HAL open science

Techno-Economic Evaluation of Cognitive Radio in a Factory Scenario

Matthias Barrie, Lieven Tytgat, Vânia Gonçalves, Opher Yaron, Ingrid Moerman, Piet Demeester, Sofie Pollin, Pieter Ballon, Simon Delaere

To cite this version:

Matthias Barrie, Lieven Tytgat, Vânia Gonçalves, Opher Yaron, Ingrid Moerman, et al.. Techno-Economic Evaluation of Cognitive Radio in a Factory Scenario. International IFIP TC 6 Workshops PE-CRN, NC-Pro, WCNS, and SUNSET 2011 Held at NETWORKING 2011 (NETWORKING), May 2011, Valencia, Spain. pp.52-61, 10.1007/978-3-642-23041-7_6 . hal-01587834

HAL Id: hal-01587834

https://inria.hal.science/hal-01587834v1

Submitted on 14 Sep 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Techno-Economic Evaluation of Cognitive Radio in a Factory Scenario

Matthias Barrie[1], Lieven Tytgat[2], Vânia Gonçalves[1], Opher Yaron[2], Ingrid Moerman[2], Piet Demeester[2], Sofie Pollin[3], Pieter Ballon[1], Simon Delaere[1],

[1] IBBT – SMIT, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium
[2] IBBT – IBCN, Ghent University, Gaston Crommenlaan 8, 9050 Ghent, Belgium
[3] imec, Kapeldreef 75, 3001 Leuven, Belgium

{lieven.tytgat, opher.yaron, ingrid.moerman, piet.demeester}@intec.ugent.be
{matthias.barrie, vania.goncalves, pieter.ballon, simon.delaere}@vub.ac.be
sofie.pollin@imec.be

Abstract. Wireless applications gradually enter every aspect of our life. Unfortunately, these applications must reuse the same scarce spectrum, resulting in increased interference and limited usability. Cognitive Radio proposes to mitigate this problem by adapting the operational parameters of wireless devices to varying interference conditions. However, it involves an increase in cost. In this paper we examine the economic balance between the added cost and the increased usability in one particular real-life scenario. We focus on the production floor of an industrial installation – where wireless sensors monitor production machinery, and a wireless LAN is used as the data backbone. We examine the effects of implementing dynamic spectrum access by means of ideal RF sensing, and model the benefit in terms of increased reliability and battery lifetime. We estimate the financial cost of interference and the potential gain, and conclude that cognitive radio can bring business gains in real-life applications.

Keywords: RF sensing, coexistence, cognitive radio, CR, dynamic spectrum access, DSA, business analysis, statistical model, Spectrum Etiquettes for Unlicensed Bands.

1 Introduction

Recent advances in microelectronics have enabled the use of wireless communication in virtually every application. As a result, the scarce spectrum is getting crowded with ever more wireless communication devices. Indeed, the need to coexist is aggravated by the fact that different applications use different wireless technologies, which are a-priori unaware of each other, and therefore cannot collaborate to best share the scarce spectrum. Dynamic Spectrum Access (DSA) is a class of mechanisms that aim at improving spectrum sharing. DSA adapts actively to the dynamic interference environment, leveraging on a variety of cognitive technologies ranging from spectrum sensing to agile radio.

When considering actual deployment of DSA in real-life, there is a natural techno-economical tradeoff between benefit and cost. In this paper we focus on a particular scenario to examine this economic balance. We consider the case of an industrial plant, where an IEEE 802.15.4 based wireless sensor network coexists with an IEEE 802.11 wireless LAN in the unlicensed ISM band. Throughout the paper we refer to IEEE 802.11 also with the terms WLAN and WiFi, and to IEEE 802.15.4 also with the terms Zigbee and sensor network. The sensor network monitors and controls the production equipment, while WLAN provides wireless access to the data network of the plant, e.g. to machinery operators that use WLAN equipped portable handheld devices. The common approach is to go to great lengths to avoid interference to the production control, e.g. the ISA100.11a industry standard [1]. We propose that a more balanced approach is in place. We suggest that the overall economic value of avoiding interference should be considered, calculating the trade-off between the advantages of the lower interference achieved; and the additional cost incurred.

In the proposed scenario the economical benefit of implementing DSA is in reducing machine failure rate and production disruption. DSA improves the reliability of the sensor network, which brings to faster identification of machine status alerts. Potential added cost is due to the actual implementation cost of the selected solution, increased maintenance, and increased cost of battery replacement due to shortened battery lifetime.

The coexistence of WiFi and Zigbee has been studied extensively from the technological perspective. Petrova et. al. [2] tested experimentally the mutual impacts between IEEE 802.15.4 and IEEE 802.11. They conclude that IEEE 802.15.4 has practically no influence on concurrent IEEE 802.11 communications, while IEEE 802.11 has significant negative effect on IEEE 802.15.4. Muoung et. al. [3] calculate mathematically the packet loss rate and throughput of IEEE 802.11b when interfered by IEEE 802.15.4. They show that in the unrealistic worst case, when the distance between the 802.11 receiver and 802.15.4 transmitter is small and the Clear Channel Assessment mechanism (CCA) of each network does not hear the other, performance degradation can be substantial. Pollin et al. [4] measure the impact of WiFi on Zigbee and show it is significant. They also show that the CCA of Zigbee can reduce collisions with WiFi, but is too slow to avoid all WiFi traffic. Thonet et al. [5] show that in typical residential environments Zigbee is not affected by WiFi, but in the lab, under controlled WiFi traffic loads, Zigbee suffers significant packet-loss when the WiFi duty cycle is above 20%. In summary, it is evident that WiFi has significant impact on Zigbee, while Zigbee has at most very low effect on WiFi.

In order to deal with WiFi interference, various measures have been proposed, focusing on three major domains – Time, Frequency and Space. Space based measures focus on spatial reuse of the spectrum. Frequency based measures focus on optimizing the use of the spectral bands, e.g. channel selection algorithms and multichannel solutions. Time based measures focus on intelligent distribution of message transmissions over time.

In this paper we focus on the Time domain. In order to avoid collisions, we propose to implement CCA by a new, cross-technology sensing engine. This new device is able to detect the presence of signals from different technologies. We examine and compare different options for the deployment of sensing engines. In what follows Alternative 1 is the reference of not using sensing engines at all,

Alternative 2 is to use sensing engines only in the Zigbee nodes, Alternative 3 is to deploy sensing engines only in the WiFi devices, and Alternative 4 is to add sensing engines to both the Zigbee nodes and the WiFi devices.

The remainder of this paper is organized as follows: Section 2 introduces the specifics of the factory scenario we consider. In section 3 we determine the technical advantages and disadvantages for using the sensing engine in the different deployment alternatives. In section 4 we model the gains achieved by spectrum sensing versus the incurred costs. We conclude this paper in section 5.

2 Scenario

In order to gain meaningful insight into the use of cognitive networking indoors, we look at a realistic scenario, for which we can discover accurate data, and make viable assumptions when such data is not available. As mentioned in the Introduction, we focus on a particular scenario of an industrial plant, where an IEEE 802.15.4 based wireless sensor network coexists with an IEEE 802.11 wireless LAN. More specifically, we consider a modern electronics contract manufacturer that operates multiple Surface Mount Technology (SMT) assembly lines. A mid-size manufacturer may operate a production floor with 15 assembly lines in parallel. Each line includes 3-4 robots and one oven, and is constantly monitored by 2 human operators on the production floor.

Each robot contains 2 cameras and 6-7 different ZigBee sensors, while the ovens contain another 10 ZigBee sensors each, bringing the total number of ZigBee sensors throughout the production floor to 600. These sensors form a Zigbee wireless sensor and actuator network (WSAN). They measure the temperature and other parameters of machinery and processes on the assembly line, and transmit it periodically to a central control and monitoring system. This system alerts human operators of various types of malfunctions, e.g. component-feed problems and overheating, which typically happen multiple times every day.

The wireless LAN in the factory is composed of 100 WiFi devices, including access points, laptops, portable terminals and smartphones. For example, each of the operators of the assembly lines has a portable terminal that he uses to control software download to the assembly machines, verify that proper material is loaded in the robots, etc. As presented in the Introduction, the WiFi devices interfere with the ZigBee sensor network. The nature of interference in this case is that ZigBee data may be lost during periods of active WiFi transmissions.

Since the sensors are located to monitor critical parameters in the assembly lines, loss of Zigbee data might lead to severe damage to machinery and significant loss of material. Two types of failure are possible. Major Failures are ones that risk damage to machinery. If, for example, a machine overheats while Zigbee packets are lost, the supervisors will not be alerted in time, which could lead to serious damage to the machine and a full stop of the assembly line until the damage is repaired. This would reduce production output, and decrease revenue as a result. Minor Failures are ones that only risk loss of material and profit. If, for example, one of the SMT component feeders gets jammed, then all products that continue to be produced before the

problem is fixed are damaged, and considered lost. In our scenario each assembly line uses $700 worth of materials and produces $300 of profit per hour of uninterrupted operation. We assume that every assembly line develops conditions that, if not detected on time, will cause a Major Failure once every year. We also assume that every assembly line suffers a Minor Failure once every hour. Furthermore, we estimate that an assembly line that suffers a Major Failure will shut down for 24 hours, and the total cost of repair, in labor, equipment and replacement parts, is $10,000. We also estimate that if a Minor Failure occurs while Zigbee packets are lost, it will take additional 30 seconds to detect the failure and stop production.

Due to the substantial opportunity costs and repair costs, it is clear that the factory owner is interested to reduce interference to an acceptable minimum. Therefore, we propose the solution of adding cognitive elements to the wireless devices. These come however at an investment and energy consumption costs that must be balanced with the performance gains they promise to deliver.

3 Technical Analysis

In our scenario automated control of machinery is achieved through the use of a Zigbee WSAN, and a WiFi WLAN is used to provide wireless access to the administrative data network of the factory. Both Zigbee and WiFi use CCA to sense if the medium is free before transmitting a packet. Although the basic mechanism is identical, the details like bandwidth, sensing time and Rx-Tx turnaround time vary. In particular, as mentioned in the Introduction, Zigbee CCA typically detects WiFi transmissions, but WiFi CCA does not detect Zigbee transmissions.

The sensing engine we propose, which is described in [6], performs cross-technology Clear Channel Assessment. It can be tuned very quickly to any channel in the ISM band, and then detect any Zigbee or WiFi transmission. Thus, if it is implemented on a Zigbee node, it can also detect WiFi transmissions, and if it is implemented in a WiFi device, it can also detect all Zigbee transmissions across the full WiFi channel. In addition, since it uses dedicated hardware, it helps reducing the Rx-Tx turnaround time significantly.

In a previous paper [7] we perform a detailed mathematical analysis, using the law of total probability, and derive closed-form formulas for the Packet Error Rate (PER) of the Zigbee network in Alternatives 1, 2 and 3 as defined in the Introduction. For Alternative 1 the packet success rate (1 – PER) is expressed as

$$1 - PER \cong e^{-\frac{T_Z + T_{Z,CCA} + T_{Z,RtT}}{T_{\overline{W}}}} * (1 - PER_Z) . \quad \textbf{(1)}$$

Where PER_Z is the PER of a stand-alone Zigbee network (without the presence of a collocated WiFi network), T_Z is the average length of a Zigbee packet, $T_{Z,CCA}$ is the CCA time of Zigbee (112μs), $T_{Z,RtT}$ is the Rx-to-Tx turnaround time of Zigbee (192μs), and $T_{\overline{W}}$ is the average Inter Packet Delay (IPD) of WiFi.

According to measurements presented in [2], and considering that Zigbee sensors send infrequent messages, we approximate $1 - PER_Z$ by 1. Consequently

$$1 - PER \cong e^{-\frac{T_Z + T_{Z,CCA} + T_{Z,RtT}}{T_{\overline{W}}}} \quad \textbf{(2)}$$

In Alternative 2 sensing engines are deployed in all Zigbee nodes, with practical effect of reducing $T_{Z,RtT}$ to zero and $T_{Z,CCA}$ to $T_{S,CCA}$, the CCA time of our sensing engine. Substituting in (2) we get

$$1 - PER \cong e^{-\frac{T_Z + T_{S,CCA}}{T_{\overline{W}}}} \quad \textbf{(3)}$$

In Alternative 3 sensing engines are deployed in all WiFi nodes. Now WiFi nodes will not start transmission when a Zigbee node transmits, and the result is

$$1 - PER \cong e^{-\frac{T_{Z,CCA} + T_{Z,RtT}}{T_{\overline{W}}}} \quad \textbf{(4)}$$

Finally, Alternative 4, in which sensing engines are deployed in both Zigbee and WiFi nodes, combines the two effects, resulting in

$$1 - PER \cong e^{-\frac{T_{S,CCA}}{T_{\overline{W}}}} \quad \textbf{(5)}$$

Fig. 1 shows the dependence of Zigbee PER on the traffic load in the WiFi network, for the different deployment alternatives of the sensing engine.

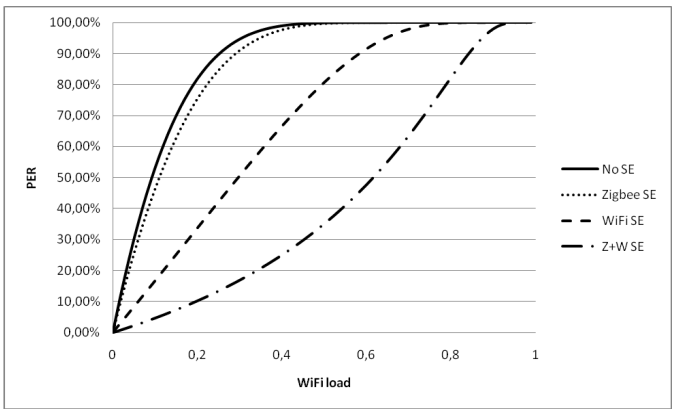

Fig. 1. Zigbee PER in different implementation alternatives of sensing engine

For example, for 10% traffic load in the WiFi network, the PER in the Zigbee network is estimated at 53%. If sensing engines are deployed only in the Zigbee

nodes, this PER reduces slightly, to 46%. If sensing engines are deployed only in the WiFi nodes, the PER in the Zigbee network reduces significantly, to 17%. Furthermore, if now sensing engines are deployed also in the Zigbee nodes, then the PER in the Zigbee network reduces further significantly, to 4%.

Power Consumption. The WiFi nodes are powered either by mains power or rechargeable batteries, therefore their cost of energy is just the actual cost of consumed electricity. WiFi nodes are typically 'On' all the time, in one of three states – Receiving, Sensing (before transmitting) and Transmitting. Typical power consumption in these states, with the sensing engine deployed, is 100mW, 50mW and 1W respectively. A typical average is 300mW, with worst case consumption of approximately 1W. Taking a typical cost of mains power electricity of $0.15 /kWh, we calculate the average total energy cost of the WiFi devices over 5 years at $0.15/kWh * 300mW * 24h/d * 365d/y * 100 * 5 = $197, with a worst case cost of $197 * (1W / 300mW) = $657. Moreover, since WiFi is not interfered by Zigbee, no additional retransmissions occur due to the presence of Zigbee.

We now turn to calculate the power consumption of the Zigbee nodes. We make the following assumptions:

- Each Zigbee sensor performs and transmits measurements once every 10 seconds. At this duty cycle, the average power consumption of the Zigbee sensor (without the sensing engine) is 2mW.
- Average power consumption of a Zigbee radio, when active, is 24mW. Average duration of radio activation for the transmission of one packet, including waiting for and reception of acknowledgement, is 1.6ms. Consequently, the average power consumed by a Zigbee radio when sending one packet per second is 24mW * 1.6ms * 1/s = 38μW.
- Average power consumption of the sensing engine, when active, is 50mW. The sensing engine is activated for 80μs prior to the transmission of every packet. Consequently, the average power consumed by the sensing engine when sending one packet per second is 50mW * 80μs * 1/s = 4.0μW.

Consequently, at a worst case of even 20 retransmissions of each packet, the power consumption of the radio and the sensing engine is estimated at (38μW + 4.0μW) * 0.1 * 20 = 84μW. This is just 4.2% of the average Zigbee sensor consumption of 2mW. A typical Zigbee sensor node is powered by two D size Lithium batteries, with the following typical characteristics: voltage 3.6V, capacity 14Ah (or 50Wh). The expected lifetime of the batteries is therefore 50Wh * 2 / 2mW = 50.000h = 5.7y, and even with the sensing engine it stays well above 5 years.

4 Economical Evaluation

Following the terminology of the technical analysis, we compare the reference Alternative 1, of a factory with standard WiFi and Zigbee networks and no cognitive solutions, to the three alternative set-ups. We seek to point out which of the alternatives would provide the most economical benefit compared to the reference

alternative, if at all. We base our calculations on a 5-year period, which is a realistic lifetime of wireless nodes.

4.1 Potential Gains of Sensing

Sensing reduces the interference between the ZigBee and WiFi networks. In fact, sensing therefore limits the amount of machinery and assembly line failures, which are caused by late alerting due to interference. The economic gains of sensing are thus derived from the amount of failures (along with their costs and losses) that can be avoided. These failures can, as mentioned in the scenario description, be divided into two groups.

In the absence of any monitoring sensors, Major failures would occur on average once a year on each line. Major failures involve damage to machinery, which according to the Scenario section, over a period of 5 years, would cost $10.000 * 15 * 5 = $750.000 to repair, and would cause loss of profit of $300 * 24 * 15 * 5 = $540.000.

With a total cost of $1.290.000 over 5 years, Major failures represent a very large potential loss for the factory.

Again, in the absence of any monitoring sensors, Minor failures would occur on average once an hour on each line. Minor failures involve assembly of defective products, which according to the Scenario section, over a period of 5 years, would cost $700 / 3600 * 30 *24 * 365 * 15 * 5 = $3.832.500 in lost material, and would cause loss of profit of $300 / 3600 * 30 * 24 * 365 * 15 * 5 = $1.642.500.

With a total cost of $5.475.000 over 5 years, Minor failures represent even a larger potential loss than the Major failures.

In summary, the potential total cost of failures in 5 years time amounts up to $6.765.000. This significant figure is the reason monitoring sensors are indeed deployed in assembly lines and other industrial plants. When alerts are sent and received, human operators can react on time and prevent damage to machines, as well as reduce the quantity of damaged products. However, as demonstrated in the Technical Analysis, interference from the WLAN network in the plant causes some packet loss in the Zigbee network, which may result in loss of important alert messages. This interference can be drastically reduced by the use of spectrum sensing and packet retransmissions.

However, variations in where the sensing engines are deployed (represented by the different Alternatives) and which loads are present in the WiFi network lead to different levels of improvement to the reliability of the Zigbee network. In turn, improved reliability reduces the number of un-alerted failures, and with them the consequent costs.

4.2 Cost of Sensing

Additional potential cost, which is associated with sensing, can be attributed to two sources – investment cost and energy cost.

Investment Cost. The additional investment cost comes down to the extra price of a node that is equipped with a sensing engine. The core of this engine is an Application Specific Integrated Circuit (ASIC), which is estimated at $1. Some additional components, e.g. RF front-end and Analog-to-Digital Converter (ADC), are necessary for the implementation of the complete sensing engine. These components are included in WiFi devices and can typically be re-used by the sensing engine, therefore we estimate the cost of one sensing engine for a WiFi device at $1. For ZigBee sensors it is necessary to add these components, and we estimate the total cost of this sensing engine at $10 at the most. Because there are 600 ZigBee nodes and 100 WiFi devices throughout the factory, we estimate the total additional investment in Alternative 2 at $6.000, in Alternative 3 at only $100 and in Alternative 4 at the sum of these 2 cases; $6.100.

Energy Cost. As shown in the Technical Analysis, the average total energy cost over 5 years of the WiFi devices with sensing engine included is estimated at $197, with a worst case cost of $657. In the context of our scenario both these numbers are negligible.

The Zigbee nodes are powered by primary (disposable) batteries, therefore their cost of energy includes the batteries themselves and the cost of replacing them. As shown in the Technical Analysis, the expected lifetime of the batteries is well above 5 years. We assume replacement every 5 years to cover for some safety margin, and intentional scheduling prior to complete depletion. Replacing batteries involves labor and temporary halt of the assembly line. As some sensors are located in hard-to-reach locations, we assume that the average cost of labor for replacing batteries in one sensor is $100, and the production line is halted for 30 minutes on the average. We therefore calculate the total energy costs for ZigBee nodes as follows:

1. Typical battery cost is $20, with total cost for 5 years of $20 * 2 * 600 = $24.000.
2. Battery replacement cost in 5 years in composed of $100 * 600 = $60.000 in labor, and $300 * 0.5 * 600 = $90.000 in loss of profit due to discontinuation of production, with a total of $150.000.

It is important to note that all energy costs apply to all four deployment alternatives of the sensing engine, since we show in the Technical Analysis that the additional power consumption directly associated with the sensing engine is negligible.

4.3 Total Savings due to Sensing

Table 1 presents the total expected savings due to the implementation of sensing engines. It is calculated by comparing the remaining cost that is attributed to failures due to interference in the Zigbee network over 5 years, to the costs of interference in the reference case (Alternative 1), while taking into account the initial investment in the sensing engines. Since it is typical to use retransmission to overcome transmission failures, we assume up to 2 retransmissions of each packet. The table shows how the expected savings vary with the different deployment alternatives of sensing engines, and with the traffic load on the WiFi network. We calculate the expected savings when up to 2 retransmissions are performed, for typical WiFi loads of 5%-20%. We

also calculate it for an extreme WiFi load of 50%, to examine the robustness of the solution and its immunity to heavy interference.

Table 1. PER and Cost of failures in the Zigbee sensor network, and the expected savings for the different deployment alternatives of sensing engines

	Alternative 1	Alternative 2	Alternative 3	Alternative 4
WiFi Load 5% – Zigbee PER	30%	26%	8%	2,3%
Failure cost – No Retransmissions	2,03M	1,76M	541K	156K
Failure cost – up to 2 retransmissions	183K	119K	3,5K	80
WiFi Load 5% – Saving with Sensing	NA	58K	179K	177K
WiFi Load 10% – Zigbee PER	53%	46%	17%	4,7%
Failure cost – No Retransmissions	3,59M	3,11M	1,15M	318K
Failure cost – up to 2 retransmissions	1,0M	659K	33K	700
WiFi Load 10% – Saving with Sensing	NA	335K	967K	993K
WiFi Load 15% – Zigbee PER	70%	63%	25%	7,3%
Failure cost – No Retransmissions	4,74M	4,26M	1,69M	494K
Failure cost – up to 2 retransmissions	2,32M	1,69M	106K	2,63K
WiFi Load 15% – Saving with Sensing	NA	624K	2,21M	2,31M
WiFi Load 20% – Zigbee PER	82%	75%	34%	10%
Failure cost – No Retransmissions	5,55M	5,07M	2,3M	677K
Failure cost – up to 2 retransmissions	3,73M	2,85M	266K	6,8K
WiFi Load 20% – Saving with Sensing	NA	874K	3,46M	3,72M
WiFi Load 50% – Zigbee PER	99.9%	99.6%	80%	35%
Failure cost – No Retransmissions	6,76M	6,74M	5,41M	2,37M
Failure cost – up to 2 retransmissions	6,74M	6,68M	3,46M	290K
WiFi Load 50% – Saving with Sensing	NA	54K	3,28M	6,44M

Looking at Table 1 it is clear that when sensing is implemented in both the WiFi and Zigbee nodes, the result is a robust solution, that even under extreme WiFi load of 50% incurs only $290.000 over 5 years due to Zigbee transmission failures. If more that 2 retransmissions are considered, the incurred cost can be reduced further, and implementing sensing engines just in the WiFi nodes can become enough.

In this analysis we completely ignore the cost of energy, as it is practically identical in all the alternatives we examine. This cost totals $174.000, which is anyway very low compared to the potential gains achieved by the sensing engines.

5 Conclusions

It is well known that in a factory setting the cost of failures can amount to significant numbers. For this reason sensors are deployed to detect failure conditions early. Sensor information is delivered over a data communication network, with clear operational advantages to using wireless technology, e.g. Zigbee. However, the reliability of the Zigbee network is strongly affected by interfering traffic from the collocated administrative WLAN network, with a direct impact on the rate of failure in the factory. To increase reliability, we propose to reduce interference by adding cross-technology sensing engines to the CCA mechanism of some network nodes. We show that from both the technical and economical points of view this improvement is beneficial. We show that adding sensing engines can indeed reduce the effects of interference significantly, and that the resulting reduction in failures outweighs the low investment costs and the negligible increase in energy costs. We conclude that for this case sensing is a viable and profitable solution. We discover that adding sensing engines to both the Zigbee sensors and the WiFi devices is the most beneficial alternative. It brings interference to the lowest level among all alternatives; it is immune to very high traffic load on the WiFi network; and it maximizes the financial gain.

Acknowledgments. The research leading to these results has received funding from the European Union's Seventh Framework Programme FP7/2007-2013 under grant agreements n° 257542 (CONSERN project) and n° 258301 (CREW project). It has also received funding from IWT under projects ESSENCES and NGWINETS.

References

1. ISA-100.11a-2009, Wireless systems for industrial automation: Process control and related applications. ISA Standards, USA (2009)
2. M. Petrova, J. Riihijarvi, P. MAhonen, S. Labella: Performance Study of IEEE 802.15.4 Using Measurements and Simulations. In: IEEE Wireless Communications and Networking Conference (WCNC). Las Vegas (2006)
3. K.-J. Muoung, S.-Y. Shin, H.-S. Park, W.-H. Kwon: 802.11b Performance Analysis in the Presence of IEEE 802.15.4 Interference. In: IEICE Transactions on Communications, vol. E90-B, No.1, pp. 176--179. Japan (2007)
4. S. Pollin, I. Tan, B. Hodge, C. Chunand A. Bahai: Harmful Coexistence Between 802.15.4 and 802.11: A measurement-based study. In: Proc. Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), vol. 1, pp. 1--6. Singapore (2008)
5. G. Thonet, P. Allard-Jacquin, P. Colle: ZigBee – WiFi Coexistence, White Paper and Test Report, http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=13184. Grenoble, France (2008)
6. imec Cognitive Reconfigurable Radio Solutions, http://www.imec.be/ScientificReport/SR2008/HTML/1225000.html
7. Lieven Tytgat, Matthias Barrie, Vânia Gonçalves, Opher Yaron, Ingrid Moerman, Piet Demeester, Sofie Pollin, Pieter Ballon, Simon Delaere: Techno-economical Viability of Cognitive Solutions for a Factory Scenario. Submitted for Publication (2010)