The Approach of European Network of Excellence CRUISE to Heterogeneous Wireless Sensor Networks Design and Integration

Francesco Chiti[◊], Romano Fantacci[◊], Leonardo Maccari[◊], Ken Murray[^], Dirk Pesch[^], Slobodanka Tomic[•], Ramon Aguero[✦], Juan José Pérez Solano[+], Tapio Suihko[⋆], Neeli R. Prasad[◆]

[◊]*Università degli Studi di Firenze,* [^]*Cork Institute of Technology,* [•]*ftw.Betriebs-GmbH,* [✦]*Universidad de Cantabria,* [+]*Universitat de Valencia,* [⋆]*Technical Research Centre of Finland,* [◆]*University of Aalborg*

***Abstract*—This paper deals with the integration of available platforms and testbeds within the Network of Excellence CRUISE, which belongs to the VI IST Framework. First, the existing testbeds are described in terms of application scenarios, hardware features and adopted communications protocols. Then, several considerations regarding the integration issues are given, involving diverse aspects, such as application area, network features and node characteristics. Finally, possible general approaches for sharing or jointly using, and eventually integrating, CRUISE partners' testbeds are presented.**

***Index Terms*—Wireless Sensor Networks Testbeds, Cooperation and Integration, Internet based approaches, Management of Databases of Experimental Data, Security.**

I. Introduction

The Network of Excellence (NoE) CRUISE (Creating Ubiquitous Intelligent Sensing Environments) intends to be a focal point in the planning and coordination of research on communication and application aspects of wireless sensor networking in Europe [1]. It brings together a diverse group of partners who will integrate their expertise and knowledge gained in projects on related fields. CRUISE partners are closely working on the joint programme of activities specified in this project, which consists of information collection, comparison, validation and dissemination.

In particular, one of the most relevant purposes of the NoE CRUISE is to provide an operational and efficient way to make use of existing testbeds, measurements and experiences with different sensor platforms. The sharing of the testbeds may allow implementation and testing of new protocols, while the sharing of measurements will provide more realistic input data for further simulation studies.

In this respect, the availability of testbeds will enable some more concrete work for researchers whose current interests are mostly focused on solving challenging optimisation problems, brought about within the sensor networking research field. Although the creation of an extensive testbed is not a goal that is targeted to be fully achieved within this network of excellence (as this is not an infrastructure project) the name of our network Creating Intelligent Ubiquitous Sensing Environments captures our great interest in physical realization of this vision.

According to this vision, partners in CRUISE Work Package 122 ("Integrating Test Beds and Measurements") have collected and disseminated information about their test beds, their experiences with different platforms by means of filling a questionnaire on existing testbeds; all the information collected is currently available within the web portal, so as to be able to monitor the future evolution of pilot sites [1].

This paper summarizes the aforementioned test beds in terms of application scenarios, hardware features and adopted communications protocols, together with indicating future possible evolutions. Next, several considerations regarding the integration issues are given, involving different aspects as: application area, network features and node characteristics. Finally, possible general approaches for sharing or jointly using, and eventually integrating the testbeds of CRUISE partners are presented.

II. Overview on Existing TestBeds Features

The following information has been collected within a questionnaire that has been filled by every WP122 participant that owns a testbed or plans to have a testbed [1]. The web questionnaire has been filled by 13 participants. The main results are graphically summarized in Figure 1, Figure 2 and Figure 3.

The 13 described testbeds can be divided according to the state of the deployment:

- 9/13 are in a set-up phase
- 2/13 are stable and running
- 1/13 is not deployed but in the planning phase

A. Application Area

The vast majority of the testbeds (9 over 13) have been projected to be applied to for environmental monitoring, we cite:

This work was supported in part by the EU Integrated Project FP6-IST-1-508774-IP "GoodFood" as well as by the EU Network of Excellence FP6-IST-4-027738-NoE "CRUISE" and EU STREP FP6-IST-045299-STREP "DustBot".

0-7695-2988-7/07 $25.00 © 2007 IEEE
DOI 10.1109/SENSORCOMM.2007.57

- Monitoring of agro-food chain with regard to the wine segment.
- Fire fighting.
- Watershed and traffic monitoring.

Among other application areas we cite:

- Domotics: home devices control.
- Health monitoring: heart rate with mobile tags positioned on athletes on a skiing field.
- Logistics/Factory automation/Surveillance.

Some of the testbeds may combine more than a single application; one in particular belonging to KU has been deployed for the study of networking issues and has no specific application.

1) Observed parameters

Data sensed are heterogeneous, and almost all of the parameters are focused on environmental conditions. Apart from heart beating for medical purposes, almost all testbeds present temperature sensors, other sensors present are:

- (5/13) Sound sensors
- (5/13) Accelerometers
- (4/13) Magnetic sensors
- (5/13) Light sensors

Sensing modes are equally divided between synchronous and asynchronous, with some of them working in both modes.

B. Networking Aspects

Almost all the testbeds are formed by a number of nodes varying between 10 and 30, with some gateways, depending on the application. Particular cases are represented by KU testbed that is constituted by 120 nodes and is conceived for the study of networking issues, and UO testbed, which is composed of 30 gateways, collecting data upon mobile tags. Topologies are miscellaneous (flat/star/tree/clustered).

1) Lower layers

Most (7/13) of the testbeds use 2.4 GHz transmission using IEEE 802.15.4 physical layer, 4/13 use also IEEE 802.15.4 MAC layer (alternatives are S-MAC/B-MAC/StarMAC and proprietary solutions), data rate range from 38.4 to 250 kbps. Heterogeneous layer 3 protocols are used.

2) Gateway

Gateway interfaces adopt heterogeneous technologies:

- 6/13 use wired LAN, connected to PCs or to dedicated gateways (Stargate SPB400, MIB600).
- 1 employs a serial connection.
- 1 uses GSM/GPRS.

3) Security

Few testbeds approach security issues, implementing symmetric (2/13) or asymmetric (1/13) key inter-node cryptography and authentication of data, or node-gateway authentication.

C. Node Characteristics

1) Communications protocols

A possible approach to pilot sites integration could resort to the communications protocols design through the same operative system, namely TinyOS [10].

In particular, Sensinode is releasing a free protocol stack for WSNs called NanoStack [11]. It gives IEEE 802.15.4 and 6LoWPAN support and is easily portable to many different platforms. It is based on FreeRTOS.

2) Hardware platforms

The majority of the testbeds (6/13) use different releases of the MICA platforms (MICA2/MICAZ/MICA2DOT [12]), some alternatives are Telos [12] or Intel devices. Most of the nodes run on AA or AAA batteries.

Intel/Texas/Atmel/MPR2400CA processors are controlled in the most common case (6/13) by Berkeley TinyOS operative system.

Finally, it is worth noticing that European WSN hardware is available from Sensinode Ltd. [11].

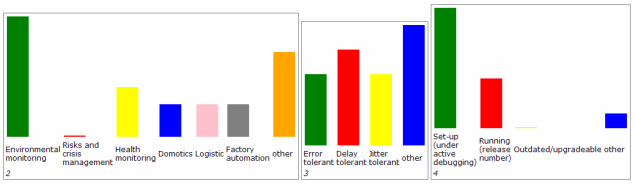

Figure 1 - Application, QoS, deployment status.

Figure 2 - Topology, nodes types, wireless technologies, traffic models, and control models.

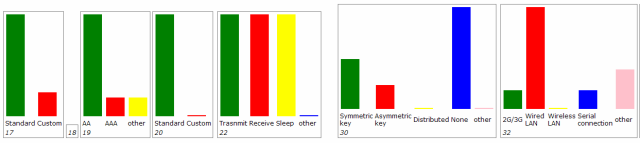

Figure 3 - Protocols, power management, security, remote connectivity.

III. General Approaches For Integrations

In this Section, a set of guidelines for testbeds joint usage and integration of testbeds is presented. These guidelines cover possible integration scenarios and approaches. According to the protocol stack representation, the integration may be performed at different levels, with an increasing degree of interoperability when approaching the lower layers, especially at the physical layer. This preliminary proposal is likely to be refined further when addressing the most suited integration plan in accordance to the partners' resources availability. It is worth recalling that WP122 activities aim at (1) *sharing and joint use*, and (2) *integration* of testbeds of CRUISE partners.

Sharing or **joint use** of testbeds can be relatively easily

achieved. Sharing scenarios may be described as following:

Local Access to a Testbed as a part of a Joint Research Activity (JRA): In this scenario, institutions involved in the joint research activity use the testbed of one institution for testing, for example, a routing protocol jointly developed. The joint activity in the testbed can be realized using an exchange action. This activity fosters diversity of joint work, as one partner may focus on simulation and the other on testbed measurements of the same scenario. On the other hand, it does not directly lead to testbeds integration.

Remote Access to a Testbed: In this case, CRUISE partners who already have the tools for the remote access to their testbeds could offer them to other participants, working in different activities. As already available (and the part of the pre-existing knowledge) the remote access may be fully proprietary. The partner offering the remote access provides the access tools and the credentials for allowing testbed accessibility. This scenario differs from the previous one in the fact that the physical presence of the partner using the testbed is not necessary, nor is the presence of the partner offering remote access. This activity provides further insights in the issues of remote access to the partners offering it, and offers the possibility to other participants to use the remote testbed in their joint work activities.

Integration of testbeds is much more challenging task than the joint use, and it includes identifying of common objectives, designing integration framework and implementing common APIs and tools (a kind of "standards" for the CRUISE). Several possible scenarios are listed below:

Data Integration: In this scenario, existing testbeds are used to produce data traces in multiple testbeds in well defined and controlled experiments that can be the basis for further joint comparison studies.

Unified Remote Access to the Testbeds: In this scenario, CRUISE partners define and implement the common remote access to the testbed. Existing proprietary solutions can be used as the first step for this activity.

Gateway-based Integration of Testbeds: In this approach, CRUISE partners define and implement the common integration layer and implement gateways to interconnect the testbeds.

Directly Inter-operable test-beds: In this scenario, CRUISE partners decide on the common physical and MAC layer and design and implement the common middleware for integration of different testbeds.

In the following, the issues related to possible approaches for the integration of testbeds are described.

A. Data Integration

The first, high level approach to achieve ***integration*** of available testbeds focuses on the ***aggregation of data*** collected in distributed measurements. High level fusion of data collected in different testbeds can be achieved in a common database. To this aim, experiment data - including scenario description, collected status data of network nodes and collected sensor data - are described in a unified way with the help a meta-language.

As an example, the same experiment, e.g. control of home device in domotics environment, could be repeated under same conditions in two different testbeds and the results might be stored in the same data format and in a single database. Data generated in different testbeds can be compared together to assess the impact of some inherently different settings of diverse testbeds. Note that, beyond WSN research, the developed data integration methodology may also have general relevance to real-world cross-disciplinary applications of WSNs. For example, different measurements could be integrated in order to provide a better insight into a certain phenomenon, e.g., the impact of environmental conditions into human health.

This kind of integration and comparison can be achieved within the same application areas of the testbeds, for well defined and controlled scenarios. The comparison studies could focus on the consistency of data generated in different testbeds.

The data integration requires the common approach to the scenario description, including the depiction of the topology and of used protocols, and the common data model for the application specific sensor data and the status data of the sensor nodes. In CRUISE, the high-level model for the scenario is already defined and used for the specification of several application scenarios [6]. Assuming that the same definition is used for describing the simulation scenarios in the corresponding work package, the collected data can be used also for comparing the simulation results and testbed results.

Apparently simple, this approach bears a serious problem related to the controlled repeatability of experiments. It is often the case that the general-usage full-description of the scenario is rather difficult to achieve. From some experience, repeating the test in the different settings, works mostly when the activities are synchronized, well discussed, done at the same time, checked and re-checked in a kind of a "joint testing campaign".

B. Common Remote Web-Based Access

This approach requires the setup of a common user interface to a number of different testbeds. The aim would be to make multiple experiments on different testbeds in parallel, and to be able to merge (i.e., to associate) in real time the state of the nodes and information from the motes.

If the devices are remotely reprogrammable and the operating system is compatible, the same algorithms could be installed and verified in different testbeds.

One suggestion is to resort to the existing Remote Java tool from DIKU, University of Copenhagen [9]. It could be a very useful starting point for remote management and testing of sensor networks. It is being used with TinyOS and can also interface with other OSs.

C. Gateway-based Integration (Weak in-situ Integration)

Gateway-based integration of the testbeds enables inter-working between the different test beds. This kind of integration, also referred as *weak in-situ* integration [8], can be both *local* and *remote*.

Whenever the available testbeds might be moved through different institutions, local *weak* in-situ integration could be viable, and thus testbeds can be gathered in the same situation (spatial vicinity) and linked using the gateway facilities. This level of integration requires compatible gateway technologies, where each gateway should be responsible for a spatially different area of the field under monitoring (occupied by the different sub-testbed), and results should be merged in a common database. Moreover, the integrated gateways can be able to cooperate and perform data fusion/aggregation algorithms. The main benefit of this approach with respect to the previous one is the monitoring of real wide area networks and the improved quality of the collected data.

Remote weak in-situ integration is also possible. In this case the testbeds are not in the same spatial area, but they can directly interwork over the gateway facilities and the data from one test bed can flow into the other test bed. Weak in-situ integration can be achieved at different layers; Figure 4 shows an illustrative example of this approach.

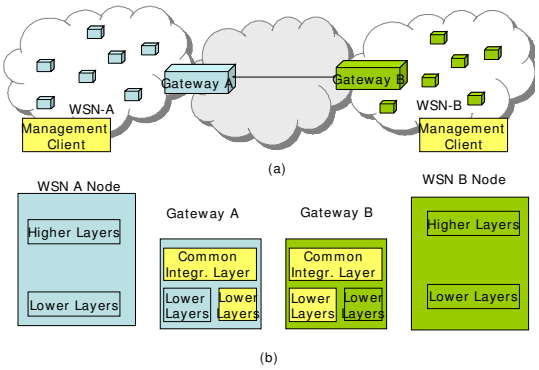

Figure 4 - Gateway-based Integration.

D. Middleware-based Integration (Strict in-situ Integration)

If motes (sensor devices) are compatible, a single testbed could be made out of the nodes belonging to distinct testbeds, to accomplish a larger one, as indicated in Figure 5. As an example, study of scalability and performance of routing protocols, or authentication protocols may be more accurate if the platform used spans over a wide area. This level of integration requires compatible radio interfaces and compatible MAC, thus it is called *strict*.

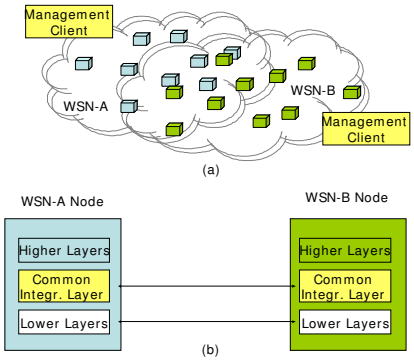

Figure 5 - Middleware-based Integration.

IV. Guide Lines For Integration Plan

In order to better align with the work that is being carried out in the rest of the CRUISE project, the integration plan would assume that the most relevant reference scenarios - i.e., those which more attention will be paid to - are both the environmental and the health monitoring ones, since they have been already selected by the corresponding work packages. These particular scenarios are also being used in the rest of technical activities so as to define the use cases which need to provide the required background.

The understanding is that the application scenario does not necessarily pose a lot of requirements on the integration work, especially considering the discussion about the different levels of integration already faced in Section III. However, for the sake of alignment with the rest of the work being done in the CRUISE project, it is believed that trying to fit the integration efforts within each of the two aforementioned scenarios is really worthwhile.

Moreover, this choice is compliant with the existing testbeds main features, as discussed in Section II. Finally this could allow the sharing of more realistic measurements, in order to provide deeper insight into practical case studies, which is one of the most relevant achievements of WP 122.

A. Adopted Integration Approaches

1) Principle

Sensor networking has demonstrated great potential in many areas of scientific exploration, including environmental, geophysical, medical, and structural monitoring [2]. However, sensor networks have largely been focused on dense, small-scale homogeneous deployments to monitor a specific physical phenomenon [7]. The integration of multiple heterogeneous sensor network environments provides the ability to monitor diverse physical phenomena at a global scale. In addition, such remote integration will provide the infrastructure for querying and fusing data across multiple, possibly overlapping, sensor networks in different scientific and administrative domains. Most sensor network applications aim at monitoring or detection of phenomena. Examples include building and environmental

control [4], wild-life habitat monitoring [3], and forest fire detection [5]. For such applications, the sensor networks cannot operate in complete isolation; there must be a way for a monitoring entity to gain access to the data produced by the sensor network. By connecting the sensor network to an existing network infrastructure such as the global Internet, a local-area network, or a private intranet, remote access to the sensor network can be achieved. Given that the TCP/IP protocol suite has become the de-facto networking standard, not only for the global Internet but also for local-area networks, it is of particular interest to look at methods for interconnecting sensor networks and IP core networks. Sensor networks often are intended to run specialized communication protocols, for example IEEE 802.15.4 and ZigBee, therefore an all-IP-network will not be viable, due to the fundamental differences in the architecture of IP-based networks and sensor networks. It is envisaged that the integration of sensor networks with the Internet will need gateways in most cases. A proxy server at the core network edge is able to communicate both with the sensors in the sensor network and hosts on the TCP/IP network, and is thereby able to either relay the information gathered by the sensors, or to act as a front-end for the sensor network. It is also envisaged that sensing devices will be equipped with interfaces to wireless access networks such as 2/3G and WLAN enabling total ubiquitous connectivity. The proposed network architecture is depicted in Figure 6.

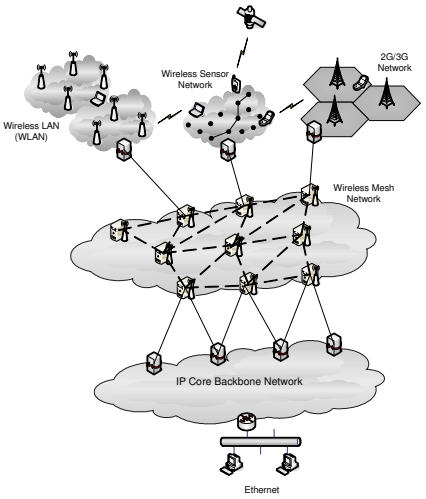

Figure 6 - Integrated Sensor Network Architecture

2) Achievable Benefits and Results

Expected achievable benefits and results depend on the adopted integration approach. According to the classification previously proposed, they could be highlighted as it follows:

a) Data Integration:

- To produce common model for description of test scenarios, network and sensor data for different WSN application fields;
- To have a common repository of comparable measurements (with meta description);
- To jointly compare obtained results, by applying data fusion algorithms;
- To perform joint measurements on practical case studies:
  - climate and environmental monitoring across different regions of Europe;
  - health monitoring with eventual application to the human health care systems;
  - mixed scenarios able to give an insight on relationship between climate and health or quality of agricultural products and human health.

b) Gateway-based Integration:

- To produce a common set of gateway functionalities, allowing for automatic integration of connected test-beds;
- To demonstrate the feasibility of hierarchical WSNs;
- To produce a proof a concept of interworking among heterogeneous pilot sites;
- To perform integrating large area scenarios.

c) Infrastructure Integration

- To decide on the common PHY and MAC protocols
- To produce a common concept for the common integration (layer middleware), which allows for automatic integration of connected test-beds.

V. A PRACTICAL APPLICATION: JOINT ACTIVITY ON SECURITY FOR MOBILE WSNS

As an example of a real application of the integration effort so far described, we present a joint work realized as a subtask of the work packages 230 (WP230: Security and Mobility) of the CRUISE NoE [13].

The aim of this activity was the realization of a common authentication procedure to be designed and realized by the University of Florence and to be implemented and optimized in the testbed offered by Aalborg University.

The authentication procedure is intended to support mobility and be lightweight and distributed.

Discussions in WP230 lead to the definition of common criteria to describe mobility and security aspects to be applied to a common framework for security and mobility (see [13]). Based on the result of such discussions the algorithm was planned to support sink node mobility, that is the presence of a mobile node that moves across the network collecting information from the sensors.

Once decided which mobility model the network should support the choice of a decentralized algorithm was taken due to the following considerations, taken from [13]. A centralized scheme works only if the server is always reachable, but it

produces high level security, since no node can join if the manager of the network doesn't allow it. If the network is large enough, though, a multi-hop path might be too much time or energy consuming. Moreover since the handshake must be bidirectional, the routing protocol should be able to map communication from the server to the nodes, which is not always needed for monitoring purposes.

If this kind of user authentication procedure is used we say that there is a *centralized trust* relationship between the new node and the authentication server, and consequently also between the new node and its neighbor that received the key from the server.

If a distributed procedure is used, the nodes on the border of the network are responsible for letting the new node in. This makes the operation quicker but delegates the trust establishment away from a centralized server, to nodes that might even behave maliciously. In this case we call the trust relation *local trust*.

If a sink node has to be authorized to enter the network multiple times as it moves across the monitored area, a multi-hop authentication would represent an unacceptable overhead. As suggested by the work of WP230 a distributed cryptographic algorithm, was used.

WP230 defined also some larger criteria that include authentication procedures but also different procedures to define *trust* between nodes. In particular, with distributed authentication a set of malicious nodes may cooperate to produce false authentication credentials, this is due to the distributed nature of any decentralized protocol. Thus, it is important to implement also some reputation scheme in order to track the behavior of nodes that will be included in the authentication procedure. The proposed protocol contains some misuse detection techniques that implement plausibility checking, as suggested in [13] for reputation monitoring.

Following the integration guidelines, the University of Florence begun the development of a common MAC layer authentication procedure that could be portable to a real testbed given by the Aalborg University. The implementation was designed with data integration in mind (the objective of the joint work was to produce a suitable authentication protocol, so the main part of data exchanged by the researchers was aimed at performance measurement of the protocol and stability tests). The code was first implemented in a simulator for WSN, but perfect integration was possible once the code was moved to Aalborg University testbed. Even if applied to a virtual testbed (the simulated one) and a real testbed the integration procedure is the same as applied to two real testbeds. The code supported data homogeneity and platform independence, so that real integration at the end has been possible.

Once ported to the platform, the results given by measurement of data confirmed the evaluations given in the simulated environment, but outlined also some problems due to implementation of the code to the chosen platform. The results of the effort are summarized in [14].

VI. Conclusions and Further Developments

In this paper the integration of available platforms and test beds within the Network of Excellence CRUISE is investigated. To this aim, the existing test beds are described in terms of application scenario, hardware features and adopted communications protocols. Then, several considerations regarding the integration issues are given involving different aspects as: application area, network features and node characteristics. Finally, possible general approaches for sharing or jointly using, and eventually integrating the testbeds of CRUISE partners, are presented. With the aim of designing the integrated test bed, the guide lines for integration plan are presented, involving the definition of a common reference scenario, the principle commonly adopted and a list of achievable benefits and results. To provide a practical example of testbeds integration by means of the above introduced principles, a shared framework to allow the realization of a common authentication procedure is finally described.

Acknowledgment

The authors would like to express their gratitude to the members of the Network of Excellence CRUISE for their supporting in this research, as well as for their comments and fruitful discussions.

References

[1] *CRUISE Network of Excellence Web Portal*, http://www.ist-cruise.eu.
[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” *IEEE Computer Networks*, vol. 38, pp. 393-422, March 2002.
[3] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao. ‘Habitat monitoring: Application driver for wireless communications technology’, In Proceedings of the 2001 ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean, April 2001
[4] S.S Intille, “Designing a Home of the Future”, IEEE Pervasive Computing, April – June 2002
[5] K. Lorincz, D.J. Malan, T.R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, “Sensor Networks for Emergency Response: Challenges and Opportunities”, IEEE Pervasive Computing, Oct – Dec 2004
[6] CRUISE WP112, Deliverable D112.1, ‘Report on WSN applications, their requirements, application-specific WSN issues and evaluation metrics’
[7] CRUISE WP113, Deliverable D113.1, ‘Report on future needs, research strategy and visionary applications for sensor networks’
[8] CRUISE WP122, Deliverable D122.1, ‘Report on existing test beds and platforms’
[9] *DIKU Testbed*, http://www.distlab.dk/remote.
[10] *TinyOS*, http://www.tinyos.net.
[11] *Sensinode*, www.sensinode.com
[12] *Wireless Sensor Network Platforms*, http://www.xbow.com/Products.
[13] CRUISE WP230, Deliverable D230.2, ‘Mobility and Security Framework for WSNs’.
[14] L. Maccari, L. Mainardi, M. A. Marchitti et al. 'Lightweight, distributed access control for wireless sensor networks supporting mobility'. Submitted to SecureComm 2007.