. Rep., 05 2009.
6. K. Traub, F. Armenio, H. Barthel, L. Burstein, P. Dietrich, J. Duker, J. Garrett, B. Hogan, O. Ryaboy, S. Sarma, J. Schmidt, K. Suen, and J. Williams, The EPCglobal Architecture Framework 1.2, GS1 Std., 09 2007. [Online]. Available: http://www.epcglobalinc.org/standards/architecture/
7. EPCglobal, Application Level Events (ALE) Specification 1.1, GS1 Std., 02 2008. [Online]. Available: http://www.epcglobalinc.org/standards/ale
8. ——, EPC Information Services (EPCIS) 1.0.1 Specification, GS1 Std., 09 2007. [Online]. Available: http://www.epcglobalinc.org/standards/epcis
9. ——, Object Name Service (ONS) 1.0.1, GS1 Std., 05 2008. [Online]. Available: http://www.epcglobalinc.org/standards/ons
10. P. Albitz and C. Liu, DNS and BIND, 5th ed. O’Reilly Media, Inc., May 2006. [Online]. Available: http://proquest.safaribooksonline.com/0596100574
11. C. Floerkemeier, C. Roduner, and M. Lampe, “RFID application development with the Accada middleware platform,” IEEE Systems Journal, Special Issue on RFID Technology, 12 2007. [Online]. Available: http://www.fosstrak.org/publ/FosstrakIEEESystems.pdf
12. S. L. Garfinkel, A. Juels, and R. Pappu, “RFID privacy: An overview of problems and proposed solutions,” IEEE Security and Privacy, vol. 3, pp. 34–43, 2005.
13. A. Juels, “RFID security and privacy: a research survey,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381–394, 02 2006.
14. B. Fabian, O. Gunther, and S. Spiekermann, “Security analysis of the object name service,” in 3rd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SECPerU), 07 2005. [Online]. Available: http://lasecwww.epfl.ch/ gavoine/download/papers/FabianGS-2005-sptpuc.pdf
15. G. Swamy and S. Sarma, “Manufacturing cost simulations for low cost RFID systems,” MIT Auto-ID Center, Tech. Rep., 2003.
16. E. Fleisch, “What is the Internet of Things? an economic perspective,” ETH Zurich / University of St. Gallen Auto-ID Labs, Tech. Rep., 01 2010.