Software Defined Radio Based Implementation of RFID Tag in Next Generation Mobiles

Petar Šolić, *Student Member*, IEEE, Joško Radić, *Member*, IEEE and Nikola Rožić, *Member*, IEEE

Abstract — *Radio Frequency identification (RFID) technology has become important tool for items identification and tracking. In those purposes different types of RFID technologies could be used, depending on its application. Limitations of passive RFID technology, related to tags reading range and confidence in harsh environments, puts restrictions on implementation in the real life scenarios. To overcome the issue, but staying within the standards, we have considered development and implementation of active backscattering tag technology, which significantly improves tag reading range and confidence. Software Defined Radio (SDR) technology is promising technology for building mobiles of multiple radio standards in 4G networks. Regarding stated RFID technologies limitations and SDR technology, we present development and implementation of the Software Defined Radio (SDR) active backscattering tag compatible with the EPCglobal UHF Class 1 Generation 2 (Gen2) RFID standard. Such technology can be used for wide spectra of applications and services. The system is developed and tested on SDR platform. Validity and performances of developed Gen2 SDR tag are shown through actual presented results*[1].

Index Terms — Software Defined Radio (SDR), Active backscattering, Gen2 RFID, Mobile phones RFID, 4th Generation Mobile Networks (4G)

I. Introduction

RFID technology based on wireless radio communication between the reader and tags is today widely used for items identification and tracking. Regarding the tag battery presence or absence, RFID can be classified into three groups: full battery powered systems in active RFID, battery-assisted semi passive systems (BAP) and battery-free tags in passive RFID technology. Low cost passive RFID tags use RF energy received from the RFID reader antenna as a tag IC power supply and as well for backscatter communication. To function properly, passive tags have to be relatively close to the reader antenna in order to absorb required power level, which makes technology limited in the communication from reader to tag (i.e. forward-link). Passive RFID disadvantages in relatively low reading range of only a few meters away from the reading antenna, and degraded tag reading performances on metal or liquid surfaces, put significant constraints on its usage [1]. BAP RFID technology differs from the passive technology because it uses battery for tag IC running, which makes BAP more reliable in the sense of responding back to the reader [2]. However, BAP tags are limited in the communication from tag to reader (i.e. backward-link), since the reader have sensitivity level, and cannot detect weak backscattered signal from large distances. Using BAP tags reading range can be increased up to a few dozens of meters, but their size, price of about 10 USD per piece and battery limited lifetime may become an issue in the typical supply chain implementation. Usage of active RFID tags (transceivers) provides reading range of up to 100 m [3], but their size and price of between 50-100 USD make them as too expensive solution in some tracking scenarios.

Today's research directions in RFID technology include improvements in the tag reading range with solutions which are of low complexity and thus low cost [2]. To increase reading range tags can use amplifiers for active backscattering [4], where independent power source is used to amplify backscattered information signal. Such approach extends tag reading range, but it implies a new and more expensive hardware device (tag). In [5] authors proposed solution for providing additional energy to charge the battery or the capacity, used for backscattered signal amplification. Simulation shows that required energy for the signal amplification could be harvested from the reader with proper energy scheduling scheme and thus increase reading range. This approach also implies the additional circuitry and logic which makes the tag more robust and thus expensive. To fill in the gap, new emerging technologies, like mobile phones, can be used to accomplish radio frequency identification, owing to their active technology and ability to transmit higher power than all types of RFID tags. Such technology can be used for human or objects identification, especially in noisy and industrial environments [6], [7] and to assure mobility for different applications and services [8].

SDR Mobile phones in 4G networks are expected to be able to load radio-applications and accomplish functionalities of different protocols and services on a single chip [9], [10], including WLAN, Bluetooth, different RFID technologies, etc. This approach gives the advantage of providing a single universal device for all radio-tasks. Development of the different system prototypes using SDR's are today comprehensively investigated in many articles [11], [12], where RFID takes a special place [13], [14]. Authors in [13] use SDR as a RFID listener for distributed tag sensing, since a number of tags could not be read due to small signal levels backscattered to the reader. In [14], authors used SDR for tag

[1] This research work has been performed within the project "ICT Systems and Services Based on Integration of Information " (P023-0231924-1661) supported by the Ministry of Science and Technology of the Republic of Croatia.

Petar Šolić, Joško Radić, and Nikola Rožić, are with the University of Split, FESB, Croatia (e-mail: psolic@fesb.hr, radic@fesb.hr, rozic@fesb.hr).

Contributed Paper
Manuscript received 06/01/12
Current version published 09/25/12
Electronic version published 09/25/12.

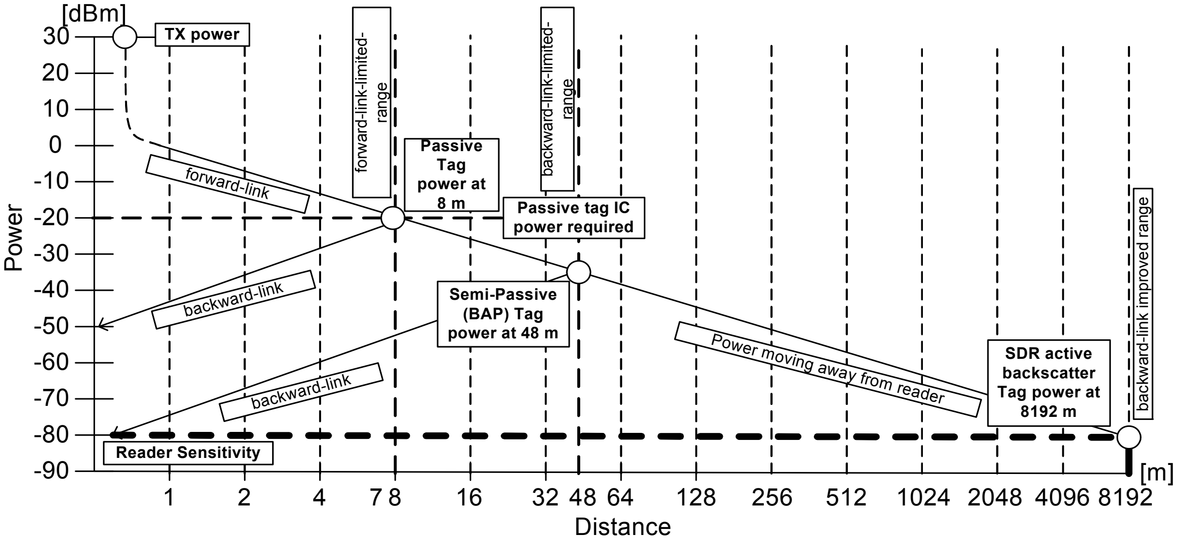

Fig. 1. Simplified description of different RFID reader-tag communication technologies, with its limitations (omnidirectional TX antenna). Theoretically, SDR tag could response from approximately 8 km away from the reader if it has the same sensitivity and output power as the reader.

signals separations in order to reduce the number of collisions, etc. SDR 4G mobiles with capability of RFID tag emulation, presents the great advantage in the usage of recently purchased RFID technologies. With implemented RFID tag radio-application, mobile phone becomes RFID tag with improved reading performances, without additional hardware costs. Figure 1 illustrates limitations on each tag type along with the proposed SDR approach. Moreover, with SDR mobile phones, all kind of RFID technologies can be implemented on single device with different PHY/MAC layer programming and thus used in variety of applications of authentication, tracking, human or object identification, etc.

In this paper we present the prototype of the Gen2 RFID active backscattering tag developed on SDR platform. We believe this is the first SDR RFID tag implementation which performs exactly the same operations as Gen2 backscatter tag. Our proposal contributes to the state of the art in the sense of the deployed RFID technology usage with extended tag reading range using SDR approach.

The paper is structured as follows: in the Section II we provide an overview of EPCglobal [15] protocol and analyze what one has to do to accomplish identification procedure described in the protocol. Section III describes some issues in SDR tag implementation and their solutions in implementation SDR tag implementation. Measurements setup and results of performance analysis is given in the Section IV. In Section V we give some concluding remarks.

II. Gen2 Protocol and the Requirements Analysis

To accomplish full tag functionalities it is necessary to follow Gen2 protocol requirements [15]. To start the interrogation, RFID reader sends *PowerUp* command, which is followed by *Select* command, where group of tags for interrogation can be selected. *Select* is an arbitrary command. After *Select*, reader sends *Query* command, where interrogation parameters that tags follow are set, including backscatter link frequency, the number of cycles in Miller-modulated subcarrier for tag response, population of tags that participate in an inventory round, and Q factor which specifies the length of interrogating frame divided into 2^Q timeslots. With *Query* command, tags slot counters are initialized to the random number in between $0 - 2^Q - 1$ Afterwards tags can, if their slot counter is set to zero, respond with 16 bit random number *RN16* to the RFID reader. If tag responds to the command, reader sends *ACKRN16* acknowledgement, and tag, if it demodulates it correctly, sends its own 96 bit Electronic Product Code (EPC) value. If tags do not respond to the *Query* command, i.e. none of the slot counters is zero, reader will send *QueryRepeat (QRep)* command to decrease slot counters by 1. After *QRep*, tag(s) can respond with the random number, which should be acknowledged before sending EPC. Number of *QRep* commands before sending new *PowerUp* and *Query* is specified with Q factor, so there will be $2^Q - 1$ *QRep* commands which decrease all possible slot counters. Time between two *Query* commands is specified as inventory (interrogation) round. During the inventory round, reader can modify the number of slots with adjustment of Q, e.g. using *QueryAdjust (QAdj)* command. Figure 2 shows an inventory round with one tag response.

III. 4G Mobile Phone UHF Gen2 Tag Implementation through SDR

A. Some Issues in the development of SDR tag

In real scenarios, passive Gen2 RFID tags are backscattering the modulated subcarrier of the assigned reader carrier transmitted at UHF frequency it is tuned. Since SDR is active transceiver and it does not backscatter signal by default, one has to deal with the problem of frequency synchronization between RFID reader and SDR tag (due to their oscillator offsets). The frequency offset which appears when RFID reader and SDR tag are not synchronized is shown in Figure 3,

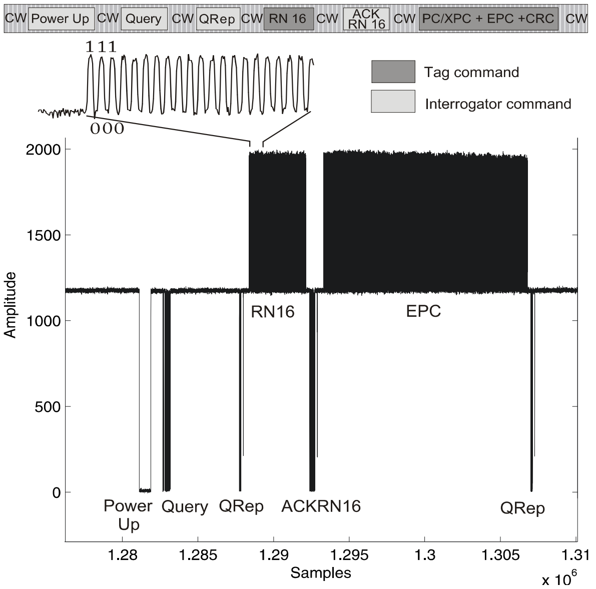

Fig. 2. Gen2 protocol interrogation round, where $Q = 1$. SDR Tag respond 4 meters away from the reader, after first *QRep* command.

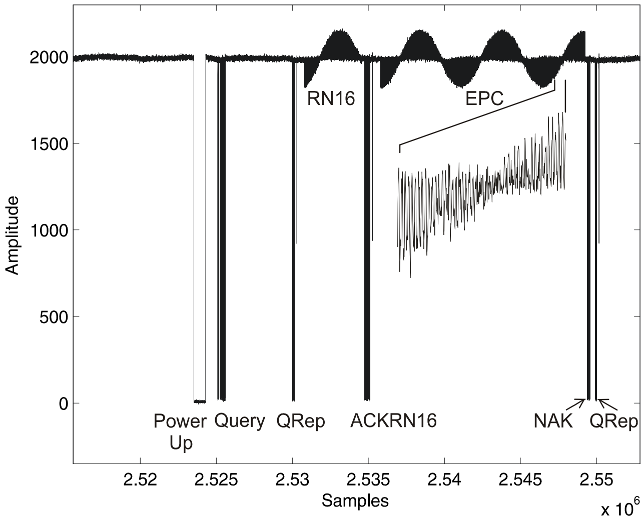

Fig. 3. Gen2 protocol interrogation round with the frequency offset. SDR tag command was not decoded correctly, since zero crossings could not be successfully decoded. Afterwards, reader sends *NAK* command to tell the tag that *RN16* was not successfully decoded.

and it causes information from SDR tag not to be correctly decoded. Moreover, timing requirements are crucial for the protocol compliance [16], [17]. For the real implementation in the mobile phones, the system latency should be reduced to 1 *ms* in order to keep timing requirements specified in [15]. In the SDR PC implementation we developed, buffer size should be set in order to receive and process the samples as soon as possible. In the same time, it is necessary to guarantee that the system is not under/overrunning samples and the processing capacity is less than 32 Mega Samples per second (MS/s) which is the maximum throughput of USB 2.0 protocol (if SDR to PC connection uses USB interface). Sampling frequency should be set properly in order to receive and decode complete information from the reader. Afterwards, when signal is sampled, it is crucial to define suitable bus block sizes in order to assure that the computer processes the information in the time window proposed by the protocol.

B. SDR tag implementation

Developed application for SDR implements and provides functionalities of Gen2 tag PHY/MAC layer. The system was tested on Buettner's SDR RFID UHF GEN2 Reader [16].

The start of an inventory round in the reader [16] is marked with *PowerUp* command. SDR tag application uses *PowerUp* command to synchronize on, and sends information compliant with the protocol [15] requirements. Its slot counter always equals 1, which means that after first *QRep*, *RN16* is sent. After *PowerUp* detection, we count number of frames when to send the *RN16* command. However, during the interrogation cycle, reader [16] sometimes sends *QRep* command, while our tag transmits the *RN*16. In those cases, reading performances are degraded. In our future work we consider possible solution for this issue using [17], due to its great flexibility.

Communication between reader and tag is based on backscattering of the same carrier, where reader expects to receive the same carrier. Since SDR tag is not synchronized to the reader's carrier due to oscillator frequency offset, for data backscattering we use the same received carrier with the offset.

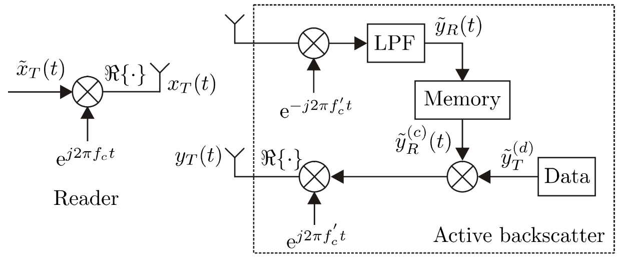

Fig. 4. Communication block scheme of the RFID reader-tag (active backscattering).

To accomplish active backscattering, received carrier pattern is stored in the memory container, amplified and modulated with tag's data (Figure 4).

To describe how to use reader's carrier, let us denote with $x_T(t)$ reader's up-converted signal, expressed as

$$x_T(t) = \Re\left\{\tilde{x}_T(t)e^{j2\pi f_c t}\right\} \quad (1)$$

where $\tilde{x}_T(t)$ and f_c represent reader's baseband signal and reader's carrier frequency, respectively. Baseband signal which tag receives is

$$\tilde{y}_R(t) = \left[\left(x_T(t) + n(t)\right)e^{-j2\pi f_c' t}\right] \otimes h_{LP}(t) \quad (2)$$

where $n(t)$ denotes noise, $h_{LP}(t)$ is the impulse response of the low-pass filter (LPF), $\otimes$ denotes convolution, and $\tilde{y}_R(t)$ represents received baseband signal with the tuned carrier frequency denoted with f_c', where $f_c \neq f_c'$. With $x_T(t)$ given by (1), we write

$$\tilde{y}_R(t) = \frac{1}{2}\left(\tilde{x}_{T,R}(t) - j\tilde{x}_{T,I}(t)\right)e^{j2\pi\Delta f t} + \tilde{n}(t) \quad (3)$$

where $\Delta f = f_c - f_c^{'}$ is the frequency offset, and $\tilde{x}_{T,R}(t)$, $\tilde{x}_{T,I}(t)$ represent real and imaginary baseband signal parts, and $\tilde{n}(t)$ is the down-converted noise. Then the up-converted tag transmitted signal $\mathrm{y_T}(t)$ is

$$\mathrm{y_T}(t) = \Re\left(\tilde{\mathrm{y}}_\mathrm{T}(t)e^{j2\pi f_c^{'} t}\right) \quad (4)$$

where $\tilde{\mathrm{y}}_\mathrm{T}(t) = \tilde{\mathrm{y}}_\mathrm{R}^{(\mathrm{c})}(t)\tilde{\mathrm{y}}_\mathrm{T}^{(\mathrm{d})}(t)$, and $\tilde{\mathrm{y}}_\mathrm{R}^{(\mathrm{c})}$ equals $\tilde{\mathrm{y}}_\mathrm{R}(t)$. Data part $\tilde{\mathrm{y}}_\mathrm{T}^{(\mathrm{d})}(t)$ represents Miller modulating subcarrier. If we use only the carrier for data modulation, then terms $\tilde{x}_{T,R}(t)$, $\tilde{x}_{T,I}(t)$ in $\tilde{\mathrm{y}}_\mathrm{R}^{(\mathrm{c})}$ are constant values *c*, and frequency of the carrier is the same on both $\mathrm{y_T}(t)$ and $\mathrm{x_T}(t)$ sides, which is given with

$$\begin{aligned} \mathrm{y_T}(t) &= \Re\left\{\left(\frac{1}{2}ce^{j2\pi\Delta ft} + \tilde{n}(t)\right)\tilde{\mathrm{y}}_\mathrm{T}^{(\mathrm{d})}(t)e^{j2\pi f_c^{'} t}\right\} \\ \mathrm{y_T}(t) &= \Re\left\{\frac{1}{2}c\tilde{\mathrm{y}}_\mathrm{T}^{(\mathrm{d})}(t)e^{j2\pi f_c t} + n(t)\tilde{\mathrm{y}}_\mathrm{T}^{(\mathrm{d})}(t)\right\} \end{aligned} \quad (5)$$

Sampled information data were prepared before signal processing, to assure minimal processing time. Developed SDR tag application uses array to store reader's CW pattern. The length of pattern is chosen in the way to store a few periods of sine wave (due to noisy sine wave, and to safely recognize zero crossing), and thus a larger pattern can be made by simply adding up the same pattern to the end of stored one.

Since we used USB 2.0 interface between SDR hardware and PC, sampling rate at the SDR sink and the SDR source were both set to the maximum throughput of 32MB/s that USB 2.0 can sustain, in order to fill in all buffers and to provide samples needed for processing as soon as possible. Processing of those samples would be time consuming, so we downsampled the signal to 500 kS/s ($t_s = 0.25 \cdot 10^{-4} s$), enough to fill out the requirements for SDR tag which uses 40 kHz Amplitude Shift Keying (ASK) backscattering modulation with 8 cycles Miller subcarrier. This approach still left 3 ms of latency, which is not enough for timely response to the *Query* command. Therefore we count frames and respond after one *Qrep* command. However, the usage of another bus for data transfer (e.g. PCIExpress [18]) would significantly reduce the latency and assure exact timing. Moreover, usage of embedded SDR platform would not have latency issue at all, since the whole processing part would be on single device.

IV. Measurement Setup and Performance Analysis

System tests were developed through SDR tag (Figure 5), which uses developed SDR application which implements fixed X10 amplification of the received signal. Figure 6 shows the measurement lab environment as well as performance results computed from

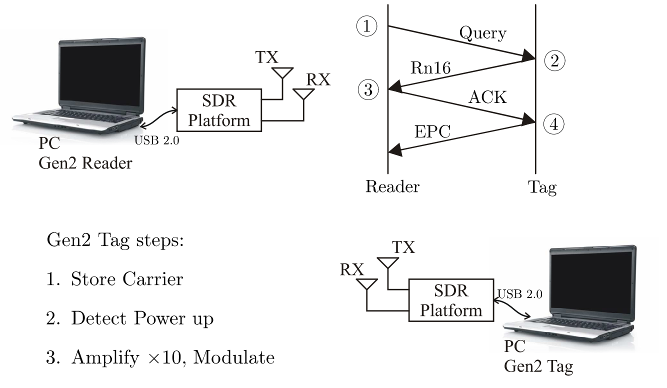

Fig. 5. Measurements setup, with the communication system block scheme. For performance measurements, SDR RFID reader [16] was used on one side and the developed SDR tag on another side.

$$\text{EPC Read Efficiency} = \frac{\text{Successful EPC Reading Rate}}{\text{Number of Inventory Rounds}} \quad (6)$$

where number of inventory rounds always equals 1000. For comparison with standard tag measurements, reader could read tags only 30 cm away with [16] transmitting at 200 mW.

The performance of the developed system can be compared with results obtained from familiar Friis Equation [2]

$$FSL = -20\log\left(\frac{\lambda}{4\pi d}\right) - (G_{TX} + G_{RX}) \quad (7)$$

With $f_c = 915$ MHz ($\lambda = 0.33$ m) and antennas gains $G_{TX} = G_{RX} = 6$ dBi, we obtained from (7) that in a free space SDR tag could be detected in a range up to $d = 105$ m. The measurement results we obtained on our test platform for SDR with CW sensitivity of -110 dBm [19], and with RFID reader with sensitivity of -80 dBm, are presented in Figure 6. In a case of SDR mobile phones, at the standard output power of 1W [15], it is reasonable to suppose that the system could respond from the distance of approximately 160 meters, even in a more noisy environments. Given ranges are obtained for fixed X10 amplification, without automatic gain control (AGC).

V. Conclusion

SDR technology generally allows great flexibility in the implementation of standard protocols and technologies, especially in the next mobile phones scenario usage. For testing purposes active backscattering SDR tag application has been developed and the reading results are presented. For a comparison, SDR tag can report through 2 walls, while standard RFID tags (labels) performances are degraded if tag is not in the reader's line of a sight. Developed SDR tag application can be used in noisy environments where tag identification performances are crucial. Our intention in this paper is to provide the proof of concept of building PHY/MAC

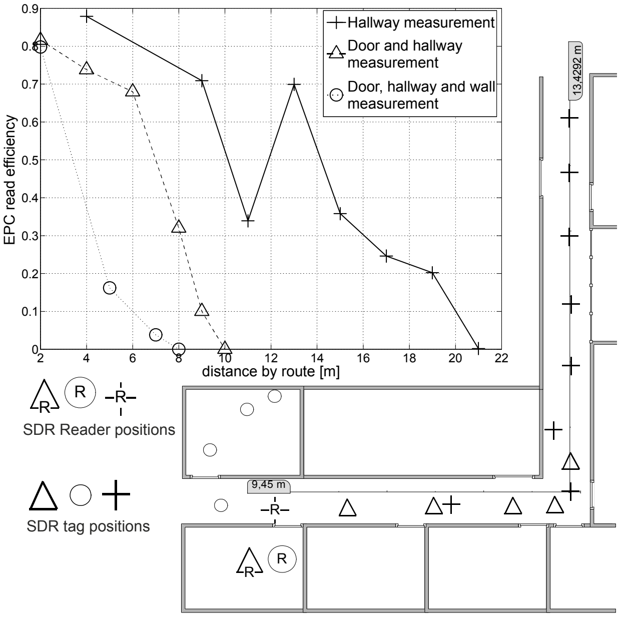

Fig. 6. Floor blueprint and the measurements plan. SDR tag reading performances are calculated from (6). Since the propagation after the Hallway corner is affected by diffraction at the edge and by reflected wave components, measurements at 11m and 13m are obviously affected by the two signal components. It is worth to mention that existing reader is reading regular tags only 30 cm away from reader antenna (200 mW of reader output power).

layer of Gen2 RFID tag using SDR. We did not provide attention to new opened numerous application scenarios and related security issues. Those concerns are left for the future research.

References

[1] D. D. Dobkin, *The RF in RFID*. Burlington, USA: Elsevier, 2008.

[2] W. Che, Y. Yang, C. Xu, N. Yan, X. Tan, Q. Li, H. Min, and J. Tan, "Analysis, Design and Implementation of Semi-Passive Gen2 Tag," in 2009 IEEE International Conference on RFID, (Orlando, USA), pp. 15–19, April 2009.

[3] H. Cho, J. Kim, Y. Baek, "Large-Scale Active RFID System Utilizing ZigBee Networks," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 2, pp. 379–385, May 2011.

[4] W. M. Mays and B. D. Moore, "Rfid Transponder Having Active Backscatter Amplifier for Re-transmitting a Received Signal," January 4. 2005. Patent. US 6,838,989 B1.

[5] F. Iannello, O. Simeone, and U. Spagnolini, "Energy Management Policies for Passive RFID Sensors with RF-Energy Harvesting ," in *IEEE* International Conference on Communications (ICC 2010), 2010, (Cape Town, South African Republic), pp. 1–6, May 23-27 2010.

[6] F. Thiesse, M. Dierkes, and E. Fleisch, "Lottrack: Rfid-based Process Control in the Semiconductor Industry," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 47–53, 2006.

[7] H.-S. Ahn and K. H. Ko, "Simple Pedestrian Localization Algorithms based on Distributed Wireless Sensor Networks," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4296–4302, 2009.

[8] D-G. Yun, J-M. Lee, M-J. Yu, S-G.Choi, "Agent-based User Mobility Support Mechanism in RFID Networking Environment," *IEEE Transactions on Consumer Electronics*, vol. 55, no. 2, pp. 800–804, May 2009.

[9] U. Ramacher, "Software-Defined Radio Prospects for Multistandard Mobile Phones," *IEEE Computer*, vol. 40, no. 10, pp. 62–69, 2007.

[10] C.H. van Berkel, "Multi-Core for Mobile Phones," Design, Automation & Test in Europe Conference and Exibition (DATE '09), (Nice, France), pp. 1260–1265, June 2009.

[11] Y. Tachwali, F. Basma, and H. H. Refai, "Cognitive Radio Architecture for Rapidly Deployable Heterogeneous Wireless Networks," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 3, pp. 1426–1432, August 2010.

[12] P. Ferrari, A. Flammini, and E. Sisinni, "New Architecture for a Wireless Smart Sensor Based on a Software-Defined Radio," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 6, pp. 2133–2141, 2011.

[13] D. D. Donno, F. Ricciato, L. Catarinucci, A. Coluccia, and L. Tarricone, "Challenge: Towards Distributed RFID Sensing with Software-Defined Radio," in Proceedings of the sixteenth annual international conference on Mobile computing and networking (MOBICOM '10), (Chicago, Illinois, USA.), pp. 97–104, September 20-24 2010.

[14] D. Shen, G. Woo, D. P. Reed, A. B. Lippman, and J. Wang, "Separation of Multiple Passive RFID Signals Using Software Defined Radio," in 2009 IEEE International Conference on RFID, (Orlando, USA), pp. 139–146, April 2009.

[15] EPCglobalInc, "Class1 Generation 2 UHF Air Interface Protocol Standard "Gen 2", v1.2.0," tech. rep., EPCglobal, October 2008.

[16] M. Buettner and D. Wetherall, "A Flexible Software Radio Transceiver for UHF RFID Experimentation," tech. rep., UW CSE, 2009.

[17] M. Buettner and D. Wetherall, "A Software Radio-based UHF RFID Reader for PHY/MAC Experimentation," in *2011 IEEE International Conference on RFID*, (Orlando, USA), pp. 134–141, April 2011.].

[18] K. Tan, J. Zhang, J. Fang, Y. Y. He Liu, S. Wang, Y. Zhang, H. Wu, W. Wang, and G. M. Voelker, "Sora: High Performance Software Radio Using General Purpose Multi-core Processors," in *NSDI 09: 6th USENIX* Symposium on Networked Systems Design and Implementation, (Boston, MA, USA), pp. 75–90, April 22-24 2009.

[19] N. Dodson, G. J. Bradford, and J. N. Laneman, "A High Performance RF Transceiver Implementation," in Proceedings of the SDR 10 Technical *Conference and Product Exposition*, (Washington, USA), pp. 652–658, 30 November - 3 December 2010.

Biographies

Petar Šolić received his Master's Degree from Computer science in 2008 at University of Split, Croatia. He is currently employed at the Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture (FESB), University of Split, Croatia, as a research assistant and Ph.D. student at Department of Electronics. His research interests include Information technologies, RFID technology and its application. He is author of several papers published at international conferences proceeding and journals.

Joško Radić (M'01) received his M.S. and Ph.D. degrees both in communication engineering from the University of Split in 2005 and 2009, respectively. He is currently Post Doctoral Researcher at the Department of Electronics, Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, University of Split. His research interests include wireless communications, signal processing, multicarrier systems, and coding theory. Dr. Radic is a member of IEEE Communications Society, Broadcast Technology, Consumer Electronics and Oceanic Engineering Societies. He is also a member of the Croatian Communications and Information Society (CCIS).

Nikola Rožić (M'89) received the B. S. Eng. Degrees in Electrical Engineering and Electronics from the Split University in 1968 and 1969, respectively, and the M.S. degree and the Ph.D. degree from the University of Ljubljana in 1977 and in 1980, respectively. Currently, he is a Full Professor in electrical and computer engineering and a head of the group for telecommunications and information systems with the Department for Electronics of the University of Split (FESB). His research interest includes information and communication theory, signal processing, source and channel coding, prediction methods and forecasting.