Emerging Information Infrastructures: Cooperation in Disasters*

Mikael Asplund[1], Simin Nadjm-Tehrani[1], and Johan Sigholm[2]

[1] Department of Computer and Information Science, Linköping University
SE-581 83 Linköping, Sweden
{mikas,simin}@ida.liu.se
[2] Swedish National Defence College
Drottning Kristinas väg 37, SE-115 93 Stockholm, Sweden
johan.sigholm@fhs.se

Abstract. Disasters are characterised by their devastating effect on human lives and the society's ability to function. Unfortunately, rescue operations and the possibility to re-establish a working society after such events is often hampered by the lack of functioning communication infrastructures. This paper describes the challenges ahead in creating new communication networks to support post-disaster operations, and sets them in the context of the current issues in protection of critical infrastructures. The analysis reveals that while there are some common concerns there are also fundamental differences. The paper serves as an overview of some promising research directions and pointers to existing works in these areas.

1 Introduction

Reliable and secure communication is at the heart of well being and delivery of critical services in today's society, making power grids, financial services, transportation, government and defence highly dependent on ICT networks. Unfortunately, the complexity and interdependencies of these systems make them vulnerable to faults, attacks and accidents. One adverse condition may have unforeseen consequences in other dependent networks (electricity networks dependence on communication protocols, leading to blackouts as opposed to local outages).

Even worse, when a major disaster strikes, such as the Hurricane Katrina or the tsunami in east Asia, large parts of the critical infrastructure can be completely incapacitated for weeks. In those situations we need to re-establish infrastructures to support rescue operations and the transition back to a normal state.

For a timely delivery of critical services to citizens and decision makers, two types of competences are therefore needed: (1) protecting existing infrastructures so that we can continue to enjoy the delivery of reliable services despite the increasing threat picture (locally and globally), (2) moving forward to study the issue of reliability and security in new networked infrastructures that represent a new paradigm in service delivery.

* This work was supported by the Swedish Civil Contingencies Agency and the second author was partially supported by the University of Luxembourg.

R. Setola and S. Geretshuber (Eds.): CRITIS 2008, LNCS 5508, pp. 258–270, 2009.

The main character of these new networks are the loosely connected nature, in some cases combined with mobility, and generally with several actors as opposed to a single owner/administrator. One example of such an "infrastructure-less" network is described by the notion of *hastily formed networks* built-up in response to disasters.

Establishing effective communication in presence of adverse events and outages requires a combination of human processes and technical development. Traditional critical infrastructures need the integration of cultural, economic, and technical analyses (security should not be considered as a cost but as an asset ensuring service continuity). Spontaneous networks require dealing with challenges of enforcing security without a central authority, in addition to novel technical solutions that provide a basis for a *conversation space* [13] from heterogeneous subnets.

The goal of this paper is to describe some of the challenges ahead in emerging critical information infrastructures. These have to be handled when considering the migration path from today's critical information infrastructures into the emerging ones. To make the challenges explicit, we use the case of infrastructures in post-disaster operation to highlight the technical issues. If we can solve the problems in this setting, we can also do it in the pre-disaster state of the convergent networks. This requires a new way of thinking about how reliable and timely message delivery can be accomplished in challenged environments. That is, without strong assumptions regarding organisations, technical equipment, or system knowledge.

The paper consists of two main parts. The first part (Section 2) deals with existing critical information infrastructures, and the second part (Section 3) with spontaneous post-disaster networks. Each part describes some of the main characteristics, the major research challenges ahead and an outlook on what we can expect in the coming years from ongoing research projects. Finally, Section 4 contains summary and conclusions.

2 Existing Critical Information Infrastructures

We will now proceed to give an overview of characteristics of current critical information infrastructures. We do not in any way provide an exhaustive coverage, but rather we try to give the background as to later be able to highlight the differences between the systems we have today, and the spontaneous information networks that we believe will continue to grow in importance.

2.1 Characteristics

The large part of today's information infrastructure is static and wireline. The networks are managed centrally or hierarchically [2] by known actors who do not change over time. Although communication problems can occur for particular links, redundancy often prevents network partitions from happening [30].

A recent trend is to put more and more services on top of the Internet [7], which has shown itself to be one of the most reliable information infrastructures even in presence of adverse conditions [26] (although susceptible to frequent misconfiguration problems [31]). One of the biggest challenges here is probably overloads which can be the result of a denial of service attack or the result of legitimate needs which peak at the

same time (e.g., major news web sites going down after 9/11). Notable illustration of this phenomenon is the adverse effects of TCP when used as the main communication protocol for connecting operation and management units in energy networks during a blackout [8].

Traditionally, many information networks have been proprietary and thus not fitted for integration with other networks. As a response to this, researchers and industry have started to explore the possibility of opening up systems in order to achieve greater resilience. However, this is not without complications [20]. Corporate entities are not willing to share too much information with other actors since it might mean losing the business advantage. Moreover, there are regulations and policies which must be adhered to regarding communication channels. The problem is further complicated by the fact that information needs span across borders, requiring international agreements.

2.2 Challenges

We believe that there are four main challenges to face in the near future in the area of information infrastructure protection, summarised in table 1.

The interdependencies between different types of infrastructures is one key aspect which makes protecting these systems a complicated task and an interesting research topic. For a nice overview we refer to Rinaldi et al. [40], as well as the outcomes from recent European projects [25,12]. For example, information infrastructures depend on electrical infrastructures and vice versa, and the same relationship holds between communication and transport systems. In order to fully understand these interdependencies it is clear that we need to provide good models of system behaviour, both under normal circumstances and in the event of crises [32].

The transition from static, managed networks to dynamic networks with little or no central control has already started. Peer-to-peer technologies are being used to share data, stream multimedia and to manage computing capacity. Such networks have proven to be resilient to failures and overloads, but they cannot easily provide absolute service guarantees. In addition, an increasing proportion of the network traffic is going through the wireless medium, using a wide variety of radio standards (e.g. GPRS, HSDPA, WiMAX, Wi-Fi). This brings new challenges of mobility, resource allocation and heterogeneity.

Heterogeneity in the technical communication platforms brings two aspects to this equation. The multiplicity of communication technologies will bring a much needed

Table 1. Challenges for traditional infrastructures

Challenge	**Emerging solutions**
Complexity and interdependencies	Modelling and risk analysis
Transition from managed to unmanaged	Peer-to-peer technologies, self-managing systems
Heterogeneity	Standardised protocols, overlay networks, software defined radio
Organised threats with economic motives or adversary disruptions	Intrusion tolerance, diversity, partial rejuvenation

diversity, but at the same time demands dealing with interoperability [39]. Solving these issues is as much an organisational problem as it is technical. Agreeing on standards between different countries and major corporations takes time and has a varying degree of success.

Cyber attacks has gone from being a rare occurrence motivated by curiosity or malice to an economical and political weapon. Despite a large amount of research in the last few years, there are still many tough problems to solve, partly because new threats appear and partly because the systems themselves are changing and evolving. Means for achieving resilience or dependability can be broadly divided in proactive or reactive approaches, and experience shows that both are required. Proactive protection includes hardware redundancy [23], defence-in-depth, diversity and active replication, transparent software recovery [49], etc. Reactive mechanisms will need to cover the events that cannot be prevented. One of the main research areas in this context is that of intrusion detection systems [33,28], where researchers are trying to tackle an almost intractable challenge in detecting significant intrusions without also producing vast amounts of false alarms.

2.3 Outlook

The research on modelling of critical infrastructures will continue to be an active field for many years. It is important to understand that there are many levels at which modelling can be done. They range from Guimera and Amaral's models of airport connections [21] to Svendsen and Wolthusen's [47] generic graph-based analysis of resource flows. We will definitely see more research of this kind, and models will become more detailed and hopefully good tools will be developed to manage them. The CRUTIAL project [12] is one of the major efforts in this direction with the focus on electric power infrastructures.

Moreover, we believe that the coming years will provide a wide range of solutions in addressing the security and reliability of information infrastructures. Specifically in Europe we have seen the launch of a number of recent projects that will bring about partial solutions to this difficult equation: DIESIS [14] providing simulation platforms for e-infrastructures, FORWARD [18] will bring about a collective knowledge on the security threat landscape, threat detection and prevention, and WOMBAT [51] will create a live repository of actual and current threats to information infrastructures on a global basis.

However, the set of solutions should also cover the migration to less centralised and more heterogeneous networks. This entails reusing some non-centralised solutions in new contexts; for example, the potential convergence of P2P technologies – that were originally intended for wired infrastructures – with the mobile ad hoc scenarios. The project HIDENETS [24] has addressed multihop vehicular networks (VANETs), that can potentially become part of a modern society's information infrastructure.

Within the defence sector, (as well as in the civilian communities) one of the possible ways to deal with heterogeneity is the migration from conventional static radio platforms to systems incorporating reconfigurable software-defined radio (SDR) technology. The change in paradigm for military radio communication is not only expected to be a major money-saver, but also to grant the adopting countries the capability to

engage in multinational cooperation, such as international disaster relief operations, by utilising SDR bridging techniques between common and nation-specific waveforms. Replacing legacy radio platforms with modern SDR-based units, conforming to international standards, gives considerable tactical and operative advantages. The capability to share information is crucial to the effectiveness and success of a cooperative mission [1]. It also makes communication more cost effective, by being able to procure commercial off-the-shelf (COTS) equipment at a significantly lower price than developing own equipment.

Since the late 1990s the United States Department of Defense has spent a great deal of time and resources on research and developing the SDR-based Joint Tactical Radio System (JTRS) [35], which is planned as the next-generation voice-and-data radio for use by the U.S. military in field operations after 2010. In Europe, similar techniques are being considered in the EDA joint research project European Secured Software Defined Radio Referential (ESSOR).

These emerging information infrastructures will bring new problems and challenges to solve. In the rest of this paper we will look at challenged networks for disaster response, in which the problems of emerging information infrastructures are taken to the extreme.

3 Disaster Response Infrastructures

3.1 Disaster Response Needs

It lies in the nature of unforeseen events and disasters that they are impossible to characterise in a uniform way. The needs and resources differ drastically depending on circumstances such as the scale of the event, which part of the world is affected, and the type of event (earthquake, flooding, fire, epidemic, etc). However, two important problems can be identified:

- the need for a common operational picture,
- and the matching of needs and resources.

The military is often one of the key actors in the event of a disaster. The initial group of problems, to establish and manage interim information infrastructures, to distribute information, and to coordinate the relief engagement, is something the armed forces have long experience of dealing with. On the other hand, one of the biggest challenges for the military is to be able to participate in collaborative networked environments, such as hastily formed networks for disaster mitigation, while safeguarding valuable information, and upholding confidentiality, integrity, and non-repudiation properties. Information security in military command and control systems often depends on an outer perimeter, a well-defined security boundary within which classified information may not be distributed [48]. Making changes to this structure, such as interconnecting information systems with collaboration partners in a hastily formed network, requires new models for trust [27] and access control [6] in the mutual conversation space.

The rest of this section will target characteristics and challenges of hastily formed communication networks. That is, our focus here is on the technical challenges rather

than the organisational. Although it is precarious to generalise, we try to find some common features and problems associated with such systems. We base most of our reasoning on two of the most well-documented disasters in recent history, the tsunami in east Asia and the Katrina hurricane.

3.2 Characteristics

The infrastructures that will be needed in the event of an emergency cannot be carefully planned and modelled beforehand. They will emerge spontaneously, and will rapidly change over time. Such systems are not intended to replace current systems for everyday use since they are in many ways suboptimal. Their strength is the fact that they can be deployed when the other communication networks have failed.

Hastily Formed Networks (HFN) is a term coined by the Naval Postgraduate School in California, USA [13]. Figure 1 shows a possible scenario where different types of actors need to communicate with each other. These networks are quickly mobilised, organised, and coordinate massive responses. Other characteristics are that they are networks with no common authority but all the same must cooperate and collaborate during a massive as well as distributed response to often a chaotic and completely surprising situation. The networks also have to cope with insufficient resources and lack of infrastructure. Their effectiveness rests on the quality of the conversation spaces established in the beginning.

An experience report by Steckler et al [46] from the aftermath of Hurricane Katrina shows that the wireless medium could be very effective when quickly establishing a network. Those networks were still mostly managed in a way similar to wired networks. Creating and using ad hoc networks might have decreased the effort needed to set up and manage. However, this is not a mature technology and there are many challenges which do not exist in wired/cellular networks [50]. For example, there is a lack of global knowledge (decisions need to be taken based on a local view), the wireless medium needs to be shared between nodes that have not agreed beforehand on when and how to communicate, and communication disruptions are much more likely to occur [5].

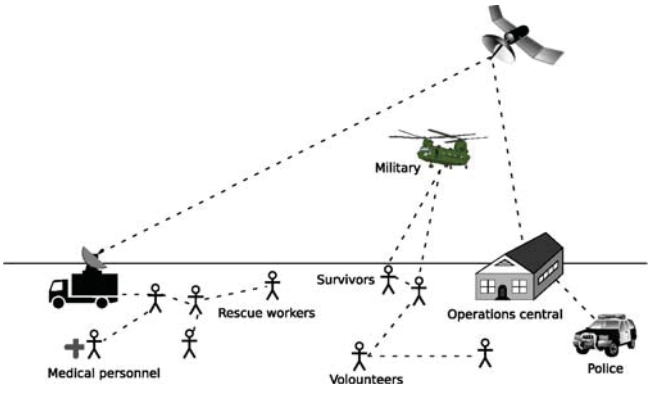

Fig. 1. Disaster Response Scenario

Just as time is an important factor in current information infrastructures (i.e. rapid discovery leads to faster containment and recovery from blackouts), it will be equally important in HFN. These networks will, for example, be used to rapidly disseminate (manycast) information on spread of damage, injuries and threats to lives. However, as opposed to fixed networks where this can be dealt with using redundancy together with some basic level of differentiation, wireless and intermittently connected networks are harder to tackle.

3.3 Challenges

We suggest that there are five main technical challenges that make reliable and timely communication difficult in post-disaster communication, summarised in Table 2. Vast amounts of research have been devoted to each of these subjects separately, but not many have tried to deal with them all at once. Unfortunately, all of them will be present in a large crisis situation.

Disconnectivity. A consequence of mobile wireless networks with resource constraints are network partitions. It will not be feasible for such a network to keep all nodes connected at all times. Network partitions do not only occur in wireless networks, fault-tolerant distributed systems research has dealt with network partitions in such cases for a long time [41]. However, in those works, disconnectivity is considered an exception and usually a rare event. This view on connectivity remained even in research within mobile ad hoc networks since most researchers assume dense networks with random mobility models leading to fairly connected networks. However, recent research emphasises that real-life mobility models, for example in, Kuiper and Nadjm-Tehrani [29], Fiore et al. [17] and Nelson et al. [36], imply that, for some applications, a contemporaneous path between nodes cannot be assumed. Although connectivity is quickly improving with maturity of new technologies, this requires the existence of in-place infrastructure (satellite communication is still expensive and not available to all). To what extent future VANETs will have to rely on a fixed infrastructure is still an open question. An alternative is to devise protocols based on a store-and-forward principle so that mobility is leveraged as a means to disseminate data in the network [45,42].

Resource constraints. Unfortunately, this is not as easy as just storing all data packets that are received, and forwarding them in the hope that the message will reach its desti-

Table 2. Challenges for disaster response infrastructures

Challenge	**Emerging solutions**
Disconnectivity as a norm	Store-and-forward techniques, delay-tolerant networks (DTN)
Resource constraints	Quality-of-service techniques, prioritisation, optimisation
Infeasibilty to centrally manage	Distributed gossip-style protocols
Heterogeneity	Overlay networks, DTN bundles
Security: less organised opportunistic threats or adversary disruptions	Reputation-based systems, selfish-resistant protocols, intrusion detection

nation. Due to the scarceness of energy and bandwidth, protocols will need to limit their transmissions and make sure that (1) packets are only disseminated if needed (i.e. have highest utility) and (2) once a packet is transmitted, it indeed has a chance of making thehop (and subsequent hops); otherwise the network resources are wasted to no avail. The problem of resource-aware delay-tolerant protocols has been studied by, for example, Haas and Small [22] and Balasubramanian et al. [4]. The key problem is deciding which packets are worthwhile to forward to neighbouring nodes, and when.

Infeasibility to centrally manage. The above approaches to optimising resource usage assume a high degree of knowledge about node movements. In a post-disaster scenario, this is not possible. Even the participants and operational clusters in a rescue operation are not known in advance. After the Katrina storm, the American Red Cross alone organised approximately 250.000 (volunteer) rescue workers [5]. This was a magnitude more than they had ever dealt with previously. Together with the fact that the situation is constantly changing, this means that nobody will have an up-to-date global view of what is going on. Thus, ideally the communication protocols will need to function without knowledge of network topology, node addresses, node movements, traffic demands, etc.

Heterogeneity. The fourth challenge is difficult to tackle. It has to do with the fact that in an emergency situation, there will be actors from many different parts of the society such as the police, military, fire fighters, medical personnel, volunteers, etc. These actors need to cooperate with each other but they will probably not have trained together, they will have different technical equipment (ranging from special-purpose hardware such as the Tetra system, to commercial off the shelf non-standardised products). One of the most challenging problems in a disaster scenario is to achieve both technical interoperability and social interoperability amongst the network of networks. A potential approach to achieving technical interoperability is the use of overlays such as delay-tolerant networks [16,38]. Moreover, software defined radio facilitates implementing bridging techniques as discussed in Section 2.3. Obtaining social interoperability on top of a given information infrastructure is a multi-disciplinary challenge.

Security. Some of the actors may even be adversarial themselves, wanting to disrupt or eavesdrop on communication. This brings us to the security challenge. How to solve the trust issue in a HFN is an open problem. Bad or selfish behaviour can be punished (e.g., by not allowing such nodes to participate in the network) if it is detected. Knowledge about misbehaving nodes can also be shared with others using reputation based systems (e.g., Buchegger and Le Boudec [10]). However, such systems creates new problems with false accusations and identity spoofing.

In addition, we need to have distributed intrusion detection as opposed to proposed solutions in existing infrastructures, which are organised with a hierarchy of (well-placed) detectors and correlation agents. In disaster response scenarios, where at least a subset of rescue workers are trained for this purpose, and given the emerging trend in standardisation of rescue terminology and exchange formats [43], we have a somewhat simpler problem than solving the general anomaly detection problem in Internet based communication. This is a situation that is reminiscent of the SCADA systems anomaly detection – which can benefit from the well-defined communication patterns in normal scenarios.

However, a technical challenge is that evaluation of a novel technology means lack of data collected over long time intervals and in realistic scenarios. Detection of attacks on a network is dependent on distinguishing normality from abnormality (for distinguishing unforeseen attack patterns). Also we need to identify the expected traffic patterns and loads on such a network to form a basis for evaluation for novel routing protocols and recovery from node and link crashes.

3.4 Outlook

To deal with these challenges we must incorporate results from a variety of areas such as wireless and delay-tolerant networking, fault-tolerant distributed systems, real-time systems, and security. We continue by presenting some of the interdisciplinary work which is being done to do just that; that is, combining techniques from several different areas to provide disaster response infrastructures.

We believe that one of the key insights required to provide communication in challenged networks is that disconnectivity is a state that is not abnormal. We already mentioned the area of delay-tolerant networking. This is currently being explored in many different directions, including interplanetary communication [16] and wildlife monitoring [44]. There are many directions for this research that are relevant in a disaster response context. We believe that two of the more urgent ones are: (1) as good as possible characterisations of node mobility and (2) timely and resource efficient dissemination protocols. The Haggle project [9] has shown some interesting results in these directions, although much remains to be done.

The RESCUE project [34] is a wide-spanning project involving several areas relating to crisis response. It tackles problems such as heterogeneity (organisational and technical), event extraction, and security. In a recent paper Dilmaghani and Rao [15] paint a similar picture regarding challenges and problems at hand. They also present a communication platform which allows wireless communication between small hand-held devices by routing traffic through wireless mesh network.

WORKPAD [11] is an ongoing European project with the aim of providing software and communication infrastructures for disaster management. They envision a two-layer architecture where the backend is composed of a peer-to-peer network, which is accessed by the frontend devices that are connected in a mobile ad-hoc network. The focus of the research in this project is on the backend, where knowledge and relevant data content is managed.

Major disasters put a huge stress on medical personnel. Not only is there a rush in patients needing medical treatment, care has to be administered under adverse conditions regarding electricity and information supply. There are many ways the situation can be improved by new technologies. As an example, Gao et al. [19] have demonstrated a system where each patient carries a monitoring system which continuously and wirelessly sends information regarding the patient's health. This way the medical personnel can monitor many patients simultaneously and react quickly to changes in their condition. Olariu et al. [37] present an architecture for a low-bandwidth wireless telemedicine system which is still able to transfer imaging data to a remote site.

From the military domain there is a clear interest in ad hoc technologies in challenged environments. For example, the Swedish Armed Forces project GTRS (Common

Tactical Radio System) [3] seeks to benefit from SDR technologies to implement a tactical IP-based ad hoc network, bridging the gap between legacy communication equipment and modern devices using internationally standardised waveforms. The fist demonstrator GTRS units were delivered to the Swedish Armed Forces during 2007, and delivery will continue until January 2014, when the system is scheduled for complete deployment both nationally and within the Nordic Battle Group. The first waveform delivered and tested for the GTRS system was Terrestrial Trunked Radio (Tetra), a mobile radio system designed primarily for emergency services and government use.

4 Summary and Conclusion

We have presented some challenges for the infrastructure systems of tomorrow. In particular we have discussed the spontaneous infrastructures that will form in disaster response situations. There are many similarities between existing infrastructures, and disaster response networks: human lives depend on their availability, time is of essence, and there is an incentive for attacking them. However, they are also very different. The disaster response infrastructures will have much less resources and need to be self-configuring and self-healing in order to be useful. On the other hand, the attacks against these networks are also likely to be less sophisticated and smaller in scale. There are also other challenges, which have not existed (at least to the same degree) in traditional infrastructures, such as mobility, disconnectivity, scarceness of resources, and heterogeneity.

These issues have been the subject of some attention in the field of mobile ad hoc networks, which is starting to mature, moving away from synthetic scenarios with general but artificial mobility models. Instead, an increasing research is being devoted to the problems which occur in particular application areas, each with their own characteristics. Disaster response networks is an instance of such an application area where this research field can expand and improve. We believe that this emerging field has a lot to gain by looking into the research on protection of critical infrastructures. The reverse is also true, even stationary networks will need to adopt methods of self-adaptation and resilience to cope with the complexity and inherent instability of converging network technologies.

Our own work in this area is directed towards finding systematic methods to design and evaluate resource-efficient protocols for disaster response management. Such an effort requires good characterisations of mobility and network connectivity, as well as distributed resource optimisation methods.

References

1. Adams, C.: Information sharing raises more questions than answers. AFCEA Signal Magazine (May 2008)
2. Amin, M.: Toward self-healing energy infrastructure systems. IEEE Comput. Appl. Power 14(1), 20–28 (2001)
3. Baddeley, A.: Sweden seeks military communications flexibility. AFCEA Signal Magazine (May 2006)

4. Balasubramanian, A., Levine, B., Venkataramani, A.: DTN routing as a resource allocation problem. SIGCOMM Comput. Commun. Rev. 37(4), 373–384 (2007)
5. Becker, J.C.: The opportunities and limits of technology in non profit disaster response. Keynote speech at the ISCRAM conference, Washington (May 2008)
6. Bengtsson, A., Westerdahl, L.: Access control in a coalition system. Technical Report FOI-R–2393–SE, Swedish Defence Research Agency (December 2007)
7. Birman, K.: Technology challenges for virtual overlay networks. IEEE Transactions on Systems, Man and Cybernetics, Part A 31(4), 319–327 (2001)
8. Birman, K., Chen, J., Hopkinson, E., Thomas, R., Thorp, J., Van Renesse, R., Vogels, W.: Overcoming communications challenges in software for monitoring and controlling power systems. Proc. IEEE 93(5), 1028–1041 (2005)
9. Bruno, R., Conti, M., Passarella, A.: Opportunistic networking overlays for ICT services in crisis management. In: Proc. 5th International ISCRAM Conference. ISCRAM (2008)
10. Buchegger, S., Le Boudec, J.: Self-policing mobile ad hoc networks by reputation systems. IEEE Communications Magazine 43(7), 101–107 (2005)
11. Catarci, T., de Leoni, M., Marrella, A., Mecella, M., Salvatore, B., Vetere, G., Dustdar, S., Juszczyk, L., Manzoor, A., Truong, H.-L.: Pervasive software environments for supporting disaster responses. IEEE Internet Comput. 12(1), 26–37 (2008)
12. CRUTIAL. European FP6 project, `http://crutial.cesiricerca.it/`
13. Denning, P.J.: Hastily formed networks. Commun. ACM 49(4), 15–20 (2006)
14. DIESIS. European FP7 project, `http://www.diesis-project.eu/`
15. Dilmaghani, R., Rao, R.: A wireless mesh infrastructure deployment with application for emergency scenarios. In: Proc. 5th International ISCRAM Conference. ISCRAM (2008)
16. Farrell, S., Cahill, V.: Delay- and Disruption-Tolerant Networking. Artech House, Inc., Norwood (2006)
17. Fiore, M., Harri, J., Filali, F., Bonnet, C.: Vehicular mobility simulation for VANETs. In: Proc. 40th Annual Simulation Symposium (ANSS) (2007)
18. FORWARD. European FP7 project, `http://www.ict-forward.eu/`
19. Gao, T., Pesto, C., Selavo, L., Chen, Y., Ko, J., Lim, J., Terzis, A., Watt, A., Jeng, J., Chen, B., Lorincz, K., Welsh, M.: Wireless medical sensor networks in emergency response: Implementation and pilot results. In: Proc. 2008 IEEE International Conference on Technologies for Homeland Security. IEEE, Los Alamitos (2008)
20. Ghorbani, A.A., Bagheri, E.: The state of the art in critical infrastructure protection: a framework for convergence. International Journal of Critical Infrastructures 4, 215–244 (2008)
21. Guimera, R., Amaral, L.: Modeling the world-wide airport network. The European Physical Journal B - Condensed Matter 38, 381–385 (2004)
22. Haas, Z.J., Small, T.: Evaluating the capacity of resource-constrained DTNs. In: Proc. 2006 international conference on Wireless communications and mobile computing (IWCMC). ACM, New York (2006)
23. Helal, A.A., Bhargava, B.K., Heddaya, A.A.: Replication Techniques in Distributed Systems. Kluwer Academic Publishers, Norwell (1996)
24. HIDENETS. European FP6 project, `http://www.hidenets.aau.dk/`
25. IRRIIS. European FP6 project, `http://www.irriis.org/`
26. Jefferson, T.L.: Using the internet to communicate during a crisis. VINE 36, 139–142 (2006)
27. Kostoulas, D., Aldunate, R., Pena-Mora, F., Lakhera, S.: A nature-inspired decentralized trust model to reduce information unreliability in complex disaster relief operations. Advanced Engineering Informatics 22(1), 45–58 (2008)
28. Krügel, C., Robertson, W.K.: Alert verification: Determining the success of intrusion attempts. In: Workshop the Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA). German Informatics Society (2004)

29. Kuiper, E., Nadjm-Tehrani, S.: Mobility models for uav group reconnaissance applications. In: Proc. International Conference on Wireless and Mobile Communications (ICWMC) (2006)
30. Labovitz, C., Ahuja, A., Jahanian, F.: Experimental study of internet stability and backbone failures. In: Twenty-Ninth Annual International Symposium on Digest of Papers Fault-Tolerant Computing (1999)
31. Labovitz, C., Wattenhofer, R., Venkatachary, S., Ahuja, A.: Resilience characteristics of the internet backbone routing infrastructure. In: Proc. Third Information Survivability Workshop (2000)
32. Laprie, J., Kanoun, K., Kaniche, M.: Modeling interdependencies between the electricity and information infrastructures. In: Saglietti, F., Oster, N. (eds.) SAFECOMP 2007. LNCS, vol. 4680, pp. 54–67. Springer, Heidelberg (2007)
33. McHugh, J., Christie, A., Allen, J.: Defending yourself: the role of intrusion detection systems. IEEE Softw. 17(5), 42–51 (2000)
34. Mehrotra, S., Butts, C.T., Kalashnikov, D., Venkatasubramanian, N., Rao, R.R., Chockalingam, G., Eguchi, R., Adams, B.J., Huyck, C.: Project RESCUE: challenges in responding to the unexpected. In: Santini, S., Schettini, R. (eds.) Internet Imaging V, vol. 5304, pp. 179–192. SPIE (2003)
35. Melby, J.: Jtrs and the evolution toward software-defined radio. In: MILCOM 2002, October 2002, pp. 1286–1290 (2002)
36. Nelson, S.C., Albert, I., Harris, F., Kravets, R.: Event-driven, role-based mobility in disaster recovery networks. In: Proc. second workshop on Challenged networks (CHANTS). ACM, New York (2007)
37. Olariu, S., Maly, K., Foutriat, E.C., Yamany, S.M., Luckenbach, T.: A Dependable Architecture for Telemedicine in Support of Diaster Relief. In: Dependable Computing Systems, pp. 349–368. Wiley, Chichester (2005)
38. Plagemann, T., Skjelsvik, K., Puzar, M., Drugan, O., Goebel, V., Munthe-Kaas, E.: Cross-layer overlay synchronization in sparse manets. In: Proc. 5th International ISCRAM Conference (2008)
39. ReSIST. Deliverable D12 resilience-building technologies: State of knowledge, ch. 2 (September 2006), `http://www.resist-noe.org/Publications/Deliverables/D12-StateKnowledge.pdf`
40. Rinaldi, S., Peerenboom, J., Kelly, T.: Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. Mag. 21(6), 11–25 (2001)
41. Saito, Y., Shapiro, M.: Optimistic replication. ACM Comput. Surv. 37(1), 42–81 (2005)
42. Sandulescu, G., Nadjm-Tehrani, S.: Opportunistic dtn routing with windows-aware adaptive replication (2008) (submitted for publication)
43. Shank, N., Sokol, B., Hayes, M., Vetrano, C.: Human services data standards: Current progress and future visions in crisis response. In: Proc. ISCRAM conference (May 2008)
44. Small, T., Haas, Z.J.: The shared wireless infostation model: a new ad hoc networking paradigm (or where there is a whale, there is a way). In: Proc. International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc). ACM, New York (2003)
45. Spyropoulos, T., Psounis, K., Raghavendra, C.S.: Spray and wait: an efficient routing scheme for intermittently connected mobile networks. In: Proc. SIGCOMM Workshop on Delay-tolerant networking (WDTN). ACM, New York (2005)
46. Steckler, B., Bradford, B.L., Urrea, S.: Hastily formed networks for complex humanitarian disasters (September 2005), `http://www.hfncenter.org/cms/KatrinaAAR`
47. Svendsen, N., Wolthusen, S.: Analysis and statistical properties of critical infrastructure interdependency multiflow models. In: Proc. IEEE SMC Information Assurance and Security Workshop (IAW) (2007)

48. Swanson, M., Hash, J., Bowen, P.: Guide for developing security plans for federal information systems. Technical Report 800-18, National Institute of Standards and Technology (February 2006)
49. Szentivanyi, D., Nadjm-Tehrani, S.: Middleware support for fault tolerance. In: Mahmoud, Q. (ed.) Middleware for Communications. John Wiley & Sons, Chichester (2004)
50. Tschudin, C., Gunningberg, P., Lundgren, H., Nordström, E.: Lessons from experimental MANET research. Ad Hoc Networks 3(2), 221–233 (2005)
51. WOMBAT. European FP7 project, http://www.wombat-project.eu/