

Programmable Logic Devices in Sensor Networks: A Survey

Lucas Iacono^{1,3,4}, Pablo Godoy^{1,4}, Ricardo Cayssials², Osvaldo Marianetti^{3,4}, Carlos García Garino^{1,4,5}

¹ITIC, Instituto universitario para las Tecnologías de la Información y las Comunicaciones, UNCuyo

²Ingeniería Eléctrica y de Computadoras, Universidad Nacional del Sur

³Facultad de Ingeniería, Universidad de Mendoza

⁴LAPIC, Laboratorio de Investigación y Desarrollo para la Producción Integrada por Computadora, Carrera de Redes y Telecomunicaciones, ITU

⁵Facultad de ingeniería, Universidad Nacional de Cuyo

lucas.iacono@um.edu.ar, pgodoy@itu.uncu.edu.ar,
ricardo.cayssials@uns.edu.ar, osvaldo.marianetti@um.edu.ar,
cgarcia@itu.uncu.edu.ar,

Abstract. This paper presents a survey about the use of reconfigurable hardware technologies in sensor networks, considering proposals published in two of the leading conferences of Programmable Logic Devices: FPL and SPL. These proposals cover different applications such as wireless communications, different networks topics and sensors. Some of the papers considered in this survey are directly related with WSN, such as reconfigurable nodes or low-power hardware platforms intended for sensor networks. Other papers are not directly related to WSN, but they present results and concepts that may be of interest in the field of the WSNs.

Keywords. WSN, FPGA, Ad Hoc Networks, Reconfigurable Architecture.

1 Introduction

The low cost of microcontrollers facilitates the diffusion of new sensors, often called “smart sensors” or “smart transducers”. These devices are replacing traditional analog sensors. Smart sensors provide improvements in terms of linearity, signal-to-noise ratio and diagnostic features; in many cases, they also support network connectivity [1].

Thanks to the possibility of forming a network, the smart sensors can interact to fulfill tasks that usually, a single node is incapable to do. They use wired or wireless communication to enable this collaboration. The medium used (wired or wireless) depends on the application to implement and will be evaluated for each particular case. Healthcare need sensor compactness and wireless communications [2], in applications like automotive and home automation, low cost is a determining factor [3]. Industrial applications (e.g. factory automation and process control) have very

different network requirements. Generally a sensor network is evaluated with respect to some characteristics such as: extension of the network (generally affected by the physical mean), and mobility (that implies wireless sensors with autonomous power source) [4].

In case of Wireless Sensor Networks (WSN) the data sensed by the smart sensors (known as nodes in WSN) can be transferred to a Gateway, and transmitted through different types of networks (such as Internet) toward computer systems. Nodes can also have the capacity to act on the environment. WSNs are mostly used in, low bandwidth and delay tolerant applications, ranging from civil and military to environmental and healthcare monitoring [5]. The nodes that make up a wireless sensor network must meet requirements of autonomy, low power consumption, low cost and robustness.

The aim of this paper is to review the diverse applications of reconfigurable hardware, which give results that can be useful and applicable to the different topics that integrate wireless sensor networks (hardware, network security, connectivity and application).

Among the topics related to WSN, low power consumption is imperative, thus we have selected papers from FPL and SPL conferences, that study consumption reduction in network applications. Most WSN applications do not need a high speed data transmission, but the constantly advancement of mWSN [6] (multimedia wireless sensor network) and transport systems [7] makes it necessary to examine papers related to the use of FPGA in wireless high speed networks (e.g. WiMax).

In applications like factory automation, process control and security alarm systems, it necessary to implement network security techniques to prevent attacks or data theft. Some implementations may require nodes that can adapt them to changing environmental conditions (it is useful that nodes obtain some benefit from the new conditions), or changing needs of users, such as, sensing new variables or transmit data with greater or lesser degree of accuracy, for which were considered works that study the FPGAs use in smart sensors.

This paper is organized as follows: Section 2 presents the review of papers related with sensor networks and nodes. Section 3 studies network security, high speed data traffic and connectivity papers. And finally Section 4 concludes this paper.

2 Wireless Sensor Networks and Nodes

This section presents the review of papers related with WSN. It is divided into subsections where each subsection corresponds to a paper, and the subsection title is the paper title

2.1 Energy Management in Battery-Powered Sensor Networks with Reconfigurable Computing Nodes.

In [8], Khan *et al.* investigate the benefits of using reconfigurable hardware in sensor networks. For this purpose, they compare a node based on a fixed hardware platform, consisting of a processor, with a reconfigurable hardware based node implemented in

a FPGA (Field Programmable Gate Arrays).

The network proposed consists of nodes randomly distributed in the field, which send data to an energy-rich sink node.

Nodes based on reconfigurable hardware change their behavior by reconfiguring themselves in order to adapt to lower power implementations, thus extending the life of the network. This is achieved by modifying the power consumption and the execution time.

An experiment was conducted, for which 50 nodes were deployed in an area of 50x50 meters, with a sink node. The maximum range of each node was 11 meters. Ten animals were used, which moved randomly and caused the sensors to generate traffic when detect an event. The experiment was simulated using LetLogo2.1. It was used an accurate battery model proposed by Rakhmatov *et al.* [9], which is based on the laws of chemical kinetics, which takes into account the rate effect and recovery capacity effect [8].

The authors calculated the lifetimes for both types of nodes (reconfigurable hardware nodes and hardware fixed node). The lifetime calculations are performed using the following relationship:

$$P_{pc}=K.P_{tx} \quad (1)$$

P_{pc} is the processing power and P_{tx} is the transmission power for a given number of packets. The authors study the effect of varying the K parameter. This means to change the current consumption during packet processing. The transmission power, depends on the distance between nodes and this cannot be modified (depends on the application), while the processing power can be modified by using reconfigurable computing. For values of $K = 10$, the lifetime of a reconfigurable hardware node is 4.99 times greater than for a node with the fixed hardware. For $K = 1$, the life of reconfigurable hardware node is 1.63 times higher.

Khan *et al.* conclude that reconfigurable computing nodes are appropriate when $K \geq 1$. This means that the processing power in the nodes is greater than the transmission power. The authors state that: the use of reconfigurable hardware nodes for values $K < 1$ is not justifiable.

It is necessary to consider whether the condition $K > 1$ is fulfilled in real applications. Khan *et al.* assume that the receiver section of transceiver has a constant consumption, but this is not common in current WSN nodes, which turn off their transceivers (both transmit and receive sections) when they are not in use (for example, XBee nodes [10]).

2.2 Exploiting Analog and Digital Reconfiguration for Smart Sensor Interfacing

The IEEE 1451.4 standard describes a set of open communication interfaces for connecting sensors or actuators to processors, instrumentation systems or communication networks and enabling plug-and-play capabilities for sensors. It

describes a set of open, common, network-independent communication interfaces for connecting transducers (sensor or actuators). The standard defines the Transducer Electronic Data Sheets (TEDS), which consists of a memory attached to the sensor, which stores information about it (identification, calibration, correction data, measurement range, manufacture-related information, etc.), and the Network Capable Application Processor (NCAP). The NCAP is a device between the STIM (smart transducer interface module) and the network, that performs network communications, STIM communications, data conversion functions, and application functions.

Morales *et al.* [11] propose the use of FPGA and FPAA (Field Programmable Analog Arrays) to implement smart sensors, instead of processor-based platforms. Specifically, the authors propose to implement a NCAP device using FPAAs and FPGAs. In the proposed platform, the FPAAs perform tasks of signal processing, analog to digital conversion, linearization of nonlinear responses, waveform synthesis, etc. The FPGAs perform tasks such as: sensor type detection (by reading the TEDS), finding appropriate settings for the FPAA (stored locally or remotely), processing of digital data supplied by the FPAA, data transmission to external networks, TCP/IP connections, remote control, etc.

The authors state that the use of processors to implement smart sensor systems is suitable for small designs. But these platforms have problems when system requirements grow (for example, for tasks such as filtering, threshold detection or scaling). In this case, the authors state that an FPGA-based platform may be more appropriate since it can handle concurrent tasks, and even a microprocessor can be embedded.

The authors state that another advantage of FPGA-based platforms over microcontroller-based platforms is the relative independence of FPGAs with regard to manufacturers, while the processors have different architectures depending on the suppliers, and even between families from the same vendor, making it difficult to change from a platform to another. To test this platform, the authors implemented an environmental monitoring application, using temperature sensor and a pressure sensor.

2.3 Design and Evaluation of an Energy-Efficient Dynamically Reconfigurable Architecture for Wireless Sensor Nodes

Hinkelmann *et al.* present the design of a reconfigurable platform for WSN nodes [12], and compare its energy consumption, area and performance against ASIC and RISC processors platforms. The authors implement two different architectures over these three platforms: a LEON2 32-bit RISC architecture, and an Atmel's 8-bit ATmega AVR architecture.

The motivation of this paper is the affirmation that processors generally cannot provide high energy efficiency for data processing on the nodes, whereas ASICs are usually too costly. The authors propose a unit called Reconfigurable Function Unit (RFU). This hardware was developed based on typical WSN characteristics. The

conventional processor platforms are designed without RFU, so all tasks are run in software.

The RFU unit is composed of different types of dedicated operator blocks of 8-bit. These blocks include a multiplication-accumulation module (MAC), consisting of an array of 4x4 cells. Each cell consists of a multiplier, an adder and 3 records. It also includes an inverter module that consists of 4 blocks working in parallel, a register module, local memory module of 256 bytes and an interface to the main system memory. See Figure 1.

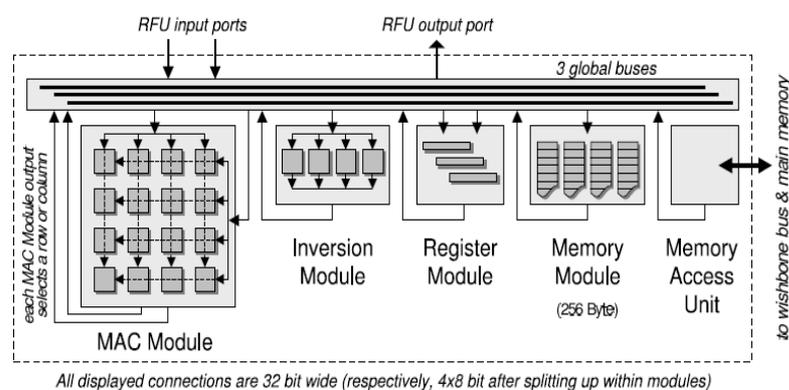


Fig. 1. Modular structure of the RFU data path [12]

The reconfiguration mechanism is described in the papers of Hinkelmann *et al.* [12] and [13]. All architectures are evaluated as VHDL models. As the authors state, this excludes a direct comparison.

A set of benchmark task was defined to run on each on each platform and each architecture. These tasks were: Computing a CRC checksum, decoding a BCH [14] code word, encryption of a block of data according to the AES standard [15] and key generation for AES encryption task.

In order to estimate power consumption was used Synopsys tool PrimePower. The experiments were performed assuming the worst scenario, in which a complete reconfiguration of the RFU is required before each task.

The authors note the small area occupied by the RFU, which is 0.45 mm², while it is in the order of 2 mm² for the other implementations. The cost of dynamic reconfiguration never reached critical levels, neither for latency nor energy consumption, Hinkelmann *et al.* attribute this fact to the reconfiguration mechanism cited in [13].

The conclusions of the study are that the RFU obtained execution times 6 to 10 times faster compared with RISC processors and ASICs microprocessors, for LEON2 architecture, and 6 to 14 for the AVR architecture.

Regarding to energy consumption, the RFU achieved a energy saving by a factor of 4 to 6 for LEON2 architecture, and 1.8 to 2.5 for AVR architecture. This leads the authors to conclude that the RFU has an important potential in WSN compared to architectures based on microprocessors.

With regard to energy consumption, the RFU is between ASICs and processors. However, the cost of ASIC-based platforms is higher. The authors reported consumption in the order of mW.

Due to the reasons explained above, RFU based platforms, are highly suitable for power-constrained applications, such as WSN. However, the authors do not compare the RFU platform against processor-based platforms with respect of the cost. This is a very important issue, since the low cost is a key parameter in WSNs. This is probably a disadvantage for a platform based on RFU, due to the low cost of current commercial platforms based on microprocessors.

2.4 Interconnecting Heterogeneous Nodes in an Adaptive Computing Machine

F. Furtek *et al.* [16] outline a network for interconnecting heterogeneous nodes in Adaptive Computing Machine (ACM). The authors define ACM as a collection of heterogeneous nodes interconnected by a scalable network. ACM are targeted for mobile, low cost and wireless devices, amongst others. [16].

The authors focus their work on two aspects of ACM architecture: A PTP (point to point) protocol for transferring data in real time, and a concept that they define as "node wrapper" that allows all nodes appear homogeneous regardless of their internal structure or functionality. The wrapper node also provides a mechanism for handling tasks, flow control and load balancing across all nodes.

The paper also introduces the network topology and protocols of the ACM architecture (these issues are not discussed in this survey). We rescued from this study the node architecture defined by the authors. Each node consists of 3 elements: a wrapper node, an execution unit (EU) and a memory.

The wrapper node makes the nodes identical in outward appearance, regardless of their internal structure or functionality. Among other things, the wrapper gives to the data an appropriate format, when they reach the node, or when data are sent by the node.

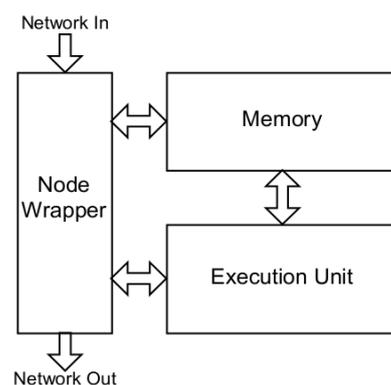


Fig. 2. Node wrapper [16]

2.5 A Reconfigurable Prototyping Platform for Smart Sensor Networks

The paper of Hinkelmann, H. *et al.* [17] presents a platform designed to rapid prototyping of wireless sensor networks. The platform is based on FPGA in order to achieve 3 major objectives: to emulate arbitrary node architectures (including smart nodes with high system complexity), to realize flexible interfaces to sensors and radio transceivers, and to embed versatile debugging and system monitoring functionality.

The prototype platform comprises four separate layers: sensing layer, communication layer, processing layer, and power supply layer (Fig. 3). This allows to implement the main functionalities of a node separately and replace certain layer implementations quickly [17].

To meet its objective, the platform requires the use of a considerable amount of logic resources. As a result, the processing layer will consist of a FPGA with high gate count. Its function is to emulate the digital part of the prototyped mote.

The sensing layer enables the use of arbitrary sensor types and allows to replace them easily by providing a simple plug-in mechanism. A slot-based concept is employed to connect small sensor modules to the platform. In order to use a specific sensor, is necessary a small PCB module for the sensor type, which can be plugged into a slot and routes some of the generic signals to the sensor pins. Besides the sensor, the module may also contain other components, e.g. for A/D conversion if the sensor has analog outputs, or sensor-specific supply or reference voltages.

For the power supply layer, the authors propose the usage of two different instances: line power and batteries. The battery-powered version uses four AA batteries (connected in series) with a capacity of 2700 mAh each one.

For debugging and monitoring system support, the authors use a wired network (Ethernet), which operates independently of the primary wireless network and therefore does not compromise the application under test. This allows remote access to all nodes in a network by a PC, and provides sufficient data rates and reliability to get detailed information about the nodes.

The authors state that it is possible to integrate additional monitoring components into the FPGA together with the nodes system. The information can be transmitted over the Ethernet link to a PC for sensor network monitoring and debugging.

Experimental results showed that the power consumption of the prototype varies between 0.7 W and 1.1 W for a clock frequency of 11 MHz, depending on the usage of the transceiver and the LEDs. Thus, batteries can supply the prototype for more than 10 hours in practical experiments.

The authors state that, in the future, the lifetime of the battery-powered version might be increased by the use of upcoming low-power FPGAs and FPGA power management techniques allowing to switch between active and low-power modes during run-time [17].

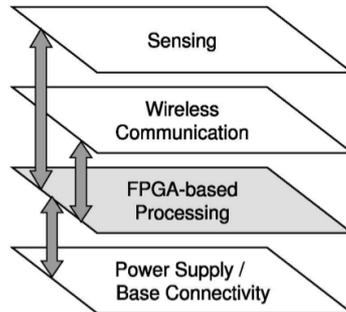


Fig. 3. Layer Model of the Prototype Platform [17]

2.6 A Reconfigurable FPGA-Based Architecture for Modular Nodes in Wireless Sensor Networks

The work of Portilla, J. *et al.* [18] presents a platform for sensor networks. This includes an FPGA platform that allows the node can be reconfigured to process signals from sensors with different interfaces without the need to redesign the system. The platform (first implementation) includes four layers, which are physical PCBs (Fig 4): communication layer, power supply layer, processing layer and sensing layer.

For the communication layer, the authors have chosen Bluetooth as a first approach. They justify their choice in that Bluetooth is a quite developed technology and there are a huge variety of commercial modules with the full protocol stack implemented. The ZigBee technology has been integrated in a new communication layer.

The power supply layer can use batteries or line power.

The processing layer consists of a microcontroller and a FPGA. In this layer the signals from the sensors are converted into digital and processed. The control of the communications are made in this layer by generating commands to the Bluetooth module, and interpreting commands from this module and other network nodes (these tasks include searching for neighbour nodes, setting and breaking links, and management of all the tasks related with the network). Power saving modes (which have the function of prolonging the life of the battery) are managed in this layer.

The sensing layer includes sensors and actuators. Multiple types of sensors can be included in this layer. This first implementation includes sensors of temperature, humidity, acceleration, threshold light, light intensity and infrared sensors. The digital sensors are connected directly to the FPGA. The FPGA processes the digital signals and sends the processed data to the microcontroller. The microcontroller takes the data and sending the information to the network. The microcontroller processes the analog signals directly, through its analog to digital converter.

As for remote reconfiguration, is not feasible to reconfigure nodes independently, because the network can consist of hundreds or thousands of nodes. Instead, it can be possible, for example, to reduce power consumption or to accelerate the processing when the application demands it. This feature can be implemented by sending the new bit stream to the FPGA, for reconfiguring it partial o totally.

The results reported in this paper show that FPGAs are not the best candidates for low power applications. However, the authors state that manufacturers are working in order to achieve new goals in power consumption of reconfigurable devices.

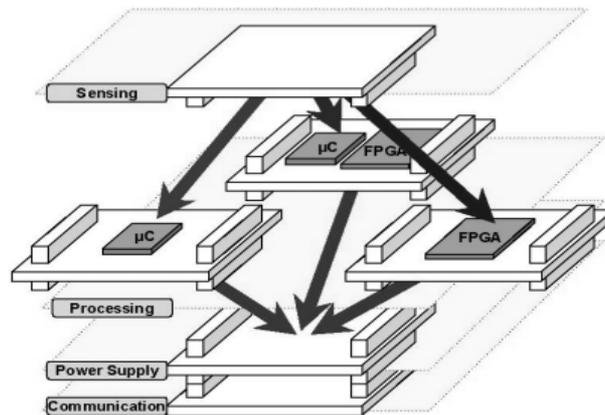


Fig. 4. Modular platform for wireless sensor networks [18]

3 Network Security, High Speed Data Traffic and Connectivity

The work of Ojail, M *et al.* [19] presents a reconfigurable unit capable of performing filtering and Fast Fourier Transform (FFT) to be used with a wireless communication standards.

Finite Impulse Response (FIR) filters are very important blocks in the Wideband Code Division Multiple Access (WCDMA) technique, and the UMTS standard is based on WCDMA. Direct an inverse Fast Fourier Transform are important functions on the Orthogonal Frequency Division Multiplexing (OFDM) technique [19].

The paper presents a new reconfigurable unit capable of executing variable-size FFT and frequency domain FIR filters. The study of FFT in WSN has been discussed by several authors. F. Zhao *et al.* [20] and H. Karl *et al.* [21] analyze the possibility to do some signal processing operations (which usually need a high power consumption and computational resources) such as fast Fourier transform, by using the nodes of the WSN.

The work of Huang-Chun Roan *et al.* [22] introduce a new architecture based on FPGA to be used as Network Intrusion Detection System (NIDS). A NIDS monitors the network for suspicious data patterns and activities, and it reports if malicious traffic is detected.

Many NIDS such as SNORT prevent computer networks against attacks using pattern-matching rules [22]. The computational complexity of these systems can be high due to the requirements of the string matching during their detección processes. The SNORT systems running on general purpose processors can only achieve relatively low throughput due to its high computational complexity. As a result, some malicious traffic may be dropped and then not be detected.

The objective of the work of Huang-Chun Roan *et al.* is to present a novel FPGA implementation approach for NIDS that achieves both high throughput and low area cost.

The work of Sghaier *et al.* [23], it is a implementation of a 802.16-2004 PHY Layer. The work consist of two approaches who are used to map the IEEE 802.16-2004 OFDM functions into FPGAs. The authors presents a complete OFDM transmitter implementation on a single FPGA with performance approaching 200 MHz.

Ortega-Cisneros, S. *et al.* [24] proposes a control system of mobile robots which moving in defined areas. The system is based on local processors installed on each robot and fixed workstations. The communication is wireless. The transmitter module was implemented with a Xbee Pro circuit [10].

4 Conclusions

The FPGA offers features of interest in the field of WSN, such as: flow data optimization, the use of different protocols, enhance the security of network in critical applications, adaptation to specific applications and to different environments, etc. However FPGAs have two major disadvantages compared to RISC processors: higher energy consumption and greater cost. Because low power and low cost are crucial parameters in WSN, the great majority of developments for WSN are based on RISC processors. However, this paper presents various FPGA applications in WSN, which shows that the FPGA can be useful for solving certain problems of WSN, besides the interest of researchers in these applications. In addition, there are many researchers working to reduce consumption and cost of the FPGA. This will allow the development of more applications of these plafaformas in the field of WSN.

5 Acknowledgements

The authors acknowledge the financial support received from the Instituto de Desarrollo Industrial Tecnológico y de Servicios (IDITS) and the Agencia Nacional de Promoción Científica y Tecnológica (ANPCyT), through the project PID-PAE 146 Embedded and Sensor Grid. Lucas Iacono and Pablo Godoy thank doctoral fellowships awarded by the ANPCyT through the project PID PAE-146 and program PRH funded by the ANPCyT and UNCuyo, respectively.

6 References

1. A. Flammini, P. Ferrari, D. Marioli, E. Sisinni, A. Taroni, "Wired and wireless sensor networks for industrial applications", *Microelectronics Journal*, Volume 40, Issue 9, Quality in Electronic Design; 2nd IEEE International Workshop on Advances in Sensors and Interfaces; Thermal Investigations of ICs and Systems, September 2009, Pages 1322-1336.
2. H.S. Ng, M.L. Sim, C.M. Tan, C.C. Wong, *Wireless technologies for telemedicine*, BT

- Technol. J. (Kluwer Academic Publishers) 24 (2) (2006)130–137.
3. C. Gabriel, H. Horia, Integrating sensor devices in a LIN bus network, in: 26th
 4. S.P. Beeby, M.J. Tudor, N.M. White, Energy harvesting vibration sources for microsystems applications, *Meas. Sci. Technol.* 17 (12) (2006) R175–R195.
 5. Potdar, V.; Sharif, A.; Chang, E.; , "Wireless Sensor Networks: A Survey," *Advanced Information Networking and Applications Workshops*, 2009. WAINA '09
 6. Sharif, A.; Potdar, V.; Chang, E.; , "Wireless multimedia sensor network technology: A survey," *Industrial Informatics*, 2009. INDIN 2009. 7th IEEE International Conference on , vol., no., pp.606-613, 23-26 June 2009.
 7. Ben-Jye Chang; Bo-Jhang Huang; Ying-Hsin Liang; , "Wireless Sensor Network-Based Adaptive Vehicle Navigation in Multihop-Relay WiMAX Networks," *Advanced Information Networking and Applications*, 2008. AINA 2008. 22nd International Conference on , vol., no., pp.56-63, 25-28 March 2008
 8. Khan, J.; Vemuri, R.; , "Energy management in battery-powered sensor networks with reconfigurable computing nodes," *Field Programmable Logic and Applications*, 2005. International Conference on , vol., no., pp. 543- 546, 24-26 Aug. 2005
 9. Rakhmatov, D.; Vrudhula, S.; Wallach, D.A.; , "A model for battery lifetime analysis for organizing applications on a pocket computer," *Very Large Scale Integration (VLSI) Systems*, *IEEE Transactions on*, vol.11, no.6, pp. 1019- 1030, Dec. 2003.
 10. Digi International Inc. "Data Sheet XBee ZB and XBee ZB Pro". Retrieved June 2010, from www.digi.com.
 11. Morales, D.P.; Garcia, A.; Palma, A.J.; Olmos, A.M.; Castillo, E.; , "Exploiting Analog and Digital Reconfiguration for Smart Sensor Interfacing," *Field Programmable Logic and Applications*, 2007. FPL 2007. International Conference on , vol., no., pp.706-709, 27-29 Aug. 2007
 12. Hinkelmann, H.; Zipf, P.; Glesner, M.; , "Design and evaluation of an energy-efficient dynamically reconfigurable architecture for wireless sensor nodes," *Field Programmable Logic and Applications*, 2009. FPL 2009. International Conference on , vol., no., pp.359-366, Aug. 31 2009-Sept. 2 2009
 13. Hinkelmann, H.; Zipf, P.; Glesner, M.; , "A scalable reconfiguration mechanism for fast dynamic reconfiguration," *ICECE Technology*, 2008. FPT 2008. International Conference on , vol., no., pp.145-152, 8-10 Dec. 2008
 14. P. Sweeney, *Error control coding: from theory to practice*. John Wiley & Sons Ltd, 2002.
 15. J. Daemen and V. Rijmen, *The Design of Rijndael: AES - theAdvanced Encryption Standard*. Springer Verlag, 2002.
 16. F. Furtek, E. Hogenauer, and J. Scheuermann, "Interconnecting Heterogeneous Nodes in an Adaptive Computing Machine," *Proc. Field-Programmable Logic and Applications (FPL)*, pp. 125-135, Sept. 2004.
 17. Hinkelmann, H.; Reinhardt, A.; Varyani, S.; Glesner, M.; , "A Reconfigurable Prototyping Platform for Smart Sensor Networks," *Programmable Logic*, 2008 4th Southern Conference on , vol., no., pp.125-130, 26-28 March 2008
 18. Portilla, J.; Riesgo, T.; de Castro, A.; , "A Reconfigurable Fpga-Based Architecture for Modular Nodes in Wireless Sensor Networks," *Programmable Logic*, 2007. SPL '07. 2007 3rd Southern Conference on , vol., no., pp.203-206, 28-26 Feb. 2007
 19. Ojail, M.; David, R.; Chevobbe, S.; Demigny, D.; , "A reconfigurable FIR/FFT unit for wireless telecommunication systems," *Field Programmable Logic and Applications*, 2009. FPL 2009. International Conference on , vol., no., pp.645-648, Aug. 31 2009-Sept. 2 2009.
 20. F. Zhao and L. Guibas. *Wireless Sensor Networks – An Information Processing Approach*. Elsevier/Morgan-Kaufman, Amsterdam, NY, 2004.

21. H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*, Wiley, London, New York (2005).
22. Huang-Chun Roan; Wen-Jyi Hwang; Chia-Tien Dan Lo; , "Shift-Or Circuit for Efficient Network Intrusion Detection Pattern Matching," *Field Programmable Logic and Applications*, 2006. FPL '06. International Conference on , vol., no., pp.1-6, 28-30 Aug. 2006
23. Sghaier, A.; Areibi, S. & Dony, R. IEEE802.16-2004 OFDM functions implementation on FPGAS with design exploration. *Proc. Int. Conf. Field Programmable Logic and Applications FPL 2008*, 2008, 519-522
24. Ortega-Cisneros, S.; Raygoza-Panduro, J.J.; de la Mora, A.; Castillo, O.; , "Implementation of a Wireless Control System with Self Timed Activation for Mobile Robots," *Programmable Logic*, 2008 4th Southern Conference on , vol., no., pp.205-208, 26-28 March 2008