Public Safety Networks

2.1 Introduction

The greatest part of this thesis is related to the application of the techniques developed to Public Safety Networks (PSNs) environments. The main aim of this chapter is to provide a broad view of the PSN field, presenting the different emergency management phases, PSNs requirements and some of the challenges for this field.

Public Safety Networks are networks established by the authorities to either warn and prepare the population for an imminent catastrophe, or to provide support during the crisis and normalization phases. As shown in Figure 2.1, catastrophes can vary in nature and intensity. PSNs have the fundamental role of providing communication and coordination for emergency operations. Many of the problems of the PSN field come from the heterogeneity of systems and agencies involved at the crisis site and from their mobility patterns within the disaster site.

2.2 Main aspects of Public Safety Networks

The characteristics and requirements of Public Safety Networks may vary considerably depending on their purpose and placement. However, they are always mission critical; once deployed, PSNs have to be reliable since lives may depend on them. As an example, reports from September 11th point

Figure 2.1: Different disaster scenarios.

out that communications failures contributed directly to the loss of at least 300 firefighters and prevented good management of the rescue efforts which contributed to the loss of many other lives, [4] [74]. Moreover, communication failures were one of the obstacles in the coordination of the rescue resources in the 1995 Kobe earthquake [72]. These failures further prevented outsiders from receiving timely information about the severity of the damages. The communication breakdowns delayed the relief efforts which could have prevented the loss of numerous human lives.

Reliability of equipments and protocols is a serious matter for any type of network, but it is even more important in the context of PSNs. Maintaining communication capabilities in a disaster scenario is a crucial factor for avoiding preventable loss of lives and damages to property [104]. During a catastrophe such as an earthquake, power outage or flooding, the main wireless network structure can be severely affected and "historically, major

disasters are the most intense generators of telecommunications traffic" [104]. The public communication networks, even when available, may fail not only because of physical damages, but also as a result of traffic overload. Therefore, the regular public networks alone are often not sufficient to allow rescue and relief operations [104].

However, equipment failures and lack of connectivity are not the only problems faced in PSNs. Traditionally, PSNs have been owned and operated by individual agencies, such as law enforcement, civil defense and firefighters. Furthermore, they may belong and obey to commands related to federal, state or municipal governments. All these different PSNs are often not interoperable, which may represent a problem in the case of a catastrophe [10]. During the last few years some initiatives, such as MESA [76], have tried to solve the problem of interconnectivity among different agencies.

2.3 Emergency management phases

Disasters can be of different types: natural disasters, such as hurricanes, floods, drought, earthquakes and epidemics, or man-made disasters, such as industrial and nuclear accidents, maritime accidents, terrorist attacks. In both cases, human lives are in danger and the telecommunication infrastructures may be seriously affected or even no longer operational.

Disaster management involves three main phases:

1. **Preparedness**, at this phase all the equipment and people should be ready to enter in action, if needed. It consists of training, equipment maintenance, hazards detection and education.

2. **Crisis**, this phases goes from the break-out point (decision to respond), to the immediate disaster aftermath, when lives can still be saved. Crisis is understood as the society's response to an imminent disaster; it is different from the disaster itself.

3. **Return to normal situation**, this phase consists of the building and maintenance of temporary communication mechanisms/structures while the regular mechanisms are being repaired or rebuild.

2.3.1 Crisis parties

In a situation of crisis the involved parties can be classified in the following way, taking also into account the degree of mobility they need:

- Local Authority(ies); fixed: the group in the administrative hierarchy competent to launch a warning to the population and to the Intervention Teams.
- Citizens; either mobile or fixed: nonprofessional people involved in the crisis.
- Intervention Teams; mobile: professionals (civil servants or militaries) in charge of rescuing Citizens in danger, preventing hazard extension or any time-critical mission just after the break-out of the crisis; in charge of caring for injured people once the crisis is over.
- Risk Management Centre; fixed: group of experts and managers in charge of supervising operations. The Risk Management Centre works in close cooperation with Local Authorities.
- Health Centers; fixed: infrastructure (e.g. hospital) dedicated to caring injured citizen and backing intervention teams as for this aspect of their mission.

2.3.2 Alert phase

It is important to manage properly this critical phase as it is the moment where a quick response is the most efficient in terms of lives and goods saved. This means notifying professionals and people of the incoming hazard. Warning makes sense if there is a delay between the very break-out of the hazard and the damages it could cause. This leaves time for people to escape and avoid the endangered area. Warning the population is typically the Local AuthoritiesŠ responsibility since they are the only ones who can clearly appreciate the danger depending on local circumstances. Deciding that the situation is critical may be taken at governmental, national level. This is the case for example for earthquakes in all European countries.

2.3.3 Crisis handling phase

Coordination of Intervention Teams begins when the crisis breaks out. The Local Authorities alert them just before the population and then transfer the supervision to the Risk Management Centre. Later on, Intervention Teams still receive instructions from their Local Authorities, from the Risk Management Centre and from the Health Centre.

Intervention Teams send back information to Local authorities, to the Risk Management Centre, to Health Centers about the situation and request

for help. They typically use a specific purpose network deployed specially to attend to the needs of that particular event. Normally the same network is used for receiving instructions and returning feedback.

2.4 Important factors for Public Safety Networks

A flexible Public Safety Communication infrastructure has some specific requirements that need to be considered within the context of emergency response scenarios [38]. They are summarized in the following sections.

2.4.1 Disaster categories

Disasters differ from each other depending on their scale, which is crucial to consider in designing an appropriate response/recovery system. This can be defined by the degree of urbanization or the geographic spread. Degree of urbanization is usually determined by the number of people in the affected area, which is very important in disaster handling as the impact of the event changes based on the number of people involved and the breadth of spatial dispersion, both of which impact response and recovery from disasters.

Another key factor to consider is whether the disasters have been predicted or not. Clearly, sudden natural or man-made disasters do not give sufficient warning time. Other disasters may give a longer time window to warn people and take appropriate actions. Thus, if there is advance notification, it is potentially possible to set up a better communication infrastructure and possibly even have a backup technology in place before the disaster occurs.

2.4.2 Specific technology requirements

Each kind of disaster site has its own nature and has specific communication needs. For example, the number of attendees, mobility pattern and QoS parameters for a wildfire differ drastically from the ones in an earthquake relief effort. Users also may have different devices such as laptops, palms, or cell phones which may work with different network technologies such as WLAN, WiMAX, WWAN, Satellite, or wired networks. Additionally a communication network needs to be easily configurable and quickly deployable at low cost.

2.4.3 Mobility, reliability and scalability

In order to help emergency personnel to concentrate on the tasks, emergency network should be mobile, deployed easily and fast with little human interference. Therefore devices must be capable of automatically organizing into a network. Procedures involved in self-organization include device discovery, connection establishment, scheduling, address allocation, routing, and topology management. The system should also be able to support large number of users and data load without noticeable impact on the performance.

2.4.4 Interoperability and interdependency

Communication technology provides the tool to send data; however when information is sent over different channels or systems, interoperability may not necessarily have been planned for. First responders should be equipped with devices capable of using different technology by choosing the appropriate interface card and still working together to form a mesh network and communicate data. Therefore, regardless of what technology each individual might use, they are uniformly connected to the relaying mesh nodes and able to exchange data.

2.4.5 Multimedia broadband services

Communications for the benefit of local rescuers, national authorities or international assistance are mainly to coordinate efforts of field teams and connect teams to remote decision-making centers. In particular, retrieving monitoring data from the disaster site and distributing data to local teams or remote expertise centers are important requirements for an emergency communication system. Thus, providing broadband communication capacity during emergency or crisis times is becoming more and more necessary. Concerning services, users' basic requirements are voice and data communications with short and long range capabilities, but users require also multimedia communications with large volume of data able to provide the logistics of the situation, medical data, digital map, blueprints or intelligence data.

2.4.6 Knowledge and training

An important issue to be considered as addressed is the lack of knowledge of exact capabilities of the new technology being deployed and lack of training. The new technology needs to be installed and fully tested in drills and preparation exercises well before it is used in an actual disaster. It is also

very important to consider who will be the users of this technology and what level of knowledge and technical background they have. We would like to design future emergency communication tools and public awareness systems to be user-friendly with minimal training requirements, yet also secure.

2.4.7 Warnings and alerts

Warning messages should be provided with the consideration that some people may disregard the warnings, therefore even the well-designed warning system must consider human error or resistance. People may not evacuate to safe areas even if asked or ordered to do so for different reasons such as family, belongings, and pets, or they may not trust the accuracy or source of the warning. They may not take the warning seriously if they hear different messages from different sources, or if the source of the warning has not proven to be accurate or reliable in the past. The warning should provide a clear explanation of the nature of the disaster and appropriate actions to be taken.

2.5 Emergency alert systems

Emergency alert systems (EASs) play an important role in many countries and have also evolved and received considerable investment through time. For example, only in 2009 the budget requested to develop the new American EAS, the Integrated Public Alert and Warning System (IPAWS), was 37 million dollars [36]. IPAWS development is under the responsibility of the Federal

Emergency Management Agency [43]. When complete it will permit the broadcast of emergency messages not only through radio and TV but also by e-mail, cell phones and other different mediums. During a test pilot conducted in 2007 in Alabama, Louisiana, and Mississippi the system was able to send alerts to 60,000 residential phones in ten minutes and also with Spanish and Vietnamese translations [43].

The Japanese nationwide warning system, J-Alert, was launched in February 2007. It uses satellite wireless communication to issue a simultaneous warning to all municipal governments and interested agencies [68]. J-Alert works with warning sirens and an emergency broadcast system. The system is automatically activated and, from the time an emergency is confirmed, it is able to warn the population in less than 7 seconds.

RATCOM project [88], depicted in Figure 2.2, is one of the next generation EAS dedicated to detect and warn of tsunamis in the Mediterranean Sea.

When RATCOM will become operational, sensors will capture data and, if a real anomaly is detected, warning messages will be distributed automatically over the endangered region. The RATCOM alert system is composed of two main components: one ascendant and one descendant. The ascendant component is responsible for sensing the related data, filter false positives and retransmitting the relevant collected information to the coordination center. The descendant component is responsible for spreading the information of the imminent dangerous situation among the authorities and population in general.

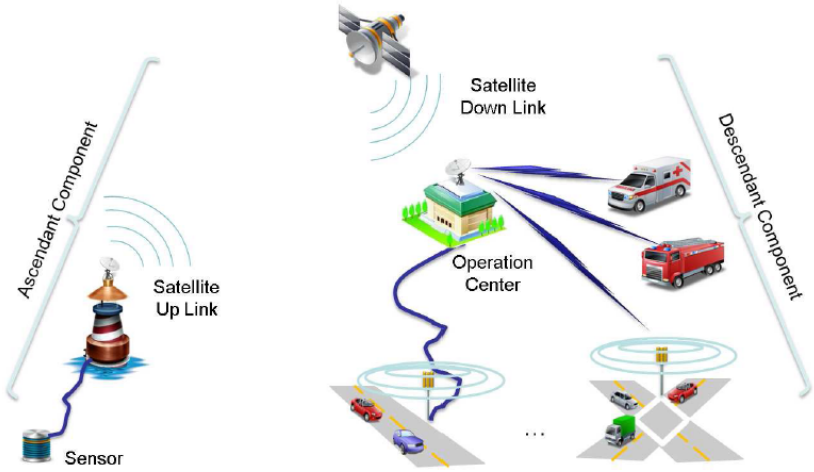

Figure 2.2: RATCOM project main architecture.

2.6 Public Safety Network projects

Public Safety Networks have attracted much research interest in the last few years. This section will present some research projects conducted in the field of PSNs.

The CHORIST project [33] is funded by the European Commission, and addresses Environmental Risk Management in relation to natural hazards and industrial accidents [33]. The backbone topology, presented in more detail in Section 7.2, is composed of Cluster Heads (CHs), Mesh Routers (MRs) and Relay Nodes (RNs). All the nodes' roles must be defined dynamically and based only on local information.

The WIDENS project [108] was a European project that aimed to design and prototype a next generation of interoperable wideband Public Safety

Networks. The project was concluded in 2006 and successfully proposed an easily deployable system for PSNs. Many of the results of the WIDENS project were incorporated in the MESA project.

The MESA project [76] is an international ongoing project in partnership between the European Telecommunications Standards Institute (ETSI) and the Telecommunications Industry Association (TIA) to create a global specification for mobile broadband public safety and disaster response networks. The mobile broadband specifications produced by the MESA project will touch the most different aspects and technologies related to PSNs, from remote patient monitoring to broadband satellite constellations interconnection, passing through mobile robotics and network reliability algorithms.

2.7 MAC layer challenges

Public Safety Networks present many challenges regarding the Medium Access Control and Physical (MAC/PHY) layers. Communication systems for this kind of network must be reliable and robust to failures. A rupture at the MAC/PHY level will compromise the whole purpose of the network. This is also true for any kind of network, but because they may be deployed in highly unstable environments, e.g. wildfire site, robustness is especially important in the context of PSNs. For this reason one of the most important research aspects of the MAC/PHY layer in PSNs is to provide robust and reliable protocols. On the other hand, past PSNs were narrow-band access only, enough for voice communication but not for multimedia applications. However, data-intensive multimedia applications have the potential to greatly improve the quality of the work and efficiency of first responders and relief efforts. For example, being able to download the blueprints of a industrial disaster site, online and on demand, can give to firefighters valuable hints of the best way to proceed during their operations. Wideband access with support for many different classes of Quality of Services (QoS) will be, in the next few years, not only desirable, but also mandatory for PSNs.

Nowadays there are many different wireless technologies in use, the integration and interoperability of such technologies is another big challenge for PSNs. However, the challenge is bigger than only taking care of the integration of the many technologies. The same technology is not necessarily suitable to every environment and every situation, seamless smart control of lower layer adaptation would enable the creation of better and more useful upper layer applications.

2.8 Network layer challenges

2.8.1 Topology control

The deployment and management of nodes for WMNs are challenging problems and they become even more interesting when we consider them in the context of PSNs. Not only PSNs are, by nature, life-critical but they also have strict requirements. Moreover, these requirements may vary significantly for different disaster sites [56]. For example, the number of nodes, people served, mobility pattern and deployment environment for a forest fire fight differs from the ones for an earthquake relief effort. Well-defined and maintained network structure is a fundamental step to enable the creation of efficient higher layer algorithms [85]. Thus topology control becomes a fundamental step for enhancing scalability and capacity of large-scale wireless ad hoc networks [91].

The main concerns in the establishment of public safety networks are rapid deployment and survivability [12]. PSNs must be reliable and endure even when deployed through rough environments. The network organization is a key factor to ensure endurance. In general, for small environments, the deployment of plain mesh networks is the easiest and fastest way to set a network in the field. However, this kind of structure is hardly scalable and appropriate for use on large scale and reliable environments. Structured networks, on the other hand, are more scalable, but the price to pay for this is the creation and maintenance of the structure.

Midkiff and Bostian [77] present a two-layer network deployment method to organize PSNs. Their network consists of a hub, and possible many-purpose specific routers, to provide access to nodes in the field. However, this work presents two characteristics that would be interesting to avoid in the PSN context. First, the hub represents a single point of failure. If something happens to it, all the communication would be down, even between nodes inside the field. It is important for PSNs to be as resilient as possible. The second issue is long range communications, all transmissions must pass through the hub, so the messages may transverse twice the whole network. Sarrafi, Firooz and Barjini [93] also present another interesting algorithm for topology control focusing on the power consumption optimality of the network.

2.8.2 Mobility management

PSNs may involve different equipments used by different Public Safety agencies, which need to move from the coverage of one mobile mesh router to

another transparently and seamlessly, relaying on a dynamic, easy to configure and scalable infrastructure at the disaster site. There is an urgent need for a local mobility management scheme for PSNs to support location and handoff management, as well as interoperability between different heterogeneous Public Safety organizations and terminals. Different solutions try to support mobility management in different layers of the TCP/IP protocol stack reference model. IP-based heterogeneous PSNs can greatly benefit of a network layer solution, which provides mobility-related features at the IP layer level without relying on or making any assumptions about the underlying wireless access technologies.

Mobility management enables the serving networks to locate a mobile subscriber's point of attachment for delivering data packets (i.e., location management) and maintain a mobile subscriber's connection as it continues to change its point of attachment (i.e., handover management). Mobile IPv6 (MIPv6) [66] is one of the most representative efforts on the way toward next generation all-IP mobile networks.

Recently, a network-based mobility management protocol called Proxy Mobile IPv6 (PMIPv6) [50] is being actively standardized by the Internet Engineering Task Force (IETF) NETLMM working group. It is starting to attract considerable attention among the telecommunication and Internet communities and we believe it has great potentialities in the field of PSNs. With PMIPv6 the serving network handles the mobility management on behalf of the Mobile Node (MN); thus, the MN is not required to participate in any mobility-related signaling. No requirement for modifications on Public Safety terminals is expected to accelerate the practical deployment of PMIPv6 for PSNs as any type of equipment from rescue teams can be used. Moreover, as the serving network at the disaster site controls the mobility management on behalf of the Public Safety users, the tunneling overhead as well as a significant number of mobility-related signaling message exchanges via wireless links can be reduced. Moreover, the handover latency is also massively reduced due to the fact the terminals keep their IPv6 addresses independently from their points of attachment to the deployed network, thus eliminating the procedures of Duplicate Address Detection (DAD), which represents one of the most time-consuming phases during handoff. Taking into account all these considerations, PMIPv6 may become an important candidate for mobility management in PSNs [59].

2.9 Application layer challenges

PSN still lack a uniform and complete solution to ensure the equipments, and applications, used by the rescue teams will always be connected to a secure and reliable communication infrastructure. The main problem comes from the fact that the IP address is used for describing the topological location of the host and, at the same time, to identify the host.

The Host Identity Protocol (HIP) [78] is a promising new basis for a secure mobile architecture for future PSNs [59]. The cornerstone of HIP is the idea of separating a host's identity from its present topological location in the Internet. HIP introduces a Host Identifier (HI) for each MN and a new layer between the network and the transport layer. In HIP, the transport layer connections are bound to the Host Identity Tag (HIT), a 128-bit hash of the HI, and no longer to the IP address. This simple idea provides a solid basis for mobility and multi-homing features [82]. HIP also includes security as an inherent part of its design, because its host identities are cryptographic keys that can be used with many established security algorithms and cryptographic identities are used to encrypt all data traffic between two HIP hosts by default.

2.10 Conclusions

This chapter provided a broad view of the PSNs field explaining the emergency management phases, challenges and highlighting some research projects in this field. Public Safety Networks play an important role in every one of the emergency management phases and, because lives may depend on them, PSNs are mission critical. They are a growing research field, which considers all the phases. This is due to the fact that, not only there are still many open problems that need to be solved, but also researchers are always trying to find better ways to improve the available infrastructure at the disaster site to provide faster and better solutions to detect hazards, manage crisis and return to the normal situation.