A GOVERNMENTAL VISION ON PUBLIC SAFETY GROUP CALLS AND OBJECT TRACING

Raphael Frank

University of Luxembourg, Luxembourg [1]

Thomas Scherer

University of Luxembourg, Luxembourg [2]

Carlo Simon

Centre de Communication du Gouvernement, Luxembourg [3]

Thomas Engel

University of Luxembourg, Luxembourg [4]

Keywords

Emergency Services, Group Call, User localisation, Telecommunication

Abstract

This work has been done within the EU integrated project u-2010 [13]. One goal of the u-2010 project is to provide interoperability over existing communication technologies for emergency and crisis situations. A concrete requirement related to this has been introduced by the National Committee on Telecommunications of Luxembourg (CONATEL) [3]: Objective is to provide push-to-talk group calls between users of different telecommunication systems, like PSTN, GSM, VoIP or radio. Further on, the system should be capable to attach specific users to a group call from a central point. Members of such group calls are mainly first responders of emergency situations, like police forces or fire brigades. Additionally, the system needs some possibility to locate these actors to be able to select the right people being able to respond as fast as possible to an emergency. The resulting application allows enhancing the communication between the different rescue entities. Using the localisation feature permits to contact users in range of the emergency and helps to improve the overall response time in case of an emergency situation.

1 Introduction

This work has been done within the EU integrated project u-2010 [13]. One goal of the u-2010 project is to provide interoperability over existing communication technologies for emergency and crisis situations. A concrete requirement related to this has been introduced by

[1] 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Raphael.Frank@uni.lu
[2] 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Thomas.Scherer@uni.lu
[3] Château de Senningen, B.P. 11, L- 6905 Niederanven, Carlo.Simon@ccg.etat.lu
[4] 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Thomas.Engel@uni.lu

the National Committee on Telecommunications of Luxembourg (CONATEL) [3]: Objective is to provide push-to-talk group calls between users of different telecommunication systems, like PSTN, GSM, VoIP or radio. Further on, the system should be capable to attach specific users to a group call from a central point. Members of such group calls are mainly fist responders of emergency situations, like police forces or fire brigades. Additionally, the system needs some possibility to locate these actors to be able to select the right people being able to respond as fast as possible to an emergency. The resulting application allows enhancing the communication between the different rescue entities. Using the localisation feature permits to contact users in range of the emergency and helps to improve the overall response time in case of an emergency situation.

Like for many real time applications, one challenge is to deal with latency caused by the transition from one network technology to another. An acceptable Quality of Service (QoS) needs to be guaranteed. Beside the technical part, there will probably be different political or legal issues, especially for the localisation.

The core of the application relies on a centralized call manger which is directly connected to a database called SPHERE (Single Physical Heterogeneous Emergency Response Environment). It contains up-to-date user information which is periodically retrieved from different external databases (Fire brigade, Police, etc), like contact information, the availability and optionally the location of the first responders to be contacted in case of an emergency situation. The group calls are initiated and managed from the head quarter. Push-to-Talk over IP is used to provide interoperable group calls as it allows voice communication over IP based networks.

For the localisation feature several conceivable techniques exist. The Global Positioning System (GPS) is the most common method. However, an additional communication channel is needed in order to transfer the position to the SPHERE database. As only few devices are equipped with a GPS receiver, other, less accurate techniques need to be considered, as well. This includes GSM cell localisation and localisation of a fixed phone jack. The object tracing feature is included in the front end to provide a high level tracing interface.

2 Group Call Architecture

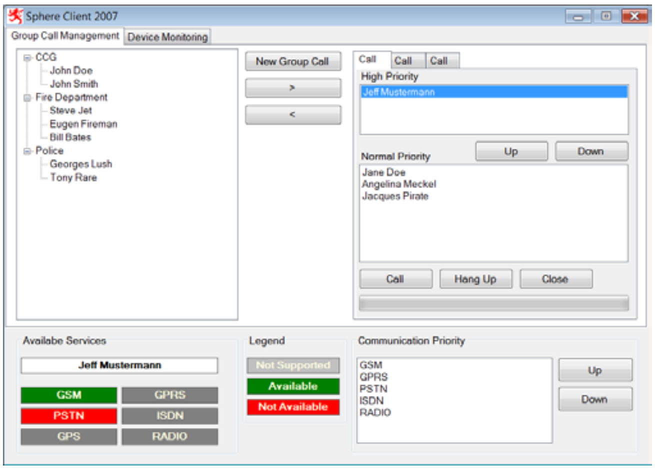

Figure 1. Call Center Application

A major requirement of the National Committee on Telecommunications of Luxembourg is the possibility to setup group calls between users, whatever communication possibilities they currently have, like PSTN, GSM, Internet access or police radio. The scenario is the following. Due to an incident detected by an entity like a 911 call service, first responders need to be contacted in such way that they are able to synchronize their working tasks. If necessary, the call service selects supplemental users to be contacted and establishes a group call architecture among them.

Which users to be involved in a group call depends on the tasks to fulfil and in case of emergencies mainly their position to achieve a fast response to the event. The application depicted in Figure 1 is the front end being used by the call centre to launch the group call. A tree of users is presented on the left side. This tree and their availability are obtained by the SPHERE database. A new group call can be initiated by pressing the "New Group Call" button. Afterwards a new tab will appear on the right side of the window. There it is possible to insert the users, who will join the group call. Two kind of group call members may exist defined by the priority the user have during the group call. Normal Priority users are provided with a Push-To-Talk like communication channel, which allows only one to talk at a time. High Priority Users are provided with a bidirectional communication channel allowing them to interrupt Normal Priority Users.

Active group calls are managed from the central service. Some of them belong to the daily operation and therefore exist permanently. It will be possible to dynamically add new users to the an ongoing call. The term user in this work does not necessarily refer to a physical person. A user may also represent an entity like a police car providing communication facilities capable to participate in several group calls.

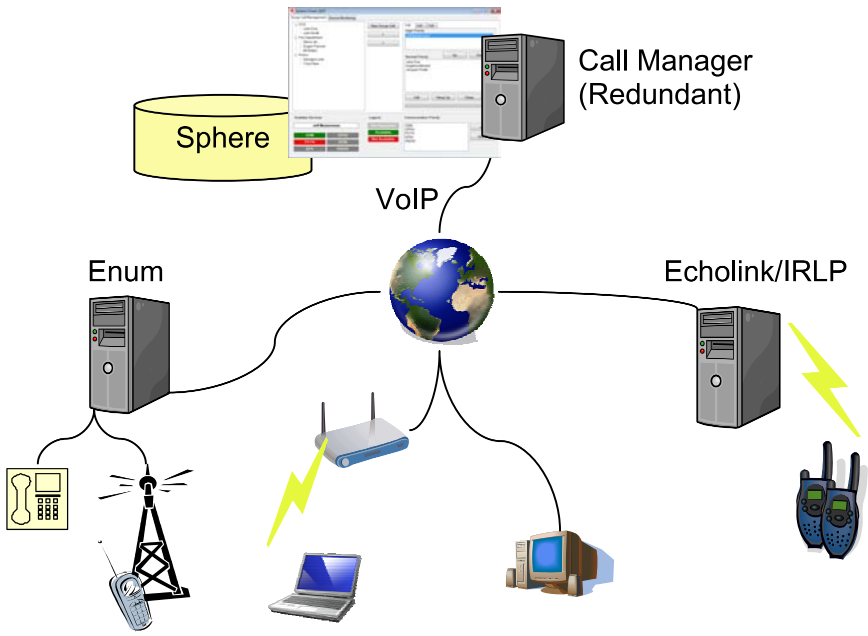

Figure 2. Group Call Architecture

The communication technology is mainly provided by Voice-over-IP (VoIP) as it allows the interoperability between the voice communication technologies. Enum server [5] allows the translation of PSTN phone numbers. Echolink [4] allows interoperability between amateur radio and VoIP but may also be used for police radio. In its easiest version it receives the radio signals via an audio-in of a sound card and translates it afterwards to VoIP.

The group call architecture is shown in Figure 2. The group call is managed from a server denoted in Figure 2 as Call Manager. It establishes the VoIP streams to the various users and relays the voice information between them. Such servers do already exist, like [1], but usually they are designed in such way to only provide the conference call platform. User may join a conference call after it has been checked whether they are authorized. So, people call the system to join. Here it is also possible to centrally call and add users to the group call. If existing conference call systems are used the users is called from the call manager. Afterwards, the call is handed over to the conference call system.

The call manager needs to relay incoming voice streams to all group call participants. For doing this it needs to consider the sender's priority sending the stream. In case it is a normal priority user, the stream is only forwarded if no other stream is currently processed. Only streams originated by high priority users are forwarded in any case.

3 User Localisation

To be able to enhance the response time of emergency services, it is important to know the location of the rescuers registered to the system. Having this information enables to create task forces of people in range of an incident. Upon the task forces, group calls can be launched in order to let the different people organize their actions.

SPHERE keeps track of the units which might be on the move. This allows taking preventive actions like for instance calculate the approximate arriving time of an ambulance at the hospital. The headquarter can this way monitor in real time the different units and take additional initiatives.

Figure 2 illustrates the different localisation possibilities used by SPHERE. Following subsections will briefly explain the basic mode of operation of each technology and how it fits in the context of the application.

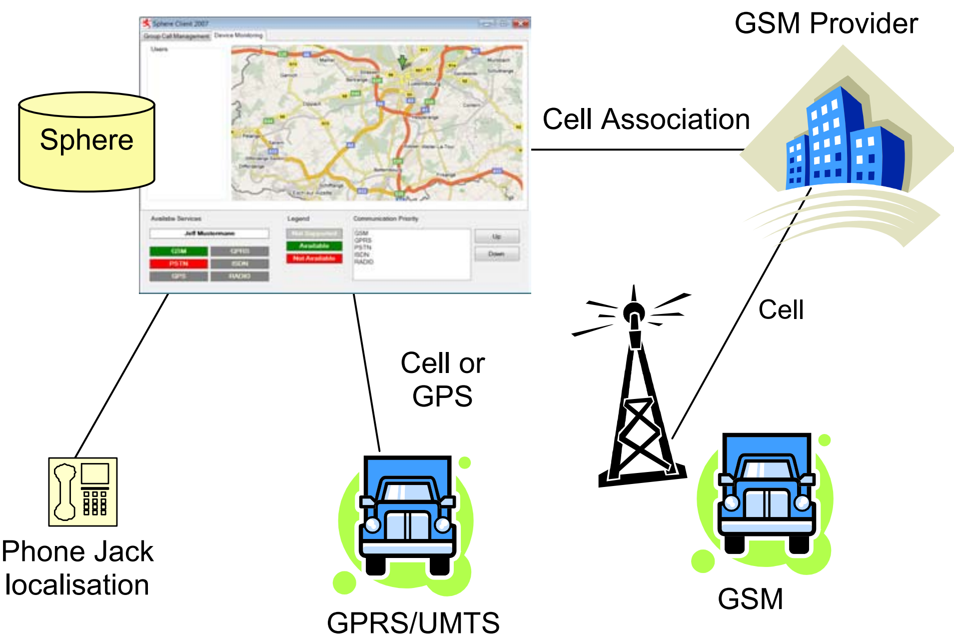

Figure 3. Object localisation architecture

3.1 Using Mobile Phone to Determine the Location

There are multiple possibilities to determine the location of mobile phones. The easiest and most common method is the Cell Identification [7]. Knowing on which cell the mobile phone is registered gives localisation accuracy from a few hundred meters in urban areas to several kilometres in rural areas. However it remains a very useful technique as it is often only necessary to know approximately in which area a certain user is located.

Another method called Time-Advance or Time of Arrival [7] gives more precise location information. It is based on the round-trip delay that can be used to measure the distance between the mobile device and the base station.

Triangulation [7] is another advanced method to determine the exact location of a mobile device using at least three base stations. The round-trip times to the different cells are compared in order to determine the location. The disadvantage is that the telecommunication providers need to install additional systems in order to provide such a service. The triangulation method is cumbersome and pretty probably limited to only localize victims.

A major advantage of mobile phone localisation is that there is no need to have a dedicated communication channel to transfer the location information back to the headquarter. However a close co-operation needs to be setup with the telecommunication provider in order to retrieve the needed data from their data repository.

3.2 Using the Global Positioning System (GPS) to Determine the Location

The most commonly used localisation system is GPS [6]. Many mobile devices are equipped with GPS receivers allowing them to determine the position with an accuracy of approximately 15 meters.

The disadvantage of GPS is that the location coordinates need to be transferred back to the headquarter in order to be evaluated. This is only possible if there is a networking technology available (GPRS/UMTS). Additional software needs to be developed and installed on the concerned mobile devices in order to perform this step automatically. Basic XML messages can be used as an envelope to periodically transfer the coordinates together with a timestamp to centralized server. It is likely that in the near future this kind of localisation technique is the prevalent one. In case no packet switched technology is available, the coordinates can be send to SPHERE via SMS or similar.

4 SPHERE

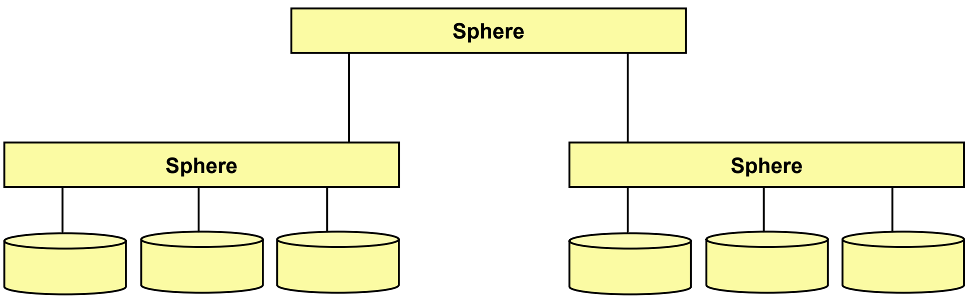

Figure 4: SPHERE Architecture

The purpose of SPHERE is to provide up to date contact information of users playing an active role in case of an emergency. The contact information includes the personal information such as name, address, affiliated rescue service, as well as additional information on individual skills, which might be important in given emergencies. The most important information is the different contact possibilities that the user might have. For instance a fire-fighter might have following communication possibilities: Fixed analogue phone, private mobile phone, radio device. This information can be seen as the static data which is not frequently changed. The dynamic part of the data gives information about the availability/reachability of the different communication possibilities at a concrete point in time. This can be achieved by evaluating information as working plans and location of a certain rescuer.

Such a data repository can only be created if it is continuously feed with up to date information. This information usually exists in the databases of the different institutions that take part in rescue operations.

To be able to use these sources for the group call and localisation technique introduced before the data needs to be transformed from the corporate data structures into a common language in such way that the group call and localisation functionality can be used across public safety institutions. Hence, SPHERE can be considered as a middleware providing a generic access to the existing databases.

Especially in case of emergency situations on the border between different administrative areas, it might become necessary to achieve interoperability across SPHERE systems. So, it is possible to provide group calls across county or country borders and to achieve a better organization of task forces. The target architecture is shown in Figure 4. SPHERE provides an interface to existing data sources on the one side but is also able to interconnect different SPHERE Systems in a hierarchical or non-hierarchical manner.

5 Future Work

Accessing external databases is one of the issues that need to be solved next. It can be seen as a political or legal problem rather then as a technical challenge. Strong security mechanisms need to be included in order to provide an architecture, which is conceivable to operate across institutional boundaries..

Another concern is the single point of failure (SPoF) which occurs when the SPHERE database fails or becomes unreachable. Hence, a certain amount of redundancy needs to be provided. This redundancy can be further utilized to better protect the system against unauthorized insight by disseminating the information in such way that the information is partly distributed among redundant parts. This can be achieved by using threshold cryptography. Using a *(k, n)* scheme [11] allows dividing SPHERE in *n* different shares. To reconstruct the data *k* of *n* shares are needed. The difficult relies in dynamically updating the shares. Additionally such a procedure would create a tremendous management overhead. Nevertheless, the concept behind secret sharing distributed databases looks promising [8].

Considering possible terrestrial network failures, satellite links will be used to provide backup connectivity. This redundancy solution will become the main link for out of area operations, like rescue operations after an earthquake in a foreign country. Users will enjoy the full services of SPHERE in any remote area.

A generic middleware can be used on top of the security protocols in order to interface the different external data source. Projects like Oasis [9] and Orchestra [10] are working on solutions that could directly be incorporated in the application. As a first step, their will be an implementation of a demonstrator using Web services, which manage the data exchange between the different actors.

6 Related Work

In case of an emergency application a good balance need to be found between security and performance. Web Services will be used as a first step to build a "Prove of Concept" demonstrator. There are related projects like OASIS [9] which provide extended web services that can be used for that purpose. It is an XML based Simple Object Access Protocol (SOAP) [12] which provides a basic messaging framework.

More advanced interfaces can be realized using middleware adapters. Orchestra [10] is one of the major projects in this research area. It provides an platform independent open architecture for spatial data infrastructures. It was specifically designed for risk management applications. The integration of the middleware component is planned as a next step in the implementation process.

To be able to directly communicate with the on site rescue units, a mobile router can be used. Cisco Systems [2] is currently testing a prototype named "Mobile Access Router" (MAR) which allows interconnecting different networking technologies in order to achieve transparent communications. It is conceivable to relay the radio transmission of the rescue units using such a device as gateway.

7 Conclusion

Communication is one of the major issues in case of an emergency situation. Improvements need to be made in this area in order to enhance the cooperation of the different rescue units.

The application presented in this work provides a powerful communication and localisation tool that can be used for that purpose. The group call feature allows a better organisation of the different emergency services. The localisation and tracing feature allows contacting relevant units near the incident and monitoring their actions. The response time could be significantly improved which might save lives.

Such an application can be implemented relatively fast. The difficulty is to find an agreement with the different organisation that need to provide access to their databases in order make it work.

References

[1] ASTERISK. (2007). *Asterisk - An Open Source PBX and telephony toolkit*. http://www.asterisk.org/. Last Accessed 18 February 2007.

[2] Cisco IPICS. (2005). *Solutions for Communications Interoperability.* White Paper. http://www.cisco.com/en/US/products/ps6718/products_white_paper0900aecd80350fee.shtml . Last Accessed 17 February 2007.

[3] CONATEL. (2001). *National Committee on Telecommunications of Luxembourg*. http://www.legilux.public.lu/leg/a/archives/2001/0701906/0701906.pdf. Last Accessed 18 February 2007.

[4] ECHOLINK. (2007). *echolink.org*. http://echlink.org. Last Accessed 18 February 2007.

[5] ENUM. (2006). *Electronic Numbering*. http://www.enum.org/. Last Accessed 12 February 2007.

[6] HowStuffWorks. (2007). *How GPS Receivers Work*. http://electronics.howstuffworks.com/gps1.htm. Last Accessed 17 February 2007.

[7] IIg, D. and Fitzi, A. (2007). *Location Based Services*. http://www-t.zhwin.ch/kurs/kn/fileadmin/mounts/kn/vortraege/Location_Based_Services_handout.pdf. Last Accessed 28 February 2007.

[8] Miyamoto, T. (2006). Vertical Partitioning Method for Secret Sharing Distributed Database System. *IEICE Trans. Fundamentals*, Vol. E89-A, No. 11 November 2006. Osaka, Japan.

[9] OASIS. (2006). *Oasis Emergency Management TC*. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency. Last Accessed 13 February 2007.

[10] ORCHESTRA. (2007). *Orchestra Open Architecture and Spatial Data Infrastructure for Risk Management*. http://www.eu-orchestra.org/. Last Accessed 10 February 2007.

[11] Shamir, A. (1979). "How to share a secret". *Communications of the ACM,* Vol. 22, No. 11, pp. 612-613.

[12] SOAP. (2003). *Simple Object Access Protocol W3C Specifications*. http://www.w3.org/TR/soap/. Last Accessed 17 February 2007.

[13] u-2010 Project. (2007). *Ubiquitous IP-Centric Government & Enterprise Next Generation Network.* http://www.u2010.eu/. Last Accessed 21 March 2007.

Author Biography

Raphael Frank was born in Luxembourg, on August 25, 1982. He received his industrial engineering diploma followed by a Master degree both in computer science form the University of Luxembourg (2005), respectively from the University Joseph Fourier, France (2006). He is currently Ph.D. candidate at the University of Luxembourg. His area of research interests includes security in wireless networks. He is a member of the EU funded integrated project u-2010.

Thomas Scherer obtained his diploma in computer science from the University of Trier, Germany in 2005. He is currently finishing his Ph.D. thesis in the area of sensor and mesh networks. His research interests include wireless telecommunication and information security. Thomas Scherer is member of the EU funded integrated project u-2010.

Carlo Simon is Lt. Col. of the Luxembourg army. Trained in Belgium and in the US, he is today in charge of the governmental communication centre of Luxembourg. At this time, he is also heading the national committee of telecommunications.

Prof. Dr. Thomas Engel is Professor for Computer Networks and Telecommunications at the University of Luxembourg. He studied Physics and Computer Science at the University of Saarbruecken, Germany, where he graduated in 1992 and received the title Dr. rer. nat. in 1996. 1996 – 2003 as joint founder he was member of the board of directors and vice director of the Fraunhofer-guided Institute for Telematics e.V. in Trier, Germany. Since 2002 he teaches and researches as a professor at the University of Luxembourg. Prof. Dr. Engel is member of the European Security Research Advisory Board (ESRAB) of the European Commission in Brussels advising the Commission on the structure, content and implementation of the future Security Research Programme and also member of the Security Taskforce of the European Commission in Brussels. He also is the coordinator of the European Integrated Project u-2010 with 16 partners on the subject of Next Generation Networks.