Using Human-Centric Wireless Sensor Networks to Support Personal Security

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

[1] Computer Science Department, Universidad de Chile
Av. Blanco Encalada 2120, 3rd floor, Santiago, Chile
{pcarreno,frgutier,sochoa}@dcc.uchile.cl
[2] DIMES, Università della Calabria
Via P. Bucci, cubo 41C, 87036 Rende (CS), Italy
g.fortino@unical.it

Abstract. Violence and crime in large urban areas are a worldwide problem that is still open. After several attempts to reduce its occurrence and impact, there seems to be an agreement that crime preventive actions, which can be taken by citizens and security organizations, are the best way to address it. This paper proposes the use of human-centric wireless sensor networks to help address this problem, and the proposed solution is complementary to those already used by security organizations. The architecture and main components of these networks are described in detail. The article also describes a software system that implements most of the components of these networks. Such a system helps 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. A preliminary evaluation of the system has been conducted, and the obtained results are also presented and discussed.

Keywords: Personal security, crime prevention, participatory sensing, human-centric wireless sensor networks, crowdsourcing, social computing.

1 Introduction

Everyday more and more applications link their functionality to social networking services (SNS) in some way. SNS capabilities, like crowdsourcing, can contribute to address challenges that were not easy to tackle in the past; particularly those requiring people opinions or observations [16, 19]. One of these problems is crime (e.g. assault, robbery, rape, vandalism, physical aggressions, and also murders) that is still an open issue in most countries around the world. Although government organizations are continually working to improve the personal security of civilians, crime rate does not seem to change too much [1, 11].

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 [9, 24, 28]. For

M. Pathan, G. Wei, and G. Fortino (Eds.): IDCS 2013, LNCS 8223, pp. 51–64, 2013.

instance, these types of solutions do not have a good scalability, because it is not feasible to flood a city with surveillance cameras or police personnel that can be active all the time protecting civilians. The cost and complexity of these solutions make them not feasible, even for developed countries.

Conscious of such situation, during the last years government organizations have involved citizens to a greater extent (e.g. through anonymous reports of crimes or suspicious activities) in the process of crime prevention. This has allowed them 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.

This article proposes the use of a participatory sensing strategy [4, 5], supported by a human-centric wireless sensor network [23], to help tackle the stated problem. The solution empowers ordinary citizens to collect and share security information from their surrounding environments, using their mobile phones in an easy and anonymous way. Considering the information provided by multiple participants, it is possible to perform an online diagnosis that allows civilians being aware of their current risk and personal security level, while they move through urban areas. The article also reports the design, development and evaluation of a mobile application that implements most of the components of this proposal.

Next section presents the related work. Section 3 briefly introduces the concept of human-centric wireless sensor networks. Section 4 discusses the main requirements and design decisions made in the system implementation. Section 5 describes the structure and main components of the solution. Section 6 shows and discusses the preliminary results. Section 7 presents the conclusions and the future work.

2 Related Work

Personal security can be understood as the level of protection of a person from intentional criminal acts [29]. It is considered a core element of the well-being of individuals. The OECD Better Life Index reports that 4.0% of people in OECD countries say they have been assaulted or mugged over the past 12 months, and the average homicide rate in those countries is 2.2 murders per 100,000 inhabitants [27].

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* [30]. Situational prevention seeks to reduce opportunities for specific categories of crime, by increasing difficulties to perform those actions and decreasing the associated risks and rewards [7]. 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 the personal security in many areas of a city, even while living in that place. This lack of information can be

managed in different ways by people. 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 (e.g. newspaper articles). For example, neighborhood programs and patrols can provide friendly, non-invasive support for members in a community, aiming to help these people feel better connected to the neighborhood and help them reduce their 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 long documents), thus being perceived as difficult to understand. Particularly, this is a problem when individuals are faced to quickly and accurately find out the inherent risk of a particular area at a particular time.

Burke et al. [4] introduced the concept of *participatory sensing*. It 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, the growth in mobile devices (e.g. smartphones) has deployed hardware capabilities in the form of multiple sensors (e.g. motion sensor or accelerometer, gyroscope, ambient light sensor). These sensors 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 [14].

Naturally, one of the critical factors to drive success in participatory sensing is related to the data collecting from users in order to generate collective intelligence. Lan et al. [18] proposed an incentive scheme for a vehicle-based mobile surveillance system by adopting participatory sensing, 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. [2] studied a set of techniques for evaluating the 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.

Estrin [10] proposed a layered architecture to support participatory sensing. The data collection performed using that architecture requires a permanent link between the sensors and the server that stores and manages the data. The dependence of particular components (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. [8] 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. Ochoa and Santos [23] go a step even further proposing a human-centric wireless sensor network

(HWSN), which include 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, in any area. Therefore, it is the alternative chosen to support participatory sensing in the described scenario.

3 Human-Centric Wireless Sensor Networks

These networks are heterogeneous in terms of the 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 heterogeneous, and they can play up to four roles: *regular sensors*, *human-based sensors*, *mules* and *witness units*. Regular sensors (RS) measure a certain context variable and transmits their value to other units. Examples of these sensors are GPS, temperature sensors, wearable sensors (also used as Body Sensor Networks - BSNs [3, 12]), and also mobile devices able to detect the presence of other devices (i.e. sensors) in the area. The 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. the 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 our best option when the observed variable is not measurable with a regular sensor but by means of virtual/logical sensors [25].

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 usually also act as 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 (e.g. about personal security) that is relevant in the area where the WU is located. 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.

Figure 1 shows the architecture of a HWSN, which is typically 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. 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.

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, and eventually in remote servers or on Cloud computing infrastructures [13]. These components are part of the information persistence layer.

Fig. 1. Layered architecture of a human-centric wireless sensor network

Finally, the mobile systems are in the application layer, which use the information managed by the lower layers to provide a direct service to the end-users; for instance to inform them their current personal security level. It is important to note that the 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.

4 Main Requirements and Design Decisions

The design of the mobile application that informs the people about their current personal security level should consider several functional (FR) and non-functional requirements (NFR). These requirements were obtained and validated through a focus group with twelve potential users of the system. By addressing these requirements the application has a chance of being usable and useful in a real scenario. Next we describe the main non-functional requirements that were defined, and also the design decisions made to address them.

- *High availability*. The system should be available independently of the possibility to access remote servers (i.e. WUs). For that reason, the geographical information of an area and also 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 WUs 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 for additional information or for a complete vulnerability diagnosis. Interactions with other network nodes require counting on access to infrastructure based on 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 most of the time with the user. Considering these restrictions, a handheld device like a smartphone or a small slate seems to be the most appropriate option for deploying the system.

- *Quick access*. In case that the user wants to get personal security information on-demand, the access to such information should be quick, and 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 can depend on it. 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.

- *Proactiveness.* 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 all the time, monitoring and evaluating the personal security context of the user. Usually this functionality is implemented through an autonomous agent. An alarm should be triggered every time that a vulnerability situation exceeds a certain threshold. Depending on its criticality, more than one alarm can be triggered using awareness mechanisms, e.g. visual messages, ringtones or tactons.

- *Information trustworthiness*. When a service quality depends on the quality of the information that it provides, the information trustworthiness becomes a critical requirement. Although there are several strategies to address this requirement, the recent research in participatory sensing indicates that crowdsourcing and reputation is usually a good combination to deal with this issue [17, 20]. Data held by other network nodes and WUs can also contribute to increase the trustfulness of the information.

- *Understandable information*. The system must notify to its users, as soon as possible, when they are in risk. Therefore, the information that the system provides them should be easy to understand by average users. In that sense, the use of visual information and voice messages seem to be appropriate to address this requirement in most work contexts. In case of messages indicating physical locations, the use of geo-referenced visual information (e.g. a map) is usually the easiest way to provide an effective communication to end-users. Provided that an

effective communication requires that input and output channels be aligned, awareness mechanisms are usually required to do that.

- *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.

Moreover, there is a list of FRs that can also be addressed by the system. The services that address those requirements must also deal with the previously presented NFR.

- *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 and GPS positively impact usability and performance of these systems [21].

- *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 only GPS can lead the system to make some error when the user is indoor, this strategy considerably reduces the complexity to implement services that perform device positioning. Devices not having positioning capabilities can request such information to neighbor nodes using ad hoc communication services.

- *Communication*. The information provided by the crowd should be shared as soon as possible to benefit the participants and reduce the feasibility that malicious interventions affect the trustworthiness of the shared data. In both cases, counting on communication among participants is mandatory. Such a communication can be done using ad hoc or infrastructure-based communication systems, or a combination of them. Typically the former helps addressing 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 allows supporting properly the crowd activities. This communication modality helps diagnosing the personal security of an ample range of users, from pedestrians to car drivers.

- *Device tracking*. This requirement allows remote users to monitor the movements of a user on a map. Typically it is required when the user is asking for help to someone else, e.g. friends or family. The tracking capability can be implemented using device positioning and communication; and the grants for monitoring the user movements can be implemented using the user's personal contacts from a SNS (like Facebook).

- *Easy 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 done using handheld devices that are easy to transport, deploy and use, and 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. 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 can contribute to enhance the data sharing among network nodes, which positively impacts on the availability, performance and trustworthiness of the whole system.
- *Warnings/alarms delivery.* The main goal of the system is to deliver notifications to users, in order to make them aware of their current vulnerability situation. The evaluation of users vulnerability requires geo-localization (GPS) to determine the users' position, and awareness mechanisms to inform them 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.

Figure 2 summarizes the relationship among the main FR, NFR and design decisions involved in the system. The relationship also indicates whether a design element is mandatory, optional or not required to implement a certain requirement.

Requirement / Design Decision	Loosely-coupled data link	Handheld devices	Fast boot devices	Autonomous agents	Context-aware behavior	Crowsourcing	Map tiles	GPS	Infrastructure-based comm. units	Ad hoc communication units	Human-based sensors	Witness units	Mules	Awareness mechanisms	Visual information	Social networking services	Reputation	Standard formats for data and services
High availability	X	X							O	O		O						
Quick access	X		X				X								X			
Proactiveness				X	X									X				
Information trustwortiness						X			O	O	O	O					X	
Understandable information														X	X			
Interoperability									O	O								X
Map navigation							X	X							X			
Device positioning								X		O	O	O	O					
Communication									O	O			O					
Device tracking								X	X							X		
Easy feeding	X	X	X					X	O	O	X				X			
Data sharing				X					X	X	O	O	O			O		
Warnings/alarms delivery									O	O				X		O		

Note: *X - Mandatory*
O - Optional

Fig. 2. Correspondence matrix: requirements vs. design decisions

5 System Implementation

The current implementation of the system determines the risks of a user to car theft and vandalism, regular delinquency (robbery and assaults), drugs traffic and disturbance (physical violence). Figure 3 describes the technologies and components used in the system implementation. The system architecture adheres to the architecture of a HWSN (see Figure 2).

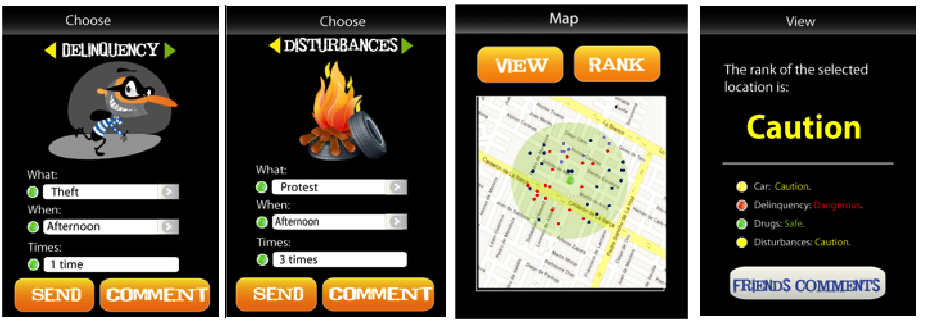
Fig. 3. Architecture of the implemented system

The sensing 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. Fig.4.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. The users indicate on a digital map the exact location of the events, and the GPS geo-references that information.

The system considers a 3G connection with a server (WU) and WiFi-based mobile ad hoc network that is implemented using an High Level MANET Protocol (HLMP) infrastructure [26]. 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.

The information persistence layer considers the participation of WU and HBS. Two particular WUs play a key role in the system: 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.



(a) (b) (c)

Fig. 4. User interfaces of the implemented system

In the application layer, we can see the information about the user vulnerability. Fig. 4.b. shows the user current location and the records of incidents in an area of 200 meters around him/her. Fig. 4.c. shows the information that the system deliver 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 system 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.

6 Results

Section 4 highlighted the importance of the usefulness and usability concerns in the design of the system. Therefore, we conducted a usability evaluation with end-users in order to assess at what extent these concerns were considered. As target end-users, we worked with individuals 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: learnability and satisfaction, and the assessment techniques used were: *questionnaire*, and *observation and thinking aloud*.

The sample was formed by following typical recommendations in usability testing [15, 22]. 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 5 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). Fig. 5 shows the median score assigned to each item in the questionnaire.

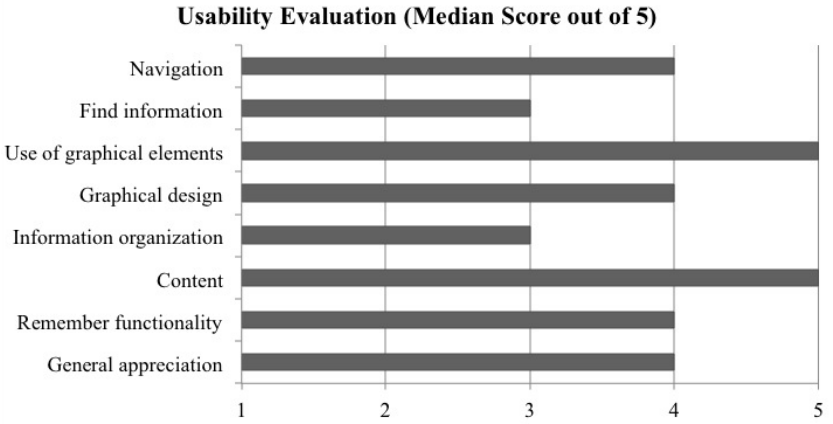


Fig. 5. Usability evaluation results

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 difficult to find, 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 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* technique. Fig. 6 shows the median 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.

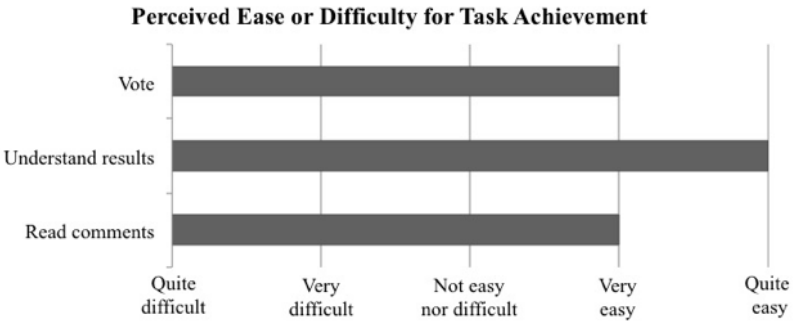


Fig. 6. Perceived ease or difficulty for task achievement

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.

7 Conclusions and Future Work

The current mechanisms to provide personal security are not particularly focused on helping potential victims 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 addressing that problem, this article proposes a participatory sensing system that complements the already used solutions by government organizations. The system is based on a human-centric wireless sensor network. It uses crowdsourcing, human-based sensors and regular sensors to collect information from the field, and 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 usability of the system was evaluated using two different techniques. The obtained results allowed us to identify 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.

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. That 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.

Acknowledgments. This work has been partially supported by the Fondecyt Project (Chile), grant: 1120207. The work of Francisco Gutierrez has been supported by the Conicyt (Chile) Ph.D. scholarship.

References

1. Aebi, M.F., Linde, M.F.: Conviction Statistics as an Indicator of Crime Trends in Europe from 1990 to 2006. European Journal on Criminal Policy and Research 18, 103–144 (2012)
2. Ballesteros, J., Rahman, M., Carbunar, B., Rishe, N.: Safe Cities. A Participatory Sensing Approach. In: Proceedings of the 37th IEEE Local Computer Networks Conference (LCN 2012), Clearwater Beach, United States (2012)
3. 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 41(3), 237–265 (2011)
4. Burke, J., Estrin, D., Hansen, M., Parker, A., Ramanathan, N., Reddy, S., Srivastava, M.B.: Participatory Sensing. In: Proceedings of the World Sensor Web Workshop, in Conjunction with ACM SenSys 2006 (2006)
5. Campbell, A., Eisenman, S., Lane, N., Miluzzo, E., Peterson, R.: People-centric Urban Sensing. In: Proceedings of 2nd Annual Int. Wireless Internet Conference, WICON 2006 (2006)
6. Cattelino, J.R.: The Difference that Citizenship Makes: Civilian Crime Prevention on the Lower East Side. Political and Legal Anthropology Review 27(1), 114–137 (2008)
7. Clarke, R.: Situational Crime Prevention. In: Tonry, M., Farrington, D. (eds.) Building a Safer Society: Strategic Approaches to Crime Prevention, University of Chicago Press, Chicago (1995)
8. Duarte, S., Navalho, D., Ferreira, H., Preguica, N.: Scalable Data Processing for Community Sensing Applications. Mobile Networks and Application 18(3), 357–372 (2013)
9. Dubbeld, L.: Observing Bodies: Camera Surveillance and the Significance of the Body. Ethics and Information Technology 5(3), 151–162 (2003)
10. Estrin, D.: Participatory sensing: applications and architecture (Internet Predictions). IEEE Internet Computing 14(1), 12–42 (2010)
11. Federal Bureau of Investigation. Crime in The United States 2010 - FBI Statistics, `http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/tables/10tbl01.xls` (last access: July 12, 2013)
12. 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 43(1), 115–133 (2013)
13. Fortino, G., Parisi, D., Pirrone, V., Di Fatta, G.: BodyCloud: A SaaS Approach for Community Body Sensor Networks. To appear in Future Generation Computer Systems (2014)
14. Hall, D., Chong, C.-Y., Llinas, J., Liggins, M.: Distributed Data Fusion for Network-Centric Operations. CRC Press, Boca Raton (2012)
15. Holzinger, A.: Usability engineering methods for software developers. Communications of the ACM 48(1), 71–74 (2005)

16. Howe, J.: Crowdsourcing: Why the power of the crowd is driving the future of business. Crown Business, New York (2008)
17. Huang, K., Kanhere, S.S., Hu, W.: Are You Contributing Trustworthy Data? The Case for A Reputation Framework in Participatory Sensing. In: Proceedings of ACM MSWiM, Bodrum, Turkey (2010)
18. Lan, K.-C., Chou, C.-M., Wang, H.-Y.: An Incentive-Based Framework for Vehicle-Based Mobile Sensing. Procedia Computer Science, 1–6 (2012)
19. Lim, S.L., Quercia, D., Finkelstein, A.: StakeSource: Harnessing the power of crowdsourcing and social networks in stakeholder analysis. In: Proceedingsof the 32nd ACM/IEEE International Conference on Software Engineering (ICSE 2010), Cape Town, South Africa (2010)
20. Mashhadi, A.J., Capra, L.: Quality control for real-time ubiquitous crowdsourcing. In: Proc. of UbiCrowd 2011, Beijing, China (2011)
21. Monares, A., Ochoa, S.F., Pino, J.A., 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 38(2), 1255–1267 (2011)
22. Nielsen, J.: Usability Engineering. AP Professional, Cambridge (1993)
23. Ochoa, S.F., Santos, R.: Human-centric Wireless Sensor Networks to Improve Information Availability During Urban Search and Rescue Activities. Information Fusion (in press, to appear, 2014)
24. Posner, R.A.: Privacy, Surveillance, and Law. The University of Chicago Law Review 75(1), 245–260 (2008)
25. 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 12(3), 583–593 (2012)
26. Rodríguez-Covili, J.F., Ochoa, S.F., Pino, J.A., Messeguer, R., Medina, E., Royo, D.: A Communication Infrastructure to Ease the Development of Mobile Collaborative Applications. Journal of Network and Computer Applications 34(6), 1883–1893 (2011)
27. Safety - OECD Better Life Index, http://www.oecdbetterlifeindex.org/topics/safety/ (last visit: July 11, 2013)
28. Travis, A.: CCTV Schemes in City and Town Centres Have Little Effect on Crime, says Report, http://www.guardian.co.uk/uk/2009/may/18/cctv-crime-police (last visit: July 20, 2013)
29. United Nations Development Programme. New Dimensions of Human Security. Human Development Report (1994), http://hdr.undp.org/en/reports/global/hdr1994/ (last visit: July 12, 2013)
30. Von Hirsch, A., Garland, D., Wakefield, A.: Ethical and Social Perspectives on Situational Crime Prevention. Hart Publishing, Oxford (2004)