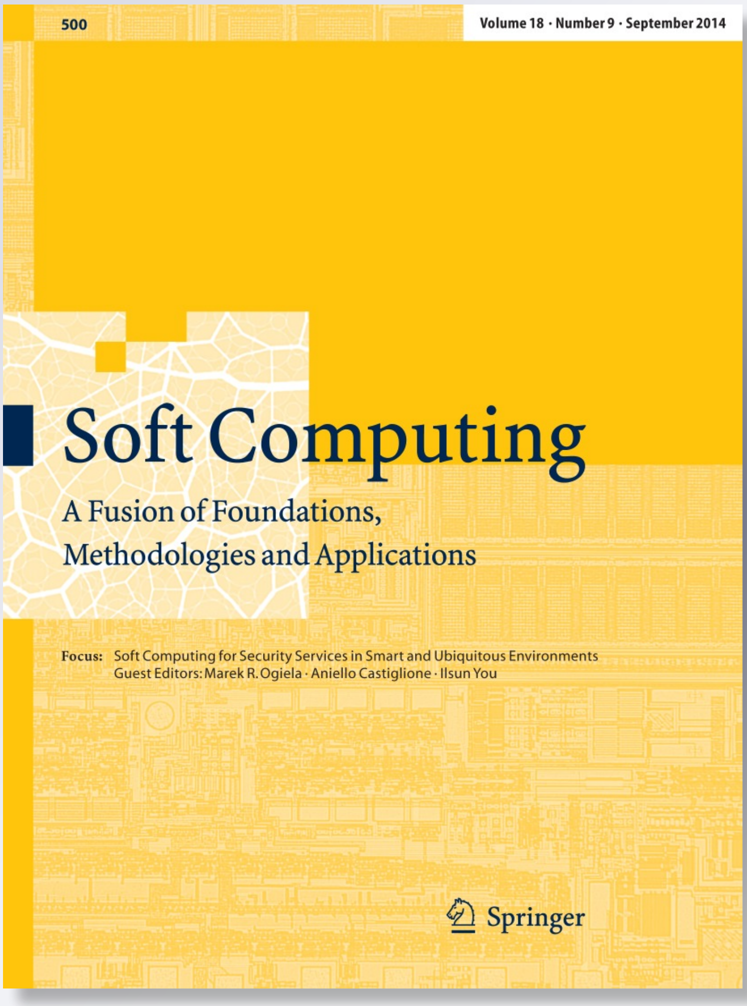
A soft computing based location-aware access control for smart buildings

José L. Hernández, M. Victoria Moreno, Antonio J. Jara & Antonio F. Skarmeta

Soft Computing
A Fusion of Foundations,
Methodologies and Applications

ISSN 1432-7643
Volume 18
Number 9

Soft Comput (2014) 18:1659-1674
DOI 10.1007/s00500-014-1278-9



500

Volume 18 · Number 9 · September 2014

Soft Computing

A Fusion of Foundations,
Methodologies and Applications

Focus: Soft Computing for Security Services in Smart and Ubiquitous Environments
Guest Editors: Marek R. Ogiela · Aniello Castiglione · Ilsun You

Springer

Springer

Soft Comput (2014) 18:1659–1674
DOI 10.1007/s00500-014-1278-9

FOCUS

A soft computing based location-aware access control for smart buildings

José L. Hernández · M. Victoria Moreno ·
Antonio J. Jara · Antonio F. Skarmeta

Published online: 13 April 2014

Abstract The evolution of wireless communications and pervasive computing is transforming current physical spaces into real smart environments. These emerging scenarios are expected to be composed by a potentially huge amount of heterogeneous smart objects which can be remotely accessed by users via their mobile devices anytime, anywhere. In this paper, we propose a distributed location-aware access control mechanism and its application in the smart building context. Our approach is based on an access control engine embedded into smart objects, which are responsible to make authorization decisions by considering both user location data and access credentials. User location data are estimated using a novel indoor localization system based on magnetic field data sent by user through her personal phone. This localization system implements a combination of soft computing techniques over the data collected by smartphones. Therefore, our location-aware access control mechanism does not require any intermediate entity, providing the benefits of a decentralized approach for smart environments. From the results obtained, we can consider our proposal as a promising approach to tackle the challenging security requirements of typical pervasive environments.

Keywords Internet of things · Smart buildings · Indoor localization · Security services · Distributed access control · Capability

1 Introduction

The increasing development of wireless communication technologies and ambient intelligence is enabling a seamless integration of smart objects in our everyday lives (Atzori et al. 2010). This emerging trend, along with the global deployment of mobile devices, such as smartphones or tablets, is redefining the way people exchange information and communicate with their surrounding environment, transforming current physical spaces into *smart buildings*. These incipient ecosystems are expected to be composed by sensors, smart devices and appliances that can be remotely monitored and accessed by users or cloud services, resulting in a new generation of intelligent and ubiquitous environments (Weiser 1991).

However, unlike the current Internet, the realization of these scenarios requires higher security and access control restrictions, since physical objects (e.g. smart door locks or lamps) in typical buildings are being integrated into the Internet infrastructure with network and processing abilities, making them vulnerable to attacks and abuse. Moreover, in these pervasive scenarios, services and resources can be accessed via mobile devices *anytime* and *anywhere* by common users. While this trend provides significant benefits regarding availability and sharing of information, there are everyday situations in which users could abuse these services if location data are not considered in the access control mechanism. For

Communicated by A. Castiglione.

J. L. Hernández · M. V. Moreno (✉) · A. F. Skarmeta
Department of Information and Communications Engineering,
University of Murcia, Murcia, Spain
e-mail: mvmoreno@um.es

J. L. Hernández
e-mail: jluis.hernandez@um.es

A. F. Skarmeta
e-mail: skarmeta@um.es

A. J. Jara
Institute of Information Systems, University of Applied Sciences
Western Switzerland (HES-SO), Sierre, Switzerland
e-mail: jara@ieee.org

example, in the smart buildings context, a smart door lock located at a certain room may require that the requesting user is in front of such door. Otherwise, the access could be denied.

Traditionally, location restrictions have been considered as a relevant factor for the corresponding access control mechanism. In this direction, many efforts based on the *Location-based Access Control (LBAC)* (Ardagna et al. 2006; Covington et al. 2001; Denning and MacDoran 1996) model have been proposed in recent years, in which the user's physical location is considered when determining her access privileges. Typically, the application of location-aware access control models in the smart buildings context has been considered through the use of central entities or back-end servers, which are responsible to infer the user's location information and her access privileges. However, these centralized proposals are not able to cope with the requirements of flexibility, interoperability and scalability that are imposed by pervasive scenarios with a potentially high number of heterogeneous devices.

The correctness and effectiveness of these systems is closely related to the accuracy of the location information and the definition of security zone, that is, the area where the smart object considers the access may be granted. However, in the context of smart buildings, how this location information is obtained is a challenging task since traditional mechanisms such as GPS (Misra and Enge 1999) are not practical due to the lack of signal in indoor environments. This has resulted in the development of alternative positioning systems, as those based on WiFi (Garcia-Valverde et al. 2013), ZigBee (Luoh 2014) and RFID (Ni et al. 2004), with acceptable results in buildings. Nevertheless, a common feature of these approaches is the need to deploy additional hardware, consequently, the cost of these solutions is high and frequent maintenance is required. In addition, an inherent aspect of localization systems is the limited accuracy of the location information, due to physical obstacles or interferences. Therefore, in location-aware access control mechanisms, authorization decisions should properly consider this degree of uncertainty associated with the vagueness of localization systems.

To overcome the aforementioned challenges, this paper presents a location-aware access control for smart buildings, in which authorization decisions are based on the combination of user location data and access credentials. The proposed indoor localization system is based on the use of sensors which are integrated in common smartphones. Therefore, unlike most of the current proposals, our approach does not require the deployment of additional hardware or devices, providing a flexible and easy manageable indoor localization system for users. To compensate this lack of infrastructure, which is usually employed to ensure good performance of localization systems, our localization proposal is based on a combination of powerful soft computing techniques (Zadeh 1997) that lets balance the constraints of the problem. In the off-line phase of our localization system, 2D maps of magnetic field measurements taken along building are generated as well as the mechanism to solve localization based on such maps. Then, during the on-line phase, user location data are estimated through Radial Basis Function Networks (RBF).

In our approach, smart objects are configured with a security zone where the requesting user could be authorized. We propose to implement an authorization mechanism in charge of evaluating different requirements for effective service provisioning. Furthermore, this mechanism copes with the uncertainty of location data provided by our indoor localization solution to adequately decide if user is actually inside the security zone. If the requesting user is in this area, her credentials are evaluated. Otherwise, access is denied. These credentials are attached in the access request as access capabilities, based on the distributed CapBAC model (Hernández-Ramos et al. 2013). Therefore, in our proposal, any intermediate entity is needed to provide location-aware access control, offering the benefits of a decentralized approach for smart environments in terms of end-to-end security, scalability, interoperability, and flexibility.

The structure of this paper is as follows: Sect. 2 presents some related works which face similar problems regarding location-aware access control in smart buildings. Section 3 describes our distributed access control approach which integrates user localization data based on magnetic field measurements. In Sect. 4, the different phases of our indoor localization system are explained. Section 5 details the implementation carried out to solve each one of the technical foundation of our proposal to location-aware access control. Section 6 describes the proposed scenario to evaluate the system as well as the experimental results obtained from the evaluations performed. Finally, Sect. 7 provides conclusions and a description of the future directions of our work.

2 Related work

While recent advances have overcome most of the technological challenges to make environments smarter, security and privacy still remain as major concerns for a full adoption of them. Because of this, the application of different access control models in these scenarios is receiving more interest from research community.

In the context of smart homes, a semantic architecture is described in Kim et al. (2012). The proposal is developed on top of the OSGi framework and incorporates a semantic model of a smart home system. In addition, an access control policy is designed to give home owners robust control over the way users can access their devices. In Ebinger et al. (2013), a privacy dashboard is designed to improve user understanding and implementation of privacy rights related to smart buildings. Specifically, the proposed approach is based on XACML (Moses et al. 2005) policies, which can be configured by non-expert users to model their privacy preferences on sensor data or actuators.

However, these proposals are based on a centralized architecture in which a home gateway is responsible for managing and enforce the access control policies defined by the users. In addition, the user's location is not considered for the authorization decision.

Furthermore, in the smart buildings context, several proposals have been designed to provide location awareness in the authorization process. In this direction, Gupta et al. (2006) introduce a proximity-based access control model (PBAC) for emergency departments. In addition, they implement a prototype by using a RFID-based solution to consider location restrictions. In Gao et al. (2009), a statistical indoor localization method is proposed using WLAN for location-based access control. In the offline phase, a LOESS (Locally Weighted Regression and Smoothing Scatterplots) model is used to build a radio map with the distribution of signal strength. Then, in the on-line phase, locations are inferred by a maximum likelihood estimation (MLE) based on the measured signal strength and the stored distribution. A LBAC system called LOCK is proposed in Wang et al. (2009). The work makes use of autonomous ultrasound positioning devices which are automatically calibrated using a Measurement-Free Calibration method (MFC) to transform their relative positioning results into an absolute coordinate system. Then, a coherent secure zone fitting (CSFZ) method to precisely characterize the secure zones is provided. In the on-line phase, a round-trip judgment (RTJ) algorithm is designed to determine the geographical relationship between the client's position and such secure zones. In Xin-fang et al. (2011), a location-based access control system for data security in mobile storage devices is introduced. The proposal makes use of an embedded RFID tag into the device and a RFID reader to implement location-based access control. In addition, it makes use of RF signals to build the security zone and gets user's location information from the tag and the reader. In Rodriguez et al. (2004), a location-aware medical information system was developed to provide access to hospital resources such as patient's records, based on the user's location. The system considers WLAN as positioning system, and a location estimation method based on a backpropagation neural-network, which is used to estimate the user's location.

Unlike previous proposals, this work presents a novel localization system based on magnetic field measurements, which are provided by current mobile devices such as smartphones or tablets. In addition, our proposal does not require additional hardware or infrastructure since the location estimation stage is embedded into smart objects. Furthermore, our approach is built on top of the distributed CapBAC model (Hernández-Ramos et al. 2013). Therefore, no intermediate entities are needed in our location-aware access control mechanism.

3 Design foundations

3.1 Distributed approach

So far, due to severe constraints in smart objects, most of the proposals have addressed the access control in smart environments by using centralized approaches in which a central entity or gateway is responsible for managing the corresponding authorization mechanism. While traditional access control models, and security standard technologies and protocols can be used in these approaches, several drawbacks arise when they are considered in a real deployment. On the one hand, the inclusion of a central entity prevents end-to-end security to be achieved. In addition, this solution cannot provide a suitable level of scalability for smart environments with a potentially huge amount of devices. On the other hand, a centralized approach increases the cost of the solution since additional hardware is needed. Furthermore, due to the fact that a single entity stores and manages all the data from a set of devices, it becomes a single point of failure. Consequently, any vulnerability might compromise a vast amount of sensitive information.

The aforementioned drawbacks could be solved by a distributed approach in which smart objects are able to make authorization decisions without any intermediate entity. In this case, all the access control logic is embedded into devices, which are enabled with abilities to obtain, process and send information to other services and entities in a direct and natural way. While most of mentioned drawbacks of centralized approaches can be solved, a fully distributed approach comes with some cost. In particular, standard security mechanisms are often based on cryptographic primitives that present a high computational cost, which is not appropriate for resource-constrained devices. In addition, the inherent features of traditional access control models, such as RBAC (Ferraiolo et al. 1995) or ABAC (Yuan and Tong 2005), make their implementation unrealistic on smart objects. Recently, we have proposed a fully distributed access control mechanism based on capabilities (distributed CapBAC) (Hernández-Ramos et al. 2013), which has been demonstrated as a feasible approach to be used on smart environments with resource-constrained devices. Therefore, our location-aware access control mechanism is built on top of distributed CapBAC, providing the mentioned benefits of a distributed approach in the context of smart buildings.

Furthermore, in our proposed localization system, each constrained device is responsible for carrying out location estimations by considering only the building's zone where they are placed. In this way, they are not required to process the location data set related to whole building space which enables location estimation functionality is embedded into resource-constrained devices. Therefore, in our approach, smart objects are enabled with the ability to infer user's location data as well as to enforce her privileges.

3.2 Integrating location data based on magnetic field measurements

The omnipresent role in the daily life of mobile devices such as smartphones or tablets, has resulted in a huge range of new solutions for the indoor localization problem (Lane et al. 2010). For our location-aware access control mechanism, we propose a novel indoor localization solution which only requires, from the hardware point of view, a smartphone and their built-in sensors. Therefore, external hardware infrastructures are not needed (for instance, no radio access points), providing an accurate, flexible and easily manageable solution for users. Specifically, we only consider the data provided by the magnetic sensors of smart phones to make our location-aware access control totally independent on the type of devices and available signals in buildings.

The proposals for indoor localization systems based on magnetic field measurements are partly inspired by the evidence that animals make use of the Earth's magnetic field not only for orientation detection, but also for true navigation (Boles and Lohmann 2003). These solutions assume that the success of magnetic sensors both for orientation and position estimation is conditioned by their capacity to sense the Earth's magnetic field in environments containing magnetic anomalies. In principle, a non-uniform indoor ambient magnetic field produces different magnetic observations depending on the path taken through it. In buildings, we can find Earth's magnetic field variations due to any object of iron, cobalt, or nickel, and also from man-made sources such as steel structures, electric power systems and electronic and mechanical appliances. Thus, static objects or infrastructures inside buildings (printers, lifts, etc.) perturb Earth's magnetic field and can make up a profile of magnetic field values (a map composed by magnetic field fingerprints), which can be used to solve localization in buildings.

Nevertheless, this magnetic profile must be well characterized and quantified previously at estimation process (Haverinen and Kemppainen 2009). To date, main efforts have been made for the study and validation of the approach of using indoor magnetic field for localization, and all these analyses conclude that it represents a stable and unique solution that can be applicable for solving the problem. Some proposals to generate magnetic maps of buildings to be used for indoor localization are presented in the literature, for instance (Gozick et al. 2011; Li et al. 2012). Most of them are based on considering only the intensity value of the magnetic fields measured inside buildings. Nevertheless, the scalability and robustness of these solutions in different types of building cannot be ensured, mainly in buildings where the number of artificial magnetic fields is low, or when the magnetic field sources of the building are of the same nature. Bearing in mind this restriction, in our approach, we consider the vectorial character of magnetic fields, and propose to use the three components (x, y, z) of a magnetic field to provide a more complete characterization of buildings. This approach is addressed by Angermann et al. (2012). It is noticeable that in this type of solutions it is required to control the orientation of the mobile phone during the measurement process. Moreover, a relevant issue for indoor localization systems is to choose the most suitable data processing techniques. For our approach, the uncertainty in the accuracy of location data must be dealt because it varies depending on the building zone where a user is located. Therefore, taking into account this constraint, it is necessary to apply suitable soft computing techniques that address this aspect to provide an accurate localization solution which will be used for the access control of services provided in buildings.

The computation techniques chosen in this work are based on the scene analysis, where, first, reference measurements (fingerprints) of the ambient magnetic field are collected and processed to generate magnetic field maps of the building. For this, powerful techniques such as clustering, classifiers, etc. compound the off-line phase of the localization system. And then, user positions are estimated by matching on-line measurements with the closest a priori location fingerprints. For this, we use an estimator based on Radial Basis Functions Network; it represents the on-line phase of the localization system. Both phases of this system (i.e. off-line and on-line) are fully explained in next section.

4 Indoor localization mechanism based on magnetic field data

4.1 Off-line phase

To generate magnetic field patterns of buildings considering the three magnetic field components to achieve accurate and reliable location estimations, it is required to apply computational techniques that estimate user location based on a particular type of data. A general description of the different actions to be performed to generate such models for localization in buildings is presented below.

1. Phone calibration: it is important to take into account that magnetometer readouts, that are readily available on the smartphones, are prone to disorientation of the sensing module and are dependent to the orientation and position

in which the user wears the phone during the data collection, e.g. whether the device is on user's trousers' pocket or in a bag. Thus, it is necessary to have phone orientation and user wearing position correctly associated to the data collection performed, and which will be considered in the off-line phase of the localization mechanism proposed.
2. Data collection: magnetic field data are gathered using a smart phone with integrated magnetometer.
3. Clustering: data processing to identify zones of the building where magnetic field distributions represent peaks to be used as landmarks of magnetic field. These landmarks will be used later to geo-reference the magnetic field values measured along the building during the on-line phase of the system.
4. Classifier: to perform the building's space division according to the identified landmarks. In this way, a higher accuracy value can be obtained in the localization results.
5. Estimator: analysis of each one of these regions in terms of magnetic field distribution associated to the space distribution, and implementation of the best regression technique to estimate user position for each one of the building's zones associated to a landmark.

Reviewing the most suitable computational techniques recommended in literature to solve each one of these objectives, we analysed contrast different alternatives. The final techniques selected are described below jointly the associated problem's description to solve.

4.1.1 Calibration

During this first stage, predefined orientation and user phone wearing positions are pre-established to be considered and associated later to the appropriate magnetic field maps generated at the end of the off-line phase of our system. Thus, we generate descriptive models based on these data for the user localization. Furthermore, several data collection processes are carried out considering different context conditions, such as: different levels of occupancy, different moments at day, etc. Thus, the building models generated will be representative enough to cover different building conditions.

4.1.2 Data collection

Considering each one of the pre-established orientations and user phone wearing positions, "snapshots" of the magnetic field are collected during short periods of time (less than a minute in each location Z_q) and along building space. Such measurements are associated to the physical positions $Z_q^{(t)}$ where they were gathered. Then, the set of data pairs are:

$$(B_q^{(t)}, Z_q^t), \quad t = 1, 2, \ldots, N \tag{1}$$

where N is the number of data instances at location Z_q, $B_q^{(t)} = [Bx_q^{(t)}, By_q^{(t)}, Bz_q^{(t)}] \in R^n$ and $Z_q^{(t)} \in R^k$.

4.1.3 Pre-processing

The pre-processing unit is responsible for preparing the measured data by transformation. Besides, feature vectors are extracted from data to be used for location estimation. The different processing techniques applied in this stage are:

1. Transformation: based on the raw dataset collected by the phone. During the features transformation, compact representations of the magnetic field values are extracted, namely features, which will be used later for localization estimation. The initial feature selection to represent magnetic field distribution is based on studies proposed in the literature that already make use of them to achieve similar goals (as it is described in Table 1). The dataset values are segmented to windows of 64 samples, and each window is processed through several feature extraction methods producing a feature vector that can be used to generate the clusters and train the classifier. The adopted features are summarized in Table 1. At this stage, 27 features were extracted for evaluation (9 features for each magnetic field component: Bx, By and Bz).
2. Filtering: it replaces all missing values for nominal and numeric attributes in a dataset with the modes and means from the training data.
3. Normalize: it normalizes all numeric values in the given dataset. The resulting values are in the [0, 1] interval for every feature extracted from the initial dataset.
4. Feature selection: it performs a *Principal Components Analysis (PCA)* and transformation of the data which are used in conjunction with a ranker search. PCA is a major technique for reducing dimensionality in high-dimensional data. PCA identifies the directions in which the observations are more variable. If we consider $b(i)$ as multi-dimensional observations and u an arbitrary direction in this multi-dimensional space, the principal components are calculated by maximizing the following equation:

$$\frac{1}{m} \cdot \sum_{i=1}^{m} (b(i)^{\mathrm{T}} \cdot u)^2 \tag{2}$$

Dimensionality reduction is accomplished by choosing enough vectors to account for some percentage of the variance in the original data (by default 0.95). In this case, the maximum number of attributes to include in transformed attribute names is established to 5, thus the final computational load of our localization system is reduced. The ranking is performed over all features, and among

Table 1 Summary of the extracted features from magnetic field measurements (in 3D)

	Feature	Description
1	Entropy	Measures the uncertainty associated with the data; measuring from different positions during a walking activity provides different periodical patterns. Adapted from Atallah et al. (2010)
2	SumPowerDetCoeff	Measure of the power of the detailed coefficients derived form the discrete wavelet transformation (Kunze et al. 2005)
3	Variance	The variance of the data is similarly taken to Ofstad et al. (2008). As the position of the device gets closer to the vertical axis of the body, this parameter is expected to reduce
4	VarFFT	The variance of FFT coefficients between 0.5 and 5.5 Hz, covering the range where the majority of the energy for daily life activities lies (Sun and Hill 1993)
5	Intensity	Analogous to Győrbíró et al. (2009), the intensity is calculated as the sum of the numerical derivative of a window of samples, normalized to the length of the window
6	ZCR	Analogous to Yang (2009), it measures zero crossing rate while zero level is set to the mean of the signal
7	Kurtosis	Measures the peakedness of the data relative to the normal distribution. It has been suggested in Shi et al. (2011), Altun and Barshan (2010), Andreu and Angelov (2010)
8	Skewness	A widely used feature e.g. Shi et al. (2011), Altun and Barshan (2010), Andreu and Angelov (2010) that measures the data symmetry
9	Correlation coefficient	The ratio of the covariance and the product of the standard deviations of each pair of axes. It has been utilized for activity recognition purposes in Atallah et al. (2011), Andreu and Angelov (2010), Bao and Intille (2004) and Ravi et al. (2005)

them we choose the first 5 features best ranked. The final selected features are:

(a) *By VarFTT* ($f1$).
(b) *Bx Intensity* ($f2$).
(c) *By Intensity* ($f3$).
(d) *Bx SumPowerDetCoeff* ($f4$).
(e) *By Entropy* ($f5$).

Considering such features, the Eq. (1) can be rewritten as:

$$\{[f1_q^{(t)}, f2_q^{(t)}, f3_q^{(t)}, f4_q^{(t)}, f5_q^{(t)}], Z_q^t\}, \quad t = 1, 2, \ldots, N \tag{3}$$

where $P_q = [f1_q, f2_q, f3_q, f4_q, f5_q]$ is the vector of features extracted from the magnetic field measurements associated to the physical location Z_q.

At this point, and based on these magnetic field features, we generate the map of the building. These maps are used during the following stages of our proposed localization mechanism.

4.1.4 Clustering

This phase performs the space division of the building according to the magnetic field value distribution. It groups the collected data according to the identified clusters, whose centroids are associated to magnetic field landmarks.

After a comparison among different techniques for clustering, the selected method is based on the *Simple Expectation Maximisation (EM)* (McGregor 2004), which shows the best performance in terms of classification error obtained.

EM assigns a probability distribution to each instance which indicates the probability of it belongs to each of the clusters. EM can decide how many clusters to create by cross validation, although this number can be previously specified. For this, we propose an automatic search of the number of clusters that optimizes the classification success and the localization estimation accuracy (Luna et al. 2011).

Each generated cluster is a vector of mean values of the magnetic field features composing the centroid of the cluster and a vector of deviation values associated to such cluster. These vectors can be represented mathematically as: $\mu_{Ci} = [\mu_{f1}, \mu_{f2}, \mu_{f3}, \mu_{f4}, \mu_{f5}, \mu_Z]$, and $\sigma_{Ci} = [\sigma_{f1}, \sigma_{f2}, \sigma_{f3}, \sigma_{f4}, \sigma_{f5}, \sigma_Z]$; where μ_{Ci} and σ_{Ci} denote the mean and deviation of the centroid of the landmark i, respectively.

4.1.5 Landmark's classifier

In this phase, we implement a classifier that lets assign each new magnetic field measurement to one landmark. In this way, we can focus on the building's zone covered by each landmark, and discriminate the rest of the building's space to carry out the location estimation.

After analysis of different proposals, the selected classifier for carrying out this assignment is the meta-classifier *Decorate* (Melville and Mooney 2005), which achieves the highest success value in classification.

Decorate is a meta-learner for building diverse ensembles of classifiers using specially constructed artificial training examples. Comprehensive experiments have demonstrated that this technique is consistently more accurate than its base classifiers [Bagging (Breiman 1996) and Random Forests (Breiman 2001)]. It also obtains higher accuracy than Boosting (Friedman et al. 2000) on small training sets, and achieves comparable performance on larger training sets.

4.1.6 Localization estimator

Once the magnetic field measurements are correctly classified to their associated landmarks, the building's zone of every measurement can be inferred. Thus, the position estimation is carried out using the available knowledge about the associated landmark. For this, a *Radial Basis Functions Network* (Simon 1999) for each landmark is computed as regression technique, which uses all training data associated to every landmark to estimate the user position according to its magnetic field feature vector.

RBF networks find approximation solutions in the form of weighted sums of basis functions based on reference data. The main advantages of using RBF for estimation are its scalability and easy deployment under different context conditions, where a variable number of centroids have been identified previously.

In our case, for each building's space division associated to one landmark, an RBF network is implemented.

The input space P of our RBF is the vector of selected features of the magnetic field. These data can be denoted as:

$$P \in R,\ P = \{p_i\}, \quad \forall p_i = [p_1, p_2, \ldots, p_n] \tag{4}$$

where n is the number of measurements received from the phone and classified within the chosen subarea associated to a landmark. The target class Z represents the position. This is denoted as:

$$Z \in R^k,\ Z = \{z_i^k\}, \quad \forall z_i^k = [z_1^k, z_2^k, \ldots, z_n^k] \tag{5}$$

where k is the dimension of the position. In our case, we assume a value of $k = 2$. Then, given the training values $\{(p_i, z_i^k), \ldots, (p_n, z_n^k)\}$, our goal is to find a function that allows us to classify the monitored tag position ($z_i = [x_i, y_i]$), knowing its vector of magnetic field features (p_i).

The vector p_j is provided as input to all functions of our RBF network, and the output $f(p_j)$ is given by:

$$f(p_j) = \sum_{i=1}^{c} w_i \cdot \varphi(\parallel p_j - c_i \parallel) \tag{6}$$

where $\parallel p_j - c_i \parallel$ is the Euclidean distance between p_j and the RBF function with center c_i.

The number of RBFs is C, and w_i is the weight of the network. The value of β specifies the width of the basis functions and allows their sensitivity to be adjusted. As β decreases, the basis functions become wider and overlapping may increase. An appropriate value of β is usually selected experimentally based on the reference data, and this can be further adjusted when testing data are available.

In our proposal, we use the k-means clustering algorithm (Kanungo et al. 2002) to provide the basis functions of our RBFs, and to learn either a linear regression on top of that. For this, symmetric multivariate gaussian functions are fit to the data from each cluster. The RBF network implementation for each one of the magnetic field landmarks, which is obtained after clustering, represents the last stage of the off-line phase of our proposed localization system.

Finally, Fig. 1 shows a schema with the sequence of all the steps involved in the off-line phase of our localization system.

4.2 On-line phase

After the off-line phase, user localization can be estimated using the magnetic field maps generated during the off-line stage, as well as the localization estimator designed. A schema of the steps carried out during the on-line phase of our localization system can be seen in Fig. 2. Input data are the magnetic field measurements sensed by user's phone magnetometer. From such measurements, the magnetic field features are extracted. Later, this feature vector is classified as belonging to one landmark's cluster. And finally, considering the RBF implemented for such landmark, user position is estimated.

This localization system is used in our proposed access control mechanism to properly evaluate if requesting user is inside the security zone defined for a specific smart object. The integration of this information and access credentials for our proposed access control mechanism is described in next section.

5 Location-aware access control

5.1 Mechanism overview

An overview of our location-aware access control system is shown in Fig. 3. The basis of the proposed approach is built on top of distributed CapBAC, which is described in

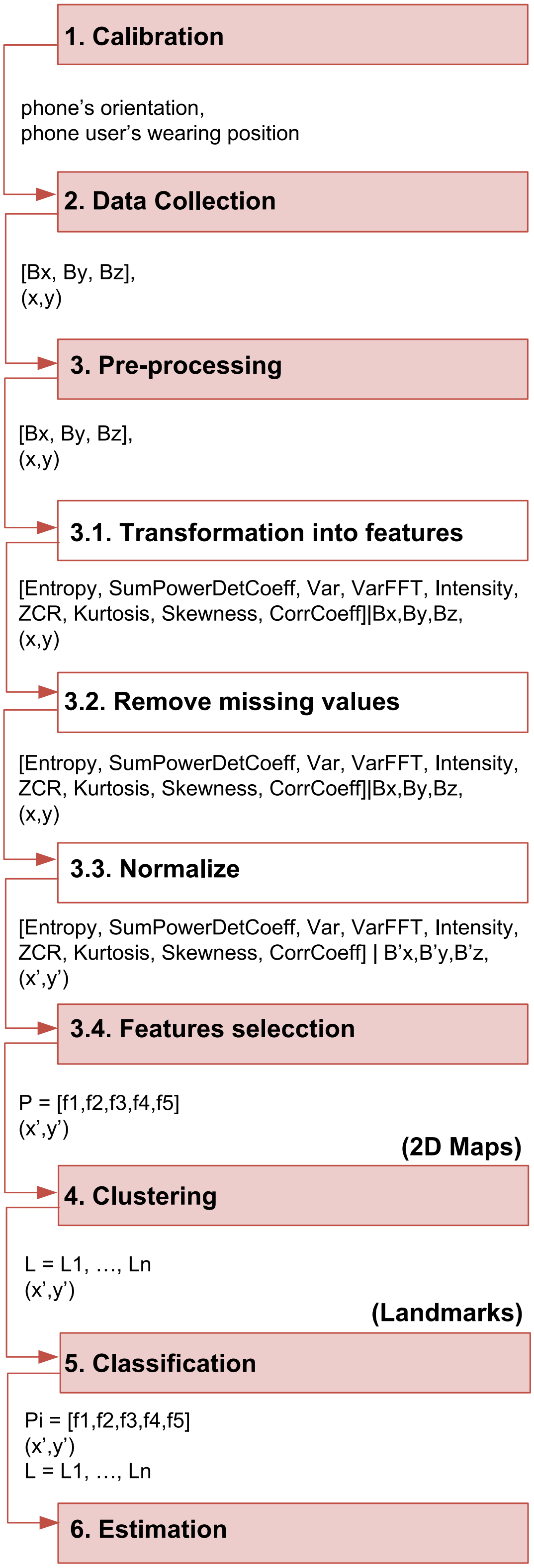

1. Calibration
phone's orientation,
phone user's wearing position
2. Data Collection
[Bx, By, Bz],
(x,y)
3. Pre-processing
[Bx, By, Bz],
(x,y)
3.1. Transformation into features
[Entropy, SumPowerDetCoeff, Var, VarFFT, Intensity, ZCR, Kurtosis, Skewness, CorrCoeff]|Bx,By,Bz,
(x,y)
3.2. Remove missing values
[Entropy, SumPowerDetCoeff, Var, VarFFT, Intensity, ZCR, Kurtosis, Skewness, CorrCoeff]|Bx,By,Bz,
(x,y)
3.3. Normalize
[Entropy, SumPowerDetCoeff, Var, VarFFT, Intensity, ZCR, Kurtosis, Skewness, CorrCoeff] | B'x,B'y,B'z,
(x',y')
3.4. Features seleccion
P = [f1,f2,f3,f4,f5]
(x',y')
(2D Maps)
4. Clustering
L = L1, …, Ln
(x',y')
(Landmarks)
5. Classification
Pi = [f1,f2,f3,f4,f5]
(x',y')
L = L1, …, Ln
6. Estimation

Fig. 1 Off-line phase of the localization mechanism

detail in Hernández-Ramos et al. (2013). This scenario has been designed taking into account the constraints which are inherent to current smart objects, as well as the requirements of smart environments regarding interoperability, flexibility and heterogeneity. Specifically, our proposal makes use of an IP-based communications architecture with emerging protocols which have been designed for constrained environments. In particular, *IPv6 over Low power Wireless Personal Area Networks* (6LoWPAN) (Mulligan 2007) is considered as the extension of IPv6 for use in 802.15.4 wireless networks, enabling end-to -end IP networking for resource-constrained devices. In Oliveira et al. (2013a) an approach based on 6LowPAN neighbor discovery protocol is proposed to mitigate attacks initiated from the Internet, without adding additional overhead on the 6LoWPAN sensor. And in Oliveira et al. (2013b) it is presented an example of access control framework for 6LoWPAN networks.

In the smart buildings context, these elements could be instantiated by typical objects such as door locks, lamps or smart meters. Moreover, the *Constrained Application Protocol* (CoAP) (Shelby et al. 2013) enables interoperability at the application layer through RESTful Web services. The protocol is designed with very low overhead and simplicity for machine-to-machine (M2M) applications such as smart energy and building automation.

The basic operation of our access control mechanism is as follows. As initial step, the issuer entity of the system, which could be the device's owner or manager, issues a capability token to the subject granting permissions on the device. Furthermore, such issuer signs this token to prevent security breaches. The value of the signature is attached to the capability token and sent to the subject. It is noteworthy that this stage actually requires an access control process, whereby a set of permissions are inferred and granted to the subject. Nevertheless, the process of how to generate the token is outside the scope of this work. An example of capability token in the smart buildings context with permissions on a smart door lock is shown in Fig. 4.

Once the subject has received the capability token, she tries to make use of the smart object (e.g. a smart door lock). To do this, when she is close to the geographical area of the target device, she generates a request including magnetic field values and the capability token. In addition, this request must be signed to get access to the smart object. For this purpose, the CoAP request format has been extended with three headers:

1. *Capability*, which contains the capability token.
2. *Signature*, including the subject's signature for the request.
3. *Magnetic field values*, which hold the magnetic measurements provided by the subject's personal phone.

The aspect of the resulting CoAP request is shown in Fig. 5. Moreover, according to Fig. 3, this request does not have to be read by any intermediate entity. Indeed, the com-

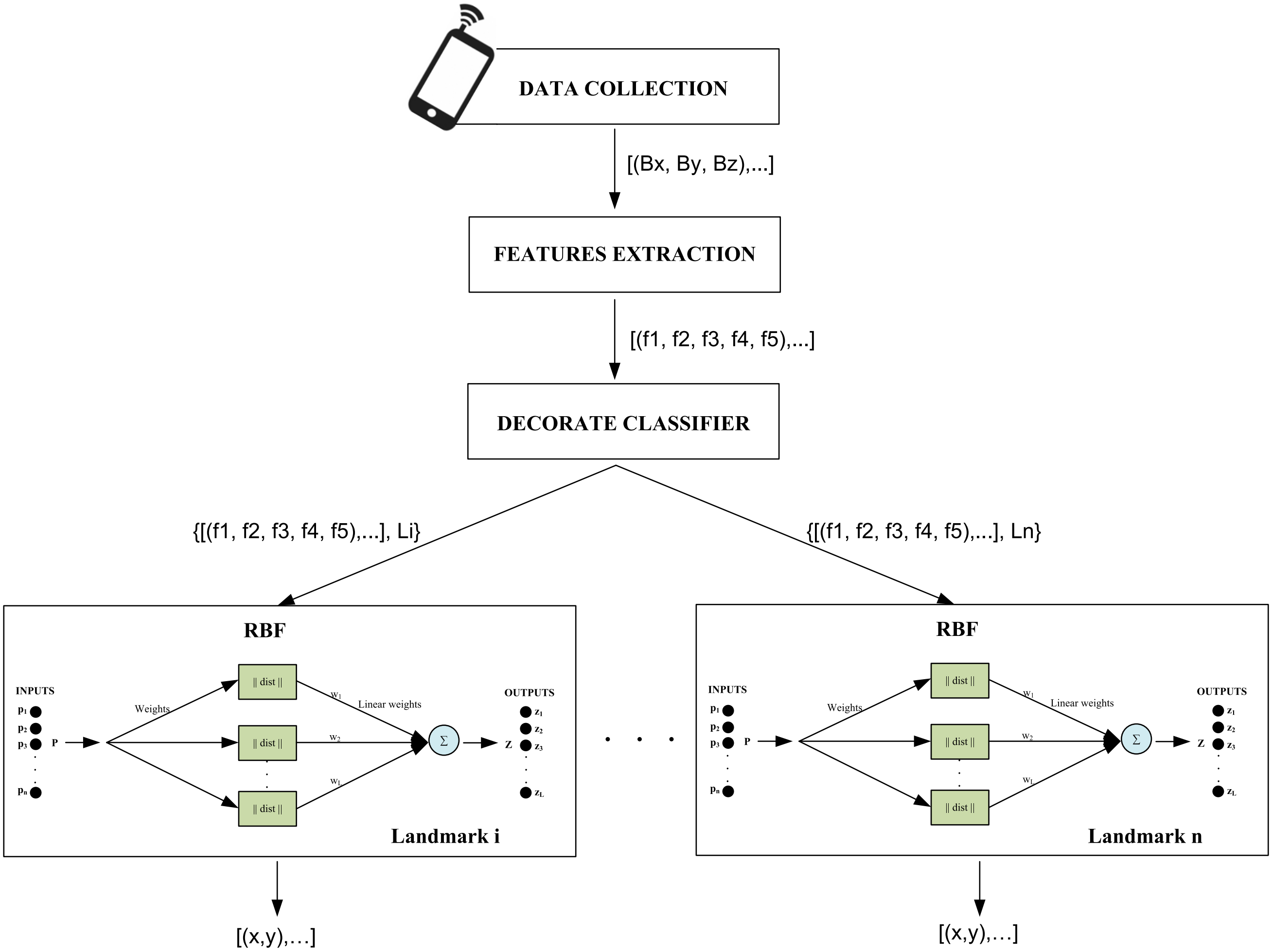


Fig. 2 Building model based on magnetic field for indoor localization

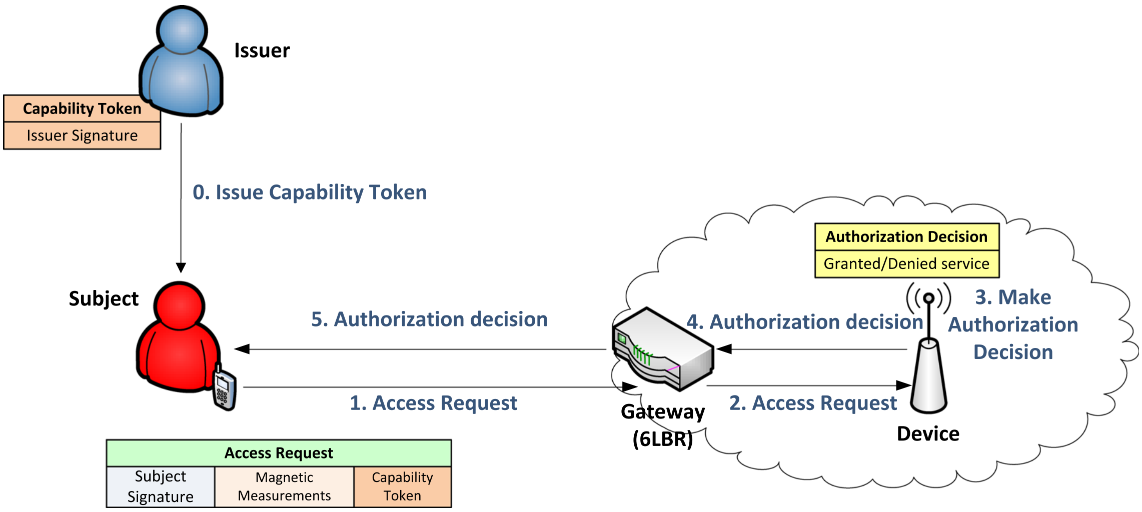


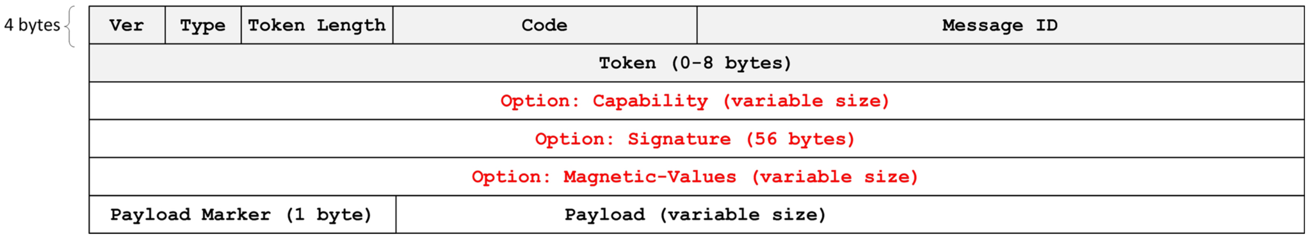
Fig. 3 Proposed scenario

ponent which is denoted as gateway could be instantiated by a 6LowPAN Border Router (6LBR) with basic routing functionalities.

When the smart object receives the request, an authorization engine is launched to make the access control decision. This mechanism has been designed by considering our indoor

Fig. 4 Example of token

```
{
   “id”: “5j3_wo20nf2n8sq9”,
   “ii”: 1382628311,
   “is”: “mvmoreno@um.es”,
   “su”: “lnnH3/IYZz/pqBbSUd+JOyMtNCM=g2o3XRd/3r7iZSjpIIX9BRRULtc=”,
   “de”: “coap://door1.floor2.example.com/”,
   “si”: “uPTor1jxykFQUGxXnRVRm01+uZM=kebPXS9VERYSyX3VFeHH9gW/yQI=”,
   “ar”: [
      {
         “ac”: “POST”,
         “re”: “open”
      }
   ]
   “nb”: 1382628311,
   “na”: 1382628431,
}
```



4 bytes	Ver	Type	Token Length	Code	Message ID
	Token (0-8 bytes)				
	Option: Capability (variable size)				
	Option: Signature (56 bytes)				
	Option: Magnetic-Values (variable size)				
	Payload Marker (1 byte)			Payload (variable size)	

Fig. 5 Appearance of the extended CoAP request format

localization proposal, which is based on magnetic field measurements. Finally, once the authorization process has been completed, the device generates a CoAP response based on the authorization decision made, which is sent to the subject. A more detailed description of the authorization engine is given in next section.

5.2 Authorization engine

Taking into account the overview of our access control mechanism, now we describe the actions performed by the authorization engine integrated in every device whose services are required.

In our proposal, each one of these smart objects only needs the map with the magnetic field characterization belonging to the building's zone where it is placed. Therefore, when devices have to evaluate their services' access, they only have to process the map's area containing the magnetic field model of the landmark associated to such building's zone. In this way, the smart object's computational load is reduced and, consequently, power consumption is saved.

Taking into account the requirements of our access control problem in which both localization data and user credentials are involved, we propose an evaluation in which different tasks are executed in ascending order of complexity. Furthermore, in the case any of the steps in the evaluation fails, the authorization engine will be immediately aborted. Therefore, remaining tasks will not be required. The first task to be performed by the authorization engine is the assessment of if the subject is inside the same building's zone where the smart object is placed. For this, we base on the magnetic field characterization associated to the landmark identified in such zone, since the characterization of every building's zone is made through the magnetic field features associated to the landmark's centroid identified there (see Sect. 4.1). Such landmarks' centroid is represented through mean and deviation values associated to each magnetic field feature. Deviation is the parameter which indicates the zone's extension covered by each landmark in terms of magnetic field. Therefore, given a device located in a building's zone where the magnetic field landmark j (l_j) with centroid Cj has been identified, the required device must assess if the distance between the mean values of the landmark centroid and the vector of magnetic field features extracted from the measurements sent by the user, is smaller than the deviation associated to such landmark's centroid. If it is smaller, the subject is inside the same building zone as the device. Otherwise, the authorization process is aborted and the service is denied. If the previous requirement is satisfied, the second evaluation task is carried out. It consists of evaluating the capability token, which is attached to the access request. The different steps to be executed for this evaluation are shown in Algorithm 2. In addition, a complete description of this process is given in Hernández-Ramos et al. (2013). In case the capability token is successfully evaluated, the last task involved in our authorization engine is launched. During this step, it is evaluated if the subject is inside the security zone defined for the required service (which can be denoted as SZ). For this evaluation, it is necessary to estimate firstly the subject position using the RBF defined for the associated landmark. Once subject location is estimated (Z^k), the distance between subject and device is calculated, and then, it is evaluated if such distance is smaller than SZ. For this last evaluation, it is considered as the mean accuracy value (μ_z) associated to the RBF utilized to estimate the subject position. The complete sequence of the authorization engine is shown in Algorithm 1.

Algorithm 1 Authorization Engine Process

```
Require: CoAP Request $req$ containing:
    – Capability token of subject $k$: $ct_k$;
    – Signature
    – Magnetic fields measurements: $(Bx, By, Bz)_n$
  Magnetic Field Map of the landmark $j$:
    – Vector of magnetic field features that compounds the centroid of the landmark $j$: $P_{l_j} = \sigma_{Ci|B} = [\sigma_{f1_{Ci}}, \sigma_{f2_{Ci}}, \sigma_{f3_{Ci}}, \sigma_{f4_{Ci}}, \sigma_{f5_{Ci}}]$
    – Deviation of magnetic field features that compounds the centroid of the landmark $j$: $\sigma_{P_{l_j}}$
    – Accuracy in location estimation of the RBF implemented in the landmark $j$: $\varepsilon_{Z_{l_j}}$
  Device Features:
    – Position of the required device $n$: $Zs^n = [xs^n, ys^n]$
    – Security zone of the device: $SZ$ = Secure Zone

Extract features vector from magnetic field measurements: $Pin^k = \mu_{f1in^k}, \mu_{f2in^k}, \mu_{f3in^k}, \mu_{f4in^k}, \mu_{f5in^k}]$
Calculate distance between the vector $Pin^k$ and $P_{l_j}$: $d_p = \| Pin^k - P_{l_j} \|$
if $d_p \le \sigma_{P_{l_j}}$ then
  if tokenEvaluated($req$) then
    Estimate position of subject $k$: $Z^k = [x^k, y^k]$
    Calculate distance between subject and device $n$: $d_z = \| Z^k - Zs^n \|$
    if $d_z - SZ \le \varepsilon_{Z_{l_j}}$ then
      Grant Service
    end if
  end if
end if
```

6 Evaluation

In this section, we show the evaluation of our location-aware access control proposal for services provisioning in the smart buildings context. For this purpose, we carry out some experiments to evaluate the performance of each one of the solutions proposed to solve the different technical issues involved in our location-aware authorization approach.

6.1 Evaluation of localization mechanism

To evaluate the proposed algorithms for localization, we have developed a sensing application on an Android G1 dev phone. The android G1 is equipped with a Hall-effect geomagnetic sensor3 in three axes. This sensor implements a Dynamic Offset Estimation (DOE) algorithm to automatically compensate the magnetic offset fluctuations thereby making it more resilient to magnetic field variation within device (Katzakis and Hori 2009). In addition, we have also mitigated the effect of high frequency ambient noise by averaging the measurements prior to the calibration of the device orientation.

Our application is able to log magnetometer signals into a database with frequency of 25 Hz. 10 Subjects were selected from the Information and Communications Engineering Department of the University of Murcia to perform the experiments during which the data were collected. During this stage, the subjects were asked to walk on predefined trajectories along the first floor of the Computer Science Faculty. In addition, the orientation of mobile phones was fixed with users and placed on the middle of their chest. We repeated the data collection during different days and considering different conditions of perturbation, specifically considering different levels of occupancy of the building. In this way, for each building, it should be required to carry out such procedure for providing its magnetic field profile which will be used for localization following our approach of solution. In this sense, the time limit specified required for each building depends on the context of each building, i.e. on the variability of the conditions according to the expected use that each building has and can affect its magnetic field profile.

Algorithm 2 Token Evaluation

```
Require: CoAP Request $req$ containing:
    – Capability token of subject $k$: $ct_k$;
    – Signature of subject $k$: $sig_k$;
    – Magnetic fields measurements: $(Bx, By, Bz)_n$

if $ct_k$ is valid then
  for all accessright $\in ct_k$.accessrights do
    if accessright.action=$req$.method AND
    accessright.resource=$req$.payload then
      permittedAction=true
      break
    end if
  end for
  if permittedAction then
    if $ct_k$.signature is valid then
      if $sig_k$ is valid then
        Authorized Token
      end if
    end if
  end if
end if
```

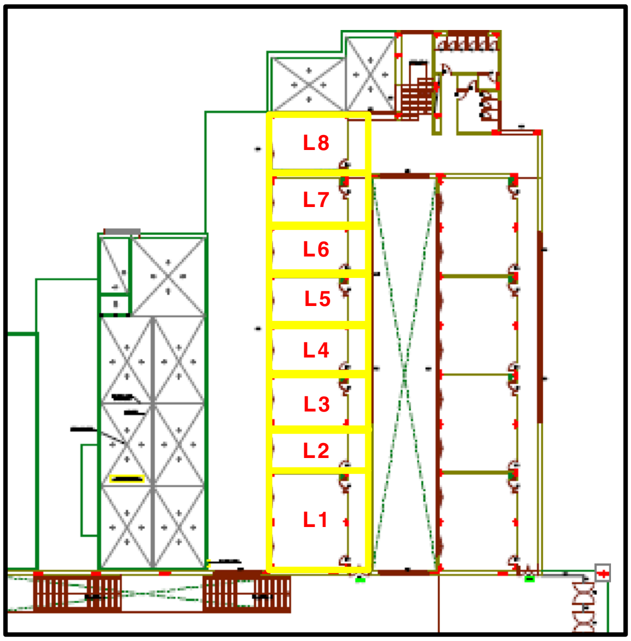


Fig. 6 Magnetic field landmarks

Once data collection was performed, the analysis and data processing techniques presented in Sect. 4.1 were offline processed with Matlab. Consequently, both a 2D building's map containing magnetic field feature vectors and the RBFs in charge of the location estimation were obtained.

Finding the optimal design parameters for implementing the location estimator in charge of providing the localization data during the on-line phase of the system represents the main requirement for providing accuracy to the final results. For this reason, we decided to focus the evaluation process of the localization system on this key issue.

Firstly, we calculate the optimum number of clusters to be considered for the classifier construction. Thus, we have to find the number of clusters that achieves a tradeoff between the error obtained in the landmark classification and the associated error in the location estimation. The distribution of magnetic field landmarks identified in such floor corresponds to building's points set where different electronic and mechanical infrastructures are placed, such as lifts, printers, servers, laboratories, etc., representing all of them as sources of perturbation of the ambient Earth's magnetic field.

We focus on the floor's corridor shown in Fig. 6 to present the results obtained from the tests performed, since this presents a high activity level and where numerous laboratories are located. Such corridor is 28 m long. In Table 2, we show the accuracy values in location estimations for different settings in our mechanism, i.e. considering different number of clusters. During this analysis, we achieved mean values of classification success between 83 and 91 %. We can see that the best performance of the mechanism in this floor corresponds to a cluster number of 8, with 2.9 m of mean error in localization estimation. It is noticeable that such accuracy value is suitable to be considered for access control, and most taking into account the common services provided in smart buildings and their service areas.

Table 2 Accuracy in location data

Number of clusters	Accuracy in positioning (m)
$K_{\text{auto}} = 3$	6.1
$K = 4$	5.1
$k = 5$	3.8
$k = 6$	4.0
$k = 7$	3.4
$k_{\text{opt}} = 8$	**2.9**
$k = 9$	4.0

Bold value indicates the best performance of the mechanism

Table 3 Deviation in the landmark position (σ_l), accuracy in location estimation (ε) and deviation in the accuracy associated (σ_ε)

Landmark	σ_l (m)	ε (m)	σ_ε (m)
1	0.2	5.8	4.2
2	0.1	2.8	1.8
3	0.3	0.1	0.1
4	0.1	7.5	3.6
5	0.1	4.5	3.1
6	0.2	4.8	4.6
7	0.1	2.5	1.8
8	0.1	3.4	2.4

Considering our location-aware authorization mechanism, the cluster number (landmark's number) established will affect directly the accuracy in the computation of the distance between subject and landmark. For access authorization, such distance should be smaller than the associated deviation of the magnetic field centroid of the landmark. Therefore, we calculate such distance considering only the magnetic field parameters. The deviation values associated to every landmark are obtained after the clustering of the magnetic field dataset collected in the off-line phase of our localization system.

Therefore, in this point we show in Table 3 the values associated to the deviation of each one of the 8 landmarks identified after clustering, as well as the mean and deviation accuracy values of each RBF implemented for each one of these 8 landmarks. From these results, we can see how it is possible to achieve very accurate localization results, and most considering the fact that there is a low number of different sources of magnetic field perturbation in the scenario under analysis, which is a constraint of the current solutions that follow the same approach for indoor localization.

Using these results, we obtain the box plots of the three configurations with the best associated location results, see

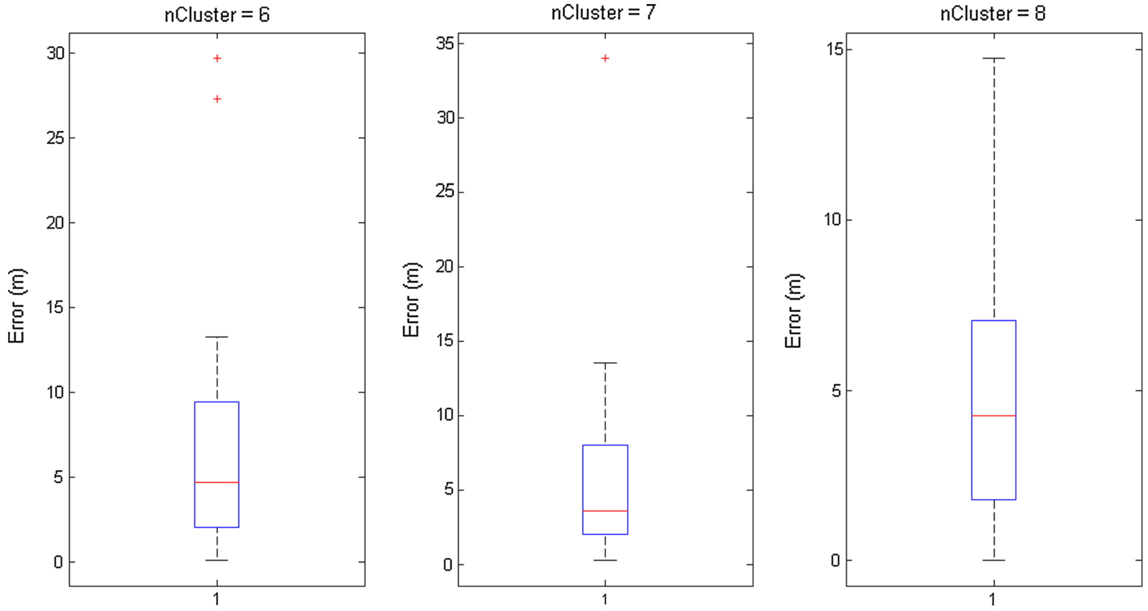


Fig. 7 Box plots for different numbers of clusters

Fig. 7. The numerical results are graphically depicted by their quartiles. The lines extending vertically from the boxes (whiskers) indicate variability outside the upper and lower quartiles. Using 8 landmarks, we achieved low dispersion among the results and a suitable degree of mean accuracy in the location data, providing a success value of 75 % in classification, and an error of 2.9 m in localization estimation. Therefore, 8 landmarks were considered suitable to generate the magnetic field map of the target corridor, and implement a RBF network for every zone in the building associated to each one of these 8 landmarks.

For a more complete assessment of the proposal to use the magnetic field for indoor localization, we present a comparison of the localization results achieved by our mechanism with those provided using another phone-based technology and considering the same test scenario (i.e. the corridor shown in Fig. 6). With this comparison, we intend to validate the results obtained with our proposal of indoor localization system comparing with the results of another system already validated as feasible solution in indoor environment and currently being used for solving such problem.

Following the approach of using WiFi signals for indoor localization, Garcia-Valverde et al. (2013) proposed a localization system which receives WiFi signals from a number of existing WiFi access points with no prior knowledge of the location of the access points and the environment. This system provides the percentages of success in the classification performed to predict location. Therefore, its level of granularity is in terms of building's zones. In this sense, we can take into account the zones resulting from the clustering mechanism applied in our localization system (which is based on the magnetic field distribution), and compare the classification results provided by the system based on using WiFi measurements. This WiFi-based localization system was developed in the University of Murcia and evaluated in different buildings of the same university. It is noticeable that it provided the most accurate results in the building of the Computer Science Faculty, since in this building the number of access points deployed and available to be used by this system is high.

In Table 4, we show the classification success results obtained with both systems. By considering the surface of the target zones, we can provide an approximate error for the WiFi-based localization system. The mean values are 73 % for WiFi and 75 % for magnetic field measurements. Considering the surface of each zone involved in the classification, a mean error of 7.6 m can be obtained using WiFi, and 6.1 m using magnetic field. But note that after this classification, our localization system provides more accurate estimates applying a regression technique to the magnetic field data associated to the zone resulting from the classification (results collected in Table 3). Nevertheless, it is previously necessary to carry out successful classification to ensure the accuracy of the location data.

Analyzing the results obtained from these two phone-based solutions to indoor localization, it can be seen that the WiFi-based system is more sensitive to the problem of adjacent zones, most of the classification errors occur in positions close, but belong to different adjacent areas. This is mainly due to the variable distribution of wireless signals in an indoor environment. However, the magnetic field-based localization is more sensitive to resolve the problem of distinguishing zones where the magnetic field variability is low, as between zones 3, 4 and 5 in Table 4.

Table 4 Success in location classification considering WiFi and Magnetic Field

Zone	Surface	Success using magnetic field (%)	Success using WiFi (%)
1	6.1 m × 6.1 m	88	75
2	3.2 m × 3.2 m	87	54
3	3.2 m × 3.2 m	70	57
4	3.2 m × 3.2 m	65	76
5	3.2 m × 3.2 m	68	92
6	3.2 m × 3.2 m	73	88
7	3.2 m × 3.2 m	75	68
8	3.2 m × 3.2 m	74	73

Table 5 Average time and deviation of the token evaluation stages for 50 tests

Stage	Average (ms)	Deviation (σ)
Request signature validation	213.9	0.7
Token signature validation	214.3	0.8
Rest of processing	79.9	5.1

6.2 Token evaluation

According to the proposed scenario, the main elements of our location-aware access control mechanism are the subject and the smart object. The former have been implemented in a common smartphone whose features have been described in the previous section. In a real deployment, it is expected that non-expert users are able to communicate with surrounding smart objects via their mobile devices such as smartphones or tablets. Moreover, the smart object of our scenario was implemented in a JN5139 mote equipped with Contiki OS. JN5139 is a low power and low cost wireless microcontroller with 16 MHz clock, which is suitable for IEEE802.15.4 applications. These devices will be instantiated by resource-constrained devices in the context of smart buildings, such as lamps or door locks.

To demonstrate the feasibility of our solution, we executed 50 tests of the token evaluation stage by taking into account the landmark values and magnetic fields measurements. The results are shown in Table 5 with a minimum time of 494 ms, and a maximum of 522 ms. The average time for the test suite is 508 ms, which represents around a 6 % increase compared to the results from Hernández-Ramos et al. (2013). This time includes the Round-Trip delay Time (RTT) since the subject does not send the request until she gets the authorization response. At this point, it is worth mentioning that this time assumes that the subject is authorized to perform the action and, therefore, all steps of the authorization evaluation must be completed. In the case any of the steps in the evaluation fails, the authorization process will be immediately aborted, without carrying out all authorization steps. Therefore, in case the subject is unauthorized, the time to get the decision will be always lesser. This positively affects the energy consumption of the smart object, since fewer operations would be required.

Table 5 shows the partial times that have been obtained from each of the tests. According to the results, and as expected, the most expensive phases correspond to stages where cryptographic operations are required. In particular, times for subject authentication and issuer's signature validation are very similar, since those times are mainly determined by our optimized ECDSA signature validation algorithm. However, it is worth mentioning that unlike most previous proposals in smart environments, our ECC optimizations have allowed to embed this functionality into constrained devices. Moreover, the remaining time includes the stage to assess if the user is inside the same building's zone where the smart object is placed and other tasks to validate the capability token which are described in more detail in Hernández-Ramos et al. (2013).

7 Conclusions and future work

Recent advancements in wireless communications and ambient intelligence are dramatically changing our perceptions of common physical places towards an integrated vision of smart objects as part of surrounding spaces. In these emerging scenarios, traditional access control mechanisms have to face new security risks since constrained devices are seamlessly integrated into the Internet infrastructure and can be accessed *anytime* and *anywhere*.

To overcome these challenges, this paper has introduced a novel location-aware access control mechanism in which authorization decisions are based on the combination of user location data and access credentials. Our proposed scenario has been designed by considering the constraints imposed by the use of resource-constrained devices, as well as the requirements of smart environments regarding flexibility and heterogeneity.

Specifically, this work has presented a novel localization system based on magnetic field measurements, which are provided by current smartphones' magnetometer. In our approach, smart objects are not required to process the location data set related to whole building space but only the building's zone where they are placed. This design has enabled location estimation functionality is embedded into smart objects, and consequently, additional hardware or infrastructure is not required. Our localization system is composed of two phases. During the off-line phase, building's maps containing magnetic field features are generated, and the mechanism to estimate location data is implemented. Then, in the on-line phase, users provide the magnetic field measurements from their phones and these are translated into their associated location positions. We have performed some experiments to validate this localization system in terms of accuracy achieved in location estimates. From these tests, a mean accuracy value of 2.9 m is achieved in a building's zone of 28 m long. This result is precise enough to be considered for our access control mechanism taking into account the usual services which are commonly considered in smart buildings. Furthermore, the proposed location-aware authorization engine has been implemented taking into account the constraints of the existing smart objects in terms of communication and processing power. The capability token design and ECC optimizations have enabled expensive cryptographic operations are embedded into resource-constrained devices. These foundations have made possible its development and evaluation over a real platform based on the Jennic/NXP JN5139 chipset. The time required for the evaluation of the capability token has been around 0.5 s, making it totally feasible for a real environment. Therefore, in our location-aware access control mechanism, no intermediate entities are required, offering the benefits of a decentralized approach for smart environments in terms of end-to-end security, scalability, interoperability, and flexibility.

The current working line is focused on testing the performance of our location-aware access control mechanism in a real smart building, specifically, the Technology Transfer Center at University of Murcia. [1] Furthermore, we are developing a fuzzy approach to address the uncertainty of our solution associated to the accuracy of our localization system. The future work will be focused on the behavior assessment of our access control mechanism when every smart object is not only aware of its building's zone, proposing to include larger magnetic field maps containing several landmark's characterization, and considering different building zones as evaluation scenarios. Moreover, given the degree of sensitivity of location information, we plan to explore the use of additional techniques for enhancing privacy, such as attribute-based signatures (ABS) as an alternative to ECC-based signature schemas.

Acknowledgments This work has been sponsored by European Commission through the FP7-IoT6-288455 and FP7-SOCIOTAL-609112 EU Projects, and the Spanish Seneca Foundation by means of the Excellence Researching Group Program (04552/GERM/06) and the FPI program (Grant 15493/FPI/10).

References

Altun K, Barshan B (2010) Human activity recognition using inertial/magnetic sensor units. In: Human behavior understanding, pp 38–51. Springer, Berlin

Andreu J, Angelov P (2010) Real-time human activity recognition from wireless sensors using evolvingfuzzy systems. In: 2010 IEEE international conference on fuzzy systems (FUZZ). IEEE, New York, pp 1–8

Angermann M, Frassl M,Doniec M, Julian BJ, Robertson P (2012) Characterization of theindoor magnetic field for applications in localization and mapping.In: 2012 International conference on indoor positioning and indoornavigation (IPIN). IEEE, New York, pp 1–9

Ardagna CA, Cremonini M, DamianiE, di Vimercati SDC, Samarati P (2006) Supporting location-basedconditions in access control policies. In: Proceedings of the 2006ACM symposium on information, computer and communications security.ACM, New York, pp 212–222

Atallah L, Lo B, King R, Yang GZ (2010) Sensor placement for activity detection using wearable accelerometers. In: 2010 International conference on body sensor networks (BSN). IEEE, New York, pp 24–29

Atallah L, Lo B, King R, Yang GZ (2011) Sensor positioning for activity recognition using wearable accelerometers. IEEE Trans Biomed Circuits Syst 5(4):320–329

Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. Comput Netw 54(15):2787–2805

Bao L, Intille SS (2004) Activity recognition from user-annotated acceleration data. In: Pervasivecomputing. Springer, Berlin, pp 1–17

Boles LC, Lohmann KJ (2003) True navigation and magnetic maps in spiny lobsters. Nature 421(6918):60–63

Breiman L (1996) Bagging predictors. Mach Learn 24(2):123–140

Breiman L (2001) Random forests. Mach Learn 45(1):5–32

Covington MJ, Long W, Srinivasan S, Dev AK, Ahamad M, Abowd GD(2001) Securing context-aware applications using environment roles. In: Proceedings of the sixth ACM symposium on access control models and technologies. ACM, New York, pp 10–20

Denning DE, MacDoran PF (1996) Location-based authentication: grounding cyberspace for better security. Comput Fraud Secur 1996(2):12–16

Ebinger P, Ramos JLH, Kikiras P, Lischka M, Wiesmaier A (2013) Privacy in smart metering ecosystems. In: Smart grid security. Springer, Berlin, pp 120–131

Ferraiolo D, Cugini J, Kuhn R (1995) Role-based access control (RBAC): features and motivations. In: Proceedings of 11th annual computer security application conference, pp 241–48

Friedman J, Hastie T, Tibshirani R (2000) Additive logistic regression: a statistical view of boosting (with discussion and a rejoinder by the authors). Ann Stat 28(2):337–407

Gao C, Yu Z, Wei Y, Russell S, Guan Y (2009) A statistical indoor localization method for supporting location-based access control. Mob Netw Appl 14(2):253–263

Garcia-Valverde T, Garcia-Sola A, Hagras H, Dooley JA, Callaghan V, Botia JA (2013) A fuzzy logic-based system for indoor localization using WiFi in ambient intelligent environments. IEEE Trans Fuzzy Syst 21(4):702–718

Gozick B, Subbu KP, Dantu R, Maeshiro T (2011) Magnetic maps for indoor navigation. IEEE Trans Instrum Meas 60(12):3883–3891

Gupta SK, Mukheriee T, Venkatasubramanian K, Taylor T (2006) Proximity based access controlin smart-emergency departments. In: Fourth annual IEEE international conference on pervasive computing and communications workshops, 2006. PerCom Workshops 2006. IEEE, New York

Győrbíró N, Fábián Á, Hományi G (2009) An activity recognition system for mobile phones. Mob Netw Appl 14(1):82–91

Haverinen J, Kemppainen A (2009) Global indoor self-localization based on the ambient magnetic field. Robot Auton Syst 57(10):1028–1035

Hernández-Ramos J et al (2013) Distributed capability-based access control for the internet of things. J Internet Serv Inf Secur 3(3/4): 1–16

[1] http://www.um.es/otri/?opc=cttfuentealamo.

Kanungo T, Mount DM, Netanyahu NS, Piatko CD, Silverman R, Wu AY (2002) An efficient k-means clustering algorithm: Analysis and implementation. IEEE Trans Pattern Anal Mach Intell 24(7):881–892

Katzakis N, Hori M (2009) Mobile phones as 3-dof controllers: a comparative study. In: DASC'09. Eighth IEEE international conference on dependable, autonomic and secure computing, 2009. IEEE, New York, pp 345–349

Kim JE, Boulos G, Yackovich J, Barth T, Beckel C, Mosse D (2012) Seamless integration of heterogeneousdevices and access control in smart homes. In: 2012 8th International conference on intelligent environments (IE). IEEE, New York, pp 206–213

Kunze K, Lukowicz P, Junker H, Tröster G (2005) Where am I: Recognizing on-body positions of wearable sensors. In: Location-and context-awareness, pp 264–275Springer, Berlin

Lane ND, Miluzzo E, Lu H, Peebles D, Choudhury T, Campbell AT (2010) A survey of mobile phone sensing. IEEE Commun Mag 48(9):140–150

Li B, Gallagher T, Dempster AG, Rizos C (2012) How feasible is the use of magnetic field alone for indoorpositioning? In: 2012 International conference on indoor positioning and indoor navigation (IPIN). IEEE, New York, pp 1–9

Luna F, Estébanez C, León C, Chaves-González JM, Nebro AJ, Aler R, Segura C, Vega-Rodríguez MA, Alba E, Valls JM et al (2011) Optimization algorithms for large-scale real-world instances of the frequency assignment problem. Soft Comput 15(5):975–990

Luoh L (2014) ZigBee-based intelligent indoor positioning system soft computing. Soft Comput 18:443–456

McGregor A, Hall M, Lorier P, Brunskill J (2004) Flow clustering using machine learning techniques. In: Passive and active network measurement. Springer, Berlin, pp 205–214

Melville P, Mooney RJ (2005) Creating diversity in ensembles using artificial data. Inf Fusion 6(1):99–111

Misra P, Enge P (1999) Special issue on global positioning system. Proc IEEE 87(1):3–15

Moses T et al (2005) Extensible access control markup language (XACML) version 2.0. Oasis Standard 200502

Mulligan G (2007) The 6lowpan architecture. In: Proceedings of the 4th workshop on embedded networked sensors. ACM, New York, pp 78–82

Ni L, Liu Y, Lau Y, Patil A (2004) LANDMARC: indoor location sensing using active RFID. Wirel Netw 10(6):701–710

Ofstad A, Nicholas E, Szcodronski R, Choudhury RR (2008) AAMPL: accelerometer augmented mobile phone localization. In: Proceedings of the first ACM international workshop on mobile entity localization and tracking in GPS-less environments. ACM, New York, pp 13–18

Oliveira LM, Rodrigues JJ, Sousa AF, Lloret J (2013a) Denial of service mitigation approach for IPv6-enabled smart object networks. Concurr Comput Pract Exp 25(1):129–142

Oliveira LM, Rodrigues JJ, de Sousa AF, Lloret J (2013b) A network access control framework for 6LoWPAN networks. Sensors 13(1):1210–1230

Ravi N, Dandekar N, Mysore P, Littman ML (2005) Activity recognition from accelerometer data. AAAI, Pittsburgh, pp 1541–1546

Rodriguez MD, Favela J, Martínez EA, Muñoz MA (2004) Location-aware access to hospital information and services. IEEE Trans Inf Technol Biomed 8(4):448–455

Shelby Z, Hartke K, Bormann C (2013) Constrained application protocol (CoAP). Constrained resources (CoRE) working group, internet engineering task force (IETF), work in progress, draft-ietf-core-coap-18. http://tools.ietf.org/html/draft-ietf-core-coap-18

Shi Y, Shi Y, Liu J (2011) A rotation based method for detecting on-body positions of mobile devices. In: Proceedings of the 13th international conference on ubiquitous computing. ACM, New York, pp 559–560

Simon H (1999) Neural networks: a comprehensive foundation. Prentice Hall, Upper Saddle River

Sun M, Hill J (1993) A method for measuring mechanical work and work efficiency during human activities. J Biomech 26(3):229–241

Wang Y, Zhao J, Fukushima T (2009) Lock: a highly accurate, easy-to-use location-based access control system. In: Location and context awareness. Springer, Berlin, pp 254–270

Weiser M (1991) The computer for the 21st century. Sci Am 265(3):94–104

Xin-fang Z, Ming-wei F, Jun-jun W (2011) An indoor location-based access control system by RFID. In: 2011 IEEE international conference on cyber technology in automation, control, and intelligent systems (CYBER). IEEE, New York, pp 43–47

Yang J (2009) Toward physical activity diary: motion recognition using simple acceleration features with mobile phones. In: Proceedings of the 1st international workshop on interactive multimedia for consumer electronics. ACM, New York, pp 1–10

Yuan E, Tong J (2005) Attributed based access control (ABAC) for web services. In: Proceedings of the 12th IEEE international conference on web services (ICWS), Orlando, USA. IEEE, New York

Zadeh LA (1997) What is soft computing? Soft Comput 1(1):1–1s