Communication Protocol for the Guardian System aimed at the Protection of Mistreated People

Dante I. Tapia, Ricardo S. Alonso, Óscar García, Fabio Guevara
R&D Department
Nebusens, S.L.
Salamanca, Spain
{dante.tapia, ricardo.alonso, oscar.garcia, fabio.guevara}@nebusens.com

David Sancho, José A. Pardo, Antonio J. Sánchez, Juan M. Corchado
Department of Computer Science and Automation
University of Salamanca
Salamanca, Spain
{david.sancho, jose.pardo, anto, corchado}@usal.es

Abstract— Thousands of people (mainly women) are daily mistreated, battered and abused by their ex-couples or their current couples. In this sense, electronic surveillance can be an efficient tool for helping to guarantee the safety of victims. Ambient Intelligence (AmI), based on ubiquitous computing, represents a promising approach to make technology adapt to people in order to solve the challenge of developing strategies that allow the early detection and prevention of problems in safety environments and, more specifically, the protection of people under risk situations, including cases of mistreatment or loss. This paper describes Guardian, an integral solution designed for improving the protection of mistreated and at-risk people by means of the integration of GPS, GPRS and ZigBee technologies. The basic architecture of the system, the proposed wireless devices, as well as the communication protocol used between the system and the devices are described. Furthermore, a first hardware and software prototype is depicted and tested.

Keywords—Ambient Intelligence; Mistreatment; Safety; GPS; GPRS; ZigBee.

I. INTRODUCTION

According to statistical data from the Ministry of Interior of Spain [1], from 2006 to 2008 more than 60 women were killed every year by their couples or ex-couples in Spain. In 2008, a 23% of the killed women had filed a formal complaint against their murderers. In situations of violence against women exercised by husbands or couples, or in the framework of other emotional relations, the authorities consider the electronic surveillance as an indispensable tool for helping to guarantee the safety of victims.

In this regard, Ambient Intelligence (AmI) is an emerging multidisciplinary area based on ubiquitous computing and that influences on the design of protocols, communications, systems, devices, etc. [2]. Ambient Intelligence proposes new ways of interaction between people and technology, making the latter to adapt to the users' needs and the environment that surrounds them [3]. This kind of interaction is reached by means of technology that is embedded, non-invasive and transparent for users, whose main aim is facilitating their daily activities [4]. Nonetheless, the development of AmI-based systems requires the creation of increasingly complex and flexible applications. In this sense, the use of context-aware technologies is an essential aspect in these developments to perceive stimuli from the context and react upon it autonomously [4]. An environment capable of recognizing the presence of people, and locating them in a geographical and activity context is the base to Ambient Intelligence to demonstrate all its potential.

There are different approaches that propose electronic telemonitoring systems aimed at tracking victims and aggressors [5] [6] in order to reduce risk situations. Even though these approaches are based on locating and data transmission technologies such as GPS [7] and GPRS [8], they do not consider the problem of indoor locating, where satellite-based positioning systems as GPS do not work properly.

In this sense, this paper describes Guardian, an Ambient Intelligence based electronic system aimed at the location and protection of people under risk situations. These risk situations include prevention of aggressions to threatened people, as well as surveillance and care of children, elderly and other vulnerable people. Therefore, the main aim is developing a system capable to protect people under risk of being mistreated, assaulted or lost, in a totally autonomous way by means of multiple wireless electronic devices.

The Guardian system makes use of different wireless technologies, such as A-GPS [7], GPRS [8] and ZigBee [9], to provide the majority of its features. Therefore, this project involves the design and creation of a completely distributed innovative hardware and software platform. This platform will have to exceed the available systems currently available in the market, integrating all its functionalities through a powerful logic of middleware layers.

The rest of the paper is organized as follows. The next section describes the problem of protecting potential victims of domestic violence, as well as some existing approaches that try to solve this problem. Then, the main components of the innovative Guardian system are depicted, including the architecture of the system, the architecture of the wireless devices involved, as well as the communication protocol used between the distinct devices and machines in the system. After that, experiments and results performed in the first hardware and software prototype of the Guardian system are presented.
Finally, the conclusions and the future lines of work are depicted.

II. BACKGROUND AND PROBLEM DESCRIPTION

It is important to point out that, in Spain, the pressure over the assistance system is growingly increasing, as well as the necessity to offer services with more quality. As mentioned above, thousands of people (mainly women) are daily mistreated, battered and abused by their ex-couples or their current couples [1]. These mistreated people suffer from a lack of freedom and the violation of their most elemental rights.

This fact represents a complex challenge, which coincides with a crisis in the support systems that try to provide solutions to these necessities. In this scenario, the technology can play a decisive role. Initiatives such as the Guardian project, oriented to improve the assistance services for these population segments, involve a strategic relevance. Although the current number of incidents related to violence against women exercised by husbands or couples, or in the framework of other emotional relations, are increasingly more advertised than in the past [1], there are still hidden facts to be known. In such situations, one of the most important aspects is assuring that the potential aggressor and victim are physically separated by a certain safety distance. In this sense, there are several approaches developed during the last years with different features that try to solve the problem of locating and detecting the proximity between aggressor and victim.

There are approaches centered on monitoring and locating accurately the aggressor, such as the BI ExacuTrack® One system [5]. This system consists of a light, resistant and tamper-proof device that is worn by the aggressor on its ankle, offering long battery autonomy. The locating process is performed using a combination of several technologies, including autonomous GPS, A-GPS [7] and AFLT (Advanced Forward Link Trilateration) [10]. Using this combination of wireless technologies, the system can estimate accurately the position of the user, even in hard conditions, such as indoors, vehicles in motion or between high buildings. Nevertheless, in this system the energy consumption and the need of battery recharge are very exigent.

Other approach is the One Piece GPS System [6], whose main objectives are the device ubiquity, less necessity of device maintenance and robustness against tries of manipulation on the aggressor's device. This system includes an integrated active GPS device [7] that combines a GPS receiver, a microprocessor and different communication components in a wrist or ankle bracelet. In situations where the aggressor's device is close to restricted areas, the device sends notifications to the supervisor agents in real time through fax, e-mail or SMS. Supervisor agents can create inclusion or exclusion areas that surround a specific geographic location, as the victim's residence or work place. This implies an increase in the total cost of the system, as it requires a management of the electronic borders by the supervisor agents, as well as a previous learning process.

Considering the limitations of the electronic borders, Omnilink [11] proposes a dynamic tracking system which calculates the distance between victim and aggressor in real time. Its monitoring system allows agents to control the movements of the aggressor according to the movements of its victim, both indoors and outdoors. Using a combination of monitoring devices in victim and aggressor, the agents can control the proximity between both. If the aggressor is too close to the victim's home, work place or some of the exclusion areas, both the agents and the victim are notified. In addition, to support the electronic borders management, this solution allows calculating the proximity between victim and aggressor in real time and acting consequently through specific software in the data center. Although this proximity calculation represents an improvement over other systems, it is important to take into account that this calculation can be conditioned by possible congestions in the communication network or by low radio coverage according to the positions of victim and aggressor. In this sense, the Guardian system solves this limitation as the calculation of proximity between victim and aggressor is not delegated to other components of the system. Thus, the own tracking devices are the ones responsible for detecting each other at a certain distance and calculating it from the parameters of the received radiofrequency signals.

Nevertheless, these approaches do not cover completely indoor situations where GPS or GPRS coverage can fail or such approaches need to define and manage exclusion areas. In this sense, the Guardian system includes devices that integrate GPS, GPRS and ZigBee in the same wireless module, thus covering all situations in an autonomous way.

III. THE GUARDIAN SYSTEM

This section describes the main components of the Guardian system, whose basic schema is shown in Figure 1. First, the basic functioning of the system is depicted. After that, the different hardware modules that make up each wireless device are described. As this is a research work that will be finished in Q4 2012, this paper presents a preliminary description, as well as the last prototype of the system, which will be extended and published further on.

The basic functioning of the Guardian system is as follows. There are two kinds of users or roles in the system: the threatened or at-risk user and the potential aggressor. Both users carry a mobile device with A-GPS, GPRS and ZigBee capabilities. Both devices (the victim's one and the potential aggressor's one) obtain their position making use of their A-GPS module. This way, both devices send its position using GPRS to the control center where the Geographic Information System (GIS) is running. Therefore, the control center keeps track of the positions of both users. However, this information is not enough to achieve an efficient protection. This is because the GPS or A-GPS technologies do not properly work on some situations, as indoor locations (e.g., buildings or tunnels) [7]. In this point where the Guardian system makes the difference over the conventional systems currently available in the market.

The ZigBee technology [9] covers those situations where GPS or A-GPS cannot work correctly. In the Guardian system, the ZigBee module is used when users are nearly located. In addition, ZigBee is activated when there is no A-GPS or GPRS coverage. At this moment, both devices (the victim's one and
the potential aggressor's one) start searching the signal from the counterpart device. That is, the system uses the ZigBee’s signal strength between both devices in order to identify a potential risk. The transmission power of both ZigBee modules can be selected by software. According to this transmission power and the sensitivity of the antennas, the ZigBee signal range can reach even several kilometers. Therefore, if one of the devices detects the other one, it sends an alert to the control center using GPRS. If there is no GPRS coverage, both devices will raise visual and acoustic alarms, using the buzzers included in the devices. Furthermore, the control center keeps track of the last positions of both devices before the A-GPS or GPRS coverage was lost. This way, the control center determine if the distance between users and the last time before losing the coverage imply a potential risk for the threatened user.

Using the combination of the three wireless technologies (A-GPS, GPRS and ZigBee) the system is always operative and does not depend on an only technology to work. Thus, the Guardian system achieves a higher level of autonomy against other similar systems. Furthermore, the flexibility of the Guardian system allows that one of the used devices can be embedded into an object, such as an access door. This way, the system can also operate in a mode that allows controlling the access to protected areas.

In order to implement many of the features of the Guardian system, it is necessary to design specific devices that accomplish the criteria established in the project. To do that, the functional architecture shown in Figure 2 is proposed. This functional architecture is based on the n-Core Sirius devices from Nebusens [12], deeply described in the next section. Each n-Core Sirius devices includes an 8-bit RISC microcontroller, a ZigBee transceiver and several internal and external communication ports (including GPIO, I2C and USB/RS-232 UART) to connect to distinct devices, including sensors, actuators, as well as other electronic devices or even computers.

![Figure 1. Basic schema of the Guardian System.](image1)

The wireless devices used in the Guardian system are formed by different functional units or hardware modules interconnected to each other. Next, the main features of each of the units are briefly described.

- **Charge and power supply**: consists of a portable power supply system, that is, a rechargeable battery and a charge and power supply system. The charge system will be implemented in the same module and will allow charging the battery through a USB port.
- **USB**: communication interface between the device and a personal computer. On the one hand, it will allow configuring the device. On the other hand, it will allow charging the internal battery.
- **GPS**: this is the module responsible for obtaining the coordinates with the device position and offering them to the microprocessor through a serial data interface.
- **GPRS**: this module facilitates the communication between the device and the control center, making use
of the TCP/IP protocol over GPRS for the information transmission.

- **ZigBee**: this is the module responsible for calculating the relative distance between two paired devices. This module can work when there is no GPS coverage or as additional information to that provided by the GPS module (e.g., in situation of imminent proximity).

- **Microprocessor and microcontroller**: these are the core of the device and are responsible for processing the information received from the different functional units, as well as giving response to them to coordinate their correct functioning. Amongst their multiple features we have the battery usage optimization.

- **On/off**: This button allows powering on or off the device.

- **Button 1**: When this button is pressed, the device sends a “Panic” alert to the control center.

- **Button 2**: General-purpose button. This button can be configured from the control center to offer specific on-demand features.

- **Status LED**: This element is made up of two Light Emitter Diodes. These LEDs will show the distinct status of the devices, such as a low battery warning, an alert situation or a network failure, amongst others.

- **Buzzer**: an acoustic indicator that alerts the user when a situation requires its attention, such as an alert or panic situation.

### A. Communication Protocol

This section describes the communication protocol used by the different elements of the Guardian system to communicate each other. The communication protocol defines a method for the transport of the necessary data so that the GIS can continuously obtain the location from all devices in the system. Likewise, this protocol allows configuring remotely some parameters in the devices, such as the period used by each device to send location data to the GIS. Furthermore, the protocol also allows the transmission of alert frames between the devices and the GIS (e.g., when the panic button is pressed) and vice versa (e.g., when the GIS alerts the victim that the aggressor has violated the safety distance).

The defined protocol is based on the delivery of different predefined frames whose basic structure consists of a fixed-length header followed by a variable-length payload. All frames used in the Guardian system between the wireless devices and the GIS have the same data header, which is shown in the Figure 3a and is described as follows.

1) **Fixed-length header common to all frames.**
   - **Src Id**: 32-bit field representing an unsigned integer in big-endian format, that is, the first transmitted byte is the most significant. This field represents univocally the device that starts the communication. The length chosen for this field is justified attending the amount of possible identifiers that can be generated.

2) **Payload for location data frame (0x00) length**

<table>
<thead>
<tr>
<th>Byte</th>
<th>4</th>
<th>4</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Src Id</td>
<td>Dst Id</td>
<td>Control byte</td>
<td>Frame Id</td>
<td>Checksum</td>
<td>Payload length</td>
</tr>
</tbody>
</table>

3) **Payload for location data response frame (0x01) length**

<table>
<thead>
<tr>
<th>Byte</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Status</td>
</tr>
</tbody>
</table>

4) **Payload for location period configuration frame (0x02) length**

<table>
<thead>
<tr>
<th>Byte</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Period</td>
</tr>
</tbody>
</table>

5) **Payload for period configuration response frame (0x03) length**

<table>
<thead>
<tr>
<th>Byte</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Status</td>
</tr>
</tbody>
</table>

6) **Payload for ZigBee status configuration frame (0x04) length**

<table>
<thead>
<tr>
<th>Byte</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ZigBee status</td>
</tr>
</tbody>
</table>

7) **Payload for ZigBee status response frame (0x05) length**

<table>
<thead>
<tr>
<th>Byte</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Status</td>
</tr>
</tbody>
</table>

Figure 3. Main frames involved in the communication protocol between the wireless devices and the control center.

- **Dst Id**: In a similar format that the **Src Id** field, this field represents the device to which the communication is addressed.

- **Control byte**: 8-bit field representing an unsigned integer value that identifies the kind of transmitted frame. This field can take the following values:
  - 0x00: **Location data frame**. This frame is periodically sent from a wireless device
(carried by the potential victim or the potential aggressor) to the control center.

- **0x01: Location response frame.** This frame is sent from the control center to a wireless device as response to the location data frame (0x00).

- **0x02: Location period configuration frame.** Command for modifying the location data frame (0x00) period. This frame is sent from the control center to a wireless device.

- **0x03: Location period response frame.** This frame has different meanings according to the source and destination nodes, as described below.

- **0x04: ZigBee status configuration frame.** This frame is sent from the control center to the wireless device to enable or disable its ZigBee module.

- **0x05: ZigBee status response frame.** This frame is sent by the wireless device to the control center as a response to the ZigBee status configuration frame (0x04).

- **Frame identifier:** 8-bit field representing an unsigned integer value. This field identifies univocally the frame in a data stream between two entities in the system. It is considered that the data stream should be fluent enough to allow each entity to receive the frame acknowledgment before reutilizing the same identifier.

- **Checksum:** 8-bit field representing an unsigned integer that stores the result of a summary function used for detecting errors in the information transmission. This function consists of the XOR sum of all other bytes in the frame. It is used at the receiver to check if there is any transmission error. If the checksum fails, the receiver will discard the frame.

This way, if we have that the bytes of the frame are \(b_0, b_1, ..., b_{m-1}\) with a frame length \(n\) and where \(b_m\) is the checksum byte, calculated by means of:

\[
b_m = b_0 \oplus b_1 \oplus ... \oplus b_{m-1} \quad (1)
\]

Therefore, the receiver can check if the received \(b_m\) accomplishes Equation 1, or, similarly, that:

\[
b_0 \oplus b_1 \oplus ... \oplus b_m \oplus ... \oplus b_{m-1} = 0 \quad (2)
\]

- **Payload length:** 8-bit unsigned integer field that represents the length, expressed in bytes, of the frame payload (excluding the header length).

2) **Payload of the different frames**

This section describes the payload of the different kinds of frames, as indicated in the Control byte field.

As mentioned before, currently there are four main frames that are transmitted between the wireless devices and the GIS.

a) **Location data frame (Control byte = 0x00)**

The most important frame is the location data frame, whose payload is shown in Figure 3b. This frame is periodically sent by each wireless device to the control center so that the latter can know the position of the device. The information transmitted in the payload includes the next data fields:

- **Status:** 8-bit field containing an unsigned integer value that represents the status of the device according to the distance between the victim and the potential aggressor. Its possible values are a bitwise OR operation of the following flags:
  - **0x00:** No incidence. Everything is ok.
  - **0x01:** Safety distance violated. Violation of the safety distance, that is, both wireless devices (victim and aggressor) can mutually detect each other via ZigBee.
  - **0x02:** Button panic. The victim has pressed the panic button on its device.
  - **0x04:** No GPS signal. Therefore, the location data in the payload contains the last GPS position estimated before losing the coverage.
  - **0x08:** Low battery level.

- **Timestamp length:** 8-bit unsigned integer field representing the length in bytes of the ASCII string with the representation of the timestamp of the device transmitted in the timestamp field.

- **Timestamp:** variable-length field which contains the data and time information in ASCII format. The format of the string follows the $GPZDA$ sentence of the NMEA 0183 protocol for GPS [13], corresponding with “hhmmsss,dd,mm,yyyy,xxx,ll”, where:
  - “hhmmsss,dd,mm,yyyy”: represents the Coordinated Universal Time (UTC) in hours (hh), minutes (mm), seconds (ss), centiseconds (cc), days (dd), months (mm), and year (yyyy).
  - “xxx”: correction in hours for the local time (from -13 to +13).
  - “ll”: correction in minutes for the local time.

- **Location data length:** 8-bit unsigned integer field representing the length in bytes of the ASCII string with the representation of the location of the device transmitted in the location data field.

- **Location data:** variable-length field which contains the location information in an ASCII string. The string format follows the $GPGLL$ sentence of the NMEA 0183 protocol for GPS [13], corresponding with “llll.ll,a,yyyyy.yy,a,hhmmss.cc,A”, where:
o “III.II”: latitude, the first two characters represents the degrees, and the rest the minutes. For example, “4916.45” means 49°16.45’.
o “a”: “N” for North, and “S” for South.
o “yyyy.yyyy”: longitude, the first three characters represents the degrees, ant the rest the minutes. For example, “12311.12” means 123°11.12’.
o “a”: “E” for East, and “W” for West.
o “hhmmss.cc”: represents the Coordinated Universal Time (UTC) in hours (hh), minutes (mm), seconds (ss) and centiseconds (cc).
o “A”: GPS status. The presence of this character indicates that the geographical position and the UTC timestamp are valid. Otherwise, the location data will contain the last valid value, and “A” will be substituted by a “*” character.

b) Location response frame (Control byte = 0x01)

After receiving a location data frame (0x00) from a wireless device, the GIS answers the device with a location response frame, whose payload is shown in Figure 3c. As can be seen, this payload only has a status byte, which can require the wireless device to send the location data frame again if something went wrong (e.g., a checksum failure).

c) Location period configuration frame (Control byte = 0x02)

According to the distance between the victim and the aggressor, the GIS can modify the location data period in order to save device batteries using a location period configuration frame. This way, if both devices are separated a long distance one from other, the period with whom the wireless devices send their location data frames to the GIS will be long. The payload transmitted by this kind of frame is shown in the Figure 3d. As can be seen, it only contains a 16-bit unsigned integer field representing the period in seconds.

d) Location period configuration response frame (Control byte = 0x03)

When a wireless device receives a location period configuration frame (0x02), it changes its location data period and answers the GIS using a location period configuration response frame, whose payload is shown in Figure 3e. As can be seen, the payload of this kind of frame includes a status byte and a 16-bit unsigned integer field echoing the new value of the location period.

e) ZigBee status configuration frame (Control byte = 0x04)

According to the distance between the victim and the aggressor, the GIS can enable or disable the ZigBee module in the wireless device in order to save device batteries. As in the location period, if both devices are separated a long distance one from other, the wireless devices does not need to use their ZigBee modules. The payload transmitted by this kind of frame is shown in the Figure 3f. As can be seen, it only contains an 8-bit unsigned integer field representing the new status of the ZigBee module (0x00 stands for disabled, while 0x01 means enabled).

f) ZigBee status response frame (Control byte = 0x05)

When a wireless device receives a ZigBee status configuration frame (0x04), it enables or disables its ZigBee module and answers the GIS using a ZigBee status response frame, whose payload is shown in Figure 3g. As can be seen, the payload of this kind of frame includes a status byte and an 8-bit unsigned integer field echoing the new value of the ZigBee module status.

IV. EXPERIMENTS AND RESULTS

In order to test the feasibility of the Guardian system, a software and hardware prototype has been implemented. This way, the risks associated to the hardware development will be minimized, and both the architecture and the own design will be validated. Because of the inherent logic of the system and the protocol used in the Guardian wireless devices, the use of micro-programmed and embedded systems have an important role in this project.

The electronic devices chosen for the implementation of the functional components have been selected taken into account the experience and knowledge previous about them, as well as their reliability, robustness and technical support. The implemented hardware prototype for the wireless device is the result of the integration of two well differentiated devices: a ZigBee communication module and a mobile phone with GPRS and GPS capabilities. This way, the combination of these two devices allows providing all the features defined by the functional units of the hardware architecture.

On the one hand, the GPS/GPRS module allows the bidirectional data transmission between the Guardian wireless device and the control center (GIS) using its GPRS capabilities. In addition, this module provides the position of the device basing on the GPS system. Furthermore, the digital input and output ports of this module allow implementing the input/output interfaces described in the architecture of the Guardian device.

On the other hand, as mentioned before, the ZigBee module provides a reinforcement to the safety, making Guardian a unique and innovative system. This module allows the detection and estimation of the distance between the wireless device and the other device paired to it a dynamic and real-time way, no matter the GPS module coverage.

As mentioned above, the main components of the Guardian wireless device are based on the architecture of the n-Core Sirius devices [12]. Each n-Core Sirius B (shown in Figure 4) device includes an 8-bit RISC (Atmel ATmega 1281) microcontroller with 8KB of RAM, 4KB of EEPROM and 128KB of Flash memory and an ZigBee transceiver. n-Core Sirius B devices have both 2.4GHz and 868/915MHz versions and have several internal and external communication ports (GPIO, I2C, PWM, and USB UART) to connect to distinct devices, including a wide range of sensors and actuators.

2491
The n-Core Sirius devices form part of the n-Core platform [12], which offers a complete API (Application Programming Interface) to access all its functionalities. This platform was chosen because it provides all the needed functionalities by means of its full-featured n-Core firmware and the n-Core API. Thus, developers do not have to write any additional embedded code to build a system as this, but just configure the n-Core Sirius devices to accomplish the required features [12].

It is used an Android smartphone, the HTC Hero, as the GPS and A-GPRS modules in the prototype. Using a Smartphone brings together Wi-Fi, Bluetooth, GPRS, UMTS and HSDPA communications in one device, while providing access to geolocation features via Wi-Fi, A-GPS and also through the cellular network. A smartphone also allows programming the behaviors required by the Guardian project by allowing enabling and disabling hardware resources for two main purposes:

1. Optimization of energy consumption.
2. Increased reliability and availability.

The second point is directly related to the Guardian system workflow, which allows saving resources (i.e., energy) depending on the location of the users. That is, a more precise geolocation requires more hardware and power consumption (Wi-Fi, A-GPS and ZigBee running simultaneously).

Figure 5 shows the latest prototype of the Guardian device launched in Q2 2012. As can be seen, the communication between the Sirius B device and the smartphone is done via the GPOs and the volume keys respectively. This allows triggering interrupts directly to the smartphone when the Sirius B device detects the paired device (e.g., the aggressors’ Guardian device) is detected and therefore there is a risk situation. The Sirius B device is powered using the battery of the smartphone.

Regarding the software side of the Guardian device, we have chosen Android 2.1 (API-7) for the prototype presented in this paper, as it is the latest official version supported by the HTC Hero smartphone. The device is programmed in Java and using the Eclipse IDE (Integrated Development Environment).

The control center of the Guardian system has two basic blocks:

- **GuardianService.** It receives the information from all the Guardian devices connected to the system and also provides control instructions to the devices (e.g., turn on/off wireless communications). It is also responsible for the management and provision of data to the GUI via XML-RPC. **GuardianService** has been developed using Python 3.1 and SQLite3.
Guardian GUI. It shows the data managed by the system (e.g., alerts, logs and access controls). 
Guardian GUI has been developed as a web application and therefore it can be displayed in both desktop and mobile devices (Figure 6). Guardian GUI has been developed using Python3.1, XML-RPC, HTML5, JavaScript, CSS3, Lungo JS Framework, JQuery Framework and Google Maps API.

This architecture allows making the hardware communication and the visualization layers independent. Therefore, the visualization layer is completely abstract with respect to the type of the underlying technology. The interface starts a Google Maps instance. This way, it is possible to see the exact location of a Guardian device.

V. CONCLUSIONS AND FUTURE WORK

The Guardian system pursues a revolutionary concept: the total supervision of people under risk situations, augmenting their safety and autonomy in a completely ubiquitous way. It is important to mention that there is no similar solution in the market, specifically a device with the characteristics specific to develop this project. This fact implies a high level of hardware development. Furthermore, there is not a hardware/software platform that fully provides the middleware layers necessary to integrate all the mentioned technologies.

In this regard, the creation of a hardware and software prototype has achieved two objectives: to validate the proposed architecture and check that the utilized technology is appropriate for the system.

Future work includes the full development of all the projected functionalities. This includes the production of an extended and more integrated hardware prototype for the wireless devices. In the future, the Sirius B device will communicate directly with an Android smartphone via the ADK interface, allowing two-way communication. At the software level, both the firmware embedded in the devices and middleware/software layers at the GIS will be completely developed, integrated and configured. Then, the system will be implemented in a simulated scenario to test if it is suitable for the situations for which it is designed. These situations include domestic violence and children/elderly care situations. Finally, the system will be implemented in a real scenario in order to test its actual performance.

ACKNOWLEDGMENT

This project has been supported by the Spanish Ministry of Science and Technology project TIN 2009-13839-C03-03: Organizaciones Virtuales Adaptativas: Mecanismos, Arquitecturas y Herramientas (OVAMAH).

REFERENCES