RFID-Based Identification: A Measurement Study

Marina Buzzi, Marco Conti, and Enrico Gregori

IIT-CNR,
via Moruzzi 1, I-56124 Pisa, Italy
{marina.buzzi,marco.conti,enrico.gregori}@iit.cnr.it

Abstract. In this paper we investigate the feasibility of using UHF RFID as a tool for identifying individuals. We first developed a demo application for greeting conference speakers by incorporating a passive UHF tag into a user badge. Next, based on participant feedback we carried out additional tests to gauge the reliability of the user identification. Results of our experiments are very encouraging. If certain technical precautions are kept in mind, UHF RFID has a high percentage of success and is more widely accepted in the user community than is active sensor technology.

Keywords: UHF RFID, identification, measurement, safety.

1 Introduction

In the late 1990s, the Internet revolutionized ICT and our entire society. The Web has changed the world profoundly, introducing millions of users to the network, with great economic, social and cultural impact. Today ubiquitous computing promises to revolutionize our society even further, providing "last mile" technology to bring applications and services to everyone.

In 1991 Mark Weiser, the father of ubiquitous computing wrote: "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it." [16]. In his prophetic vision, Weiser imagines that computers vanish into the background, technology is embedded in the environment and user interaction becomes simple and natural. The future is thus "disappearing computing" and "calm technology", no effort is required of users to use the technology [16]. According this philosophy, RFID technology (Radio-frequency identification) could be a valuable tool for building context and position-aware services if it allows people to behave naturally without imposing constraints (i.e. requiring a short read distance or the use of active tags). In this paper we describe an experimental study that investigates the feasibility of UHF RFID as a tool for identifying individuals.

As ubiquitous computing becomes increasingly common, new applications begin to permeate every aspect of daily life. Today RFID and sensor technologies embedded in everyday objects are used to sense environmental data, convey information and enable services. Specifically Radio-frequency identification is a technology for

F. Granelli et al. (Eds.): MOBILIGHT 2009, LNICST 13, pp. 220–229, 2009.

automatic identification of objects, persons and animals, using radio waves. It consists of two components: readers and tags. Tags store information (usually a unique identifier) that can be retrieved by readers. This kind of distributed information transmitted via wireless networks and elaborated from resource-rich devices, makes services available everywhere and under any conditions. Thus RFID has become a key technology for enabling “object-based” services.

Tags can be passive, active (battery-powered) or semi-active. Passive tags transmit their unique id by using the energy induced by the reader. Passive tags are especially convenient since they are small, cheap and do not pose maintenance problems, i.e. have a potentially infinite life. Tags and readers operate in four frequency ranges, which are usually applied in different fields ([17]):

- Low-frequency (LF), i.e. 125/134 kHz and 140/148.5 kHz, used for tracking animals, human implants (to store personal medical info), and electronic keys (to access hotel rooms, controlled areas);
- High-frequency (HF) 13.56 MHz which follows two standard specifications with different aims:
    - ISO 15693, which optimizes performance of tag reading, is used for inventory and tracking of food, goods, etc. and also for automating libraries;
    - ISO 14443 which supports high levels of security, for e-passports, non-contact payments, credit cards, e-tickets, etc.
- Ultra-high frequency (UHF) 915 MHz (US) and 868 MHz (Europe), applied in logistics and inventory systems;
- 2.4 GHz and higher (Microwave tags) are commonly used for mobility and interports.

Radio-frequency identification may be a valuable tool for building new ubiquitous applications, if it allows people to behave naturally without imposing any awkward constraints. This paper investigates the feasibility of using UHF RFID technology for identification of people by inserting a passive tag in a badge, creating a kind of "intelligent badge”. As previously discussed we aim to remove user constraints, and thus chose to focus on ultra-high frequency, which allows greater read distance of tags compared to high frequency (HF). Hereafter, we only refer to UHF RFID systems and passive tags.

RFID passive tags include an integrated circuit (for storing information, modulating/demodulating a signal) and one or more antennas, for receiving and transmitting the signal (from/to the RFID reader) [17]. Each tag comes with a unique id stored in its memory (usually a 24-character code). New generation tags are programmable, which means it is possible via SW to write product codes and other information in their memories. Therefore, RFID tags form a kind of distributed memory surrounding persons and environments, which may be advantageously used in a great number of new applications [9]. Considering that tag memory is constantly increasing, new and powerful applications will be designed in the near future.

The reader utilizes one or more antennas (linearly or circularly polarized). Depending on the frequency used and antenna features (i.e. size, polarization) the read distance of tags varies from one-half to seven meters. The availability in the market of different reader families (small, medium, large) offers a vast range of choices.

Readers integrated in handheld devices are interesting due to their effectiveness and simple use. Obviously an antenna integrated in a handheld device is small so the read distance is reduced as well. For example, at the moment the maximum declared read range of the Psion palm device, which integrates an RFID reader, is 80 cm or 1.50 m depending on the frequency (868 or 915 MHz) [12].

2 Issues in UHF RFID Technology

When applying RFID technology to a real case, reliability of the reading is crucial. RFID data are large-volume streams characterized by inaccuracy; duplicate, missed and ghost reads due to interference or temporary malfunction of some components make RFID data noisy and unreliable [14]. Thus reliable SW for data filtering and aggregation is crucial for the successful introduction of RFID technology.

Different frequencies can present different challenges. In the following we only consider problems of UHF RFID technology.

Tag reading may be challenging depending on features of tagged items: i.e. size, composition of materials, packaging, and tag placement. Three issues affect the reading: RF reflection, shadowing and absorption [15]:

- Metal reflects UHF; however an appropriate insulation separating the tag from the surface can improve reading;
- Shadowing occurs when several tags are placed very close and their antennas mask each other, by decreasing the read rate;
- Liquids (such as water) absorb RF and hinder tag reading. Since the human body is mostly composed of water and thus absorbs RF, this means that a person placed between the reader antenna and the tagged item prevents the reading (i.e. breaks RF propagation).

Furthermore, tag placement (i.e. its physical position in space) is crucial: in the worst case, if antenna and tag are perpendicular, the reading may fail. Lastly, motion (handheld readers or tagged items) facilitates tag reading [15].

3 Examples of Presence-Aware Applications

In the following we briefly outline three possible uses of RFID-based identification, conceived for our work environment. An extensive analysis of RFID state-of-art which also includes several examples of applications and future developments to enable pervasive computing is addressed by [13].

Public Safety

One possible application of the intelligent badge is in the field of public safety, such as in the case of fire. In our Research Area there are two very large 3-floor buildings containing offices with one, two or three desks. There are only a few labs with four or more people. Every building has numerous exits every 100 m. Thus, in case of evacuation people should be evenly distributed throughout the area. The only crowded place might be the 300-seat conference room located on the ground floor, with three emergency exits opening directly onto the lawn.

At entry/exit points of the building all persons would be identified by their intelligent badge and the relative data inserted in a database. In the event of evacuation and reunion at a meeting point (1 for each institute), a portable reader (connected to a wireless network) belonging to the security guard receives the list of all present in the institute. As individuals arrive at the meeting point they are crossed off the list. Anyone missing is thus quickly identified without resorting to a roll-call.

Speaker Introduction

Another use of the intelligent badge and vocal synthesis (as shown in the following in our SW prototype) could be automatic speaker presentations in conference sessions, to speed up the process. A few sentences could be loaded by the speaker (describing his/her activities) via web. When speakers wear the intelligent badge, the session chair is aware of their presence without needing to ask if all speakers are present, who they are, etc. Furthermore, if one speaker arrives late during the session, the chair knows exactly who is entering the room, identifying him visually and leading to greater flexibility in last-minute scheduling.

When the speaker is approaching the speech area, the reader gets the tag id and, if the person is the next speaker (the time schedule of talks is checked via SW) his/her description starts automatically after a few seconds (or alternatively can be activated by one click).

Traffic Gate Control

The intelligent badge could be used to control access to the CNR area, automatically opening/closing a traffic gate.

Each worker wears an intelligent badge. The UHF reader reads the unique id and opens the traffic gate. This would have an advantage over inserting the badge into the magnetic band reader (as currently used), by activating the bar from a configurable distance, for instance inside a car (in case of rain) or in a pocket, wallet or bag, if the user is on a bike or walking, thus shortening access time.

Compared to using an HF RFID reader which requires the badge to be a short distance away (5-10 cm), UHF technology allows greater reading distance, with all its related advantages.

4 Study Start-Up

In order to understand how introducing RFID is perceived, we set up a demo application to show the potential of this technology, then stimulated a discussion about designing new ubiquitous applications. Previous studies showed that systems are more successful when associated with a wide range of organizational issues dealt with throughout the development process and ensuring that members of the user community are actively involved [2].

We created a simple application for greeting conference speakers and committee members. Inside additional participant badges we inserted the Alien 9540 passive tags, which have a bi-directional circle-polarized antenna. The application interacts with the Alien ALR-8800 Enterprise RFID Reader (http:// www. alientechnology. com/), which is EPC Gen 2 and ETSI-Compliant (EN 302-08 and EN 300-220 compliant) and operates at 915 MHz. The Alien evaluation kit includes two circularly polarized antennas (called in the following antenna 0 and antenna 1) which are connected to the reader via cables. In this configuration the read distance covers up to 2 meters.

The application is developed by using the Alien Java SDK (which interfaces the ALR-8800 RFID Reader) and relies on open source SW:

- Java SPEECH APIs which relies on the Java voice synthesizer FreeTTS (http://freetts.sourceforge.net/);
- JDBC APIs which interacts with the MySQL DB running on a Linux server is used for storage.

In order to simplify deployment, the application was split into two parts:

- a java code for checking the RFID reader and for writing tag information in a mySQL database; for the demo the database was populated with 30 entries;
- a graphical UI which is actually a web page including details about observed tags, which reads entries from the database. The interface is built in PHP and refreshes every 3 seconds.

The reader runs in autonomous mode and, when it sees tags, it sends the Java application a table containing all tag identifiers and other associated information. The reader was set up in inventory command mode for multiple contemporary readings. The reading time was set up at 1 second.

The two antennas were located 4 m apart on the same side of a wall. Access to the demo room consisted of a single door, thus 2 antennas were sufficient to perceive entering and exiting individuals. When there is a transition from antenna 0 to 1 (i.e. the reader first sees the tag_i with antenna 0 and then with antenna 1) the voice synthesizer announces "Hello $Name_i$ $Surname_i$" of the person wearing the badge containing the tag_i. This info was previously stored in the db with other data (role, organization, email). Vice versa, when a person leaves the room the SW announces the appropriate phrase, i.e. "Bye bye $Name_i$". Simultaneously to vocal synthesis, the Name, Surname and Role of individuals were shown in a web interface (Fig. 1).

By performing the demo we learned a great deal. First, our SW suffered from a lack of synchronization between voice (i.e. greetings) and the text shown in the web user interface since speech consisting of several words is intrinsically sequential while their visualization is parallel. If a group of attendees came close to the reader antenna, there was a delay in the announcement of their names since the speaking queue was longer. This could be annoying.

We also encountered one reading problem (no tags were perceived) when a person carried a cell phone next to the RFID tag (i.e. in a shirt pocket). Holding the tagged badge in one's hand facilitated the reading but a feeling of unreliability was perceived. As remarked in [7] trustiness of service depends on the reliability and robustness of the application and its ability to manage any event that might occur in a production environment. In addition, one individual was not recognized in a group crossing the room, possibly due to RF emission broken by the person's body, since the only two available antennas were located on the same side of the wall in order to track the subject's entry/exit. Thus position as well as number of antennas is crucial for successful reading.

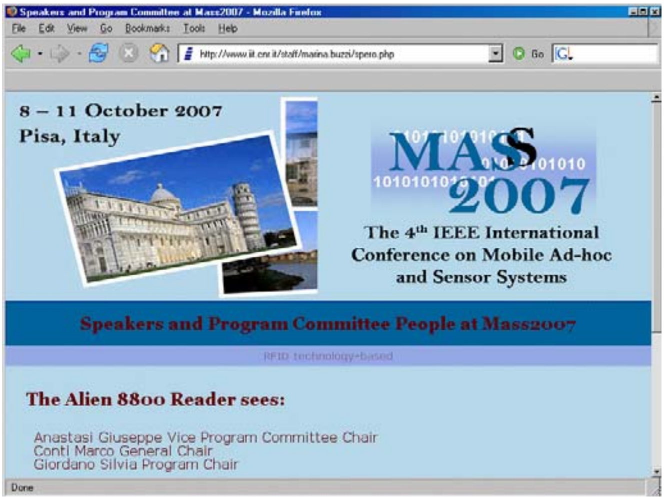

Fig. 1. A screenshot of the web UI shown in the Demo

5 Measurements

The demo was designed to stimulate user curiosity, encourage discussion, gather new ideas, and verify acceptance of automating some basic organizational processes and services. After the demo we decided to perform some tests to verify the amplitude of the abovementioned problems. At the beginning we performed a pre-test to verify RF adsorption by the human body and potential interference with handheld devices and in general with devices which produce electro-magnetic fields.

We verify that RF is absorbed independently of body size. A hand covering the entire badge (and thus the tag) was enough to make the reading impossible. Instead, the reading was successful if one of the tag antennas remained uncovered.

Then we performed a test with a G17 Sharp cell phone. Interference when the cell phone was ringing or a person was talking was not observed, but the reading was impossible if the phone covered both antennas of the tag. Partial covering of one antenna did not impact reading reliability. Furthermore, placing the phone behind the tag (from the keyboard side) with the antenna in front hid the tag from the reader.

In order to verify reliability of the tag reading, we then carried out two tests with 10 colleagues wearing the "intelligent badge". We also split the group into two subsets of five persons each to determine whether any variation occurs according to the sample size.

Pilot Test and Set-Up

We arranged the 2 antennas of the Alien reader in different positions on the walls of our Institute building, to verify whether and how tag-reading percentage varies in different configurations. Antennas 0 and antenna 1 have the same features (i.e. size, polarization, etc.) and configurations (RF attenuation, etc.).

We registered tag read details (i.e. tag id, antenna, data, time) in a file and then processed collected data, calculating the average of readings for each tag. Specifically, single percentages were calculated for each tag as $N_i/20$ values where N_i is the number of readings for each tag_i during 20 passages between antennas.

Since the reading was set at 1 second, a slow subject may be identified more than once during each passage. The total read percentage, shown in Table 1 is the mean of read percentages of each tag, for each experiment.

A pilot test was carried out before starting the experiments. Analyzing the data we found that not all tags performed in the same way. Specifically, one tag was read only once in this test. Thus during setup we checked all tags involved in the tests before starting data collection and defective tags were discarded. In the following our data refers to reliable tags; however on a large scale defective tags might be found, which would affect the reading.

Tag size also influences the success of a reading. We used squiggle tags, which are small and thin. Other tags may present different reading percentages. Last, as already mentioned, movements and positioning of participants may also cause results to vary.

Lateral Antennas

In this experiment, the two antennas were located on two parallel walls 2 m apart, at 1.25 m from the ground. Then we instructed the groups of subjects to walk between the reader antennas 10 times in one direction (until exiting the antennas' range of action) and 10 times in the opposite direction, for a total of 20 passages. In order to simulate behavior in case of building evacuation, we asked people to walk rapidly, talking and trying to remain as close to each other as possible. Table 1 summarizes results.

By using two antennas, results showed 100% identification of a 5-member as well as the 10-member groups. Identification with only one antenna decreased to 85.25% for the 10-person group and to 86.5% for the 5-person group, depending on antenna position (right or left) and the location and movement of participants.

Orientation of tags may lead to a missed reading when the badge is perpendicular to the antennas (parallel to RF flow). In addition, unless people are in single file, one body may block another and absorb the radio emission flow. The number of readings varies depending on the physical distribution of group components: people in the external lines are read more frequently than subjects on the inside.

As previously mentioned, a slow individual might be identified more than once during each passage. The maximum number of readings for a single tag (by both antennas) was 56 while the minimum was 27. With only one antenna, the maximum number of readings for a single tag was 37 (or 28) while the minimum was 8 (or 7) for antenna 0 (for antenna 1).

Frontal, Inclined Antennas

In this experiment the two antennas were placed on both sides of a wall over the door at a height of 2.10 m, and inclined at a 30^o angle from the wall (60^o angle from the floor) in order to "see" people entering the door from the front. In this case the tag was parallel to the antennas (i.e. perpendicular to RF flow). In this set-up the reliability of identification was 100% for both groups (Table1).

With only one antenna identification decreased to 89.25% for the 10-member group and to 95% for the 5-person group depending on antenna position and the location and movement of participants (Table 1). Probably to permit easy walking, each individual was physically somewhat distant from the next in line, so antenna coverage increased compared to the previous test.

The maximum number of readings for a single tag was 64 and the minimum was 23 for two antennas. With only one antenna, the maximum number of readings for a single tag was 37 (or 28) while the minimum was 8 (or 7) for antenna 0 (or antenna 1).

Table 1. Percentage of identification of two groups (of 5 or 10 persons) with different locations and number of antennas

Persons	1 antenna h. 1.25 m. (lateral)	2 parallel antennas at 2 m.; h. 1.25 (lateral)	1 antenna h. 2.10 m. (frontal, inclined)	2 antennas h. 2.10 m. (frontal, inclined)
5	86.5%	100%	95%	100%
10	85.25%	100%	89.25%	100%

6 Discussion

Concerning tag reading, we believe that in order to obtain a reliable degree of identification, four antennas should be placed at every gate. Two or more antennas may offer a good degree of identification, however a 100% reading is not always guaranteed due to several factors: 1) cooperation of people is essential for allowing tag reading 2) position of tag in relation to the antenna is unpredictable 4) absorption or reflection is possible 5) rarely, a tag may be defective. With only one antenna the percentage of identification greatly decreases. Results of our experiments showed the technical feasibility of UHF-based identification if there is user collaboration. Thus user acceptance is a key factor in the success of presence-awareness services.

By simplifying processes and increasing efficiency, ubiquitous computing enables new ways of working but user acceptance plays a critical role in widespread adoption of ubiquitous applications. The perception of losing both privacy and control of the RFID environment is a great concern [4]. Although security and privacy issues are widely addressed in numerous studies and surveys [6], [10], [5], [3], [11], classic security data techniques such as user authentication, symmetric and asymmetric ciphering algorithms, public key infrastructure combined with ad hoc techniques such as killing, sleeping or blocking tags, tag password, tag pseudonyms, or the proxy approach are not enough to disperse the black cloud that surrounds the use of RFID systems. Thus, security and privacy issues should be carefully considered and included in the design of new pervasive services.

In our application, RFID-based identification may pose a serious privacy problem since including tags in worker badges could allow people within the Institute to be tracked without user knowledge (if readers were scattered throughout the Institute area). Several colleagues have expressed doubts about this.

Another common concern was related to the safety level of exposure to RF emitted from antennas, for human beings. It is remarkable that people are not equally afraid of using their cell phones or computers! As stated in the reader manual, there is a safe distance (at least 20 cm) which should be maintained by workers in daily contact with antennas. In our empirical experience we noticed that women were more sensitive to this problem. Two pregnant women at our Institute were extremely worried about having contact with RF. To our knowledge the very few studies in this field have not proved any health damage in the short term but we are unable to exclude it over time since reliable results should include very long-range data and observations (at least one or two decades). In the context of our application, exposure to RF is sporadic, limited to crossing the traffic gate of the Institute, and thus is not a problem.

However, in real applications, improved efficiency may overcome user fear. Kourouthanassis et al. by implementing and testing a prototypal application with users in a retail context, verified enhanced user experience in supermarket shopping [8]. Furthermore, Konomi et al. [7] observed that after an initial skepticism the introduction of smart shelves in a shoe shop gained wide acceptance from sale staff, due to improved efficiency and work simplification. In our experience, after people's initial fear of being tracked and having their privacy invaded, we observed a general interest in this technology as a way to simplify tasks and automate work. For instance, its potential for tracking objects, such as inventory and document workflow, appears to be quite useful and interesting.

7 Conclusion

This paper investigates the feasibility of using UHF RFID readers and passive tags for identification purposes. We performed this experimental study in order to better understand the limits, costs and performance of UHF RFID as a tool for identifying individuals.

First, we developed a simple application for greeting speakers at a conference. We then carried out several tests to verify the feasibility of using UHF RFID technology in "intelligent" badges in terms of percentage of successful readings. Results showed the technical feasibility of this approach, as long as the user collaborates. Despite its simplicity, and keeping in mind certain technical precautions, UHF RFID has a high percentage of success and is more widely accepted in the user community than active sensor technology.

In conclusion, UHF RFID is technically suitable for creating a range of useful new applications beyond the usual fields of logistics and inventory; however privacy and security issues should be carefully considered even in the design phase, to encourage general acceptance and ensure user collaboration.

References

1. Alien Technology: Tag Feng Shui. A Practical Guide to Selecting and Applying RFID Tags, `http://www.alientechnology.com/docs/WP_Alien_Tag.pdf`
2. Doherty, N.F., King, M., Al-Mushayt, O.: The impact of inadequacies in the treatment of organizational issues on information systems development projects. In: International Journal of Information & Management, vol. 41, pp. 49–62. Elsevier, Amsterdam (2003)

3. Dritsas, S., Gritzalis, D., Lambrinoudakis, C.: Protecting privacy and anonymity in pervasive computing: trends and perspectives. Telematics and Informatics Journal 23(3), 196–210 (2006)
4. Günther, O., Spiekermann, S.: RFID: tagging the world: RFID and the perception of control: the consumer's view. Communications of the ACM 48(9), 73–76 (2005)
5. Juels, A.: RFID Security and privacy: a research survey. IEEE Journal on Selected Areas in Communications 24(2), 381–394 (2006)
6. Hyangjin, L., Jeeyeon, K.: Privacy threats and issues in mobile RFID. In: First International Conference on Availability, Reliability and Security, pp. 510–514 (2006)
7. Konomi, S., Roussos, G.: Ubiquitous computing in the real world: lessons learnt from large scale RFID deployments. Personal and Ubiquitous Computing 11(7), 507–521 (2007)
8. Kourouthanassis, P.E., Giaglis, G.M., Vrechopoulos, A.P.: Enhancing user experience through pervasive information systems: The case of pervasive retailing. International Journal of Information Management 27, 319–335 (2007)
9. Mamei, M., Quaglieri, R., Zambonelli, F.: Making tuple spaces physical with RFID tags. In: Proceedings of the 2006 ACM symposium on Applied computing, pp. 434–439. ACM Press, New York (2006)
10. Paar, C., Weimerskirch, A.: Embedded security in a pervasive world - Information Security Technical Report, vol. 12, pp. 155–161. Elsevier, Amsterdam (2007)
11. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez, J.M.: RFID Systems: A Survey on Security Threats and Proposed Solutions. In: Cuenca, P., Orozco-Barbosa, L. (eds.) PWC 2006. LNCS, vol. 4217, pp. 159–170. Springer, Heidelberg (2006)
12. Psion Teklogix. WorkAbout Pro Second Generation Hand-Held Computer, `http://www.psionteklogix.com/`
13. Roussos, G., Kostakos, V.: RFID in pervasive computing: State-of-the-art and outlook. Pervasive and Mobile Computing 5, 110–131 (2009)
14. Sheng, Q.Z., Li, X., Zeadally, S.: Enabling Next-Generation RFID Applications: Solutions and Challenges. Computer 41(9), 21–28 (2008)
15. Vega, V.: Common RFID Implementation Issues: 10 Considerations for Deployment, `http://www.alientechnology.com/blog/`
16. Weiser, M.D.: The Computer for the 21st Century. Scientific American Special Issue on Communications, Computers, and Networks, 66–75 (1991)
17. Wikipedia. Radio-frequency identification, `http://en.wikipedia.org/wiki/RFID`