Chapter 11
Emergency Networks for Post-Disaster Scenarios

Gianluca Rizzo, Sasko Ristov, Thomas Fahringer, Marjan Gusev, Matija Dzanko, Ivana Bilic, Christian Esposito, and Torsten Braun

Abstract The focus of this chapter is on communication (and partially, computing) solutions which allow satisfying demands from the immediate aftermath of a disaster until full restoration of pre-disaster communication infrastructure and services. As traffic demand might differ substantially from the one in the pre-disaster scenario, due to the specific needs of post-disaster scenarios, it appears evident that a simple restoration of existing infrastructure and services might not be sufficient to satisfy it, and that specific solutions are required. This chapter reviews the most relevant

G. Rizzo (✉)
HES-SO Valais, Institute of Information Systems, Sierre, Switzerland
e-mail: gianluca.rizzo@hevs.ch

S. Ristov
Ss. Cyril and Methodius University in Skopje, Skopje, North Macedonia
e-mail: sashko.ristov@finki.ukim.mk; sashko@dps.uibk.ac.at

S. Ristov · T. Fahringer
University of Innsbruck, Distributed and Parallel Systems Group, Innsbruck, Austria
e-mail: tf@dps.uibk.ac.at

M. Gusev
Ss. Cyril and Methodius University in Skopje FCSE, Skopje, North Macedonia
e-mail: marjan.gushev@finki.ukim.mk

M. Dzanko
Faculty of Electrical Engineering and Computing, University of Zagreb, Zagreb, Croatia
e-mail: matija.dzanko@fer.hr

I. Bilic
Faculty of Economics Business and Tourism, University of Split, Split, Croatia
e-mail: ivana.bilic@efst.hr

C. Esposito
University of Salerno, Via Giovanni Paolo II 132, 84084 Fisciano (SA), Italy
e-mail: esposito@unisa.it

T. Braun
University of Bern, Institute of Computer Science, Bern, Switzerland
e-mail: torsten.braun@unibe.ch

J. Rak and D. Hutchison (eds.), *Guide to Disaster-Resilient Communication Networks*,
Computer Communications and Networks,
https://doi.org/10.1007/978-3-030-44685-7_11

post-disaster scenarios, outlining a set of reference use cases and their communication requirements. Then, it presents an overview of the state of the art for emergency and post-disaster communications. Finally, it focuses on a set of specific solutions of special relevance for disaster scenarios, outlining the main research challenges which are open to date.

11.1 Introduction

One of the key features of network failures originated by disasters which distinguishes them from other types of network failures is their larger geographical scope and their dynamism. The first feature translates into a high occurrence of *regional failures*, i.e. of simultaneous outages of sets of network devices within a given geographical area [57, 58]. As an example, hurricanes are often the cause of massive power outages in the USA and in Europe, causing the simultaneous failure of large sets of network devices within the affected region, and for relatively long periods of time (typically more than one week [24]). Heavy rainfall is another source of correlated and geographically constrained failures, often involving those wireless mesh network links with high capacity. The 2014 flood in Zagreb was at the origin of the unavailability of the whole national flight control system for several hours, due to a power outage and to the consequent unavailability of critical communication infrastructure [18].

When the disastrous event at the origin of an outage is an earthquake or a volcanic eruption, typically the damages to the communication infrastructure are heavier, and the recovery of the network connectivity slower due to mobility and logistic issues associated to such types of disasters. As an example, the earthquake of magnitude 7.1 which struck Taiwan in 2006 severed several undersea cables, causing the interruption, for several weeks, of the Internet connectivity between North America and Asia. The 9.0-magnitude earthquake which struck Japan in 2011 affected the operativeness of 1500 switching sites by damaging undersea cables and causing several power outages. Similar patterns occurred in Europe, where the earthquake which took place in Greece in 2011, and which affected mainly the city of Patras, collapsed the telecommunication network [58].

An example of post-disaster scenario related to volcanic eruptions, quite frequent in Iceland, is given by floods due to subglacial volcanic eruptions, such as the one involving the Katla volcano, which rapidly generate a large mass of water by melting of the ice from the glacier. As volcanic sites are of particular interest for tourism, they are often relatively densely populated (e.g. on campsites, hostels, connecting roads and hiking trails). Often, cellular coverage in the area is absent/insufficient even before the disaster strikes, so that not all of the population can be effectively warned through SMS cell broadcast.

Fires, resulting in millions of acres of the EU land being burnt to ashes every year in Greece, Spain, Italy, France or Portugal, are in turn reported to be frequent reasons for failures of communication infrastructure in Southern Europe. Climatologists confirm that due to global warming, the frequency of weather-based disaster occurrence is predicted to increase. Another important reason for disruptions on a massive scale is related to intentional human activities, referred to as attacks (e.g. bombing or use of weapons of mass destruction attacks, electromagnetic pulse attacks) whose goal is to cause failures of important equipment (e.g. nodes switching/storing large amount of data; high capacity links).

During and after a disaster, communications play a key role in facilitating response and rescue operations, and in decreasing risks and negative consequences for the involved population, such as limiting secondary morbidity and disease [40, 64]. The population in the disaster area needs to be informed on how to obtain assistance, on the personal risks and on how to protect from them [62], but it also needs to communicate with family and acquaintances.

The involved institutions must communicate early and frequently with multiple stakeholders to promote an orderly response plan [52] and to prevent public disorder, crime and theft. Decision makers need to be constantly updated on the status of the ongoing response efforts and to coordinate relief actions. Health professionals need to be updated on health risks or diseases and on their evolution in the involved area and on how to inform and advice the involved population.

The instruments typically used for exchanging this type of information include press releases, media interviews, articles on blog, on news and on social media, town hall forums, together with real-time communications among responders. Challenges here include the difficulty in designing an effective, comprehensive disaster communication plan [66] and communications preparedness [8], which is frequently overlooked and underdeveloped. However, the most serious challenge to such information exchange during disasters is typically represented by the consequences of disasters themselves on the infrastructure for power supply and on the telecommunication network.

The focus of this chapter is on communication (and partially, computing) solutions which allow serving demands from the immediate aftermath of a disaster until full restoration of pre-disaster communication infrastructure and services. As traffic demand might differ substantially from the one in the pre-disaster scenario, due to the specific needs of post-disaster scenarios, it appears evident that a simple restoration of existing infrastructure and services might not be sufficient to satisfy it and that specific solutions are required. This chapter is organized as follows. Section 11.2 reviews the most relevant post-disaster scenarios, outlining a set of reference use cases and their communication requirements. Then, Sect. 11.3 presents an overview of the state of the art for emergency communications in post-disaster scenarios. Section 11.4 focuses on a set of specific solutions of special relevance, outlining the main research challenges which are open to date. The chapter is concluded in Sect. 11.5.

11.2 Post-Disaster Scenarios Characterization and Emerging Communication Requirements

In what follows, we focus on a set of representative services which are relevant in case of disaster, and on their communication and computing requirements, reviewing a set of representative services which play a key role in the context of a disaster and the mode(s) of communication on which they are based.

11.2.1 Social Media for Disaster Communications

Typically, one of the consequences of disastrous events consists in making more difficult the mobility and the exchange of goods and of information between the population residing on the site of the disaster and the rest of the world. Reaching out to other people in case of a disaster is a primal instinct, and enabling such communications is an essential aspect of any disaster response and mitigation solution. However, typically on the onset of a disaster the volume of communication exchanges increases often way beyond the capacity of existing networks. This phenomenon gets to its worst immediately after the disaster, with a peak demand for communication and information exchange. For instance, 6,732,546 tweets were collected for Hurricane Harvey, 1,207,272 tweets for Hurricane Irma [1], and out of them, 300,000 tweets were in the first day of the emergency.

Based on the stories of people who found themselves in the disaster areas, it is clear that establishing a communication immediately after the disaster occurs is very challenging. A promising solution is represented by the implementation of hotspots offering exchange of short text messages, particularly in the immediate aftermath of the disaster, when the need to communicate is stronger, due to people seeking to contact family and friends, and looking for information regarding food, shelter and transportation.

There are several existing solutions for the delivery of a limited set of services in a disaster area, such as use smaller text messaging services, instead of normal phone services for communication or web browsing on Internet. Examples of solutions include Comcast (which opened more than 137,000 hotspots for Floridians to use for free, so people can stay connected during the latest Florida Hurricane) and Everbridge Critical Event Management Platform (which sent over 20 Million Hurricane Irma-related messages).

One of the first uses of social media in disaster communication has been during the Haitian earthquake of 2010, for which various social media have kept the world informed [70], allowing people to share critical information about post-disaster issues and availability of resources. Moreover, there is evidence suggesting that the experience of the Haitian earthquake has stimulated the elaboration of new mechanisms of communication about disasters, among which we have information dissemination and crowd funding via social media [25]. Following that experience, social media is currently used by several actors (e.g. media outlets, communities, governments, organizations and individuals) in post-disaster scenarios and for various other purposes [28].

11.2.2 Situational Awareness

The ability to exchange information on the status of rescue operations, on the conditions of the affected population, on the availability of services, and more generally, about the context in which rescue teams have to operate, is one of the main challenges which result from the onset of a disastrous event. The unavailability of (at least part of) the communication infrastructure hampers the ability of rescue operators to collect data also about pre-disaster conditions, further complicating the implementation of a common, shared vision of the conditions of the area affected, as well as of the various rescue and disaster mitigation actions.

In this respect, a crucial issue is the coordination of the efforts of disaster response teams. Among the factors which make it very challenging to coordinate such efforts, often with heavy consequences in terms of waste of time and resources, is the integration of untrained rescuers and of heterogeneous rescue teams. Indeed, such integration is often inevitable when disasters strike a large region, such as in earthquakes or in massive floods, and when the delay of intervention plays a key role in determining its effectiveness. In such scenarios, it is inevitable to involve the local population in the process of information collection and sharing. Indeed, the affected population typically has precious information for the rescuers (e.g. number of people affected, their medical condition, availability of food, shelter or clean water, or presence of disaster induced hazards, such as gas leaks, etc.).

To this end, it is crucial to share a common information base among all these actors, in order to achieve some form of coordination and to prioritize interventions. However, this is a particularly challenging goal in those contexts where communication infrastructure is unavailable and where some form of pre-disaster coordination among these actors has not been implemented. The effectiveness with which information is shared is indeed key in order to speed up interventions, to optimize the utilization of available resources and to establish effective priorities for interventions. A critical requirement for facilitating coordination in search and rescue operations is therefore the possibility to establish a coherent, reliable common vision of the status of the territory, of the population affected, of those in need of some form of help or rescue and of the number, distribution and status of the resources available to implement such rescue actions.

11.2.3 Complex Crises: Recovery and Reconstruction

Nowadays, a large number of populations, more or less evenly spread around the globe, are periodically under critical conditions, originated from natural events, such as floods or earthquakes, or due to malicious attacks, such as acts of terrorism. Besides dramatic structural damages, Chemical Biological Radiological Nuclear (CBRN) contamination risks can arise as a consequence of these events (the Fukushima accident is among the most known examples) leading to both economic and humanitarian tragedies. On the onset of such disasters, large geographic regions are typically affected, often encompassing several countries. At the same time, the activities of recovery and reconstruction are getting increasingly costly, complex and long-lasting, particularly in those cases where a decontamination of the affected environment is required. In these cases, local authorities or dedicated civil protection organizations usually coordinate the emergency management, the Post-Crisis Needs Assessment (PCNA) and the Reconstruction and Recovery Planning (RRP) [16], possibly supported by a various national and international organizations for disaster relief, often operating in a relative autonomy.

The damage assessment needs analysis of a massive volume of data, and the recovery and reconstruction planning process is typically coordinated through periodic physical meetings of the involved organizations, in which information is shared about the situation, priorities set and responsibilities allocated. Follow-up and execution of tasks is managed by each individual relief organization, by sharing assessment data or acquiring valuable information from teams deployed on the field, based on international standards, procedures and methodologies (e.g. Damage and Loss Assessment (DaLA) Methodology [44]). Harmonizing, coordinating and aligning data collection processes, offering state of the art surveillance technologies within an integrated information management system for PCNA and RRP, is a demanding capability for emergency networks used for damage assessment. Earth observation data and aerial imagery are acquired by the involved organizations and authorities, and they needs to be exchanged among all the involved organizations, so as to have a general idea of the extent of the areas affected by the disaster (pollution and temporal dispersion in water/soil/air), and to assess the infrastructure affected by pollution and/or contamination. The geo-spatial tools integrated within emergency networks provide relevant information in identifying the location and the extent of the disaster and predicting its dynamic evolution, in locating the people and critical infrastructures affected, and finally by assisting the assessment of accessibility to these people and critical infrastructures. During the reconstruction phase, further analysis of damages as well as short- and long-term impacts on environment, human safety and economy can be provided and the emergency networks are leveraged for this scope.

11.2.4 Disruption of Vehicular Traffic

On the occurrence of natural disasters which have an impact on road infrastructure (e.g. floods wiping off roads, earthquakes destroying bridges or under heavily adverse weather conditions), vehicular traffic is typically deeply perturbed, in ways which are often hard to predict. Often the consequences of a disaster make it unsafe and difficult to move in (or through) the affected areas. In addition, the needs arising from the consequences of a disaster (due, for instance, to rescue operations, or to the population moving out of the affected area) translate into new traffic patterns, which the post-disaster road network is often not capable of supporting adequately.

An interesting example is represented by the post-eruption scenarios in Iceland. The whole island is characterized by unbridged river crossings, which typically require off-road cars. The viability of such crossings depends strongly on current and past weather conditions, as well as on the type of off-road vehicle. Even in regular scenarios, the frequency of accidents due to errors of evaluation is very high. The fact that those accidents take place in remote and uninhabited regions, with poor or no cellular coverage, makes rescue operations difficult.

In those environments, the primary source of disasters are volcanic eruptions, which often take place suddenly and which typically have a heavy impact on viability of the island, either direct (i.e. with lava invading roads) or indirectly (i.e. when lava melts ice and snow, provoking floods in vast regions). As a result, the already difficult transit in those regions becomes even more so, generating a high rate of accidents and leaving many small communities and people in transit isolated from the rest of the country. Very similar consequences to viability are produced in other countries by floods due to heavy rains, by fires or earthquakes. The impossibility to move people and information between different groups of people in the disaster scenarios is one of the key sources of hazards for the involved population and one of the main factor affecting the effectiveness of the rescue operations.

The importance of the availability of communication services in such scenarios resides in the possibility for drivers to take decisions at the right time and while being aware of the context and of possible risks, and possibly to ask for help. In a scenario of a flood or of a fire, for instance, the possibility of alerting vehicles of the hazards associated with crossing the affected regions is crucial to avoid increasing the amount of people affected by the disaster. Moreover, in such conditions vehicles moving out of the affected areas posses valuable first-hand information about the disaster and the associated hazards, which should be made available to other vehicles and people in the region.

11.2.5 Management of Medical Emergencies

One of the key issues arising in post-disaster crisis is the difficulty in providing effective and timely medical assistance, due to lack of personnel, of appropriate medical equipment, but also the lack of information which could help establishing appropriate priorities of intervention. First aid responders use triage to classify the patient's condition based on fast scanning and decision making by determining the priority of treatments and urgency for patient transportation to the hospital. Emergency protocols which are well defined before the disaster strikes are crucial to ensure adequate medical assistance in most efficient way, serving the largest number of injured in the shortest period [17]. Preparedness of management of medical institution and capacity of first aid responders are crucial factors, aiming to reduce further damage, to reach high percentages of survival rate, and to prevent or reduce further injuries, which might arise from inadequate or delayed emergency assistance.

Specific emergency equipment can be used in triage to speed up the process and make it more efficient, such as the one described in [27]. It includes use of an IoT wireless connected sensor for analysis of health-related parameters. The communication needs to be established via personal area network technology, in order to save the energy of used sensors and devices.

11.2.6 Post-Disaster Service and Communication Requirements

In a communication solution for post-disaster scenarios, communication services can be broadly grouped into the following categories [51]:

- **Data messages**. Many types of data messages should be transported by wireless or wired equipment. In emergency scenarios, such messages may consist in location information, building plan download, health status of rescue workers transmission to remotely monitor their health, sensor data for monitoring surrounding and special alarm transport;
- **Real-time voice**. This is by far one of the most requested services in the immediate aftermath. It enables efficient coordination of the efforts between rescue team members and between on-field teams and other first-responder team members;
- **Picture/Video**. Exchange of still pictures or videos is useful to locate victims or suspicious elements in the surroundings. It also helps in achieving effective coordination of rescue operation;
- **Real-time video**. Real-time video sent from the scene is useful for surveillance and remote medical treatment;
- **Remote control**. It is needed in the rescue operations as an extension to human activities, for example to steer robots to access dangerous areas.

Such a diversity in communication services implies a wide diversity in QoS requirements and constraints in terms of delay, jitter, packet error, loss rate and bandwidth. For instance, voice/video calls are sensitive to delay and jitter, while services based on the exchange of data messages for critical warnings and alarms require tighter constraints on packet error or loss rates.

In addition to the specific communication service required, a communication solution for post-disaster scenario is also characterized by a set of requirements deriving from the domain of operation. They include [51]:

- *Self-organization*. A critical requirement for emergency networks is simplicity and rapidity of deployment, possibly with little human intervention. Whenever possible, communicating devices should be able to autonomously and automatically set up a network and coordinate the exchange of information. Among the main functionalities which such devices should implement in such a self-organized fashion are scheduling, address allocation, device discovery, connection establishment, topology management and routing;

- *Autonomous functioning*. The disaster-resilient communication system should operate in a way which is as much as possible independent of any other system, including wireless or mobile operator networks, and power supply network. An aspect of this requirement is represented by power efficiency, which is crucial in guaranteeing an acceptable level of service availability even in contexts with intermittent or absent power supply;
- *Reliability*. In emergency situations, poor communication availability, possibly due to mobility, may result in rescue workers getting isolated from the command centre and/or from other team members. Hence the ability to maintain a high level of connection and service availability, possibly through a design which adapts to network dynamics and harsh situations, is a key requirement;
- *Data storage capability* is an important issue, since the system must function with limited energy supply and no connectivity to other systems. Keeping data at the premises of a given server planned to act as emergency solution, introduces some amount of redundancy in essential information;
- *Interoperability and scalability*. Emergency networks should provide a common communication platform between various organizations involved in disaster assessment, recovery and reconstruction. The issues posed by technological, syntactical and semantic heterogeneity among the ICT infrastructures put in place at each organization need to be addressed. Moreover, the system should be able to support a large number of communicating entities and high traffic load levels without impacting the performance of the services it delivers;
- *Security*. Emergency networks exchange very sensitive or classified information. The involved entities should be able to define access rights for the information they store or exchange. An adequate protection against data stealing and data forging is a key requirement.

11.3 State of the Art on Post-Disaster Emergency Networks

Emergency response system uses various wireless technology such as cellular network, Wi-Fi and LR-WPANs (IEEE 802.15.4) [53, 59]. The majority of these are based on a client–server mode of communication, and they depend completely on the service provider, such as those requiring base stations and access points. In addition, the architecture underlying several of them makes them prone to congestion and/or to system performance degradation due to node (base station or access point) failure. In order to overcome these issues, several network models and frameworks have been investigated [36, 46, 71]. A few of them are discussed here briefly, following the analysis in [59].

In [41], authors propose the OEMAN architecture for disaster recovery. Its main goal is to deliver Internet connectivity in the region affected by the disaster. When the disaster occurs, a network controller initiates the configuration and sets nodes into an emergency state, in which nodes download the software for disaster recovery configuration by connecting to an access point. This configuration implements a routing strategy based on a tree topology, and it manages the allocation of IP addresses. The OEMAN architecture is able to detect unbalanced traffic patterns and to take appropriate measures to change the network configuration and rebalance the traffic. Thanks to the use of virtual access points, overloaded nodes are able to transfer the traffic to other, less loaded nodes. Finally, the proposed architecture is capable of handling node failures and node mobility.

Minh et al. [42] propose a solution for a disaster recovery access network based on a tree topology, in which software-based access nodes operate in two modes. In one mode, they manage their own network, while in other mode they provide connectivity to other networks by acting as relays. The basic technological elements of the proposed solution include virtual AP abstraction, reconfiguration support, wireless interface abstraction and triggers for NAS auto-downloading. The resulting network is able to establish connectivity quite rapidly, and it easily supports extension to large networks. One of its main drawbacks is the difficulty with which link failures can be detected, particularly in large networks.

Briante et al. [11] propose a framework for enabling disaster survivors to communicate, based on strategy of smart node positioning in order to facilitate the diffusion of messages, on virtual networking and on opportunistic communications. A key role in the framework is played by special purpose nodes, which trigger the process of epidemic spreading, advertise evolution modules and implement long range connection links. The proposed approach is based on a strategy for optimizing the positioning of the special purpose nodes, which changes the location of nodes in order to improve the diffusion performance. Experimental results show the effectiveness of the mechanism for smart node positioning in enhancing the dynamics of message diffusion.

P2P architectures based on delay-tolerant networking (DTN) are another approach adopted by some systems in order to maintain end-to-end routes. George et al. [23] propose an architecture based on IEEE 802.15.4 aiming at monitoring the messages of survivors in an area affected by a disaster. The network supports various routing strategies according to the available nodes, their topology and mobility characteristics and the degree of connectedness of the network, including delay-tolerant routing and on demand routing.

Fujiwara and Watanabe [21] present a routing protocol for emergency communications. It considers a hybrid network to maintain connectivity between base stations and nodes in a disaster scenario, based on both ad-hoc networking and cellular access networks. In the proposed architecture, nodes switch to ad-hoc mode whenever the cellular connectivity is absent or fails. The route discovery mechanism is based on monitoring the communications of neighbouring nodes, rather than on diffusion of route request packets. The MAC protocol adopted is based on time division multiplexing, and hence, it is able to provide low latency at the cost of a reduced network throughput.

Another emergency networking solution based on a heterogeneous network, and on the combination of ad-hoc and infrastructure communications, is proposed in [47].

Its key features are ease of deployment and maintenance and the automatic determination of the location of each node. Its assessment is based on a two-dimensional random walk mobility model for survivors.

Chipara et al. [14] describe an emergency response framework which is able to adapt to dynamic environments and provide reliable communications. The proposed framework is functional even in settings where infrastructure support is absent or only partially available, and it is able to adapt to various connectivity technologies and different mobility scenarios.

Aschenbruck et al. [7] propose a mobility model for populations in a disaster area, which is based on movements on an optimal path within the given area, and which includes node churn. The paper shows that the proposed model enables realistic modelling of mobility in disaster scenarios, delivering results in the performance analysis of routing protocols in such scenarios which are substantially different than those obtainable with classical random waypoint models.

Finally, Król et al. [35] compare various techniques for coverage extension in disaster areas, based on both mobile and static nodes. The power outage probability of mobile stations is modelled using measured data. The paper shows through simulations that solutions based on static relays offer a greater efficiency and reliability for implementing coverage extension.

11.4 Post-Disaster Emergency Networks

11.4.1 Floating Content Support to Disaster Relief and Situational Awareness

Since their first appearance, opportunistic communications have been considered as key in enabling communications in challenged environments. This is particularly true of post-disaster scenarios, due to their ability to adapt the communication mode to the available infrastructure and transmission conditions. In such settings, ad-hoc networks may involve in the information exchange a large variety of devices, such as Internet of Things (IoT) devices (e.g. devices embedded in the environment, such as in buildings), UAVs and smartphones, together with moving and parked vehicles. Such a heterogeneous set of communicating devices holds the potential to enable the exchange of critical information in support of the population struck by the disaster, and of any organized or spontaneous relief initiatives. Ultimately, such a network could be connected to the Internet (e.g. through surviving Wi-Fi access points or cellular base stations, or by means of data mules and agent-based forwarding mechanisms [9]), thus ultimately breaking the isolation in which disastrous events typically force large fractions of the local population.

In this section, we focus on a specific approach to opportunistic information exchange, which goes under the name of Floating Content (FC) [33], but also Hovering Information [13], Locus [67], LINGER [10], among others. Floating Content is

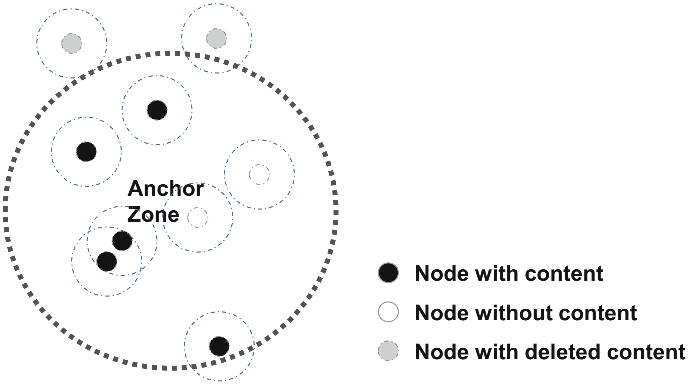

Fig. 11.1 Content floating in an anchor zone [2]

an opportunistic ad-hoc communication paradigm conceived for delay and disruption tolerant networking (DTN), i.e. for conditions in which nodes are sparsely located, and in which store-carry-and-forward is the main mode of communication. The goal of FC is not to support one-to-one information exchange, but the sharing of information of common interest over a given geographic area referred to as the *Anchor Zone* (AZ). Every time a node intends to share a piece of content (e.g. a critical information about the local environment, such as the availability of medical support or the presence of a dangerous item) it defines an AZ, usually centred around the location to which the content refers to, and wide enough to guarantee that (I) everyone who needs the information actually gets it, and that (II) the content does not disappear from the given area due to node mobility or failure. Inside the AZ, every time a node with the content gets in range of a node without it, the content is replicated, while outside the AZ nodes are allowed to erase the content if needed (Fig. 11.1). A large amount of research on such communication paradigm has focused on establishing strategies for dimensioning size and shape of the AZ as a function of a specific performance parameter for FC [4, 30, 33, 38, 50], defined according to application-level performance requirements. Other works focus on adapting FC strategies to practical settings and realistic mobility patterns [3, 37]. Collectively, these results suggest that the FC paradigm, when appropriately engineered and despite its best-effort character, is able to deliver satisfactory performance for a large spectrum of applications and in a wide variety of realistic set-ups and mobility patterns. Experimental set-ups such as the one in [2] show that FC performs even better than expected in realistic settings, thanks to node clustering which is a key feature of vehicular and of human mobility, and which naturally arises in disaster scenarios. Other features which make FC a good fit for such scenarios are its relative simplicity of implementation and of dimensioning, its ability to work even in completely infrastructure-less set-ups while at the same time being able to take advantage of static nodes and of infrastructure whenever available and its adaptability to any mobility pattern.

In disaster scenarios, several typical features of human mobility, such as the tendency to cluster in order to stay close to available basic services, and to get information, and the tendency to use a restricted subset of communication roads and paths, clearly facilitate content diffusion and persistence. For instance, patterns of traffic in opposite directions in the same road (people fleeing from an area and rescuers entering that area), which is a specific feature of disaster scenarios, greatly facilitate content spreading.

In what follows, we analyze the suitability of FC as a communication paradigm in support of situational awareness application for post-disaster settings, and we consider the main technical challenges which have to be addressed in order to implement such a service.

A key assumption on which our analysis relies is that smartphones of at least a fraction of the people present in the given scenario (including both affected population and members of rescue teams) are endowed with an application which implements the FC paradigm, in order to enable content exchange. This assumption is related to the more general issue of disaster preparedness, which is one of the most critical aspects of emergency response. In the absence of any pre-disaster initiative aiming at diffusing the FC application among at least a fraction of the population, the use of the FC paradigm must rely on some form of epidemic diffusion of the FC application itself in the aftermath of the disaster. Indeed, as fast response and coordination among the various actors and penetration of external rescue teams into the affected area might be slow and very challenging, it would be hard to spread such application by relying only on direct delivery from rescue teams, as such approach might prove ineffective, or too slow if compared with the reaction times typically required to address medical emergencies. A possible way to tackle this issue is to design a strategy for FC application dissemination based on the use of the very same FC paradigm, in which the FC application, in addition to supporting the diffusion of information relevant to the context in which it is used, replicates itself in the process, in order to increase the amount of nodes participating in the process, hence improving its performance and that of the supported service. A possible way to implement this is to let every FC application play the role of a Wi-Fi access point, and to use the captive portal technique [22] to let every user associated to the access point download the FC application.

In a possible implementation of a situational awareness service based on FC, the application would spread via FC a map of the region affected by the disaster. Then, every participant node would take care of annotating the map, by adding geographically contextualized pieces of information (such as indications of where are people in need of care, of their specific need, and of the level of urgency of the desired intervention), each with an indication of the expected AZ. For each message, the choice of the AZ size as well as of the time of validity of the annotation is crucial to the performance of the overall FC scheme. Indeed, too small AZs would result in the annotation getting lost and not reaching the intended receivers, while an AZ which is too large (possibly spanning the whole map) and annotations which never expire would result in a large amount of information to be exchanged between nodes, with consequent waste of energy of the device/smartphone, which is typically scarce, in post-disaster set-ups. In addition, such large contents would easily result into the impossibility of exchanging the whole annotated maps during a contact between two nodes, and hence, into rapid and severe performance degradation of the situational awareness service. How to design a strategy for optimally dimensioning the AZ in such scenario is still an open issue. However, some of the approaches proposed in the literature [2, 3, 37] could be taken as reasonable first-order solutions. Finally, after possibly adding its own contribution to the map, the node would replicate opportunistically the resulting annotated map to all nodes which would come in to its range, according to the AZ of each annotation in the map. We assume that whenever a node receives different versions of the annotated map, it consolidates the annotations, updating each annotation to its latest version and by eliminating contributions which are expired and out of their own AZ of reference (note that the AZ of reference of the whole map is assumed to be the whole map, which we assume to coincide with the disaster area).

As an example, in a scenario of a flooded city, either rescuers or the local population (e.g. people who got isolated in their homes) could start floating a map annotated with the information on where they are located, and on what are their needs. As rescue operations progress, these annotations get updated by rescuers. The final result is the creation of shared data on the status of disaster area, of the affected population and of rescue operations, which could serve as a basis for implementing some form of coordination among rescue teams.

In addition to nodes present in the scenario due to pre-disaster conditions, the FC scheme for situational awareness could be enhanced by the use of static nodes deployed on purpose by rescue teams, or by UAVs. Such additional nodes could help improving the performance of the service in conditions of low density of nodes, or relieve (at least in part) local nodes (such as smartphones, which in a post-disaster set-up have little chances of getting recharged) from the burden of replicating the Floating Content [61].

A key aspect of FC performance is the transmission range of the radio technology used. Indeed, a large transmission range is essential for facilitating content replication and enhancing FC performance. To this end, exploiting opportunistically the combined use of Bluetooth (as in [2]) and Wi-Fi Direct [72] seems to be the best option, as it would allow exploiting the large range of Wi-Fi direct and the energy efficiency of Bluetooth.

11.4.2 Information-Centric Networking and Delay-Tolerant Networking

Delay-tolerant networking (DTN) has been suggested for communication in disaster cases, since it does not require fixed infrastructure and permanent connectivity among network devices. Information-centric networking (ICN) mechanisms have been proposed to be integrated with DTN protocols or to be changed to enable DTN communication with ICN. Content-centric networking (CCN) and named data networking (NDN) [75], which are based on Interest (to request information) and Data messages (to deliver information), have been used to realize DTNs for disaster scenario communication. There are several synergies between the ICN and DTN architectures

[68], since both approaches use in-network storage, late binding of names to locations, long-term data units (ICN data objects, DTN bundles) compared to IP packets and more flexible routing and transport mechanisms, e.g. multi-homing. Tyson et al. [69] argue that ICN could improve connectivity resilience in disaster scenarios because nodes can explore multi-homing in ICN. ICN is completely connectionless and does not suffer from connection breaks. ICN requires no particular underlying network layer as it creates its own ad-hoc network. ICN can support QoS by handling different requests differently. ICN nodes with caches support store, carry and forward mechanisms, which is important in disaster scenarios with temporary connectivity. Content replication, content migration, redundant caching, and proactive caching at strategically well-chosen locations can improve resilience in ICN. In the following, we discuss various related works integrating ICN and DTN in more detail.

Name-based replication priorities (NREP) [54] leverages certain ICN characteristics to support after-disaster communications. Intermediate nodes use the message name to decide whether and with which priority a message should be replicated. The name might have an impact on how long a message should be stored. NREP assumes that the name of an NDN Interest or Data message can give some indication about the type and priority of the requested/delivered content. NREP suggests a hierarchical name space to distinguish different priority levels. As example, Weather/Storm could have a higher priority than Weather/Rain. Each device stores a message in its memory according to their expiration times as long it is in the geographical scope. When two devices are close to each other, they start exchanging messages. Messages with higher weights are exchanged first, messages with lower weights are deleted first in case of limited memory. Weights can be calculated as a linear combination of distance from origin of the message, message lifetime and its priority. Simulation results show the benefits of NREP over FIFO and random replication and forwarding approaches.

Monticelli et al. suggest ICN to support communications in disaster scenarios [45]. NDN's data authenticity and integrity are useful for communication during disaster situations with untrusted mobile-hoc devices. Delay-tolerant ICN for disaster management (DID) targets Interest-based content retrieval between fragmented networks after a disaster. DID aims to support Interest and Data message muling between mobile end systems of people from ambulances, police and other organizations. Data mules are responsible to transport messages between communities. It delivers messages believed to be destined for a community and collects messages from a community for delivery to another community. When a community and a mule meet, the mule transmits its encounter table, so that the community knows which destinations are more likely to be reached by the mule. Based on this information and on the message priority, the community assigns a transmission priority to each outgoing message.

DTN and CCN share some commonalities in their designs [31], but there are also fundamental differences between them. CCN poses some limitations in disruptive network, e.g. if a reverse path based on PIT entries fails for intermittent connections or a next hop may not be available for some time. The CCN strategy layer provides flexibility to operate on top of IP or Layer 2 protocols and it can utilize multiple network technologies, e.g. cellular networks, Wi-Fi, simultaneously through the FIB. Similarly, the DTN Bundle Protocol (BP) enables operation on top of underlying network-specific protocols through a convergence layer. Integrating BP with CCN enhances connectivity options of the strategy layer and CCN can deal with network disruptions through BP. CCNDTN extends CCN forwarding to fragmented networks. The strategy layer dynamically chooses interfaces from FIB entries under changing conditions. Therefore, a CCNDTN router creates a FIB entry pointing to a bundle daemon, once it receives prefix announcement from DTN. Subsequently, the bundle layer provides seamless communication by masking potential discontinuity and long delays of underlying networks.

By targeting named data rather than node endpoints, ICN can support efficient DTN communication enabling requesters to retrieve desired content quickly from any neighbouring device. CEDO [63] extends CCN with DTN functionality. Interests stay in the PIT until they are satisfied. Whenever a contact is detected, a message that summarizes all pending Interests is transmitted. A receiver of such a message sends back all Data messages that it has in the cache. CEDO [63] keeps Interest messages in the PIT until nodes encounter the desired content source. An appropriate number of Interest messages must be sent to request all Data messages of a content object.

DT-ICAN [74] provides bandwidth-efficient network operations to address disruptions in ICN-based networks. DT-ICAN suggests hierarchical naming. It leverages node-based Interest aggregation and epidemic Interest dissemination to overcome network partitions in ICN-based wireless ad-hoc networks. DT-ICAN uses Bloom Filters for searching content. DT-ICAN introduces several new messages compared to NDN. All of them carry Bloom Filter information:

- Node-Interest messages are broadcast periodically to indicate available content objects. Nodes propagate such information.
- Request messages carry identifiers of content objects a node is willing to receive and are broadcast to one-hop neighbours.
- Cache Summary messages—broadcast to one-hop neighbours—indicate availability of cached content.

DT-ICAN uses randomized ordering of requested data transmissions to improve cached chunk diversity in the opportunistic network. Evaluations in vehicular ad-hoc network scenarios indicate that DT-ICAN improves content download performance in terms of success rates and time duration compared to standard ICN mechanisms.

Agent-based content retrieval (ACR) [5] enables information-centric delay-tolerant communication as an application module. The decision when to forward Interests in sparse environments is provided by the application module enabling more flexible application-specific connection criteria. ACR requesters can delegate content retrieval to agent nodes. After receiving a notification from the agent, the requester can regularly retrieve the content from the agent via multiple Interests. ACR uses three phases: agent delegation, content retrieval and content notification.

1. Agent delegation deals with finding an agent and delegating content retrieval to it. The requester broadcasts an Exploration Interest message with the pre-

fix/ferrying, the content name and optional selection parameters, e.g. coordinates where the content may be found, to its one-hop neighbours. If agents have sufficient resources to perform the task and agree with the optional parameters, they reply with Exploration Data appending their nodeID uniquely identifying the agent. Since the Exploration Interest is broadcast, the requester may receive multiple Exploration Data replies from agents in one-hop distance. After a short delegation time the requester can select an agent for delegation. Agent selection can be based on diverse criteria such as social relations or past GPS traces. The requester sends a Delegation Interest to the selected agent using its nodeID, a jobID, an expiration time and optional parameters such as the notification type push or pull. The jobID is used in the notification phase (see below) and the expiration time limits the duration that an agent is looking for the content. Finally, the agent has to confirm the delegation with an acknowledgement (ACK).

2. Content retrieval follows agent delegation. The agent can find and retrieve content for the requester by periodic Interests (Interest probing, e.g. every 1 s). Broadcast requests enable implicit content discovery, i.e. a broadcast request can address multiple nodes at the same time but only a content source, which holds the desired content, will reply. Content retrieval can also be performed via Dynamic Unicast [6], where content requests are transmitted via broadcast only until a content source is found. Then, subsequent Interests are addressed via unicast to the same content source until it becomes unavailable.
3. Content notification is happening after an agent has retrieved the content. An agent can notify the requester via push or pull notifications. The decision which notification type to use is made by the requester during agent delegation. Both notification types assume that agents meet requesters again after a while.

   - As soon as an agent has retrieved the content, it can start the notification phase by periodically transmitting push notifications. Push notifications are Interest messages with the prefix/notify, the jobID and the content version. When the requester receives the push notification, it can start retrieving the content from the agent. As soon as content retrieval has finished, the requester notifies the agent indicating that no more notifications are required.
   - Pull notifications are based on periodic Notification Requests transmitted by requesters followed by Notification Responses transmitted by agents if they have retrieved the content. Agents that have completed content retrieval can register an Interest filter in the jobID to receive Notification Requests, i.e. Interests for the jobID. Then, as soon as an agent comes into the requester's transmission range and receives the Notification Request, it can respond with a Notification Response containing the content version and optionally the nodeID (for direct content retrieval similar to push notifications). After receiving a notification, the requester can retrieve the content from the agent.

Since multiple agents may be delegated with the same jobID for redundancy, a requester can retrieve notifications from any agent in its neighbourhood with one message. Push notifications have a larger size than pull notifications, because they contain all information to retrieve content (e.g. nodeID, content version).

Pull notifications can be short because additional information is only transmitted if requester and agent meet.

11.4.3 Edge Computing Solutions for Post-Disaster Emergency Networks

Edge computing is an architectural approach that brings the computing closer to the user. It is realized by offloading the data and computation to the local server which performs most of the computing requirements and exchanges information with the cloud server.

A typical edge computing solution [26] is presented in Fig. 11.2. IoT devices or end-user devices communicate to the edge devices and edge servers. The performance of end-user devices in the core edge computing concept is based on communications between the layers, assuming that the cloud and edge servers will always exchange information.

However, an emergency network in post-disaster scenario requires that the edge devices will seamlessly continue to perform their essential function autonomously without contacting the cloud server or other nearby systems. The possibility to work independently and autonomously determines the edge computing to become a *dew computing* solution. A dew computing solution can exchange data with other systems when there is network connectivity and synchronize relevant data. This process is identified as a collaboration feature in addition to the independence.

When edge computing solutions offer independent autonomous function, they may be characterized as solutions for post-disaster and emergency networks. In such a case, edge computing devices bring the processing and communication closer to the users in the areas affected by a disaster.

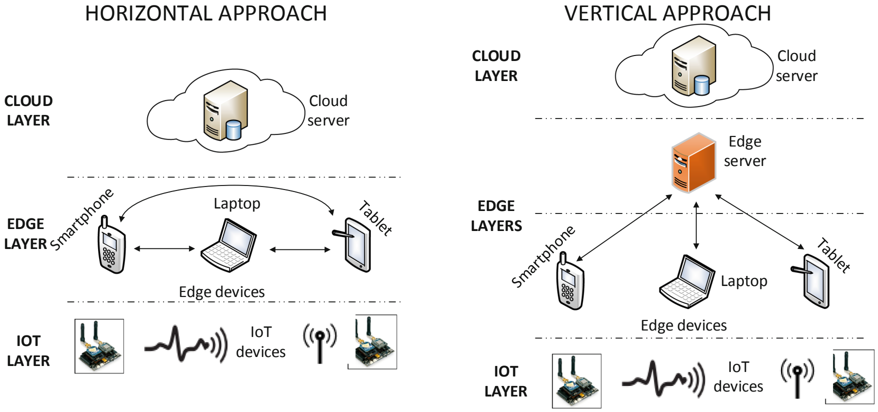

Fig. 11.2 Edge computing approaches for post-disaster IoT eHealth solutions

The edge computing approach may be realized as a solution that uses *horizontal* or *vertical* edge computing communication. The horizontal solution means that several edge devices may communicate as a kind of an ad-hoc network, while the vertical solution means implementation of a master-slave scheme. These communication requirements may work independently of other systems and serve as a solution for post-disaster and emergency networks.

The edge computing solution for post-disaster and emergency network can be realized by one of the following processing concepts:

- a classical edge approach with a smaller master edge server that delivers most of the required services without connecting to the cloud server,
- a serverless solution [48], where all edge devices share information and computing tasks without identified server to deliver the required services.

The classical edge computing approach assumes a vertical offloading scheme, where the first device will be the master, and all other edge devices will act as slaves. The master edge device can be doctor's tablet, and the other edge devices are just intermediate devices to establish the communication with the IoT devices and will still capture signals from nearby sensors, store them and transmit all relevant data to the master device.

The serverless solution does not introduce a master edge device (server), but use horizontal offloading of data between edge devices. Each edge device is performing its own function, and the doctor's tablet, which is still another edge device, collects all information and displays a summary.

As a conclusion, a service provider should configure the operator's infrastructure and solutions to use edge devices implementing the dew concept in order to be resilient to communication failures that might occur in disasters. Implementing the serverless solution will increase resilience, since the edge devices can cooperate in an emergency network. A failover feature is one of the most desirable functions to be incorporated in such a solution, since in case of a lack of power supply then another edge device may continue providing emergency services.

11.4.4 Information Resilience Task Scheduling

We assume the case of a disaster with high impact, on the communication infrastructure. Specifically, we assume that communications with the cloud data center are not available, and that in order to achieve information resilience, all computing must be performed with the available edge devices. We present two *best-effort* approaches in task scheduling: Intra- and inter-edge, described in the following subsections.

11.4.4.1 Intra-Edge Task Scheduling Techniques

As we mentioned earlier, a single edge device can be connected several IoT devices, thereby offering several services simultaneously. This leaves open the issue of how to perform of intra-edge task scheduling.

Solutions: The simplest intra-edge scheduling strategy is FCFS (First Come First Served), in which the edge device will wait the data to be transmitted before starting the computation. However, this method is not optimal when the network is blocked with a large amount of data (file) and the edge devices spend their energy without any computation.

An enhanced version of FCFS consists of a two-staged algorithm to minimize the makespan for task scheduling. The first stage in task offloading is to retrieve the input data and state variables, after which, in the second phase, the task is executed.

Two different approaches are available, depending on whether the tasks are independent or there is some dependency between a pair of tasks. For the former case, Johnson's rule [32] can be applied, while the B&B method [12] for the latter case. Nevertheless, the latter method is not scalable, and therefore, Johnson's rule can be applied in two levels, i.e. to group-dependent tasks and executed as a group sequentially on the same edge device, which will also reduce the inter-task communication. The second stage will be to schedule the grouped jobs in order to minimize the objective function.

11.4.4.2 Inter-Edge Task Scheduling Techniques

An IoT device should select which edge device to send the data to, which is known as the edge-front computation offloading [73]:

- An IoT device can offload the computing to the nearest edge device, which can be denoted as *edge-front*.
- The underlying inter-edge task placement schemes should be agnostic to IoT devices, that is, to use a serverless architecture.
- A mobile IoT or edge device should resort to its own local computing resources in all cases when it is disconnected from any other edge device or even cloud.

Intra-edge task scheduling techniques are useful if the edge device is available (e.g. battery life) or the network has not reached the bottleneck. Therefore, inter-edge task scheduling techniques are necessary in order to balance the computing among the limited set of edge devices [60].

Solutions: We present three different inter-edge task scheduling techniques, as candidates to provide the best performance:

- *Shortest Transmission Time First (STTF)* tries to offload (schedule) tasks on another edge device to which the latency to transfer the task is the shortest. The edge-front device should maintain the estimated latency of transmitting data to each available edge device. Due to the performance uncertainties (mobile devices, different distance, different network bandwidth, etc.), the periodical update of latencies should be performed.

- *Shortest Queue Length First (SQLF)* tends to transfer a task to another edge device whose task queue is the smallest at the time of the decision. This scheduling technique has two steps. When the edge-front device is overloaded (e.g. too many requests or tasks), it should first ask all other edge devices about their task queue length. After achieving information about all task queues, the edge-front device will offload tasks to the edge device whose queue is the shortest.
- *Shortest Scheduling Latency First (SSLF)* predicts which edge device will have the shortest response time, and then, the tasks are offloaded to that edge device. The response time is the time period from offloading a task to another available edge device until the edge-front device receives the result back. Instead of keeping the information about the queue length, the edge-front device will keep the data about the response time.

11.4.5 Middleware Solutions for Emergency Networks

On top of the basic networking solutions and technologies to interconnect the ICT infrastructures of multiple rescue teams deployed in a disaster area, a proper middleware solution is needed so as to provide interoperability among heterogeneous platforms, to orchestrate operational processes and to coordinate the rescue and recovery actions. The core capabilities of this middleware [29] are represented in Fig. 11.3. The first capability is messaging, representing the capability of the middleware to allow data sharing among the interconnected ICT platforms. Multiple possible technologies have been used, starting from service-oriented architectures to queueing solutions for the request/reply (synchronous or even asynchronous) and

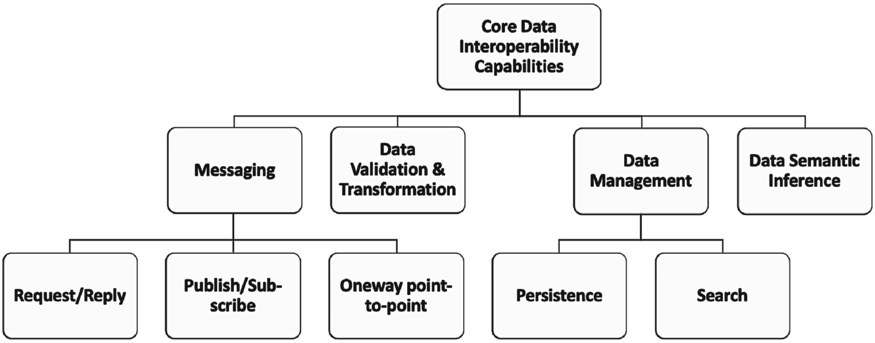

Fig. 11.3 Core capabilities of a middleware for emergency networks

one way point-to-point communications by providing precise API to the offered functionalities of these emergency networks.

A particularly interesting approach is the publish/subscribe paradigm (one-to-many and many-to-many with call-back and pull-style subscriptions) [15], where publishers produce messages to be distributed, subscribers indicate the information they want to receive via a subscription and receive it accordingly, and a middleware abstraction able to provide the communication among the publishers and subscribers. The main strengths of publish/subscribe-based solutions are the possibility to simplify the interconnections among the end points thanks to a mediator-like approach rather than having to establish each possible connection. This enforces the interoperability and flexibility of the approach, thanks also to a dynamic discovery of the end points and strong decoupling guarantees. Examples of the use of publish/subscribe-based messaging solutions for emergency networks can be found in [15, 49, 55].

Another important capability is related to Data Validation and Transformation (DVT), where the first one is the capability to compare the data against a specific scheme while the second one is the process that allows transforming data to/from one representation to/from another. These are particularly demanding for interoperability as each ICT platform may be characterized by a precise data schema to be used when producing data or to interpret the received data. When using binary formats, if the scheme applied to a received message differs from the expected one, the message content cannot be understood. So, data validation is pivotal to check if the received message is comprehensible, and if the check is not passed a suitable transformation is needed. Such an issue can be avoided by using structured data formats [20], such as JSON or XML, so that the received message can be traversed even without known the applied scheme. However, this is paid at the cost of an increased message size, with the consequence of higher latency and workload applied to the network. It is assumed that the network operator should realize all required services for data validation and transformation.

Therefore, binary data formats are still the most adopted ones, and DVTs are suggested within the middleware. The experience of the DESTRIERO project described in [39] designed and implemented a DVT solution based on the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) [43], as the data model for sharing Command and Control (C2) information, properly adapted to the case of the coordination of rescue teams in post-disaster scenarios. The DVT solution was able to check if a given data instance was compliant to such a model and to transform data from one format in another one, passing by an internal object-oriented representation.

Data management is another key aspect of an emergency network so as to offer persistent storage of the collected data. Each of the integrated platforms may have its own local data storage, so that the data related to the disaster can be spread across all the involved organizations. A solution may be to have a centralized storage, possibly hosted within the cloud, that holds replicas of the data for each organization and offers proper search capabilities. However, this can be overwhelming as the volume of data can be extremely large. The most suitable solution is a distributed data storage and a federated search engine, as the one presented in [19], that hide the distributed nature of the data and allows users to search for and retrieve data without being aware of their location but giving the illusion of a centralized storage.

The last capability is the data semantic inference, consisting in the management of the semantic aspects of the exchanged data. Specifically, heterogeneity can occur at the technological, syntactical and semantic manner, where interconnected ICT platforms may adopt different networking and middleware solutions. Technological bridges (such as a network bridge between a wireless and wired networks, or a software bridge between a web service and a CORBA distributed object) allow interconnecting systems with the first level of heterogeneity, while data validation and transformation or the use of structured data formats enforces the syntactical interoperability, allowing systems with different data formats to interoperate and comprehend their mutual messages. However, when transnational organization needs to cooperate it is needed to overcome their semantic heterogeneity, due to the use of different languages. Basically speaking, each organization has its own vocabulary and it is possible to have different interpretations of the same terms within each of these vocabularies or multiple terms with the same meaning. An ontological approach is a viable solution to overcome semantic heterogeneity, and varies attempts within the context of emergency networks have been conducted, such as in [16, 34], with the intent of storing and updating a proper ontology schema and instantiating objects based on the ontology scheme so as to have the required semantic meta-data relative to the data stored within an emergency network. Searchs can be done on these meta-data by submitting semantic predicates expressed in SPARQL Protocol and RDF Query Language (SPARQL), so as to infer the semantic information contained in the ontology and meta-data available within the emergency network.

Emergency networks implement an inter-organizational access to shared information, since it is a feature that allows more comprehensive analysis and better decision making. However, its realization within the context of disaster management in which sensitive data is handled requires suitable mechanisms to control the access to shared data. The open nature of current emergency networks may give data providers the impression that their content is not safe, making them reluctant to be involved. Hence, facilitating trust in controlled access to information published in the emergency networks is of strategic importance. In a collaborative environment, where a set of interlinked data will be shared and consumed by different agents, ensuring that shared data remains secure and only accessible to authorized members is a crucial issue. Security provisioning possesses a twofold challenge, a technological one related to which ICT techniques and methods, mainly coming from the cryptography such as group encryption [56], be put in place to protect data and functionalities from misuse, but a second one has an organization nature. Each domain (organization) administrates its own data and security policies independently, by managing its users and holding its own security policies and models. In a collaborative environment, it normally occurs that a user from a organization A (domain A) wants to access some information from another organization B (domain B). This calls out for a cross-domain authentication, so that the target domain trusts the security attributes and identifies claims obtained from the origin domain. In fact, as the different domains are just responsible of managing their own users, a user from domain A will have to authenticate against its own domain and deliver a security assertion to domain B so that it can now trust the requester. Quite some literature is available on this topic, even applied to emergency networks, based on standards such as Security Assertion MarkUp Language (SAML) or eXtensible Access Control Markup Language (XACML) [15, 65].

11.5 Conclusions

In this chapter, we have analyzed the requirements for a communication network operating in a post-disaster scenario, and we have reviewed a set of approaches for delivering communication services in these settings. The broad diversity of communication requirements, due to the heterogeneity of the services to be supported, and the needs arising from the specific post-disaster conditions, generates a broad spectrum of approaches to post-disaster communications. When making the key design choices for an emergency communication system, this diversity calls for an holistic approach, capable of making the most of several techniques in order to flexibly adapt to a specific set of services and to their requirements, and to the specific conditions in which the communication systems will operate.

From the overview presented in this chapter, a few general considerations can be made, which could be of use in the design of communication systems for post-disaster scenarios.

- *Disaster preparedness is key, but be prepared to do without it.* Almost all the approaches presented require at least a subset of the communication devices on the location of the disaster to be pre-configured to operate according to a given algorithm, once the disaster strikes. In some cases, new devices must be introduced on the disaster location (e.g. by first responders and rescue teams) in order to establish emergency communications. Even if some infrastructure is still available on-site, it is still necessary to assume that such infrastructure can be easily reconfigured and integrated into the new emergency communication system, by adding such flexibility and reconfigurability to the system before the disaster strikes. Ultimately, all approaches require some form of preparatory steps, which in turn require an idea of the nature of the possible disaster, of its consequences and of the needs arising in the post-disaster scenario. However, it is seldom the case that reliable information on these aspects is available. And when it is the case, disasters and their consequences become "planned", usually causing only minor disruptions in the communication infrastructure, such as in the case of hurricanes which periodically strike the US east coast. Hence an ideal feature of an effective post-disaster communication system is to require as little preparedness as possible, while at the same time being rapidly deployable.
- *Voice is not enough.* Traditionally, the issue of post-disaster communication boiled down to re-establish voice communications between the largest number of users on the site of the disaster, and the rest of the world. And this because the main purpose was to empower first responders and rescue teams to communicate among them

and with the coordination services. However, given the increasing pervasiveness of smart devices with communication capabilities (such as personal smartphones, or IoT devices) even in post-disaster settings, the goal of emergency communications has gradually broadened to include data communications, seen as a key enabler of effective and rapid interventions thanks to the possibility of real-time data collection, of remote medical assistance, and of real-time risk assessment for the local population, to mention only a few.

Acknowledgements This chapter is based on work from COST Action CA15127 ("Resilient communication services protecting end-user applications from disaster-based failures—RECODIS") supported by COST (European Cooperation in Science and Technology).

References

1. Alam F, Ofli F, Imran M (2018) A Twitter tale of three hurricanes: Harvey, Irma, and Maria. arXiv preprint:1805.05144
2. Ali S, Rizzo G, Mancuso V, Marsan MA (2015) Persistence and availability of floating content in a campus environment. In: IEEE INFOCOM, pp 2326–2334
3. Ali S, Rizzo G, Marsan MA, Mancuso V (2013) Impact of mobility on the performance of context-aware applications using floating content. In: ICCASA, pp 198–208. Springer, Berlin
4. Ali S, Rizzo G, Rengarajan B, Marsan MA (2013) A simple approximate analysis of floating content for context-aware applications. In: IEEE INFOCOM, pp 21–22
5. Anastasiades C, Schmid T, Weber J, Braun T (2016) Information-centric content retrieval for delay-tolerant networks. Comput Netw 107:194–207
6. Anastasiades C, Weber J, Braun T (2016) Dynamic unicast: information-centric multi-hop routing for mobile ad-hoc networks. Comput Netw 107:208–219
7. Aschenbruck N, Gerhards-Padilla E, Gerharz M, Frank M, Martini P (2007) Modelling mobility in disaster area scenarios. In: MSWiM, pp 4–12
8. Becker SM (2011) Risk communication and radiological/nuclear terrorism: a strategic view. Health Phys 101(5):551–558
9. Bircher E, Braun T (2004) An agent-based architecture for service discovery and negotiation in wireless networks. In: WWIC, pp 295–306. Springer, Berlin
10. Borsetti D, Fiore M, Casetti C, Chiasserini CF (2009) Cooperative support for localized services in VANETs. In: ACM MSWiM, pp 1–10
11. Briante O, Loscrí V, Pace P, Ruggeri G, Zema NR (2015) Comvivor: an evolutionary communication framework based on survivors' devices reuse. Wirel Pers Commun 85:2021–2040
12. Brucker P, Jurisch B, Sievers B (1994) A branch and bound algorithm for the job-shop scheduling problem. Discrete Appl Math 49(1–3):107–127
13. Castro AAV, Serugendo GDM, Konstantas D (2009) Hovering information—self-organizing information that finds its own storage. In: Autonomic Communication, pp 111–145. Springer, Berlin
14. Chipara O, Griswold WG, Plymoth AN, Huang R, Liu F, Johansson P, Rao RR, Chan TC, Buono C (2012) WIISARD: a measurement study of network properties and protocol reliability during an emergency response. In: MobiSys, pp 407–420
15. Cinque M, Cotroneo D, Esposito C, Fiorentino M (2017) Secure crisis information sharing through an interoperability framework among first responders: the SECTOR practical experience. In: IEEE WiMob, pp 316–323
16. Cinque M, Esposito C, Fiorentino M, Carrasco FJP, Matarese F (2015) A collaboration platform for data sharing among heterogeneous relief organizations for disaster management. In: ISCRAM

17. Cojocaru S, Gaindric C, Secrieru I, Puiu S, Popcova O (2016) Multilayered knowledge base for triage task in mass casualty situations. Comput Sci J Mold 24(2):202–212
18. Dikbiyik F, Tornatore M, Mukherjee B (2014) Minimizing the risk from disaster failures in optical backbone networks. J Lightwave Technol 32(18):3175–3183
19. Esposito C, Ciampi M (2013) A hierarchical event-based architecture for the notification of medical document availability. In: IWBBIO, pp 585–592
20. Esposito C, Cotroneo D, Russo S (2010) An investigation on flexible communications in publish/subscribe services. In: SEUS, pp 204–215
21. Fujiwara T, Watanabe T (2005) An ad hoc networking scheme in hybrid networks for emergency communications. Ad Hoc Netw 3:607–620
22. Gamma G (2016) Fake captive portal with an Android phone. URL https://null-byte.wonderhowto.com/how-to/fake-captive-portal-with-android-phone-0167030/
23. George SM, Zhou W, Chenji H, Won M, Lee YO, Pazarloglou A, Stoleru R, Barooah P (2010) DistressNet: a wireless ad hoc and sensor network architecture for situation management in disaster response. IEEE Commun Mag 48(3):128–136
24. Goscien R, Walkowiak K, Klinkowski M, Rak J (2015) Protection in elastic optical networks. IEEE Netw 29(6):88–96
25. Gurman TA, Ellenberger N (2015) Reaching the global community during disasters: findings from a content analysis of the organizational use of Twitter after the 2010 Haiti earthquake. J Health Commun 20(6):687–696
26. Gusev M, Dustdar S (2018) Going back to the roots-the evolution of edge computing, an IoT perspective. IEEE Internet Comput 22(2):5–15
27. Gusev M, Ristov S, Prodan R, Dzanko M, Bilic I (2017) Resilient IoT eHealth solutions in case of disasters. In: RNDM, pp 1–7
28. Houston JB, Hawthorne J, Perreault MF, Park EH, Goldstein Hode M, Halliwell MR, Turner McGowen SE, Davis R, Vaid S, McElderry JA et al (2015) Social media and disasters: a functional framework for social media use in disaster planning, response, and research. Disasters 39(1):1–22
29. Hristidis V, Chen SC, Li T, Luis S, Deng Y (2010) Survey of data management and analysis in disaster situations. J Syst Softw 83(10):1701–1714
30. Hyytiä E, Virtamo J, Lassila P, Kangasharju J, Ott J (2011) When does content float? Characterizing availability of anchored information in opportunistic content sharing. In: IEEE INFOCOM, pp 3123–3131. Shanghai, China
31. Islam HMA, Lukyanenko A, Tarkoma S, Yla-Jaaski A (2015) Towards disruption tolerant ICN. In: IEEE ISCC, pp 212–219
32. Johnson SM (1954) Optimal two-and three-stage production schedules with setup times included. Naval Res Logist (NRL) 1(1):61–68
33. Kangasharju J, Ott J, Karkulahti O (2010) Floating content: Information availability in urban environments. In: IEEE PERCOM Workshops, pp 804–808. IEEE, New York
34. Khazai B, Kunz-Plapp T, Büscher C, Wegner A (2014) VuWiki: an ontology-based semantic wiki for vulnerability assessments. Int J Disaster Risk Sci 5(1):55–73
35. Król M, Ji Y, Yamada S, Borcea C, Zhong L, Takano K (2016) Extending network coverage by using static and mobile relays during natural disasters. In: WAINA, pp 681–686
36. Krug S, Seitz J (2016) Challenges of applying DTN routing protocols in realistic disaster scenarios. In: ICUFN, pp 784–789
37. Manzo G, Marsan MA, Rizzo G (2017) Performance modeling of vehicular floating content in urban settings. In: IEEE ITC 29, vol 1, pp 99–107
38. Manzo G, Soua R, Di Maio A, Engel T, Palattella MR, Rizzo G (2017) Coordination mechanisms for floating content in realistic vehicular scenarios. In: IEEE MobiWorld
39. Matarese F, Di Crescenzo D, Strano A, Aligne F, Mattioli J (2012) An interoperable reconstruction and recovery decision support tool for complex crises situations. In: IEEE SoSE, pp 525–530
40. Medford-Davis LN, Kapur GB (2014) Preparing for effective communications during disasters: lessons from a World Health Organization quality improvement project. Int J Emerg Med 7(15):1–7

41. Minh QT, Nguyen K, Borcea C, Yamada S (2014) On-the-fly establishment of multihop wireless access networks for disaster recovery. IEEE Commun Mag 52:60–66
42. Minh QT, Shibata Y, Borcea C, Yamada S (2016) On-site configuration of disaster recovery access networks made easy. Ad Hoc Netw 40:46–60
43. MIP: The joint c3 information exchange data model metamodel (jc3iedm metamodel), jc3iedm-metamodel-specification-3.1.4.pdf. https://public.mip-interop.org/. Accessed on 25/02/2019
44. Molinari D, Menoni S, Aronica G, Ballio F, Berni N, Pandolfo C, Stelluti M, Minucci G (2014) Ex post damage assessment: an Italian experience. Nat Hazards Earth Syst Sci 14(4):901–916
45. Monticelli E, Schubert BM, Arumaithurai M, Fu X, Ramakrishnan KK (2014) An information centric approach for communications in disaster situations. In: IEEE LANMAN, pp 1–6. https://doi.org/10.1109/LANMAN.2014.7028630
46. Morreale P, Goncalves A, Silva C (2015) Mobile ad hoc network communication for disaster recovery. Int J Space-Based Situated Comput 5(3):178–186. https://doi.org/10.1504/IJSSC.2015.070949. URL https://doi.org/10.1504/IJSSC.2015.070949
47. Narayanan RGL, Ibe OC (2012) A joint network for disaster recovery and search and rescue operations. Comput Netw 56:3347–3373
48. Nastic S, Rausch T, Scekic O, Dustdar S, Gusev M, Koteska B, Kostoska M, Jakimovski B, Ristov S, Prodan R (2017) A serverless real-time data analytics platform for edge computing. IEEE Internet Comput 21(4):64–71. https://doi.org/10.1109/MIC.2017.2911430
49. Ordille JJ, Tendick P, Yang Q (2009) Publish-subscribe services for urgent and emergency response. In: ACM Comsware, pp 8:1–8:10
50. Ott J, Hyytiä E, Lassila P, Vaegs T, Kangasharju J (2011) Floating content: information sharing in urban areas. In: IEEE PerCom, Seattle, USA, pp 136–146
51. Pawelczak P, Prasad RV, Xia L, Niemegeers IG (2005) Cognitive radio emergency networks-requirements and design. In: IEEE DySPAN, pp 601–606
52. Perko T (2011) Importance of risk communication during and after a nuclear accident. Integr Environ Assess Manag 7(3):388–392
53. Petersen H, Baccelli E, Wählisch M, Schmidt TC, Schiller J (2014) The role of the Internet of Things in network resilience. In: International Internet of Things Summit, pp 283–296. Springer, Berlin
54. Psaras I, Saino L, Arumaithurai M, Ramakrishnan KK, Pavlou G (2014) Name-based replication priorities in disaster cases. In: 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp 434–439. https://doi.org/10.1109/INFCOMW.2014.6849271
55. Radianti J, Gonzalez JJ, Granmo OC (2014) Publish-subscribe smartphone sensing platform for the acute phase of a disaster: a framework for emergency management support. In: IEEE PerCom Workshops, pp 285–290
56. Rafaeli S, Hutchison D (2003) A survey of key management for secure group communication. ACM Comput Surv (CSUR) 35(3):309–329
57. Rak J (2015) Resilient routing in communication networks. Springer, Berlin
58. Rak J, Hutchison D, Calle E, Gomes T, Gunkel M, Smith P, Tapolcai J, Verbrugge S, Wosinska L (2016) RECODIS: resilient communication services protecting end-user applications from disaster-based failures. In: ICTON, pp 1–4
59. Ray NK, Turuk AK (2017) A framework for post-disaster communication using wireless ad hoc networks. Integrat VLSI J 58:274–285
60. Ristov S, Cvetkov K, Gusev M (2016) Implementation of a horizontal scalable balancer for dew computing services. Scalable Comput Pract Exp 17(2):79–90
61. Rizzo G, Neukirchen H (2017) Geo-based content sharing for disaster relief applications. In: IMIS, pp 894–903. Springer, Berlin
62. Rubin GJ, Amlôt R, Page L (2011) The London polonium incident: lessons in risk communications. Health Phys 101(5):545–550
63. Neves dos Santos F, Ertl B, Barakat C, Spyropoulos T, Turletti T (2013) CEDO: content-centric dissemination algorithm for delay-tolerant networks. In: MSWiM, pp 377–386. ACM

64. Sellnow TL, Sellnow DD, Lane DR, Littlefield RS (2012) The value of instructional communication in crisis situations: restoring order to chaos. Risk Anal Int J 32(4):633–643
65. Sicuranza M, Ciampi M, Pietro GD, Esposito C (2013) Secure healthcare data sharing among federated health information systems. IJCCBS 4(4):349–373. https://doi.org/10.1504/IJCCBS.2013.059023
66. Sugerman DE, Keir JM, Dee DL, Lipman H, Waterman SH, Ginsberg M, Fishbein DB (2012) Emergency health risk communication during the 2007 San Diego wildfires: comprehension, compliance, and recall. J Health Commun 17(6):698–712
67. Thompson N, Crepaldi R, Kravets R (2010) Locus: a location-based data overlay for disruption-tolerant networks. In: CHANTS, pp 47–54. ACM
68. Tyson G, Bigham J, Bodanese E (2013) Towards an information-centric delay-tolerant network. In: 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp 387–392. https://doi.org/10.1109/INFCOMW.2013.6970723
69. Tyson G, Bodanese E, Bigham J, Mauthe A (2014) Beyond content delivery: can ICNs help emergency scenarios? IEEE Netw 28(3):44–49. https://doi.org/10.1109/MNET.2014.6843231
70. Velev D, Zlateva P (2012) Use of social media in natural disaster management. In: International Proceedings of Economic Development and Research, vol 39, pp 41–45
71. Wang J, Wu Y, Yen N, Guo S, Cheng Z (2016) Big data analytics for emergency communication networks: a survey. IEEE Commun Surv Tutor 18(3):1758–1778. https://doi.org/10.1109/COMST.2016.2540004
72. Wi-Fi Alliance: Wi-Fi peer-to-peer (P2P) technical specification
73. Yi S, Hao Z, Zhang Q, Zhang Q, Shi W, Li Q (2017) Lavea: latency-aware video analytics on edge computing platform. In: IEEE ICDCS, pp 2573–2574
74. Yu Y, Joy J, Fan R, Lu Y, Gerla M, Sanadidi MY (2014) DT-ICAN: a disruption-tolerant information-centric ad-hoc network. In: IEEE Military Communications Conference, pp 1021–1026
75. Zhang L, Afanasyev A, Burke J, Jacobson V, Claffy K, Crowley P, Papadopoulos C, Wang L, Zhang B (2014) Named data networking. In: SIGCOMM, vol 44, pp 66–73. ACM