Design of a Backup Network for Catastrophe Scenarios

Position Paper

S. Alves
Portugal

B. Koldehofe
IPVS Stuttgart, Germany

H. Miranda
University of Lisbon, Portugal

F. Taiani
University of Lancaster, UK

ABSTRACT

Communication networks play a fundamental role in the response to a massive catastrophe, like an earthquake or a large-scale terrorist attack to a major urban area. In such situations, command centres must be able to rely on a fully operational communication network, for example to learn about on-going situations and allocate and guide the rescue teams. Communication is bidirectional: once in the field, these teams will feed the command centre with a more accurate view of the situation, contributing to the efficient allocation of the resources. Failures in this network, even if localised to some of the regions affected by the catastrophe, can have costs both monetary and in human lives.

In this position paper, we propose the creation of a redundant, best-effort, emergency communication network that could serve to mitigate localised failures using off-the-shelf widespread technology. We give an overview of an architecture for a backup network, highlight the possible advantage of such an architecture to disaster management and discuss challenges that need to be overcome in realising it.

Categories and Subject Descriptors

C.2.5 [**Local and Wide-Area Networks**]: Internet; C.2.2 [**Network Protocols**]: Protocol architecture

1. INTRODUCTION

In large urban areas, catastrophes like earthquakes, fires or massive terrorist attacks are more subject to acquire large proportion in both human and infra-structural costs. After such an event, public authorities are expected, among others, to locate and rescue the victims; preserve or restore public order and identify locations where threats persist or are imminent. Disaster management is usually delegated to a central authority which coordinates all the teams deployed within the catastrophe area.

In such a scenario, a reliable communication infrastructure is fundamental to perform an optimal allocation of the available resources. To be effective, coordination must be able to rely on communication mechanisms that allow management teams to: *i*) learn about the occurrence of new events as they unfold; *ii*) continuously gather feedback from the personnel on the ground; and *iii*) deliver orders or updates.

In an effort to ensure optimal communication, military and civil defence forces of most countries reserve part of the wireless radio spectrum for their networks and have a private wireless communication infrastructure deployed. A lot of research effort has been spend on setting up such specialised networks we refer to as *rescue networks* (e.g. [5, 13, 24, 11, 2]). While rescue networks already consider to support (ad-hoc) communication over heterogeneous devices and networks, they typically neglect interactions with devices provided by civilians in order to ensure best service performance for the rescue teams. However, the early deployment of the rescue teams will be mostly dictated by the events learnt by the coordination authority from the alerts provided by civilians. At this stage, the *civil network*, composed of the wired and wireless network infrastructure operated by telecommunication companies, will play a fundamental role, given that civilians do not have access to the rescue network.

The infrastructure supporting civil and rescue networks should be considered as vulnerable to the catastrophe as any other infrastructure. Falling antennas or interference from malfunction devices can disrupt communication in some regions. Disruption will especially affect the infrastructure of civil networks, which is not designed to be as resilient as rescue networks.[1] However, one should not exclude the possibility of disruptions on the rescue network. Besides damages on constructions and on the hardware, terrorists could include the rescue network infrastructure in their preferential targets to maximise the cost, in lives, of an attack.

In this paper, we discuss the construction of a *Backup Network* to help mitigate the adverse impact of failures in both the civil and rescue networks. The goal is to provide coverage in locations where Rescue and/or Civil Networks have been affected. The network is composed by off-the-shelf equipment commercially available and puts together a number of technologies that have recently gained attention. Components of this network are made available by civilians and rescue teams, in response to the occurrence of the catastrophe. The network provides a best effort service, under the perspective that some connectivity would be better than none. In the line of what has been proposed for ad-hoc

[1]Note for example that, in large urban areas, is standard practise to install antennas of mobile operators on top of residential buildings.

IWCMC'09, June 21–24, 2009, Leipzig, Germany.

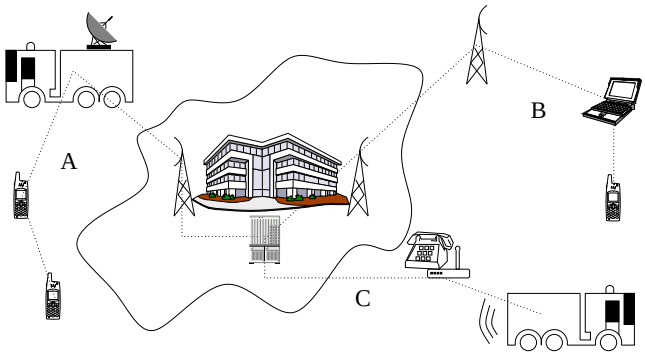

Figure 1: Application examples of the Backup Network

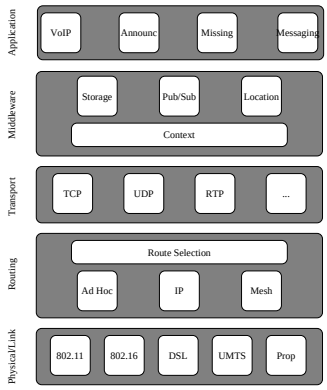

Figure 2: Components of the Backup Network

networks, our network is self-manageable and therefore does not represent an additional burden to the participants.

The contributions of a backup network would be two-fold: *i*) emergency personnel would benefit of an extended coverage, improving the quality and amount of data provided and received from the command centre; and *ii*) civilians would have an additional mechanism to make emergency calls.

2. OVERVIEW

The Backup Network we propose is formed by heterogeneous devices, the majority of them made available by civilians. Examples are smart phones, PDA's, laptops and domestic or institutional WiFi access points (e.g. located at public schools or universities). Rescue teams contribute with their own personal communication equipment and with mobile base stations, integrated in emergency vehicles. Private operators contribute by making their infrastructure available, possibly relaxing access constraints.

In our architecture, this myriad of devices and technologies is integrated in a coherent data network by specialised software, made publicly available in advance, for example at the web site of the national civil protection authority. The software remains deactivated by default and is manually activated by the users in response to the catastrophe.

The network leverages on well-known protocols for ad-hoc, mesh, delay tolerant and wired networks. Devices cooperatively learn the routes available between the command centre and the participants. These routes may traverse different networking technologies. Therefore, devices simultaneously accessing multiple networks are required to act as gateways.

Routes are selected according to the available quality of service. In the general case, the goal of the nodes in the Backup Network is to deliver packets to the more "stable" parts of the network, that is, to the locations where either the civil or rescue networks are operational.

Figure 1 illustrates 3 examples of operation of the Backup Network. Case *A* illustrates the establishment of a voice call using a smart phone. Since the civil network infrastructure of the region was affected, communication is mediated by another smart phone and a mobile base station that connects to the Rescue Network. Mediation also takes place for the establishment of the call in case *B*. However, in this case the connection uses the civil network. Finally, case *C* depicts an example where, due to the local failure of the rescue network, a passing by rescue vehicle communicates its current location using an access point in the neighbourhood. In our idealised network, a myriad of other combinations of the different medias involved is possible.

Although most of the hardware required to achieve such a generic and transparent network is already in place, the deployment of the network poses a number of challenges that have still to be resolved and which are the focus of the following section.

3. CHALLENGES

The Backup Network leverages on a number of well-known and established networking technologies. However, most of these technologies have so far been developed and used separately. Therefore, we anticipate that the main challenges will arise from their integration. To facilitate this integration, we propose to rely on the overall architecture of the network depicted in Figure 2.

The architecture is divided in five layers, with most of them mirroring the standard TCP/IP protocol composition stack. In brief, each layer will be composed of multiple protocols and software to provide their integration. In most of the devices, only a subset of these protocols, those relevant for the network technologies supported, will be implemented. The most significant challenges are expected to appear at the routing and middleware layers as these encapsulate the key functionality of the various networking technologies to be integrated.

In the following subsections, we discuss the challenges posed to each layer and outline the principal components that are envisioned to resolve them.

3.1 Physical and Link Layer

To be useful, the Backup Network must support a number of physical and link layer protocols. Wireless protocols include IEEE 802.11 (WiFi), IEEE 802.16 (WiMAX), GSM/GPRS, UMTS and possibly some proprietary protocol used on the rescue network. The network is also expected to access wired protocols like DSL and Ethernet. To facilitate, the location of the resources available to the network, participants must agree on a unique, link layer independent, network ID.

Because of the extraordinary circumstances we are considering, we expect that limitations of associations between devices and infra-structured networks to be alleviated. In the case of WiFi networks, this includes the dismiss of any secu-

rity mechanisms. In mobile telephones, telecommunication companies are expected to temporary drop the restrictions of use of clients from other operators or from those with their service suspended. Section 3.5 discusses some measures to prevent abuses of the Backup Network.

It is common to use any of these wireless protocols for data delivery. The challenge resides in their integration. Link layer bridging is expected to be performed by any device with two or more network interfaces, namely, access points, base stations and smart phones. The later are expected to present a significant challenge because the multiple interfaces provided by smart phones are aimed to serve exclusively as alternative communication points for applications. Most likely, the design of smart phones will not consider problems like concurrent packet reception.

3.2 Network Layer

The role of the network layer is to drive data packets to the destination. In the Backup Network, a number of unique challenges are posed to this layer.

Addressing. The unstructured model of the Backup Network conflicts with the structured IP addressing scheme. However, the infra-structured components of the Backup Network are likely to use the ubiquitous Internet protocols. Therefore, the Backup Network must provide to all participants some schema permitting to acquire IP addresses. Recent research results propose to delegate on the gateways between the infra-structured and the ad-hoc components of the network the role of DHCP servers [17, 14]. The solution is not straightforward and two problems must be resolved: *i*) confirming the uniqueness of IP addresses consumes a non-negligible amount of resources and; *ii*) depending on the available connectivity and node movement, mobile nodes may become associated to the infrastructure on different points, possibly changing their addresses. On federations of access points (e.g. on an operational rescue network) this problem is trivially solved using hand off protocols like HAWAII [20]. At the Internet scale, Mobile IP [18] Home Agents can be used to keep the mapping of each device on its current (foreign) IP address. However, Mobile IP is designed assuming that devices have a Home Network. To provide to devices participating in the Backup Network a similar functionality, it would be necessary to define a default Home Network and a corresponding Home Agent. This can raise scalability problems due to the expectantly large number of devices that would try to associate to this network.

Routing Metrics. The majority of routing protocols, for both wired [16] and wireless [12, 19] networks, select the route with the lowest number of intermediary hops between the source and the destination. In homogeneous networks, the number of intermediary hops is roughly proportional to the packet delay.

In the Backup Network, the preferable route may not be the one with a lower number of intermediary hops. Instead, the routing protocol should privilege those routes that tend to be more stable and are less congested. In general, these should be routes traversing infra-structured networks. However, to reach the infrastructure, packets may have to be driven by ad-hoc networks. That is, routing is likely to require vertical and horizontal hand offs. The definition of novel metrics, weighting the particularities of each network type is therefore a critical enabler of the Backup Network this paper advocates.

Packet Prioritisation. The bandwidth differences in the networks traversed by packets in transit is likely to produce traffic accumulation at the nodes. The Backup Network must provide the means to prioritise traffic. The contribution of priorities is two-fold: *i*) they allow the network to privilege traffic produced or directed to rescue teams; and *ii*) they assure the rescue network is used for the purpose it was initially designed for so that other traffic, produced by civilians, does not interfere with rescue operations.

Packet Tagging. Route selection can also be influenced by the type of data carried in packets. The Backup Network should therefore provide a packet-level tagging mechanism that includes potential Quality of Service attributes. For example, a Voice Over IP (VoIP) conversation should not not be forwarded over a network that is subject to large latencies like a Delay Tolerant Network. On the other hand, batch application messages, like updates to the location of the emergency vehicles can suffer some delay and jitter without severely affecting the service they support.

Network Status. Collecting all the information that will assist route selection is challenging, given that one must consider functional and non-functional requirements and that most of this information can not be inferred locally by each device. Instead, devices must agree on a protocol to construct an up-to-date distributed view of the network and the devices it contains.

An accurate view of the Backup Network status allows, for example, to identify working connection points with Civilian and Rescue Networks. Such a separation can be used to limit the use of the Rescue Network by civilians exclusively as a last resort; to avoid routes traversing congested regions or to avoid mobile devices with low battery.

3.3 Middleware Layer

One of the objectives of the middleware layer is to provide services that hide from the application the complexity of the underlying network. This objective gains relevance in the highly heterogeneous environment of the Backup Network. As a minimal set, the Backup Network should provide the following middleware services:

Distributed Data Storage. The exchange of data plays a key role in the kind of backup network we envisage. For instance the command centre will need to disseminate to rescue teams guidelines, maps, reports of the most critical situations, alerts for missing persons, etc. Reciprocally rescue teams will need to produce regular updates regarding the situation they are facing, possibly in the form of annotation of shared digital documents, such as maps, or by updating the system's collective view of the situation (e.g. by removing a person from the list of missing persons when this person is found).

To support this kind of collaborative interactions, the middleware of the Backup Network should provide a distributed storage that is accessible to both producers and consumers of data. This data management service should also be replicated, to improve its accessibility even in periods and areas with limited connectivity. It should also tolerate a high rate of ongoing failures, as these are bound to be present in a major catastrophe scenario.

Publish/Subscribe Service. In a catastrophe situation, many of the messages produced will have a destination that is not fully specified. Instead, the destination of a message can be specified by some (possibly not formal) class of par-

ticipant in the rescue missions such as ambulance drivers or members of rescue teams in proximity of some location. If a communication media providing this class of addresses was available, it would serve nicely queries to the closest ambulance available, or to advertise the locations with explosion danger due to gas leaks.

The properties of a publish/subscribe service (cf. [1, 3, 6]) fit nicely in this communication model, with users subscribing to all the topics or attributes they find relevant. An important aspect is that in publish/subscribe, producers are decoupled from subscribers. This contributes to reduce the application programing complexity and copes well with the communication model of the network expected to present frequent disconnections and changes in the topology.

Context Service. Applications designed for the Backup Network will be required to cope with intermittent connectivity and high variations of bandwidth, latency and jitter. In addition, applications will be developed for a high number of brands of mobile devices and it should be impractical to configure each brand and model individually. The context service facilitates applications self-adaptation by gathering, summarising and interpreting context information.

Location Service. Accurate location is fundamental for an efficient management of the resources and for the rapid localisation of the events. However, it should not be expected that all participating devices are equipped with GPS receivers. The role of this service is to allow any device to retrieve its location with a reasonable accuracy. This service will not represent any burden to the infrastructure. Devices not equipped with GPS receivers can estimate their location from the information provided by nodes in the neighbourhood.

Implementing the above services in the context of a major catastrophe is particularly difficult. As mentioned above, the middleware will have to face extreme levels of heterogeneity, in terms of devices, bandwidth, connectivity, robustness. Our general philosophy consists in relying on decentralised schemes to reduce the load at the command centre and to alleviate the traffic on the infrastructure. In particular, epidemic protocols (e.g. [4, 10, 8, 23]), and middleware based on them [15] seem particularly promising to provide both a high level of resilience, and the kind of self-organisation required in an adverse and unpredictable environment. Key challenges will be to trade-off between conflicting requirements, and understand how to use epidemic protocols as a gluing technology between heterogeneous and possibly damaged underlying infrastructure (WiFi, GSM, dedicated civil and military networks, etc.).

In terms of architecture, the Backup Network can be perceived to be a *system of systems* (or a network of networks) [22]. In this context existing middleware architectures such as Ambient Networks [25], Open Overlays [7] or SpoVNet [26], seem particularly promising to support the integration of the heterogeneous systems. The challenge again will consist of adapting these approaches to the particular requirements of a Backup Network, and provide a close integration at the middleware level between QoS, robustness, and scalability under adverse and unpredictable conditions.

3.4 Applications

The primary role of the Backup Network is to provide an alternative communication channel between rescue teams and the command centre. However, the availability of this communication channel makes room for a number of additional applications that can contribute to rapidly mitigate the adverse effects of the catastrophe. In particular, the Backup Network opens a bidirectional communication channel between authorities and the public. In addition to emergency calls, it can also be used to make public announcements that contribute to preserve public order.

If conditions permit it, the network could be used for the establishment of bidirectional communication channels between civilians. Depending of the quality of service available, the application could establish voice communication, chats or off-line messaging. The distributed data storage middleware can be used for a missing persons location service.

Preventing data overload at the command centre is a challenge. According to newspaper reports[21, 9], in a recent large scale simulation of an earthquake in the Lisbon urban area, communication was identified as a major bottleneck that limited the operational capacity of the rescue teams and hospitals. The simulation was mostly driven by the civil protection authorities and should have not considered the immense number of calls to emergency numbers that would have occurred in a real situation. Large scale message tagging, detection of duplicates and appropriate filtering and routing are fundamental criteria for a successful management of a crisis situation. A first level of filtering could be applied on applications deployed upstream of the command centre, for example in rescue vehicles, thus reducing message flow up to the command centre.

In complement, a data concentration application at the command centre would refine event filtering and tagging, ensuring a scalable and manageable flow of information.

3.5 Security and Privacy Considerations

Deployment of this communication media would be mostly performed in advance of the catastrophe using trusted web sites allowing users to download and install the required applications and middleware. Due to privacy and security issues, users are invited to activate the application only upon the occurrence of the catastrophe. Therefore, the impact of the application would be restricted to the memory consumed on the devices. Because the application is not operational, no privacy concerns are raised. In operation, preventing devices from leaking personal information requires the consumption of additional resources of the devices, which would be undesirable. However, we expect users to relax their privacy concerns in the aftermath of a catastrophe.

Due to its open nature, the Backup Network is vulnerable to intentional and unintentional attacks. An interesting aspect of this model is that problems can be contained in each ad-hoc component of the network by requesting gateways to filter the traffic forwarded to the infrastructure component. Gateways can for example, drop traffic not addressed to the command centre (thus prohibiting calls between civilians) or impose a limit on the number of packets forwarded to the command centre, contributing to the mitigation of a potential DDoS attack.

4. CONCLUSIONS AND FUTURE WORK

Reliable and pervasive communications play a fundamental role in the coordination of the rescue efforts after a major catastrophe. Unfortunately, in large scale events, one cannot assume the complete resilience of the infrastructure. This position paper outlines the challenges that must be ad-

dressed for the establishment of a backup network, aiming to mitigate localised failures in the infrastructure. The network is created by the off-the-shelf networking equipment that is now ubiquitous in any European city. Examples are smart phones, laptops and access points. These devices cooperate to establish the first hop of a network providing access to the infrastructure that survived the catastrophe. The primary goal of this network is to mitigate failures in communication of rescue teams. However, a number of additional applications, possibly used by civilians, can also be considered.

In the near future, the authors plan to investigate these challenges in detail and perform small scale localised experiments of integration of the myriad of technologies involved.

5. REFERENCES

[1] R. Baldoni, R. Beraldi, G. Cugola, M. Migliavacca, and L. Querzoni. Structure-less content-based routing in mobile ad hoc networks. In *Int'l Conf. on Pervasive Services (ICPS'05)*, pages 37–46, 2005.

[2] P. Costa, G. Coulson, C. Mascolo, G. Picco, and S. Zachariadis. The RUNES middleware: a reconfigurable component-based approach to networked embedded systems. In *16th Int'l Symp. on Personal, Indoor and Mobile Radio Comm. (PIMRC 2005)*, volume 2, pages 806–810, 2005.

[3] G. Cugola, E. D. Nitto, and A. Fuggetta. The JEDI event-based infrastructure and its application to the development of the OPSS WFMS. *Trans. on Software Engineering*, 27(9):827–850, 2001.

[4] A. Demers, D. Greene, C. Hauser, and et al. Epidemic algorithms for replicated database maintenance. In *Symp. on Principles of Distributed Computing*, 1987.

[5] O. Drugan, T. Plagemann, and E. Munthe-Kaas. Resource aware middleware services over manets. In *25th Int'l Conf. on Computer Comm. (INFOCOM 2006)*, pages 1–2, 2006.

[6] P. Eugster, P. Felber, R. Guerraoui, and A.-M. Kermarrec. The many faces of publish/subscribe. *Computing Surveys (CSUR)*, 35(2):114–131, 2003.

[7] P. Grace, D. Hughes, B. Porter, G. Blair, G. Coulson, and F. Taiani. Experiences with open overlays: a middleware approach to network heterogeneity. In *3rd SIGOPS/EuroSys European Conference on Computer Systems (Eurosys '08)*, pages 123–136, 2008.

[8] Z. Haas, J. Halpern, and L. Li. Gossip-based ad-hoc routing. In *Trans. on Networking*, 2006.

[9] IOL Diário. Simulacro de sismo revelou "fragilidades" nos meios. http://diario.iol.pt/sociedade/sismo-simulacro-proteccao-civil-lisboa/1016368-4071.html, Nov. 23 2008. In portuguese.

[10] M. Jelasity and O. Babaoglu. T-man: Gossip-based overlay topology management. In *Engineering Self-Organising Systems*, 2005.

[11] X. Jiang, N. Chen, J. Hong, K. Wang, L. Takayama, and J. A. L. Siren: Context-aware computing for firefighting. In *2nd Int'l Conf. on Pervasive Computing (Pervasive 2004)*, volume 3001 of *Lecture Notes in Computer Science*, pages 87–105, 2004.

[12] D. Johnson, D. Maltz, and J. Broch. *Ad Hoc Networking*, chapter DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, pages 139–172. Addison-Wesley, 2001.

[13] K. Kanchanasut, A. Tunpan, M. Awal, D. Das, T. Wongsaardsakul, and Y. Tsuchimoto. DUMBONET: a multimedia communication system for collaborative emergency response operations in disaster-affected areas. *Int'l Journal of Emergency Management*, 4(4):670–681, 2007.

[14] S.-C. Kim and J.-M. Chung. Message complexity analysis of mobile ad hoc network address autoconfiguration protocols. *Trans. on Mobile Computing*, 7(3):358–371, 2008.

[15] S. Lin, F. Taïani, and G. Blair. Facilitating gossip programming with the gossipkit framework. In *8th IFIP Conf. on Distributed Applications and Interoperable Systems*, 2008.

[16] G. Malkin. RIP version 2. RFC 2453, IETF, 1998.

[17] A. Misra, S. Das, A. Mcauley, and S. Das. Autoconfiguration, registration and mobility management for pervasive computing. *Personal Communications Systems Magazine*, 8:24–31, Aug. 2001.

[18] C. Perkins. IP mobility support for IPv4. RFC 3344, IETF, 2002.

[19] C. Perkins and E. Royer. Ad-hoc on-demand distance vector routing. In *2nd IEEE Workshop on Mobile Computing Systems and Applications*, pages 90–100, 1999.

[20] R. Ramjee, T. L. Porta, S. Thuel, K. Varadhan, and S. Wang. HAWAII: A domain-based approach for supporting mobility in wide-area wireless networks. In *7th Int'l Conf. on Network Protocols*, pages 283–292, 1999.

[21] RTP. Sismo/simulacro: Dificuldades nas comunicações encontradas no início do exercício já foram ultrapassadas. http://ww1.rtp.pt/noticias/index.php?-article=374301&visual=26&tema=1, Nov. 21 2008. In portuguese.

[22] A. Sage and C. Cuppan. On the systems engineering and management of systems of systems and federations of systems. *Information, Knowledge, Systems Management*, 2(4):325–345, 2001.

[23] Y. Sasson, D. Cavin, and A. Schiper. Probabilistic broadcast for flooding in wireless mobile adhoc networks. *Wireless Comm. and Networking*, 2003.

[24] Y. Shibata and K. Takahata. Performance evaluation of large scale disaster information network. In *Int'l Conf. on Parallel Processing Works. (ICPPW'07)*, page 7, 2007.

[25] M. Stiemerling et al. System Design of SATO and ASI. Deliverable D12-F.1, Ambient Networks Project, 2006.

[26] W. Waldhorst, C. Blankenhorn, D. Haage, R. Holz, G. Koch, B. Koldehofe, F. Lampi, C. Mayer, and S. Mies. Spontaneous virtual networks: On the road towards the internet's next generation. *it- Information Technology*, Dec. 2008.