Secure, Mobile Visual Sensor Networks Architecture

E. Ladis
Hellenic Aerospace Industry, Greece
egladis@haicorp.com

I. Papaefstathiou
Telecommunication Systems Institute, TU Chania, Greece
ygp@ece.tuc.gr

R. Marchesani
Thales Telecommunication, Italy

K. Tuinenbreijer
Philips Consumer Lifetime, Netherlands

P. Langendörfer
IHP, Germany

T. Zahariadis, H. C. Leligou
TEI of Halkida, Greece

L. Redondo
Metodos y Tecnologia, Spain

T. Riesgo
Universidad Politécnica de Madrid, Spain

P. Kannegiesser
Lippert, Germany

M. Berekovic
TU Braunschweig, Germany

C. J. M. van Rijn
Nanosens, Netherlands

***Abstract*: As Wireless Sensor Network–based solutions are proliferating they are facing new challenges: they must be capable of adapting to rapidly changing environments and requirements while their nodes should have low power consumption as they usually run on batteries. Moreover, the security aspect is crucial since they frequently transmit and process very sensitive data, while it is important to be able to support real-time video or processed images over their limited bandwidth links. SMART targets to design and implement a highly reconfigurable Wireless Visual Sensor Node (WVSN) defined as a miniaturized, light-weight, secure, low-cost, battery powered sensing device, enriched with video and data compression capabilities.**

Index Items: component Wireless sensor networks, reconfigurable hardware, security, video transmission

I. INTRODUCTION

The "Internet of the Things" is currently one of the major networking trends. It is foreseen that in the near future, any device or asset, even tiny wireless sensors, may be accessible and traceable, anytime and from anywhere, through the next generation (mobile) Internet. On the other hand, Wireless Sensor Networks (WSNs) have been identified as one of the most important technologies for the 21st century [1] and according to current market projections, more than half a billion nodes will have been shipped for wireless sensor applications by 2010. The evolving "Internet of Things" raises even more the already high hopes of WS[1]N and has attracted the interest of the research community and the electronics development giants worldwide. Before their wide deployment however, WSNs have to solve some significant problems; they must be capable of adapting to rapidly changing environments and requirements while their nodes should have low power consumption since they usually run on batteries. Moreover, the security aspect is crucial since they frequently transmit and process very sensitive data, while it is important to be able to support real-time video or processed images over their limited bandwidth links.

In general, there are specific and very important, for numerous application domains, features of WSNs such as high-security levels [2], low-power consumption [3], video-capabilities, auto-configuration and self-organization [4], [5] that are not efficiently addressed by today's offerings; SMART (Secure, Mobile visual sensor networks ArchiTecture) aims at providing an infrastructure that will support all those features efficiently and inexpensively. This innovative infrastructure will be based on both an off-the-shelf reconfigurable device and on a specially designed and implemented, within SMART, Reconfigurable Application-Specific Instruction-set Processor (RASIP). The SMART system will also take advantage of the partial real-time reconfiguration feature of state-of-the-art reconfigurable devices and will be able to alter their processing tasks according to the environment in which the sensor network operates so as to allow for very power efficient operation under the rapidly changing sensor environment.

The ultimate objective of SMART is to deliver a reconfigurable sensor platform prototype with excessive cross-domain applicability. In SMART, we foresee that in a few years each individual will be surrounded by his/her own Personal Area Sensor Network as well as by various WSNs, while the vision of ambient intelligence and the "Internet of Things" require extended usage of intelligent nano-sensors. Thus, we have to place the user at the centre of the future developments and offer efficient and secure WSN embedded infrastructures at personal and environment basis, which will be part of every day's activities of millions of European citizens.

This work constitutes background for the ARTEMIS project ARTEMIS-2008-100032 SMART (Secure, Mobile Visual Sensor Networks Architecture), www.artemis-smart.eu .

978-1-4244-3938-6/09/$25.00 (c)2009 IEEE

II. TECHNICAL APPROACH AND INNOVATIONS

The SMART project will progress the state-of-the art, described in the previous section, in numerous ways. It will provide a very flexible and efficient WSN node combining high-levels of security and video-capability with low power consumption and unprecedented levels of flexibility. Fig. 1 depicts the reconfigurable FPGA-based hardware architecture which will be used for the implementation of the video and data compression as well as the security- related algorithms. It is interesting to notice that for each considered function, more than one algorithms will be implemented and the node can be (re)configured to execute any of the developed blocks.

SMART's most innovative components are:

a) Develop and implement, in hardware, novel encryption/authentication systems addressing WSN's requirements. As no hardware-based encryption schemes exist for WSNs' environments, SMART will develop and implement in the nodes' reconfigurable device a number of novel such schemes that will consume small amounts of energy while being more secure than the existing software-based solutions. Special emphasis will be placed on the reduction of energy consumption.

b) Develop and implement, in hardware, innovative data-compression systems addressing WSN's requirements. SMART will develop and implement in the nodes' Reconfigurable Device a number of novel compression modules that will compress efficiently the WSN's data therefore reducing the power consumption for the transmission of them.

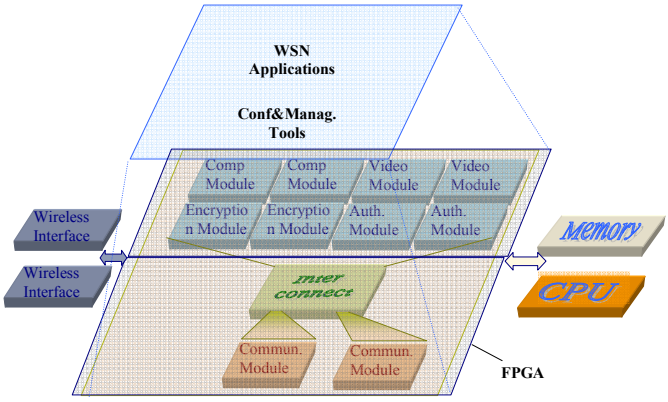

Figure 1. FPGA-based Architecture

c) Develop and implement in hardware pioneering video-compression systems addressing WSN's requirements. Recent video-compression algorithms provide scalability features so that : (1) all heterogeneous clients are able to decode video streams (whatever CPU/hardware resources they have) and (2) it is possible to easily transcode video streams to adapt it to available bandwidth. The SMART approach of having specialised hardware resources which also offer real-time reconfigurability so as to fulfil specific (and changing over-time) bandwidth requirements which also heavily reduces the overall power consumption is very innovative. Thus, those systems will enable, for the first time, the transmission of relatively high-quality video over the low-bandwidth and low power infrastructure of certain WSNs.

d) Develop and implement a novel reconfigurable processing device (called RASIP) that makes use of reconfiguration technology and have a low-power CPU on the same chip. The envisaged architecture is shown in fig. 2. The integration of FPGA-like technology and a low-power CPU on the same chip will offer unprecedented power savings for future wireless sensor nodes technology. This task would be heavily facilitated by a sophisticated design flow that two of the partners are using extensively; this tool will take as the input the encryption, authentication, video- and data-compression schemes developed and create an ASIP which will be optimised for those algorithms. Then a special real-time reconfiguration mechanism will be added. The final specially designed reconfigurable ASIP (RASIP) will trigger power savings of up to an order of magnitude when compared with an off-the-shelf FPGA.

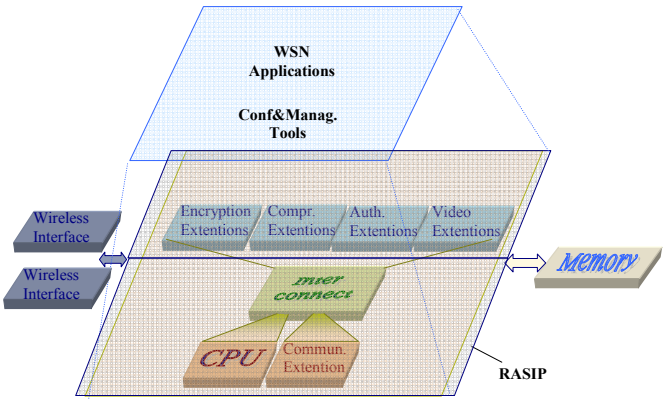

Figure 2. RASIP-based Architecture

e) Develop and implement an innovative middleware framework allowing the end-user to seamlessly take advantage of the novel features of the SMART infrastructure. The developed middleware will provide an abstract, yet efficient, framework for programming, configuring and managing the developed hardware infrastructure. The designed middleware will co-operate with the self reconfiguring mechanisms, and will allow the end-user to easily incorporate the provided by the SMART infrastructure innovative features in his/her applications.

f) Implement highly-secure nodes providing high resistance to side-channel attacks. There have been certain schemes proposed for increasing the resistance of hardware modules to side-channel attacks which however, do not take into account the low-power budget that the WSN environment implies, (e.g. such as the dual-rail encoding technique, or the random-switching one). Within SMART we will investigate the existing solutions and develop and implement a similar approach, that will increase the resistance to those attacks, while only modestly increase the power consumption of the node.

g) Develop and implement mechanisms and architectures for real-time partial reconfiguration that will be optimised for low-power consumption. All the real-time reconfiguration schemes that have been implemented and presented so far are optimised for high-performance. In the case of WSNs the critical factor is the power consumption, so certain mechanisms and hardware organizations that will take advantage of the real-time partial reconfiguration features of today's Reconfigurable Devices will be developed and implemented. This is certainly an open-research problem, and the scheme that will be proposed will also be very useful in other low-power environments (e.g. battery-operated stand-alone embedded systems).

h) Propose and implement a mechanism that will allow for the self reconfiguration of the nodes based on the conditions of the environment. The reconfiguration aspect of the SMART nodes, together with a novel mechanism that will be developed, will allow the node to be configured in a very-close-to-optimal manner at any given time. For example the security levels will be altered depending on the threat imposed by the environment, the compression tasks enabled/disabled depending on the available battery power, and the video-compression tasks altered depending on the quality needed at a given period. This flexibility will certainly make the SMART nodes more useful than any other nodes currently proposed for a variety of different WSNs environments. The self-reconfiguration mechanisms will be applicable to both off-the shelf FPGA and RASIP.

One of the major advantages of the SMART framework is its ability to support various modes of operations (e.g. low-power and low-secure one, high-power and high-quality video one etc); each one of those real-time configured modes has quite different requirements and it will be served by a different set of compression/encryption/authentication modules. Moreover, we will implement two different, yet fully compatible, approaches: One will be based on standard off-the-shelf reconfigurable components (FPGAs), and another one on a reconfigurable processing unit (RASIP) implemented in silicon within SMART. The advantage of the FPGA-approach is that it will offer an extremely flexible and low-cost solution supported by very efficient tools employed by millions of engineers worldwide [6]. The RASIP approach will have lower power consumption but its programming tools will not certainly be as mature/efficient as the FPGA-based ones and they are not employed by the requested critical mass. In other words if someone needs an extremely low-power node it will adopt the RASIP-based one at the cost of possible small deficiencies in the development environment, while the FPGA-based ones will be a very efficient approach that anyone familiar with embedded systems will be able to seamlessly utilize.

Meanwhile, it should be stressed that the proposed system will have significant lower power requirements, while offering much higher performance when compared to legacy microprocessor based sensor nodes, as it will be based on research results of numerous groups worldwide (including those of the participating research centres) [6] - [8], showing that the reconfigurable devices (i.e. FPGAs, and Reconfigurable ASIPs) are much more efficient when implementing security, data-compression and video-compression tasks that standard microprocessors.

SMART is an initiative of the most important European industries in micro-systems, communications and sensor Networks, namely: (a) Thales with a comprehensive set of sensor equipment and secure access components covering a wide area of use from home to military applications, (b) Philips one of world's largest entertainment and communication solutions provider marketing and developing numerous components of the "smart environments", and (c) Hellenic Aerospace Industry a multi-billion company implementing aerospace and smart telecommunication equipments. The initiative is also driven by three pioneering and rapidly expanding SMEs active solely on the low-power, internetworking equipments market. Moreover, the world-wide research activities of Innovations of High Performance Microelectronics (IHP), Telecommunication Systems Institute (TSI), Universidad Politécnica de Madrid (UPM), and Technische Universität Braunschweig (TUBS) clearly show the research knowledge and background contained in the SMART consortium. To this end, both the research aspects as well as the proposed development activities of the project clearly turn out to address the real needs of the market and the stimulation of future perspectives, have clear industrial orientation and fair knowledge of the current state-of-the-art scene. Also their technological background and deep industrial products know-how ensures the proposed advancement of the state-of-the-art through the aforementioned innovations and validates its importance.

REFERENCES

[1] K. Sohraby, D. Minoli, T. Znati, "*Wireless Sensor Networks*", Wiley Publisher, 2007

[2] F-X Standaert, "Side-Channel Attacks – Introduction", *IEEE DATE*, April 15-20, 2007

[3] J. Majeed, "Less Power Security Techniques for Sensor Networks", International Conference on Mobile Computing and Ubiquitous Networking (*ICMU 2005*) April 13 - 15, 2005

[4] Todman, T., Constantinides, G., Wilton, S., Mencer, O., Luk, W., and Cheung, P. "Reconfigurable Computing Architectures and Design Methods". *IEE Proc.-Comput. Digit.Tech* 152, 2 (Mar.) 2005, 193–207.

[5] W.B. Heinzelman et al., "Middleware to Support Sensor Network Applications," *IEEE Network*, Vol. 18, No. 1, pp. 6–14, 2004.

[6] D. Meintanis, I. Papaefstathiou,"Hardware and Software Power Consumption Measurements for security applications on FPGAs", IEEE Field Programmable Technology Conference (ICFPT2008), Dec 8-10, Taipei, Taiwan

[7] I. Papaefstathiou, "Titan II : An IPComp Processor for 10Gbit/sec network*", IEEE Design & Test* (D&T), Nov. 2004.

[8] J.L Núñez, S. Jones, "Gbit/Second Lossless Data Compression Hardware", *IEEE Transactions in VLSI Systems* (TVLSI), Vo. 11, No. 3, pp. 499-510, June, 2003