Sensors and RFID Enabling Smart Space

Simona Temelkova, Natasha Paunkoska, Mihajlo Pavloski,
Vladimir Atanasovski, *Student Member, IEEE,* and Liljana Gavrilovska, *Member, IEEE*

***Abstract* — The smart space paradigm has been a popular research topic lately. Its concept allows ambient intelligence in living and working environments that can upgrade people's quality of life. Smart space technology enablers are found among sensors and Radio Frequency Identification (RFID) tags used in many different applications. They facilitate creation of surroundings that are smarter, safer and more organized. This paper proposes an implementation example in setting of intelligent space concept that is implemented in order to save time, better organize the resources and take care about building safety.**

***Keywords* — Sensors, RFID, Smart space, Intelligent environment.**

I. Introduction

Enabling flexible smart space architecture aims to introduce a higher level of automation and monitoring of different environments. This intelligent surrounding promotes occupants' comfort, anticipates and responds to their needs and provides convenience and security through management of technology. Giving our everyday surroundings the ability to sense and identify every object, every person and their respective activities would experience enormous benefits.

Wireless Sensor Networks (WSNs) are foothold of the future generation of intelligent space systems. They serve as acquisition tools of ambient circumstances in order to replace or upgrade users' experiences. Successful ambient adaptation leads to automatic execution of users' activities and needs. On the other hand, being able to identify surrounding entities and to organize them in a desired way is a characteristic that is found only with RFID technology. Therefore, this paper will exploit both, i.e. WSN and RFID, for realizing a vision of a smart space arrangement.

The scope of the paper is to present a possible intelligent scenario in the premises of the Institute of Telecommunications at the Faculty of Electrical Engineering and Information Technologies (FEEIT) in Skopje. The motivation for building this solution is based on the need of better organization, time saving and objects monitoring options. Such solution would also support and simplify everyday users' activities. Additionally, access control and emergency situation notification are assumed as important necessities in this realization.

This paper is organized as follows. Section II briefly illustrates numerous challenges in smart space and gives a short overview and comparison of technologies of interest as representatives of sensor networks and RFID equipment. Section III describes the usage scenarios for RFID and WSN implementation at the targeted premises and the end results obtained by this realization. Finally, Section IV concludes the paper.

All authors are with the Ss Cyril and Methodius University in Skopje, Faculty of Electrical Engineering and Information Technologies, Macedonia (phone: 389-2-3099114; fax: 389-2-3064262; e-mail: liljana@feit.ukim.edu.mk).

II. Smart Space Implementation Issues

Current works defining a smart space concentrate on:

- autonomous behavior (services are autonomous by means of interactions with the user, with resources and with other services) [1],
- dynamic environment adaptation (dynamically adapt to users' activities and available resources) [2],
- emergency situation indication (on-time information distribution),
- optimal energy sourcing (maximizing network lifetime) [3],
- differentiated surveillance (enabling different security levels for various target areas) [4],
- distributed optimization ("in-network" data processing eliminating a central point) [5].

All these challenges converge to attain the common goal of reducing the operating cost of a building or home, but still maintaining maximum efficiency for the occupants, which includes the desired internal environment.

The definition of a smart space has always been changing depending on the currently available technology and the environment where it is to be implemented. Today many relevant standards and technologies such as Bluetooth technology [6], IrDA [7], RFID [8], WLAN [9], Zigbee [10] etc. are on disposal for smart space implementation. Despite of many common characteristics, like the used frequency band or purpose, the scope of these technologies can be in totally different implementation examples. WLAN is a broadband communication technology that enables transmission of multimedia contents, video streaming and high-speed application support. Bluetooth technology and ZigBee achieve much lower data rates and therefore are used in a different way. While ZigBee is focused on control and automation, Bluetooth is focused on connectivity between laptops, PDAs and in cable replacement in general. ZigBee uses low data rate, low power consumption and works with small packet devices, whereas Bluetooth technology uses a higher data rate, higher power consumption and works with large packet devices. Also, ZigBee networks can support a larger number of devices and a longer range

between devices then Bluetooth networks. For its applications, Bluetooth technology must rely on fairly frequent battery recharging, while the goal of ZigBee is to use the same battery for a prolonged period (one month to a year). In timing critical applications, ZigBee is designed to respond quickly, while Bluetooth technology takes much longer and could be detrimental to the application.

Another emerging technology is the Radio Frequency Identifier (RFID), intended for providing identification numbers to objects. RFID uses devices called readers for emission of radio waves and tags for reflecting back the waves with the needed ID. Tags are small electric circuits placed in tracking objects, animals, humans and usually have small amount of memory capable of storing the unique identification number. This type of tags with small read/write range, small memory and power supplied by the radio waves are called *passive* tags. There are also *active* tags which are battery power supplied, have bigger dimensions, read/write range and memory. The choice of tags to be used depends on the type of the application and its demands. The working frequencies for reader – tag communication belong to the Industrial, Scientific and Medical (ISM) radio band [11]. A comparison of all potentially used technologies for smart space enabling is given in Table 1.

Table 1: Comparison of communication technologies for enabling smart space [13, 14]

Technology	WLAN	Bluetooth	ZigBee	RFID
Frequency band	2.4 GHz – b/g 5.8 GHz – a	2.4 GHz	868/915 MHz 2.4 GHz	13.56 MHz, 868/915 MHz, 2.4 GHz
Typical range	100 m	< 10 m	10-100 m	< 16 m (passive) < 80 m (active)
Data rate	54 Mbps	1 Mbps	20-250 kbps	10 – 640 kbps
Application	LAN, Internet	Cable replace-ment	Sensor network	Item identifi-cation

It is obvious that ZigBee and RFID are the most appropriate technologies for a potential smart space implementation. The former one is used for communication between SunSPOT [15] devices which form the WSN in the smart space under consideration, while the latter one is used for identifying objects and people in the smart space.

III. IMPLEMENTATION

A complementary combination of WSN and RFID technology can be used in creating a smart space. The aim of this integration is to demonstrate the possibilities of the WSN and RFID combination through a practical setup and to develop an application which can be used in many different indoor surveillance systems. The envisioned usage scenario for building a smart institute space is divided into two main parts: *identification scenario* and *protected institute scenario*.

A. Identification Scenario

It is assumed that identifying objects and people at the targeted premises is of great importance in enabling an intelligent environment. Therefore, RFID technology is in the focus of the implementation case. Active tags are used for identifying people and passive ones for identifying objects.

The "active" scenario is chosen because of the daily difficulties the students are faced with when looking for a professor in the Institute, as well as for saving the professors' and employees' time. In this case, every employee of the Institute has a badge holder ID. When a student enters the faculty premises he can check (on the monitor placed in the entrance door) if the professor/employee he needs is in the Institute.

RFID equipment is used for the purposes of this scenario. Some important characteristics of the active tags and reader are multi-tag read capability and read range that covers an area with a radius of 30m. Tags transmit on a central frequency of 868 MHz and receive on 433 MHz. The reader and host computer may be connected through two possible ways, either RS232 (9600-115200 Baud) or Ethernet (10/100 Mbps).

The "passive" scenario distinguishes two different types of use-cases: *permanent* and *non-permanent* case, enabling constant item observation and a one-time emergency use, respectively. The permanent case is intended for surveillance of items with steady point of presence and is suitable for monitoring office and computer equipment in the institute. Any change in these object's location results in proper signalization using email messages and sound warnings. The non-permanent case on the other hand is based on a one-time selection of "important" items and can be used in everyday purposes and emergency situations. By detecting missed "important" items, this case acts like a reminder when the user leaves a location. On-time information is provided by sound indications.

The used equipment includes tags and a reader as follows: passive UHF 96-bit tags, EPC Gen 2 and ISO 18000-B compliant, compatible with a Gen 2 passive reader. The reader's parameters are: tag identifying speed of 8m/s, read distance of 2m and 1000 tags per second reads, which make it suitable for an indoor implementation. A compromise must be made between the size of the tags and the read/write range to the reader, since smaller sized tags have shorter range. As standardized by the European Telecommunications Standardization Institute (ETSI), the communication tag – reader works on 868 MHz central frequency (same as the active - equipment case), with 200 kHz available bandwidth per channel. Based on the 96-bit identification scheme by EPCGlobal, each tag has a unique number (code) as given in Fig. 1. This code can enable a unique identification of 2^{28} product manufacturers, 2^{24} types of product classes and 2^{36} products among each class. [11][12]

01.	0000A89.	00016F.	000247DC0
Header	EPC Manager	Object Class	Serial Number
8 bits	28 bits	24 bits	36 bits

Fig. 1. Electronic Product Code (EPC) hexadecimal representation [11]

The connection reader – host computer is an important factor in building a smart space. At the moment of writing, wireless solutions are still in development phase and mostly pointed to WLAN which should make the actual implementation easier. Among LAN and a serial RS-232 connection the second one is chosen as a more effective way to program the reader function. This way, the application, which is made in C--Sharp [16], makes use of System.IO.Ports namespace integrated in the C#.NET Framework [17]. SerialPort is the most important class which establishes the connection with setting parameters like: port name, baud rate, parity, stop bits etc. A connection to an ADO.NET database [18] is also established in order to store all tagged objects. When successfully connected to the reader, the host computer can easily compare the tag's ID-s and arrival times and thus make a correct decision.

B. *Protected Institute Scenario*

The choice of the protected institute scenario arises from the security issues, i.e. the important equipment needs to be kept in order, the employees need to have appropriate working conditions and to be protected from unexpected dangerous situations etc. The WSN deployed in the Institute's premises aims to provide the employees' protection from environmental and human made disasters (e.g. fire) through their early detection and timely notification. The WSN network assisted by the RFIDs can provide access control to protect some particular areas of interest.

The wireless sensor nodes, with the attached sensors communicate with the base station which is connected with the server. They measure the environmental variables constantly, and in case of increased/decreased measured values the authorities are notified of an emergency situation by receiving an e-mail, SMS message or receiving a call.

This scenario also includes limited access in the part of the institute where the notifying devices are placed. The control is provided by using an RFID passive reader placed at the protected room entrance. Only authorized personnel have permitted access by using passive RFID tags.

Protected institute scenario description provides enumeration of the required hardware for its realization. Mainly modules from Sun Microsystems are chosen to be used in the part about protection from environmental and human made disasters, since their characteristics are usually desirable for research and educational needs. Each SunSPOT module consists of battery, processor board and sensor board. Some of there main features are: battery (720 mAh litium-ion), CPU (180 MHZ 32 bit ARM920T), memory (512K RAM/4M Flash), radio (2.4 GHz IEEE 802.15.4). SunSPOTs, based on ZigBee communication, represent an open source platform built on Java VM (Virtual machine) [15]. On each SunSPOT, 2 types of sensors are connected, i.e. a temperature sensor 1124 Phidget Inc., which should be calibrated for every SunSPOT separately and smoke detector, which is highly sensitive on carbon dioxide. Measurements from the sensors are made constantly. After that the measured results are sent to the base station. The main idea of the algorithm, placed in the SunSPOTs, is dividing the temperature scale in five intervals and combining this ambient variable with possible presence of smoke. The string dedicated for the database consists of SPOT_ID, measured temperature, detected smoke and appropriate message calculated with the algorithm deployed on the Sun SPOT. The GUI developed for this purpose displays the current status of the SPOTs' and sensors' parameters.

Notification devices are activated depending on the criticality of the circumstances. In case of temperature measurement higher than 50 degrees Celsius and smoke indication, a notification is sent for high probability of fire situation.

Apart from the WSN system, the protected room scenario is realized with passive RFID components. The used equipment includes passive reader OC200 and passive tags. Important characteristics of those devices are: operating distance of 20 cm, operation time of less than 1s, supply voltage DC 12V, LCD 128x64 blue screen etc.

C. *System Architecture and Performance*

The logical architecture of the smart institute implementation is represented on Fig. 2. It illustrates the combination of both scenarios that were previously elaborated.

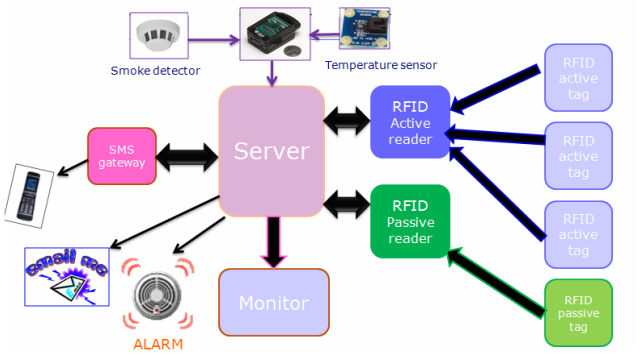

Fig. 2. Logical system architecture

The alert information is sent in a form of a SMS message through the GSM/GPRS gateway connected directly to the server's USB port. The sound&light alarm and the dialing device, which are connected to the server through the Phidget Interface Kit 8/8/8 port hub, are also activated.

Fig. 3 presents an alarm situation in the identification scenario. A sound warning notifies the user of a forgotten important object which is also displayed on the monitor. Combining different identification situations and different

alarm indications provides this scenario with a plethora of options.

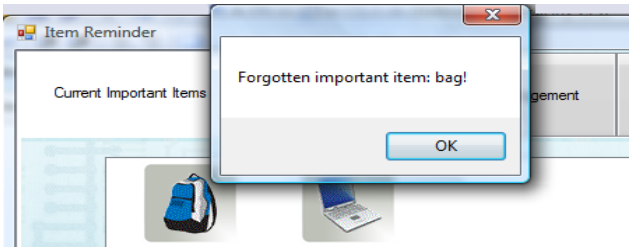

Fig. 3. Indication of a forgotten item, accompanied by a sound warning

On the other hand, Fig. 4 illustrates an abnormal situation in the protected institute scenario displayed on the GUI, which is followed by an alarm, an SMS and an e-mail message and a call establishment using a dialing device. The pink line represents a threshold for normal temperature measurements. In this case it is crossed by the high daily temperature measurement values, given as an output from the temperature sensors, which is presented with the black line and defines an irregularity.

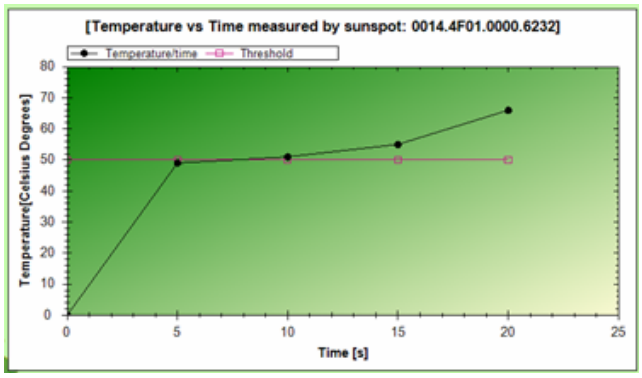

Fig. 4. Temperature measurement values

It is obvious that by monitoring done through the GUI of the applications and activation of the specific devices depending on the criticality of the circumstances, end result helps institutions to be more efficient and flexible to employees needs, also decreases the damages and upgrades the security.

IV. Conclusions

The smart space implementation concept is an important future field of research and business due to numerous users' benefits. Enabling an intelligent space includes combining several communication technologies, wired or wireless. This paper examined and compared some of them and provided their possible smart institute implementation and assignation.

A solution for a smart institute organization, including identification of objects and people and covering security issues is given. The identification scenario gives an automated picture of targeted premises, while the security scenario enables normal working conditions, access control etc. Tagging and monitoring objects, as well as their future Internet connection brings closer the idea of Internet of Things [19]. Further work in this direction could employ on-line system monitoring, improved object localization, different security levels.

Acknowledgment

This work was funded by the EC FP7 ProSense project (http://www.prosense-project.eu). The authors would like to thank everyone involved.

References

[1] S. Meer, B. Jennings, "Design Principles for Smart Space Management", Waterford institute of technology, Waterford 2004.
[2] M. Vall´ee, F. Ramparany, L. Vercouter, "Dynamic Service Composition in Ambient Intelligence Environments: a Multi-Agent Approach", France Telecom 2005.
[3] T. Yan, T. He, J. A. Stankovic, "Differentiated Surveillance for Sensor Networks", in Proc. of the 1st international conference on Embedded networked sensor systems, Los Angeles 2003.
[4] M. Rabbat, R. Nowak, "Distributed optimization in sensor networks", Proc. of the 3rd international symposium on Information processing in sensor networks, Berkeley 2004.
[5] A. Giridhar, P.R. Kumar, "Maximizing the Functional Lifetime of Sensor Networks", Proc. of the 4th international symposium on Information processing in sensor networks, Los Angeles 2005.
[6] The 802 IEEE Standard for Information Technology – Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)
Available: http://www.ieee802.org/15/pub/TG1.html
[7] Infrared short range communications Standards
Available:
http://www.irda.org/displaycommon.cfm?an=1&subarticlenbr=7
[8] Radio Frequency Identification Standards
Available:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46145
[9] The 802 IEEE Standard for Information Technology – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications
Available: http://www.ieee802.org/11/index.shtml
[10] The 802 IEEE Standard for Information Technology – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)
Available: http://www.ieee802.org/15/pub/TG4.html
[11] Daniel Dobkin – "The RF in RFID – passive UHF RFID in practice", Newnes 2008.
[12] Matt Ward, Rob van Kranenburg – "RFID: Frequency, standards, adoption and innovation", Goldsmiths College, University of London, May 2006.
[13] M. Galeev, "Home networking with Zigbee", Embedded System Design, April 2004
Available:
http://www.embedded.com/52600868?_requestid=162203
[14] *Adopting Ultra-Wideband for Memsen's file sharing and wireless marketing platform*, Memsen Corp.
Available:
http://wireless.fcc.gov/outreach/2004broadbandforum/comments/ultrawideband.pdf
[15] *Sun™ SPOT Developers Guide*, Sun Microsystems Inc., August 2008
Available: http://www.sunspotworld.com/Tutorial/index.html
[16] C-Sharp multi-paradigm programming language, Microsoft Corp.
Available: http://msdn.microsoft.com/en-us/vcsharp/aa336809.aspx
[17] *.NET Framework*, Microsoft's platform for building applications
Available: http://www.microsoft.com/net/Overview.aspx
[18] *ActiveX Data Objects.NET class library*, Microsoft Corp.
Available: http://msdn.microsoft.com/en-us/library/aa286484.aspx
[19] *Internet of Things,* International Telecommunications Union Internet Report, 2007
Available: http://www.itu.int/publ/S-POL-IR.IT-2005/e