3

Automatic Personal Identification System for Security in Critical Services: Two Case Studies Based on a Wireless Biometric Badge

Stefano Tennina[1], Luigi Pomante[2], Francesco Tarquini[2], Roberto Alesii[2], Fabio Graziosi[2], Fortunato Santucci[2] and Marco Di Renzo[3]
[1]*CISTER Research Unit, ISEP/IPP Rua Dr. António Bernardino de Almeida, Porto*
[2]*Dept. of Electrical and Information Engineering and Center of Excellence in Research DEWS, University of L'Aquila, Poggio di Roio, L'Aquila (AQ)*
[3]*Laboratory of Signals and Systems (L2S), CNRS - SUPELEC - Univ Paris-Sud 3 rue Joliot-Curie, Gif-sur-Yvette (Paris)*
[1]*Portugal*
[2]*Italy*
[3]*France*

1. Introduction

Due to the relevant innovations in the ICT domain, today, a lot of services is being provided with a self–service approach to an even more great number of people simplifying several tasks of everyday life (e.g., cash retrieval by ATM, remote-banking, etc.). The key aspect to fully enable such services and make them wide accepted by peopole is the possibility to reliably count on biometric identification mechanisms (Adeoye, 2010; BTAM, 2010; Elliott et al., 2007; Li & Zhang, 2010; Sonkamble et al., 2010). Some of them are already exploited in several real–life scenarios, like the Access Control–Border Management in Hong Kong or the Access Control–Restricted Area Access by Canadian Air Transport Authority (BTAM, 2010). However, some of such services could be very critical and so, their provisioning, should be managed very carefully in order to avoid the possibility of malicious operations. So, the best way to support the evolution of automatic services providing is to develop a system, also automatic, which is able to trust in a secure and flexible way the identity of people that need to access such services. Such a system should be of easy integration in several scenarios, especially with respect to existing infrastructures, and should be designed to respect all the relevant privacy issues while providing to the users all the feelings (about reliability, safety and usability) needed to make the system acceptable.
In such a context, this book chapter aims at presenting an automatic personal identification system developed by WEST Aquila (WESTAquila, 2010). The system, described in detail later, exploits the recent advances in the biometric and heterogeneous wireless networks fields to provide a true authentication platform supporting several services encompassing physical access (e.g., to restricted areas or vehicles) as well as logical access (e.g., to personal services like e-banking) management. This is realized by maintaining a full control over critical data (biometric) that are used for the authentication. In fact, the main component of the system is

a novel biometric badge, i.e., a smartcard equipped with a biometric reader (i.e., a fingerprint reader) and a short–medium range wireless transceiver which allow the identification of both the card and the card owner. In other words, it constitutes a system–on–badge: when required, the card owner is identified through an on–system biometric matching and only the result of such a matching is sent (appropriately ciphered) through the wireless interface towards the rest of the system. Therefore, personal biometric data is always under the full control of its owner, leading to high levels of security and privacy protection.
The intended content of this chapter will be to illustrate the badge as a biometric system and its usage in two case studies: (i) physical access of authorized people in a restricted area, which involves also physical positioning of the badge owner and (ii) logical access of authorized people in an e-banking–like scenario.

2. System architecture description

The proposed system is composed by a set of elements (Fig. 1) enabling high level of flexibility and reliability, needed to make this proposal as a reference in the field of personal automatic identification systems, where particular emphasis is on aspects like robustness, ease–of–use and privacy.

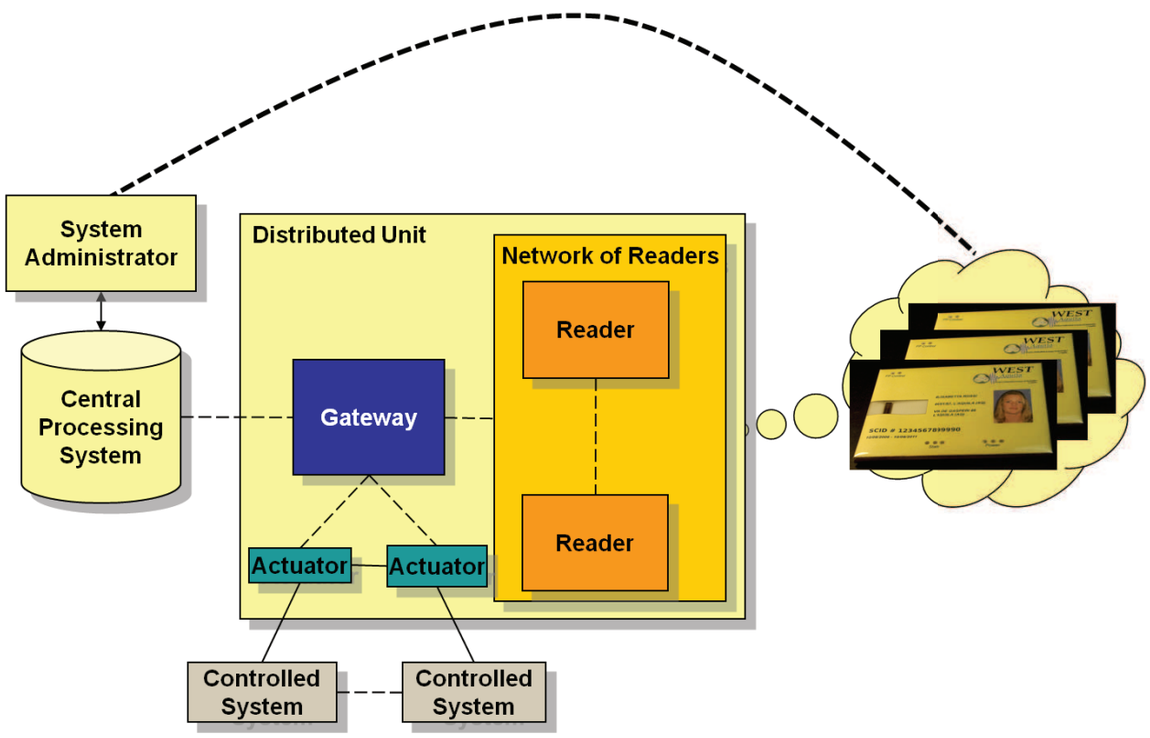


Fig. 1. Logical System Architecture

2.1 Biometric Badge (BB)

The key point of the proposed system is our embedded biometric badge (Fig. 2), which is a "system–on–badge" performing four main tasks: (i) enable the localization of its owner using distributed positioning techniques, (ii) scan and verify fingerprints of people, (iii) check if an user is the badge's owner based on fingerprint matching, and (iv) send related outcomes

wirelessly to the rest of the system (e.g., the DU which interconnects the badge to the rest of the infrastructure), without the need to transmit the owners' biometric data over the wireless medium (so, in a secure way from the point of view of transmitting critical data of the users).

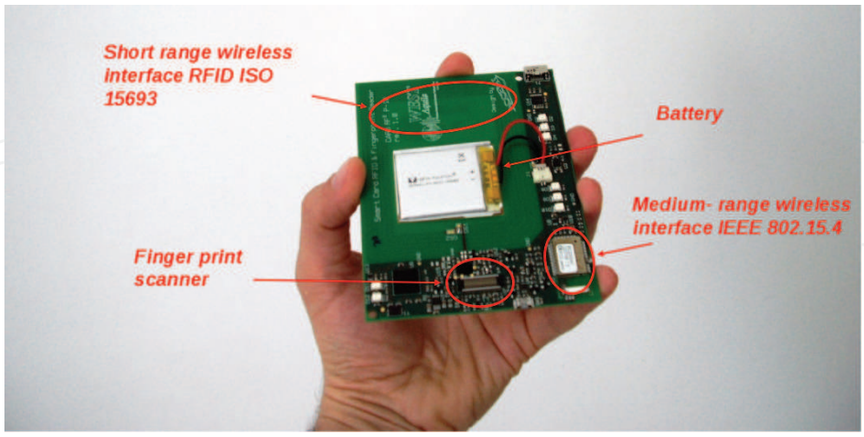


Fig. 2. WEST Aquila's Biometric Badge – components

The badge is equipped with:

- the Texas Instruments' SoC CC2430 (TI, 2009), which embeds a 8051 micro controller and a CC2420 radio transceiver, compliant with the IEEE 802.15.4 (IEEE, 2006) standard. It is used for wireless medium-range communications, as well as localization operations;
- a fingerprint sensor reader with its embedded "companion chip" provided by UPEK (UPEK, 2009). This chip is the key element for handling biometric data: it allows to authenticate people based on fingerprint information, as well as store data in a memory protected even from physical external attacks. Moreover, only this chip and the gateway are aware on how to decode the messages they send to each other;
- a RFID tag based on the ISO15693 standard and its companion chip provided by Montalbano Technology (Montalbano, 2009), which allow the microcontroller to get access to data stored in the tag;
- a rechargeable battery, its driver to monitor the charge status, and a user interface with 8 leds and a push-button.

Such features allow the badge to support a full range of applications (Fig. 3), mainly due to the embedded fingerprint reader enabling both civil and military use of such a technology in a secure and safe way.

2.2 Distributed Unit (DU)

Every DU is logically constituted by a "Gateway" (GW), one or more "Readers" (RDs) and one or more "Actuators" (ATs) communicating one another using wireless or wired technologies. The whole system can rely on several DUs, networked through secure communications with a Central Processing Station (CPS) and related controlled systems (Fig. 1). Each DU maintains synchronization of data with the central system and allows secure communications among the system components.

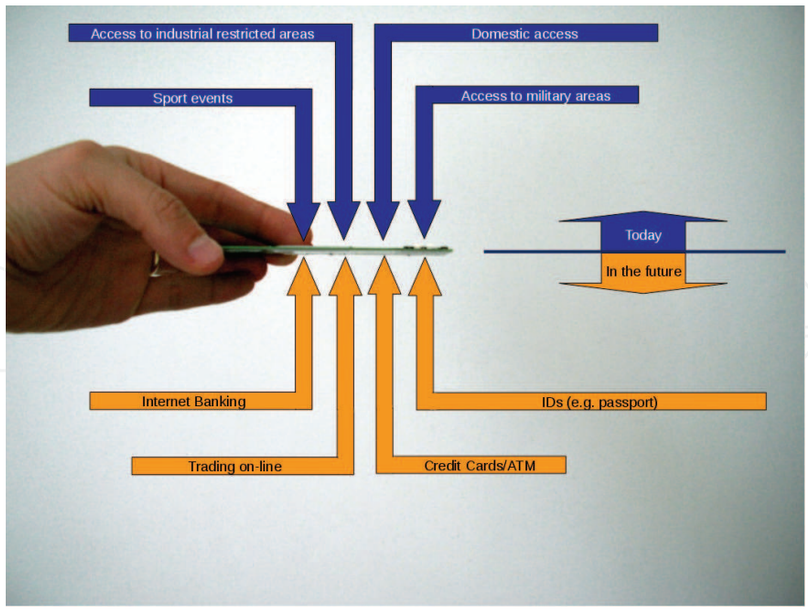


Fig. 3. WEST Aquila's Biometric Badge – features

2.3 Gateway (GW)

The Gateway is the central element of each DU. It communicates in a secure way with the RDs, with the ATs and back with the Central Processing Station (CPS). Its main function is to provide an interface between the BBs and the CPS, both upwards and downwards. In the upwards flow, the GW collects data from BBs through its associated RDs, interprets the information contained within each packet and sends it to the CPS. In the downwards flow, the GW receives instructions from the CPS and controls accordingly the ATs to grant or deny the access to the BB.

2.4 Reader (RD)

The Reader is the element for interfacing the DU with the BBs. Its role is to communicate wirelessly with the BBs, and it uses two mechanisms: the IEEE 802.15.4 communication standard and a proximity–based RFID technology. As a logical component of the system, it is not allowed to locally decode the data, but it simply forwards it towards the GW over a secure communication channel. The communication between the RD and the GW can be either wired or wireless. In the latter case, it can be direct, when they are in the communication range of each other, or indirect, i.e., multi-hop through intermediate RDs. When it is wireless and indirect, then the RDs constitutes a network of readers (NRD), organized into a ZigBee Cluster Tree (ZigBee, 2008), (Koubâa et. al, 2008).

2.5 Actuator (AT)

The Actuator is a device in direct contact with the Controlled System (Fig. 1) and it constitutes the interface with the GW so that the operations needed to provide the requested services to the BB owner are executed, when he/she has passed the authentication process, or the safety procedures when the authentication fails are applied. Similarly to the NRD, multiple ATs might form a multi–hop wireless network (NAT) to reach the GW.

2.6 Central Processing System (CPS)

The Central Processing System contains all data related to the whole system configuration. This implies that it stores and handles all the data related to the UDs and the BBs that have grants with the different UDs, as well as it handles the services that BB's owners can use when they request for them after a successful authentication. CPS communicates in a secure way with UDs and it is the interface with "System Administrator" (SA). The SA is in charge of two main tasks: (i) deliver the BBs to the people having rights of owning one of them and (ii) add and update in the CPS all data related to the system configuration, i.e., the association between the BB's ID and the services to which it can grant the access to its owner.
Table 1 summarizes the acronyms used in this book chapter.

Acronym	Meaning
AT	Actuator
BB	Biometric Badge
CPS	Central Processing Unit
DU	Distributed Unit
FP	Fingerprint scanner/sensor
GW	Gateway
NAT	Network of Actuators
NRD	Network of Readers
RD	Reader
RFID	Radio Frequency Identification
RSSI	Received Signal Strength Indicator
SA	System Administrator
SoC	System-on-Chip
SW	The application module running on the GW for communicating with the companion chip on the BB
uC	Micro Controller

Table 1. Acronyms

2.7 System security framework

It is of paramount importance to clearly state that the security of the system is based on a novel framework of network security built on top of the framework provided by UPEK (UPEK, 2009) for its chips.
The "companion chip" is embedded in the fingerprint reader on board of each badge and is the element able to handle all the biometric aspects. When the authentication process is running, this chip is in communication with the GW over a wireless secure channel, where data travels ciphered by that chip. On the GW a UPEK–made application runs: it is the only component in the whole system able to decode these messages. This leads to an interesting aspect of the system in terms of security: the microcontroller on board of the badge is definitely not able to communicate with the companion chip. It can only switch it on or off or ask the GW to activate the procedures. In other words, the biometric part is usable if and only if the proposed system is able to establish a secure connection between the companion chip on the badge and the application running on the GW (Fig. 4). The security of this communication is granted by the fact that it is ciphered using a symmetric key based mechanism. These keys are unique for each badge and provided during the so called "key provisioning" performed

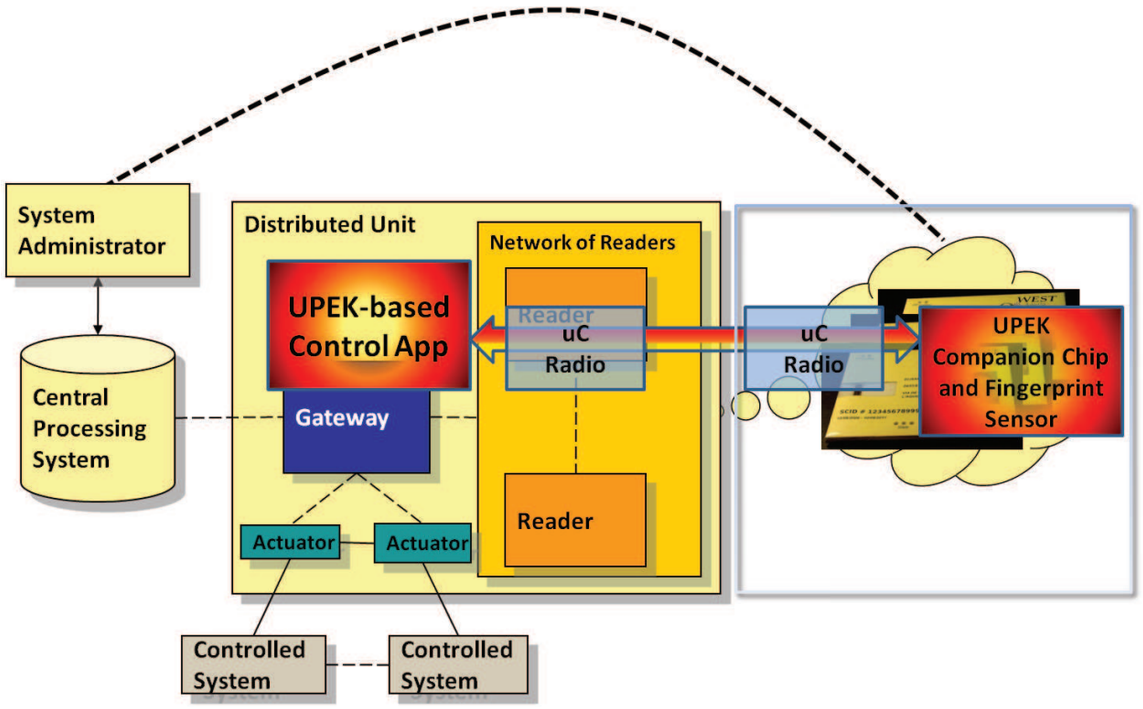


Fig. 4. Secure connection for biometric operations

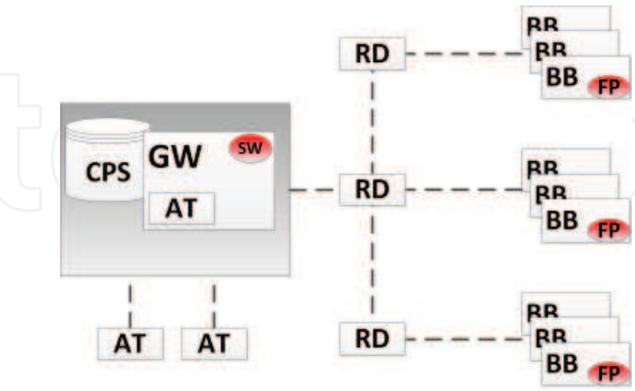
when the badge is registered into the system for the first time. They are stored both in the gateway and in the "secure memory" of the companion chip. This memory is designed by UPEK to resist also to HW attacks and contains the fingerprints template. Furthermore, the communication is ciphered using a random component that modifies the content of the message so that its eventual sniffing doesn't provide useful information. The intermediate software and hardware elements between the companion chip and the application running on the GW during the authentication process simply act as packets' forwarders.

Since the BB is also equipped with RFID communication capabilities, there is the possibility to introduce another level of system security, granted by a novel mechanism we called "ring check". When the BB is really close to a RD, the RFID technology is activated. Then, RD writes in the BB's tag memory a ciphered code to allow the BB to recognize it as a qualified reader. The uC on the badge gets this code and checks its consistency to identify if it has not been altered. If it recognizes it, then on the BB side there is a confidence to be communicating with a verified reader. Then BB builds a packet with a "reader ok" status field set and that code, then sends this message to the GW, using the IEEE 802.15.4 transceiver. By this way, the BB can authenticate the system with which it is currently communicating and the system can check if the BB is not corrupted, by checking the integrity of the code returned back to it. In other words, the system checks if the RFID and IEEE 802.15.4 transceivers and related storage areas are both working.

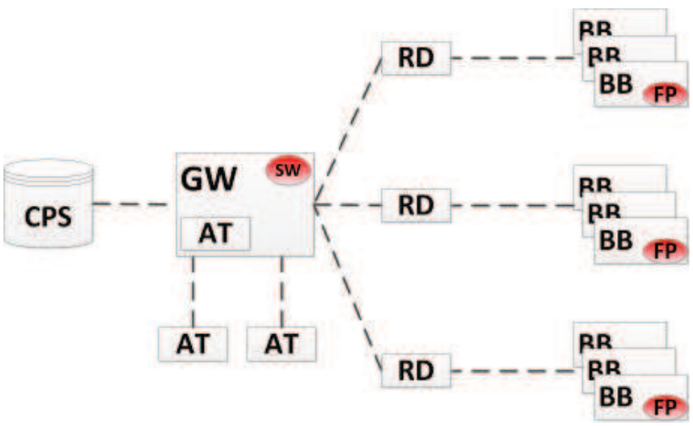
2.8 System configurations

Starting from the logical architecture shown in Fig. 1, it is possible to derive several physical configurations that could be applied depending on the different needs. In particular, based on the possibilities offered by the allocation of the different components of the DU and the CPS onto a single HW or multiple communicating devices, several combinations of alternative

configurations can be identified. As an example, Fig. 5 shows 2 different scenarios. The red elements, FP and SW, represent the components dedicated to manage the biometrics operations. i.e., SW is the only component able to decode and manage information about the result of biometric verification coming from FP.



(a)



(b)

Fig. 5. Two different configurations

Fig. 5a refers to a scenario where CPS and GW are allocated on a single physical machine. A wireless interface is used to communicate with the RD units, organized into a network of readers. Fig. 5b shows a configuration where the system is fully distributed, i.e., CPS, GW and RDs are mapped onto different machines. The communication between these components might be based on IP protocols, like over Internet.
Although several other combinations are possible, these two scenarios are our reference to the case studies described in the following sections.

3. Case Study 1 – Physical access to a critical area

Let us assume that a SA has released a number of BBs to a number of authorized people by means of an enrollment procedure, then each one of them will have an enabled BB storing their own fingerprint, while the central system will be aware of the basic access rights of BB and related persons.

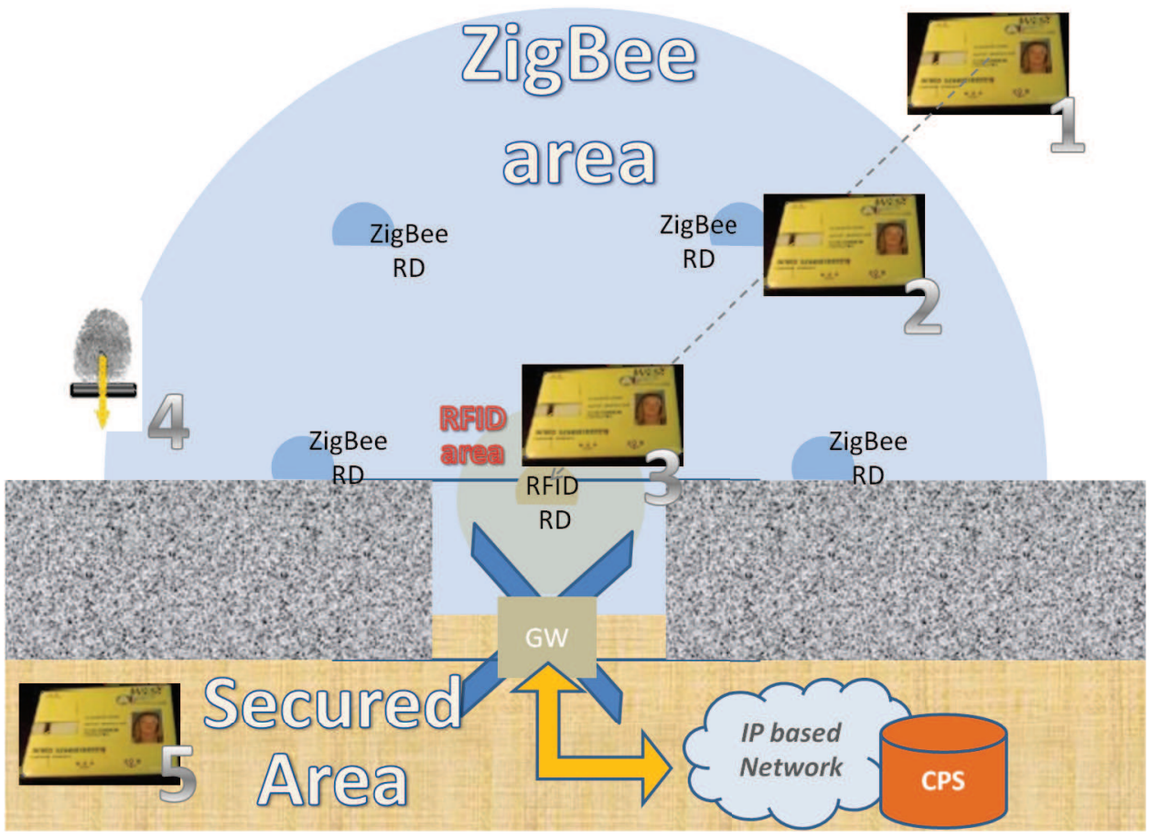


Fig. 6. Case Study 1 – Physical access to a critical area

The access to a critical area towards a controlled gate will be performed by means of the following steps (Fig. 6):

1. The BB is in stand–by mode, i.e., it is waiting for a beacon sent by one of the ZigBee RD forming a Cluster Tree topology (Hauer et al., 2011; Jurcik et al., 2010).
2. When the BB enters the ZigBee area, it is able to ear the beacons sent by the RDs and to communicate with the control unit on the gate in order to communicate its arrival. In this context, the badge implements the positioning solution as described in (Tennina, Di Renzo, Santucci & Graziosi, 2009) and summarized in the next subsections. In such a way, the DU is able to communicate with the central system in order to make in advance any control related to the badge identification (i.e., to check if it is allowed to access the gate it is approaching).
3. The BB is allowed to pass the gate, the DU will wait for the proximity of the BB.
4. When the BB is close to the gate then DU will request to the BB to start the personal identification, i.e., the BB will ask the owner to scan his/her fingerprint, it compares that scan with the stored one, and the result of such a verification is sent back to the DU, being the only unit able to decode that information.
5. If the identification is successful the DU will open the gate, otherwise proper actions defined by the system administrator will be taken.

Fig. 7 shows the setup used for the experimental testbed, where a Notebook plays the role of the GW: it has a RFID reader (on the right–hand side) and a ZigBee reader (on the left–hand side); furthermore it switches on a lamp to confirm the successful authentication, as well as feedbacks the user in a demo GUI (Fig. 8).

Fig. 7. Biometric Authentication – Setup

Fig. 8. Biometric Authentication – Successful verification

3.1 ESD: an improved optimization SW routine for positioning

The badge is equipped with a novel distributed localization algorithm, which is called ESD (Enhanced Steepest Descent) (Tennina, Di Renzo, Santucci & Graziosi, 2009). In particular, since this method represents an improved version of the well-known Steepest Descent (SD), the latter one is briefly summarized as well.

Let us consider N_A wireless nodes $\{A_i\}_{i=1}^{N_A}$ distributed in the region of interest, whose exact locations in the considered scenario are known, based on a predefined and common reference system of coordinates. These nodes are called *reference* or *anchors* nodes. Let us assume

also that N_U wireless nodes $\left\{U_j\right\}_{j=1}^{N_U}$ with unknown location are present in the same area. These nodes are called *unknown* or *blind* nodes. Both these wireless nodes have a simple radio interface to communicate, which allows not only data exchange but also distance measurements. The main goal of a positioning system is to use the anchor nodes to estimate the position of the blind nodes in the specified coordinate system. In particular, position estimation algorithms require a minimum of either three or four reference nodes in a two– and tree–dimensional coordinate system, respectively (Perkins et al., 2006). In our context it is obviously assumed that Ai are the ZigBee Readers, while U_j are the Biometric Badges.
The following notation will be used to describe the algorithm: (i) bold symbols are used to denote vectors and matrices, (ii) $(\cdot)^T$ denotes transpose operation, (iii) $\nabla(\cdot)$ is the gradient operator, (iv) $\|\cdot\|$ is the Euclidean distance, (v) $\angle(\cdot,\cdot)$ is the phase angle between two vectors, (vi) $\hat{\mathbf{u}}_\mathbf{j} = [\mathbf{u_{j,x}}, \mathbf{u_{j,y}}, \mathbf{u_{j,z}}]^\mathbf{T}$ with j=1,.., N_U denotes the estimated position of the unknown node U_j, (vii) $\mathbf{u}_j = [u_{j,x}, u_{j,y}, u_{j,z}]^T$ is the trial solution of the optimization algorithm for the unknown node U_j, (viii) $\mathbf{a}_i = [x_i, y_i, z_i]^T$ with i=1,.., N_A are the positions of the anchor/reference nodes A_i, and (ix) $d_{j,i}$ denotes the estimated (via ranging measurements) distance between reference node A_i and the unknown node U_j.

3.1.1 Multilateration methods

Both SD and ESD algorithms belong to the family of the multilateration methods. In particular, in such methods the position of an unknown node U_j is obtained by minimizing the error cost function $F(\cdot)$ defined as in Equation 1:

$$F\left(u_j\right) = \sum_{i=1}^{N_A} \left(d_{j,i} - \left\|\mathbf{u}_j - \mathbf{a}_i\right\|\right)^2 \tag{1}$$

The minimization of the error cost function can be realized using a variety of numerical optimization techniques, each one having its own advantages and disadvantages in terms of accuracy, robustness, speed, complexity, and storage requirements (Nocedal & Wright, 2006). Since optimization methods are iterative by nature, we will denote by the index k the k–th iteration of the algorithm, and with $F(\mathbf{u}_j(k))$ and $\mathbf{u}_j(k)$ the error cost function and the estimated position at the k–th iteration, respectively.
Steepest Descent (SD) The SD is an iterative line search method that allows to find the (local) minimum of the cost function in Equation 1 at step $k+1$ as follows (Nocedal & Wright, 2006, pp. 22, sec. 2.2):

$$\mathbf{u}_j(k+1) = \mathbf{u}_j(k) + \alpha_k \cdot \mathbf{p}(k) \tag{2}$$

where α_k is a step length factor, which can be chosen as described in (Nocedal & Wright, 2006, pp. 36, ch. 3), and $\mathbf{p}(k) = -\nabla(F(\mathbf{u}_j(k)))$ is the search direction of the algorithm. In particular, when the optimization problem is linear, some expressions exist to compute the optimal step length in order to improve the convergence speed of the algorithm. On the other hand, when the optimization problem is non-linear, as considered for positioning problems, a fixed and small step value is in general preferred in order to reduce the oscillatory effect when the algorithm approaches a solution. In such a case, we have $\alpha_k = 0.5\mu$ (Santucci et al., 2006), where μ is the learning speed.
Enhanced Steepest Descent (ESD) The SD method provides, in general, a good accuracy in estimating the final solution. However, it often requires a large number of iterations, which may result in a too slow convergence speed for mobile ad–hoc wireless networks. The

proposed ESD algorithm aims at improving the convergence speed of the SD algorithm, while trying to maintain its good accuracy for position estimation. The basic idea behind the ESD algorithm is to adjust the step length value α_k as a function of the current and previous search directions $\mathbf{p}(k)$ and $\mathbf{p}(k-1)$, respectively. In particular, α_k is adjusted as shown in Equation 3, where $\theta_k = \angle(\mathbf{p}(k), \mathbf{p}(k-1))$, $0 < \gamma < 1$ is a linear increment factor, $\delta > 1$ is a multiplicative decrement factor, and θ_{min} and θ_{max} are two threshold values which control the step length update.

$$\begin{cases} \alpha_k = \alpha_{k-1} + \gamma & if\ \theta_k < \theta_{\min} \\ \alpha_k = \alpha_{k-1}/\delta & if\ \theta_k > \theta_{\max} \\ \alpha_k = \alpha_{k-1} & otherwise \end{cases} \tag{3}$$

By using the four degrees of freedom $\gamma, \delta, \theta_{min}$ and θ_{max}, the convergence rate of the algorithm, and the oscillatory phenomenon when approaching the final solution can be simultaneously controlled in a simple way and without appreciably increasing the complexity of the algorithm when compared to the SD method. Basically, the main advantage of the ESD algorithm is the adaptive optimization of the step length factor α_k at run time, which allows to dynamically either accelerate or decelerate the convergence speed of the algorithm as a function of the actual value of the function to be optimized

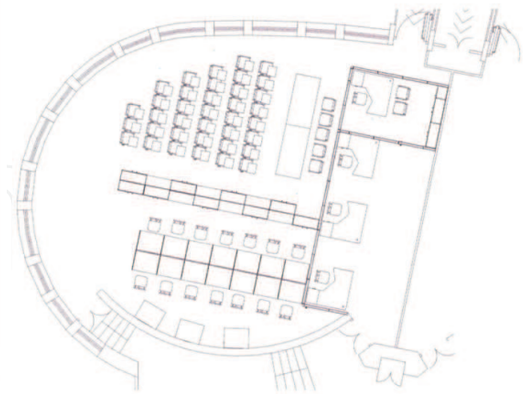
3.1.2 Positioning system validation

Localization is performed in a fully RSSI–based distributed and decentralized fashion for the blind node. In other words, each blind node receives data from the fixed anchor/reference nodes (see Fig. 9a) and convert the RSSI measurements of each packet into an estimation of distance. It is well known that RSSI is as simple as really inaccurate, but this distance estimation accuracy has been improved on the blind node side, by allowing anchor nodes to perform an innovative on–line radio signal propagation characteristics estimation (Tennina et al., 2008).

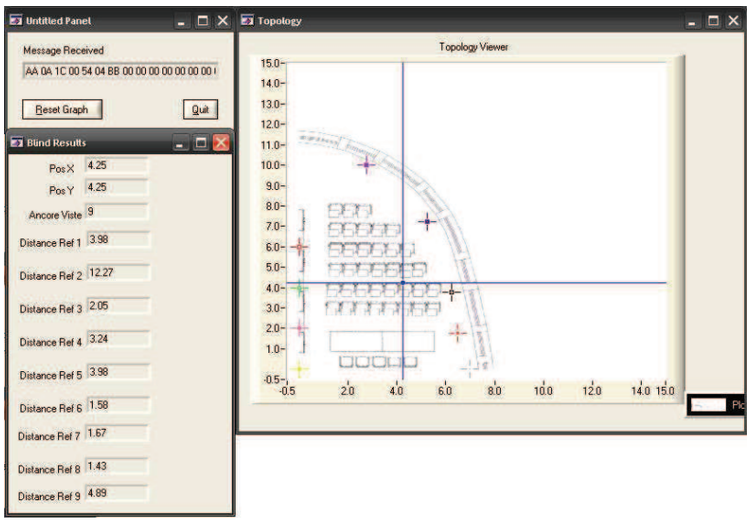
In order to validate the proposed solutions, and have a sound understanding of the performance of the ESD algorithm in realistic scenarios, we have conducted a campaign of measurements during the opening ceremony day of the NCSlab on March 27, 2008 (Fig. 9b). The event was characterized by a half-day kick–off conference during which the past, present, and future activities of the laboratory were presented. The kick–off conference was attended by several people, and offered a good occasion to test the performance of the deployed network, and, in particular, to test the achievable performance in a realistic GPS-denied environment, where the propagation characteristics of the radio channel changed appreciably during the event due to the people's movement inside the room (i.e., dynamic indoor environment). The duration of the event was approximately three hours and forty minutes, thus providing enough statistical data to well support our findings and conclusions. This ceremony was characterized by four main phases, well describing the dynamic nature of the event and, as a consequence, the dynamic nature of the propagation environment to be analyzed. In what follows there is a brief description of each phase.

1. The first phase, which took place before the starting of the opening ceremony, is characterized by a progressive increase of the number of people inside the room, some of them very close and in motion around the blind node to be localized (i.e., the dot point in Fig. 9c).

(a) Battery powered anchor node



(b) Plan of the NCSlab



(c) Host Application

Fig. 9. ESD Positioning Validation – Experimental Setup

2. The second phase, which took place during the development of the ceremony, is characterized by several people (staying either seated or stand) inside the room, and some people coming in and going out the room.
3. The third phase, which took place at the end of the ceremony, is characterized by the vast majority of people staying stand and leaving the conference room.
4. The fourth phase corresponds to the scenario with no people in the room, thus giving a virtually static indoor scenario with almost fixed propagation characteristics.

Fig. 9c the host application interface with anchor (cross points) and blind (dot point) nodes deployed during the field tests and available to the user to analyze the behavior of localization and tracking operations.

The setup was characterized by the following main settings: (i) 9 anchor nodes, distributed on the room's perimeter, and 1 blind node have been considered, (ii) all the nodes were placed on the top of wood supports, (iii) the anchor nodes broadcasted their ID and position every 800 milliseconds as well as estimated the radio signal propagation characteristics as described in (Tennina et al., 2008), and (iv) every RSSI used by the blind node was obtained by averaging 10 RSSIs (Average RSSI) per anchor.

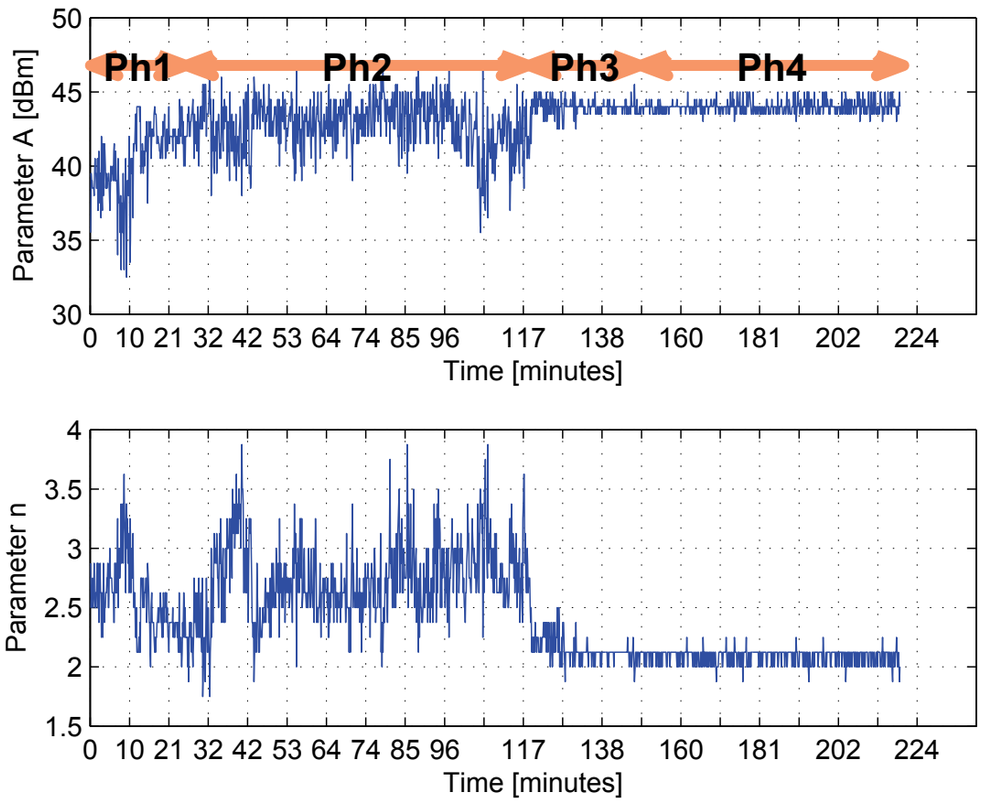


Fig. 10. Estimated propagation parameters during the NCSlab's opening ceremony

In Fig. 10, the estimated propagation parameters A and n (Tennina et al., 2008) are reported as a function of time. We can readily figure out that there is a significant fluctuation of these parameters during the progress of the conference, and, as expected, the variation gets large during Phase 1 and 3, and, in particular, during Phase 2, while they are almost constant during Phase 4, which represents a virtually static reference scenario. This figure qualitatively suggests that using an outdated estimate for the channel parameters may certainly yields less accurate estimates of the distances and thus of the position of the blind node.

Finally, Fig. 11 shows the positioning accuracy of the proposed ESD algorithm running on the blind node when it can resort on the estimations of the propagation parameters updated on–line by the anchor nodes. As we can see, even if the dynamic of the environment might change dramatically the propagation conditions, the positioning accuracy is good enough, i.e., with an average error generally less than 2 meters, and stable, i.e., no major fluctuations.

Similar accuracies have been obtained in recent experimental trials (Tennina, Pomante, Graziosi, Di Renzo, Alesii & Santucci, 2009).

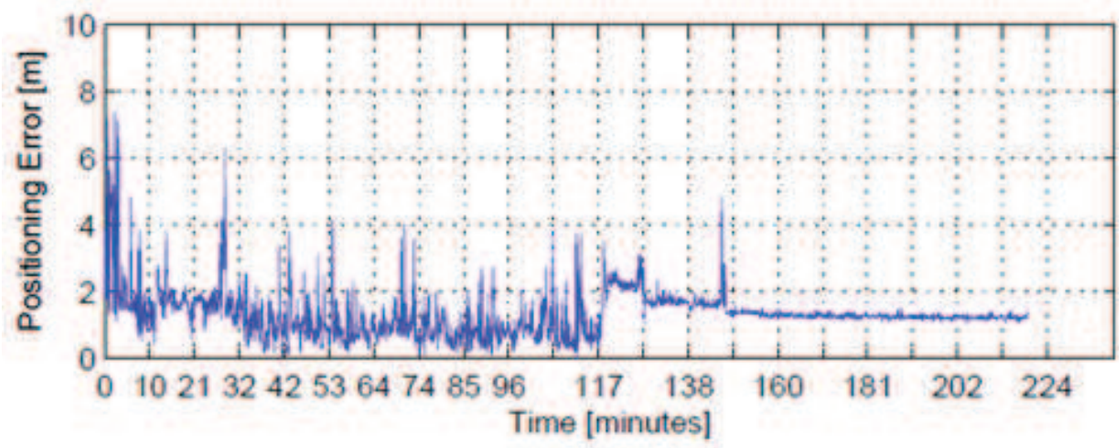


Fig. 11. ESD positioning accuracy with on-line dynamic propagation parameters estimation

4. Case Study 2 – Logical access to a critical area

The security framework described in Section 2.7 allows the exploitation of the badge virtually everywhere. A typical scenario is the home banking, where users access remotely to their bank account. Nowadays they usually receive a one–time password generator, which is used when the bank's web page ask it. The idea is to grant access to such services by relying on the higher security levels guaranteed by the usage of biometric–based authentication. By simply using a PC with an IEEE 802.15.4 radio interface (today it is available as an external USB dongle, but in the near future it will be probably integrated into the PC's motherboards as for IEEE 802.11 radio interfaces) and a classical Internet connection, the badge is able to establish a secure connection between its on-board companion chip and the management SW by means of the PC and the Internet that are used to reach the gateway. Basically, the PC acts as a RD.
Fig. 12 shows an example of such a configuration where the access to a web site is authorized only when a verification operations is correctly performed by means of the biometric badge. In such a scenario, the web server acts as the GW, so managing the companion chip of the badge by means of a secure connection that exploits the Internet and the connection from the PC to the badge. The web server asks the badge for the authentication of its owner and based on the result (that, in this case, only the web server is able to decode) it grants or denies the access to the web site.
In order to clarify the whole procedure, let assume that the system is used to manage the access to an online bank account. As for the case study 1, the SA has released a number of BB to a number of authorized people by means of an enrollment procedure. Some of these BB are enabled to identify the user in order to allow him/her to access to the bank account. Finally, the user has a personal computer with an IEEE 802.15.4 transceiver in order to communicate with the BB (like the one shown in Fig. 13).
The access to the bank account will be performed through a web interface and by means of the following steps:

1. The user tries to access the bank account on the server and he/she is accordingly redirected to an identification page where some credentials (i.e., username and password) are requested (Fig. 14).

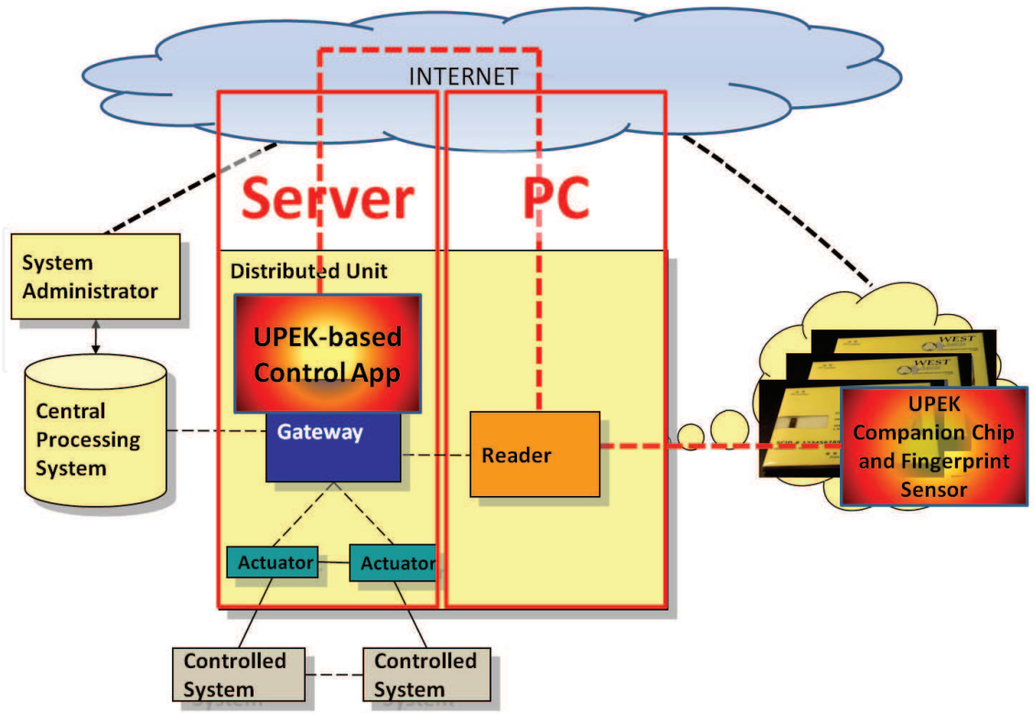


Fig. 12. Case Study 2 – Logical Access to a Critical Area

(a) USB IEEE 802.15.4 dongle and the badge

(b) Personal web site

Fig. 13. Case Study 2 – Logical Access to a Critical Area – Prototypes

2. Then the system asks the user to activates the badge. The BB is then able to establish a secure connection with the web server and the SW running therein starts communicating with the companion chip.

Fig. 14. Case Study 2 – Logical Access to a Critical Area – Login

Fig. 15. Case Study 2 – Logical Access to a Critical Area – Biometric Authentication

3. The web server asks the BB to start the personal identification, i.e., the user will scan his/her fingerprint, while the BB compares it with the stored one, and the result of such a verification is sent back to the web server that is the only unit able to decode such an information (Fig. 15).
4. If the identification is successful, the web server grants the access to the bank account web site (Fig. 16), otherwise the proper actions defined by the system administrator are taken.

It is worth noting that the user's PC and the server can be in different location everywhere in the world, they only need an Internet connection to communicate.

5. Conclusions

The system presented in this chapter is an innovative solution to the problem of automatic and secure advanced services provision, and it is able to guarantee users' identity in a easy and safe way. Although this system is flexible enough to be used in several domains, it meets

Fig. 16. Case Study 2 – Logical Access to a Critical Area – Success

the more rigid laws about the users' privacy without compromising its ease of use, that is the main factor to make it accepted and widely used. The key component is the innovative biometric badge which implements the concept of system–on–badge: a system that is able to automatically perform and check fingerprint scans, in order to verify if the badge owner is actually the person to whom the badge was delivered. Furthermore, it is able to communicate only the results of this verification to the remaining part of the system without the need to share sensible data, i.e., users' biometric information. The use of mature, reliable and low-cost technologies, accurately integrated, is the basis to truly achieve high level of pervasiveness of the biometric techniques in order to support the most important human activities.

6. References

Adeoye, O. S. (2010). A survey of emerging biometric technologies, *International Journal of Computer Applications* 9(10): 1–5. Published By Foundation of Computer Science.

BTAM (2010). Biometric technology application manual.
URL: *www.nationalbiometric.org*

Elliott, S., Massie, S. & Sutton, M. (2007). The perception of biometric technology: A survey, *Automatic Identification Advanced Technologies, 2007 IEEE Workshop on*, pp. 259 –264.

Hauer, J.-H., Daidone, R., Severino, R., Busch, J., Tiloca, M. & Tennina, S. (2011). An open-source ieee 802.15.4 mac implementation for tinyos 2.1. Poster Session at 8th European Conference on Wireless Sensor Networks.
URL: *http://www.nes.uni-due.de/ewsn2011*

IEEE (2006). Standard for information technology part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low rate wireless personal area networks (lr-wpans), LAN/MAN Standards Committee of the IEEE Computer Society Std.
URL: *http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf*

Jurcik, P., Severino, R., Koubaa, A., Alves, M. & Tovar, E. (2010). Dimensioning and worst-case analysis of cluster-tree sensor networks, *ACM Transactions on Sensor Networks* 7(2).

Li, P. & Zhang, R. (2010). The evolution of biometrics, *Anti-Counterfeiting Security and Identification in Communication (ASID), 2010 International Conference on*, pp. 253 –256.

Montalbano (2009). Mtsens iso 15693 compatible 13.56 mhz rfid tag.
URL: *http://www.montalbanotechnology.com*

Nocedal, J. & Wright, S. (2006). *Numerical Optimization*, second edn, Springer.

Perkins, D., Tumati, R., Wu, H. & Ajbar, I. (2006). Localization in wireless ad hoc networks, 16: 507–542.

Santucci, F., Graziosi, F. & Tennina, S. (2006). Service design and simulation in ad-hoc wireless sensor networks, *International Journal on Mobile Networks Design and Innovation* 1: 208–214.

Sonkamble, S., Thool, R. & Sonkamble, B. (2010). Survey of biometric recognition systems and their applications, *Journal of Theoretical and Applied Information Technology* 11(1).

Tennina, S., Di Renzo, M., Graziosi, F. & Santucci, F. (2008). Locating zigbee nodes using the ti's cc2431 location engine: a testbed platform and new solutions for positioning estimation of wsns in dynamic indoor environments, *Proceedings of the first ACM international workshop on Mobile entity localization and tracking in GPS-less environments*, International Conference on Mobile Computing and Networking, San Francisco, California, USA, pp. 37–42. SESSION: Radio/RSSI based methods.

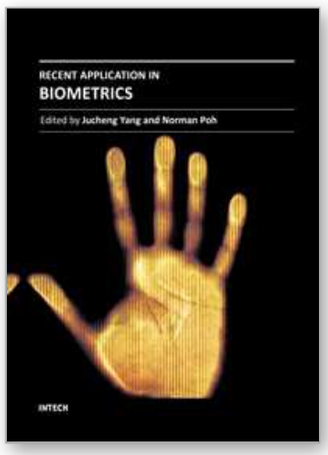
Tennina, S., Di Renzo, M., Santucci, F. & Graziosi, F. (2009). Esd: A novel optimization algorithm for positioning estimation of wsns in gps–denied environments – from simulation to experimentation, *International Journal of Sensor Networks* 6(3/4): 131–156.

Tennina, S., Pomante, L., Graziosi, F., Di Renzo, M., Alesii, R. & Santucci, F. (2009). Localization, tracking, and automatic personal identification in gps-denied environments a solution based on a wireless biometric badge, *Tridentcom, 5th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities and Workshops*, pp. 1–3.

TI (2009). A true system-on-chip solution for 2.4 ghz ieee 802.15.4 / zigbee(tm). Datasheet, Rev. F.
URL: *http://focus.ti.com/docs/prod/folders/print/cc2430.html*

UPEK (2009). Chipset tcs3-tcd42, touchstripő fingerprint authentication solution. TouchStrip Fingerprint Sensor (TCS3) and the Digital ID Hardware Engine.
URL: *http://www.upek.com/solutions/portable/chipset.asp*

WESTAquila (2010). Wireless embedded systems technologies – l'aquila.
URL: *http://www.westaquila.com*



Recent Application in Biometrics

Edited by Dr. Jucheng Yang

ISBN 978-953-307-488-7
Hard cover, 302 pages
Publisher InTech
Published online 27, July, 2011
Published in print edition July, 2011

In the recent years, a number of recognition and authentication systems based on biometric measurements have been proposed. Algorithms and sensors have been developed to acquire and process many different biometric traits. Moreover, the biometric technology is being used in novel ways, with potential commercial and practical implications to our daily activities. The key objective of the book is to provide a collection of comprehensive references on some recent theoretical development as well as novel applications in biometrics. The topics covered in this book reflect well both aspects of development. They include biometric sample quality, privacy preserving and cancellable biometrics, contactless biometrics, novel and unconventional biometrics, and the technical challenges in implementing the technology in portable devices. The book consists of 15 chapters. It is divided into four sections, namely, biometric applications on mobile platforms, cancelable biometrics, biometric encryption, and other applications. The book was reviewed by editors Dr. Jucheng Yang and Dr. Norman Poh. We deeply appreciate the efforts of our guest editors: Dr. Girija Chetty, Dr. Loris Nanni, Dr. Jianjiang Feng, Dr. Dongsun Park and Dr. Sook Yoon, as well as a number of anonymous reviewers.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen