Research Trends in RFID Technology

Charles Mutigwe and Farhad Aghdasi
School of Electrical and Computer Systems Engineering
Central University of Technology, Free State, South Africa
Email: *cmutigwe@ieee.org, faghdasi@cut.ac.za*

Abstract

While the adoption rate of Radio Frequency Identification (RFID) technology is increasing, mass-market adoption will not be achieved until a few major challenges are addressed. These challenges are: privacy, security and costs from the end-user's view point and limited power supply to the tag from the engineering perspective. We discuss the research efforts aimed at addressing these challenges. We focus our attention on research in: RFID privacy and security, antennas, polymer electronics-based RFID devices, power management circuits and techniques, and efficient RF spectrum utilization. We conclude by drawing attention to three additional areas that we believe are in need of more research.

1. Introduction

A Radio Frequency Identification (RFID) system consists of one or more tags (or transponders) that store data and transfer the data to one or more readers (or interrogators) over a wireless interface. In practical RFID systems the readers are networked to a wider enterprise computer system. The main function of an RFID system is to enable tagged items or persons to automatically state their identity to other systems wirelessly. Like most of today's technologies that are based on cutting-edge research, RFID technology is both very promising and controversial. As a result this technology is rapidly expanding in some areas, while in other areas it has failed to make significant headway thus far.

Advances in RFID technology are dependent on contributions from many areas such as: *device physics* and *molecular electronics* for fabrication, *electromagnetic field theory* for device operations, *mathematics* and *computer science* for data processing and security, and *operations research* for supply chain management.

1.1 Motivation for paper

Given the breath of the fields contributing to RFID technology and the fast changing nature of the technology it is difficult for students and others who want to begin research in this area to find a comprehensive survey of the entire landscape. As outlined in the next section some good survey papers on some particular aspects of the technology do exist, but no source exists where a new researcher can get an overview of the main research efforts taking place in the field as a whole in order to help determine where one might want to focus one's research.

1.2 Organization of the Paper

The remainder of the paper is organized as follows; in Section 2 we review related work and discuss our contributions. The next two sections form the crux of the paper, in Section 3 we outline the primary challenges for RFID technology today, and then in Section 4 we discuss the main research efforts related to RFID. We conclude with a few remarks in Section 5.

2. Related Work

Arguably the most comprehensive single source on the subject of RFID technology is the book by Finkenzeller (2003) that covers the physical principles of RFID systems and issues related to RFID data processing. Hassan and Chatterjee (2006) present a taxonomy for RFID, we have compiled the figures in their paper into a single hierarchical chart that we present as an appendix in Section 7, in order to try and show the breath of this field. Juels (2006) gives a comprehensive survey of the security and privacy issues related to RFID, while Shih *et al.* (2006) present a survey and taxonomy of RFID anti-collision protocols. Abraham *et al.* (n.d.), also present a survey paper focusing on anti-collision protocols for RFID systems and how these systems can be used in inventory management applications.

2.1 Our Contributions

In this paper we look at on-going research activities in the RFID field as a whole and begin by discussing the major challenges that RFID technology is facing today and next we discuss the research efforts that are underway to try and address these challenges. We also draw attention to three areas that we believe need more research in order for the goal of wide spread adoption of this technology to be achieved. In this work we aim to illustrate the inter-disciplinary nature of the research contributions to this technology.

3. Challenges for RFID

While the number of RFID implementations continues to grow at a rapid pace, mass-market adoption of this technology is being hampered by:

- *Privacy* concerns in the form of clandestine tracking and inventorying of tagged items and *security* concerns related to authentication of tags and readers (Juels 2006). For individuals, the limited privacy protection in current RFID systems is the major concern, as the article by Zappone (2007) shows. For the corporate executive, the limited privacy protection in many of RFID systems in place today can leave the entire supply chain exposed to industrial espionage, while the security vulnerabilities can lead to counterfeiting and other acts of economic sabotage.
- The high *costs* of the tags and readers. Current projections are to have tags that cost about 5 US cents each in order to facilitate wider adoption of RFID for

tagging individual items. It appears that the target of 5 US cents per tag (Sarma 2001) is arbitrary, as our attempts to find an economic justification for this target have failed and so costs may not be as a big a drawback on wider adoption as some might be claiming.

- The constrained electrical *power supply* for the mass-market components of the RFID systems; that is the tags. This is directly related to the first two issues above. Low cost tags are for the most part *passive*; they do not have an on-board power source, they derive their power from the signal sent by the interrogating reader. As a result they generally are, smaller in size, chip-less, easier to manufacture and to apply onto products and require no in-field maintenance. However, they have lower transmission ranges and are cryptographically-weak. *Active* tags have an on-board power source and, when appropriately configured, address all the weaknesses of their passive counterparts; however they have as weaknesses all the strengths of their passive counterparts. The power characteristics of the tags influence the frequency and potential applications of an RFID system, as the table below shows.

	Frequency	**Distance**	**Example Application**
LF	125 - 134 KHz	Few cm	Vehicle Immobilizer
HF	13.56 MHz	1m	Building Access, Smart cards
UHF	860 - 930MHz	~ 3m	Supply Chain and logistics
microwave	2.45 GHz	10m	Traffic toll collections

Table 1. RFID Frequencies

In this paper, unless otherwise specified when we say RFID system, we are referring to a system with *passive* tags.

- The limited capabilities of current *information technology systems* to handle the large data sets generated by RFID systems when deployed widely (Chawathe *et al.* 2004). The vision of most RFID enthusiasts in the operations management world is that RFID systems will facilitate the real-time tracking of physical items in the supply chain, thus the physical flow of the item will be matched with the information flow in the enterprises' information management systems (Henry 2005). The data will flow up from the tagged item and its present location to the enterprise information management systems.
- *Social and legal issues*, such as the health implications of continuous exposure to electro-magnetic waves, if and when all items carry an RFID tag and the fact that currently the allocation electromagnetic spectrum bandwidth for RFID systems is determined on a country by country basis.

4. Research Areas

In this section we present current RFID-related research initiatives aimed at addressing the challenges listed above. The list of research initiatives discussed below were primarily drawn from the list presented by Furness (*c*. 2006) and shown in Figure 1

below, we have however added a few more areas to this list.

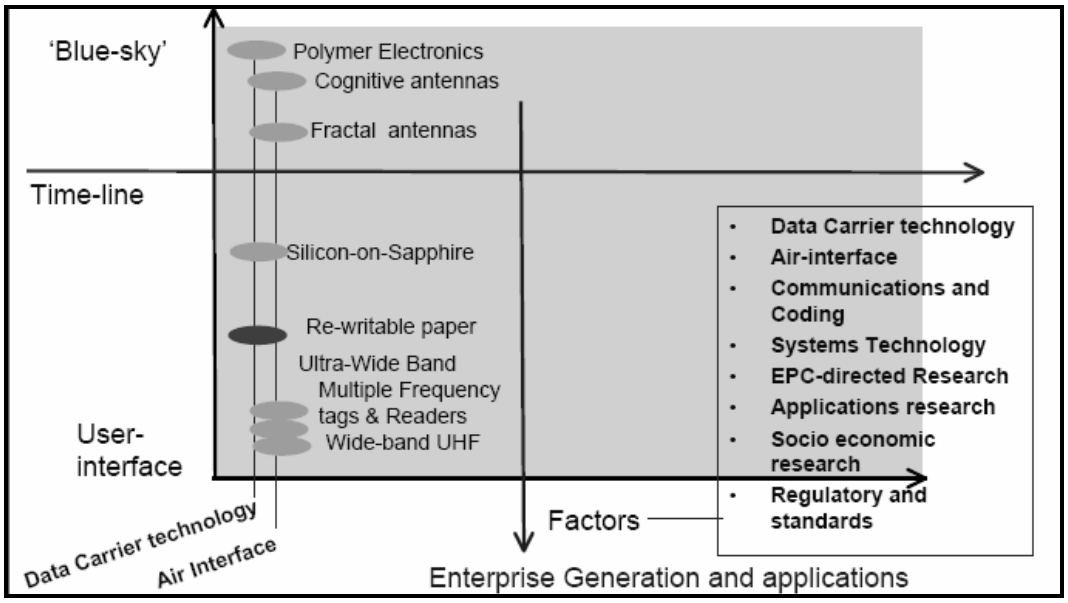


Figure 1. Research continuum and feature space (Furness *c.* 2006: 5).

4.1 Privacy and Security

As Zappone's (2007) article infers, RFID systems have become synonymous with "insecure" systems, a situation that must be thoroughly addressed before it severely limits widespread deployment of RFID systems. Research in security and privacy is arguably the most active area in RFID research at the moment. This view is backed by an inspection of the publication dates of papers in Avoine's RFID security bibliography, which shows the number of RFID security-related publications growing annually from 1 in 2002 to 65 in 2006 (Avione 2007). Juels surveys the current research in this area, the components receiving the most attention are the tags; he categorizes them as basic RFID tags, which are passive, chipless tags, and symmetric RFID tags, which are primarily active, chip-based tags (2006). RFID system designs where tags promiscuously surrender their identity when queried by any interrogator operating at the appropriate frequency cannot be tolerated in a secure environment. A multi-step authentication process is required in order to create a secure channel of communication between the tag and the interrogator. Batina *et al.* (2006) and others have gone further and proposed custom RFID cryptographic processors for this task.

Most research in this area is focused on symmetric RFID tags and involves attempts to develop the ideal security model and the ideal protocol that is both secure and privacy-preserving. The prevailing view is that passive or chipless tags cannot be truly secured, a position that is strengthened by Oren and Shamir's recent demonstration of a side-channel attack on EPC Class 1 (or passive) RFID tags and also their assertion that this attack could have been accomplished using cell phones (2006).

Other research in this area is focused on hybrid implementations consisting of an RFID system and a biometric or an image/voice recognition system.

4.2 Antennas

For an RFID system to operate the tag has to receive a signal of sufficient strength from the reader, while the reader must be sensitive enough to capture the tag's weaker response. The tag and reader in an RFID system can be coupled in one of two ways: either through reactive coupling (*near-field*) or by the propagation of an electromagnetic field (*far-field*). Reactively coupled systems typically use inductive coupling. In inductively coupled systems the magnetic component of the field dominates and is used to carry the data and energy between the reader and the tag using the appropriate modulation techniques. Inductively coupled systems do not require "line-of-site" readings, however they have a very short range, typically less than 1 meter, their field strength is inversely proportional to the cube of the distance between reader and tag. Far-field or propagation systems operate at UHF frequencies and above. For these systems the electric component of the field dominates and they have a much longer range and their field strength is inversely proportional to the square of the distance between reader and tag and furthermore these signals can penetrate dielectric materials (AIM UK n.d.). However, far-field systems often require "line-of-site" readings as the operating frequency increases.

The coupling between the tag and reader is dependent on their antenna structures, as these determine the shape and other attributes of the radiated or captured fields. Fractal antennas are an active area of research. Fractals are objects or quantities that display self-similarity (Weisstein 1999). Figure 2 shows an example of a fractal structure that is constructed iteratively.

Figure 2. Iterations of the Sierpinski gasket.

In the figure each iteration starting from the left is a fractal of higher order. The higher the order of the fractal (Heder *et al.* 2005):

- The higher the number of resonant frequencies, i.e. where maximum energy transfer can occur between the reader and the tag.
- The wider the bandwidth of the centre frequency.
- The lower the first resonant frequency.

This multi-band behavior of fractal antennas is desirable in RFID systems as it offers an opportunity to develop readers or tags that operate at multiple frequencies using a single antenna. An equally important property of fractal antennas is their space-filling behavior that can be used to miniaturize the antenna (Giavittorio, and Rahmat-Samii 2002). This research is beginning to show positive results as recent test have demonstrated that fractal

antenna provide a better read range for UHF RFID readers (Ukkonem, Sydänheimo, and Kivikoski 2007).

Another area of research in antennas with potential benefits to RFID systems is that of cognitive antennas. These are antennas that can reconfigure their spatial transmit and receive characteristics on demand.

4.3 Organic / Polymer Electronics

Some polymers exhibit conducting or semiconducting electrical properties, and of particular interest are semiconducting polymers called conjugate polymers (Friend 1990). The key advantages of polymers (Samuel 2000) are that:

- They are easy to shape and process.
- Their properties can be tuned by modifying their structures or processing.
- They can be doped (this applies to conjugate polymers only).

Based, in part, on these properties, it is expected that the manufacturing costs of polymer-based electronic devices will be considerably less than those for silicon-based devices. It is expected that polymer electronics is going to transform the electronics industry (Hofstraat 2001); to date it has been successfully applied in the area of displays as exemplified by the variety of commercially available rollable polymer electronic display products from Polymer Vision (2007). Significant research is taking place to try and produce polymer electronics through the inkjet printing process (Molesa 2006) it is expected that this process will reduce the manufacturing costs dramatically.

Research on polymer-based RFID devices is an active area; Cui *et al.* (2005) successfully used commercial ink-jet printers in the fabrication of all polymer RC filters, Redinger *et al.* (2004) proposed an ink-jet process to deposit RFID components, while Baude *et al.* (2003) have developed polymer-based RFID circuits. Printed organic RFID systems are now in the field trials stages of commercialization (Clarke 2007).

4.4 Power Management

Research targeting the constrained power availability for RFID tags is being addressed on two fronts, the first is attempting to maximize the energy transferred to the tag by the reader and this is also related to the antennas discussion above, while the other is related to developing low-power circuits that can have increased functionality on the same low power budgets available today.

4.4.1 Wireless Energy Transfers

Research in the area of maximizing energy transfers is focused on non-radiative (*near-field*) energy transfers and recent results from Kurs *et al.* (2007) are very promising for applications such as RFID. Techniques on radiative (*far-field*) energy transfers are quite well developed (Brown 1984), however these are of limited applicability to RFID systems owing to health exposure risks and other concerns and also the fact that these systems are very dependent on line-of-sight arrangements between the reader and tags.

4.4.2 Silicon-On-Sapphire and Other CMOS Devices

Replacing the traditional silicon substrate with sapphire has been found to result in CMOS circuits with "superb thermal conductivity and excellent high speed device characteristics" (Andreou *et al.* 2001: 23). The silicon-on-sapphire (SOS) devices are a subset of the silicon-on-insulator (SOI) devices. Some SOI devices have been reported to operate at frequencies of up to 100GHz (Wann *et al.* 1998). The advantage of SOI processes over bulk CMOS according to Andreou *et al.* (2001: 24) are:

- reduced short channel effects
- reduced parasitic capacitances
- reduced body effect (transconductance degradation)
- reduced latch-up
- reduced leakage currents due to lower area parasitic junctions
- ultra low noise figure

Or briefly stated these devices "perform high-speed operations while consuming low amounts of power" (Nakamura, Matsuhashi, and Nagatomo 2004: 66) and are ideal for RF operations. An added feature is that they are also ultra thin. Figure 3 shows the Peregrine Semiconductor Inc.'s Ultra thin SOS CMOS process compared to a standard bulk CMOS Process.

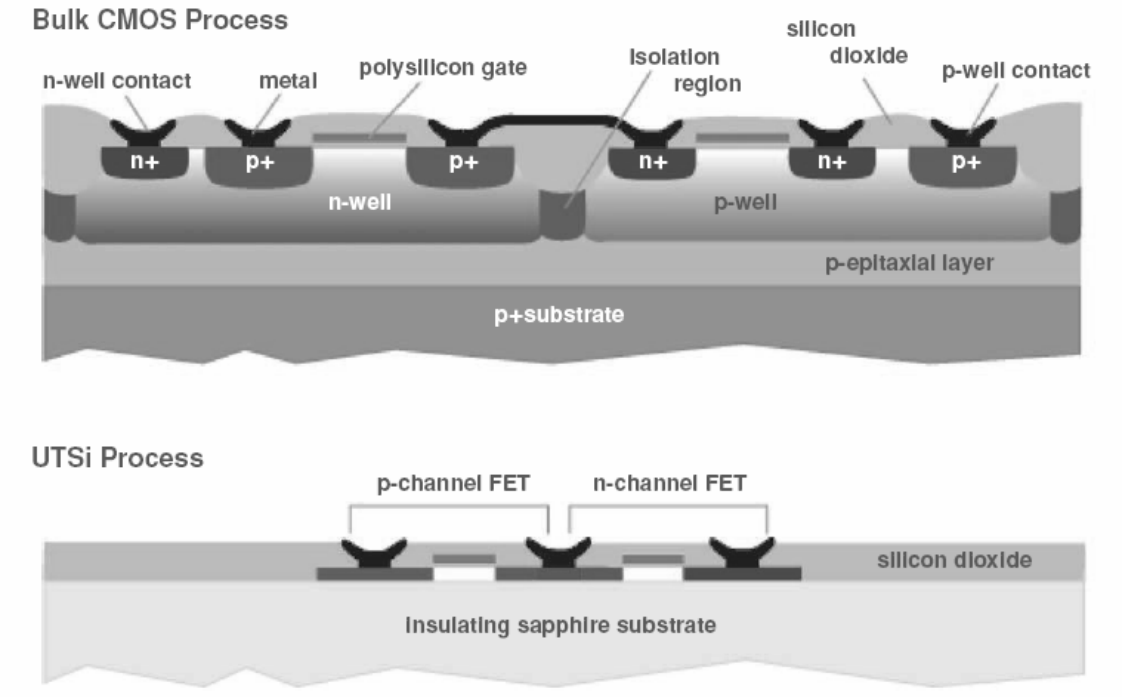


Figure 3. Ultra thin silicon on sapphire CMOS process compared to a standard bulk CMOS Process (Andreou *et al.* 2001: 24).

It should be noted however, that Lam *et al.* (2001) have questioned the benefits of SOS technology over the traditional bulk CMOS process.

4.4.3 Asynchronous Circuits

In most standard CMOS circuits, the dynamic component of the power equation is dominant and it is directly proportional to the clock frequency (Rabaey, Chandrakasan, and Nikolic 2003: 602).
An asynchronous circuit is one that does not have a global clock to synchronize all its activities. According to Sparsø and Furber (2001: 3-4) asynchronous circuits offer the following potential benefits over their synchronous counterparts:
- *Low power consumption*, due to fine-grain clock gating and zero standby power consumption.
- *High operating speed*, as operating speed is determined by actual local latencies rather than global worst case latency.
- *Less emission of electromagnetic noise*, because the local clocks tend to tick at random points in time.
- *Robustness towards variations in supply voltage, temperature, and fabrication process parameters*, because timing is based on matched delays (and can even be insensitive to circuit and wire delays).

However, these potential benefits have to be balanced against the area, circuit speed and power consumption penalties incurred by the control logic for the handshaking between asynchronous modules. In general asynchronous circuits are larger than their synchronous counterparts.

Research is taking place in this area with the aim of adding functionality to the RFID tags while lowering their power consumption.

4.5 Efficient Spectrum Utilization

The spectrum of frequencies available for RFID applications is limited and allocated by various national and regional regulatory authorities. Given this limited bandwidth and the variability of operating frequencies, most RFID readers have to operate at multiple frequencies and the communication protocols between the readers and tags have to utilize the available spectrum efficiently. Marsh has shown that *tag-talk-first* RFID protocols are more efficient at utilizing the available spectrum than *reader-talks-first* protocols (Marsh 2007). However, as we will show in an upcoming paper, systems based on the *tag-talk-first* protocols are not only difficult to secure, but they are not privacy-preserving. As a result trade-offs will need to be made between maximizing privacy and security and maximizing spectral utilization. Research in this area is also related to the antennas discussion above.

As more RFID systems are implemented the available bandwidth becomes over-utilized and message collisions between readers and between tags increase, resulting in lower overall system performance. To address these concerns research is on-going in the areas of tag anti-collision protocols (Shih *et al.* 2006) and the RFID reader collision problem (Engels, and Sarma 2002, Leong, Ng, and Cole 2005).

4.6 IT Infrastructure and Data Management

In order to gain maximum benefits from RFID technology, implementations will need to be fully integrated to the enterprise IT infrastructure. The RFID systems act as data sources (or inputs) into this infrastructure; however when tags are incorporated into sensors and other devices then the tagged item can act as a network node with data flowing in both directions between the node and the backend servers. The amount of data generated by an RFID system is a function of the number of tagged items, the number of readers in the supply chain and the security protocol used if any. This data needs to be sent to backend systems where it is 'scrubbed' in order to deal with issues, such as multiple reads of an item at a given location.

Several privacy-preserving security protocols have been proposed that rely on the tag identifier being stored in a central database, while the tag stores a key or PIN that is linked by some mathematical function to the tag identifier (Weis *et al.* 2003, Ohkubo, Suzuki, and Kinoshita 2004, Dimitiou 2005). The key stored on the tags changes 'randomly', typically after each response to a query from the reader, thus providing anonymity for the tag. The central database in these security schemes is required to be available at all times, hence these schemes are also referred to as online security protocols. This last condition will further strain network resources for systems adopting these online security protocols. These security protocols will need to be studied from a network scalability and availability perspective.

The Electronic Product Code Information Services (EPCIS) standard by EPCglobal allows for seamless interchange of RFID information across and within organizations (EPCglobal 2007). However, this standard is based on sharing data from Class 1 tags and as Oren and Shamir (2006) have already demonstrated this process is not secure. The interchange of RFID information between business partners in an environment with secure RFID systems is an area that still requires some research, once the secure RFID systems have been developed. Further study is also required in order to address issues such as:

- Occasional missed reads of a tagged item in a supply chain with multiple-tracking locations, resulting in a partially complete tracking record for the tagged item.
- Evaluating the capabilities of existing networking protocols' to handle the mass-market adoption of RFID systems.

4.7 Analytics and Enterprise Use of RFID Data

Data from RFID systems provides a three-dimensional view (product, spatial and temporal) of an item at a minimum; the tag ID identifies the product, the reader provides the location where the tag was read and the time when the tag was read. Each data dimension can be used individually or in aggregate to track items. Further data dimensions can be provided by adding more memory to the tag to enable tracking of

additional states, such as manufacture date or expiration date. More research is required in order to look at ways to:

- Utilize this data to improve business functions, such as supply chain management and product pricing.
- Combine and present these data dimensions in meaningful ways to potential users, in order to facilitate better business decisions.

4.8 Consumer Post-Purchase Uses

Mass-market adoption of RFID will have to be driven by consumer demand. For the consumer there is a delivered value versus acceptable risk (in terms of privacy, costs, safety and other concerns) equation and any successful RFID application will have to consider this equation from the consumer's point of view (Eckeldt 2005). Research into post-purchase uses of tagged products and at-home RFID systems will be an on-going process, and the more consumers can benefit from RFID technology directly the more they will demand RFID enabled products from suppliers. Some of the post-purchase uses being touted are (Günther, and Spiekermann 2005: 75):

- Warranties without receipt
- Product return without receipt
- Medicine cabinets that warn and remind users
- Washing machines that automatically 'know' how best to wash a given load
- RFID-enabled refrigerators and closets
- Better food durability when expiration dates can be tracked electronically
- Shopping list generators

5. Conclusion

RFID is a technology with the potential to improve the way we live our lives and the way we conduct business. However, for this potential to be realized the challenges listed above, particularly those relating to security and privacy, will have to be thoroughly addressed. It is our hope that this paper has highlighted the technology's potentials, the on-going research to address the challenges, and the areas in need of more attention in terms of research.

6. References

Abraham, C., Ahuja, V., Ghosh, A.K., and Pakanati, P. (n.d.) "Inventory Management Using Passive RFID Tags: A Survey." [online] available from <http://www.cs.rutgers.edu/~badri/553dir/papers/MCPaperFinal-coldetect.pdf> [10 August 2007]

AIM UK (n.d.) "RFID Technical Basics." [online] available from <http://www.aimuk.org/pdfs/Comp04-4.pdf > [10 August 2007]

Andreou, A.G., Kalayjian, Z.K., Apsel, A., Pouliquen, P.O., Athale, R.A., Simonis, G., and Reedy, R. (2001) "Silicon on Sapphire CMOS for Optoelectronic Microsystems." *IEEE Circuits and Systems Magazine* 1, (3)

Avoine, G. (2007) "Bibliography on Security and Privacy in RFID Systems." [online] available from <http://lasecwww.epfl.ch/~gavoine/download/bib/bibliography-rfid.pdf> [10 August 2007]

Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., and Verbauwhede, I. (2006) "An Elliptic Curve Processor Suitable For RFID-Tags." *Cryptology ePrint Archive* [online] Report 2006/227. Available from <http://eprint.iacr.org/2006/227.pdf> [10 August 2007]

Baude, P.F., Ender, D.A., Kelley, T.W., Haase, M.A., Muyres, D.V., and Theiss, S.D. (2003) "Organic Semiconductor RFID Transponders." *IEEE International Electron Devices Meeting Technical Digest* [online] available from <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1269238> [10 August 2007]

Brown, W.C. (1984) "The History of Power Transmission by Radio Waves." *IEEE Transactions on Microwave Theory and Techniques* 32, (9) 1230-1242

Chawathe, S.S., Krishnamurthyy, V., Ramachandrany, S., and Sarma, S. (2004) "Managing RFID Data." In *Proceedings of the 30th VLDB Conference* Held in Toronto, Canada

Clarke, P. (2007) "Conference to Trial Printed Organic RFID in Badges." [online] available from <http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=201200130> [10 August 2007]

Cui, T., Liu, Y., Chen, B., Zhu, M., and Varahramyan, K. (2005) "Printed Polymeric Passive RC Filters and Degradation Characteristics." *Solid-State Electronics* 49, 853–859

Dimitriou, T. (2005) "A lightweight RFID protocol to protect against traceability and cloning attacks." [online] *IEEE/Create Net Secure Communications.* Available from <http://www.ait.edu.gr/faculty/T_Dimitriou_files/RFID-securecomm05.pdf> [10 August 2007]

Eckeldt, B. (2005) "What does RFID do for the consumer." *Communications of the ACM* 48, (9) 77-79

Engels, D.W., and Sarma, S.E. (2002) "The Reader Collision Problem." In *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics* 3, (10)

EPCglobal (2007) *EPC Information Services (EPCIS) Specification* Version 1.0 [online] available from <http://www.epcglobalinc.org/standards/epcis/EPCIS_1_0-StandardRatified-20070412.pdf> [10 August 2007]

Finkenzeller, K. (2003) *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. New York: Wiley

Friend, R.H. (1990) "Semiconductor Device Physics of Conjugated Polymers." *IEE Colloquium on Molecular Electronics* [online] available from <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=190651> [10 August 2007]

Furness, A. (c. 2006) "Research Dimensions for RFID." [online] available from <http://www.uknow.or.jp/be/science/seminar/RFID/Anthony_Furness.pdf> [10 August 2007]

Gianvittorio, J.P., and Rahmat-Samii, Y. (2002) "Fractal Antennas: A Novel Antenna Miniaturization Technique, and Applications." *IEEE Antennas and Propagation Magazine* 44, (1)

Günther, O., and Spiekermann, S. (2005) "RFID and the perception of control: The consumer's view." *Communications of the ACM* 48, (9) 73-76

Hassan, T., and Chatterjee, S. (2006) "A Taxonomy for RFID." In Sprague R. (ed.) *Proceedings of the 39th IEEE Hawaii International Conference on Systems Science*

Heder, S.H.M., Silvadurai, V., Brandon, L.H.S., and Vetharatnam, G. (2005) "Basic Properties of Fractal Antennas." [online] *MMU International Symposium on Information and Communication Technologies.* Available from <http://fist2.mmu.edu.my/~m2usic/proceedings05/TS05/04-187> [10 August 2007]

Henry, P. (2005) "Coming to a Store near You." *Software Development* 13, (1)

Hofstraat, H. (2001) "Will polymer electronics change the electronics industry?" *First International IEEE Conference on Polymers and Adhesives in Microelectronics and Photonics*

Juels, A. (2006) "RFID Security and Privacy: A Research Survey." *IEEE Journal on Selected Areas in Communications*, 24, (2)

Kurs, A., Karalis, A., Moffatt, R., Joannopoulos, J.D., Fisher, P., and Soljai, M. (2007) "Wireless Power Transfer via Strongly Coupled Magnetic Resonances." *Science* 317, (5834) 83-86

Lam, S., Hung Ki, W., and Chan, M. (2001) "The Silicon-on-sapphire Technology for RF Integrated Circuits: Potential and Limitations." In *Proceedings of IEEE Region 10 International Conference on Electrical and Electronic Technology* 1, 483-486

Leong, K.S., Ng, M.L., and Cole, P.H. (2005) "The Reader Collision Problem in RFID Systems." In *Proceedings of the IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications*

Marsh, M. (2007) "Impact of different air protocols on the use of the radio spectrum by Radio Frequency Identification (RFID) devices in the 860 to 960MHz bands." [Newsletter] Trolley Scan Pty, South Africa, January 2007

Molesa, S.E. (2006) *Ultra-Low-Cost Printed Electronics.* Unpublished PhD Dissertation, University of California at Berkeley [online] available from <http://www.eecs.berkeley.edu/Pubs/TechRpts/2006/EECS-2006-55.html> [10 August 2007]

Nakamura, T., Matsuhashi, H., and Nagatomo, Y. (2004) "Silicon on Sapphire (SOS) Device Technology." *Oki Technical Review* [online] 71, (4). Available from <http://www.oki.com/en/otr/200/downloads/otr-200-R18.pdf> [10 August 2007]

Ohkubo, M., Suzuki, K., and Kinoshita, S. (2004) "Efficient hash-chain based RFID privacy protection scheme." In *Proceedings of the International Conference on Ubiquitous Computing,* 'Workshop on Privacy: Current Status and Future Directions'

Oren, Y., and Shamir, A. [2006] "Power Analysis of RFID Tags." [online] available from <http://www.wisdom.weizmann.ac.il/~yossio/rfid/> [10 August 2007]

Polymer Vision (2007) *Polymer Vision Home Page* [online] available from <http://www.polymervision.com/index.html> [10 August 2007]

Rabaey, J.M., Chandrakasan, A.P., and Nikolic, B. (2003) 2nd edn. *Digital Integrated Circuits*. Upper Saddle River: Pearson Education

Redinger, D., Molesa, S., Yin, S., Farschi, R., and Subramanian, V. (2004) "An Ink-Jet-Deposited Passive Component Process for RFID." *IEEE Transactions on Electronic Devices* [online] 51, (12). Available from <http://organics.eecs.berkeley.edu/pdf/1978TED51.pdf> [10 August 2007]

Samuel, I.D.W. (2000) "Polymer Electronics." *Philosophical Transactions Royal Society London A* 358, 193-210

Sarma, S. (2001) "Towards the Five-Cent Tag." Auto-ID Center Technical Report [online] Cambridge: MIT. Available from <http://www.autoidlabs.org/uploads/media/mit-autoid-wh-006.pdf > [10 August 2007]

Shih, D.-H., Sun, P.-L., Yen, D.C., and Huang, S.-M. (2006) “Taxonomy and Survey of RFID Anti-Collision Protocols.” *Computer Communications* 29, (11) 2150–2166

Sparsø, J., and Furber, S. (eds.) (2001) *Principles of Asynchronous Circuit Design: A Systems Perspective*. Dordrecht: Kluwer Academic Publishers

Ukkonen, L., Sydänheimo, L., and Kivikoski, M. (2007) “Read range performance comparison of compact reader antennas for a handheld UHF RFID reader.” *IEEE Communications Magazine* 45, (4) 24-31

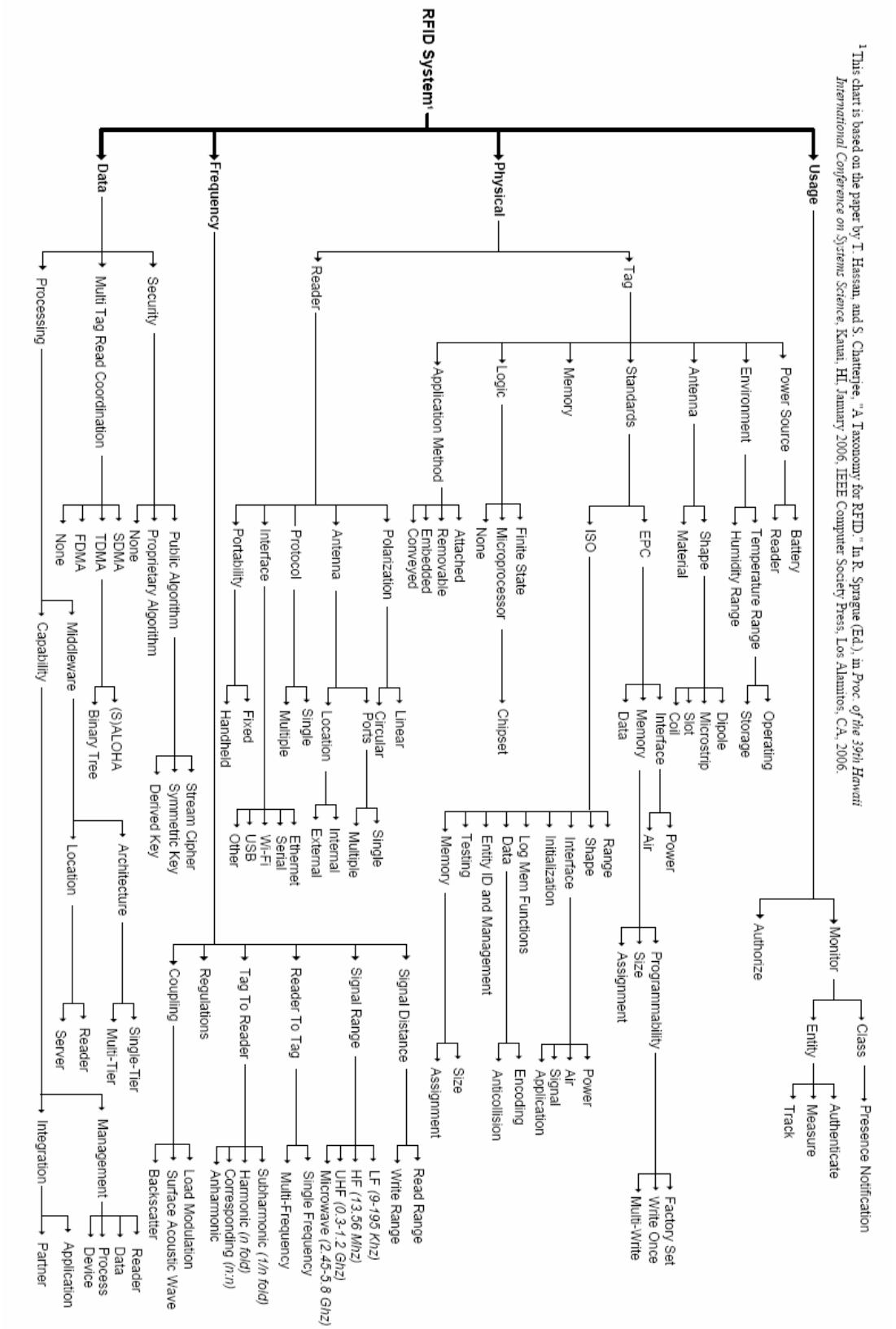
Wann, C., Su, L., Jenkins, K., Chang, R., and Taur, Y. (1998) “RF Perspective of Sub-Tenth- Micron CMOS.” *ISSCC98 Technical Digest*, 254–255

Weis, S., Sarma, S., Rivest, R., and Engels, D. (2003) “Security and privacy aspects of low-cost radio frequency identification systems.” In Hutter, D., Müller, G., Stephan, W., and Ullmann, M. (eds.) *Proceedings of the International Conference on Security in Pervasive Computing*, ‘Lecture Notes in Computer Science’ New York: Springer-Verlag: 2802, 454-469

Weisstein, E.W. (1999) "Fractal." [online] available from <http://mathworld.wolfram.com/Fractal.html> [10 August 2007]

Zappone, C. (2007) “Backlash against RFID is Growing.” [online] available from <http://money.cnn.com/2007/05/21/technology/rfid/index.htm?postversion=2007052113 > [21 May 2007]

7. Appendix: Taxonomy for RFID



[1] This chart is based on the paper by T. Hassan, and S. Chatterjee, "A Taxonomy for RFID." In R. Sprague (Ed.), in *Proc. of the 39th Hawaii International Conference on Systems Science*, Kauai, HI, January 2006. IEEE Computer Society Press, Los Alamitos, CA, 2006.