Public Safety Networks

ABSTRACT

Disaster can be defined as the onset of an extreme event causing profound damage or loss as perceived by the afflicted people. The networks built in order to detect and handle these events are called Public Safety Networks (PSNs). These networks 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 in the crisis site and from their mobility at the disaster site.

The main aim of this book chapter is to provide a broad view of the PSN field, presenting the different emergency management phases, PSNs requirements, technologies and some of the future research directions for this field.

1 INTRODUCTION

Public Safety Networks (PSNs) are networks established by the authorities to either warn and prepare the population for an eminent catastrophe, or as support during the crisis and normalization phases. The characteristics and requirements of these networks may vary considerably depending on their purpose and placement. 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 out that communications failures contributed directly to the loss of at least 300 fire-fighters and prevented a good management of the rescue efforts which contributed to the loss of many other lives, (9/11 Commission, 2004), (McKinsey & Co, 2002). Moreover, communication failures were one of the obstacles in the co-ordination of the rescue resources in the 1995 Kobe earthquake (Lorin, Unger, Kulling & Ytterborn, 1996). 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 on 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 (Townsend & Moss, 2005). 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” (Townsend & Moss, 2005). 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 (Townsend & Moss, 2005).

However, equipment failures and lack of connectivity are not the only problems faced by PSNs. Traditionally, PSNs have been owned and operated by individual agencies, such as law enforcement, civil

defense and firefighters. Even further, 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 (Balachandran, Budka, Chu, Doumi, & Kang, 2006). During the last few years some initiatives, such as MESA, have tried to solve the problem of interconnectivity among different agencies.

The main objective of this book chapter is to give to the reader a broad view of Public Safety Networks and to highlight some of the next challenges and research issues on this field. The rest of this chapter is organized as follows: Sections 2 and 3 introduce respectively the disaster management phases and the most important factors for Public Safety Networks in emergency situations. After that, on Section 4, we present some of the most important tools, projects and initiatives on the field of PSNs. Section 5 describes some of the most challenging aspects of the ongoing research on PSNs, and finally, Section 6 presents some final considerations about the field.

2 EMERGENCY MANAGEMENT PHASES

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

1. Preparedness must be to some extent envisaged:
   - PSN must be operational when some disaster occurs.
   - To observe the Earth, to detect hazards at an early stage.
2. Crisis from break-out (decision to respond) to immediate disaster aftermath, when lives can still be saved. Crisis is understood as the society's response to an imminent disaster; it must be distinguished from the disaster itself.
3. Return to normal situation must be envisaged with provisory networks.

Figure 1 represents the three main phases of a disaster management in a temporal scale underlining each different state.

Figure 1: Successive phases of an emergency situation

In this way it is possible to represent all the phases in a state diagram as shown in Figure 2.

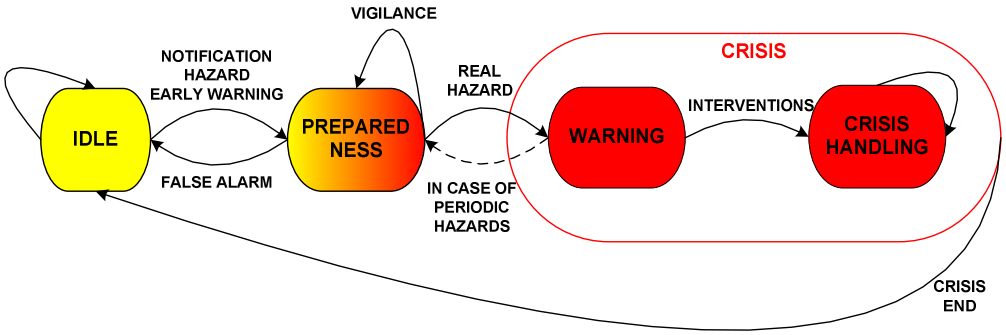

Figure 2: Emergency state diagram

2.1 Preparedness

The first phase called preparedness involves missions accomplished in normal situation. They are basically of three kinds:

1. Observation. The observation system has two main functions:
   - Detection of hazards. Satellite can play a role to that respect by means of observation and scientific satellites. A typical case when satellites can detect hazards prior to any other means is meteorological hazards.
   - Location of the source of hazards. Satellite is nowadays the best means to provide the geographical coordinates of any object thanks to GPS/Galileo/Glonass constellations. The idea is to have terrestrial sensors coupled with a GPS/Galileo/Glonass sensor.
2. Maintenance of the system. An emergency system must be ready to start at any time. To that end, it must be tested at regular time intervals in quiet times from end to end.
3. Education of professionals and citizens.

2.1.1 Detection of a hazard

In terms of networks, detection may be considered as the essential function of a *feeder link* or *uplink*. Detection of a hazard may be done by several means:

- Emergency call: this is the case where a citizen is calling a dedicated emergency call centre e.g. dialing 112 in Europe to witness of the break out of a hazard.
- Systematic watch by professionals e.g. helicopters flying over forests in summertime to detect fires.
- Sensors involved in a complex network with machine-to-machine connections. Sensors are useful in places where human being can not go (nuclear reactor) or actually rarely goes (water level sensor upward a river to detect inundations).

2.2 Crisis

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) (LA); *fixed*: the person (or group of persons) in the administrative hierarchy competent to launch a warning to the population and to the Intervention Teams ;
- Citizens (Cs); *either mobile or fixed*: non professional people involved in the crisis.
- Intervention Teams (ITs); *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 injured people once the crisis is over.

- Risk Management Centre (RMC); *fixed*: group of experts and managers in charge of supervising operations. The Risk Management Centre works in close cooperation with Local Authorities.
- Health Centers (HC); *fixed*: infrastructure (e.g. hospital) dedicated to caring injured citizen and backing intervention teams as for this aspect of their mission.

2.3 Warning

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 advertising professionals of the incoming hazard.
Warning makes sense if and only if there is a delay between the very break out of the hazard and the damages it could cause which leaves time to people to escape. Warning to the population is always Local Authorities' responsibility since they are the only one 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 examples for earthquakes in all European countries.

2.3.1 Crisis handling

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. In general, instructions are transmitted through a back-up network made up by a satellite terminal which links the disaster area to terrestrial backbones.
It is worth to create a "cell" surrounding the satellite terminal within which Intervention Teams communicate by terrestrial mobile radio means. This is called an EDECC (Easily Deployable Emergency Communications Cell). It is a very flexible solution based on radio mobile communication. In an EDECC, it is possible for example recreate a GSM communication cell by means of a mini Base Transceiver Station linked to a Mobile Switch Centre of any operator. Other technologies are possible too (e.g. Wi-Fi).
Intervention Teams return information to Local authorities, to the Risk Management Centre, to Health Centers about the situation and request for help. They use one and the same network for receiving instructions and returning feedback.

2.4 Return to normal situation

At that point, the crisis is over and the situation has come back to a stable point. The ordinary networks are down and it is necessary to set up a network able to work on a regular basis.
The main functions of the network are the following:

- Coordinating intervention teams and returning feedback from the field which is still necessary at that point.
- As far as possible enabling the same services as before the crisis and offering public access.

The architecture may be the same as the one outlined above with a satellite link but the network should be more stable and powerful.

3 IMPORTANT FACTORS FOR PUBLIC SAFETY NETWORKS IN EMERGENCY SITUATIONS

A flexible Public Safety Communication infrastructure has some specific requirements that need to be considered within the context of emergency response scenarios (Dilmaghani, & Rao, 2006). They are summarized in the following.

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, which makes a big difference in the response and recovery stage, 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.

Specific technology requirements:

Sometimes depending on the nature of disaster, there are more specific communication needs. For example, telemedicine communication may require interactive real-time communication. Transferring data, audio and video require special bandwidth requirements and high network security. The service needs to be reliable and continuous and work with other different first responder organizations' devices if necessary. Users 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.

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 maintenance. 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 reason for reliability is twofold. First, in emergency situations each rescue worker must neither be isolated from the command center nor from other team members. Second, mobility is likely to occur frequently in an emergency network. Thus, ability to adapt to network dynamics and harsh situations plays a major role in the design.

Scalability refers to the ability of a system to support large number of parameters without impacting the performance. These parameters include number of nodes, traffic load and mobility aspects. Limited processing and storage capacities of some of the radio devices are also a concern.

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 provided. First responder 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.

Another factor which needs to be considered in the design of future communication technology is minimizing possible interdependencies in a system. This helps to design a more robust system which is resilient to failures in sub-components of the system.

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, to retrieve monitoring data from the disaster site and to distribute 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.

Knowledge and training:

An important factor to be considered as addressed is the lack of knowledge on 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.

Information sharing and data dissemination:

In some disaster scenarios when people have important information, they may share this information wit the first responders if they feel safe to do so. Not only privacy is a factor that needs to be considered but also mechanisms to verify the accuracy of the information provided.

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 serious 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.

4 TERRESTRIAL AND SATELLITE PUBLIC SAFETY SYSTEMS FOR EMERGENCY COMMUNICATIONS: STATE OF THE ART

4.1 Terrestrial-based solutions

When faced with a situation of a disaster, rescue forces often rely on very simple communication systems as analogue and digital radio systems described hereafter.

4.1.1 HF, VHF, UHF equipments

In times of crisis and natural disasters, Amateur radio is often used as a means of emergency communication when wired communication networks, cellular wireless networks and other conventional means of communications fail.

High Frequency (HF) designates a range of electromagnetic waves whose frequency is between 3 MHz and 30 MHz. Very High Frequency (VHF) designates a range of electromagnetic waves whose frequency is between 30 MHz and 300 MHz. Ultra High Frequency (UHF) designates a range of electromagnetic waves whose frequency is between 300 MHz and 3.0 GHz. It is the actual most common tool used for communications by rescue teams because UHF is very easy to use and widely deployed in most of countries. Different rescue organizations can use the same frequency and so can communicate with each another (firemen, police officers). This solution is quite limited because the basic services provided by HF, VHF and UHF communication devices are voice.

4.1.2 PMR

The Professional Mobile Radio (PMR) is a communication system, which is composed of portable, mobile, base stations and some console radios. The antenna must be mounted in height. The coverage can vary significantly (between 3 and 7 km for point to point, up to 50 km for an extend networks). The PMR system is actually used by police centers and fire brigades. It is easy to use and to deploy. Many rescue teams are now familiar with these equipments in all the kinds of crises.
Some standards have been developed for specific usage and the Trans European Trunked Radio (TETRA) (TETRA, 2009) is the most developed. Several manufacturers propose different terminals for the communications, but all these equipments offer interoperability. The user can choose the manufacturer and the product he prefers.

4.1.2.1 TETRA

It is an open digital standard defined by the European Telecommunications Standard Institute (ETSI). The purpose of TETRA is to cover the different needs of traditional user organizations such as public safety, transportation, military and government.
TETRA is based on a suite of standards that are constantly evolving. It can support the transportation of voice and data in different ways. It is able to operate in direct mode (DMO) by building local radio nets and in standard mode (TMO). TETRA can thus be used as walkie-talkie (DMO) or as cell phones (TMO). Another mode, called “Gateway” allows TETRA terminals to use a gateway in order to extend the coverage zone.
The different network elements of a typical TETRA architecture makes it fully operational with other infrastructures (PSTN, ISDN and/or PABX, GSM, etc.). TETRA provides excellent voice quality through individual calls (one-to-one) but also through group communication. This technology can be utilized for emergency calls and ensure secure encrypted communications. The Release 2 of TETRA improves the range of the TMO (up to 83 km), introduces new voice codecs and speeds up the transmission of data up to 500 kbps.
Thus, the high coverage provided by TETRA, the fast call set-up (less than 1 s), both direct and gateway modes make of TETRA an interesting communication technology.

4.2 Satellite-based solutions

International rescue forces have nowadays started more and more to use satellite communications. After a disaster, even if the terrestrial network is completely out of order, it remains always possible to communicate using the satellite network.
Satellite communications are highly *survivable*, *independent* of terrestrial infrastructure, able to provide the load sharing and *surge capacity solution* for larger sites, best for redundancy: they add a layer of *path diversity* and *link availability*.
Thus, the benefits of using satellite in emergency communications are:

- Ubiquitous Coverage: a group of satellites can cover virtually the entire Earth’s surface.
- Instant Infrastructure: satellite services can be offered in area where there is no terrestrial infrastructure and the costs of deploying a fiber or microwave network are prohibitive. It can also support services in areas where exiting infrastructure is outdated, insufficient or damaged.

- Independent of Terrestrial Infrastructure: satellite service can provide additional bandwidth to divert traffic from congested areas, provide overflow during peak usage periods, and provide redundancy in the case of terrestrial network outages.
- Temporary Network Solutions: for applications such as news gathering, homeland security, or military activities, satellite can often provide the only practical, short-term solution for getting necessary information in and out.
- Rapid Provisioning of Services: since satellite solutions can be set up quickly, communications networks and new services can be quickly recovered and reconfigured. In addition, it is possible to expand services electronically without traditional terrestrial networks, achieving a high level of communications rapidly without high budget expenditures.

In times of disaster recovery, solutions provided via satellite are more reliable than communications utilizing land-based connections.

4.2.1 Fixed satellite services

Fixed Satellite Service (FSS) has traditionally referred to a satellite service that uses terrestrial terminals communicating with satellites in geosynchronous orbit. New technologies allow FSS to communicate with mobile platforms.

4.2.1.1 Satellite VSAT network

A satellite Very Small Aperture Terminal (VSAT) network consists of a pre-positioned, fixed, or transportable VSAT that connects to a hub station to provide broadband communications to hospitals, command posts, emergency field operations and other sites. Very small aperture terminal refers to small earth stations, with antennas usually in the 1.2 to 2.4 m range. Small aperture terminals under 0.5 m are referred to Ultra Small Aperture Terminals (USATs). There are also variants of VSATs that are transportable which can be on-the-air within 30 minutes and require no special tools or test equipment for installation. Remote FSS VSAT equipment requires standard AC power for operation, but comes equipped with lightweight, 1 and 2KW, highly efficient and self-contained power generator equipment for continuous operation, regardless of local power availability.
Internet access and Internet applications (i.e. VoIP) are supported through the remote VSAT back through the FSS provider teleport location which is connected to the PSTN and/or the Internet. A typical VSAT used by a first responder may have full two-way connectivity up to several Mbps for any desired combination of voice, data, video, and Internet service capability. VSATs are also capable of supporting higher bandwidth requirements of up to 4 Mbps outbound and up to 10 Mbps inbound.

4.2.2 Mobile Satellite services

Mobile Satellite Service (MSS) uses portable satellite phones and terminals. MSS terminals may be mounted on a ship, an airplane, truck, or an automobile. MSS terminals may even be carried by an individual. The most promising applications are portable satellite telephones and broadband terminals that enable global service.

4.2.2.1 Satellite phones

Several manufacturers offer mobile phones providing different coverage of the earth (IRIDIUM, 2009), (GLOBALSTAR, 2009), (THURAYA, 2009). In general, satellite phone is very user friendly; it looks like GSM mobile phone with one telephone number and one mini personal subscriber identity module (SIM). Satellite phones are water, shock and dust resistant for rugged environment and offer voice and data services with additional capabilities as call forwarding, two-way SMS, one touch dialling, headset/hands-free capability. The major advantage of this solution is the possibility to phone anywhere, any time, using a satellite link and then the normal public terrestrial phone network.

4.2.2.2 BGAN system

Broadband Global Area Network (BGAN) from Inmarsat (BGAN, 2009) operates in L-band and offers a number of innovative services (3G like) in the arena of mobile multimedia, video and audio multicasting and advanced broadcasting, with three land portable terminal types. Target users are professional mobile users (on-ground, maritime, aeronautical) in any service area worldwide, except Polar Regions. The service is IP-based and allows data transfer speeds up to 492 kbps, streaming up to 256 kbps. The high levels of portability of BGAN terminals, as well as the easiness of use, make BGAN attractive for emergency services. It is also the first mobile communications service to offer guaranteed data rates on demand.

It is relatively easy to plug a laptop on this equipment and to have an Internet access; this enables the use of IP facilities like Visio conference or other real time applications, with a correct quality thanks to the guaranteed data rate.

Currently the solution yet is not very exploited but tends to be developed. Its major advantage is the quasi-total cover of planet thus same that the polar zones and oceans.

4.2.3 COTM solution

Communications On The Move (COTM) is the most promising solution for emergency communications. FSS and MSS COTM solutions can provide fully mobile IP data and voice services to vehicles on the move up to 100 km/h (Figure 3). The comprehensive FSS COTM offering includes the terminal, teleport, and satellite capacity to provide high performance COTM IP connectivity.

Typical applications supported:

- Any vehicle can also serve as a mobile command post while in-route and as a fixed command access point for personnel upon arrival at the designated location when local Telco terrestrial and wireless infrastructures are not available.
- A full 10 Mbps downlink channel is delivered via FSS to the vehicle and 512 Kbps uplink channel transmitted from the vehicle to the Internet using IP support for voice, video and data simultaneously.
- Support for 802.11x wireless access allows vehicle to function as wireless hot spot access point for a First Responder convoy while in-route or a fixed hot spot for personnel upon arrival.

Figure 3: COTM equipments

4.3 Hybrid satellite/terrestrial solutions

4.3.1 TRACKS

TRACKS (TRACKS, 2005) deals with the development of the prototype of a van transportable communication station (VSAT terminal, GSM Micro Switch, BSC and BTS, internet access) dedicated to support pre-operational applications. It represents a good candidate telecom solution in case of crisis, when terrestrial communication are damaged or destroyed after a disaster.
TRACKS is deployed on the disaster area by local rescue teams. A local command centre can be deployed using the services provided by the van. Thanks to the satellite link, the teams are directly connected to a global command centre, which collect all the information (weather forecast, satellite images) and coordinate the local actions.
Thanks to the Wi-Fi Equipments, the rescue team on site can use the network developed by TRACKS with the office tools: PC, PDA and laptop. The services are not limited. Some applications like videoconference, telemedicine, cartography can be used thanks the internet access provided by the van.

4.3.2 Emergesat

Emergesat (EMERGESAT, 2009) is a system developed by Thales Alenia Space as an initiative funded by the French government in response to needs of responding to humanitarian crises.
Emergesat is basically a container specially designed in its dimensions, weight and the composite materials used in its construction, for transport in the luggage hold of any passenger line aircraft. It has rings for slinging under a helicopter, and is seal-tight under the most extreme weather conditions and totally autonomous in terms of power supply. The basic container incorporates its own communication equipment, and can also be used to transport a complete, autonomous water purification plant or small medical centre.
The core of the Emergesat communication system is a satellite transceiver unit, providing for high-rate communication from any point on the globe. Its automatic dish antenna ensures that the system can be placed in service immediately. A GSM transmission BTS connected to the satellite system makes it possible to set up a complete GSM network. A long-range Wi-Fi network system provides for connection with a large action perimeter.
A remote server collects all information required by the rear support bases. A software suite enables the operational teams to keep themselves fully informed about the evolution of the crisis, treatment of victims, civil engineering problems, etc. in real time. This system is fully open to all users. The teams in the field can hook up using a conventional tool (PC, PDA, etc.), and obtain information and decision-making aid services, including cartography, meteorology, languages and dialects, and also access collaborative working tools such as videoconference, messaging, application sharing.

4.4 Emergency alert systems

Emergency alert systems play an important role on 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, (Congressional Budget Office, 2008). IPAWS development is under the responsibility of the Federal Emergency Management Agency, (FEMA, 2009). 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, (FEMA, 2009).

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, (Kaneda, Kobayashi, Tajima, & Tosaki, 2007). J-Alert works with warn sirens and an

emergency broadcast system. The system is automatically activated and, from the time an emergency is confirmed, it is able warn the population in less than 7 seconds.

Ratcom project, (RATCOM, 2009), depicted at Figure 4, is one of the next generation EAS dedicated to detect and warn tsunamis on 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.

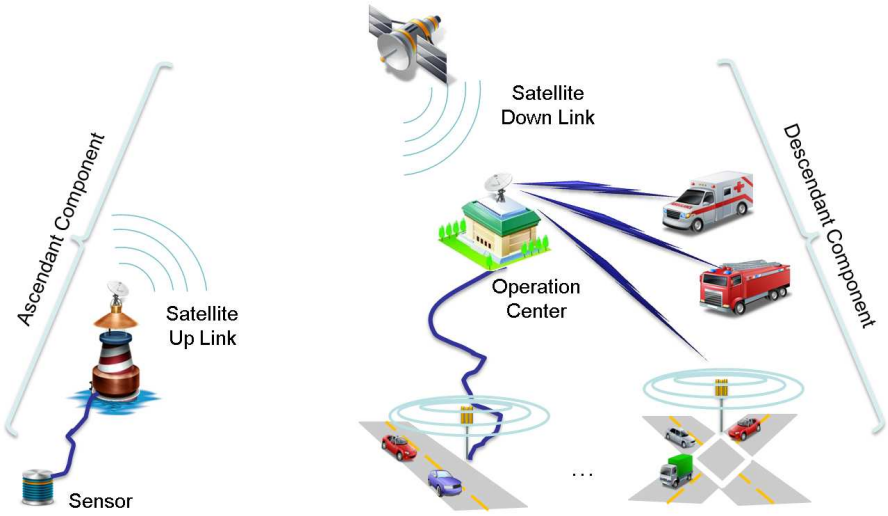

Figure 4 - Ratcom project main architecture

4.5 Public Safety Network projects

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

The CHORIST project, (CHORIST, 2009), is funded by the European Commission, and addresses Environmental Risk Management in relation to natural hazards and industrial accidents, (CHORIST, 2009). The backbone topology, depicted in Figure 5, 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.

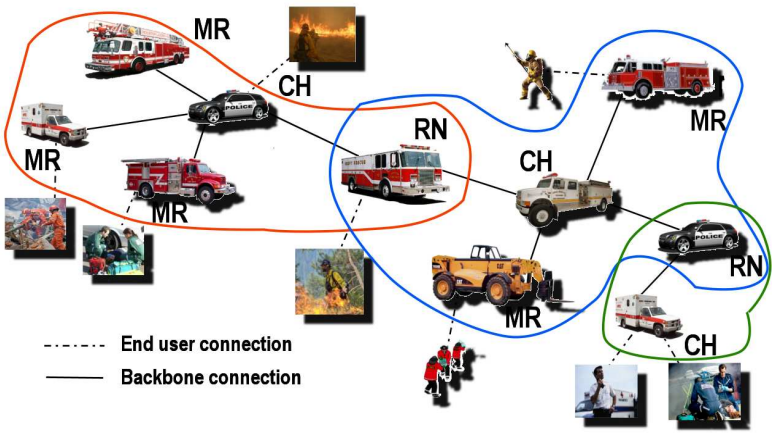

Figure 5 – CHORIST network description and components

The WIDENS project, (WIDENS, 2006), 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.

MESA project, (MESA, 2009), 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.

5 FUTURE RESEARCH DIRECTIONS

When a large scale disaster strikes, first responders are sent to the site immediately. One of the main needs of these teams is communication to efficiently organize the first responders operations. Unfortunately the disaster site may either not present a previous network infrastructure or this could have been damaged by the disaster itself. The communication infrastructure needs to be reliable and interoperable with the existing responder organizations' devices in a distributed system. Additionally, it needs to be easily configurable and quickly deployable at low cost. The system should be designed in a modular fashion that is easily upgradeable with the technology evolvement without the need to replace the entire system. This leads to an economic deployment solution which is affordable for different public and private agencies. Furthermore, it is desirable to provide redundancy for an effective network management based on the trade-off between reliability and cost.
Wireless Mesh Network (WMN) infrastructure well fulfils these application domain's specific requirements (Portmann, & Pirzada, 2008), but to assess its complete suitability to Public Safety and disaster recovery applications, it is necessary to include mobility support requirements to WMNs.

5.1 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 to be reliable and robust to failures. A rupture on 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. firewood site, robustness is especially important in the context of PSNs. In this sense one of the most

important research aspects for MAC/PHY layer research for 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 blue prints of a industrial disaster site, on line and on demand, can give to fire-fighters 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, on the next few years, more than desirable, will be mandatory for PSNs.

Nowadays we have 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. Not necessarily the same technology is suitable to every environment and every situation, seamless smart controls for the lower layers adaptation would enable the creation of better and more useful upper layer applications.

5.2 Network Layer Challenges

5.2.1 Topology Control

The deployment and the management of nodes for WMNs are challenging problems and they become even more interesting when we consider them in the context of PSNs environment. Not only PSNs are, by nature, life-critical but they also have strict requirements. Moreover, these requirements may vary significantly for different disaster sites, (Huang, He, Nahrstedt, & Lee, 2008). 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 (Rajaraman, 2005). In this sense topology control becomes a fundamental step to enhance scalability and capacity for large-scale wireless ad hoc networks (Santi, 2005).

The main concerns in the establishment of public safety networks are rapid deployment and survivability, (Bao, & Lee, 2007). 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 & Bostian (2002) 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 & Barjini (2006) also present another interesting algorithm for topology control focusing, the power consumption optimality of the network.

Câmara & Bonnet (2009), consider the problem of different deployment sites having different requirements and present a technique to dynamic adapt the topology to different requirements. The technique is inspired in the economy laws of supply and demand to dynamically organize the network. The authors argue that these economic concepts can perfectly map the main requirements of a topology management algorithm (stability, load balancing and connection demand). The first law of supply and

demand states that when demand is greater than supply, prices rise and when supply is greater than demand, prices fall. These forces depend on how great the difference between supply and demand is. The second law of supply and demand, then, states that the greater the difference between supply and demand is, the greater are the forces on prices. The third law states that prices tend to the equilibrium point, where supply is equal to demand. These same concepts are used to control the network behavior. Câmara & Bonnet defined a cost function to enable the network to self-organize and manage its topology and admission control.

5.2.2 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 IP layer without relying on or making assumption 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) (Johnson, Perkins, & Arkko, 2004) is one of the most representative efforts on the way toward next generation all-IP mobile networks. MIPv6 is a well-known mature standard for IPv6 mobility support and solves many problems seen in Mobile IPv4 (MIPv4) (Perkins, 2002). However, despite the reputation of this protocol, it has been slowly deployed in real implementations over the past years, and does not appear to receive widespread acceptance in the market. Furthermore, it has still revealed some problems such as handover latency, packet loss, and signaling overhead. Therefore, various MIPv6 enhancements such as Hierarchical Mobile IPv6 (HMIPv6) (Soliman, Castelluccia, El Malki, & Bellier, 2005) and Fast Handover for Mobile IPv6 (FMIPv6) (Koodli, 2005) have been reported over the past years, mainly focused on performance improvement in MIPv6. However, MIPv6 and its various enhancements are host-based mobility management protocols which require mobile nodes (MNs) to be involved in the mobility signaling messages and, therefore, they basically require protocol stack modification of the MNs in order to support them. In addition, the requirement for modification of MNs may cause increased complexity on them.

Recently, a network-based mobility management protocol called Proxy Mobile IPv6 (PMIPv6) (Gundavelli, Leung, Devarapalli, Chowdhury, & Patil, 2008) is being actively standardized by the 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 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 massive 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 (Iapichino, Bonnet, Del Rio Herrero, Baudoin, & Buret, 2009).

5.3 Application Layer Challenges

As already specified in the requirements of PSNs, it is important to provide mobility support to rescue teams ensuring connection always on during their movements in the disaster field and, at the same time, security and reliability, thus multihoming, to the system architecture at the crisis area. Although many of these requirements have been widely recognized for some time, a complete and adequate solution is still missing. Most existing approaches are point-solutions that patch support for a subset of the required improvements into the current Internet architecture, but do not cleanly integrate with each other and do not present a stable base for future evolution. As an example, Mobile IP (Perkins, 2002) (Johnson, Perkins, & Arkko, 2004) provides some support for host mobility, but still has major security flaws that prevent its widespread deployment.

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. Host Identity Protocol (HIP) (Moskowitz, Nikander, Jokela, & Henderson, 2008) is a promising new basis for a secure mobile architecture for future PSNs (Iapichino, Bonnet, Del Rio Herrero, Baudoin, & Buret, 2009). 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, not anymore to the IP address. This simple idea provides a solid basis for mobility and multihoming features (Nikander, Henderson, Vogt, & Arkko, 2008). 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.

6 CONCLUSION

This book chapter provided a broad view of the PSNs field explaining the emergency management phases, challenges and research directions related to PSNs. 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 regards 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.

REFERENCES

9/11 Commission (2004), National Commission on Terrorist Attacks Upon the United States. 2004. The 9/11 Commission Report: final Report of the National Commission on Terrorist Attacks Upon the United States, Retrieved October 13, 2009, from http://www.9-11commission.gov.

Balachandran, K., Budka, K. C., Chu, T. P., Doumi, T. L., & Kang, J. H. (2006, January). Mobile Responder Communication Networks for Public Safety, IEEE Communications Magazine.

Bao, J. Q. & Lee, W. C. (2007, November), Rapid deployment of wireless ad hoc backbone networks for public safety incident management, in Proc. IEEE Globecom.

BGAN (2009), Broadband Global Area Network from Inmarsat, Retrieved October 13, 2009, from http://www.inmarsat.com/Services/Land/BGAN/default.aspx.

Câmara, D. & Bonnet, C. (2009, June), Topology Management for Public Safety Networks, International Workshop on Advanced Topics in Mobile Computing for Emergency Management: Communication and Computing Platforms (MCEM 2009), ACM, Leipzig, Germany.

CHORIST (2009), CHORIST, A European Commission project, Retrieved October 13, 2009, from http://www.chorist.eu.

Congressional Budget Office (2008, October), H.R. 6658 Disaster Response, Recovery, and Mitigation Enhancement Act of 2008, Congressional Budget Office Cost Estimate.

Dilmaghani, R. B., & Rao, R. R. (2006, June), On Designing Communication Networks for Emergency Situations, In Proc. IEEE International Symposium on Technology and Society (ISTAS 2006).

EMERGESAT (2009), Emergesat from Centre National d'Etudes Spatiales website, Retrieved October 13, 2009, from http://www.cnes.fr/web/CNES-en/4972-emergesat.php.

FEMA (2009), Integrated Public Alert and Warning System (IPAWS), FEMA website, Retrieved October 13, 2009, from http://www.fema.gov/emergency/ipaws/.

GLOBALSTAR (2009), Retrieved October 13, 2009, from http://www.globalstareurope.com/en/.

Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., & Patil, L. (2008, August). Proxy Mobile IPv6, IETF RFC 5213.

Huang, Y., He, W., Nahrstedt, K. & Lee, W. C. (2008, May), Incident Scene Mobility Analysis, IEEE Conference on Technologies for Homeland Security: Enhancing Critical Infrastructure Dependability.

Iapichino, G., Bonnet, C., Del Rio Herrero, O., Baudoin, C., & Buret, I. (2009, June). Combining Mobility and Heterogeneous Networking for Emergency Management : a PMIPv6 and HIP-based Approach, International Workshop on Advanced Topics in Mobile Computing for Emergency Management: Communication and Computing Platforms (MCEM 2009), ACM, Leipzig, Germany.

IRIDIUM (2009), Retrieved October 13, 2009, from http://www.iridium.com/.

Johnson, D., Perkins, C., & Arkko, J. (2004, June). Mobility Support in IPv6, IETF RFC 3775.

Kaneda, H., Kobayashi, K., Tajima, H. & Tosaki H. (2007, March), Japan's Missile Defense: Diplomatic and Security Policies in a Changing Strategic Environment, Japan Institute of International Affairs.

Koodli, R. (2005, July). Fast Handovers for Mobile IPv6, IETF RFC 4068.

Lorin, H., Unger, H., Kulling, P. & Ytterborn, L. (1996), The great Hanshin-Awaji (Kobe) earthquake January 17, 1995, KAMEDO Report No 66, SoS Report 1996: 12

McKinsey & Co (2002), Increasing FDNY's Preparedness", City of New York: New York City Fire Department web site, Retrieved October 13, 2009, from http://www.nyc.gov/html/fdny/html/mck_report/toc.html.

MESA (2009), Project MESA - Mobile Broadband for Public Safety, Retrieved October 13, 2009, from http://www.projectmesa.org/.

Midkiff, S. F. & Bostia, C. W. (2002, June), Rapidly-deployable broadband wireless networks for disaster and emergency response. In Proc. First IEEE Workshop on Disaster Recover Networks.

Moskowitz, R., Nikander, P., Jokela, P., & Henderson, T. (2008, April). Host Identity Protocol, IETF RFC 5201.

Nikander, P., Henderson, T., Vogt, C., & Arkko, J. (2008, April). End-Host Mobility and Multihoming with the Host Identity Protocol, IETF RFC 5206.

Perkins, C. (2002, August). IP Mobility Support for IPv4, IETF RFC 3344.

Portmann, M., & Pirzada, A. A. (2008, January). Wireless Mesh Networks for Public Safety and Crisis Management Applications, IEEE Internet Computing, vol. 12, no. 1, pp.18 25.

Rajaraman, R. (2005), Topology control and routing in ad-hoc networks: a survey, SIGACT News, vol. 33, pp. 60-73, Jan.2002.

RATCOM (2009), RATCOM, the Risk prevention, RATCOM website, Retrieved October 13, 2009, from http://ratcom.org/default.aspx.

Santi, P. (2005), Topology Control in Wireless Ad Hoc and Sensor Networks, WILEY, July 2005.

Sarrafi, A., Firooz, M. H. & Barjini, H. (2006, October), A Cluster Based Topology Control Algorithm for Wireless Ad-Hoc Networks, International Conference on Systems and Networks Communication.

Soliman, H., Castelluccia, C., El Malki, K., & Bellier, L. (2005, August). Hierarchical Mobile IPv6 Mobility Management, IETF RFC 4140.

TETRA (2009), TETRA, Terrestrial Trunked Radio, Retrieved October 13, 2009, from http://www.tetra-association.com/.

THURAYA (2009), Retrieved October 13, 2009, from http://www.thuraya.com/.

Townsend, A. M., & and Moss, M. L. (2005, May), Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications, Center for Catastrophe Preparedness and Response & Robert F. Wagner Graduate School of Public Service, New York University.

TRACKS (2005), TRACKS, Transportable Station for Communication Network Extension by Satellite from European Space Agency website, Retrieved October 13, 2009, from http://telecom.esa.int/telecom/www/object/index.cfm?fobjectid=11550.

WIDENS (2006), WIDENS, Wireless Deployable Network System, Retrieved October 13, 2009, from http://www.comlab.hut.fi/projects/WIDENS/.