Evolution of Wireless Sensor Networks towards the Internet of Things: a Survey

Luca Mainetti[1], Luigi Patrono[1], and Antonio Vilei[2]

[1]University of Salento, Dept. of Innovation Engineering
[2]STMicroelectronics
Lecce, ITALY

Abstract: **Wireless Sensor Networks (WSNs) are playing more and more a key role in several application scenarios such as healthcare, agriculture, environment monitoring, and smart metering. Furthermore, WSNs are characterized by high heterogeneity because there are many different proprietary and non-proprietary solutions. This wide range of technologies has delayed new deployments and integration with existing sensor networks. The current trend, however, is to move away from proprietary and closed standards, to embrace IP-based sensor networks using the emerging standard 6LoWPAN/IPv6. This allows native connectivity between WSN and Internet, enabling smart objects to participate to the Internet of Things (IoT). Building an all-IP infrastructure from scratch, however, would be difficult because many different sensors and actuators technologies (both wired and wireless) have already been deployed over the years. After a review of the state of the art, this paper sketches a framework able to harmonize legacy and new installations, allowing migrating to an all-IP environment at a later stage. The Building Automation use case has been chosen to discuss potential benefits of the proposed framework.**

1. INTRODUCTION

The Future Internet aims to integrate heterogeneous communication technologies, both wired and wireless, in order to contribute substantially to assert the concept of Internet of Things (IoT) [1]. Although there are many ways to describe an IoT, we can define it as a worldwide network of uniquely addressable interconnected objects, based on standard communication protocols.

The low cost of sensor technology has eased the proliferation of Wireless Sensor Networks (WSNs) in many applicative scenarios such as environmental monitoring, agriculture, healthcare, and smart buildings. WSNs are characterized by high heterogeneity because they are compliant with different proprietary and non-proprietary solutions. This wide range of solutions is currently delaying a large-scale deployment of these technologies in order to obtain a virtual wide sensor network able to integrate all existing sensor networks. Interoperability among heterogeneous sensing systems and abstraction between low layers (i.e. hardware) and high layers (i.e. user applications) are thus very important challenges [2].

Sensor networks based on closed or proprietary systems are connectivity islands with limited communication to the external world. There usually is the need to use gateways with application specific knowledge to export WSN data to other devices connected to the Internet. Moreover, there is no direct communication between different standards unless complex application-specific conversions are implemented in gateways or proxies (Fig. 1).

The current trend, however, is to use the Internet Protocol (IP) to achieve native connectivity between WSNs and the Internet [3]. In this way, smart objects (e.g., tiny sensors or actuators with a network interface) are interconnected in order to make an IoT, based mainly on open standards and where every device has its own IP address.

The IoT will allow collecting any useful information about the physical world's smart objects to use this information in various applications during the objects' life cycle. The Web enablement of smart objects, for example, will deliver more flexibility and customization possibilities for the Future Internet. For example, following the trend of Web mashups (like Yahoo Pipes) [4], end users can create applications mixing real-world devices such as home appliances with virtual services on the Web. This type of applications is often referred to as physical mashups [5].

This work offers a state of the art related to standards and solutions for WSNs, in order to make an IoT. Furthermore, this paper sketches a framework able to harmonize legacy and new installations, allowing migrating to an all-IP environment at a later stage. The Building Automation use case has been chosen to discuss potential benefits of the proposed framework.

The rest of the paper is organized as follows. Section 2 presents scenarios and challenges with regards to the IoT. In

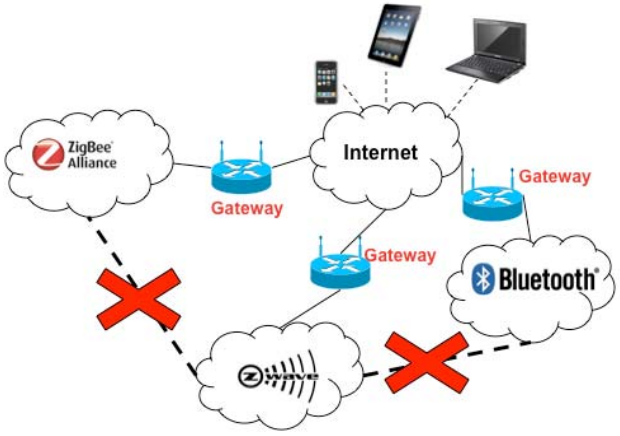

Figure 1. Interworking among heterogeneous WSNs.

Section 3, an overview of the existing technologies in the context of wireless sensor and actuator networks is reported. The paper continues with an analysis of the Building Automation scenario in section 4. This analysis allows identifying the requirements for the proposed framework. Section 5 describes a possible test environment, while section 6 presents the authors' conclusions.

2. SCENARIOS AND CHALLANGES

The Internet of Things is playing more and more a key role in several scenarios like:

- Healthcare and wellness,
- Home and building automation,
- Improved energy efficiency,
- Industrial automation,
- Smart metering and smart grid infrastructures,
- Environmental monitoring and forecasting,
- More flexible RFID infrastructures,
- Asset management and logistics,
- Vehicular automation and smart transport,
- Agriculture,
- Smart shopping.

This wide range of applications, with great differences in terms of requirements, scale and total available market, has led to a proliferation of technical solutions for the embedded networking field [6]. Smart objects have different communication, information and processing capabilities, and interoperability should be maintained to provide seamless interaction among them. Scalability is another issue for the IoT because of the large scope of communication needed to seamlessly interconnect objects and people [2]. Moreover, in a dynamic environment of ubiquitous networking, services exported by the objects must be automatically identified by means of a discovery mechanism. Confidentiality, authenticity and trustworthiness of communication are essential to guarantee personal privacy and security (for example when billing information depends on sensors' data).

Even though the amount of data transferred from/to a single sensor or actuator is very limited, the overall amount of data could be huge due to the large number of objects and their frequent interaction [7]. How to handle a big volume of data is one of the important challenges of the Future Internet. Fault-tolerance is another problem of the IoT: ubiquitous networking requires redundancy in several levels and ability to automatically adapt to changed conditions in order to guarantee robust communication [2].

Finally, when dealing with battery-operated smart objects, another critical aspect is their power consumption [7]. Therefore, energy efficient communication mechanisms are essential.

3. OVERVIEW OF EXISTING SOLUTIONS

This paragraph presents a quick overview of the main technologies used for WSNs [8]. We start by analyzing solutions whose protocol stacks are not based on the Internet Protocol. Then we discuss about IPv6/6LoWPAN and, finally, we deal with high-level technologies and middleware.

3.1 Non-IP Solutions

ZIGBEE

ZigBee is a wireless networking technology developed by the ZigBee Alliance for low-datarate and short-range applications [9]. The ZigBee protocol stack is composed of four main layers: the physical (PHY) layer, the medium access control (MAC) layer, the network (NWK) layer, and the application (APL) layer. PHY and MAC of ZigBee are defined by the IEEE 802.15.4 standard, while the rest of the stack is defined by the ZigBee specification.

The initial version of IEEE 802.15.4, on which ZigBee is based, operates in the 868 MHz (Europe), 915 MHz (North America) and 2.4 GHz (worldwide) bands. The data rates are 20 kb/s, 40 kb/s, and 250 kb/s, respectively.

The ZigBee network layer specifically supports addressing and routing for the tree and mesh topologies. The development of ZigBee applications relies on application profiles. The most important ZigBee application profiles are the ZigBee Home Automation Public Application Profile [9] and the ZigBee Smart Energy Profile [10]. The main application areas for the Home Automation profile are lighting, HVAC, and security. The Smart Energy profile deals with energy demand response and load management applications for power grids.

A new ZigBee specification is RF4CE [11], which has a simplified networking stack for star topologies only, offering a simple solution for consumer electronics remote control.

Z-WAVE

Z-Wave is a wireless protocol architecture developed by ZenSys and promoted by the Z-Wave Alliance for automation in residential and light commercial environments. The main purpose of Z-Wave is to allow reliable transmission of short messages from a control unit to one or more nodes in the network [12]. Z-Wave is organized according to an architecture composed of five main layers: PHY, MAC, transfer, routing, and application layers.

The Z-Wave radio mainly operates in the 900 MHz (868 MHz in Europe and 908 MHz in the United States) and 2.4 GHz. Z-Wave allows transmission at 9.6 kb/s, 40 kb/s and 200 kb/s data rates.

Z-Wave defines two types of devices: controllers and slaves. Controllers poll or send commands to the slaves, which reply to the controllers or execute the commands.

The Z-Wave routing layer performs routing based on a source routing approach.

INSTEON

INSTEON [13] is a solution developed for home automation by SmartLabs and promoted by the INSTEON Alliance. One of the distinctive features of INSTEON is the fact that it defines a mesh topology composed of RF and power line links. Devices can be RF-only or power-line only, or can support both types of communication.

INSTEON RF operates at the 904 MHz center frequency, with a raw data rate of 38.4 kb/s.

INSTEON devices are peers, which means that any of them can play the role of sender, receiver, or relayer. Communication between devices that are not within the same range is achieved by means of a multihop approach that relies on a time slot synchronization scheme.

WAVENIS

Wavenis is a wireless protocol stack developed by Coronis Systems for control and monitoring applications in several environments, including home and building automation. Wavenis is currently being promoted and managed by the Wavenis Open Standard Alliance (Wavenis-OSA). It defines the functionality of physical, link, and network layers [14]. Wavenis services can be accessed from upper layers through an application programming interface (API).

Wavenis operates mainly in the 433 MHz, 868 MHz, and 915 MHz bands, which are ISM bands in Asia, Europe, and the United States. Some products also operate in the 2.4 GHz band. The minimum and maximum data rates offered by Wavenis are 4.8 kb/s and 100 kb/s, respectively, with 19.2 kb/s being the typical value.

3.2 IP-based Solutions

Despite the initial skepticism of many researchers about the suitability of the Internet architecture for sensor networks, today the general trend is to move away from proprietary or closed standards solutions to embrace IP. In fact, the performance advances of recent 32-bit microcontrollers and the availability of highly optimized protocol stack implementations, makes it feasible to add IP connectivity to smart objects. This trend is also confirmed by the ZigBee Alliance and its choice of IP for the Smart Energy 2.0 Profile [15].

Given the potentially huge number of connected devices (Ericsson foresees more than 50 billion) [16], IPv4 cannot be used because of its limited address space. A much better choice, of course, is using IPv6 with its 128-bit addresses. Moreover, IPv6 allows network auto-configuration and stateless operation.

Thanks to IPv6, every smart object can be connected readily to other IP-based networks, without the need for intermediate entities like translation gateways or proxies. Given the limited packet size and other constraints of Low-Power Wireless Personal Area Networks, an adaptation layer to perform header compression, fragmentation and address auto-configuration is needed to use IPv6 [6]. The 6LoWPAN IETF Working group has already defined the format for adaptation between IPv6 and IEEE 802.15.4.

The ideal use of 6LoWPAN is with applications where embedded devices need to communicate with Internet-based services using open standards able to scale across large network infrastructures with mobility. In Fig. 2, the 6LoWPAN protocol stack is shown.

The 6LoWPAN architecture is made up of low-power wireless area networks (LoWPANs), which are connected to other IP networks through edge routers. The edge router plays an important role as it routes traffic in and out of the LoWPAN, while handling 6LoWPAN compression and NeighborDiscovery for the LoWPAN. If the LoWPAN is to be connected to an IPv4 network, the edge router will also handle IPv4 interconnectivity. Each LoWPAN node is identified by a unique IPv6 address, and is capable of sending and receiving IPv6 packets. Typically LoWPAN nodes support ICMPv6 traffic such as “ping”, and use the User Datagram Protocol (UDP) as a transport protocol. Adaptation between full IPv6 and the LoWPAN format is performed by routers at the edge of 6LoWPAN islands, referred to as edge routers. This transformation is transparent, efficient and stateless in both directions. Furthermore, 6LoWPAN does not require an infrastructure to operate, but may also operate as an ad hoc LoWPAN.

At the time of this writing, the IETF Routing Over Low Power and Lossy Networks (ROLL) Working Group is defining the IPv6 Routing Protocol for Low power and lossy networks (RPL).

3.3 High level and middleware solutions

One of the main benefits related to use of internetworking based on IP protocol is, undoubtedly, to enable the use of Web services. Recently, another working group of the IETF has proposed a new web service into networks of smart objects. This protocol is called Constrained Application Protocol (CoAP) [17], is developed to run in special environments, typically of an IoT, that have strict constraints in terms of limited energy resources, high packet loss rates, limited hardware capabilities and so on. CoAP is a protocol optimized for resource constrained networks typical of IoT and Machine-to-Machine (M2M) applications. CoAP consists of a subset of the HyperText Transport Protocol (HTTP) functionalities, which have been re-designed taking into account the low processing power and energy consumption constraints of small embedded devices such as sensors and actuators. CoAP is organized in two sub-layers (i.e. Request/response, and Transaction), and it is built on top of the User Datagram Protocol (UDP). CoAP uses a short fixed-length compact binary header of 4 bytes followed by compact binary options. CoAP supports several payload-encoding standards such as the Extensible Markup Language (XML).

A complete protocol stack used by CoAP is shown in Fig. 2. Although CoAP is work in progress, several open source implementations are already available, including two well-known operating systems for WSNs, Contiki [18] and Tiny OS [19].

CoAP usage is optimal when using an all-IP infrastructure. When coexistence of IP-based solutions with legacy technology is needed, a viable alternative could be using a high level middleware able to improve flexibility and interoperability, and to support every kind of application. Ideally, such a middleware should be able to maintain an Internet overlay architecture in which network protocols are all inherited from the Internet backbone.

Global Sensor Network (GSN) [20, 21] is an open source framework that meets the previous requirements, developed in Java programming language. One key concept for GSN is represented by the virtual sensor abstraction. A virtual sensor corresponds either to a data stream received directly from sensors or to a data stream derived from other virtual sensors. In the latter case, using a peer-to-peer overlay network can improve the communication performance. A virtual sensor is composed by:

- A wrapper: a class containing the functional logic for reading data from a kind of data source.
- Processing class(es): one or more classes containing the post-processing functional logic. This represents the post-processing code that will be executed after a wrapper read data from data source.
- A descriptor file: a XML file for configuring the virtual sensor. In this file, generally, there are information about description of virtual sensor, geographical localization data like latitude/longitude and other kinds of information for describing a particular virtual sensor.

GSN uses SQL-based queries to create streams of data from the sensor network sources to the data users using the Internet as a network backbone. The architecture is necessarily distributed. Additionally, there is a sensor discovery protocol consisting of query, subscription, and registration processes. Data aggregation is available as a technique to reduce network traffic load by combining information at intermediate nodes for later transmission. GSN is able to aggregate query responses, discover new sensor nodes, and register available sensor nodes. GSN adopts a service-oriented architecture and does not exclude the possibility to use other standards for the IoT such as 6LoWPAN, previously described.

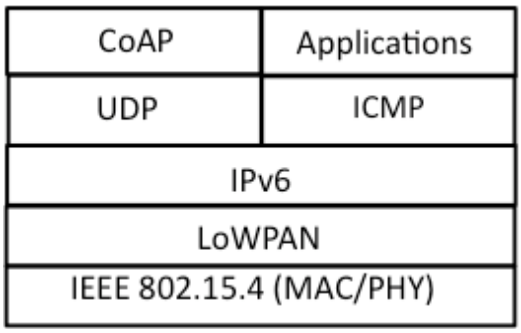

Figure 2. 6LoWPAN protocol stack.

4. A CASE STUDY FOR BUILDING AUTOMATION

To illustrate the potential benefits of the above-described technologies, a specific reference scenario has been chosen. In particular, this work deals with the Building Automation (BA) scenario, where the IoT can substantially improve the efficiency of the traditional energy management systems. It has been demonstrated that more than 40% of the energy consumption in Europe is building-related (residential, public, commercial and industrial) [22]. Advanced, flexible and integrated ICT-based energy management systems for both new and old buildings, in combination with widespread control of natural lighting and ventilation as well as better insulation (of windows, floors and ceilings), will help not only to reduce energy consumption but also to increase safety and security, to promote welfare, and to facilitate assisted living.

A university campus has been chosen as the use case to show the potential benefits of the integration of heterogeneous sensors and actuators networks. The design of a smart building able to save energy maintaining comfort and operative levels in a university campus is a very interesting challenge. BA aims at orchestrating many heterogeneous devices for heating, lighting, shading, and door/window control, to provide users with real comfort but also security, and the ability to monitor multiple environments. All these devices can be seen such as sensors and smart actuators of a wide WSN.

University buildings are composed of heterogeneous environments, in terms of energy requirements, such as classrooms, laboratories, professors' offices, administrative offices, and common parts. A smart building should be able to minimize every kind of energy waste. Currently there is a wide variety of low-cost sensors and actuators, produced by different vendors, able to measure temperature, humidity, air quality, brightness, and luminosity. Unfortunately, these sensors and smart metering systems are often unable to interoperate. It is fundamental to define an overall control strategy able to link all the energy consumption components (e.g. heating, air conditioning, lighting, energy production and storage, etc.) among them and to guarantee a complete control centre at building level. To implement this strategy, it is very important to guarantee interoperability, scalability, and sufficient semantics in order to achieve data independence between producer and consumer.

A possible strategy to meet the requirements listed above could be adopting an all-IP solution based on 6LoWPAN/IPv6 at the network layer, and on CoAP to

implement web access to the sensors and actuators. As stated before, however, the heterogeneity of technologies (both wired and wireless) deployed over the years makes it difficult to deploy an all-IP solution from scratch. Taking this into account, we propose a framework that tries to harmonize legacy and new installations, allowing migrating toward an all-IP environment at a later stage. In particular, we suggest the adoption of GSN as the unifying middleware for 6LoWPAN/IPv6 networks and legacy WSNs. The proposed architecture is depicted in Fig. 3.

In this framework, the 6LoWPAN edge router device has a dual functionality: it connects the LoWPAN to the Internet and acts as a virtual sensor for the GSN middleware. With regards to non-IP technology (e.g. ZigBee, Z-Wave, etc.), instead, every WSN gateway will need to implement a specific GSN virtual sensor. The dependency between sensors data and user applications (e.g., energy management system, people tracking system, environment monitoring system, etc.) is a major problem. The adoption of a GSN-based framework makes things simpler as it allows data independence. Thanks to GSN, the user applications can abstract from details related to heterogeneous physical infrastructures such as wired or wireless sensors, RFID readers, smart meters, cameras, server, etc. GSN provides a logical overlay on sensor networks that exploits the virtual sensor concept. Some modules of the GSN architecture are able to carry out fundamental tasks such as storage and querying of historical data in repositories. Unfortunately, the current version of the GSN framework has some drawbacks: for instance, it is necessary to implement new wrappers every time the user applications' requirements change. In order to mitigate these problems, a semantic query mechanism is required. Semantic Web Services are innovative and flexible mechanisms for data retrieving and dynamic discovery services. Another weakness of the current GSN is its centralized architecture where point-to-point communications only are allowed. An improvement to GSN could be developing an efficient discovery service adopting a peer-to-peer (P2P) approach, able to improve the management of the virtual sensors overlay network, exploiting for instance a Distributed Hash Table (DHT).

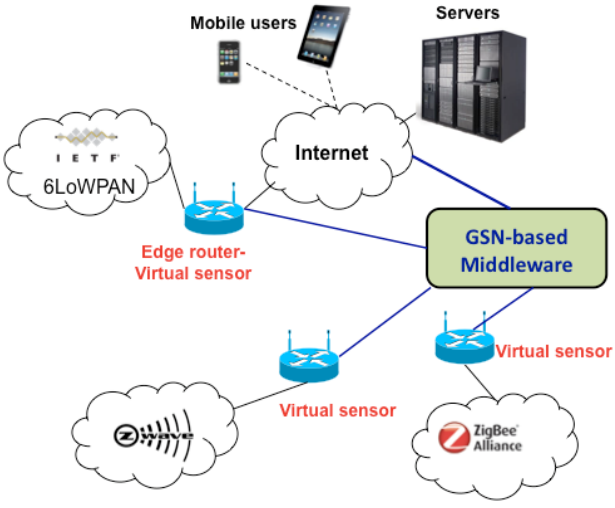

Figure 3. Proposed framework to integrate heterogeneous WSNs through Internet.

5. SETTING OF A TEST ENVIRONMENT

At the time of this writing, we are setting up a test environment to experiment with the combined use of 6LoWPAN/IPv6 (at the network layer) and GSN (as an higher level application middleware) in the context of a Building Automation scenario, as described before. The wireless node for this test-bed is based on STMicroelectronics' MB851 application board shown in Fig. 4. The latter features the STM32W108 [23] System-on_Chip (SoC), integrating a 32-bit ARM® Cortex™-M3 microprocessor @ 24 MHz, 128 Kbyte flash, 8Kbyte RAM and a 2.4 GHz 802.15.4-compliant transceiver. In this test environment, the application boards run Contiki, an open source operating system for memory-efficient networked embedded systems and wireless sensor networks. Contiki is designed for microcontrollers with small amounts of memory. A typical Contiki configuration is 2 kilobytes of RAM and 40 kilobytes of ROM. It provides IP communication, both for IPv4 and IPv6, thanks to the embedded uIPv6 subsystem. The latter is an implementation of an IPv6/6LoWPAN stack, able to transmit IPv6 packets using the IEEE 802.15.4 radio of STM32W108 chip.

The Gateway device for this test-bed is based on STMicroelectronics' SPEAr1310 [24], a state-of-the-art multi-core multi-purpose embedded system platform running Linux. The Gateway will implement the 6LoWPAN "Edge Router" functionality, thus allowing the WSN to connect to the Internet. The Gateway will also perform the management

Figure 4. Wireless node (MB851 application board) based on STMicroelectronics' STM32W108 SoC.

of the WSN in terms of remote nodes configuration, bootstrapping, node monitoring and links status, and real time evaluation using GSN. At the time of this writing, the implementation of this test environment has just started, so there are not enough details to share, yet.

6. CONCLUSION

The high heterogeneity of existing WSN technologies, characterized by the presence of many different proprietary and non-proprietary solutions deployed over the years, is a big challenge that the research community has to face to achieve a pervasive integration of sensors with the Future Internet. The current trend is to move away from proprietary and closed standards, to embrace IP-based sensor networks using the emerging standard 6LoWPAN/IPv6. In this work, standards and solutions able to guarantee the integration among several heterogeneous WSNs have been discussed. Furthermore, the authors sketched a framework able to harmonize new installations and legacy ones (non-IP based), preserving the possibility to migrate to an all-IP environment at later stage. The proposed framework is currently being tested in the Building Automation scenario. More information about the proposed framework will be disclosed at a later stage, after extensive field trials.

REFERENCES

[1] G. Kortuem, et al.: "Smart objects as building blocks for the Internet of things", IEEE Internet Computing, vol. 14, no.1, 2009.

[2] M. Zorzi, A. Gluhak, S. lange, A. Bassi: "From today's INTRAnet of things to a future INTERnet of things: a wireless- and mobility-related view", IEEE Wireless Communications, vol.17, no. 6, 2010.

[3] J. Vasseur and A. Dunkels: "Interconnecting Smart Objects with IP - The Next Internet", Morgan Kaufmann, 2010.

[4] N. Zang, M. B. Rosson, and V. Nasser: "Mashups: who? what? why?", Proceedings of CHI, Florence, Italy, April 2008.

[5] M. Kovatsch, M. Weiss, D. Guinard: "Embedding Internet Technology for Home Automation", Proceedings of ETFA, Bilbao, Spain, September 2010.

[6] Z. Shelby and C. Bormann: "6LoWPAN: The Wireless Embedded Internet", Wiley Publishing, November 2009.

[7] G. M Lee, N. Crespi: "The Internet of Things - Challenge for a New Architecture from Problems", IETF Internet Architecture Board, Interconnecting Smart Objects with the Internet Workshop, Prague, Czech Republic, March 2011.

[8] C. Gomez, J. Paradells: "Wireless home automation networks: a survey of architectures and technologies", IEEE Communications Magazine, Volume 48 Issue 6, June 2010.

[9] ZigBee Alliance: "ZigBee Home Automation Public Application Profile", revision 25, v. 1.0, Oct. 2007.

[10] ZigBee Alliance: "ZigBee Smart Energy Profile Specification", revision 15, Dec. 2008.

[11] ZigBee Alliance: "ZigBee RF4CE Specification", Version 1.00, March 2009.

[12] Z-Wave: "Z-Wave Protocol Overview", v. 4, May 2007.

[13] P. Darbee: "INSTEON: The Details", Aug. 2005.

[14] A. Garcia-Hernando et al.: "Problem Solving for Wireless Sensor Networks", Springer, July 2008.

[15] ZigBee Alliance: "ZigBee Smart Energy 2.0 DRAFT 0.7 Public Application Profile", June 2010

[16] Ericsson: "More than 50 Billion Connected Devices", White Paper, February 2011, available at http://www.ericsson.com/res/docs/whitepapers/wp-50-billions.pdf

[17] Z. Shelby, K. Hartke, C. Bormann and B. Frank: "Constrained Application Protocol (CoAP)", draft-ietf-core-coap-06, May 2011.

[18] A. Dunkels, B. Gronvall, T. Voigt, "Contiki - A Lightweight and Flexible Operating System for Tiny Networked Sensors", Proc. of the 29th Annual IEEE International Conference on Local Computer Networks, p.455-462, November 2004.

[19] J. Hill, et. al.: "System architecture directions for networked sensors", In Proc. ASPLOS-IX, November 2000.

[20] K. Aberer, M. Hauswirth, A. Salehi: "Global Sensor Networks", Technical report LSIR-REPORT-2006-001, Lausanne, Switzerlan, 2006.

[21] K. Aberer, M. Hauswirth, A. Salehi: "A middleware for fast and flexible sensor network Deployment", Proc. of International Conference on Very Large Data Bases (VLDB 2006), Seoul, Korea, September, 2006.

[22] European Parliament: "Directive 2002/91/EC", Council on the Energy Performance of Buildings, December 2002.

[23] STMicroelectronics: "High-performance, IEEE 802.15.4 wireless system-on-chip with 128-Kbyte Flash memory", Data Sheet, April 2011, available at http://www.st.com/internet/com/TECHNICAL_RESOURCES/TECHNICAL_LITERATURE/DATASHEET/CD00248316.pdf

[24] STMicroelectronics: "Dual-core Cortex A9 embedded MPU for communications", September 2010, available at http://www.st.com/internet/com/TECHNICAL_RESOURCES/TECHNICAL_LITERATURE/DATA_BRIEF/CD00274166.pdf