Best Effort Identification

Fábio Constantino

Instituto Superior Técnico (fabio.constantino@ist.utl.pt).

Abstract: This work presents a Best Effort Identification system which provides an identification service of people in the vicinity of a set of sensors. This service is intended to supply applications that create a customized interaction for each client with the needed identification information of this person. Typical approaches to obtain the identification of an individual, mainly based on the filling of forms, are often intrusive and time-consuming, making them unappealing. As such, this system intends to carry out the identification of individuals in a non-intrusive, automatic fashion, collecting available information, avoiding user interaction unless strictly necessary. The main focus of the system, in order to make good identifications, is the correlation of the collected data from the various sensors along with some external data, given their synergy. We expect this approach to facilitate the lives of marketers and improve the overall customer experience when using applications equipped with this system.

Keywords: Identification, Location, Middleware, Event, Sensor, Synergy

1. INTRODUCTION

In current times, almost every piece of information is placed online through several means. With the appearance of social networks, this has become even more evident, and almost everyone uses them. In an age where technology has reached a point that enables information to be gathered and analyzed with relative ease, having an identification of an individual leads to much more information about the subject through searches on the Internet.

Certain applications which serve a vast diversity of goals, such as an online store or a simple clothes shop in the supermarket, utilize information such as this about the people using them. This information must come from somewhere. The usual approach to this revolves around presenting a series of predefined boring questions to the clients, in the shape of forms, which most people don't have the time or patience to answer.

Given the slow and uninteresting nature of these typical information gathering systems, the need is rising to create something flexible and more advanced to captivate people's attention. A more interesting method would be to create a system which would gather this information in a non-intrusive, automatic fashion, allowing the users to focus on their task instead of wasting time.

As such, the focus of this work is to develop a middleware which can successfully identify individuals inside a coverage area, through the use of several sensors. Each sensor is programmed to sense a specific set of data and contribute its findings in the form of events, which will be managed by an event manager, reachable by every sensor. The captured data is then used to identify the individuals, prepare a rich information "package", filled with all the personal information known about the customer, and send it to applications (that have previously registered to the system) which will consume this information, generating personalized actions to each customer.

The main challenge here comes from the fact that it is not possible to program every sensor to generate 100% accurate identifications. Each of the sensors has a certain confidence interval which impacts the system as a whole. As identifications cannot be generated with zero margin for error from each sensor, it is necessary to correlate the data generated by several sensors in order to increase the confidence of the identifications made. The system will, thus, exploit the best features of every sensor in order to learn about the individuals inside the coverage area, combining this information with other relevant external data.

2. STATE OF THE ART

In the development of this work, a rich bibliography was analyzed, ranging from methods and algorithms for multi-sensor data sensing, Wi-Fi localization and biometric identifications, to social network data mining and some insight on the potential of smart cards. Only the most relevant parts of the state of the art will be detailed here, given their importance for the developed solution.

Multi-sensor data sensing brings the concept of data fusion techniques which combine data from multiple sensors, and related information from associated databases or relevant external data to achieve improved accuracies and more specific inferences than could be achieved by the use of a single sensor alone. While this concept is not new, the emergence of new sensors, advanced processing techniques, and improved processing hardware make real-time fusion of data increasingly possible [5].

As for what concerns Wi-Fi localization techniques, indoor radio-location systems were considered. These consist of two separate hardware components: a signal transmitter and a measuring unit (where most of the system "intelligence" is placed) and can be classified on the signal types (infrared, ultrasound, ultra-wideband, and radio frequency), signal metrics (AOA: angle of arrival, TOA:

time of arrival, TDOA: time difference of arrival, and RSS: received signal strength), and the metric processing methods (triangulation and scene profiling). Systems based on AOA, TOA or TDOA have been proposed and have reportedly achieved good precision, however, these measurements necessitate special hardware at either the infrastructure side or the client side which contributes to increase the cost of these solutions and makes its use intrusive. Since received signal strength (RSS) measurement is based on a sensory function already available in most 802.11 interfaces, RSS-based indoor localization therefore receives significant attention. Literature can be found on some of the current existing techniques for indoor localization: [7], [9], [2], [14].

The literature on biometric identifications was the most extensive, given the many different types of biometric sensors available, having [10], [11], [3] and [8] among the most relevant. However, more emphasis was given to facial recognition which seemed most adequate for this system. A facial recognition system is a computer application that allows for an automatic identification or verification of a person from a digital image or video frame from a video source. This is done by comparing the collected facial features from the image with a facial database. Face recognition systems usually proceed by detecting the face in an image, estimating and normalizing it for translation, scale and in-plane rotation. Given a normalized image, the features are extracted and condensed in a compact face representation which can then be stored in a database or smart card and compared with face representations derived at later times.

Given that social networks represent not only an online socialization platform but also a sort of database of knowledge about each of the users, a new topic comes to mind: information extraction. From the several current social networks, Facebook was chosen since it is currently the most widely used one. More recently, in order to facilitate the work of developers, Facebook made available a tool by the name of "Graph API"[13] which presents a simple, consistent view of the Facebook social graph, uniformly representing objects in the graph (e.g., people, photos, events, and pages) and the connections between them (e.g., friend relationships, shared content, and photo tags). From a business perspective, this tool would *"give marketers new ways to make sense of a user's preferences, passions and connections, which are the 'objects' of their lives."*[15].

By definition, a Smart Card is an electronic device that can participate in an automated electronic transaction, with security, and is not easily forged or copied [6]. Smart cards are also a very portable technology enabling their users to access privileges virtually anywhere. They will be able to insert their cards into computers, telephones or terminals that are equipped with smart card readers, turning a generic device into a highly personalized one. The three core functions of smart cards are:

- Information storage and management
- Identification of the card holder
- Calculation (especially for encryption/decryption)

This gives a short summary on the current state of the art considered for the development of this work.

2.1 Contributions and paper structure

The main contribution of the paper consists in the experimental demonstration of this best effort identification system which correlates information gathered by various sensors, into more complex, meaningful data, leading to the adequate identification of individuals inside an area of interest, and the subsequent association to their personal profiles.

The paper is organized as follows: After the introduction in which the work is motivated, a short literature review is made and the main contributions are presented, the problem addressed is formulated in section 3. Sections 4 and 5 describe the system architecture and implementation respectively, and section 6 presents the experimental results obtained. Finally, section 7 draws conclusions.

3. PROBLEM FORMULATION

The developed work proposes a middleware that aims to provide a best effort identification service of people around a set of sensors to registered applications, based on the available information. Each sensor will gather particular features of an individual, such as network communications made by their mobile devices through Wi-Fi, an image of their face, the use of an identifying smart card, among others, generating special events containing information about the collected features. Identification will then be inferred from all the information collected given the synergy between the sensors/features - "The whole is greater than the sum of its parts". It is the correlation of the data being generated by each sensor that will constitute the core of this work, leading to better and more complex identifications.

Since most of the information that this middleware intends to use is already made available by the users, even if indirectly, all that needs to be done is capture the identifying attributes of a given individual in order to make an online search.

After identifying an individual, many things about him can be found, especially through searches in social networks, such as personal information (sex, age, address, work place, etc.) or things that interest them (products, brands, groups, etc.) effectively creating a profile for that individual. This middleware also aims to provide the service to as many people as possible, making use of various sensors for different types of sensing. This will allow for an identification even if an individual does not have the necessary attributes for all the different types of sensors. However, the more information extracted from a single individual, the more accurate the identification will be.

The service provided by this middleware will allow marketers to have more information about their customers, enabling them to provide a better service. Service will improve by, for example, making good suggestions of products the customers might enjoy, given the profiles created by the system. This will facilitate the work of the marketers and will improve the overall experience of the customers, serving them better.

All of the information used by this system is gathered respecting the privacy of the users.

4. SYSTEM ARCHITECTURE

The system created here acts a middleware, serving applications that have registered in the system. These applications expect to receive information about people inside certain areas of interest, allowing some personalized action or information to be presented to that person. As such, the main focus of this work resides on the identification of individuals that enter these areas of interest which consist of the coverage area of a set of sensors. These sensors could be of many different types, but what is important is that each of the sensors is capable of sensing a particular set of data. Relevant data is defined as the personal characteristics of each individual, which may come from different sources, but all have something that is specific to that user and adds knowledge to the system. This relevant data is not only comprised of identifying attributes of the individual, but also information that is somehow connected to this person, which serves to create a user profile. After an identification is made, all information about that given individual is sent to the registered applications.

For the system to be able to provide good quality of service for the users, a set of system requirements must be ensured.

(1) The identification of the individuals should be as non-intrusive as possible, i.e. the interaction between the user and the sensors should be as little as possible and adequate to the level of identification requirement.
(2) The system should try to identify as many people as possible, relating information gathered from the various sensors in order to gain more information.
(3) Identification must be made in a time window that makes sense to the business logic.
(4) Disclosure of private information should be explicitly controlled by the users.

4.1 The sensors

In this architecture, four different types of sensor were implemented. They are: Wi-Fi sensor for mobile devices; Smart card sensor; Biometric sensor (Kinect) for facial recognition; Social network (Facebook) sensor. Each of these sensors will collect specific kinds of data and were chosen considering that simplicity and ubiquity were desired.

- The Wi-Fi sensor will scan for the periodic communications made by Wi-Fi devices. Wi-Fi capable mobile devices are something which is nowadays used by everyone and their Wi-Fi communications contain some powerful data, such as a unique identifier and location information.
- The smart card sensor will make use of identifying smart cards in order to retrieve as much information as possible, by accessing the card's data. These smart cards are small, very portable items, packed with important and useful features, namely authentication and the storage of personal data. Looking at citizen cards, which nowadays are also smart cards, this becomes another item which is also used by everyone.
- Facial recognition is an identification technique which is performed over images of an individual's face, which by using the biometric sensor, can be captured easily and analyzed. Again, this is usable by everyone, as long as a non-obstructed face is presented.
- Finally, the social network sensor will complement the profile of an individual with his publicly available information on this person's Facebook page. The choice of the social network was obvious, since it is the current number one social network in the world, and the number of people using it is very large and is continuing to rise.

As can be seen, each of the sensors is equipped with very distinct sensory capabilities. They will capture different types of data in very different ways and it is important that each of the sensors performs well to guarantee a smooth operation of the overall system. One of the most important parts for this is the collection and management of the available data. As was just mentioned, each of the sensors operates in a very specific way and the data each one collects is unique, however, in order for the system to function correctly, the data must be analyzed properly by a common unit to every sensor, which can process the information from each of them and make sense of it as a whole. Therefore, when one of the sensors captures meaningful data, it must be able to send it to the system, and this is done in the form of an event. The information captured by the sensors is encapsulated in events and sent to an event management unit, which is programmed to receive them and take some sort of action upon them.

The events generated by these sensors will be correlated by the event manager which consumes them, stores them and generates new events. By storing information the event manager will enrich its knowledge, thus allowing for the generation of more complex events. One of the relevant aspects for the effective correlation of the events is the combination of localization and timing. The sensors will, as best as possible, tag all the events generated with the spatial-temporal location of the individual that originated it. This feature will effectively allow the middleware to decide that several events generated in the same spatial-temporal area, relate to the same individual.

Figure1 illustrates the network topology used.

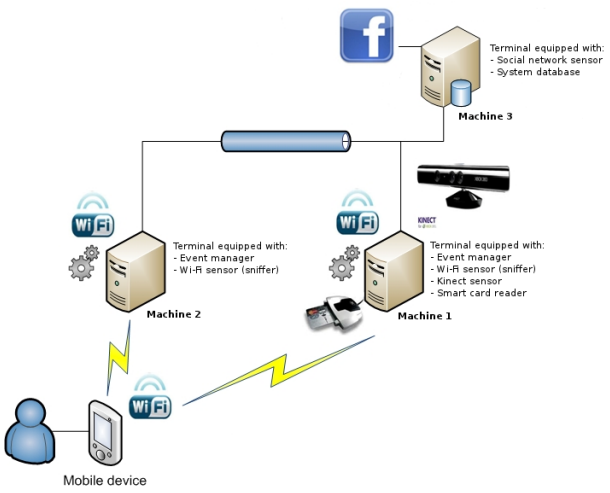

Fig. 1. Network topology of the developed system.

4.2 Confidence levels of identification

One of the most important characteristics of this system is the fact that it deals with a lot of uncertainty. Each of the sensors chosen have a specific margin for error which must be taken into account in order to produce good results. As the title of this dissertation suggests, the system operates on a best effort premise, and as such, most of the times, the information generated will not be 100% accurate. The most challenging aspect of this work is precisely dealing with these uncertainties in such a way, that by looking at several events generated from different sources, more information can be inferred, producing better results even if the original pieces of information were not very reliable. A case where this can be easily demonstrated is when capturing Wi-Fi information in the coverage area. Even if the Wi-Fi sensor is working perfectly and generating extremely accurate information, the information itself is mostly useless. The applications registered in the system would have no use for information about a random Wi-Fi capable device in the coverage area. The same happens with facial recognition, as an image of a face alone also means nothing. It is the fact that this information can be correlated that makes this work interesting and worthwhile for the registered applications, e.g. if the Wi-Fi information previously captured could be associated with an individual, this would provide an accurate identification in future visits by this person. Also, if the previously captured face image could be matched against a training facial database which contained sample images of registered clients, an identification could be performed with that face image.

After such associations are made, the system has much better means of identifying individuals in the area. This identification can come from an event generated by a single sensor, given a correct association to this type of sensor had been done previously. But again, each sensor has a specific error margin, which means that identifications made from different sensors would have distinct accuracy. To manage this, each identification made has its own confidence level corresponding to which and how many sensors participated in that identification.

5. IMPLEMENTATION

After presenting the system architecture, this section will provide the core implementation details for each of the relevant parts of the system.

5.1 Development Environment

All of the work done for this system was developed over machines running Linux Debian based distributions, Ubuntu 11.04 and Debian 6.0.5. Most of the programming done was written in Java with the assistance of external Linux programs. HTML and PHP were also used for web development, Python and C++ for programming some of the face recognition functions, and MySQL to create the system database along with JDBC to access it using Java. The entire development was made using Eclipse, a multi-language software development environment comprising an IDE and an extensible plug-in system.

5.2 Social network sensor

Facebook was used for this part of the work as it is currently the most popular social network around, contains a lot of useful information, is very easy to use, and offers several important development tools through its Graph API. It consists of a big network of people which have their own profiles available online, filled with as much personal information as the user chooses to upload. The system presented here has a lot of use for information such as this in order to profile and identify individuals.

In order to protect the privacy of the individuals in the system's coverage area, personal information will only be gathered and used if the individual is already a registered client in the system. To provide this feature, a small registration step is required, having the user simply do a Facebook login on the system's Facebook page. By using Facebook's Graph API, it is possible to create a registration method using an information disclosure agreement, which, if accepted, successfully registers the new client in the system. This registration method was chosen taking into account the fact that people do not want to waste their time with boring registrations, and that the login feature in Facebook is fast, simple to use and is known to everyone using this social network. At the time of registration, if the information disclosure agreement is accepted, all information from the user is pulled from Facebook by the system and stored in a database.

All the data collected by this sensor is used to create a personal profile for that client, and used in associations with the information gathered by the remaining sensors.

5.3 Wi-Fi sensor

This sensor will monitor the network, searching for wireless signals which correspond to potential customers. It is composed by the receiver, a simple Wi-Fi card in monitor mode, and the transmitter, the user's mobile device. Since ubiquity is desired, the choice for these two components was very straightforward. A Wi-Fi card is now a very common component in any computer, and having the users' mobile devices serve as the transmitters removes the need for any other specialized hardware that the user would need to carry otherwise (very intrusive).

This sensor was developed using *tcpdump* and *iwlist* managed by a Java program, and *aircrack-ng* to set the Wi-Fi cards to monitor mode.

The capture of network information comes in the form of network packets which are sent in the effective range of the sensor. When doing this type of sniffing, every single packet in the area is captured, and thus, some filtering must be done as the only relevant information here are the packets being sent by the mobile devices of the clients. Since every Wi-Fi device has a unique identifier, the MAC address, it is easy to identify and differentiate incoming packets, grouping them up based on their types. In order to filter the relevant data, all MAC addresses originated by access points are discarded, leaving only the client communications to analyze.

Network information captured by this sensor contains the Received Signal Strength (RSS) which is very useful to

try and locate the mobile device who sent the signal. By having more than one Wi-Fi sensor, these sensors will communicate with each other about which W-Fi signals they see. If all Wi-Fi sensors see the same MAC address, and it is within an acceptable power range, it is determined that the device is inside the coverage area, and represents a potential customer.

Relevant information such as this is then encapsulated in the form of an event and sent into the event manager to be analyzed and associated to events received by other sensors.

5.4 Biometric sensor

For the biometric sensor, face recognition was the method chosen to perform identification of individuals. This type of sensor was chosen given its innate ubiquitous nature, especially when compared with other types of biometric sensors, and the fact that biometric information is provided when a user registers in the system, the Facebook profile picture.

The facial recognition part of this work was developed using Microsoft's XBOX360 Kinect as the sensor; OpenKinect to provide the open source drivers, *libfreenect*, that enables the Kinect to be used with Windows, Linux and Mac; OpenCV as the library of programming functions for real time computer vision; *haarcascades* to perform face detection in the video frames or pictures of the individual; *libfacerec* as a complement of OpenCV for more specific recognition functions. A Java wrapper, JavaCV, was used to integrate this development section in the remaining code, and a Python wrapper was used in order to be able to program both the Kinect interactions and the face recognition algorithm in the same language.

To do face recognition on pictures or video frames from a live video feed, several steps must be followed. The first step is to train the recognition system with a set of facial pictures to be able to later have a matching set for the test pictures. This set of training facial pictures will come from the system's face database, comprised of the profile pictures collected from each individual upon their registration on Facebook, Smart Card pictures in case the client uses the Smart Card sensor, and some video frame captures which are stored in very specific conditions. Every face image will be stored in the face database, identified by the clients' respective Facebook id.

However, the images need some pre-processing before being used to clean up the facial image for easier recognition. In this solution, the following pre-processing methods were used:

(1) Resize of the images, so that every picture is in the same resolution.
(2) Converting the color image to *greyscale*.
(3) Apply Histogram Equalization for consistent brightness and contrast of the facial images.

After the training set has been completed, the system is ready to receive new facial images to compare with the already known ones and identify the individuals. These test images will come from the video frames captured with the Kinect and from the smart card facial images. Pre-processing is also done on the test images, as they do not come in the correct format for recognition. After they are pre-processed, a matching algorithm is used to compare the test images with the ones in the facial database and determine which of the stored faces is most similar. For this, the Local Binary Patterns Histograms[1] (LBPH) method was used, along with the TanTriggs[12] processing method which provided the most accurate and robust identification when compared to the Eigenfaces and Fisherfaces methods (most commonly used methods).

This sensor is also capable of determining the distance at which a person is from the camera, by using the Kinect's Depth feature. By measuring this distance, location information can be inferred for this client, adding to the knowledge of the system.

5.5 Smart card sensor

The smart card sensor was also implemented in this work, providing a strong identification element, when an unequivocal identification of an individual is required. This is the most intrusive part of the developed system, since it requires the user to have an interaction with the system by inserting his identifying smart card into a reader. Given that some applications might need this strong identification, it justifies its use.

This type of sensor was chosen taking into consideration that most countries already make their citizens carry a citizen card, which is a secure smart card containing authentication applications which identify an individual in a safe and reliable way, and are not easily forged or copied. The fact that these cards are nowadays part of everyday life and people always have them on their person, and having the smart card be a relatively small and light product, minimizes the intrusiveness of the sensor.

This sensor is composed of a reader, the *gemalto* PC USB-TR, and an identifying smart card, the Portuguese Citizen Card. It was implemented in Java, using the *pteidlib* as the API to retrieve information from the card.

Upon the insertion of the card, communication with it is initialized and all relevant information about the client is retrieved. This is easily done with the functions provided by *pteidlib* which serves to abstract the low level, much harder to understand Protocol Data Unit (PDU) communications. This action will also trigger the generation of a "smart card event" which is sent to the event manager, trying to figure out if the card belongs to a registered user. When the event is received by the event manager, the system will look in the known users database searching for users with similar attributes.

5.6 Event manager

As has been mentioned along this dissertation, the implemented system makes use of several sensors, each capable of sensing a different type of feature. These sensors are constantly collecting data and need to feed it to the system in order to make sense of it. As such, each of the sensors will generate an event when meaningful data is captured and feed it to applications or services which generate new events on their turn. To provide this feature,

an event management unit was chosen in order to correlate events generated by the various sensors. This will allow the system to generate more complex and meaningful events, leading to more information and a better identification of a person.

Esper[4] was chosen taking into consideration that it is Open Source Software (OSS), well-documented, designed specifically for real-time architectures, and written in Java, providing an easy programming interface and is suitable for integration into any Java process. It enables rapid development of applications that process large volumes of incoming messages or events. It filters and analyzes events in various ways, and responds to conditions of interest in real-time. While discrete events when looked one by one might be meaningless, event streams, i.e. that is a continuous set of events, considered over various factors, such as time or location of occurrence, and further correlated, are highly meaningful, providing the applications using the middleware with enough information to take decisive action.

Esper basically instead of working as a database where data is stored to later poll it using SQL queries, works as a real time engine that triggers actions when event conditions occur among event streams.

The event manager is essentially a software component which is prepared to receive events from multiple sources, passing each one through defined rules which will analyze these events and decide if action needs to be taken upon them.

5.7 System learning

Many times along this paper, associations between data from the sensors and the clients' personal profiles has been mentioned. It is a very useful and core feature in this work, although, it is not error free. Since at times many customers may be inside the coverage area, doing similar actions at the same time, some confusion might be generated. The most common type of mix-up happens with network information being associated to the wrong people, given their close proximity at the time of identification and different power output levels of different mobile devices. To try and fix these kind of issues a learning mechanism was also implemented. It's function is to look at identifications of individuals and comparing them to a previous stored history, thus removing previously associated wrongful information and at the same time avoiding the addition of bad data. This will strengthen the confidence level of the correct data, contributing to the better functioning of the entire system, producing more accurate identifications. This mechanism works by making use of another very important external feature: repeated visits by the clients.

5.8 Final output

After an identification has been made, something must be sent to the applications registered in the middleware. As such, all the information contained in an identification event is converted into XML format using *xstream*, making it ready to deliver to the applications. XML format was chosen since it provides simplicity, generality and usability. This *xstream* library also simplifies things, since it is capable of serializing Java objects into XML and back again through a very simple API, making the conversion of any type of event a breeze. The fact that XML is a universally accepted language, using this type of output will make it simple for any application wanting to use the middleware, to read and parse the output though one of the many available APIs for XML parsing.

6. EXPERIMENTAL RESULTS

The main focus of this work has always been the identification of individuals. This identification is to be done through several sensors, each of them collecting a specific kind of information, but what is most important is the information gain by correlating the data being generated by the various sensors, along with extra information such as time, location, and repeated visits of the customer.

In this section, various test scenarios are presented, and the information collected, along with its confidence level is shown for each identifying sensor, as well as for the overall system.

The test environment consists of a small room with 2 computers, each equipped with a Wi-Fi sensor and placed on opposite sides of the room, having the Kinect and smart card sensor placed on the furthest machine from the entrance. The social network sensor and system database are placed in another computer, not present in the room. Throughout this chapter, the machines will be referenced as machine 1 (computer at the end of the room, equipped with Wi-Fi, smart card, and biometric sensor), machine 2 (computer near the entrance of the room, equipped with a Wi-Fi sensor), and machine 3 (computer not present in the room, equipped with the system's database, and social network sensor). Every scenario presented contains at least one individual inside the coverage area, and every individual is equipped with a personal Wi-Fi capable device and identifying smart card (Portuguese citizen card). The machines are connected via ethernet. For testing, 7 clients were registered in the system.

The following test cases were created:

(1) Non-registered individual enters coverage area, walks to the end of the room, does a simple action in front of machine 1 and then leaves.
(2) Registered user enters the coverage area of the system for the first time and stays in the room for a while. During this time he walks around the room, stops to perform an action with his smart card and then leaves.
(3) Same user from test 2 re-enters the coverage area, walks around the room and leaves.
(4) Two registered users enter the room. User B stays idle near the entrance while user A walks to machine 1 and does an action requiring the use of his smart card. Both users leave at the same time, after user A's action is completed.
(5) User A from previous test enters the room with a different registered individual. They both walk around the entire room making quick stops at each machine and then proceed to leaving the area.

(6) Registered user carrying 2 mobile devices was identified by the system in an older visit. This same user now enters the room with only one of those mobile devices.

These test cases were chosen since they demonstrate how the system deals with most of the possible situations, and how the confidence levels in identification grows as the system learns more from the individuals.

For the evaluation of these test cases, a graph is produced to better illustrate the information gain of the system. It will show the confidence levels of the identifications done by the system over time, qualitatively evaluating these values over 3 different levels: low, medium, and high. It is important to note that the graph will depict the confidence level at each time, taking into account the amount of sensors identifying the individual at that given time and the amount of data that the system has for that person. Every time an identification is made, it is also displayed in the graph a simple annotation indicating which sensor(s) generated it, represented by the initials of their respecting sensors: w for Wi-Fi identification; b for biometric identification; sc for smart card identification.

6.1 Scenario 1 - Unknown individual

For this test scenario, no identification was produced. These results are expected since the user has not been registered in the system.

The individual's Wi-Fi signals were detected by both machine 1 and machine 2 while he was inside the room, however, since no association had been made to the collected MAC address, the system assumed it was from an unknown person. When the individual spent some time in front of machine 1, his face was captured by the Kinect camera and face recognition was attempted. However, it did not reach the accepted threshold, and therefore, was unable to identify this person.

6.2 Scenario 2 - Registered individual, first visit

This test was successful as identification events were generated from multiple sensors during the presence of the client. The best identification made was of the highest level possible, generated by the smart card sensor.

Figure 2 shows the graph of the confidence levels of identification throughout the experiment, based on the information gain of the system.

This scenario shows perfectly the various confidence levels in identifications produced over time. It starts out with the system only having social network information about the client, thus explaining the lack of Wi-Fi identification during the first moments. However, among the social network information in the system, a facial picture was present, providing the biometric sensor with the needed data to attempt recognition, which proved successful (seen at t2). A short while after, the client used his identifying smart card, providing the system with very important information, leading to a spike in the confidence values of identifications at that time (t3-t4) and associations being made to the information gathered by the other sensors. At t4, the individual removes his smart card, only being

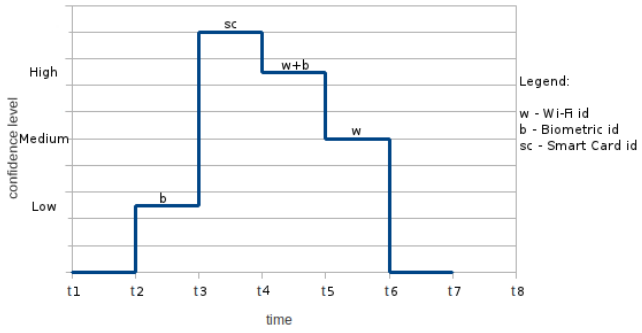

Fig. 2. Confidence level of identifications for scenario 2.

identified by the biometric sensor and now also by the Wi-Fi sensor (because of the successful association created at t3), leading to a much higher identification than at t2. After the user leaves the coverage area of the biometric sensor (instant t5) he is now only identified by Wi-Fi, and after leaving the room (instant t6), no identification is possible since he is out of the coverage area of the system.

6.3 Scenario 3 - Registered individual, repeated visit

This scenario is very similar to the previous one, once more including just one person (same client from the previous test), but this time the individual is not visiting for the first time, i.e. the system already has good associations made to this person and possesses a lot of relevant data in his profile. The results were good, as a correct identification of the individual was obtained. The best identification level achieved was "High" since this time there was no use of the smart card.

Figure 3 shows the results graph of this experiment.

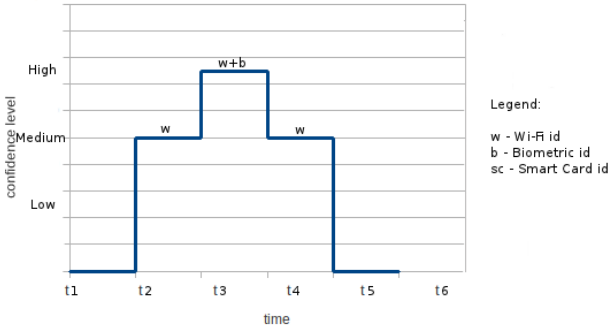

Fig. 3. Confidence level of identifications for scenario 3.

The purpose of this test scenario is to show that in a repeated visit by the client, the system is now able to immediately identify him as soon as network information is generated by his mobile device. This is now possible since in the previous test, an association of his Wi-Fi information was made to his personal profile, increasing the knowledge of the system. In this case, at t2, the first Wi-Fi signals were captured by the system, allowing the sensor to produce a correct identification. This identification will only carry a medium level confidence since the

client is, at this time, only seen by a single sensor. At t3 however, the client spends some time in the coverage area of the Kinect while also being detected by the Wi-Fi sensor, leading to the production of a more complex event, containing a higher information identification, with improved confidence. Instant t4 represents the time at which the user left the Kinect's coverage area, and t5 when the individual leaves the room.

6.4 Scenario 4 - Multiple registered individuals, first visits

This fourth scenario introduces the concept of multiple individuals in the test area at the same time. This particular test required the participation of two individuals, both registered in the system, where one of them (user A) walks around in the room and interacts with the smart card reader while the other person (user B) stands idle near machine 2. Both users were visiting the system's coverage area for the first time. The results produced by this test were expected, generating the highest confidence identification possible for user A and no identification being made for user B as shown in figure 4, having a line representation for each user.

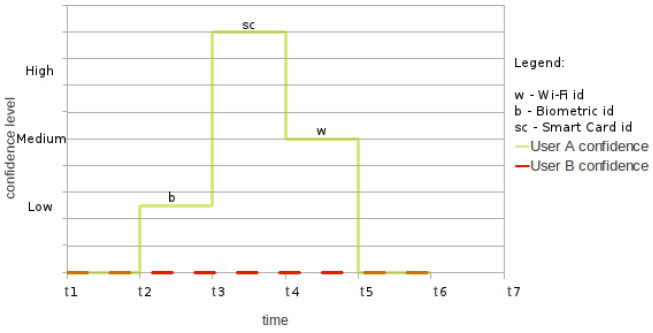

Fig. 4. Confidence level of identifications for scenario 4.

Since user B only stayed at the entrance, the only sensor capable of receiving any information about this customer was the Wi-Fi sensor. However, since it is his first visit, no association had been made and the system sees his network information as random Wi-Fi data, discarding it as if it belonged to an unknown user. User A on the other hand, did a route similar to the one made in test scenario 2, leading to very good identifications and associations during his time in the coverage area, being identified by the biometric, smart card and Wi-Fi sensors.

6.5 Scenario 5 - Multiple registered individuals, repeated visits

This test scenario brings no new information about the identifications being made or the confidence levels achieved, it serves only to better illustrate the difference in confidence from identifications made on clients with rich profiles and those with basic ones. Once more, two registered users enter the coverage area of the system. One of these clients, was also present in the previous test, user A. The other client (user C) is also entering the room for the second time, however, on his first visit, he did not use his identifying smart card, leading to less information gain by the system. To better demonstrate the difference in levels of identification between these two clients, the two individuals did the exact same route through the room, being subjected to the same tests. Figure 5 represents the various identifications done for the two clients, each one represented by a different line in the graph.

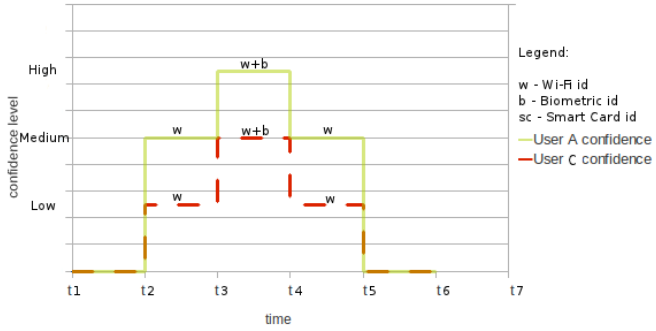

Fig. 5. Confidence level of identifications for scenario 5.

6.6 Scenario 6 - Registered individual, multiple mobile devices

This scenario served to test a "strange" situation. Since the part of the system being tested here is only referent to the associations made to the clients, no result graph is presented. For this test, an individual equipped with 2 Wi-Fi capable mobile devices is inserted in the coverage area of the system for the first time. This person walked around the room, having the Wi-Fi signals from both devices being detected by the respective sensors. This client was also identified by both the biometric and smart card sensors, effectively associating the Wi-Fi data in the area with the client. After these identifications and data association were completed, the client left the test area.

At a later time, the client entered the room once more, this time having one of the mobile devices turned off. Upon a second identification by either the smart card or biometric sensor, the learning mechanism came into play, removing the MAC address of the offline mobile device from the user's profile. Since this Wi-Fi identifier is now tagged as a bad association for this client, even if communications from this mobile device are detected in future visits, it will no longer be associated to the client even though it belongs to him. Only when none of the previously associated Wi-Fi identifiers are detected upon an identification of this individual (which clears the Wi-Fi data from this client's profile) will it be possible to associate this MAC address to that client again. This test served to demonstrate one of the features that the system is not currently equipped to handle, since it assumes that a client only carries a single personal mobile device. This would also be an interesting topic for future work, further improving the learning function.

7. CONCLUSIONS

In this work, a best effort identification system was developed. This system is composed of several different sensors,

each sensing a specific kind of feature, relevant for the identification of the individuals inside the sensors' coverage area. The main goal of this work was to take each of the features gathered by the sensors, correlating them in an event manager in order to produce better, more meaningful identifications, feeding applications registered in the system with personal information known about its clients.

The goal of this work was achieved, by setting up a diversity of sensors which contributed to the identifications, while keeping the system as ubiquitous as possible. As was presented in the results section, all this was possible by working with the information coming from the sensors as well as external data, such as timing, location and repeated visits by the clients. With this, the system is able to learn about its clients, leading to a more complete profile of each individual at each step.

This work could have been done in many different ways, producing more accurate information with lower recognition rates, or more identifications with a higher false positive rate. In the final version of this work, an intermediate solution was created, as to not limit the system too much. The confidence levels attached to every identification allow the applications receiving the information to have a better understanding of where the identifications are coming from and how much they can "trust" it.

REFERENCES

[1] Timo Ahonen, Abdenour Hadid, and Matti Pietik. Face Recognition with Local Binary Patterns. pages 469–481, 2004.

[2] Paramvir Bahl and Venkata N Padmanabhan. RADAR : An In-Building RF-based User Location and Tracking System. *Data Processing*.

[3] Biometricnewsportal. Face biometrics. `http://www.biometricnewsportal.com/face\_biometrics.asp`.

[4] EsperTech. Tutorials and case studies. `http://esper.codehaus.org/tutorials/tutorial/tutorial.html`, 2011.

[5] David L Hall, Senior Member, and James Llinas. An Introduction to Multisensor Data Fusion. 85(1), 1997.

[6] IBM. Multi-Application Smart Cards :.

[7] Kuo-fong Kao, I-en Liao, and Jia-siang Lyu. An Indoor Location-Based Service Using Access Points as Signal Strength Data Collectors. *System*, (September):15–17, 2010.

[8] Kyungnam Kim. Face Recognition using Principle Component Analysis. *Science*, pages 1–7.

[9] Hyuk Lim, Lu-Chuan Kung, Jennifer C. Hou, and Haiyun Luo. Zero-configuration indoor localization over IEEE 802.11 wireless infrastructure. *Wireless Networks*, 16(2):405–420, October 2008.

[10] P Jonathon Phillips and R Michael Mccabe. BIOMETRIC IMAGE PROCESSING AND RECOGNITION. *Technology*.

[11] Henry A Rowley, Student Member, Shumeet Baluja, and Takeo Kanade. Neural Network-Based Face Detection. *Analysis*, 20(1):23–38, 1998.

[12] Xiaoyang Tan and Bill Triggs. Enhanced local texture feature sets for face recognition under difficult lighting conditions. *IEEE transactions on image processing : a publication of the IEEE Signal Processing Society*, 19(6):1635–50, June 2010.

[13] Www.facebook.com. Graph API. `http://developers.facebook.com/docs/reference/api/`.

[14] Moustafa Youssef. Handling Samples Correlation in the Horus System. *Analysis*, 00(C), 2004.

[15] Mark Zuckerberg. Open Graph. In *f8 Developer Conference*, 2010.