

Investigating RFID Enabled Devices in Smart Electronic Learning Environments

[doi:10.3991/ijim.v4i1.1139](https://doi.org/10.3991/ijim.v4i1.1139)

M.S. Soliman¹ and S. Guizani¹

¹ Qatar University, Doha, Qatar

Abstract—For e-learning systems to be successful, proper understanding of the learner is crucial. This can be done with the use of learners’ profiles. However, there is a need for the availability of such information for mobile learning environments to make it available when the learner roams between different spaces. This paper investigates the application of RFID technologies for this use. We suggest using new advancements in RFID technologies with smart tags to identify and extract learners’ data/profile in the move. Furthermore, the learner will be carrying this data for better learning interoperability in smart spaces. New interesting educational scenarios are becoming available to provide context-awareness for the educational process. The tradeoffs between the availability of further information and privacy are discussed.

Index Terms—Mobile Learning, PLE, RFID, Smart Spaces

I. INTRODUCTION

With new e-learning tools and methods are evolving, the use of the classical classrooms becomes more questionable. Will classical rooms in traditional teaching/university disappear? An alternative way of thinking is to improve and redesign the traditional classroom. Since the proper learning should be a balance between all methods, we should also advance the physical space. Several Universities such as MIT started projects in this regard. Smart spaces and highly personalized location-based services are keys for this advancement. Augmented reality tries to relate the virtual environment to the physical space with location-services thus benefiting both environments. The revolutionary RFID technology acts as an enabler for these augmented paradigms since it provides location-based information.

RFID (Radio Frequency IDentification) is a broad-based rapid expanding technology that impacts business and society. An RFID tag is a microchip attached to a minuscule antenna. As depicted in Figure 1, an RFID reader transmits commands and energy to active tags by electromagnetic wave tags. Communication from tag to reader is based on inductive coupling (LF and HF tags) or on electromagnetic wave backscattering (UHF tags) modulation by the data stored on tag. The scanning device (reader) converts the radio waves reflected (scattered) back from the tag into digital information that can then be passed on to the computer network.

II. RELATED WORK

Since we are concerned with implementing active data through RFID, in addition to the technology itself, we are



Figure 1. RFID Overview

also interested in its regulation. Both domains are surveyed below:

RFID Technologies [1][2]: This topic includes contributions related to the development or to the study of physical and software components of RFID systems (tags, antennas, middleware, etc.), to recent technical advances, and performance analysis to the problem environment. Recently, references [3] and [4] have demonstrated the relationship between the reading distance of an RFID tag, the power transmitted by the reader and the gain antennas. Another study comparing two different antenna technologies has been presented in reference [5]. The results of this study show that the choice of a label should consider its antenna technology as well as attributes (size, shape, material) of the entity to be identified. Most of the studies are based on empirical approaches. The results indicate the importance of the choice of physical parameters for an efficient successful capture of data. For information subsystems, work [6] tries to include generic parameters that determine the performance of the middleware for RFID use. The parameters considered, among others the type of interrogators, the place of label reading and the rate of arrival of requests from users of RFID data. This study is interesting but it is not very detailed. It, however, confirmed the need for models to test the influence of parameters of subsystem on the overall performance.

RFID Safety and Regulation [2]: This topic includes various contributions on the standards governing the use of RFID technology for information security and the warranty of users’ privacy. The transmission of data via radio waves, despite its interesting potential, poses real challenges with respect to security and privacy. In the context of learning, learner surveillance and control is counterproductive for the learning result. The information ambient in air makes it more likely to be "captured" by malicious interrogators. Security is already a challenge for wired/wireless networks (the Internet), but not RF based networks alone. It is obvious that efforts must be viewed and implemented by the promoters of wireless networks from RFID technology as discussed in [7]. Researchers have even designed viruses and flaws in RFID technology to challenge and improve existing standards of security [8].

Our innovative work with respect to these themes:

1. For RFID technologies, we propose using cost-effective solutions for the sensors that launch and then stop the reading of the tags. These sensors are activated when a learner or an object enters or leaves the classroom zone.
2. For the applications, having the learner model/profile implemented on an RFID like card gives better knowledge management that facilitates its interoperability among different e-learning domains and smart learning environments.
3. In terms of security, the model/profile can be made safe and secure by having the tag carrying only the identification number. With this identification, we can request the protected database to provide us with data assigned to the tag in question. We can add data and modify it in the database without need to change anything in the tag or the RFID system, which presents a high degree of flexibility. Moreover, we suggest to crypt the identifier.

III. RFID-ENABLED SCENARIOS FOR SMART EDUCATIONAL SPACES

Introducing RFID in educational environments adds context and location-awareness that can create new educational scenarios not existed before. This is particularly useful for mobile learning. An example is provided in Figure 2 which shows how learner's data (e.g. on a profile), realized in an active card, can be detected and accessed. Other examples are shortly described below.

- **Training scenario:** A trainee enters a training room/workshop, when he enters the room, the RFID reader of the trainer will read the RFID tag on his card to know the presence of the trainee and extract the profile from the relevant database or card to present more trainee information to the trainer or tools. Such information can be useful for embedding better teaching styles, for example, they can be formed into groups of matching learning styles.
- **Smart Labs, Learning Equipments and Labs Discovery:** When a student enters a lab, he/she can scan the devices with an NFC (Near Field Communication)-enabled device to discover equipment that has attached RFID tags. With this identification, students can get more information about the device such as capabilities, and how to access devices (student registration requirements for example).
- **Learning Material Extraction:** An RFID reader (with mobile device of the learner) can read an RFID tag from the training manual with the Instructor to enable access to the training material information.
- **Smart Conferences:** students in workshops and conferences can capture further education resources instantaneously. For example, a tag can be attached to posters in a poster session. When the mobile reader reads it, further information will be presented. Similar scenarios can occur in a library, fairs, reading rooms etc.
- **Group Collaboration and Identification.** For matching styles of learners.

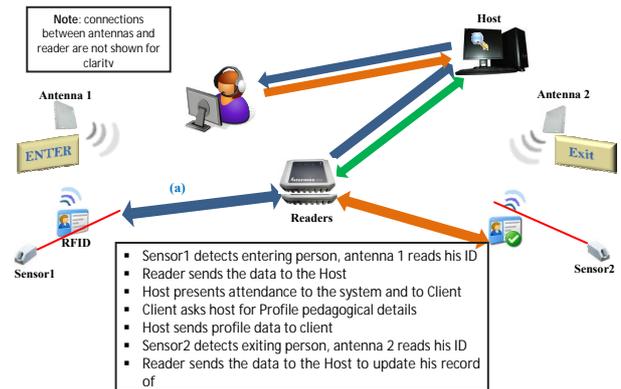


Figure 2. RFID Scenario in a Smart Space

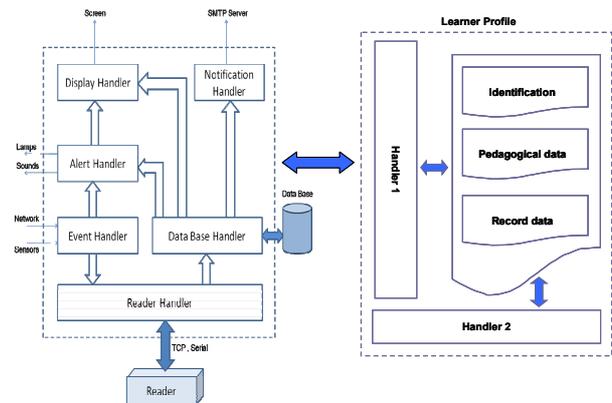


Figure 3. Profile Interaction with RFID reader

IV. INVESTIGATING BEST REPRESENTATION OF PROFILE INFORMATION

Figure 3 illustrates an interaction scenario between an RFID Reader and an RFID Profile. The representation mechanism of the profile information is crucial to achieve maximum interoperability between educational and e-learning systems for different scenarios. If the portable learner profile in card can act for this integration (with proper representation), then this method is encouraged more than storing information in a centralized database. Furthermore, [9] demonstrated some problems happening in distributed user-profile management. Our work is expected to provide a standard schema representation for the profile in a portable and interoperable format obeying recent standards and technological achievements.

V. HARDWARE REQUIREMENTS

A. Placement and Orientation of the Antennas

To ensure reliability, all users and objects concerned by the application should be discovered and their IDs, profiles, and data should be correctly read. For this purpose, the following are required:

- Determining the radiation diagram for each antenna.
- Optimizing the positions of this antenna with respect to their radiation diagrams

- Optimizing the orientations of the antennas to cover the entire region through which users or objects go.
- Optimizing on-line and in real-time the system with respect to position and orientation (moving tags in all directions and positions in 3D-space while reading by the reader)

B. Optimizing the System with Respect to Obstacles

The major challenge is the human body, which contains 60 to 70% water. This liquid hugely refrains the backscattering of high, ultra high frequency and micro-waves, which is the way of reading tags. If one tag is put in the trouser (pant) pocket, the hip or the legs present an obstacle impenetrable by the wave. A solution to this problem is proposed in [2].

C. Reducing the Cost of the Sensor

This is while maintaining or improving sensor performance (coverage, sensitivity, response time, use of power)

VI. EXPERIMENTAL DESIGN AND PROCEDURE

In order to implement the above-mentioned scenarios based on RF Identification of Learning Profiles, we find that the following experiment settings are needed:

RFID system for smart two-door Classroom: Figure 2 illustrates the principle of the smart classroom in a scenario. Each reader is connected to antennas. Each antenna is placed in an optimized way to cover a reading zone where people or objects are very likely or imperatively go through. To avoid saturating the buffer of the readers and to optimize energy consumption, we insert sensors that are activated to signalize that a person or an object is entering or exiting the reading zone. The above Figure 1 shows the case where the room has two doors; one is reserved for entry and the other for exit.

Making a conventional classroom smart: To make an existing classroom smart, no infrastructural modifications are required. For this purpose, we suggest an alternative to above where exit and entry are on the same side. The availability of WIFI routers in current classroom and its use in conjunction will be also investigated

One-door Smart Classroom: We suggest using only two antennas but to optimize their positions and orientations to capture all entering or leaving events. An example of this configuration is given in Figure 4.

Mobile reader for scanning: We suggest studying mobile readers in addition to the above paradigm [1] to scan the whole classroom and for learner usage.

Other Scenarios Implementation: When the above setting is complete and operational, other experiments will become easier to test such as automated attendance recording, training scenario, training material extraction, and smart posters.

Profile Access Scenarios: This experiment will provide input to a proof-of-concept as follows:

1. Testing recording to the profile
2. Testing retrieving a record from the profile
3. Given a learner schema, sample learning data (from local institution) will be filled and presented through a user-interface to a proposed instructional session

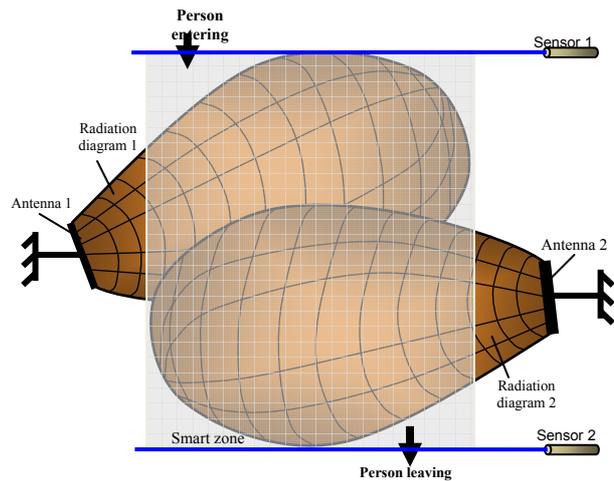


Figure 4. Two antennas are used to recognize students entering a smart space

4. An e-learning tool will be modified (or use one that has required feature) to modify the learner profile with a record
5. The same learning tool used in 4 can be used to retrieve similar data or different record for input.
6. Experiment results will be evaluated pedagogically as well.

VII. CONCLUSION

This paper proposed the use of RFID for learning scenarios. RFID devices can add another aspect for mobile learning by proving learner and learner data identification thus providing smart learning experiences. It serves as a personalization enabler for e-learning systems. It also facilitates interoperability if the learner card will be carried over to roam in difference learning environments. Furthermore, it can provide context and location-awareness services to learners. With these services, the debate of whether e-learning systems are replacing the traditional campus will be changed to having augmentation between the smart campus and e-learning systems each serving the other.

REFERENCES

- [1] Nokia RFID-enabled mobile phones [Online]. Available: <http://www.nokia.com>
- [2] Chetouane F. and H. Hamam H., "RFID lab for the Canadian University of Dubai: Overview & Technical Specifications", Nov. 2007.
- [3] Keskilammi M., L. Sydänheimo and M. Kivikoski (2003). Radio frequency technology for automated manufacturing and logistics control. Part 1: Passive RFID systems and the effects of antenna parameters on operational distance. *Int J Adv Manuf Technol*, 21, 769–774. (doi:10.1007/s00170-002-1392-1)
- [4] Penttilä K., M. Keskilammi, L. Sydänheimo and M. Kivikoski (2006). Radio frequency technology for automated manufacturing and logistics control. Part 2: RFID antenna utilisation in industrial applications. *Int J Adv Manuf Technol*, 31, 116–124. (doi:10.1007/s00170-005-0174-y)
- [5] Sydänheimo L., L. Ukkonen, and M. Kivikoski (2006). Effects of size and shape of metallic objects on performance of passive radio frequency identification. *Int J Adv Manuf Technol*, 30, 897–905. (doi:10.1007/s00170-005-0133-7)
- [6] Jongyoung L. and K. Naesoo (2006). Performance test tool for RFID middleware: Parameters, design, implementation, and fea-

tures. *In proceeding of IEEE ICACT*, Feb. 20-22, Gangwon-Do (Korea), 149-152.

- [7] Reid A.S. (2007). RFID smart cards. Is society smart enough to deal with smart cards? *Computer Law & Security Report*, 23, 53–61. ([doi:10.1016/j.clsr.2006.11.006](https://doi.org/10.1016/j.clsr.2006.11.006))
- [8] Rieback M.R., P.N.D. Simpson, B. Crispo, and A. S. Tanenbaum (2006). RFID malware: Design principles and examples. *Pervasive and Mobile Computing*, 2, 405–426. ([doi:10.1016/j.pmcj.2006.07.008](https://doi.org/10.1016/j.pmcj.2006.07.008))
- [9] Lora Aroyo et al, “Interoperability in Personalized Adaptive Learning,” Special Issue on Interoperability of Educational Systems, *Journal of Educational Technology & Society*, Vol. 9, 2006.

AUTHORS

M. S. Soliman is with the Math and Computer Department, Foundation Program of Qatar University, P.O. Box 2713, Doha, Qatar (e-mail: msoliman@qu.edu.qa).

S. Guizani is with the Math and Computer Department, Foundation Program of Qatar University, P.O. Box 2713, Doha, Qatar (e-mail: sguizani@qu.edu.qa).

Submitted November, 20, 2009. Published as resubmitted by the authors on December, 2, 2009.