Guardian: Electronic System Aimed at the Protection of Mistreated and At-risk People

Ricardo S. Alonso, Dante I. Tapia, Óscar García, Fabio Guevara, José A. Pardo, Antonio J. Sánchez, and Juan M. Corchado

Abstract. Ambient Intelligence (AmI), based on ubiquitous computing, represents the most promising approach between people and technology to solve the challenge of developing strategies that allow the early detection and prevention of problems in automated dependence environments. One of the most influenced areas by AmI-based systems will be security and, more specifically, the protection of people under risk situations, including cases of mistreatment or loss. This will contribute to improve important aspects of the quality of life of these people, specially their safety. This paper describes Guardian, an integral solution designed for improving the protection of mistreated and at-risk people.

Keywords: Ambient Intelligence, Mistreatment, Safety, GPS, GPRS, ZigBee.

Introduction

According to statistical data from the Ministry of Interior of Spain [1], from 2006 to 2008 more than 60 women were killed in Spain each year by their couples or ex-couples. In 2008, a 23% of the killed women had filed a formal complaint against their murderers. In this regard, this paper describes *Guardian*, an Ambient

Ricardo S. Alonso · Dante I. Tapia · Óscar García · Fabio Guevara
R&D Department, Nebusens, S.L., Scientific Park of the University of Salamanca,
Edificio M2, Calle Adaja, s/n, 37185, Villamayor de la Armuña, Salamanca, Spain
e-mail: {ricardo.alonso,dante.tapia,oscar.garcia,
fabio.guevara}@nebusens.com

José A. Pardo · Antonio J. Sánchez · Juan M. Corchado
Department of Computer Science and Automation, University of Salamanca,
Plaza de la Merced, s/n, 37008, Salamanca, Spain
e-mail: {jose.pardo,anto,corchado}@usal.es

P. Novais et al. (Eds.): Ambient Intelligence - Software and Applications, AISC 153, pp. 11–18.
springerlink.com

Intelligence (AmI) [2] 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 wireless electronic devices.

In this sense, 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]. An environment capable of recognizing the presence of people, and locating them in a geographical an activity context is the base to AmI to demonstrate all its potential.

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. Thus, there are different approaches that propose electronic telemonitoring systems for tracking victims and aggressors [5] [6] to reduce risk situations.

The Guardian system will make 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 by means of a powerful logic of middleware layers.

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. After that, the main components of the novel Guardian system are depicted. Finally, the conclusions and the future work are presented.

Background and Problem Description

It is important to point out that, in Spain, the pressure over the assistance system is growly increasing, as well as the necessity to offer services with more quality. 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, email 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.

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 that will be extended and published further on.

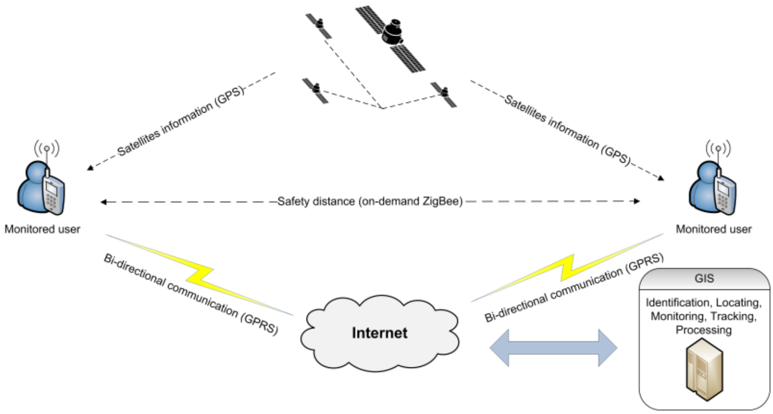
Satellites information (GPS)
Satellites information (GPS)
Monitored user
Safety distance (on-demand ZigBee)
Monitored user
Bi-directional communication (GPRS)
Bi-directional communication (GPRS)
Internet
GIS
Identification, Locating, Monitoring, Tracking, Processing

Fig. 1 Basic schema of the Guardian system.

Figure 2 shows the flow diagram representing the basic functioning of the system at the wireless infrastructure level. The basic functioning of the Guardian system is as follows. There are two kinds of users or roles in the system. On the one hand, the first kind of user, the threatened or at-risk user, carries or wears a mobile phone or other mobile device (e.g., a bracelet). This device includes A-GPS, GPRS and ZigBee capabilities. On the other hand, the other kind of user (i.e., the potential aggressor) also wears another device with similar wireless 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]. Is in this point where the Guardian system makes the difference over the conventional systems currently available in the market.

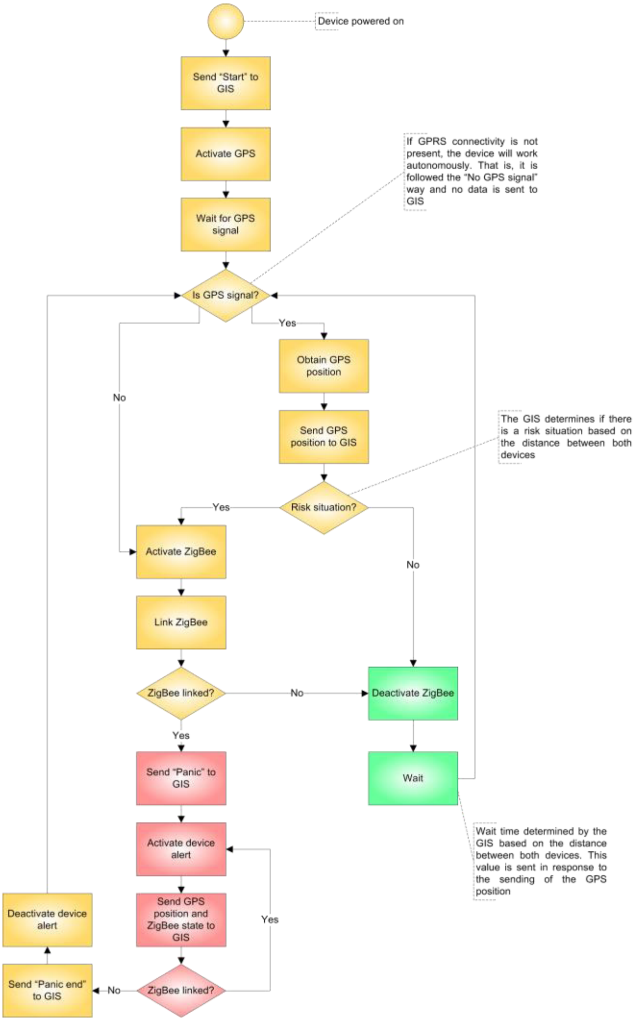
Device powered on
Send "Start" to GIS
Activate GPS
Wait for GPS signal
If GPRS connectivity is not present, the device will work autonomously. That is, it is followed the "No GPS signal" way and no data is sent to GIS
Is GPS signal?
Yes
No
Obtain GPS position
Send GPS position to GIS
The GIS determines if there is a risk situation based on the distance between both devices
Risk situation?
Yes
No
Activate ZigBee
Link ZigBee
ZigBee linked?
No
Deactivate ZigBee
Yes
Send "Panic" to GIS
Wait
Wait time determined by the GIS based on the distance between both devices. This value is sent in response to the sending of the GPS position
Activate device alert
Send GPS position and ZigBee state to GIS
Yes
Deactivate device alert
Send "Panic end" to GIS
No
ZigBee linked?

Fig. 2 Flow diagram of the Guardian system at the wireless infrastructure level.

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. 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 3 is proposed.

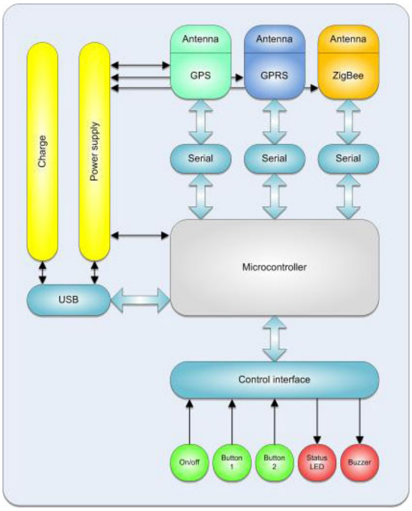

Fig. 3 Functional architecture of the Guardian system's devices.

This functional architecture is based on the n-Core® Sirius B devices from Nebusens [12]. Each n-Core® Sirius B 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, ADC, I2C, PWM, and USB/RS-232 UART) to connect to distinct devices, including a wide range of sensors and actuators. 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].

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 microcontroller 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).
- *Microcontroller*: this is the core of the device and is responsible for processing the information received from the different functional units, as well as giving response to them to coordinate their correct functioning. Amongst its 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.

Conclusions and Future Work

The Guardian system pursuits 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.

Future work includes the full development of all the projected functionalities. This includes the production of the first hardware prototype for the wireless devices. 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 on a real scenario in order to test its actual performance.

Acknowledgments. This project has been supported by the Spanish Ministry of Science and Innovation. Project IPT-430000-2010-035.

References

1. Ministry of Interior of Spain, Violencia de género. Programa de Intervención para Agresores (2010), http://www.mir.es/file/53/53009/53009.pdf (accessed December 31, 2011)
2. Aarts, E., de Ruyter, B.: New research perspectives on Ambient Intelligence. Journal of Ambient Intelligence and Smart Environments 1(1), 5–14 (2009)
3. Bajo, J., de Paz, J.F., de Paz, Y., Corchado, J.M.: Integrating case-based planning and RPTW neural networks to construct an intelligent environment for health care. Expert Syst. Appl. 36, 5844–5858 (2009)
4. Tapia, D.I., Abraham, A., Corchado, J.M., Alonso, R.S.: Agents and ambient intelligence: case studies. Journal of Ambient Intelligence and Humanized Computing 1(2), 85–93 (2010)
5. BI Incorporated. One-piece active GPS offender tracking: BI ExacuTrack® One (2011), http://bi.com/exacutrackone (accessed September 9, 2011)
6. iSECUREtrac. One-piece GPS Systems from iSECUREtrac (2011), http://www.isecuretrac.com/Services.aspx?p=GPS#onepiece (accessed September 9, 2011)
7. Djuknic, G.M., Richton, R.E.: Geolocation and Assisted GPS. Computer 34(2), 123–125 (2001)
8. Haung, Y.-R., Lin, Y.-B.: A bandwidth-on-demand strategy for GPRS. IEEE Transactions on Wireless Communications 4(4), 1294–1399 (2005)
9. Baronti, P., Pillai, P., Chook, V.W.C., Chessa, S., Gotta, A., Hu, Y.F.: Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. Comput. Commun. 30(7), 1655–1695 (2007)
10. Küpper, A.: Location-Based Services: Fundamentals and Operation, 1st edn. Wiley (2005)
11. Anynye, S., Rajala, Y.: System and Method for Tracking, Monitoring, Collecting, Reporting and Communicating with the Movement of Individuals. U.S. Patent Application, 20100222073 (February 9, 2010)
12. Nebusens: n-Core®: A faster and easier way to create Wireless Sensor Networks (2012), http://www.n-core.info (accessed January 2, 2012)