Secure Mobile Notifications of Civilians in Case of a Disaster

Heiko Rossnagel and Tobias Scherner

Chair of Mobile Commerce and Multilateral Security
Johann Wolfgang Goethe - University Frankfurt,
Gräfstr. 78, 60054 Frankfurt, Germany
heiko.rossnagel@m-lehrstuhl.de,
tobias.scherner@m-lehrstuhl.de
http://www.m-lehrstuhl.de

Abstract. Disaster management using mobile telecommunication networks provides a new and attractive possibility to save human lives in emergencies. With this contribution, we present a possible disaster management system based on mobile telecommunication. In order to use such a system in the real world, security requirements such as availability, accountability, integrity and confidentiality have to be ensured by the disaster management system (DMS). We summarize these requirements and propose ways of addressing them with a multilateral secure approach. Using electronic signatures based on SIM-cards, we assure integrity, accountability and confidentiality of the notification messages. We also discuss how availability could be increased.

1 Introduction

Historic examples demonstrate that disasters had a strong influence on the development of nations [3]. Sometimes, the consequences were so enormous that the effected cultures vanished from the world's stage [26].

People usually have problems to recognize leading signs of natural disasters and the possible magnitude of damages. One example is the eruption of Mount Thera and the disappearance of the Minoan culture [17] [7]. Another tragic example is the 2004 Tsunami [34].

Disasters can be caused by natural reasons or can be driven by humans. In the majority of cases, the latter ones do not have any leading signs, like for example the Chernobyl explosion [35] or the September 11th attacks [33]. Therefore, promptly notification and evacuation of the people who are endangered by the disaster is especially desirable in order to save as much lives as possible.

Mobile communication infrastructures offer standardized wireless communication services in almost all countries [19] and allow a fast diffusion of information. This existing and deployed infrastructure could be used for emergency service applications using location-based services (LBS). Currently, these emergency services are discussed and standardized by organizations and bodies like the European Telecommunications Standards Institute (ETSI) with the aim of preparing a framework for worldwide interoperable emergency services [15] [13] [12] [14]. In

H. Leitold and E. Markatos (Eds.): CMS 2006, LNCS 4237, pp. 33 – 42, 2006.

addition, the European Commission is strongly interested in this topic and encourages research and standardization of electronic communication networks [9] [25]. Thereby, the European approach focuses on what can be delivered instead of defining services and service levels without having the available technology like the E911 project [5]. Along with these new opportunities of fine-grained disaster management, new possibilities of abuse also do emerge. For example, it is possible to send fake disaster warnings via the Short Message Service (SMS) [27]. Therefore, it is necessary to analyze the security requirements of such DMSs and to meet these requirements when designing a future system. Naturally, privacy concerns have to be discussed in the setting of mobile network based DMS. However, this is out of scope of this paper as privacy issues have already been discussed in [18].

In section 2 of this paper, we present a DMS based on mobile communications infrastructure similar to [30] [18]. We then analyze the security requirements of such a system in section 3, propose some refinements in order to address the requirements in section 4 and then conclude our findings.

2 Disaster Management System

DMS are complex systems and should be designed in an integrated approach from detecting events up to eliminating possible threats to people and infrastructures [16].

In particular, DMSs should enable disaster forces to manage disaster events, including detection and analysis of incidents. Persons in charge should be supported to prepare evacuations, control and support disaster forces and to locate victims. An example of requirements with local characteristics of a DMS in Indonesia can be found in [2].

2.1 General Requirements

Yuan and Detlor [36] have undertaken a possible categorization of requirements. Based on this study, Scherner and Fritsch [30] augmented this categorization by extending it to popular and promising technologies that are currently in use or being discussed, and analyzing their strengths and weaknesses. Their analysis shows that mobile communication infrastructures are superior to other technologies. Some of these advantages are:

- Identification and locating experts
- Custom tailored messages to different parties and locations
- Dynamical notification updates while individuals are passing over to another danger zone
- Measuring of movements of the holders of mobile phones
- Providing back channels to victims[30]

However, to use this technology, the market penetration of mobile devices and the network coverage have to be sufficient. Both factors are crucial for success of a mobile network-based DMS. Currently, worldwide over 1.5 Billion GSM-subscribers are registered [1]. The market penetration of mobile devices differs in Western Europe between 97,1% in Sweden and 68,8% in France (population / mobile

subscribers[1]) [6]. Naturally, it is impossible to make general statements about the network coverage in Europe. Multiple factors have influenced the development of mobile networks in different countries. Examples are the amount of fixed lines before the emergence of mobile networks, the population density, and economic drivers that speed up different communication technologies.

Nevertheless, even sparsely populated countries have invested in mobile networks, instead of providing fixed-lines in remote areas. One example is the GSM-network coverage of Sweden, which is shown in Fig. 1.

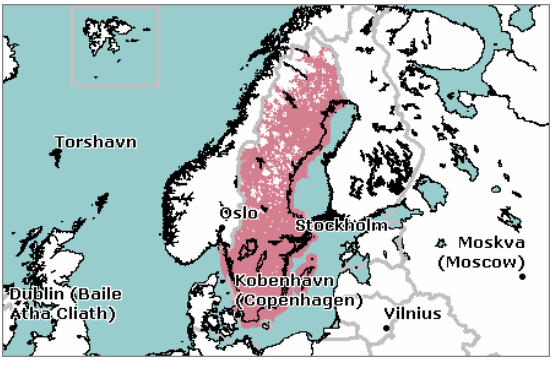

Fig. 1. GSM-network coverage of Sweden [18]

2.2 A DMS Based on GSM Networks

The participating parties in our scenario are mobile subscribers, disaster managers, mobile operators, and a DMS. Mobile subscribers are able to register themselves during the preparatory phase (before the occurrence of disasters) and can define and approve observation rules. The observation rules are stored in a separated part of the infrastructure and are executed if one of the parties is located within a defined disaster area. In Addition, geographical areas can also be observed. An exemplary use case is the observation of chemical warehouses by safety inspectors.

Furthermore, users are able to register themselves as specialists like medics, fire fighters or other disaster forces. This self-declaration as a specialist has to be confirmed by the employer or aid organization. Because instructions for specialist are tailored for the individual recipient, these messages and the replies to disaster managers have to be sent by point-to-point technologies like SMS or Multimedia Message Service (MMS). On possible restrictions on applying point-to-point technologies in emergency cases, see [22] and [8]. In contrast, warnings to civilians will be send via Cell Broadcast Service (CBS). CBS belongs to the point-to-multipoint technologies and offers the following useful characteristics [23]:

- CBS has very low setup costs for operators, users and disaster managers.
- Activation of CBS can be provided by the operator via SIM Application Toolkit (SIM AT).

[1] A certain subscriber is counted multiple times if he has several mobile communication accounts.

- CBS reduces the traffic as recipients in the disaster area receive the notification just in time.
- Privacy concerns about CBS do not exist.
- Mobile networks can be secured against power outages.
- Mobile phones offer the possibility of direct communication between rescue forces and victims.

Disaster managers use a geographic information system (GIS)-supported platform to manage disaster activities, like warnings, locating and routing of victims, and controlling the disaster forces as described in [18] and similar in [37]. If a disaster event occurs, the disaster manager sends out warnings to the effected areas by cell broadcast to ensure in-time warnings of potential victims. Afterwards, he is able to locate the victims and pre-registered specialists through the DMS. This information is required for controlled evacuations of disaster areas. Thereby, the timing of warnings in different areas can be used to prevent overcrowded escape routes. The accuracy of the detected positions may differ from cell to cell due to locating methods and cell dimensions [37]. This has to be considered while planning and executing evacuations. An overview of the proposed infrastructure can be found in Fig. 2.

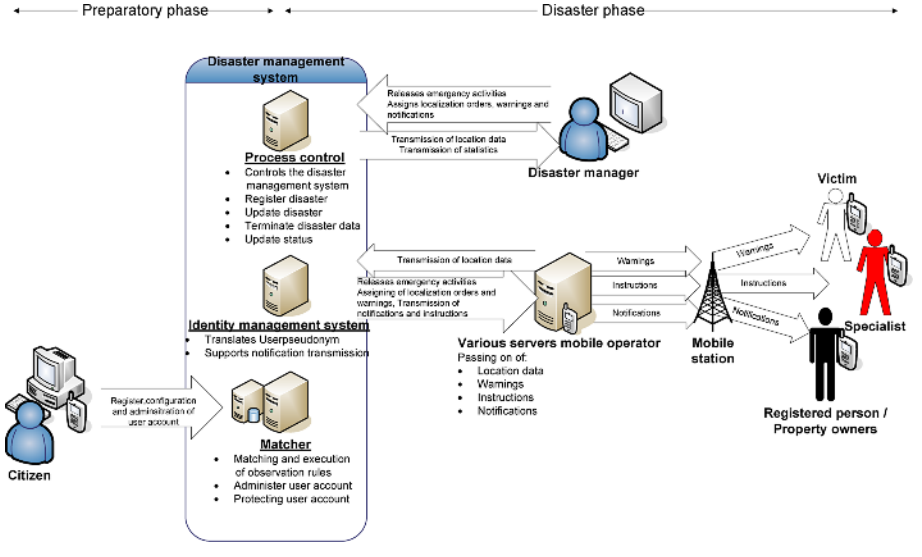

Fig. 2. Disaster management solution overview

Mobile operators provide the communication infrastructure, send out warnings and deliver location information based on cell IDs.

The DMS is the core component of our proposed infrastructure and consists of a middleware solution between mobile operator and disaster manager. It is separated into three independent architectural elements, called Matcher, Identity Management Control (IDM), and Process Control. The Matcher locates civilians within the disaster area. It matches the disaster area with observation rules of the users and protects persistent store of individual observation rules. It matches profiles of threatened

person with their registered contact person. The Identity Management System controls the information exchange between the disaster management, the mobile operator and the civilians. Information exchange between disaster manager and mobile operator is done by using different user pseudonyms to avoid linkability for unauthorized observations. Borking [4] described this kind of identity protector first. The Process Control administers the DMS, represents an interface to the disaster manager and is responsible for temporary storage of disaster data (observation rules and localization information).

Advantages of this system are the ability to monitoring victims, pseudonymous identification of certain mobile subscribers, and operational control of individuals.

3 Security Requirements of the Notification Infrastructure

The proposed infrastructure also has to be protected in regard to the four traditional security targets availability, integrity, accountability and confidentiality [28]. Therefore, we develop a set of application and security requirements in this section that has to be fulfilled by the DMS.

3.1 Notification of Mobile Subscribers

In order to leave as much time as possible for evacuation, the notification of civilians has to be as little time consuming as possible. Therefore, we formulate an application requirement.

Requirement I:	*The notification process has to be as little time consuming as possible.*

Since mobile subscribers use a great variety of different mobile devices, the service should be as compatible as possible to most devices. Therefore, we formulate another requirement.

Requirement II:	*The notification service should be useable with (almost) any mobile phone on the market.*

Because of the short time span in which the mobile subscriber has to react to the notification it is not possible to crosscheck the received information. Therefore, the notification service must provide a way to ensure the integrity and authenticity of the notifications. Otherwise, a potential attacker could alter notification messages or create false notification messages that could lead to a disaster by itself. Terrorists for example could use the DMS to create a mass panic.

Requirement III:	*The notification service has to ensure that the user can determine that the notification is from an authorized disaster management authority and that the integrity of the notification message has not been violated.*

It is also important that the notification does not get lost or delayed (availability is the corresponding property). Consequently, we formulate a third requirement, which should be fulfilled by the notification service. Obviously, the notification service on its own cannot guarantee fulfillment of any of these requirements (e.g. when communications are interrupted or tampered within parts of the network outside of its control), but it is important that the user knows about the state of the message he receives.

Requirement IV::	*The notification system has to ensure that messages reach subscribers in time.*

3.2 Notification of Specialists

Since specialists are a special form of mobile subscribers all requirements stated above also apply for them. Furthermore, some additional requirements have to be determined for specialists. If the DMS is notifying specialists, there might be reasons that some of this information should not be publicly available. Therefore, the notification service should, in addition to the requirements stated above, provide means to ensure that confidentiality of the notification is preserved. Therefore, we formulate another requirement.

Requirement V:	*When notifying specialists, the notification messages should be confidential.*

Furthermore, the specialist should be capable to interact with the disaster manager, in order to provide updates of the local situation and for instance, his availability to ease up resource scheduling. Therefore, the specialist will send messages back to the disaster manager. However, the disaster manager has to be able to verify the authenticity and integrity of these messages. Otherwise, a potential attacker could change messages or create false ones in order to hamper rescue efforts. In addition, these messages should also be confidential. Therefore, we present two more requirements.

Requirement VI:	*Specialists have to be able to send confidential messages to the disaster manager.*

Requirement VII:	*Disaster managers have to be able to check the authenticity and integrity of incoming messages.*

4 Further Refinement of Proposed Infrastructure

The changes to the infrastructure we are going to propose are based on the assumption that the mobile subscribers are using SIM cards that are capable of creating and verifying electronic signatures. The technology for such SIM cards exists but has not gained much market penetration so far. The WiTness project [10] sponsored by the

European Union has developed such a SIM card that is capable of creating RSA signatures [29] and also provides 3DES encryption. Using such a SIM card, the mobile subscriber can obtain a copy of the public key of the notification service provider. Furthermore, specialist can register their public keys in the DMS. Having defined the necessary premises, we can now propose the following infrastructure that is illustrated in Fig. 3.

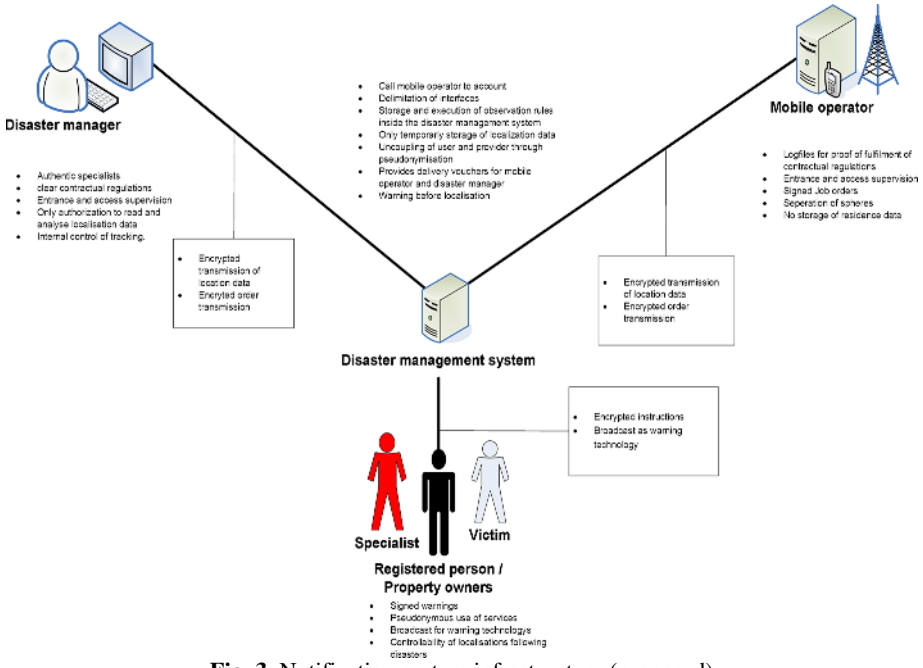

Fig. 3. Notification system infrastructure (proposed)

Our goal is to achieve as many of the application and security requirements defined in section 3 as possible. Therefore, we propose an implementation using the SIM AT, which also ensures compatibility to almost all mobile phones.

When a disaster occurs, the disaster manager initiates a notification and sends it to the SIM AT application running on the mobile device of the addressee [11] by SMS in case of specialists or CBS for normal subscribers. The notification is electronically signed with the private key of the notification service provider. After receiving the signed push notification, the application can check the integrity and authenticity of the notification by verifying the signature. If the signature is valid, the mobile subscriber can now follow the given instructions. Since they have registered their public keys, specialists are also able to send electronically signed messages back to the disaster manager, who can check the authenticity and integrity of these messages. Encryption of these messages could be provided by using 3DES encryption.

Since the notification is electronically signed and its authenticity and integrity is automatically checked, it does require as little time of the mobile subscriber as possible. Therefore, we can state that Requirement I has been met. Because most

current mobile phones support SIM AT, we can also conclude that Requirement II has been fulfilled. By checking the validity of the electronically signed notification message the SIM AT application is able to check the authenticity (only the service provider can make a valid signature) and the integrity of the notification message automatically. Therefore, we conclude that Requirement III has been fulfilled.

Our solution has several shortcomings regarding the availability of the notification service. The used SMS service does not provide acknowledgements for delivered messages and is dependent on the availability of the infrastructure of the mobile operator. If the mobile subscribers phone is unreachable or even switched off, a notification in time is impossible. Furthermore, SMS depends on unused capacity in the signaling channels and has consequently low priority within the channel utilization [31]. However, additional steps could be undertaken to improve the probability that the mobile subscriber receives the needed information in time. For example, different channels could be used, like sending the notification via CBS, SMS as well as e-mail. Furthermore, the availability of any service during disasters is dependent on the robustness of the underlying infrastructure [24]. Many disasters have had direct impact on communication infrastructures within disaster areas. In centralized communication infrastructures, disasters also have effects on the non-directly effected parts of the infrastructure if nodes are in the disaster area. One example is the failure of communication infrastructures during and after the hurricane "Katrina" in 2005 [20]. Network providers anticipated the probability of such an event in this area and protected their underlying communication infrastructure against outer influencing factors like heat, humidity, dust, and mud.

Additionally, mobile networks have been abused by terrorists, e.g. for setting off bombs like in Madrid in 2004 [20]. To prevent further explosions, officials claim the need to be able to shut down mobile networks in an emergency case. Schneier [32] argues that this would not significantly reduce the risk of further detonations. Terrorists might anticipate this behavior and might use alternative ways, like kitchen timers, for setting off bombs. He also concludes that victims benefit far more from telecommunication infrastructures than attackers do. Summarizing, we conclude that Requirement IV cannot completely be fulfilled. When communicating with specialists, confidentiality can be provided by ciphering the data using Wireless Transport Layer Security (WTLS), Secure Socket Layer (SSL). Therefore, Requirements V and VI have been fulfilled. By signing the messages to the disaster manager, the specialist ensures their integrity and authenticity. Therefore, we can state that Requirement VII has been met. The proposed solution has almost fulfilled the requirements that we defined in the previous section, except Requirement IV (Availability).

5 Conclusion

With this contribution, we proposed a DMS based on mobile communication infrastructures. In order to use such a system in the real world, security requirements such as availability, accountability, integrity and confidentiality have to be ensured by the DMS. Therefore, we derived security requirements for notifying civilians and specialists. Based on these requirements we proposed further refinements of the infrastructure, that address these issues. These refinements are based on SIM cards that are capable to create and verify electronic signatures. Such SIM cards are not

widely deployed, but the technology exists. How to achieve a broad diffusion of such SIM cards is outside the scope of this paper.

However, not all requirements could reliably be achieved by using one single communication infrastructure but disaster management would clearly benefit from communication infrastructures that are more sophisticated.

References

1. 3G (2005) 1.5 Billion GSM Wireles Customers Across the Globe, *http://www.3g.co.uk/PR/Sept2005/1875.htm,* accessed 9 September 2005.
2. Abdulharis, R., Hakim, D., Riqqi, A. and Zlatanova, S. (2005) Geo-information as Disaster Management Tools in Aceh and Nias, Indonesia: a Post-disaster Area: Workshop on tools for emergency and disaster management, Brno.
3. Barry, J. M. (1998) Rising Tide: The Great Mississippi Flood of 1927 and How It Changed America, Simon & Schuster.
4. Borking, J. (1996) Der Identity Protector, *Datenschutz und Datensicherheit (DuD),* 20, 11, 654-658.
5. Burke, K. and Yasinsac, A. (2004) The ramifications of E911, College of Arts and Science, Tallahassee, Florida, USA.
6. Büllingen, F. and Stamm, P. (2004) Mobile Mulitmediadienste, Deutschlandschancen im internationalen Wettbewerb: Eine Internationale Vergleichsstudie, Bad Honnef.
7. Dietrich, V. J. (2004) Die Wiege der abendländischen Kultur und die minoische Katastrophe - ein Vulkan verändert die Welt, Alpnach Dorf.
8. Ellington, B. (2004) Enhancing E911 Systems a usability plan, *Proceedings of the Tenth Americas Conference on Information Systems (AMCIS 2004),,* August 2004, New York, ACM, 3419 - 3425.
9. European Commission (2003) COMMISSION RECOMMENDATION on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services, Official Journal of the European Union, Brussels.
10. European IST Project 'Wireless Trust for Mobile Business' (WiTness) (2004) SIM Application Hosting - Detailed description of the concept, www.wirelesstrust.org/publicdocs/Witness_32275_D4_ExecSum.pdf, March 2005.
11. European Telecommunications Standards Institute (1992) GSM 3.40 - Technical Realization of the Short Message Service - Point-to-Point.
12. European Telecommunications Standards Institute (ETSI) (2003) Requirements for communication of citizens with authorities/organisations in case of distress (emergency call handling), ETSI SR 002 180 V1.1.1 (2003-12),ETSI, Sophie-Antipolis.
13. European Telecommunications Standards Institute (ETSI) (2004) Requirements for communication between authorities/organisations during emergencies, DRAFT ETSI SR 002 181 V0.3.0 (2004-12), ETSI, Sophie-Antipolis.
14. European Telecommunications Standards Institute (ETSI) (2004) Requirements for communications between citizens during emergencies, Draft ETSI SR 002 410 V0.0.1 (2004-09),ETSI, Sophie-Antipolis.
15. European Telecommunications Standards Institute (ETSI) (2004) Requirements for communications from authorities/organisations to the citizens during emergencies, DRAFT ETSI SR 002 182 V0.1.3 (2004-11),ETSI, Sophie-Antipolis.
16. EWCII (2003) Integrating Early Warning into Relevant Policies, Bonn

17. Forsyth, P. Y. (1999) Thera in the bronze age, Lang, New York u.a.
18. Fritsch, L. and Scherner, T. (2005) A Multilaterally Secure, Privacy-Friendly Location-based Service for Disaster Management and Civil Protection, *Proceedings of the AICED/ICN 2005, (LNCS 3421),* Berlin, Heidelberg, New York, Springer, 1130-1137.
19. GSM Association (2006) GSM Coverage Maps, *http://www.gsmworld.com/roaming/gsminfo/index.shtml,* accessed 22.02.2006.
20. GSM World Series online "A Week in Wireless #194,"2005.
21. Ghosh, A. G. J. "A Strike At Europe's Heart, "TIME Europe2004, online version.
22. Ian Harris (2005) LS - Use of SMS and CBS for Emergencies: Technical Specification Group Terminals TSGT#27(05)0051, Meeting #27, 09 - 11 March 2005, ETSI, Tokyo.
23. Lane, N. (2000) Effective Disaster Warnings, Subcommittee on Natural Disaster Reduction, Working Group on Natural Disaster Information Systems, Washington.
24. Little, R. G. (2003) Toward More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems, in IEEEE (Eds.), *Proceedings of the 36th Hawaii International Conference on System Sciences,* Hawai, IEEE.
25. Ludden, B., Pickford, A., Medland, J. and Johnson, H.(2002) Cgalies final report V1.0, Report on implementation issues related to access to location information by emergency services (E112) in the European Union.
26. McNeil, D. G. J."What happens after disaster? Calamity, or reason to unite?" Milwaukee Journal Sentinel 2005.
27. Muntermann, J. and Rossnagel, H. (2006) Security Issues and Capabilities of Mobile Brokerage Services and Infrastructures, *Journal of Information System Security,* 2, 1.
28. Rannenberg, K. (2000) Multilateral Security - A concept and examples for balanced security, *Proceedings of the 9th ACM New Security Paradims Workshop,* Cork, Ireland, ACM Press, 151-162.
29. Rivest, R. L., Shamir, A. and Adleman, L. (1978) A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM,* 21, 2, 120-126.
30. Scherner, T. and Fritsch, L. (2005) Notifying Civilians in Time - Disaster Warning Systems Based on a Multilaterally Secure, Economic, and Mobile Infrastructure, in AMCIS (Eds.), *Proceedings of the Eleventh Americas Conference on Information Systems (AMCIS) 2005.*
31. Schiller, J. (2003) Mobilkommunikation, Pearson Studium, München.
32. Schneier, B. (2005) Schneier on Security; A weblog covering security and secuirity technologies: Turning Cell Phones off in Tunnels, *http://www.schneier.com/blog/archives/2005/07/turning_cell_ph.html,* accessed July 19, 2005.
33. September 11th.com (2003) September 11, 2001-The Day the World Changed, *http://www.september11news.com/,* accessed 01 January 2006.
34. Spiegel online (2004) The Wall of Water: Part I, *http://service.spiegel.de/cache/international/spiegel/0,1518,335281,00.html,* accessed December 31, 2004.
35. Visscher, R. (2000) Chernobyl Nuclear Disaster, *http://www.chernobyl.co.uk/chernobyl_in_the_news.htm,* accessed 21st February 2006.
36. Yuan, Y. and Detlor, B. (2005) Intelligent Mobile Crisis Response Systems,: Systems to help coordinate responder communication and response in order to minimize the threat to human life and damage to property, *Communications of the ACM, Volume 48, Issue 2* February 2005, New York, ACM Press, 95- 98.
37. van der Togt, R., Beinat, E. Z. S. and Scholten, H. J. (2005) Location Interoperability Services for Medical Emergency Operations during Disasters, in P. van Oosterom, S. Zlatanova and E. M. Fendel (Eds.), *Geo-information for Disaster Management,* Heidelberg, Springer Verlag, 1127 - 1141.