Wireless Sensor Networks for the Protection of an Electrical Energy Distribution Infrastructure

António Grilo, Augusto Casaca, Mário Nunes, Carlos Fortunato

Wireless Sensor Networks for the Protection of an Electrical Energy Distribution Infrastructure

António Grilo[1], Augusto Casaca[1], Mário Nunes[1] and Carlos Fortunato[2]

[1] INESC-ID/IST, R. Alves Redol, 9, 1000-029 Lisboa, Portugal
[2] EDP Distribuição, R. Camilo Castelo Branco, 43, 1050-044 Lisboa, Portugal
antonio.grilo@inesc-id.pt, augusto.casaca@inesc-id.pt,
mario.nunes@inesc-id.pt, carlos.fortunato@edp.pt

Abstract. From a safety and security point of view, the electrical energy distribution infrastructure needs to be protected.. In this paper solutions to increase the safety aspects of substation components, power lines and power transformers are discussed. Also security solutions related to perimeter intrusion detection in substations and remote surveillance of power transformer installations are introduced. All the solutions are based on the deployment of wireless sensor and actuator networks in the substation, power lines and power transformers, which perform remote monitoring and provide alarms when required. The sensor network interacts with the SCADA system of the electricity provider to allow for centralised control of the protection system.

Keywords: Wireless Sensor Networks, Critical Infrastructure Protection, Electrical Energy Distribution Infrastructure.

1 Introduction

The electrical energy distribution infrastructure is a critical infrastructure that requires protection for safety and security reasons. The energy distribution infrastructure mainly consists of a set of substations, Medium Voltage (MV)/ Low Voltage (LV) power transformers outside the substation, MV power lines connecting substations to MV/LV power transformers and LV power lines from the MV/LV power transformers to the customers. Some industrial customers may also get direct MV power lines. Associated to this infrastructure we should also consider the SCADA system, which is a supervisory control and data acquisition system for the infrastructure. This infrastructure is illustrated in Figure 1.

For safety reasons remote surveillance of the electrical energy distribution network is already established to some extent based on wired sensors. The use of wireless sensor and actuator networks (WSAN) can lead to a more powerful and efficient protection scenario for the substations, power lines and power transformers. Their higher deployment

flexibility allows wireless sensors to capture more status parameters than the existing fixed sensor infrastructure. Specific actuators can also be included in the infrastructure as part of the WSAN. The wireless nature of communication can also contribute to the avoidance of critical points of failure.

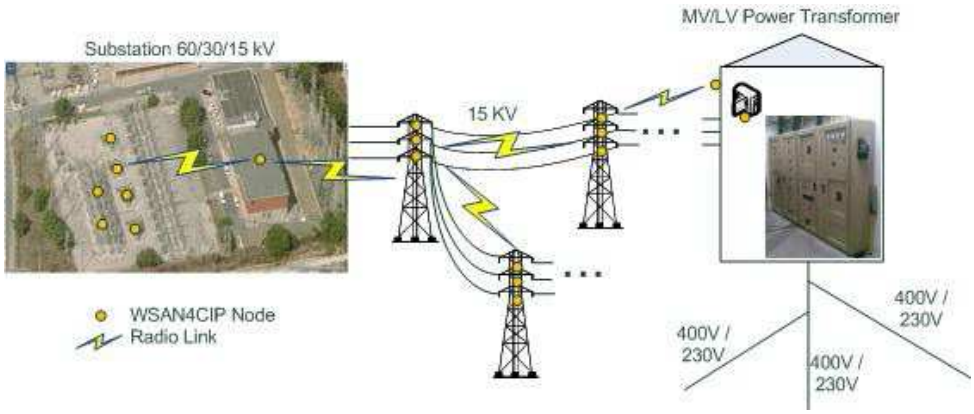

Fig. 1. MV/LV electricity distribution infrastructure.

The Wireless Sensor and Actuator Networks for the Protection of Critical Infrastructures (WSAN4CIP) project, which is a European collaborative project running in the 7th Framework Program, has the high level objective of enhancing the reliability of critical infrastructures by providing surveillance data for the management of the infrastructure and to increase the dependability of the critical infrastructure security by providing self-healing and dependability modules for the WSAN. The feasibility of the approach developed in the project is demonstrated using electrical energy distribution and water distribution as representatives of critical infrastructures. In this paper we will focus exclusively on the energy distribution case and primarily at the application level.

From the safety and security analysis made in the project we have concluded that based on the WSAN we can provide a set of solutions capable of improving the protection of this infrastructure. From the safety point of view, some remote monitoring processes have been identified to be deployed, and from the security point of view, the use of cameras associated with WSAN can significantly improve the robustness of the solutions for the physical protection of substations and MV/LV power transformer installations.

In the safety area we have defined solutions for the remote active monitoring of: i) substation circuit breaker trip coil status; ii) substation power transformer oil temperature; iii) substation neutral reactance oil temperature; iv) substation neutral resistor coil box temperature; v) MV power line activity in all the three phases; vi) MV/LV power transformer hotspot detection. All the monitored parameters will be visualized at the SCADA system through a special-purpose interface and a graphical user interface. In the security area we will focus on substation perimeter unauthorized intrusion detection by

using a combination of PTZ cameras, motion detectors and WSAN. Additionally, video cameras are also deployed and integrated with the WSAN in order to improve the physical protection of the MV/LV power transformer installations.

The requirement for video transmission and the long-distances between power line towers place additional requirements in terms of the communications and processing capabilities of the WSAN nodes. We have defined a sensor mote architecture which can be used in all these applications and that can run a standard operating system like Linux. Communication interfaces capable of connecting to powerful communication networks like Wi-Fi are also part of this architecture.

The energy consumption of this WSAN node cannot be overlooked. Although the power distribution network carries energy by definition, its use as a WSAN power source presents many challenges. This is especially true in the MV power lines outside the substations, where the voltages are too high (e.g. 15 kV) to be used directly by the WSAN nodes, prompting the use of intelligent energy harvesting techniques.

The paper, in sections 2, 3 and 4, will make a detailed analysis of the application cases indicated for the protection of the electrical energy distribution network. In section 5 we will analyse the interaction with the SCADA system. The hardware and software architectures of the envisaged sensor mote solution will be discussed in section 6 and, finally, some conclusions will be drawn in section 7.

2 Application Scenarios in the Substation

For the protection scenarios implemented in the substation, four of them have the aim of increasing the safety of the infrastructure components, and a fifth has that of increasing security through the deployment of perimeter intrusion detection. The substation safety improvement demonstration scenarios monitor the status of essential components of the substation and the results can be generalized for other components. The target substation is located at S. Sebastião, Setúbal, Portugal, and belongs to the energy distribution infrastructure operated by EDP Distribuição, a company whose primary mission is the distribution of energy in Portugal. The S. Sebastião substation is an important element in the context of the wider regional grid it belongs to. The substation safety and security protection scenarios are described next.

2.1 Circuit Breaker Trip Coil Condition Active Status Monitoring

In this scenario we consider a sensor and actuator for periodically evaluating the operating status of the circuit breaker trip coil element. The trip coil is a fundamental component of the circuit breaker that sometimes breaks down even when under normal use. The trip coil activates the circuit breaker when a 110V DC voltage is applied at its terminals, cutting the energy supply to the power line. It happens that after activating the circuit breaker

there is a chance that the coil may be damaged and the circuit breaker will not function properly in the next event.

This scenario aims to check the working status of this component in a pro-active way. A 5V DC voltage will be applied every 60 minutes by an actuator. The magnetic field generated by the coil will be measured by a Hall-effect transistor. In the event of failure, meaning that no magnetic field is detected when a 5V DC voltage is applied, the sensor will report the failure back to the network. The sensor will also test the coil after a trip. In an activation event, the circuit breaker coil is under an 110 V DC voltage for 50 to 150 ms, the Hall-effect sensor sampling rate shall be at least half of the shorter time, i.e. at least 25 ms. Thus, when the activation of the breaker happens, the sensor detects it and can program an extra test shortly after the activation, checking if the circuit break remains functional for the next time it is called into duty.

The sensor would also allow for on demand requests to immediately probe the coil and report back its status. The sensing and controlling of the trip coil test is done locally. The information sent back to the sink consists only of the test results. In total there are 24 circuit breakers in this substation.

2.2 HV/MV Power Transformer Oil Temperature Active Monitoring

In this scenario we use a wireless temperature sensor for monitoring the oil temperature of the HV/MV power transformers in the substation (see Figure 2). The substation has four power transformers: two 60 KV/15 KV and two 60 KV/30 KV. Due to the value and importance of these elements to the EDP distribution network the scenario will monitor the temperature of all of them. A failure on one of the power transformers affects a series of power lines and all the downstream MV/LV power transformers, meaning thousands of homes and businesses are affected.

The temperature sensor probe is placed in the external side of the metallic oil tank, firmly and thermally attached to the tanks external wall. The sensor probe is isolated from the external environment with thermal foam. The sensor is driven by a 110VDC power source from the substation DC grid. Calibration of the sensor is needed and can be done by locally reading the analogue temperature gauge and the value read by the sensor.

On normal status a measure will be taken every minute, but uploaded to the network only every 15 minutes. When reaching a temperature 20% below the alarm threshold of 95ºC or when a 1ºC or higher increase happens over consecutive readings, the sensor will upload all temperature readings to the network and increase the sampling rate to one reading every one second. The temperature sensor will also allow for on demand temperature reading.

2.3 Neutral Reactance Oil Temperature Active Monitoring

In the third scenario we have a temperature sensor for monitoring the oil temperature of the neutral reactance element (see Figure 2). S. Sebastião substation has two neutral reactances for phase-earth failures limitation and detection on the 15KV power transformers. On a typical failure event this element is under great stress, dissipating 2.6 MW of power for as long as 4 seconds. If the defect persists the reactance may be under this heavy load several more times in a short period, causing it to overheat and raising the risk of failure spreading to other elements in the failing circuit.

Due to the importance of this element in the detection and prevention of failures on the network, and the protection it grants to other equipment (like the power transformer), this scenario will monitor the temperature of all the neutral reactances.

Each reactance tank is similar to a power transformer tank and the methodology used to monitor its temperature is identical to the previous scenario.

2.4 Neutral Resistor Coil Box Temperature Active Monitoring

In scenario four we consider a temperature sensor for monitoring the neutral resistor coils (see Figure 2). The substation has two neutral resistors for phase-earth failures limitation and detection on the 30 KV power transformers. The neutral resistor limits the current in a phase-earth failure to 300 A. On a typical failure event this element is under great stress, dissipating 5.2 MW of power for as long as 4 seconds. If the defect persists the resistor may be under this heavy load several more times in a short period, causing it to overheat and raising the risk of failure.

Due to the importance of this element in the detection and prevention of failures on the network and the protection it grants to other equipment, this scenario will monitor the temperature of all the neutral resistors.

Each neutral resistor box has 4-5 coils inside. An internal temperature probe shall be placed inside the neutral resistor box near the top where the temperature rises quicker. An external temperature probe is needed for comparison and shall be placed on the outside of the box, in the north facing side and out of direct sun light.

The normal operating temperature should be the outside environment temperature, because at normal operation the voltage is 0V, hence no current is flowing through the neutral resistor and no power (heat) is being dissipated.

On normal status a measurement will be taken every thirty seconds, but uploaded to the network only every 15 minutes. When reaching a temperature 20% above the external temperature or when a 1ºC or more increase happens over consecutive readings the sensor will upload all temperature readings to the network and increase the sampling rate to one reading every second.

Fig. 2. Protected substation components: HV/MV Power Transformer (left), Neutral Reactance (centre) and Neutral Resistor (right).

2.5 Perimeter Unauthorized Intrusion Detection

This scenario is quite different from the previous ones. It aims to maintain the substation premises security against trespassers by detecting their presence and providing a video feed that can be served to a mobile or fixed terminal of security personnel. Movement detectors will be used to infer the area where the intrusion is taking place. Sensors placed at diagonally opposed corners of the substation square, monitoring two orthogonal sides of the fence can detect an intrusion from any direction and measure the distance to the intruder. The sensor can then quickly send an alarm to the network and sharply point its camera to the hot area.

While no intrusion is detected, the movement detectors send keep-alive messages every five seconds. Once an intruder is detected by a movement sensor, an alarm message is sent and one or more cameras are activated and start to transmit the video stream to the control center. The cameras can also be controlled remotely from the control centre. A diagram for this scenario is illustrated in Figure 3.

Fig. 3. Substation perimeter surveillance.

3 Application Scenario in the MV Power Line

This scenario aims to monitor the status of an MV power line section, stretching from S. Sebastião substation to several MV/LV power transformers in the vicinity of the substation (less than 5Km). It is therefore possible to know centrally the location of a power line failure.

The power line chosen is a medium voltage 15KV line that feeds a set of urban and suburban MV/LV Power Stations in the city of Setubal. The line topology is a tree shape with several branch leaves, the leaves being the MV/LV power transformers (see Figure 1).

The physical measurement to be taken is the electrical current flowing through the line; a current transformer shall be used to measure its value and to derive a parasitic power source for the wireless sensor, eliminating the need for batteries on the sensor and at the same time posing no power constrains on the wireless protocols.

Each tower carries three 15 KV power lines (3 phases) in parallel, and each one needs its own sensor. Therefore, three current sensors will be placed in the lines in each tower. We also need three router nodes for bridging buried segments along the line. These router nodes shall be installed in the outside of MV/LV power transformers located between towers. The router shall be placed in high ground or at the end of a pole if more elevation is needed, to achieve line-of-sight to the next node site. The maximum distance between towers is 723 meters. The current sensor samples the current on the line every second.

4 Application Scenario in the MV/LV Power Transformer

In this scenario we use the wireless communications link built in the previous scenario to upload a video/image feed of the MV/LV power transformer house interior to the network. At the same time an infrared thermo sensor attached to the camera will sweep the power transformer critical elements, such as the main switch board, for hotspots. The detection of a hotspot will trigger an alarm on the network.

This scenario also includes an actuator. The remote user shall be able to turn on the lights on the MV/LV power transformer house. Thus, the camera shall be night and day capable. The user can get a better color video stream, even at night, improving on the black-and-white stream available in night mode. This feature improves the remote MV/LV power transformer physical security.

While no intrusion or hotspot is detected by the infrared sensor, the latter sends a keep-alive message every five seconds. Once an event is detected by the infrared sensor, the latter starts sending alarms every second and the camera is activated, transmitting the video stream to the control center. The lights can also be controlled remotely from the control center.

5 Interaction with the SCADA System

The substation devices are nowadays monitored and controlled through the Supervisory Control and Data Acquisition (SCADA) system. The WSAN shall be integrated with this existing system in order to provide a unified power distribution infrastructure interface to the human operators, which also optimizes the hardware/software resources and learning effort.

The SCADA protocol architecture is generic enough to be operated in an Internet Protocol (IP) environment on top of different network technologies, such as Ethernet and SONET/SDH. However, the WSAN presents a specific networking environment where the energy and bandwidth optimization requirements are often incompatible with the request/response philosophy behind SCADA. For example, in some applications that involve the timely detection of critical events, it is more efficient to rely on the remote sensing device to take the initiative to send an alarm message when the event happens, rather than allowing the supervisory system to issue periodical queries with a very high frequency. These differences lead to the need of translating SCADA procedures to WSAN procedures and vice versa, which is the purpose of the SCADA/WSAN gateway. The gateway consists of a PC equipped with an Ethernet interface and WSAN radio interface; the Ethernet is connected to the SCADA supervisory system and the radio interface to the WSAN.

From the point of view of the SCADA system, the SCADA/WSAN gateway behaves as a database that responds to its queries about the status of WSAN devices. The application interface for these queries is based on Web Services [1], with the gateway

implementing the server side. The use of the Web Service interface performs an adequate mapping of the SCADA data access mechanisms, which follows a client/server paradigm.

From the point of view of the WSAN, the SCADA/WSAN gateway takes the role of the sink node, which makes it the main destination of sensor data and the main source of queries and configuration/command requests. It also includes a database of sensing and management data, which serves as a buffer between the SCADA system and the WSAN.

6 Hardware and Software Architecture

The overall hardware architecture is depicted in Figure 4 and comprises three main components: SCADA supervisory station, SCADA/WSAN gateway and WSAN nodes. The latter has the capability to self-organize into a multi-hop network.

The SCADA station is PC based and will reside inside the Substation's main building. The SCADA/WSAN gateway fulfills also the role of a WSAN sink node, and hence must be equipped with a WSAN radio module able to communicate with the WSAN sensor and actuator nodes. The SCADA/WSAN gateway resides also at the Substation's main building, and hence will have access to 220 V AC line power. The most important critical requirements are related with the WSAN nodes, whose architecture is discussed next.

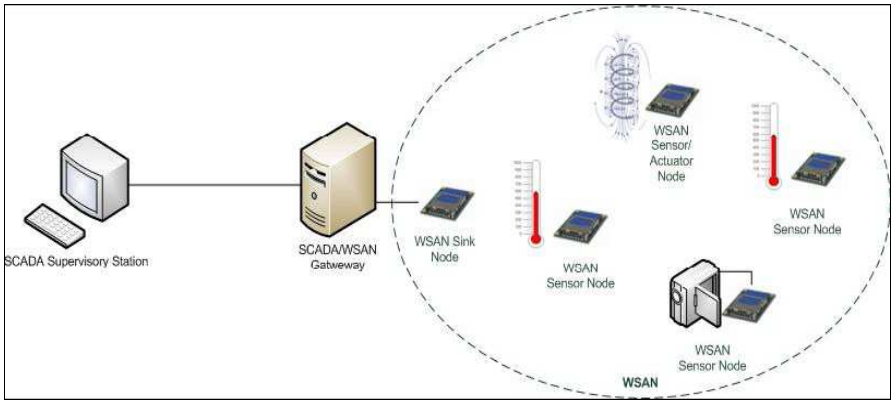

Fig. 4. High-level hardware architecture of the WSAN based system.

The video surveillance service is incompatible with a low rate technology like IEEE 802.15.4 [2]. It demands the use of a broadband wireless technology such as IEEE 802.11 [3]. The latter also makes sense given the expected maximum distance between sensors. The ensemble of requirements led to the choice of the Silex SX-560 Intelligent Programmable WLAN Module [4] as the platform for the WSAN node.

The basic architecture of the WSAN node is depicted in Figure 5. The SX-560 core is common to all WSAN nodes. The PCB designed at INOV includes a common voltage converter able to generate 3.3 V DC to feed the Silex and 5 V DC to feed the USB interface (considered a part of the Sensor Interface Unit) based on an input of 6-20 V DC. The differences between the WSAN nodes concern the Energy Unit and Sensor Interface Unit, which depend on the deployment spot and attached sensor, respectively.

Three different energy units exist, which allow operation at the three different locations within the EDP Distribuição network:

- **Substation WSAN node:** the energy unit will use the 220 V AC power line, performing the conversion to a voltage in the range 6-20 V DC.
- **MV/LV power transformer WSAN node:** the energy unit will use the 220 V AC power line, performing the conversion to a voltage in the range 6-20 V DC.
- **15 KV power line towers WSAN node:** the energy unit is able to harvest energy from the 15 KV power line current, being able to generate a voltage in the range 6-20 V DC and a current up to 500 mA.

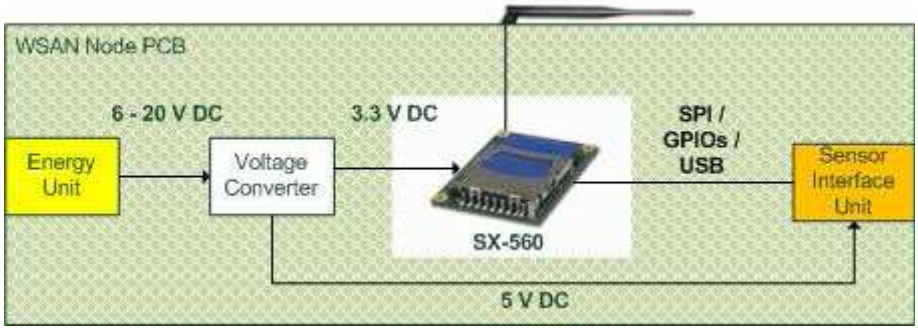

Fig. 5. Base architecture of WSAN node.

The software architecture of the WSAN node is depicted in Figure 6. The selected Operating System is LINUX, which is supported by the Silex SX-560 module. Among the advantages presented by LINUX is the intrinsic support of the dynamic code update (DCU) function, avoiding the development of specific DCU software. It should be noted that the DCU functionality is very important in the case of the power line and MV/LV power station monitoring scenario, where sensor nodes can be located far away from the substation, preventing the update of the WSAN node software without significant costs.

The main software modules of the WSAN node are the following:

- **WSAN Sensor/Actuator Application Logic:** This software block implements the application logic of the WSAN node, which consists of three main functions:
  - To receive and process commands from the SCADA/WSAN gateway.

• To retrieve sensor data from sensors and deliver it to the SCADA/WSAN gateway.

• To manage the configuration MIB based on the commands received from the SCADA/WSAN gateway and the status of the WSAN node.

- **Dependable Protocol Stack:** The limited capabilities of the WSAN nodes demand an optimized protocol stack able to find the best compromise between energy-efficiency, communications reliability and communications performance. The Dependable Protocol Stack spans the MAC, Routing and Transport protocols. The transport layer consists of a secured version of the Distributed Transport for Sensor Networks (DTSN) protocol developed by INOV [5]. The protocol provides message delivery guarantees to applications, optimizing retransmissions based on intermediate node caching. DTSN runs on top of a secure routing protocol. The latter will consist of a secured version of DSDV [6][7], optimized for WSAN applications (e.g. advertisement broadcasts limited to the sink node, and multipath forwarding for load and energy balancing and improved security). IEEE 802.11 is used for PHY and MAC layers.
- **Sensor/Actuator Device Driver:** Each different kind of sensor/actuator must be accessed in a different way and generates data and/or status of a specific type. This software block offers an abstract interface to the sensor/actuator hardware, allowing the design of the WSAN Application Logic to be as independent as possible from the intricacies of the sensor/actuator hardware.
- **Management Information Base (MIB):** This software block keeps the configuration parameters of the WSAN nodes, which can be changed by the SCADA/WSAN gateway.
- **Security Functions:** The WSAN constitutes a vulnerable part of the CIP System from the security point of view. Confidentiality, Authentication, Integrity and Non-repudiation solutions exist, which are part of the deployed WSAN.

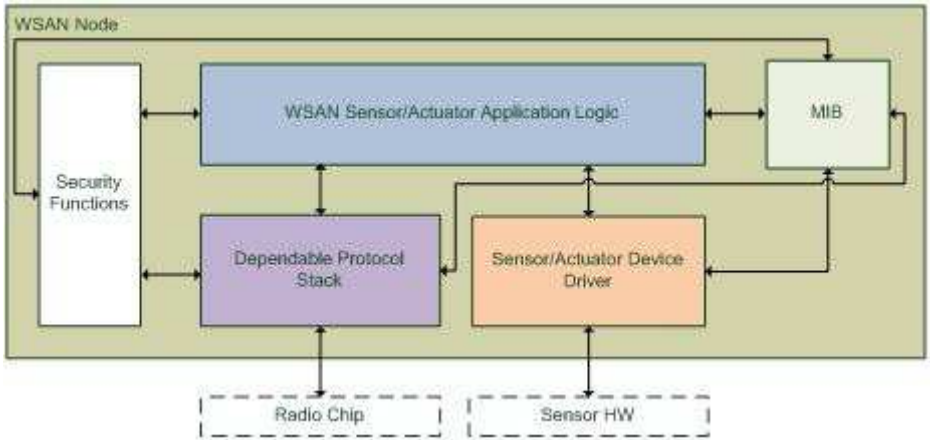

Fig. 6. Software architecture of the WSAN node.

7 Conclusion

The electrical energy distribution constitutes a critical infrastructure in contemporary industrially developed societies, which requires protection regarding safety and security threats. The fact that this infrastructure is geographically spread across huge areas puts difficult technological challenges to real-time prevention, detection and precise localization of anomalies. This paper presented a WSAN-based solution to protect the core elements of an electrical energy distribution infrastructure at three interconnected locations: substation, MV power-lines and MV/LV power transformer. The presented WSAN system is under development as part of the FP7 WSAN4CIP project.

This paper has discussed the planned architecture and high-level implementation solutions for the WSAN system, including a description of the protected equipments, the hardware and software architecture. A pilot system will be demonstrated in a subset of the Portuguese energy distribution infrastructure operated by EDP Distribuição.

Acknowledgment: The research leading to these results has received funding from the European Community's Seventh Framework Programme under grant agreement no. 225186. Consortium: Eurescom, IHP Microelectronics, NEC Europe, INOV, EDP Distribuição, Budapest University of Technology and Economics, INRIA, Lulea University of Technology, Sirrix, Tecnatom, University of Malaga and FWA.

References

1. W3C, Web Services Architecture, W3C Working Group Note 11, February (2004), http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/.
2. IEEE Std. 802.15.4, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) (2003).
3. IEEE Std. 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (1999).
4. Silex Technology, SX-560 Intelligent Programmable WLAN Module, SX-5602009EN (2009), http://www.silexeurope.com/media/datasheets/SX-560-ds_en_0902.pdf.
5. Rocha, F., Grilo, A., Pereira, P., Nunes, M., Casaca, A.: Performance Evaluation of DTSN in Wireless Sensor Networks. In: Cerdà-Alabern, L. (Ed.) Wireless Systems and Mobility in Next Generation Internet, Proc. EuroNGI 4th Workshop on Mobility and Wireless 2007, Lecture Notes in Computer Science, vol. 5122, pp. 1-9. Springer-Verlag (2008).
6. Perkins, C., Bhagwat, P.: Highly Destination-Sequenced Dynamic Distance Vector Routing (DSDV) for Mobile Computers. In: Proc. of the ACM SIGCOMM'94, London, UK, pp. 234-244 (1994).
7. Grilo, A., Piotrowski, K., Langendoerfer, P., Casaca, A.: A Wireless Sensor Network Architecture for Homeland Security Application. In: Ruiz, P.M.; Garcia-Luna-Aceves, J.J. (eds.) Ad-Hoc, Mobile and Wireless Networks, Proc. 8th International Conference on Ad-Hoc Networks and Wireless (ADHOCNOW-2009), Murcia, Spain, September 2009. Lecture Notes in Computer Science, vol. 5793. Springer-Verlag (2009).