EMERGENCY ANNOUNCEMENTS TO MOBILE USER DEVICES IN GEOGRAPHICALLY DEFINED AREAS

Elina Valtonen, Ronja Addams-Moring, Teemupekka Virtanen
Helsinki University of Technology (HUT), Telecommunications Software and Multimedia Laboratory

Email: elina.valtonen@hut.fi , ronja.addams-moring@hut.fi , teemupekka.virtanen@hut.fi

Antti Järvinen; Mikael Moring
YLE - Finnish Broadcasting Company ; STUK - Radiation and Nuclear Safety Authority, Finland

Email: antti.jarvinen@yle.fi ; mikael.moring@stuk.fi

Keywords: Emergency announcement systems, civil defence, mobile phone networks, mobile devices

Abstract: When emergency announcements (EA) to a population in a crisis area are needed, avoiding single points of failure in the EA sending and forwarding systems is essential. We present a new concept, an extension to existing EA sending systems, which is based on real-time location information about mobile devices. Such a solution would increase the EA sending systems' robustness through redundancy and technology diversity. At the same time, these mobile emergency announcement (MEA) sending systems would increase the percentage of the threatened population that can be reached fast. The proposition is based on a set of requirements for EA sending systems, the most important of which turned out to be ensuring the authenticity and integrity of the EA information content. We found our preliminary results too optimistic: current GSM networks should **not** be used for sending EAs, as it is quite possible to forge SMS text messages, even to multiple GSM phones in a specific target area. The next generations of mobile phone networks (3G/UMTS and 4G) seem more promising, due to their packet-oriented architectures, as each data packet can be stamped with verifiable information about the source of the data. However, the development of communications networks with features compatible with MEA sending will demand that both authorities and independent experts take an active, early role in networks design right beside the commercial organisations.

1 INTRODUCTION

When a crisis occurs, whether caused by a natural catastrophe (forest fire, flooding), a large-scale accident (explosion, major traffic accident) or the uncontrolled spread of some hazardous substance (fire at a chemicals factory, radioactive leakage), authorities need to send emergency announcements (EA) to the population in the threatened areas. The EAs warn about dangers connected to the incident and instruct the population as to what they should and should not do. To be effective, the EAs should reach a high enough percentage of the population in question.

In many European Union (EU) Member States the delivering of emergency announcements is delegated

to public broadcasting companies, typically national radio channels (BBC, 2002; Held, 1999; SR, 2001; Act_YLE, 1993). However, information media and technologies have become diverse, so that a growing part of the population in developed countries receives most of their information through personalized messages (Manber et al., 2000; MTV3, 2004). These "customized news deliveries" have nothing to do with traditional radio channels.

In many developing countries, too, the information scene is also quite diverse, though the reason is different: no media or technology has yet reached all of the population.

Consequently, nowhere in the world can we accurately predict the information media or technologies that a large enough percentage of any population will routinely be following at the time of a future crisis, when EAs would be sent.

If we can not predict the popular information media or technologies of even the near future, could we, instead, make an educated enough guess about future communication habits? If some type of equipment with communications capabilities will be routinely "following" a high enough percentage of the population, could those mobile communications devices be correctly located and receive emergency announcements, when needed?

Our research questions thus became:

- Do such technologies exist that make it possible to locate a large number of mobile devices (and thus their human users) in a geographically defined crisis area?
- Do such technologies exist that make it possible to use that location information in a timely manner to transmit emergency announcements (EA) to a large enough percentage of the mobile devices in that area?
- Can the identified technologies be combined into an "add-on" part that can be integrated with the already existing emergency announcement sending systems and organisations, with tolerable costs?

We analysed the situation from the EU point of view, using Finland as our principal frame of reference. Our original hypotheses were that using mobile networks and devices for emergency announcements would be either technically impossible or illegal. After both these hypotheses were proven wrong, we evaluated currently used mobile messaging networks and currently available locating technologies, based on a set of requirements for EA sending systems.

We present our requirements for EA sending systems, the currently existing systems that have some of the features that a mobile emergency announcements (MEA) sending system would need to have, the relevant EU legislation and the results of our evaluation of the existing messaging and locating technologies. Then, we study the technical possibilities for ensuring that only legitimate MEAs reach the population.

We aim to develop a technical concept for reaching populations at risk through mobile devices that people routinely carry with them. Our secondary goal is to open the discussion about what organising, communication and cooperation efforts are needed within the EU to actually build such systems.

2 REQUIREMENTS FOR EMERGENCY ANNOUNCEMENT SENDING SYSTEMS

We define the requirements for an emergency announcements sending system (regardless of the technology used) as follows, in an approximate order of importance. These requirements have been inspired by works of Anderson, , Hanke and Wiio (Anderson, 2001; Hanke, 2002; Wiio, 1995), some Finnish laws (Act_Prepar, 2003; Act_YLE, 1993) and three of us (Järvinen, Moring and Virtanen) personal experiences (30 years combined) from national security, military, rescue, and civil defence duties.

- Authenticity, integrity and non-repudiation of the messages (emergency announcements may not be forged nor become corrupted because of weaknesses in the sending technology; also, no party should be able to successfully deny their responsibility for sending an emergency announcement if they indeed sent one)
- Sufficient payload size - message content space - for efficient crisis information (an emergency announcement that is misunderstood by the population does easily more harm than good)

- Timing (sending each emergency announcement when the information is needed, and at no other time)
- Capability to force a pushed message to each device, regardless of other ongoing communications or transmissions and regardless of if the owner (or user) of the device agrees to receive
- High population reachability (high availability and use percentage of the technology or media)
- Functional reliability even during sudden and massive use peaks (minimal risk for Denial of Service or Flash Crowd)
- Targetability (localising the EA to the population specifically concerned)
- Tolerable costs, both for the infrastructure needed and for sending an emergency announcement

Furthermore, with MEA sending systems, the delay between identifying the mobile devices at the target location and sending the MEA to them should be as short as possible.

3 MOBILE EMERGENCY ANNOUNCEMENT SYSTEMS – A NEW CONCEPT

To our knowledge, there are no location-based MEA sending services anywhere in the world. Therefore, the concept of the service needs to be built from scratch. There are, however, at least two SMS-based mobile information services, concerning risks to the population, already in use in Europe. Also a pager-based emergency information service has been developed in the US (NASA, 1998). Although none of these fully meet the requirements described above or even utilises real-time localisation, they represent experiences to learn from.

The Austrian environment organization "Global 2000" launched the RAMOS SMS service for alarming a predefined group of users about radiation leakage accidents in April 2003 (Global2000, 2003). The service requires subscription and there is an annual fee, for which the subscribers get a weekly radiation report and, most importantly, are among the first to be warned if the amount of radiation in one of the monitoring stations increases.

In Finland, STUK (Radiation and Nuclear Safety Authority) replaced their preparedness personnel's pagers with GSM phones in 2002. Through the new system, a group of approximately 130 employees can receive alarm or information messages on their mobile phones via SMS and phone calls. The messages are sent, if needed, by the on-duty expert. During preparedness exercises in 2003 alarm messages were sent and they were received within less than 5 minutes by the target group (Weltner, 2004). Furthermore, 1998-2002 the general reachability of the employees was tested three or four times each year. After the change from pagers to GSM phones, the reachability (within 30 minutes) increased from slightly less than 70% to slightly over 80% (STUK, 2002).

The RAMOS and STUK systems prove the usefulness of SMS based alarm or information systems in a limited scale. However, both these systems send messages only to predefined mobile phone numbers: the question of locating mobile devices in a crisis area still needs to be addressed.

4 RELEVANT EU LEGISLATION

Localisation (targetability) is the one criterion in chapter 2 that would most likely conflict with legislation concerning personal privacy, as a mobile device's identity (name and/or number) typically is a key to the user's identity as well. However, since 2002, EU legislation makes it possible to use location information from communications networks for authorised civil defence and rescue purposes. The directive of the European Parliament and the European Council 2002/58/EC takes these central stands on the issue (EP_EC, 2002):

- The routine locating of the origin of emergency calls ***must*** be implemented.
- Locating in other situations where it is apparent for the authorities that someone is in danger ***may*** be implemented.
- In the above mentioned situations, telecommunications networks' operators have the legal duty to hand over location information to the authorities without delay and free of charge.
- The directive 2002/58/EC must be incorporated in the national legislation of each Member State by the end of October 2003.

The current legislation in Finland follows the directive (Act_Change, 2002; Act_Comm_Marc, 2003; Act_Priv_Tele, 2001).

A criterion, which would maybe conflict with legislation that protects the legitimate use of communications networks, is pushing content to user devices (e.g. mobile phones) without prior user consent. Such pushed content clearly interrupts telecommunications. However, as EAs are an established exception to the protection of communications (radio transmissions must also be interrupted for sending an EA), it can be assumed that legislating specifically about using mobile devices for EA sending should not be a problem. Already, the EU directive 2002/58/EC entitles providers of electronic communications services to provide access to location information in emergency situations without the prior consent of the users concerned.

5 THE EVALUATED TECHNOLOGIES

Regarding the high population reachability criterion in chapter 2: GSM mobile phone networks are in use worldwide. Furthermore, GSM mobile phone use percentage is already high in the northern parts of the European Union (e.g. 86 % of the whole population of Finland (Taloustutkimus, 2002)) and rising in all of the EU Member States (Tilastokeskus, 2002).

Because of GSM networks' superior population reachability within the EU, we evaluated four mobile messaging technologies, which are all compatible with the current GSM mobile telephony architecture (or its future replacements), and the two existing locating technologies that cover all of Europe, based on the rest of the criteria in chapter 2. The criteria that clearly differentiated the technologies are presented in sections 5.1 and 5.2 below.

5.1 Messaging technologies

We evaluated these messaging technologies for mobile emergency announcements: the Short Message Service (SMS), the Multimedia Messaging Service (MMS), the Wireless Application Protocol (WAP), the Push Access Protocol (PAP or WAP Push) and the Session Initiation Protocol (SIP).

Criterion	SMS	MMS, SIP	WAP/PAP
Reachability	High	Low	Low
Payload size	160 char	Large	Large
Reliability	Fairly high	Fairly high	Fairly high
Cost, infrastructure	Low	Low	Low
Cost, message	Low	Fairly low	Fairly low

Table 1: Messaging technology comparison

Of the evaluated messaging technologies, only SMS (ordinary text message) is widely adopted by users. All the other technologies are promising, each in their own manner, but they are not mainstream technologies, yet. It is not apparent, either, if one of these newer messaging technologies will be a winner in the competition for the next de-facto standard mobile messaging technology in Europe.

5.2 Locating technologies

We evaluated these locating technologies: GSM Cell Identification based locating and the Global Positioning System (GPS).

Criterion	GSM cID	GPS
Reachability	Fairly high	Moderate
Reliability	Moderate	Fairly high
Cost, infrastructure	Low	High
Cost, message	Moderate	N/A

Table 2: Locating technology comparison

Of the two locating technologies that work practically everywhere in Europe, only GSM Cell Identification based locating has high population reachability and low cost of the infrastructure. GPS, even though it provides clearly more accurate locating, is impeded by usually not working indoors and, most importantly, not being naturally connected to any existing messaging systems.

5.3 Results

We evaluated the messaging and locating technologies in relationship to the requirements for EA sending systems presented in chapter 2. Only one pair of technologies, SMS (ordinary text message) combined with GSM Cell Identification based locating fulfil the high population reachability

criterion. This combination is also rather inexpensive, both when it comes to the building of the infrastructure and to the price of each message sent.
However, the most important criterion: "authenticity, integrity and non-repudiation" is not met with this otherwise attractive pair of technologies. There is no standard technology for authenticating SMS messages. What is worse, there is at least one, very cheap way to forge the SMS sender's number (with a pirate SIM card) and, with a rather moderate sum of money, at least one way to push fake SMS messages to a targeted area (with a rogue GSM base station that is placed e.g. in a van). (Kari, 2004)
In light of the second criterion, payload size, SMS's 160 characters per message might also be insufficient.
Consequently, no currently existing technology is an obvious choice for a mobile emergency announcement (MEA) sending system.

6 CAN THIS BE FIXED?

If none of the currently available technologies or message formats is suitable for MEA sending as is, can they be altered so that they would fulfil the criteria of chapter 2?
For message formats that are based only on the GSM network, the answer is probably "no". GSM was designed and built for confidential talk between trusted enough parties. One's number and voice together provided strong enough authentication. GSM was never designed for strong technical integrity or non-repudiation (Karila, 1997): in a human discussion one can always ask the other party to repeat what they just said.
For message formats of the now-in-launch 3G (UMTS) networks, the answer is "maybe". When networks are designed based on packet connection (as opposed to circuit connetion), authenticating becomes a small problem that has to be solved billions of times, instead of a bigger problem that must stay solved as long as a secure connection between the two endpoints is needed) (Karila, 1997). There is at least one prototype solution to packet-level authentication that should be usable in any packet-based network (Kari, 2003). It could be wise to test it also in the 3G networks as soon as possible.

For the 4G networks now on the drawing board, the answer is, in our opinion, also only "maybe". We find it likely that the network operators would want to buy networks that can create as much cash flow as possible, and that demanding features, which would provide efficient tools for authorities, are not their top priorities. If, on the other hand, features that serve the authorities can double as business necessities or advantages, the situation may look very different, indeed. But that would require the authorities to get strongly involved in the security and functionality design of mobile communications networks at a very early stage. This would require both support from legislation and funding. It remains to be seen, if this will happen.

7 DISCUSSION

The main reason for our not being able to find an already existing technology that would be usable for a MEA sending system appears to be that none of the evaluated systems or message formats have been designed with the explicit consideration of authority use. For example, SMS is just an add-on afterthought on the GSM network. Furthermore, SMS uses the GSM signalling channel, which is not guaranteed to be secure in any manner.
Many of the newer message formats have been designed primarily with more complicated end-user service concepts in mind: they are content-oriented and live or die with user popularity. When popularity in the end-user market is the driving force of design, it is unrealistic to expect the market to develop systems that just happen to be suitable for official use by the authorities, too.

8 CONCLUSIONS

Having evaluated against our full list of criteria (chapter 2), we did not find a usable existing technology for a location-based mobile emergency announcement (MEA) sending system. Contrary to what we suggested in December 2003, SMS-based MEAs proved, with closer inspection, to risk becoming a very tempting target for all who profit from a society in disarray. Using SMS-based MEAs would not be secure, and we advice strongly against them.

So, where do we go from here?

It is our belief that everywhere in the world the information market will continue to diversify and the use of personal communication devices will

increase. This will, in five to twenty years, lead to a situation where authorities can no more efficiently send emergency announcements based on currently typical media distribution channels.

It is also our belief that all single-technology solutions that make up central functions of the society are more vulnerable to malfunction and malice than technologically diverse solutions.

For efficient future civil defence we will need a family of open MEA standards, which all communicating user devices must support. Since an emergency situation most often occurs when something unexpected happens, the MEA sending systems, the authorities, the system operators and the user devices need to fluently adapt to the altered circumstances. One manner of adapting is to have many enough choices for how the MEA systems communicate. The risk for communications breaking down completely, just when they are most needed, is very real. We can minimize this risk, if we design with cooperation between authorities, independent experts and the market and with technological diversity as an explicit goal.

Acknowledgements

We wish to sincerely thank prof. Hannu Kari for patiently answering our many questions about how mobile phone networks *really* work.

REFERENCES

Act_Change, 2002. Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräiden siihen liittyvien lakien muuttamisesta. (referenced 5.4.2004) http://www.mintc.fi/www/sivut/suomi/tele/tietosuoja.htm

Act_Comm_Marc, 2003. Viestintämarkkinalaki N:o 393/2003. Available at: http://www.finlex.fi/

Act_Prepar, 2003. Valtioneuvoston asetus viestintämarkkinoihin liittyvästä varautumisvelvollisuudesta ja viranomaistiedotteiden välittämisvelvollisuudesta 838/2003. Available at: http://www.finlex.fi/

Act_Priv_Tele, 2001. Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta annetun lain 7 ja 18 §:n muuttamisesta. N:o 1148/2001. Available at: http://www.finlex.fi/

Act_YLE, 1993. Laki Yleisradio OY:stä. N:o 1380/1993. Available at: http://www.finlex.fi/

Anderson, R., 2001. *Security Engineering*, John Wiley & Sons. ISBN: 0-471-38922-6

BBC, 2002. Connecting in a Crisis - a guide to working with the BBC during an emergency. (referenced 5.4.2004) http://www.bbc.co.uk/connectinginacrisis/index.shtml

EP_EC, 2002. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. Available at: http://europa.eu.int/eur-lex/

Global2000, 2003. RAMOS Alarm-SMS. (referenced 22.10.2003) http://www.global2000.at/index1.htm?/pages/tatom_alarmsms.htm

Hanke, S., 2002. Untersuchung zur Nutzung und Aktualisierung raumbezogener Daten im Katastrophenmanagement. Dissertation zur Erlangung des Doktorgrades. (referenced 22.10.2003) http://www.kfs.uni-kiel.de/Hanke_Diss.pdf

Held, V., 1999. Technologische Möglichkeiten einer möglichst frühzeitigen Warnung der Bevölkerung. (referenced 19.11.2003) http://www.bzs.bund.de/bzsinfo/broschur/zsforschung/band42/v99-08.pdf

Kari, H. H., 2003. Packet Level Authentication (PLA). *Data Security Workshop*. 22-23 October 2003, Helsinki, Finland.

Kari, H. H., 2004. Personal communication.

Karila, A., 1997. Lectures of the course Tik-110.300 Telecommunications architectures (HUT).

Manber, U., Patel, A., Robinson, J., 2000. Experience with Personalization on Yahoo! *Communications of the ACM, 8/43, p. 35-39.*

MTV3 2004. Uutisia matkapuhelimiin. (referenced 5.4.2004) http://www.mtv3.fi/uutiset/mobiiliuutiset/

NASA SBIR, 1998. Earth Alert. (referenced 5.4.2004) http://sbir.gsfc.nasa.gov/SBIR/successes/ss/5-055text.html

SR, 2001. Sändningstillstånd för Sveriges Radio AB. (referenced 19.11.2003) http://www.sr.se/omsr/om_public_service/tillstand.pdf

STUK, 2002. Toimintakertomus ja tilinpäätöslaskelmat. (referenced 22.10.2003) http://www.stuk.fi/julkaisut/pdf/toimintakertomus2002.pdf

Taloustutkimus, 2002. Kännykkä 2002. (referenced 22.10.2003) http://www.toy.fi/data.asp?articleid=447&pgid=2

Tilastokeskus, 2002. Tietoyhteiskunta-tutkimukset. (referenced 5.4.2004) http://www.stat.fi/tk/yr/tietoyhteiskunta/

Weltner, A., 2004. Personal communication.

Wiio, O. A., 1995. What We Know About Communication in a Crisis. *IAEA Workshop on Information to the Public*. 9-12 May, 1995, Helsinki, Finland.