Enhancing Disaster Management by Taking Advantage of General Public Mobile Devices: Trends and Possible Scenarios

Olivier Sébastien, Fanilo Harivelo

Enhancing disaster management by taking advantage of general public mobile devices: trends and possible scenarios

Olivier SEBASTIEN, Fanilo HARIVELO
Laboratoire d'Informatique et de Mathématiques,
University of Réunion

Introduction

When a crisis occurs, particular infrastructures that are specific to the emergency situation are deployed in order to support rescue operations. Indeed, the normally used ones may have suffered from the disaster resulting in an altered service or may not be available at all. This process concerns physical (logistics) as well as immaterial (information) items delivery. Nowadays, a special emphasize has been put on the latter as it has been proven ([CAM 12], [TAN 09] and [LEF 14]) that it is a major requirement to ensure that the former is realized properly and more generally to address the crisis. Generally, required information aims at answering to the following basic questions: What (happened)? When (did it happened)? Where (is the disaster located)? And possibly How (can it be reached)?

That is why research and development works have been led to create technologies that can manage information acquisition and delivery in harsh environments: specific communication networks, rugged equipment, solar-powered devices, etc. Those means are dedicated to risk and emergency experts who are specially trained to evolve under difficult circumstances and the tools they rely on are designed to cope with this context.

But on the other hand, a new generation of mobile consumer electronic devices has appeared during the past decade: smartphones, tablets, connected devices, etc. They have been adopted all over the world at an astonishing rate so that Gartner claims that more than one billion units of smartphones were sold during 2014 [GOA 15]. This phenomenon was made possible by the combination of several factors: decrease of prices, improvement of many multimedia features and of course availability of an appropriate communication infrastructure. All of this has been the support for new usages which are very popular among the population, such as social networking, permanent possibility to reach somebody and ability to produce information in addition to consulting what was produced by others (as it was in the past). Current development work aims at making digital personal devices more "aware" of user environment [KHA 13], in order to have them automatically assist him/her in each encountered situation.

Therefore, one may legitimately wonder whether it would be possible to take advantage of this new trend to gather information and communicate with victims when a crisis occurs. The idea is not to replace the professional equipment and networks but to add new ways of interacting with the terrain of a disaster at every stages of the phenomenon. In this chapter, we thus aim at presenting how this can be achieved, what the parameters that efficiency rely on are and discuss what issues can

be encountered and why.

To browse a realistic panel of the situation, we propose the following path: in a first part, we will depict an overview of crisis management as it is in mid-2010's that is to say the actors and the way information technologies play a major role in their duty. Then we will move to mobile equipment and proximity communication aspects in order to show what can be expected from non-dedicated devices and network protocols in information gathering and in-situ transmission. Finally, we will focus on how mobile devices and proximity networks-assisted crisis management operations can be led.

1 Crisis management overview

The goal of this section is to shed light on main processes that are implemented by the various actors of risk management, quite independently from how they achieve them. We will also evoke the difficulties that can be encountered. This will allow us in the forthcoming section do draw a link with the new trend we would like to describe using general public devices and infrastructures. We will start with listing the different actors involved.

1.1 Actors

As far as actors are concerned, a separation can be made between risk professionals and the population.

1.1.1 Risk professionals

This category of actors involves people that have acquired dedicated skills to manage emergency situations (including civilian volunteers that resides in the area) as well as stakeholders, who have to take decisions in the context of a disaster.

Professionals operating physically on the terrain are experts in various domains: rescue teams, firemen, Emergency Service Unit (ESU) members, etc. Their profile of course depends on the type of disaster that must be addressed. They have two points in common. Firstly, the fact that they have been specifically trained to act accordingly under harsh circumstances and to make use of professional-level procedures and devices. Secondly, they evolve in the area of the crisis, that is to say they do not have an overview of the situation, they work at a very localized level.

Stakeholders on the other hand have a globalized view in order to allow them to take decisions in addressing the crisis. What is critical to them, more than the formers, is to have reliable information in the shortest time possible. For example, distribution of the population density at the time a disaster strikes is precious information to set priorities in emergency resources allocation because it will raise chances to rescue more people within a single terrain operation.

Both terrain experts and stakeholders share the fact that they are very few in comparison to the population. This is a drawback as well as an advantage as they are clearly identified and a clear communication channel between them exist most of the time.

1.1.2 Population

People living in the area a disaster occurs constitute most of the actors. They are the potential victims as an unknown amount of them at the time a phenomenon strikes is to be impacted: they may be injured, buried, flooded or even if they are safe, they may need supply (food, water, covers, etc.). They await a response from the professionals evoked before.

One of the main aspects here is that people are permanently in the area the crisis happens: before, during and after. Beside, most of them have a good knowledge of this area.

We therefore aim at taking into account this fact as an advantage in the following part that will describe how general public mobile devices can be used to enhance

disaster management for each stage of the process.

1.2 Different stages

In this section, we will list the different stages of the crisis according to [TAN 09] but adding the period before its occurrence too. For each of them, we will focus on how consumer mobile equipment can assist victims and experts and what are the limitations raised from a conceptual point of view.

1.2.1 Before a crisis: early warning system

A disaster may not necessarily be expected or even if it can be predicted some time before the strike, location of the areas that are to be the most damaged along with the precise nature of the threat cannot be expected. That is why, as described by [CHA 11], stakeholders have to anticipate by proceeding to:

1. Risk assessment
2. Safe areas identification
3. Creation of disaster-proof building codes
4. Early warning systems implementation

Information of course plays a major role to achieve these tasks and professional high-end techniques and technologies, as evoked in [LEF 14], are required.

But general public devices can also play a role as far as task 4) is concerned. Indeed, they firstly have the advantage to be permanently located on the terrain, which means that there is no costly deployment to be done. Secondly, there are many of them, generally from hundreds to thousands for large cities.

That is why they can be used to detect the early signs of a disaster in a way that will be described thereafter. Of course, this does not replace the scientific tools but it is an auxiliary mean of gathering early information about a trend (from a statistical point of view) rather than granular data. Indeed, such an expert network already exists: the Disaster Charter is based on a list of authorized users from all over the world. The idea is to build a complementary network involving non-specialized users to build an alert map similar to the one available at https://www.disasterscharter.org/web/guest/activations/activations-map

Next step of the process takes place once the disaster strikes.

1.2.2 During crisis: victim localization and assistance system

When the catastrophe occurs, the main priorities are to search and rescue victims while in the same time assisting people that are not injured to guide them to a safe place.

From an information point of view, the questions for ESU teams are: who? From where? To where? Time is also a major constraint [TAN 09]. In this context, popular devices like smartphones or connected devices can help to acquire this information and communicate between professionals and the population. Indeed, nowadays devices embed lots of sensors which can be used to capture data on the immediate environment of their owner.

Actually, one could even think that it is already a widely spread process thanks to the now very common telephone service. But we have to take into account the fact that the normally available communication infrastructure may be totally or partially down at that time. Moreover, from a user point of view, a victim may not be able to make use of its mobile phone for many reasons (he/she may be unconscious, buried under rubble, unable to move arms or fingers, etc.).

An appropriate solution must therefore be designed to support population assistance in those harsh conditions. Propositions will be given in an upcoming part of this chapter.

1.2.3 After crisis

Once the crisis is over, that is to say emergency tasks have been accomplished at their best and no other threat is expected (for example, the aftershock after a seism), time for resilience takes place. The goals are to rebuild what has been destroyed or damaged, assess and analyze the disaster (human and material casualties), and take measures to improve the management if another catastrophe happens in the future.

Impact of general public mobile devices may be here smaller than in the two previous stages because, resilience is not a matter of emergency and rely a lot on scientific data. However, they can be used to acquire auxiliary data to achieve tasks 1) and 2) of [CHA11]. They can indeed be useful to have a simple overview of areas that need a special attention by allowing users to report priorities (according to them) in their neighborhood.

The limitation here lay in the fact that too much non-sorted data may be acquired from such a system, as there is no validation from specialists.

1.3 Resulting information chain

Given this overview, we can propose a specific information chain, which is a variation of the information chain shown by [TAN 09]. The result is visible in Figure 1.

To build it, we include the inputs and outputs of the consumer mobile devices as evoked before where they are useful.

The arrows show that communication can be mono-directional (for data acquisition purpose) as well as bi-directional (for victim localization and terrain communication), but data processed is not the same according to the stage of the chain. Technical mechanisms that enable that in this particular context will be presented and discussed in a forthcoming part.

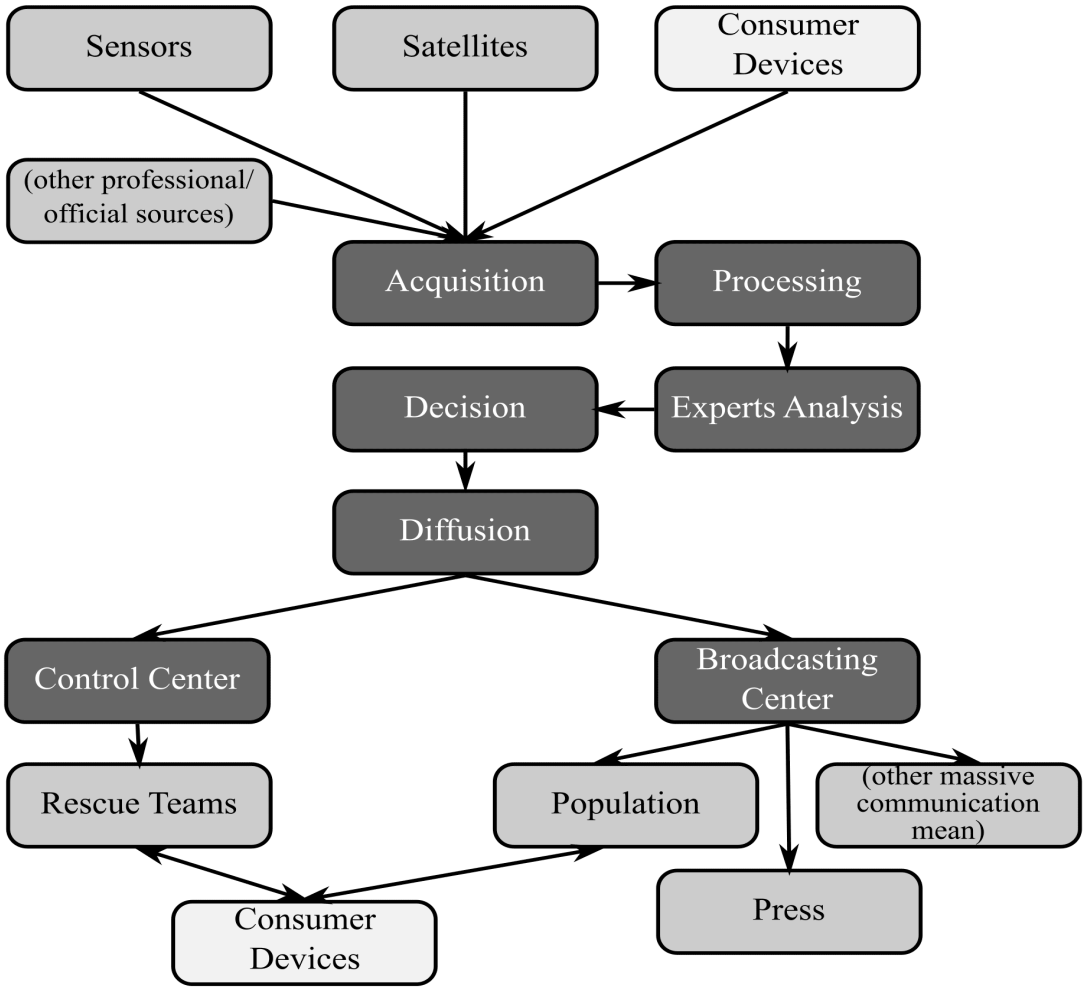

Figure 1: resulting information chain

1.4 Perimeter of action

It is necessary to draw the limits of such a consumer-equipment-assisted process. Firstly, one must realize that data obtained from the devices is not guaranteed to be exact, without mentioning that data directly given by users themselves (i.e. manually and voluntarily entered) can be erroneous too (on purpose or involuntarily). That is why our goal is less to provide a one-to-one communication system than to enable the creation of a map showing the spots where probability is high to have an event occurring concerning lots of persons, thus following a "best-effort" philosophy.

Secondly, this process raises the question of the interface between professional equipment, networks, procedures on one hand and consumer devices and infrastructures on the other. The expert environment has priority and must be secured from the consumer one so that if the latter is faulty (or attacked), it does not bring down the former along. Consequently, implementation limits are also given by this rule: an information source must be dropped whether there is a probability that it can damage or alter the primary professional risk management environment.

Thirdly, by nature, there is no obligation of result on the general public part of

the system. It means that it may be partially or totally inoperative without creating a new threat in the context of the disaster.

That say, we will now focus on more technical aspects regarding the implementation of such a system.

2 Mobile equipment and proximity communication

In this section, we will present the technical features of average consumer devices nowadays, the communication networks that can be used to reach the goals described before and finally the architecture that links them.

2.1 Mobile devices

2.1.1 Definition

First of all, we have to define more precisely what we call mobile devices. Indeed, this phrase can match several types of devices as shown in [SEB 14]. We will focus on the following ones, as they are the more appropriate given the context of our chapter:

- Smartphone: advanced mobile phone that is fitted with various input/output interfaces along with a good processing power and at least 2 network interfaces (Mobile phone (3G/4G) and Wi-Fi)

- Smart watch: a small computer housed in a watch-like format that is attached to user arm. It is generally equipped with biometric sensors and Bluetooth and Wi-Fi network interfaces. Most popular models work paired with a smartphone, hence a communication link between both

- Activity tracker: usually looks like a bracelet that measure biostatistics to keep logs of physical condition of the user. User Interface (UI) is very limited (a few buttons, no screen) but the device is generally configured and piloted from another paired device (smartphone or computer) that may not be always connected because the tracker is autonomous. Networking interface is in general Bluetooth

Those mobile devices we rely on share common specifications in addition to being mobile: they embed sensors, an easy-to-use UI, a decent processing power and one or more wireless networking interfaces. However, they are very different as far as autonomy, form factor and UI are concerned.

Finally, one important characteristic, which is a strong hypothesis for us, comes from the fact that they are attached to a person rather than group of persons or a place. We therefore made the assumption that one kind of device corresponds to one person. Categorization is indeed possible because each of them has a different signature. One person can wear a smartphone, a smart watch and an activity tracker at the same time. In order not to be counted as three different persons, it is possible to rely on each device signature, such as the MAC Address. Moreover, smart watches and activity trackers must usually be paired with a smartphone to work, which gives it a central role in the personal area data and communication management.

That say, we can browse the technical features that are related.

2.1.2 Features

In this part, we will present what kind of useful data can be acquired and transmitted from embedded equipment. We will first deal with sensors.

2.1.2.1 Relevant sensors

The idea in this section is not to make an exhaustive list of the typical sensors provided in an average smartphone in 2015 but to point out the few ones that can be used for disaster management:

- GPS: allows recording current position (given the fact that conditions are good enough)

- Camera: allows taking still images and video enabling transmitting a view of a devastated area. Nowadays, thanks to GPS, the location where the image has been taken is automatically recorded in the EXIF picture metadata

- Microphone: allows recording user voice and communicating with others. Also allows capturing environment noise to try to define it if a victim is unconscious under rubble (in this case, GPS may be useless)

- Speaker: allows to communicate with others but also to stimulate an unconscious victim with specific sounds to awake him/her

- Light sensor: allows to measure light at the surface of the device. Initially, this sensor was integrated to adapt display brightness to ambient condition, especially to dim it when the user holds it near his/her ear. In our context, it can be used to determine the kind of environment a person is in according to the time of the day. For instance, if there is very low amount of light on the sensor at noon, it may indicate that device owner is in a closed area

- Biometric sensors: usually measures heart beat and/or blood pressure. When sensors are attached to a watch or an activity tracker, measuring is permanent whereas when embedded in a smartphone, user has to put a finger on the sensor to acquire a measure. The former is far more interesting for us in order to have an overview of the owner's health

- Accelerometer/gyroscope: allows to determine device position. It is rather difficult to deduce a problematic situation for the owner from this information because there are lots of normal situations where the device could be either vertical or horizontal. However, the idea here is to compare this information between groups of users in a particular area to determine if there are similarities at a given time, possibly indicating people laying on the ground. Experiments are led to evaluate how it can be used to detect earthquakes [LAW 14]

These features can of course be used in combination. Indeed, in the pre-disaster stage, some recent studies [MIN 15] are led to check whether accelerometers and GPS can be used to automatically detect seismic activity in a more reliable way than using only one sensor. Of course, the results will have to be updated according to technological evolution: sensors precision is expected to increase with newer devices [LAW 14].

We must also add the fact that other types of sensors can be embedded in devices, such as barometer, temperature or humidity sensors. But at the time this chapter was wrote, they were featured in a limited number of high-end devices, whereas the ones we listed above are very common.

Let us now focus on network interfaces.

2.1.2.2 Network interfaces

Nowadays, lots of consumer wireless communication standards are proposed with very different specifications. Actually, manufacturers tried to find the best compromise between range, speed, reliability, energy requirements, etc. This led them to build devices that embed several interfaces, such as smartphones, in order to use the most appropriate one for a given situation.

In the risk management context, this is a desirable feature as those devices can play a bridge role between a device having a short-range connectivity (a bracelet for instance) and a broader-range network.

Finally, common consumer network interfaces remain evolution of standards that exist since a dozen years [SEB 14]:

- UMTS and now Long-Term Evolution (LTE) have the maximum range but an average speed
- Wi-Fi is adapted to a domestic use, that is to say, it has an average range but at a rather high speed
- Bluetooth has been created to achieve personal-range communication. It has low range and speed but consume less energy than the two other standards

[SEB 14] depicts the differences between those interfaces in terms of capacity, range, frequencies, etc. Of course, other wireless communication standards exist, however, they are quite rare or very specific, that is why we restricted ourselves to those ones.

2.1.2.3 Software development concerns

Hardware features presented before give interesting perspectives regarding our goal but they have to be driven accordingly by the software. This raises many concerns.

The first one deals with software environment. Indeed, one must take into account popular platforms market shares to create a solution that works on most user devices. The idea there is to broaden the range of potential users that will involve in the system. Early 2015 figures [GOA 15] show that Google's environment Android is the leading mobile Operating System (OS) with about 80% market share. Thus, its software development environment is to be selected. It has the reputation to be less restrictive than its main competitors (Apple iOS and Microsoft Windows Mobile) as far as installing programs and accessing to on-board sensors and services are concerned. But competitors should not be put aside too. They can easily be involved in the system by using Android devices as gateways for them. Thus, despite being more closed environments, they can provide data without having to redevelop specific workaround solutions to overcome the limits imposed by their respective companies. Only the sensor-related features are to be conceived according to the device. Finally, agreements could be made with leading brands to have privileged access to the hardware.

The second concern is energy-related: as we deal with mobile devices powered by a battery, it is mandatory to ensure that the additional consumption provoked by the disaster-management solution working in background is not too high. This is a severe issue as polling continuously and permanently data from sensors causes a high

energetic cost. That is why various energy-saving strategies have to be set in order to limit this cost. Moreover, restrictions may be applied directly by the OS for that purpose. Finally new rules[1] are set as default with each major update released, which can prevent a risk-related application to work correctly once updated. We are therefore currently facing regular changes in applied policies regarding specific access to sensors and interfaces, making the creation of a ready-to-release software (i.e. not demanding specific technical operations from a user, like rooting or jailbreaking the terminal) sometime difficult.

The last concern deals with the differences existing between devices. They are from different manufacturers, different generation and even at a component level, several references exist for a given specification. Indeed, OSes like Android demand dedicated specifications to ensure a given version can run on a given hardware. However, those are minimal specifications. Thus, an accelerometer may have a finer precision than another one, both running the same software. To address this fact, current tests have been (and still are) led (for example by [LAW 14]) to determine how this variability can impact the conclusion that can be made of the measurements.

2.2 Device-to-device communication technologies

Device-to-device (D2D) communication is a solution to the ever-increasing number of users and the ever-growing traffic demand from applications and services. It permits users physically close to each other to communicate directly and efficiently without going through an Access Point (AP) or a cellular infrastructural node (e.g., Evolved Node B (eNB) of LTE that connects the User Equipment (UE) to the network). Thus, communication is made opportunistically on local links. This approach has many advantages such as the emergence of new proximity services and applications for the user and enhanced networking (extended coverage, improved Quality of Service (QoS), traffic offload, special efficiency gain, etc.) for the operator. If not specifically addressed, public safety network is a privileged ground for D2D communication-based network. Indeed, it constitutes a fallback network when classical wireless and cellular networks are not available or fail.

Operations involve primarily communicating devices but can also call on infrastructural nodes or entities for coordination and control. D2D communication comprises two minimal phases: discovery and data communication. Devices in geographical proximity have to discover each other before being able to exchange data directly.

Two major and promising evolutions of existing technologies have emerged recently: WiFi Direct [WIF 09] for Wireless Local Area Network (WLAN) and 3GPP LTE D2D for Telecommunication Network [SA2 13], [SA1 14].

2.2.1 Wi-Fi Direct

Classical WiFi network requires a client device to connect to an AP to join the rest of the network. WiFi Direct makes it possible for two or more devices to communicate directly [CAM 13]. The basic WiFi specifies an Ad hoc mode for infrastructure-less network. However, the support of this mode is limited in existing devices and its usage introduces difficulties such as a lack of efficient power saving mechanism and an unpredictable QoS. WiFi Alliance that promotes WiFi technology decides to rely on

1 An example of such a new rule is the « Doze Mode » that is expected to be released with the next version of Android, currently called Android M, prior to being given a commercial name. This particular mode automatically decides which applications should be deactivated or put on standby when user is not using the device (i.e. at night).

widely deployed infrastructure mode for WiFi Direct. It consists in software update and does not require specific hardware. Former versions of the technology are supported, with their corresponding ranges and rates, except IEEE 802.11b.

Nearby communicating devices form a Peer-to-Peer (P2P) group that can be viewed as an equivalent to a traditional WiFi infrastructure network. Multiple P2P groups can coexist in the same vicinity. The device assuming the role of AP, after discovery and negotiation phases, is named P2P Group Owner (GO). Other devices of the group are named P2P Clients. Role in a group is merely functional and dynamic. A device can be member of multiple groups and assumes different roles in every group. In this case, the WiFi interface is time-shared between those distinct roles.

Along with the discovery phase, upper layer protocol such as Bonjour and uPnP can handle service publication and discovery. If present, deduced available services are considered to decide whether the group formation continues or not. It is a cross-layer approach in the sense that higher layer information are transported, recognized and used in link layer operations.

Acting as an AP, P2P GO provides network configuration, gateway function, security support and power saving coordination. Assuming those burdens can draw dramatically P2P GO battery. To save energy, it can switch to sleep mode according to two mechanisms: Opportunistic Power Save (OPS) and Notice of Absence (NoA). OPS leverages the sleep period of P2P clients deduced from transmission scheduling. NoA is at the P2P GO's own initiative: it informs absence periods to other devices.

2.2.2 LTE D2D

Two main enhancements introduced in 3GPP LTE release 12 address D2D communication referred to as Proximity Services (ProSe) and group communication (one-to-many) in public safety network known as Group Call System Enablers for LTE (GCSE_LTE). They intend to reuse as much as possible technologies of LTE especially in MAC and physical features, easing by this way, the integration with existing LTE network. Operations can be performed under the supervision of the operator for in-coverage situation or in a complete autonomous manner in out-of-coverage situation [FEN 13], [PAN 2015]. Communication can be direct from one end-UE to another end-UE or multi-hop by the use of at least an intermediary relay.

Discovery phase can be open or restricted. In open scenario, UE, given an identity, can discover other UEs or publishes its presence and, can be discovered by other UE. We note that identity can comprise a group identity useful for group communication. Process is realized mainly in link layer using pre-defined parameters. For restricted scenario, the core network of the LTE system Evolved Packet Core (EPC), assists the discovery process by tracking involved UEs locations and providing necessary information for them to discover each other. It means that UEs are identified, authenticated and authorized according to operator's policy and user consent to be discovered.

ProSe communication takes place on a LTE-based path established between the UEs. It requires allocated resource that can be done in two different manners whether the UEs are under the supervision on the network or not. For in-coverage situation, resource allocation is centralized. Transmission schedules, and thus, used resources, are maintained by the network. Transmission features, like power control, are also managed by the infrastructure. For out-of-coverage situation, pre-defined resources are allocated in a pool. Transmitting UEs contend for resources using random algorithm such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

In addition to in-band ProSe communication in within licensed spectrum, 3GPP LTE release 12 provided a way to established out-band communication through WLAN technology (e.g., WiFi Direct). EPC handles WLAN discovery and configuration. Third-party developers are offered API to develop proximity-based and proximity-aware services and applications. Users can benefit of a rich variety of evolving services and applications. The current specifications release restricts the use of group/one-to-many communication to public safety networks. A use case of such a service is for example the broadcast of information to all UEs in a disaster area.

2.3 Mobile-based networks

The two presented technologies are the most serious candidates for device-to-device communication in the market. WiFi Direct specifications were released on December 2009, while the release 12 of 3GPP LTE was functionally frozen on March 2015. Several handhelds and mobile devices are already equipped with WiFi Direct. Deployment was made easier because of the upward compatibility of the technology with the previous versions of WiFi: it boils down to software upgrade on existing hardware. LTE D2D deployment presents more difficulties. To mention two of them, we can cite roaming situation and interference management when multiple operators operate simultaneously on out-band frequency.

WiFi Direct inherits from WiFi security concerns. LTE D2D provides robuster security. It covers wider range (about 1km) compared to WiFi Direct (about 200m). LTE D2D operates on licensed spectrum, offering in this way a better and more predictable QoS and provides more reliability as resource usage and power control are managed by the network. Configuration is expected to be less cumbersome in LTE D2D as it is done upstream. Either the network controls D2D communication establishment or it provides pre-defined parameters to UEs for them to function autonomously. As operations are network-assisted, they will drain less energy from the UEs. LTE D2D was designed to be a more complete platform for the deployment and running third party proximity-based applications and services.

2.4 Architecture

A specific architecture is required to allows consumer mobile devices communicate with the rest of the infrastructure, more specifically the one that is used by disaster managers. Figure 2 shows this architecture.

Its goal is to allow information to be transferred bi-directionally between operators that are localized in three areas:

- Crisis area: the place where population (including victims) is and where a disaster strikes. At this time, rescue units are also in this area but to communicate, they have specific professional tools that are built to work in those conditions, that's why they do not appear on the figure.

- Nearest safe area: the place where Control Center is in order to monitor the situation.

- Any safe area: this is the place where the computing infrastructure is located. Actually, it could be anywhere in the world.

Stakeholders, for their part, are essentially localized in the nearest safe area, they may also be in capital cities, far from the crisis area.

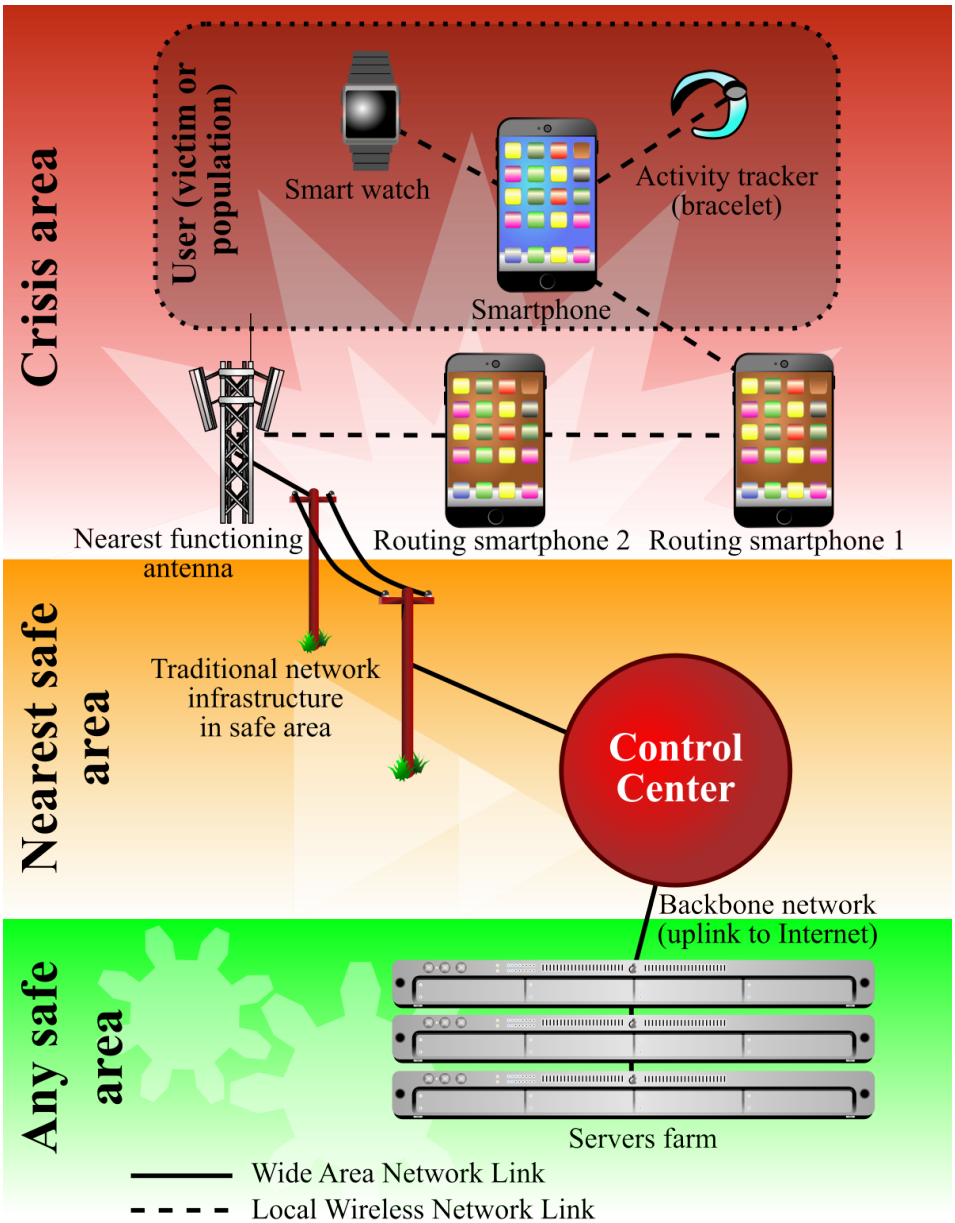

Figure 2: architecture

The most critical part of the architecture is in the crisis area. Autonomous configuration and networking are therefore required to allow communication (Local Wireless Network Link in the Figure) between mobile devices to the nearest working fixed infrastructure (Wide Area Network Link). This is achieved using the standards evoked before. Implementations concerns will be discussed in an upcoming part of this chapter. From a global point of view, what must be remember is the fact that this architecture permits to create and maintain an information link that will adapt itself dynamically to the available resources. In the example depicted in the Figure, information outputted by a user is routed via two other smartphones, the second one being connected to the nearest functioning antenna that is able to ensure relay to the final destination via normal means. The idea is thus to provide service for crisis management systems, which we will describe in the following section.

3 Mobile devices and proximity networks-assisted crisis management operations

In this section, we aim at presenting and discussing in detail how mobile devices can be used practically in the information chain depicted at Figure 1. Four systems are proposed each of them being a response in the global duty of disaster management:

- Early detection of a crisis
- Victim localization and characterization
- Victim and population on-site assistance
- Information gathering, dissemination and exploitation

Each system share a user profile completed during installation process on the mobile devices. This profile allows to specify user data and special needs: blood type, allergies, handicap, pregnancy, etc. Real name is not mandatory for people who care about privacy.

For each system, we will firstly present it, then evoke technical concerns and finally discuss the difficulties and/or limitations that can be raised and how to address them.

3.1 Early detection system

The first system is dedicated to early crisis detection by people living or passing by the concerned area.

3.1.1 Description

This warning system is based on capturing “visible” events that occur when a disaster strikes or is about to strike. For instance: fumes in a volcanic area, earth tremor, or other harbingers. The idea is to take advantage of the fact that although not being specialists, people living in such an area are able to detect unusual events. Even passing-by persons can even notice particular signs that indicate something is about to happen.

Those signs can be detected in two ways, from the device owner point of view:

- Actively: one or more persons send an alert signal because he/they have seen or heard something. In addition to the normal attitude for someone to trigger an alert when something dangerous happens, the development of social networks like Twitter, Facebook or Instagram has made people sharing with communities even events that may not be an immediate threat. That is to say, “odd” or unusual facts are to be reported on these online services. People are used to share information. Researcher and engineer working in the field of disaster management are thus willing to make use of this mechanism [TER 12].

- Passively: the device autonomously captures data, which is processed to determine if something special is happening (for example, a specific pattern is detected in the values acquired by an accelerometer).

3.1.2 Comparison with traditional approach

At this stage, it is interesting to make a comparison between the proposed approach and the professional one in order to show how they are complementary.

	Consumer mobile devices-assisted data acquisition approach	Usual expert devices-driven data acquisition approach
Number of acquisition devices (=nodes)	~100s possibly ~1000s in urban area	~10s
Data accuracy	Uncertain	Strong
Scientific level	Weak	Strong
Cost management	Shared with all actors	Paid by stakeholders
Obligation of result	No	Yes
Robustness	Uncertain	High

Table 1: differences between the proposed approach and the usual one

As 1 shows, the proposed approach has many limitations but they are balanced by the facts that on one hand the number of data sources is much higher and on the other hand by the cost issue. Indeed, in this situation, cost is largely shared by all the actors because consumers devices are paid by the population, and so is their access to the network. Stakeholders have to fund the centralization system. Actually, they normally already have one, what remains to be done is to update it in order to support as an input what mobile devices can send.

Finally, there is another reason that could justify such a warning system: it allows gathering information from an area not covered by expert/scientific devices. It is actually a current trend to create low-cost devices to detect disasters at an early stage [BHA 15]. This proposition thus also takes place in this particular context. But as shown in [HUA 12], the notion of "low-cost" is highly variable as in this article, the designed device costs $3,000 in regard to the typical cost of $25,000 for such a measuring station.

From these conditions, we can deduce that a mobile devices-based disaster warning system can only be used to find out area that may be the theater of a crisis occurring from a statistical point of view only. The idea is to quickly draw attention of stakeholders to a particular area that may not be equipped with professional devices, based on the fact that if hundreds of consumer devices report the same kind of data in a short time lapse, there are chances that something is really happening. This allows experts to draw a map of with hot spots. Those hot spots have a hierarchy according to the density of reports per area. Figure 3 shows an example of such a map.

This example depicts a fictive scenario: a tsunami striking Saint-Pierre, a town located in the south of Reunion Island, in the Indian Ocean, next to Madagascar. Three levels of priority are defined, thus allowing stakeholders to find out areas where

lots of people are located and giving most crowded area a higher probability of event occurring. Indeed, the more similar reports are emitted concerning a given area, the less chances are that information is erroneous (even if a massive malfunction remains possible).

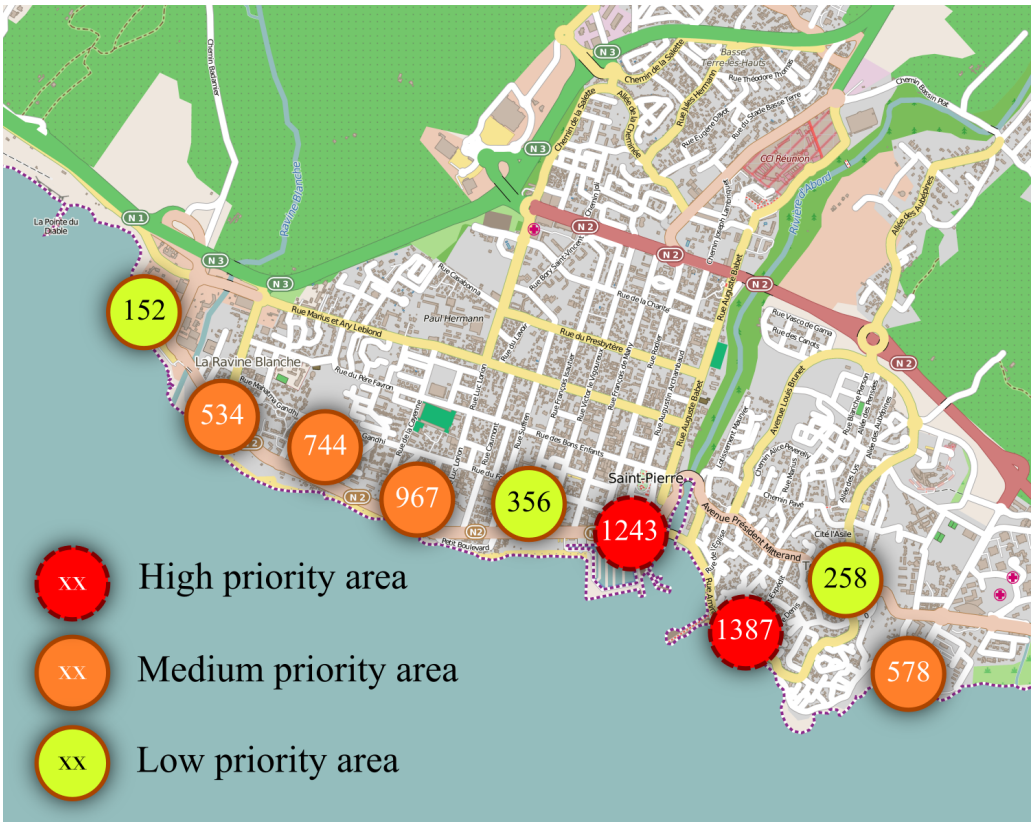

Figure 3: detection report map (background map provided by Open Street Map)

However, that is all that can be expected as "highly probable": crisis characterization from this point of view (i.e. knowing what is happening in addition to knowing that something is occurring and where) is a "best effort" feature: reliability maybe poor for lots of reasons: relevancy of information provided by non-specialists, poor sensors precision, faulty devices, etc.

That said, we can focus on the technical concerns that are raised.

3.1.3 Technical concerns

To deal with this topic, we will split the discussion between the active and then the passive way of detecting an event. Then we will evoke encountered difficulties.

3.1.3.1 Active warning system: user triggered alert

This system is actually very simple: it consists in an application installed in the device that can be launched by a user to emit a warning message. One could notice that it plays the same role as SMS (Short Message Service). The difference here is that there is no need write a message or to select a recipient to report a problem because conditions may not be good enough for the user to concentrate or even type-in all this information in case of emergency.

UI is therefore a major point to design this application. Specific features can be built to facilitate reporting a problem in tough time: simple visual interface with large buttons, voice-controlled interaction, gesture-based commands, etc. Doing so also allows the application to be operated by all profiles of users: young, old, disabled, illiterate, etc.

Finally, according to the situation, additional data (such as GPS position, time stamp, etc.) can also be sent with the warning message in a similar way as the passive warning system, which we will now present.

3.1.3.2 Passive warning system: sensors based detection

As seen in 2.1.2.1, connected devices embed sensors that can be used in combination to detect and report automatically a non-usual event occurring: accelerometers, gyroscope and GPS as evoked before. When a specific threshold is exceeded or a typical pattern appears, an alert message is emitted along with metadata consisting in:

- Time stamp: date and time of the detected event to allow all the reports to be sorted

- Geographical position: device location based on multiple sensors: GPS, Wi-Fi and 3G Cell-phone infrastructure. [ZOR 10] presents research work to achieve such a positioning even indoor

- Amount of brightness: this measure can give additional indication about conditions around the device to determine if they are consistent: for instance, if the device is located in a building at day time, a low value of brightness may indicate that it is in a bag or a pocket as well as the fact that the owner is stuck in a lift

Other data could possibly be captured such as a photo or a sound sample, but without an active participation of the user, resulting data may not have the required level of quality to be relevant.

This philosophy of passive detection of events by the device takes part in a more global one called “device sensing”. It aims at allowing a digital personal device to deduce the current situation its user is in from all the data it can get from its own: calendar, day and time, habits, sound, localization, sight, etc. From this, the device can automatically offer assistance for that particular situation. This is a long-term effort but new contributions are regularly made in this direction. [LAN 10] presents the concept and proposes a frame to develop dedicated applications. Three years later, [KHA 13] browses a state-of-the-art of the situation by listing applications and the context in which they apply.

Risk management is a domain where there are still lots of development to achieve before being able to release a ready-to-use solution. Indeed, there are specific parameters to take into account, even for a best-effort service. [RAD 14] presents an architecture that integrates many of them.

3.1.4 Difficulties

Implementing such an early detection system raises both technical and organizational questions.

Concerning the former, three issues can be listed. Firstly, sensors-based detection requires the developer to know the specification of the embedded hardware: precision of a sensor may vary from one model to another. Moreover, newer systems have higher precision. This makes rather difficult the process of aggregating and comparing the reports from users possessing very different devices performing the same tasks. Experiments must be led to determine whether it should be a big issue or not. Secondly, a major energy issue is raised: the principle of early detection supposes that data is acquired from sensors continuously, which tend to lower dramatically battery life if a special policy is not applied. Users may not will to involve in the early warning system otherwise. Finally, a smaller issue resides in the fact that researchers and developers have to access to specific programming modes to read raw sensors values for instance or to poll them in an usual way [MIN 15]. These modes are locked for security and commercial reasons for most users. In order to enable them for consumer use, it is necessary to work more closely with device and OS manufacturers, which is not always easy to do and also becomes an organizational issue.

On this side, another phenomenon can be noticed: lots of dedicated applications aiming at managing disaster already exist as evoked by [TAN 14]. The most useful ones are restricted to a particular area (for instance, a country) and/or a particular type of disaster. Disaster Kit from the Japanese operator NTT Docomo is a good example of such a tool. It is dedicated to Japan and has been designed to manage earthquakes, which are likely to happen in this country.

These applications share the fact that they are (officially) disconnected to a public safety organization. For us, this is a need because data provided by user devices should be aggregated at the highest level of crisis management, that is to say national Control Centers. Otherwise, there is a risk that information does not reach stakeholders who are in charge of management. Therefore, a special effort is expected to connect the general-public-side operations to the professional-side ones at the highest level.

3.1.5 Ethical concern

The passive automatic detection system raises an ethical question: its efficiency is linked to the fact that it is permanently acquiring data about the environment the user evolves in. That is why a privacy issue exists: he may feel tracked by the system.

This issue is a lot more general than the way we present it as lots of famous applications are regularly pointed out by Information Technology specialists for accessing personal data that is not related to their role. There are lots of debates between users who care and those who don't.

In our context, the idea is to define a compromise: acquired data is not stored permanently, and a message is sent only when a special event occurs. Finally, the reports can be anonymous because from a stakeholder's point of view, only a statistical use matters.

3.2 Victim localization and characterization system

As for the early detection system, we will first describe the victim localization and characterization system and then discuss the various concerns that must be addressed to build such a system.

3.2.1 Description

This system aims at assisting search-and-rescue operations by reporting to the

Control Center where victims are and what they are suffering from. To achieve this, an application, probably the same as the early detection system, is deployed on each personal device to send a message to authorities giving them the necessary information. Questions that must find answer here are: who? What? Where?

In comparison to the previous system, the main difference consists in the fact that the transmitted report has a true signification on its own and not only from a statistical point of view. Each report stands for a person who needs care.

In this context, most concerns discussed for the previous system are still valid. We will thus focus on the items that are specific to this goal.

3.2.2 Technical concerns

Ideally, such an assistance request system should work automatically: if the connected devices detect that their owner is injured, unconscious or sick, they should take the decision to call for help.

But as of 2015, technology is not reliable enough to proceed in total autonomy as expected by [LAN 10]. Devices are not yet able to "sense" such situation, for plenty of reasons: biometric sensors are still rare, environmental sensors such as camera or microphone can not operate all around the user (because they move according to him) to target useful points of interest and finally "collaborative work" between multiple personal devices is still poor. That is why a compromise must be done for the moment: user interaction is required but limited to the minimum.

Our proposition consists in a simple questions/answers system with time-out and default answers if no answer is given. It can be fingers or voice-operated and communicate with visual as well as aural information. Three steps are necessary to complete the operation of emitting an assistance request:

- Triggering a request: since device sensing is still a work in progress, chances are high that a victim has to be conscious to activate the process. He/she can operate the device directly or call the feature thanks to a keyword, in a similar way that digital personal assistants are invoked in a normal dialog (examples: "OK Google" for Android or "Hey Siri" for iOS). In rare serious situations, paired devices could automatically detect that a request has to be sent. For instance, if a heartbeat monitor has no signal after accelerometers detected a brutal activity

- Characterization of the request: the goal here is to answer to the questions Who? What? Where? Information is asked be a device that can handle sound (typically a smartphone). If there is no reaction from the user before a certain amount of time, particular sounds (high frequencies) are played to try to wake him/her, making the hypothesis that he/she may have fainted. As far as the questions themselves are concerned, Who? and Where? can be obtained automatically, but not the What?

    - Who: is defined from the application user profile which can thus give very detailed information about the person's health. But it can be completed thanks to user ID from the SIM chip too. Each one has a unique International Mobile Equipment Identity (IMEI), linked to a user account at the line operator. Of course, the device could have been lent to somebody else

- Where: positioning techniques evoked before are used. Of course, there might have a slight difference between the device and his/her owner's positions but we make the assumption that in most cases, they should be close

- What: user is requested to answer to a few questions about his/her health situation in order to allow ESU teams to anticipate the needed equipment. Other questions are asked about the environment: rubbles, specific danger around, etc. No response at all indicates an unknown issue

- Sending the request: a message is sent to the network (based on the protocols and techniques presented previously) for delivery to stakeholders whatever the answers for the previous step are (even in the "no response" case)

From a technical point of view, difficulties are still the same as those mentioned for the early detection system. The UI aspects are even more important to build an efficient system to gather answers for the characterization process. Actually, software libraries provided by mobile OS makers support all the requested features. The timed question-response feature is easy to implement: in case no input is given after a certain amount of time, the information is sent that the user has not replied which can indicate a problematic situation.

3.2.3 Ethical concerns

From the ethical point of view, a major issue is pointed here: can the system override user settings to assist him/her? Indeed, there are situations where this is necessary to have the system work correctly. Here is are three examples:

- if sound has been muted, should the software be given the authorization to unmute it in order to use voice communication?

- if privacy settings deny the application to use GPS and/or other sensors, should they be ignored to allow it to accomplish its duty?

- even worse: to help ESU assist a fainted person, can they take the control of a smartphone, for instance, to give additional information?

There is no simple answer to these questions. Societal studies have to be led in order to find out a compromise between user control and system efficiency. This takes part in a global reflection about Ethical, Legal and Social (ELS) aspects, which is discussed by Social Sciences communities. [RIZ 14] is an example of what can be analyzed for a given situation.

3.3 Victim and population on-site assistance

We will follow the same path to present this system: a description, then the various concerns it raises.

3.3.1 Description

This system aims at enabling a communication channel between risk managers and people located in the area where a disaster strikes to provide on-site assistance to individuals. It relies on any remaining networking infrastructure available and can transfer any type of data: text of course, but audio and even images if needed. Video,

for its part, maybe too resource-demanding (from energy and networking points of view) given its relevancy. The system also takes the appearance of a mobile application as the two other ones, communication with a server. It may of course be the same application which play the various roles.

It allows sharing three categories of information:

- Stakeholders to population information: it consists in general information concerning the whole population, for instance a forthcoming threat like the aftershock than can be expected after an earthquake. This information is broadcasted, that is to say there is no condition for a person in the area to receive it

- Stakeholders to a person information: it consists in information that is sent to a particular person regarding its situation: he/she may not be a victim but has some specific needs:

    - Nearest safe place (or how to be extracted from the danger zone)
    - Nearest place to have water and food
    - Nearest place to find accommodation
    - Survival advises

  This information may automatically be sent given the information acquired from the owner's devices when using the previous systems. Thus, it eases a lot risks experts work who don't have to answer repetitive requests manually anymore

- Person to stakeholders information: this allows to manage special requests triggered from users that are too specific. It may concern a limited amount of situations: for instance, one person reporting the situation another (who does not have a smartphone or is not able to use it). Further test simulation with the system should give in a near future the most probable use-cases

One could also include a person-to-person information transfer system, but it may be less useful regarding the risk-management operations. Moreover, general-purpose applications like the Serval Project [GAR 11] already exist for device-to-device personal communication when the normal infrastructure is lacking.

3.3.2 Technical concerns

All systems presented in this chapter were described starting from the user devices point of view. But in all situations, there is an information system, that is to say a server receiving information from the devices. It was not a particular issue until this system because the communication was rather simple: the server role was to store data sent by devices and report it to stakeholders, eventually processed to calculate statistics and send them to a Geographical Information System (GIS) to display a map. This is an easy task given the resources available nowadays in servers. That is why we have not focused on this aspect of the systems until now.

Indeed, this particular system has higher needs in term of processing: an individual response must be calculated for every single user, according to his/her very

own data. Operations include:

- a constraint solver: to compute a recommendation taking into account all the data available about a user, in particular regarding his/her profile, not only the environment he/she currently is

- a navigation unit: to guide the user, most certainly a pedestrian, to a particular point (for safety or supply) in relation with the constraint solver

To achieve this at a relative low computing cost, techniques from the simulation and videogames industry can be used, for example for real time path finding [LAM 04]. Of course, algorithms have to be adapted, as the model does not match completely reality, without mentioning the fact that users are not tracked in real time, in our proposition.

Nevertheless, the demand for the server side is higher than before and it must be anticipated. However, there are solutions, as servers don't have to be physically in the area the disaster strikes. Moreover, cloud computing paradigm allows to increase processing capacity on-the-go, by aggregating physical machines into a virtual one to face the increasing workload.

3.3.3 Difficulties

The energy issue is even more important for this on-site assistance system because the demand increase because of the number of peripherals that have to work at the same time: network interfaces, screen always on to display a map an indications, audio indications, positioning interfaces, etc. In addition to this, the time during the battery drain is high is quite long because devices have to work during all the time the user looks for a particular place.

There is currently no solution that could limit energy consumption in this particular context. One must take the risk to have the mobile terminals (and more particularly the smartphone) to power off before the user reaching his goal.

Network aspects are a less important matter, although congestion can occur because of the multiple one-to-one communications that can occur in a WiFi-Direct or LTE D2D mesh network. The real trouble here is the lack of feedback given the fact that those standards are new. Large experiments still have to be done to check their robustness in harsh conditions.

3.3.4 Ethical concerns

In this context, ethical concerns are less critical than the previous system. General issues about privacy remains, because the application has access to the user profile which can contain very personal information.

A solution could consist in creating a file at a country scale level. However, constraints exist about the legal frame that must exist to support such an action. Quite surprisingly, it is easier for private firms like Google or Microsoft to gather and especially use publicly information about people than for states, without mentioning the costs.

3.4 Information gathering, dissemination and exploitation

As for the previous systems, we will firstly present a description of the goals

concerning this topic and then discuss technical and non-technical trends and difficulties. This subsection presents lower level concerns compared to previous ones: the discussion will be centered on some specific technical issues.

3.4.1 Description

Conventional communication networks are the first systems that fail during disasters [PAL 12]. This results in poor level of initial response. The majority of existing applications uses some form of centralized processing, communication or storage. They suffer from the common communication network failure. However, alternatives for usable communication exist. One of them consists in leveraging the opportunistic and collaborative network formed by surrounding mobile devices. As we've seen earlier, more mobile phones are likely to be present in the terrain disaster than expert specialized devices. They have computing, storage and communication capabilities. The association of multiple devices coupled with wireless communication makes it possible to build or support distributed applications or systems. We will focus in the following on the possibilities offered by such collaborative network to information gathering, dissemination and exploitation.

3.4.2 Technical concerns

Each participant contributes to the establishment and the maintenance of a distributed application or system. However, challenges are inherent to such an association [GAL 06]. To mention some of them, we can cite the following:

- Wireless communications are often faulty: connectivity between devices is weak; exchanged data can be lost
- Topology is dynamic: devices can move; some of them can leave while some join the network
- Communication delay or latency is not null and can fluctuate even with the same participants
- Wireless communication is unsecure: exchanged data can be intercepted, altered in transit or recovered by unintended entities
- Control is distributed: any operation in the network is realized with the coordination of the members
- Network is often partitioned or not fully connected: a device may be or become unreachable by other devices
- Operations are concurrent: multiple devices can modify the same data concurrently

3.4.2.1 Information gathering

The collection of gathered data represents a valuable shared common good [PAL 12]. Studies demonstrate the willingness of users to participate in building the collection [AL 01]. This collaborative gathering of data while resulting in a rich source of information, may introduce conflicts and inconsistency. One illustration of a conflict is when two or more incoming data report inconsistent values for a piece of information that permits a single value at most. That is for example, the case when a

user receives contradictory danger levels for the current place. One behavior is to consider the most recent information and discard the others. Dynamics (in terms of latency, topology or partitioning) in the network favor the occurrence of conflicts. Dissemination of outdated information illustrates such a situation. Conflicts resolution and consistency preservation mechanisms, are, then, of capital importance: they result in either, a new value of the information combining all or partial conflicting ones or an existing value that should be considered as the correct one by all participating devices.

Conflicts resolution is commonly encountered in distributed database. A participant runs a partial or a full replica of the database. The major issue consists in dealing with multiple successive conflicting (and non-conflicting) versions of a piece of data: How to guarantee data consistency while allowing concurrent read and write operations. Several solutions exist:

- Optimistic replication: This approach maximizes the availability of the system in presence of network partitioning. A replica may run operation (e.g., data modification, removal, etc.) without requiring immediate synchronization, coordination or consensus with other replicas. Changes are reported later on. Thus, at a given time, the value of a data may not be the same on different replicas. However, on the long run, the data eventually converges to the same value when all changes are reported. There is no a priori conflict avoidance (e.g., by setting lock). A conflict is resolved at the time it is detected. Bayou [TER 95] is one of the first replicated databases proposed for mobile computing environment. A device designated as a primary replica for a particular data item commits all write attempts. Application defines how a conflict is characterized and how to resolve it for the system to work autonomously. The main drawback of Bayou is that the primary replica becomes a single point of failure. Constant Data Availability (CODA) [COD] is a distributed file system based on optimistic replication and designed for disconnected operation in mobile computing. A support for Linux Kernel exists starting from 2.6 version.

- Multi-Version Concurrency Control (MVCC): it is a control scheme permitting concurrent access to a distributed database. Successive versions are stored in the database. Old versions are kept but marked as obsolete. A new version is visible only when the related update has been completed. It means that a read results in a snapshot of the database regardless of ongoing updates. Thus, write operation does not require locking previous versions of the data: reading never blocks writing and vice versa. However, maintaining multiple versions of data incurs costs in terms of storage. Periodic purges or archiving of obsolete versions are necessary to save space. CouchDB [COUD] and its derivative CouchBase [COUB] are flagship MVCC-based databases. They are document-oriented databases: stored information is semi-structured in that document contains both data and schema. Multiple instances replicate their data through HTTP-based synchronization protocol. CouchDB and CouchBase were designed with offline use in mind. An embedded version of CouchBase named CouchBase Lite is available for mobile.

- Operational transformation (OT): it addresses synchronous realtime collaborative applications. Participants can view and edit the same document at the same time. Each participant maintains locally a replica of the shared document. OT ensures the consistency over the multiple replicas. Local modifications also called operations are expected to be highly responsive: they are performed immediately [KUM 10]. Operations are, then, propagated to

other participants in timely manner. They will eventually converge to a version reflecting the intention of editors. A participant can edit any part of the document. Document must be linearly addressable. A received remote operation is transformed against previous operation before being executed locally. The new form preserves the intention of the editor and ensures the convergence over all participants. Suppose two users A and B that collaborates on a document containing the string "abc". User A inserts the character "z" at position 0 resulting to the operation OpA = Insert(0, "z"). User B deletes the character "c" with the operation OpB = Delete(2). We will consider processing on A when receiving OpB, however, the mechanic is the same on B. OpB is transformed to OpB' = Delete(3) facing the previous execution of OpA on A. Finally, OpB' is executed on A and results in string "zab". Asynchronous and non-realtime situations limit the usage of OT. Indeed, a high latency of operations propagation blurs the intention of multiple editors. A suitable use case of OT in disaster management is for example, a fully connected network composed by nearby devices. Collaborative editing applications such as Google Docs [DOC], Apache Wave [WAV] and Etherpad [ETH] leverage OT.

3.4.2.2 Information dissemination

We will focus in this section, on ways to capitalize on mobile phones network to convey information from a source to a destination. In a classical situation, a mobile phone is a terminal node: it is either the source of communication or a final destination. The network infrastructure transports the data from a terminal node to another terminal node. In the considered infrastructure-less network of mobile phones, some devices may be out of communication range of others. Given the absence of infrastructural nodes, mobile devices have to be in charge themselves of relaying and routing functions.

Routing is widely studied in Mobile Ad hoc Network (MANET). A MANET is an autonomous self-configured network composed of mobile nodes over wireless links. All nodes act as routers, discover and maintain route to each node of the network. Coordination between nodes is necessary for conveying information to its destination. Routing protocols have been designed for MANETs. To mention two of them, we can cite Optimized link state routing protocol (OLSR) and Better Approach To Mobile Adhoc Networking (BATMAN). The key concept of OLSR [CLA 03] lies in the use of Multi-Point Relays (MPR) that relay information. MPRs are chosen among nodes in such a way that any node of network is covered by at least one MPR. MPRs exchange regularly routing information. BATMAN [JOH 08] is intended to replace OLSR. It does not maintain the full route to the destination: each node along the route only maintains the information about the next link through which you can find the best route. Serval Project [GAR 11] relies on BATMAN. Routing protocols for MANET are usually designed for general-purpose application. Maintaining route in permanence is costly and may not be necessary in all cases.

Opportunistic networks are an alternative solution. A device may communicate with another device even if a complete path connecting them is missing. An intermediate device can be involved in an opportunistic manner to relay data if it allows to come closer to the recipient. Thus, data transport is done step by step according to this scheme to the final destination. Opportunistic networks exploit node mobility. In this perspective, the Twimight system [LEG 11] offers a microblogging service similar to Twitter, dedicated to emergency and crisis situations.

3.4.2.3 Information exploitation

In collaborative network, information is received from different sources. It is

essential to identify and authenticate the sender for security concerns. It is also vital to certify and track back received information to the sender or the data collector. Incorrect information, or doubts about the veracity of information can lead to very poor resource allocation, which in turn can cause needless suffering and loss of life [PAL 12]. From practical point of view, asymmetric cryptography represents a response to identification and authentication issue. Pretty Good Privacy (PGP), is one the most widely used program for privacy and authentication. A user generates a private key and the associated public key. He sends the public key to his contacts and keeps the private key confidential. User's contacts use the public key to encrypt information intended for him and to authenticate information coming from him. Conversely, the private key is used by the user to sign issued information and decrypt received information. PGP comprises "Web of trust" feature that permits to establish the authenticity of the binding between a public key and its owner. For this aim, other users can certify the public key associated to the owner. Networking and Cryptography library (NaCl) is another candidate to authentication for mobile phone environment [NAC]. It avoids various types of cryptographic disaster suffered by previous cryptographic libraries and uses shorter public key compared to PGP.

Considering the possibility for participants to share information securely, we will focus now on the form in which information is exchanged and how applications will use it. Information can be structured, unstructured or semi-structured. Structured information means that it follows a fixed pre-defined formal data model. The data model explicitly defines the structure of data. It eases data processing. For example, any profile information must include the fields "name" and "email". Unstructured information does not conform to a pre-defined data model nor is organized in a pre-defined manner. Semi-structured information does not follow a pre-defined formal data model but includes markers that describe its structure. Information is self-described. It benefits from the structure-oriented processing similar to structured information and exhibits the flexibility of structure defined at runtime. Semi-structured information is described by markup language. EXtensible Markup Language (XML) and JavaScript Object Notation (JSON) represent two popular markup languages.

An application can exploit the flexibility of semi-structured information. Its design can even be data-centric. That choice simplifies the development and maintenance of the application over a collaborative network. Indeed, it benefits from underlying information gathering and replication as presented earlier. RAVEN is an implementation of this approach [PAL 12a]. It is a framework which makes it possible to build applications for collaborative edition. RAVEN offers developers compile time tools, which use only the schema to generate all database handling components, edit and list user interfaces. It also provides a schema editing application as a portion of the framework in order to allow users to define a new database on the phone at runtime. CouchApps constitute another mature and production grade alternative. They are web applications, represented as JSON document, served directly from CouchDB. A CouchApp uses web technologies (HTML/CSS/Javascript) and can be replicated by CouchDB.

3.4.3 Ethical concerns

When participating in a collaborative network, a mobile phone can process, store or relay information of other devices in addition to its own information. Those functions drain energy and decrease the lifetime of the device. It is essential to ensure that this cost matches the willingness of the device owner to allocate resources for the common good. The system must also guarantee the security of the data and the communication while ensuring the privacy of the users.

On the other hand, user information can be conveyed by intermediary devices. User should be aware of the burden of transporting that information. As resources (battery, bandwidth, etc.) are constrained in the whole network, communication must be limited to vital information. Even if this policy is ultimately achieved via technical means, communications are triggered on the user's initiative.

Conclusion/Perspectives

In this chapter, we attempted to provide a complementary mean of managing a crisis by relying on mobile consumer devices as a personal assistant for the population. The idea is to gather information and communicate with people in an efficient way to ease stakeholders and risk professional duty.

To achieve this, lots of technical concerns must be taken into account, but scientific and technological progress are regularly made to address the issues: for example, as far as the energy question is concerned, one of the major one, it is a necessity for devices manufacturers to create more efficient batteries and there is no doubt they will.

Non-technical aspects could actually raise problems that may slow down dramatically the development of such a solution if they are not taken into account at a very early stage. That is why we put emphasize on the fact that all the actors should collaborate as soon as terrain experiments are ready to be launched.

Ethical concerns also emerge from this proposition: researchers must integrate what people are ready to do and what they are willing to let specialists do with their private data, in order to receive assistance in case of emergency. That is why experiments must also be led with ELS specialists to have quantitative as well as qualitative feedback.

Such experiments need support from local and national organization (such as civil security, coastguards, municipal officials, etc.) to be conducted in the most realistic condition. It also allows people to work together by making every actor aware of what the others are doing. It is a non-technical aspect but it remains essential regardless of the system used.

References

[AL 01] AL-AKKAD, A., ZIMMERMANN, A., "User Study: Involving Civilians by Smart Phones During Emergency Situations", 8th International ISCRAM Conference, 2011.

[BHA 15] BHAT, A. P., MESHRAM, N. S., DHOBLE, S. J., et al., “Microcontroller Based Low Cost Earthquake Monitoring Using Lab-View”, International Symposium on Ultrasonics, Vol. 22. No. 24. 2015.

[CAM 12] CAMERON, M. A., POWER, R., ROBINSON, B., & YIN, J., “Emergency situation awareness from twitter for crisis management”, Proceedings of the 21st international conference companion on World Wide Web, April 2012, Lyon, ACM, p. 695-698.

[CAM 13] CAMPS-MUR, D., GARCIA-SAAVEDRA, A., SERRANO, P., "Device to device communications with WiFi Direct: overview and experimentation", IEEE Wireless Communications, Vol. 20 no. 3, 2015, p. 96-104.

[CHA 11] CHANDRAPPA, R., GUPTA, S., et KULSHRESTHA, U. C., “Predicting Disaster: Asian Scenario”, Coping with Climate Change, Springer Berlin Heidelberg, 2011. p. 149-154.

[CLA 03] CLAUSEN, T., JACQUET, P., "Optimized Link State Routing Protocol (OLSR)", RFC 3626, 2003 [COD] http://www.coda.cs.cmu.edu/

[COUD] http://couchdb.apache.org/

[COUB] http://www.couchbase.com/

[DOC] https://docs.google.com/

[ETH] http://etherpad.org/

[FEN 13] FENG, J., "Device-to-Device Communications in LTE-Advanced Network", PhD Thesis, Télécom Bretagne, Université de Bretagne-Sud, 2013.

[GAL 06] ROTEM-GAL-OZ, A., "Fallacies of Distributed Computing Explained", RGOArchitects, 2006.

[GAR 11] GARDNER-STEPHEN, P., The serval project: Practical wireless ad-hoc mobile telecommunications. Flinders University, Adelaide, South Australia, Tech. Rep, 2011.

[GOA 15] GOASDUFF, L., RIVERA, J., Press Release March 2015, Gartner Group, Egham, 2015.

[HUA 12] HUANG, R., SONG, W.-Z., XU, M., et al., "Real-world sensor network for long-term volcano monitoring: Design and findings", Parallel and Distributed Systems, IEEE Transactions on, 2012, vol. 23, no 2, p. 321-329.

[JOH 08] JOHNSON, D., NTLATLAPA, N., AICHELE, C., "A simple pragmatic approach to mesh routing using BATMAN", 2nd IFIP International Symposium on Wireless Communications and Information Technology in Developing Countries, 2008.

[KHA 13] KHAN, W. Z., XIANG, Y., AALSALEM, M. Y., et al., "Mobile phone sensing systems: A survey", Communications Surveys & Tutorials, IEEE, 2013, vol. 15, no 1, p. 402-427.

[KUM 10] KUMAWAT, S., KHUNTETA, A., "A Survey on Operational Transformation Algorithms: Challenges, Issues and Achievements", International Journal of Computer Applications, Vol. 3 no. 12, p. 30-38, 2010.

[LAM 04] LAMARCHE, F., DONIKIAN, S., "Crowd of virtual humans: a new approach for real time navigation in complex and structured environments", Computer Graphics Forum, Blackwell Publishing, Inc, 2004. p. 509-518.

[LAN 10] LANE, N. D., MILUZZO, E., LU, H., et al., "A survey of mobile phone sensing", Communications Magazine, IEEE, 2010, vol. 48, no 9, p. 140-150.

[LAW 14] LAWRENCE, J. F., COCHRAN, E. S., CHUNG, A., et al., "Rapid earthquake characterization using MEMS accelerometers and volunteer hosts following the M 7.2 Darfield, New Zealand, earthquake", Bulletin of the Seismological Society of America, 2014, vol. 104, no 1, p. 184-192.

[LEF 14] LEFEUVRE, F., TANZI, T. J., "Radio Science's Contribution to Disaster Emergencies". The Radio Science Bulletin, 348, 2014.

[LEG 11] LEGENDRE, F. et al., "30 Years of Wireless Ad Hoc Networking Research: What about Humanitarian and Disaster Relief Solutions? What are we still missing?", ACWR, 2011

[PAL 12] PALMER, N., O., "Smartphones: A Platform For Disaster Management", PhD Thesis, VRIJE UNIVERSITEIT, 2012.

[MIN 15] MINSON, S. E., BROOKS, B. A., GLENNIE, C. L., MURRAY, J. R., LANGBEIN, J. O., OWEN, S. E., HEATON, T. H., IANNUCCI, R. A., HAUSER, D. L., "Crowdsourced earthquake early warning", Science Advances, Vol. 1 no. 3, 2015.

[NAC] http://nacl.cr.yp.to/

[PAN 2015] PANAITOPOL, D. et al., "Recent Advances in 3GPP Rel-12 Standardization related to D2D and Public Safety Communications", 2015

[RAD 14] RADIANTI, J., DUGDALE, J., et al., "Smartphone sensing platform for emergency

management". arXiv preprint arXiv:1406.3848, 2014.

[RIZ 14] RIZZA, C., PEREIRA, A. G., "Building a resilient community through social network: ethical considerations about the 2011 Genoa floods", 11th International ISCRAM Conference, 2014, p. 289-293.

[SA2 13] 3GPP WG SA2, Technical Specification 22.278, "Service Requirements for the Evolved Packet System", 2013

[SA1 14] 3GPP WG SA1, Technical Specification 22.468, "Group Communication System Enablers for LTE (GCSE_LTE)", 2014

[SEB 14] SEBASTIEN, O., HARIVELO, F., SEBASTIEN, D., "Using general public connected devices for disasters victims location", General Assembly and Scientific Symposium (URSI GASS), 2014 XXXIth, URSI, 6-23 Aug. 2014, p.1,4.

[TAN 09] TANZI, T. J., LEFEUVRE, F., "L'apport des radios sciences à la gestion des catastrophes", Journées scientifiques 2009 d'URSI-France: Propagation et Télédétection, 24-25 mars 2009, Paris, URSI, p. 401-428.

[TAN 14] TANZI, T. J., SEBASTIEN, O., et HARIVELO, F., "Towards a Collaborative Approach for Disaster Management Using Radio Science Technologies", Radio Science Bulletin, 2014, no 348, p. 25.

[TER 12] TERPSTRA, T., de VRIES, A., STRONKMAN, R., & PARADIES, G. L., "Towards a realtime Twitter analysis during crises for operational crisis management", Proceedings of the 9th international ISCRAM conference, Vancouver, Canada, April, 2012.

[WAV] https://incubator.apache.org/wave/

[WIF 09] WI-FI ALIANCE, "Wi-Fi Peer-to-Peer (P2P) Technical Specification v1.0", December, 2009.

[ZOR 10] ZORN, S., ROSE, R., GOETZ, A., et al., "A novel technique for mobile phone localization for search and rescue applications", Indoor Positioning and Indoor Navigation (IPIN), 2010 International Conference on, IEEE, 2010. p. 1-4.