CONCURRENCY AND COMPUTATION: PRACTICE AND EXPERIENCE
Concurrency Computat.: Pract. Exper. 2015; **27**:2531–2546
Published online 12 December 2014 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/cpe.3450

SPECIAL ISSUE PAPER

Supporting personal security using participatory sensing

Pablo Carreño[1], Francisco J. Gutierrez[1], Sergio F. Ochoa[1,*,†] and Giancarlo Fortino[2]

[1]*Computer Science Department, Universidad de Chile Beauchef 851, 3rd floor, Santiago, Chile*
[2]*DIMES, Università della Calabria Via P. Bucci, cubo 41C, 87036 Rende (CS), Italy*

SUMMARY

Personal security is an open problem in large cities. After several attempts to reduce violence and crime, there seems to be an agreement that preventive actions are the best way to address this problem. Trying to help deal with that challenge, this paper proposes a mobile collaborative application, named Personal Guardian, which is used by civilians while walking in urban areas. The application is focused on crime prevention and it implements participatory sensing to help people be aware of the risks that appear to exist in a certain place at a certain time. Based on that information, citizens can take appropriate and on-time preventive actions. The system is supported by a human-centric wireless sensor network, and it is complementary to the security solutions already used by public and private organizations. The system architecture and its main components are described, and the main requirements and design decisions are also discussed. A preliminary evaluation of the solution was conducted to determine its strengths and weaknesses in terms of quality of service. The obtained results indicate that the information feeding process is more relevant for end-users than the unattended delivery of awareness information about their personal security. In addition, this former capability does not require to be adjusted to the end-users' context. Copyright © 2014 John Wiley & Sons, Ltd.

Received 21 January 2014; Revised 18 October 2014; Accepted 19 October 2014

KEY WORDS: personal security; crime prevention; smart cities; participatory sensing; human-centric wireless sensor networks; crowdsourcing; social computing

1. INTRODUCTION

Crime (e.g. assault, robbery, rape, vandalism, physical aggressions, and murders) is an open issue in most countries around the world, particularly in large urban areas. Although government organizations are continually working to improve the personal security of civilians, crime rate does not seem to change too much [1, 2].

Today there seems to be a consensus that crime prevention is the best way to address this problem. Unfortunately most solutions used to try reducing crime, like the use of surveillance cameras or increasing the presence of security agents in the field, are not robust enough in terms of crime prevention for civilians [3–5]. For instance, these types of solutions do not have good scalability, because it is not feasible to flood a city with surveillance cameras or police personnel permanently in duty protecting civilians. The cost and complexity of these solutions make them also not feasible, even for developed countries.

Conscious of such situation, government organizations have involved citizens to a greater extent during the last years in the process of crime prevention; e.g. through anonymous reports of crimes

*Correspondence to: Sergio F. Ochoa, Computer Science Department, Universidad de Chile, Beauchef 851, Santiago, Chile.
†E-mail: sochoa@dcc.uchile.cl

or suspicious activities. This has allowed civil authorities to increase the coverage area and the monitoring capability of security organizations [6]. However, citizen participation is still bureaucratic (e.g. it requires to do a phone call or fill a denounce form); therefore, it tends to be slow and with a low participation rate.

Social networking services (SNS) provide a platform that allows people to participate through a simple and direct way (e.g. through crowdsourcing or participatory sensing), in activities that are relevant for them [7, 8]. Examples of such activities are diagnosing the vehicular traffic, tagging places in a physical environment, or rating the quality of service of a certain provider.

This article presents a tool that allows civilians to perform participatory sensing [9, 10] as a way to help them tackle the stated security problem. The implemented solution is a mobile collaborative system, named *Personal Guardian* (PG), which empowers ordinary citizens to collect and share security information from their surrounding environment, using their mobile phones in an easy and anonymous way. Considering the information provided by multiple participants, the PG system performs an online diagnosis that allows civilians being aware of their current risk and personal security level while they move through urban areas. Thus, they can take preventive actions in case of need.

The system, which is supported by a human-centric wireless sensor network (HWSN) [11], is complementary to regular solutions provided by other organizations. The functional and non-functional requirements of PG were established with the help of 31 people, who participated through five focus groups.

Once implemented, the system was evaluated considering its service availability, performance, information trustworthiness, and usability. The system showed good results in the four evaluated aspects. Both the information feeding process and the usability of the application were indicated as the most important features according to the end-users' opinion. During such process we also identified the need to provide context-aware mechanisms for delivering notifications to end-users, in order to not bother them. Typically, people manage their personal security in different ways; therefore, they want to receive notifications according to their personal level of apprehension to risk situations.

Next section presents the related work. Section 3 briefly introduces the concept of human-centric wireless sensor networks and explains the architecture of the Personal Guardian system. Section 4 presents and discusses the main requirements and design decisions made in the system implementation. Section 5 describes the system evaluation process, in which formal tests were conducted to determine the level of accomplishment of non-functional requirements (i.e. quality requirements). It also discusses the obtained results. Finally, section 6 presents the conclusions and the future work.

2. RELATED WORK

Personal security corresponds to the level of protection of a person from intentional criminal acts [12]. It is considered a core element of the well-being of individuals. The OECD Better Life Index [13] reports that 4% of people in OECD countries say they have been assaulted or mugged over the past 12 months, where the average homicide rate in those countries is 2.2 murders per 100,000 inhabitants.

Criminologists recognize crime prevention strategies aimed at reducing the criminal opportunities that arise from the routines of everyday life (e.g. improving surveillance of areas that might attract crime by using closed-circuit television). These strategies are conceptualized under the notion of *situational crime prevention* [14], which seeks to reduce opportunities for specific categories of crime, by increasing difficulties to perform those actions and decreasing the associated risks and rewards [15]. This crime prevention strategy requires that the potential victims be conscious of their current risk situation, which seems to be the most unexplored and complex part of the problem.

Typically, people do not have supporting information about their personal security in many areas of a city, even while living in that place. People can manage this lack of information in multiple ways. Individuals can use their own experience to quantify the security level of the area in which they are located, or they can use the experience of their contacts (e.g. friends in a SNS) or mainstream media

DOI: 10.1002/cpe

(e.g. newspaper articles). For example, neighborhood programs and patrols can provide a friendly and non-invasive support to members of a community, helping them feel better connected to their neighbors. Thus, these programs contribute to reduce the neighbors' risk of becoming victims of frauds and scams, as well as other crimes.

Information is also usually managed by official sources from the government and other public agencies, which publish studies and relevant statistics related to homeland security. Even if these latter sources provide good references to estimate the inherent risk of a particular area, users may be confronted to information provided in a complex format (e.g. in confusing or long documents), thus being perceived as difficult to understand. Particularly, this is a problem when individuals are faced to quickly and accurately find the inherent risk of a particular area at a particular time.

With the rise of social computing and ubiquitous technologies, Web applications have evolved from serving users at an individual scale, to content-providers at a community scale. Moreover, these services may actually go beyond the scope of a community and impact life in cities. There is a current trend around the notion of *smart city* [16], which are characterized by an integration of infrastructures and technology-mediated services, the social learning for strengthening human infrastructure, and the governance for institutional improvement and citizen engagement [17]. In particular, our proposal aims to provide a mechanism for helping citizens take an active role in crime prevention in a way that would allow transform ordinary cities into smart ones.

Since the concept of smart city can be understood as a more user-centered evolution of other city-related concepts, it is natural to conceive the generation of ideas for innovative uses of information technology driven by user participation or crowdsourcing [18]. One of these techniques is what Burke et al. call *participatory sensing* [9]. This notion refers to 'task deployed mobile devices to form interactive, participatory sensor networks that enable public and professional users to gather, analyze, and share local knowledge'. Currently, mobile devices (e.g. smartphones) embed multiple sensors (e.g. motion sensor or accelerometer, gyroscope, and ambient light sensor), which have made participatory sensing viable in the large-scale. Therefore, individuals and groups of people actively participate in the collection of information for purposes ranging from crime prevention to scientific studies [19].

Naturally, one of the critical factors to drive success in participatory sensing is the data collecting process performed by users in order to generate collective intelligence. Lan et al. [20] proposed an incentive scheme for a vehicle-based mobile surveillance system. The authors adopted a participatory sensing strategy under the assumption that video surveillance is commonly used by the police and private security officers to determine and investigate crimes and other incidents. Ballesteros et al. [21] studied a set of techniques for evaluating people security based on their spatial and temporal dimensions. The authors show that information collected from geo-social networks can be used to prevent crimes. Therefore, it seems to be clear that participatory sensing could be a good strategy to address the stated problem; however the way in which we implement the supporting solution can affect its usability and usefulness. Privacy and anonymity of the participating people must also be considered in the design of these solutions. Wang et al. [22] propose the ARTSense framework, which precisely deals with these issues. This framework consists of two main components: (1) an assessment algorithm to compute the trustworthiness of sensing reports, based on anonymous user reputation levels and privacy-preserving contextual factors (such as location, time, sensor mode, and traveling mode), and (2) an anonymous reputation management mechanism to maintain the anonymity properties of the user, while also enforcing positive or negative user reputation updates.

In order to try inferring criminally risky locations, we need to tackle the problem of accurately characterizing event locations using crowdsourcing mechanisms. In that sense, Ouyang et al. [23] developed a crowdsourcing-based approach, where users swipe on their smartphones' touchscreens in the direction of the event of interest. This particular kind of interaction can actually inspire the design of applications that strongly rely in crowdsourcing and ubiquitous technologies. For instance, applications for monitoring outdoor events, especially in densely populated public areas.

Finally, regarding the software architecture to support participatory sensing, Estrin [24] proposed a layered architecture where the collected data requires a permanent link between the sensors and the server that stores and manages such information. The dependence of particular components

DOI: 10.1002/cpe

(e.g. server or communication links) represents a serious restriction to address personal security evaluation, because the system should be available when required. Duarte et al. [25] go a step forward in the decentralization of the system architecture for participatory sensing and propose the use of mobile units acting as an intermediary between servers and the sensors, which eventually can support asynchronous communication among the network components. Finally, Ochoa and Santos [11] go a step even further proposing a human-centric wireless sensor network, which includes all the components of its predecessors, but also witness units that act as a repository of information for users located in a particular area. These units considerably increase the system availability in terms of information support to make decisions. Therefore, this is the alternative chosen to support participatory sensing in the PG system.

3. THE PERSONAL GUARDIAN SYSTEM

Figure 1 shows the architecture of the human-centric wireless sensor network (HWSN) that supports the PG system, which was initially introduced in [26]. HWSNs are heterogeneous in terms of communication support and the type of nodes that can participate to them. The communication support can be any that allows interaction between two or more nodes. The nodes are also

Figure 1. Layered architecture of the HWSN that supports the PG system.

DOI: 10.1002/cpe

heterogeneous, and they can play several roles, for instance they can be: *regular sensors*, *human-based sensors*, *mules, witness units*, and *actuators*.

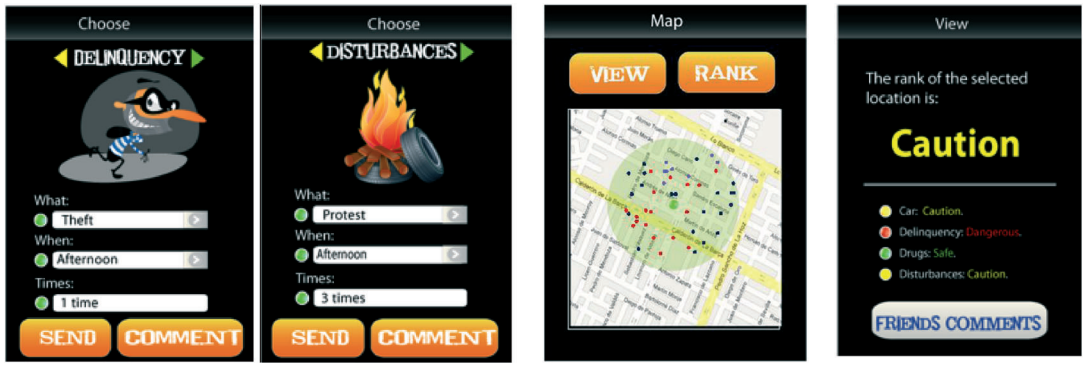
Regular sensors (RS) are instruments that measure a certain context variable and transmit its value to other units. Examples of these sensors are GPS, temperature sensors, wearable sensors (also used as Body Sensor Networks—BSNs [27, 28]), and also mobile devices able to detect the presence of other devices in the area.

Human-based sensors (HBS) are people that use their senses (possibly complemented by regular sensors, especially belonging to BSNs) to capture information about a certain variable of interest (e.g. delinquency in a particular area), elaborate on it, and then produce knowledge that represents the current value of that variable. HBS use a mobile device and a wireless network to share the generated knowledge with other network nodes. Although the information provided by HBS is not accurate, they represent the best option when the observed variable is not measurable with a regular sensor but by means of virtual/logical sensors [29].

Mules (Mu) are mobile units that connect two or more disconnected networks. Examples of mules are vehicles and passersby having a mobile computing device. These mules can also act as temporal witness units (WU), i.e. network nodes that store the information shared by other nodes in a certain area. These units are passive repositories of information that is relevant in the area where the WU is located (e.g. about personal security). These units interact on-demand with the HBS, and they can be implemented using almost any computing device with ad hoc communication and storage capability; i.e. from tiny computing devices to servers. Cloud computing services are an interesting way to implement WU, particularly if the information shared by them is highly demanded.

Actuators (Ac) are devices able to receive an order and perform an output action. Examples of these devices may be a horn that emits a sound when an alarm order is received from the smartphone of a HBS. It is important to remark that a same network node can play several roles at the same time. For instance, an HBS can act as a sensor when its user shares information through the network, as a Mu while the user move through a certain area, and as a WU when the user is in the neighborhood where he/she lives. The roles of a network node in a certain instant are given by the services it provides to other nodes and also to its user.

The architecture of the HWSN is composed of four layers: *sensing*, *communication*, *information persistence*, and *application*. The lower layer is in charge of sensing the variables to be considered in the process that is being supported; in our case, the evaluation of the personal security of people in a certain area at a certain time. This layer considers HBS (e.g. passersby or neighbors) that use smartphones and simple GUI forms to add information to the system in a loosely coupled way. Figure 2.a shows two samples of these forms, through which the HBS indicates what event they saw or suffered, when it happened, and how many times they have seen similar situations in that place. Users indicate on a digital map the exact location of the events, and the GPS geo-references that information.



(a) (b) (c)

Figure 2. User interfaces of the Personal Guardian system.

DOI: 10.1002/cpe

The information captured by the sensors is then shared using the services provided by communication units (e.g. WiFi or cellular antennas) or mules. These components are part of the communication layer. The system considers a 3G connection with a server (WU) and WiFi-based mobile ad hoc network that is implemented using a High Level MANET Protocol (HLMP) infrastructure [30]. Such an infrastructure also allows a network node (e.g. a HBS or WU) to detect other nodes in the area and exchange information among them.

In order to increase the information availability in the area where it is required, the shared information is temporarily or permanently stored in HBS and witness units located in the area, as well as eventually in remote servers or on cloud computing infrastructures [31]. These components are part of the information persistence layer. This layer considers the participation of WU and HBS. Two particular WUs play a key role in this system (Figure 1): the system server and the Facebook server. The first one stores and makes the fusion of the security information of every area, considering the reports features and the reputation of the users reporting the incidents. The Facebook server is used to authenticate the users and to retrieve the users' contact list, in case that an 'ask for help' message is delivered. The HBS (i.e. HLMP network nodes) participating in this layer act as temporal repositories of the security information of the area where they are located. They exchange information with other nodes through the HLMP infrastructure.

Finally, in the application layer we can see the information about the user vulnerability. Figure 2.b. shows the user current location and the records of incidents in an area of 200 meters around him/her. Figure 2.c. shows the information that the PG system delivers to the user when a risk overcame a certain threshold. The colors used to represent the risk level of a user follow the same semantics as a semaphore: green means 'ok', red means 'dangerous situation', and yellow means 'caution'. The application also allows filtering the incident records and shows only those added by Facebook contacts of the user. Several awareness mechanisms (from ringtones to tactoons) were implemented to notify the user about his/her current risk level. The current implementation of Personal Guardian determines the risks of a user to car theft and vandalism, regular delinquency (robbery and assaults), drugs traffic, and disturbance (physical violence).

4. SYSTEM REQUIREMENTS AND DESIGN DECISIONS

The design of the PG system considered several functional (FR) and non-functional requirements (NFR) to try ensure that it would usable and useful in a real scenario. In a first stage, these requirements were obtained and validated through a focus group with twelve potential users of the system. Then, the completeness and suitability of the obtained requirements were evaluated and adjusted by three experienced developers of mobile collaborative applications. This process only considered the main requirements of the system; i.e. those that are part of the application core. Next we describe the main functional and non-functional requirements that were defined in this process, and also the design decisions made to address them.

4.1. Functional requirements

Although the list of functional requirements (FRs) involved in the development of this system is quite long, next we present the most important ones from a usability and usefulness point of view. These FRs can be understood as services that the application must provide to the end-user (i.e. the citizens) or to other software services. For each FR we indicate the design decisions made to address it.

- *Map navigation*. The system must provide geo-referenced visual information, because warnings are typically related to a particular place or area of the city. Therefore the user should be able to navigate the map of the area, using several zoom levels. The use of geo-referenced tiles to manage the map positively impact usability and performance of the system [32]. Moreover, this service must count on positioning capabilities, through the use of GPS or others mechanisms. Relevant (i.e. context-aware) information must be clearly identifiable at a first glance; e.g. using blinking icons or bright colors.

DOI: 10.1002/cpe

- *Device positioning*. In order to determine the personal security of people, the system needs to know its users' location. Since a risk evaluation requires a coarse-grain position of the user, in most cases the use of GPS is a good option to make a diagnosis of the area. In the case of indoor locations, the use of the last known outdoor position of the user could be enough to determine his/her vulnerability level. Although using just GPS can lead the system to make some error when the user is indoors, this strategy considerably reduces the complexity to implement services that perform indoor positioning. Devices not having positioning capabilities can request such information to neighbor nodes (e.g. HBS, mules or witness units) using ad hoc communication services; for instance a mobile ad hoc network. Using positioning by nodes proximity is also an option that can be used in case of need.
- *Communication*. The information provided by the crowd should be shared as soon as possible to benefit the participants and to reduce the impact of possible malicious interventions affecting the trustworthiness of the shared data. In both cases, counting on communication among participants is mandatory. Such communication can be performed using ad hoc or infrastructure-based communication systems, or a combination of them. Typically, the former helps address information sharing in a small area, and it is usually enough to support the diagnosis of pedestrians' personal security. The latter covers larger areas and provides a wider bandwidth that properly allows supporting the crowd activities. This communication modality helps diagnose the personal security of an ample range of users, from pedestrians to car drivers. Although the system implements loosely coupled data links (i.e. the PG system does not require a permanent data link with the server or other nodes), counting on stable communication when required helps the application be more effective in both, the diagnosis and alarm delivery processes.
- *Device tracking*. This requirement allows users to monitor the whereabouts of a remote user on a map. It is typically required when the monitored person is asking for help to someone else, e.g. friends or family. The tracking capability can be implemented using device positioning and communication (e.g. detecting the cellular antenna that is being used by the monitored person to be connected with the system); and the means for monitoring the user movements can be implemented using the user's personal contacts from a SNS (like Facebook).
- *Visual handheld-based feeding*. If we want that many people report vulnerability (in terms of crime) of city areas, the reporting process should be easy and fast. This process can be accomplished using handheld devices that are easy to transport, deploy, and use. Indeed, most of them have GPS that allows users to geo-reference their vulnerability reports. The information of these reports should be locally stored into the device, and then appropriately transferred to a WU to avoid delays in the feeding process. The system server is the main repository (i.e. WU) of shared information, and it is the node in charge of determining the accuracy and trustworthiness of each information piece. People reporting information about vulnerability are HBS that use their senses, knowledge, and experience to determine that a place or area, under certain conditions, is vulnerable to specific types of crimes. The use of visual information during the feeding process usually contributes to reduce the users' error rate.
- *Data sharing*. Data sharing benefits the system users and reduces the impact of malicious interventions. The ad hoc and infrastructure-based communication units play a key role in this process. Moreover, the presence of MUs and WUs typically contribute to enhance the data sharing among network nodes, which positively impacts on the availability, performance, and trustworthiness of the whole system. Autonomous agents can be used to share data in an unattended way; thus, we avoid distracting the users and increase the system ubiquity. The shared information should be in a standard format that allows other nodes to interpret it correctly.
- *Warnings/alarms delivery*. The main goals of the system are to diagnose the user current situation and deliver appropriate notifications in order to make him/her aware of his/her risk level. The diagnosis process and also delivery of notifications are in charge of autonomous agents to avoid distracting the end-user. The evaluation of users' vulnerability requires geo-localization (GPS) to determine the users' position, and awareness mechanisms to inform people about their possible risks. In case that a user asks for external help (e.g. friends or family), the system would require connecting to a social networking service to retrieve the user's personal contact information, and deliver the alarms accordingly. The mechanisms used to deploy the alarm should be

DOI: 10.1002/cpe

context-aware. For instance, the smartphone can vibrate instead of sounding to indicate that the user is already in a dangerous area. Thus, the application avoids calling someone's attention.

4.2. Non-functional requirements

The non-functional requirements (NFR) establish restrictions to the services provided by the software. The quality of these services depends on how well these requirements are addressed. Typically, every NFR should have a minimum acceptance level, which should be achieved (during a formal test) by the system services. NFRs are also transversal; this means that they affect every service of the system.

- *High availability*. The system should be available as well as the supporting information that it provides, independently of the possibility to count on access to the system server. For that reason, the geographical information of an area and its vulnerability information should be managed using a loosely coupled schema. This means that a mobile device running the system must locally keep all the information of the area where it is located. Periodically the device synchronizes its information with the server (i.e. WU) in charge of the information persistence, and eventually downloads information of new areas that are now relevant, if the user moved to other places. If the system does not have access to a WU, it evaluates the user vulnerability based on the local information. Eventually, if it does not have enough information to determine the user vulnerability, it can ask to neighbor devices (i.e. HBS or Mules) for additional information or for a complete vulnerability diagnosis. Interactions with other network nodes require counting on access to infrastructure-based or ad hoc communication units. Since the system availability also depends on the availability of the device where it runs, the target device should be mobile and be with the user most of the time. Considering these restrictions, a handheld device, like a smartphone or a small slate, seems to be the most appropriate option for deploying the system. The information availability should be measured from the end-user point of view; therefore, autonomous agents are required to diagnose an area and eventually deliver context-aware notifications.
- *Quick access*. If the user wants to get personal security information on-demand, the access to such information should be fast, where the most relevant information must be shown first. In that sense, the use of visual information is usually the best alternative to deliver information to the user. The type of actions for crime prevention that can be taken by the user depends on how well this visual information can be captured in a first glance. Moreover, it is important to use a mobile device with fast boot, like a smartphone or a slate. The use of a loosely coupled data link strategy, which prioritizes the use of locally stored map tiles, also contributes to have a quick access to the supporting information.
- *Proactivity.* The system should contribute to prevent crime by autonomously informing the user about possible vulnerability situations that it identifies. For that reason, the system should be active at all times, monitoring and evaluating the personal security context of the user. Usually, this functionality is implemented through an autonomous agent. A context-aware alarm (e.g. visual messages, ringtones or tactoons) should be triggered every time that a vulnerability situation exceeds a certain threshold. Depending on its criticality, more than one alarm could be sent not only to the local user but also to his/her closest contacts. The way in which these alarms are deployed on the mobile device depends on the user preferences.
- *Information trustworthiness.* When the quality of a service depends on the quality of the information that it provides, information trustworthiness becomes a critical requirement. Although there are several strategies to address this requirement, recent research in participatory sensing indicates that crowdsourcing and reputation are usually a good combination to deal with this issue [33, 34]. Data held by other network nodes and WUs can also contribute to increase the trustfulness of the information. In order to help increase the information trustworthiness, users can vote or add annotations only if they are located near to the place they are referencing. Thus, we avoid that people spread personal security information everywhere. Autonomous agents running in the system server periodically reevaluate the votes, considering the reputation of the voters, in order to determine vulnerability of particular areas. The aggregated information about vulnerability is shared on-demand with the mobile nodes.

DOI: 10.1002/cpe

- *Understandable information*. The system must notify to its users as soon as possible if they are in risk. Therefore, the information that the system provides them should be easy to understand by average users at a first glance. In that sense, the use of visual information and voice messages seem to be appropriate to address this requirement in most work contexts. In the case of messages indicating physical locations, the use of geo-referenced visual information (e.g. a map or a radar view) is usually the easiest way to provide an effective communication to end-users. Provided that effective communication requires that input and output channels be aligned, awareness mechanisms are usually required.
- *Interoperability*. The system should be able to exchange data and requests services to other devices, as a way to provide more accurate and on-time advices/alarms to end-users. This interoperability requirement has a well-known solution, which consists on using data and service representations that adhere to standard formats (e.g. XML for data, and Web services to implement functionality). The interaction between nodes will require counting on infrastructure-based or ad hoc communication units.

4.3. System requirements versus design decisions

Figure 3 summarizes the relationships among the main FR, NFR, and design decisions involved in the system. These relationships also indicate whether a design element is mandatory, optional or not required to implement a certain requirement. The type of relationship was established according to the opinion of both, the end-users that participated in the focus groups, and the developers of mobile collaborative applications.

In Figure 3 we can see that the information feeding process is highly relevant for the users. Particularly, the visual handheld-based feeding and the data sharing processes are the most needed for them. The access to the shared information on-demand through the map was also required (map navigation); however, the proactive delivery of warnings and alarms was considered invasive by various users.

In every service, the users also indicated three non-functional requirements as being the most relevant ones: information availability, trustworthiness, and the quick access to it. Other NFR such as information understandability were not too relevant for the users, because they assumed that the system cannot be put into production if it does not properly address this aspect of the information

	Requirement / Design Decision	Loosely-coupled data link	Handheld devices	Fast boot devices	Autonomous agents	Context-aware behavior	Crowsourcing	Map tiles	Positioning (e.g. through GPS)	Infrastructure-based communic. units	Ad hoc communication units	Human-based sensors	Witness units	Mules	Awareness mechanisms	Visual information w/explicit relevance	Social networking services	Reputation	Standard formats for data and services
NFR	High availability	M	M		M	M				O	O	O	O	O					
	Quick access	M		M				M							M	M			
	Proactivity				M	M									M	O			
	Information trustworthiness				M		M		M	A	A	O	O					M	
	Understandable information														M	M			
	Interoperability									O	O								M
FR	Map navigation							M	M						M	M			
	Device positioning								M		O	O	O	O					
	Communication	M								A	A			O					
	Device tracking								A	A							M		
	Visual handheld-based feeding	M	M	M					M	O	O	M				M			
	Data sharing				M					M	M	O	O	O			O		M
	Warnings/alarms delivery				M	M				O	O				M		O		

Note: *X - Mandatory*
A - Alternative
O - Optional

Figure 3. Correspondence matrix: requirements vs. design decisions.

DOI: 10.1002/cpe

delivery. The proactivity of the system was also few relevant for the users due the previously mentioned reason; i.e. they prefer to access the information on-demand and do not receive regularly the notifications of the system.

Figure 3 also shows various design decisions that can contribute to reach several FR and NFR. The most relevant ones are: the support for performing loosely coupled work, the use of autonomous agents for information processing, the use of positioning for determining the information relevance, the provision of awareness mechanisms to help users understand this information relevance, and the visual representation of such information. These design components must be addressed by developers of mobile applications that support participatory sensing.

5. SYSTEM EVALUATION

In this stage we have to determine if the system accomplishes with the FRs and NFRs specified in the previous section. In case of the FRs, the evaluation is objective and has a binary result; i.e. the system accomplishes or not with a certain requirement. This evaluation type is replicable; therefore, the obtained results can be verified using low effort.

In case of the NFRs, their accomplishment is represented as a value in a range, which usually requires the interpretation of system users and experts to determine if that quality of the product is acceptable to address the problem. Trying to reduce the subjectivity of these tests, it is recommended to determine a minimum acceptance level [35]; however, such a value is also subjective.

After evaluating the Personal Guardian system, the engineers in charge of the process determined that the application accomplished with all FRs. This does not mean that the system is usable and useful for end-users. In fact, determining usability and usefulness requires also that all NFRs of the system core achieve at least the minimum acceptance level. Therefore, the next sections describe the evaluation processes performed to determine the accomplishment level of these NFRs.

5.1. System availability

The availability of the system, in terms of the services that it provides, should be high. Therefore, each mobile device running the system should work autonomously instead of being connected to a remote resource. Thus, the system increases its performance and reduces the dependencies of remote units. Contrarily, software systems implementing participatory sensing must always try to use information as complete and updated as possible in order to generate and deliver appropriate notifications. This means that the system should try to work connected to the server, which is the node where the information is more complete and updated. Therefore, the system availability should be evaluated in these two scenarios.

Trying to determine this two-fold feature of the system, we evaluated the availability and performance of the main services provided to end-users, and then the information availability considering the whole information available in the network (i.e. in the HWSN). For the first case, we created a simulated area of 300 meters by 300 meters. Twenty annotations were available in the server for such area. After downloading these annotations to a smartphone running the PG system, we added five more annotations to the server and then we evaluated the main systems services in three different situations: when the system is connected to the server, when connected to a HBS (a neighbor with additional information of the area) and when it is disconnected. Ten times the person using the application accessed the study area. We simulated these accesses at different days and times to see the appropriateness of the notifications delivered by the system. Table I summarizes the main results.

As a first step, we manually identified the information that the system must show to the user and also the notifications that should be delivered, according to the annotations stored in the system and depending of the day and time at which the area is accessed. Then, we compared such data with the information actually displayed by the application during the simulations. The results indicate that the information was correctly shown in the three cases according to the local information stored in the smartphone. However there was an 8% (average) of outdated relevant information in the first

DOI: 10.1002/cpe

Table I. Evaluation results of the local services.

Service/work scenario	Connected to the server	Connected to a HBS	Disconnected
% of deployed notifications	100%	100%	100%
% of outdated relevant information	8%	10%	–
% of appropriate notifications	98%	94%	94%
Detection time of the obsolete information	5–6 s	3–5 s	–
Duration of the data synchronization	8–13 s	5–7 s	–

work scenario, due to the new annotations that we added to the server after the data synchronization process. Because of the same reason, such a percentage was 10% when the node was connected to a HBS, which was already updated and also had new annotations. The presence of outdated information had a low impact on the appropriateness of the notifications delivered to the user. If we consider only the local information stored in the mobile unit, the percentage of appropriate notifications was 100%. Therefore, the appropriateness of the notifications delivered by the PG system depends only on how update is the local information.

In this setting, the system requires less than 6 s to identify outdated relevant information and also to determine the percentage of such information portion. If that portion is over 20%, the mobile unit triggers a synchronization process for updating its local information and thus making appropriate diagnoses and notifications. The data synchronization process for a specific area took up to 13 s (mainly because of communication delays) and the diagnose process took between 1 and 2 s. The delivery of notifications can be considered as almost instantaneous after the system has a diagnosis of the area. Therefore, considering the current setting (i.e. a user, the server and a neighbor participating in the HWSN), in the worst case the mobile user would receive notifications with approximately 20 s of delay and a 94% of accuracy. Clearly the performance of these processes is inversely proportional to the accuracy of the results that they obtain.

The periodicity used by the system to re-check the current vulnerability of the user is configurable, and it typically depends on the speed to which the user is moving. For car drivers that time could be 15–30 s while for walking people usually is 60–90 s. A higher periodicity for re-checking makes the system more proactive, but it increases the energy consumption.

The results shown in Table I are just illustrative. The performance of the system should not change too much, given that the reference points for data synchronization and obsolescence calculation are always the server or the neighbor HBS that are to one hop of distance. However, there could be an important degradation of the diagnosis made by a mobile unit if the nodes belonging to the HWSN do not report frequently their local annotations to the server. Summarizing, the loosely coupled data link contributes to increase the information and services availability, but each node must also perform frequent data synchronization processes with the server to avoid degrade the accuracy of the diagnoses and notifications made to the end-users.

5.2. Delay to access the information and services

In the previous section we show part of the performance results of the system. Those results have a low dependence on the structure of the HWSN, because the system services mainly uses local information. Additionally to these tests, we have also measured the times involved in various other operations; most of them involving specific actions of the end-user. These operations were repeated ten times each and involved three users. Table II summarizes the average values of the obtained results. The standard deviation in all cases was low.

These numbers indicate low delays to access the system services and information, which make us to expect that the solution provides a ‘quick access’ (i.e. it overcomes the minimum acceptance level for this NFR).

5.3. System proactivity

Considering the problem that the application is trying to address, and the fact that the focus of this application is crime prevention, it is clear that the system proactivity is mandatory. In section 5.1 we

DOI: 10.1002/cpe

Table II. Delays to access system information and services.

Operation	Average delay
System start-up time	1 s
Delay in deploying a notification having a diagnosis	<0.5 s
Delay in deploying the visual information	<1 s
Delay in visualizing the after a zoom-in/out operation	<2 s
Delay in opening the vote service	<2 s
Delay in recording and computing a vote	<3 s
Delay in opening the annotation form	<2 s

indicated that the system triggers all notifications, and that these notifications are appropriate, according to the local information of the mobile unit being studied. In section 5.2 we indicated that the time to deploy a notification is less than 0.5 s once the system has a diagnosis of the area in which the user is located. The time to diagnose or recalculate a diagnosis is 1–2 s the setting specified in section 5.1. Therefore in the worst case in such a setting, the system will spend around 3 s to notify the user about a vulnerability situation based on the local information. This time involves 2 s for re-diagnosing, and 1 s for the notification delivery and (eventually) information deployment.

As mentioned in section 5.1, we have also to add the periodicity specified by the user for re-checking his vulnerability situation, which can affect considerably the system proactivity. However, if the time between re-checking points degrades the system proactivity, the only responsible for that situation will be the user, given that the system adds no more than 3 s of extra delay to each notification.

5.4. Information trustworthiness

In order to determine how trustworthy the information provided by the Personal Guardian system can be, we used the NS-3 simulator [36] to create a HWSN composed by the server (i.e. a WU) and 100 HBS. We simulated a voting process in which the HBS indicated if a piece of information about the vulnerability of a place is correct or incorrect. A vote per minute is added to the system, and after each vote the system recalculates the vulnerability of that place. If the system performs a wrong diagnose, because there are nodes that lie (non-trustworthy nodes), then we determined the time required by the system to make a right diagnose. We have called to such a metric *correction delay*. All voters had the same reputation and the order in which the nodes deliver their vote was random. Figure 4 shows the obtained results (average) after then simulation rounds.

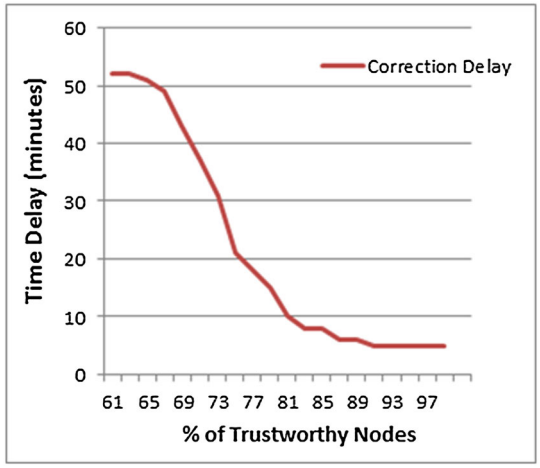


Figure 4. Usability evaluation results.

DOI: 10.1002/cpe

These results show that the HWSN requires at least a 60% of trustworthy nodes (i.e. nodes that do not lie) to reach a right diagnose after a wrong one. The time spent by the system to make such a correction depends on the percentage of trustworthy nodes. Correcting a wrong diagnose in a favorable scenarios (e.g. with over 90% of trustworthy nodes) could be up to ten times faster than in an unfavorable scenario (e.g. with 60–65% of trustworthy nodes). After each voting the reputation of the nodes is updated; therefore the trustworthy nodes increase their reputation, contrarily to the liar nodes. This means that the opinion of the trustworthy nodes during the next voting will be stronger, which reduces the times required to correct a wrong diagnose.

In this application scenario we can expect that most nodes do not lie, because there is a common interest for counting on right information to determine the people current vulnerability. Moreover, when an interest point reaches a right diagnosis involving high participating, it is difficult that liar nodes can change it. This makes us to expect that the system accomplishes with the minimum acceptance level to be useful in practice.

5.5. *System usability*

The information understandability was evaluated as part of the system usability. This evaluation involved end-users aged between 18 and 35 years old that extensively use smartphones and SNS. As an additional constraint, we limited the evaluation to the city of Santiago, Chile, in order to have a common geographical context within the group of evaluators. The usability attributes considered in the evaluation were the system learnability and the user satisfaction; and the assessment techniques used were questionnaire, and observation and thinking aloud [37].

The sample was formed by following typical recommendations in usability testing [38, 39]. On one hand, the *questionnaire* consisted of items graded in a 5-point Likert scale that intended to assess satisfaction and learnability. It was applied to 20 evaluators once they have used the application. On the other hand, we applied the *observation and thinking aloud* technique to a group of five evaluators. We assigned them a set of tasks to be performed by interacting with the application and we noted relevant observations regarding their performance (i.e. task easily completed, completed, completed with difficulty, or not completed) and user experience (i.e. spontaneous reactions indicating frustration and/or ease of use). Figure 5 shows the median score assigned to each item in the questionnaire.

According to the evaluators, the current design of the application allows an easy navigation. However, the information architecture (at the user interface) can be improved, as the evaluators consider that some elements are not intuitive, as well as the logic behind the organization of some visual elements. A plausible explanation to this latter result may be linked to the lack of familiarity of evaluators with social applications specifically designed to provide awareness in security matters. Regarding the esthetics and graphical design of the application, the evaluators liked this particular point, as the fonts and used colors are sober and try to enhance the value of the information that is

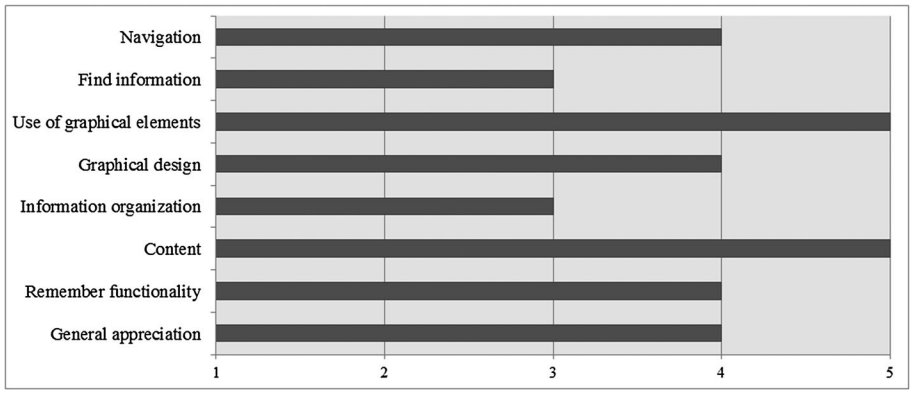


Figure 5. Usability evaluation results.

DOI: 10.1002/cpe

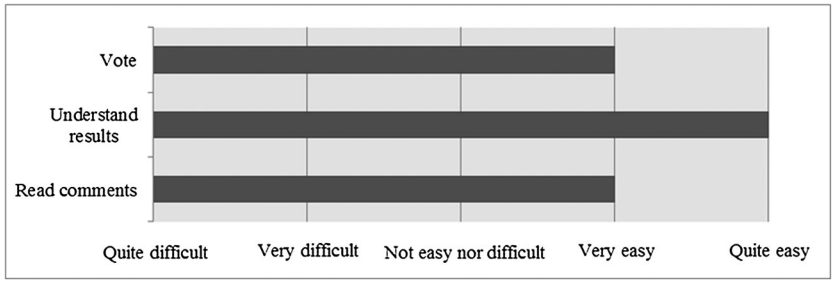


Figure 6. Perceived complexity for task achievement.

presented in the interface. Moreover, the evaluators praised the content of the application, as they consider it to be relevant and useful in the context for what the service is provided.

Next we present the results of the evaluation using the *observation and thinking aloud* techniques. Figure 6 shows the median value for the perceived ease or difficulty for achieving the proposed tasks: (1) voting for a particular place, (2) understanding the presented results, and (3) reading comments.

According to the results, the three proposed tasks were perceived as easy to achieve. Regarding the spontaneous comments stated by the evaluators, there was no difficulty for integrating *Facebook* as a SNS working with the application. However, two users showed frustration when deciding how to cast a vote for a particular spot. This was partly due to a problem when launching the application, since it displayed sometimes a spot that was not known or recognized beforehand by the evaluators.

This was improved in the next iteration in the development life cycle of the application. The system performance was not formally evaluated in this stage, but it was indirectly evaluated through the system usability. No evaluator mentioned this issue, which probably means that the system performance was considered as appropriate.

Concerning the interoperability aspect, which is the last NFR considered in the system, it was not formally evaluated. However, such a requirement was addressed through the use of information representation in XML and implementation of services in WS format. Thus adhering to well-known standards for data and services representation we tried to address this last NFR.

6. CONCLUSIONS AND FUTURE WORK

Crime is still an open issue in most countries, particularly in large urban areas. The current mechanisms to provide personal security are not particularly focused on helping potential victims to easily determine their inherent risk to crimes in real-time. Therefore, their capability to take appropriate and on-time preventive actions is diminished. Trying to help address that problem, this article proposes a participatory sensing system (named Personal Guardian—PG) that complements the already used solutions by government organizations. The PG system is a mobile collaborative application based on a human-centric wireless sensor network, in which most nodes are human-based sensors (represented by civilians using smartphones).

This system uses participatory sensing, human-based sensors and regular sensors to collect information from the field, and utilizes several awareness mechanisms to inform the users about their current personal security risks. The information provided by the system can also be used to build a spatiotemporal view of crime (e.g. by incident type) that allows security organizations to understand its evolution and improve the prevention/fight actions.

The functional and non-functional requirements of the system were determined with the help of end-users and also experienced developers. These requirements indicate that the feeding process is the most important feature for the users. Moreover, they prefer to access on-demand the information provided by the system; i.e. the proactive notifications were not valuable for them. However, most users agreed that a context awareness mechanism for delivering these notifications could reach the original goal without bothering end-users. The provision of this mechanism will require modeling the users, and keeping and evolving their preferences according to the users' behavior.

DOI: 10.1002/cpe

The most relevant NFR for users were the information availability and trustworthiness, and also the quick access to such information. This means that the users realize the role of the time in the use of this application; i.e. the system must be available when required, and in these applications it must provide quick, trustworthy, and understandable information to the end-user. In case of the feeding process, the application must allow the user to do a quick and anonymous report of a situation, without compromising his personal security.

The functional and non-functional requirements of the system were evaluated involving formal tests. Particularly the evaluation of NFRs indicates that the system availability, performance, proactivity, trustworthiness (in terms of the advices that it delivers), and understandability overcome the quality minimum acceptance level to address the problem by the end-users.

The usability of the system was identified as a highly important feature; therefore it was evaluated using two complementary techniques and a new set of users. The obtained results allowed us to determine the need to adjust some components of the user interface, even though they were minor issues. The system performance and the pertinence of the warnings given by the application were not formally evaluated at this stage. However, they were indirectly assessed through the activity test performed by the evaluators. Our preliminary feelings indicate that these aspects of the solution are at least between the regular values that a user can expect for these systems.

Concerning the information feeding and delivering processes, they were performed in a suitable way according to users. The former process kept the high relevance identified in the requirement elicitation. These results indicate that the proposed system is usable and useful for addressing the stated problem.

The article also presents a correspondence matrix where we indicate the design decisions made to address the FRs and NFRs. That matrix represents reusable knowledge that can help other software designers to address the development of mobile collaborative systems when they are based on a HWSN or similar structures.

The next step in this initiative is to evaluate the quality aspects of the solution that were not considered in this first stage. Moreover, we want to evaluate the information flow in the field using different quantities and distribution of WUs. This is a research issue that this initiative wants to explore, because it could indicate that, by increasing the number of witness units and HBS, society could become more resilient to physical delinquency and crime. Such a strategy will be particularly focused on crime prevention.

ACKNOWLEDGEMENTS

This work has been partially supported by the Fondecyt Project (Chile), grant: 1120207. The work of Francisco J. Gutierrez has been supported by the Ph.D. Scholarship Program of Conicyt Chile (CONICYT-PCHA/Doctorado Nacional/2013-21130075).

REFERENCES

1. Aebi MF, Linde MF. Conviction Statistics as an Indicator of Crime Trends in Europe from 1990 to 2006. *European Journal on Criminal Policy and Research* 2012; **18**:103–144.
2. Federal Bureau of Investigation. Crime in The United States 2010 - FBI Statistics. (Available at: http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/tables/10tbl01.xls) [May 17, 2014].
3. Dubbeld L. Observing Bodies: Camera Surveillance and the Significance of the Body. *Ethics and Information Technology* 2003; **5**(3):151–162.
4. Posner RA. Privacy, Surveillance and Law. *The University of Chicago Law Review* 2008; **75**(1):245–260.
5. Travis A. CCTV Schemes in City and Town Centres Have Little Effect on Crime. (Available at: http://www.guardian.co.uk/uk/2009/may/18/cctv-crime-police) [May 17, 2014].
6. Cattelino JR. The Difference that Citizenship Makes: Civilian Crime Prevention on the Lower East Side. *Political and Legal Anthropology Review* 2008; **27**(1):114–137.
7. Howe J. *Crowdsourcing: Why the power of the crowd is driving the future of business*. Crown Business: New York, USA, 2008.
8. Lim SL, Quercia D, Finkelstein A. StakeSource: Harnessing the power of crowdsourcing and social networks in stakeholder analysis. *Proceedings of the 32nd ACM/IEEE International Conference on Software Engineering (ICSE'10)*. Cape Town, South Africa, 2010.
9. Burke J, Estrin D, Hansen M, Parker A, Ramanathan N, Reddy S, Srivastava MB. Participatory Sensing. *Proceedings of the World Sensor Web Workshop*, in Conjunction with ACM SenSys'06, 2006.
10. Campbell A, Eisenman S, Lane N, Miluzzo E, Peterson R. People-centric Urban Sensing. *Proceedings of 2nd Annual Int. Wireless Internet Conference (WICON'06)*, 2006.

DOI: 10.1002/cpe

11. Ochoa SF, Santos R. Human-centric Wireless Sensor Networks to Improve Information Availability During Urban Search and Rescue Activities. *Information Fusion* 2015; **22**.
12. United Nations Development Programme. New Dimensions of Human Security. *Human Development Report*, 1994. (Available at: http://hdr.undp.org/en/reports/global/hdr1994/) [May 17, 2014].
13. Safety - OECD Better Life Index. (Available at: http://www.oecdbetterlifeindex.org/topics/safety/) [May 17, 2014].
14. Von Hirsch A, Garland D, Wakefield A. *Ethical and Social Perspectives on Situational Crime Prevention*. Hart Publishing: Oxford, UK, 2004.
15. Clarke R. Situational Crime Prevention. In *Building a Safer Society: Strategic Approaches to Crime Prevention*, Tonry M, Farrington D (eds). University of Chicago Press: Chicago, USA, 1995.
16. Partridge H. Developing a Human Perspective to the Digital Divide in the Smart City. *Proceedings of the ALIA 2004 Biennial Conference – Challenging Ideas.* Kingstone, Australia, 2004.
17. Nam T, Pardo TA. Conceptualizing Smart City with Dimensions of Technology, People, and Institutions. *Proceedings of the 12th Annual International Conference of Digital Government Research*. College Park MD, United States, 2011.
18. Schuurman D, Baccarne B, De Marez L, Mechant P. Smart Ideas for Smart Cities: Investigating Crowdsourcing for Generating and Selecting Ideas for ICT Innovation in a City Context. *Journal of Theoretical and Applied Electronic Commerce Research* 2012; **7**(3):49–62.
19. Hall D, Chong C-Y, Llinas J, Liggins M. *Distributed Data Fusion for Network-Centric Operations*. CRC Press: Boca Raton, USA, 2012.
20. Lan K-C, Chou C-M, Wang H-Y. An Incentive-Based Framework for Vehicle-Based Mobile Sensing. *Procedia Computer Science*, 2012; 1–6.
21. Ballesteros J, Rahman M, Carbunar B, Rishe N. Safe Cities. A Participatory Sensing Approach. *Proceedings of the 37th IEEE Local Computer Networks Conference (LCN'12).* Clearwater Beach, USA, 2012.
22. Wang X, Cheng W, Mohapatra P, Abdelzaher T. ARTSense: Anonymous Reputation and Trust in Participatory Sensing. *Proceedings of the 32nd IEEE International Conference on Computer Communications.* Turin, Italy, 2013.
23. Ouyang RW, Srivastava A, Prabahar P, Choudhury RR, Addicott M, McClernon FJ. If You See Something, Swipe Towards It: Crowdsourced Event Localization Using Smartphones. *Proceedings of UbiComp '13.* Zurich, Switzerland, 2013.
24. Estrin D. Participatory sensing: applications and architecture. *IEEE Internet Computing* 2010; **14**(1):12–42.
25. Duarte S, Navalho D, Ferreira H, Preguica N. Scalable Data Processing for Community Sensing Applications. *Mobile Networks and Applications* 2013; **18**(3):357–372.
26. Carreño P, Gutierrez F, Ochoa SF, Fortino G. Using Human-centric Wireless Sensor Networks to Support Personal Security. *Proc. of the 6th Int. Conf. on Internet and Distributed Computing Systems (IDCS13)*, LNCS 8223, pp. 51-64. Hangzhou, China. Oct. 28-30th, 2013.
27. Bellifemine F, Fortino G, Giannantonio R, Gravina R, Guerrieri A, Sgroi M. SPINE: A domain-specific framework for rapid prototyping of WBSN applications. *Software Practice and Experience* 2011; **41**(3):237–265.
28. Fortino G, Giannantonio R, Gravina R, Kuryloski P, Jafari R. Enabling Effective Programming and Flexible Management of Efficient Body Sensor Network Applications. *IEEE Transactions on Human-Machine Systems* 2013; **43**(1):115–133.
29. Raveendranathan N, Galzarano S, Loseu V, Gravina R, Giannantonio R, Sgroi M, Jafari R, Fortino G. From Modeling to Implementation of Virtual Sensors in Body Sensor Networks. *IEEE Sensors Journal* 2012; **12**(3):583–593.
30. Rodríguez-Covili JF, Ochoa SF, Pino JA, Messeguer R, Medina E, Royo D. A Communication Infrastructure to Ease the Development of Mobile Collaborative Applications. *Journal of Network and Computer Applications* 2011; **34** (6):1883–1893.
31. Fortino G, Parisi D, Pirrone V, Di Fatta G. BodyCloud: A SaaS Approach for Community Body Sensor Networks. *Future Generation Computer Systems* In Press, DOI: doi.org/10.1016/j.future.2013.12.015.
32. Monares A, Ochoa SF, Pino JA, Herskovic V, Rodriguez-Covili J, Neyem A. Mobile Computing in Urban Emergency Situations: Improving the Support to Firefighters in the Field. *Expert Systems with Applications* 2011; **38**(2):1255–1267.
33. Huang K, Kanhere SS, Hu W. Are You Contributing Trustworthy Data? The Case for A Reputation Framework in Participatory Sensing. *Proceedings of ACM MSWiM*, Bodrum, Turkey, 2010.
34. Mashhadi AJ, Capra L. Quality control for real-time ubiquitous crowdsourcing. *Proceedings of UbiCrowd'11.* Beijing, China, 2011.
35. Gilb T, Finzi S. *Principles of Software Engineering Management*. Addison Wesley, 1988.
36. Network Simulator (NS-3). (Available at: http://www.nsnam.org/) [May 17, 2014].
37. Aitken LM, Marshall A, Elliott R, McKinley S. Comparison of 'think aloud' and observation as data collection methods in the study of decision making regarding sedation in intensive care patients. *International Journal of Nursing Studies* 2011; **48**(3):318–325.
38. Holzinger A. Usability engineering methods for software developers. *Communications of the ACM* 2005; **48**(1):71–74.
39. Nielsen J. *Usability Engineering*. AP Professional: Cambridge, UK, 1993.

DOI: 10.1002/cpe