Interoperable Networking Applications for Emergency Services

Raphael Frank[1] , Benjamin Hourte[2], Dan Jungels[2], Thomas Engel[1]
[1] *University of Luxembourg, 1359 Luxembourg*
[2] *HITEC Luxembourg, 1458 Luxembourg*
{Raphael.Frank; Thomas.Engel}@uni.lu, {Benjamin.Hourte; Dan.Jungels}@hitec.lu

Abstract

Efficient communication is a major requirement in crisis situations. This research is motivated by the need to develop new communication tools to enhance the coordination and response time of first responders. In this paper we present an application which enables group calls among different rescue entities. Additionally, we present a video application that provides a real time access to surveillance cameras. The objective is to provide a powerful communication tool that can be used over different network technologies. As opposed to other existing systems, our application provides a complete communication platform that relies on open standards. A prototype has been implemented and tested during a demonstration held in July 2007 in Luxembourg. In this paper we provide technical details on how the applications were realized and evaluate the outcome of the demonstration. We also propose future improvements based on the outcome to enhance the system.

1 Introduction

This work has been done within the integrated EU project u-2010 [1]. One goal of u-2010 is to provide interoperability of existing communication technologies for emergency and crisis situations. A concrete requirement has been introduced by the National Committee on Telecommunications of Luxembourg (CONATEL) [2]. Objective is to enable group calls between users of different telecommunication systems, like PSTN, GSM, VoIP and radio. Further on, the system should be capable to attach specific users to a group call from a central or remote point. Members of such group calls are mainly first responders of emergency situations, like police forces or fire brigades. The resulting application should allow to enhance the communication between the different rescue entities. Another application that has been demonstrated is a video platform that provides real time access to surveillance cameras. The technical innovation of the system is that it can be used seamlessly over different network technologies, meaning that rescue services can access the video streaming wherever they are without being disconnected when switching the networks. Current communication technologies [3] used by first responders are mostly standalone and do not provide “out of -the-box” interoperability between other network technologies. During the last few years only little research has been conducted in that area. Cisco Systems developed a proprietary system called IPICS [4] that acts as a gateway between different voice technologies. Other more specific systems have been proposed to enhance communication in mountain rescue operations [5]. In our approach, we focus on a general communication platform that can be used for all kind of rescue operations where coordination between different rescue entities is needed. Additionally, our solution relies exclusively open standards in order to encourage collaborating work and facilitate future improvements. In order to prove the feasibility of such a system, a demonstration was held in July 2007 in Luxembourg. A car crash was simulated in a highway tunnel. The overall demonstration included three distinct parts. The first two provided video and voice services for first responders. The latter presented a victim tracking and tracing system. In this paper we will focus on the voice and video parts of the demonstration and provide technical details on how the applications were realized. Thereafter we will analyze the outcome of the demonstration and propose future enhancements. The paper is organized as follows. Section 2 summarizes briefly the storyboard of the demonstration. Section 3 describes technical details of the Voice Infrastructure followed by the technical details of the Video Infrastructure in Section 4. In Section 5 we will evaluate the outcome of the demonstration and propose improvements. In Section 6 the future work is motivated. Conclusions are drawn in Section 7.

2. Storyboard

To understand how the audio and video systems can be used in emergency situations, we will briefly introduce the different steps simulated in the demonstration. The scenario is as follows: A car accident is detected in a highway tunnel by surveillance cameras. First responders are alarmed and send to the crash site. During the entire way from the fire brigade to the crash site, the first responders have access to the video camera located near the accident sing mobile devices such as PDAs, Laptops and Smart Phones. This includes three steps: At the headquarter; the first responders connect through a Wi-Fi Access Point (AP) to the Internet to retrieve the video streaming of the crash site. On their way to the tunnel, the video is retrieved via a 3G (UMTS/HSDPA) connection. Finally, at the tunnel the streaming continues using a satellite over IP connection. Arrived at the crash site, two firemen equipped with IP radio devices are automatically connected to the system via an AP.A coordinator located at the headquarters initiates a group call among them. The coordinator participates actively to the group call and may add or remove users on the fly. After evaluating the situation, one of the firemen requests medical support. A military tent is erected in the area around the tunnel in order to take care of the heavily injured victims. Additionally, an ambulance is requested to carry the lightly injured persons to the hospital. Once the military tent has been deployed, a doctor is added to the group call to inform the firemen that medical stuff is ready to take care of the injured people. The next actor added to the group call is the ambulance driver who is still on the road to the tunnel. He is called on this standard mobile phone and informs the other participants of the expected time of arrival of the ambulance. Finally, other involved first responders alternately dial into the group call to provide additional information or to check the current status. Remote users will use their standard mobile phone to dial-in. User on site will be able to choose between IP and GSM. Due to the quick response time and efficient information flow, the situation is rapidly under control. The call coordinator can now terminate the group call.

3. The voice infrastructure

The group call system is based on a centralized client-server model. This allows concentrating all emergency relevant information in one central point to obtain a better view on the crisis situation. The voice communications which are relayed through the central server can easily be stored and used for post evaluation of the emergency situation. The outcome can be used to enhance the procedure for future operations. The central entity used in the concept, is a Voice-over-IP server (VoIP) based on the open source software Asterisk [6]. The server is equipped with a additional Primary Rate Interface (PRI) cards1 to connect to PSTN/ISDN and GSM networks. The purpose of using such a setup in emergency situations is to interconnect the VoIP communications with traditional circuit switched communications. Standard features such as group calls are provided 1Digium TE120P in E1 mode (30 channels) and managed by the VoIP server. Using IP as central addressing protocol allows to easily build monitoring and coordination tools. Figure 1 gives a high level overview of the group call architecture.

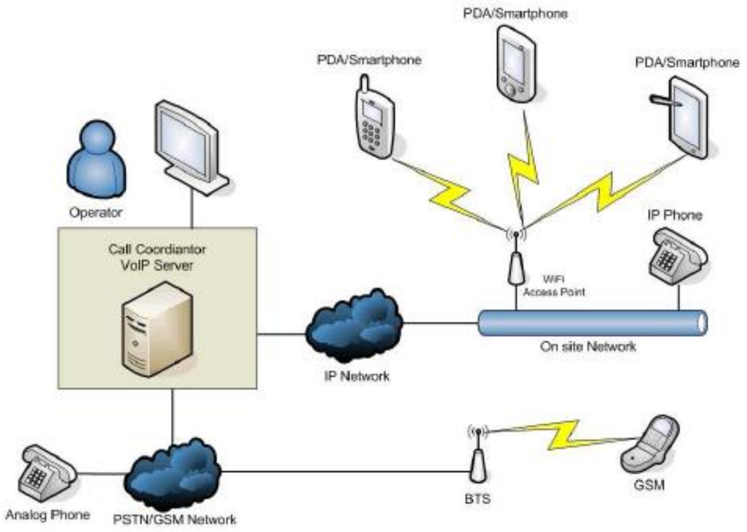


Figure 1. Group Call Concept

The main problem of a centralized architecture is the single point of failure (SPOF) which is the link to the VoIP server. If this link fails, the group call system will stop working. Redundant paths cannot always be guaranteed, additional mechanisms need to be considered. Ideas on how this can be done will briefly be discussed in Section 5.

3.1 Components

The different network and server components were installed on two different sites. The first is the demonstration site located in front of the tunnel entrance. The second is the u-2010 hosting center which provided the needed network interfaces. Figure 2 illustrates the different components and how they are interconnected. The central VoIP server was installed in the u-2010 hosting center where it was connected to the Internet via a gigabit backbone and to the circuit switched network using an dedicated E1 line. The other equipment was located at the demonstration site. The emergency management headquarter, was established at the tunnel entrance for demonstration purposes. In order to connect back to the central VoIP server, a 2Mbps synchronous DSL line was installed. Due to the lack of public IPv4 addresses, a Virtual Private Network (VPN) was used to allow the different network components to communicate with each other. The VPN gateway, located at the headquarter, provided all the needed services to the client devices at the tunnel. This allowed the client devices to connect to the network in a plug'n'play manner. The communication between both sites was realized via public Internet. As this link is vital for the operation of the system, it was mandatory to protect it against attacks. Using a VPN has the advantage to provide an encrypted communication channel by default. Local sub-networks were created for the different services. The voice network was further divided in two categories. One for the wired end-devices and the second for the wireless end-devices. The fixed IP phone was located inside the military tent. The other IP based end-devices automatically connected via a secured AP to the system. In order to provide best Wi-Fi coverage on site, the AP was deployed at the entrance of the tunnel. Figure 3 summarizes the location of the different entities around the tunnel. The Non-IP end-devices used for the demonstration were standard GSM mobile phones.

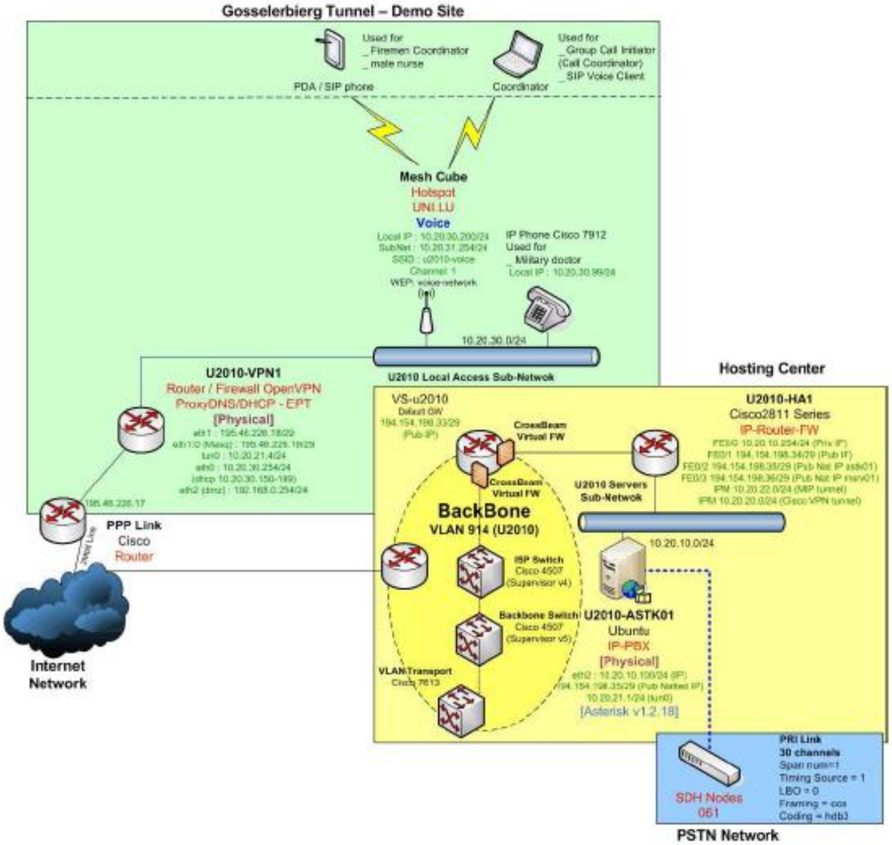


Figure 2. Group Call Architecture

They connected via the Base Transceiver Station (BTS) back to the VoIP server where the communication was linked to the group all. Other circuit switched network terminals like PSTN or ISDN phones could have been included to the group call in a similar way, but for demonstration purposes we choose to only use GSM. 3.2 Group call establishment Central part of the group call system is the call coordinator software. It is a Java based client application which allows the initiation, management and termination of multiple group calls. The application allows to drag and drop known users in a list in order to establish a group call among them. User specific information is retrieved from the central server using the Session Initiation Protocol (SIP) [7]. In our concept, SIP is used as central signaling protocol. It is reliable application layer protocol used to control sessions between one or more participants. Currently SIP is supported by most IP based end-devices. This is one of the major advantages of using such devices for the group calls. Once the clients have registered at the server, the call coordinator application is informed via SIP about the status of the users. Other services like instant messaging or video can easily be added using SIP as signaling protocol. Status information is not available for GSM users. However phone numbers stored in the database of the VoIP server are retrieved the same way. Additionally, the call coordinator application allows to remotely create new users. Another advantage of SIP is the flexibility of the packet header [8]. The so called extension header can be used to transmit custom parameters. One example of such a custom header can be found in figure 4. This SIP message was send from the call coordinator to the VoIP server. The packet is addressed to the extension 667. This extension acts as a hook to intercept custom SIP packets. Two custom parameters are contained in the header.

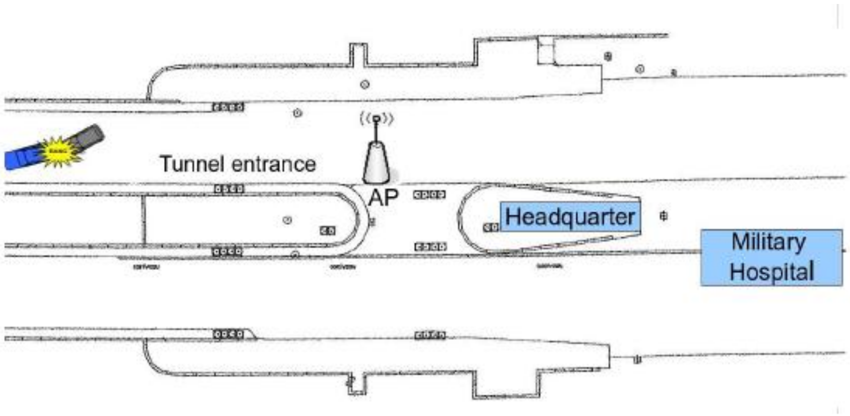
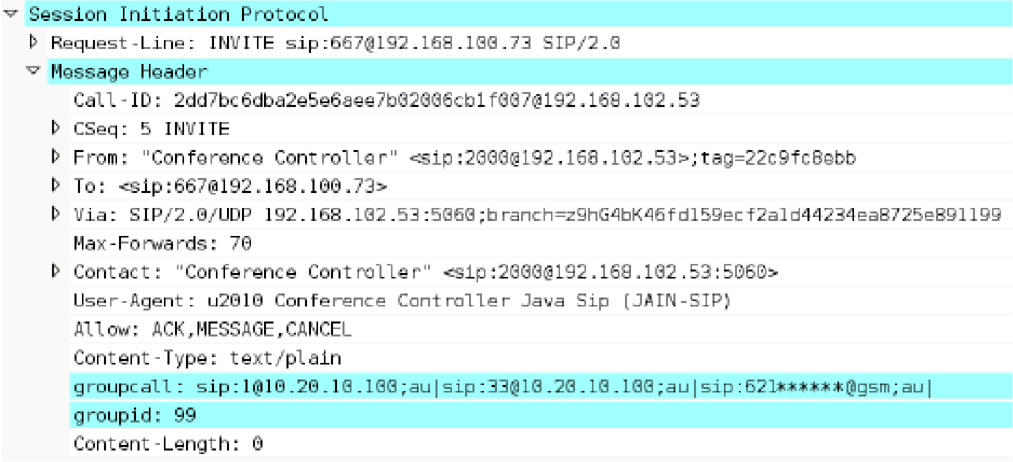


Figure 3. Tunnel Map

The first is a list of the users to be added to the group call and the second denotes conference call extension. Those parameters are parsed using the Asterisk Gateway Interface (AGI) [9]. The resulting information can be used to initiate a group call among the requested users. The software used by Asterisk to create group calls is MeetMe. It is a built-in module that provides all the needed configuration options.



```
▽ Session Initiation Protocol
  ▷ Request-Line: INVITE sip:667@192.168.100.73 SIP/2.0
  ▽ Message Header
      Call-ID: 2dd7bc6dba2e5e6aee7b02006cb1f007@192.168.102.53
    ▷ CSeq: 5 INVITE
    ▷ From: "Conference Controller" <sip:2000@192.168.102.53>;tag=22c9fc8ebb
    ▷ To: <sip:667@192.168.100.73>
    ▷ Via: SIP/2.0/UDP 192.168.102.53:5060;branch=z9hG4bK46fd159ecf2a1d44234ea8725e891199
      Max-Forwards: 70
    ▷ Contact: "Conference Controller" <sip:2000@192.168.102.53:5060>
      User-Agent: u2010 Conference Controller Java Sip (JAIN-SIP)
      Allow: ACK,MESSAGE,CANCEL
      Content-Type: text/plain
      groupcall: sip:1@10.20.10.100;au|sip:33@10.20.10.100;au|sip:621******@gsm;au|
      groupid: 99
      Content-Length: 0
```

Figure 4. SIP packet

Once the group call is initiated, it remains possible to add or remove users from the ongoing conference using SIP messages. Additionally, it is possible for users known by the system to individually dial into the group call. The initialization of a group call is handled as follows: The conference is initiated by the call coordinator by sending a SIP message to the VoIP server. This SIP message contains among other things a list of users and their contact information. An INVITE request is then send from the server to the different IP based users using SIP messages. For the Non-IP based users a standard call is placed. Once the IP based users have accepted the call, the real time voice traffic is send using IP unicast to the centralized VoIP server which relays the data to every single group call participant. In order to reach the Non-IP based users, the different VoIP streams are multiplexed, converted to an analog signal and send via PSTN/ISDN/GSM network to the respective users.

4. The video infrastructure

The existing CITA [10] video surveillance infrastructure was used as video source. We used the normal switching facilities in place: no part of the existing production system had to be changed, we only added some additional infrastructure not interfering with the system already in place. The video was available through the CITA surveillance center as an analogue CVBS signal. To get the signal back to our mobile devices, an encoder server as added to re-encode this signal according to our needs. Please note that we have chosen not to use the original digital signal because first the bandwidth is way too high (several megabits), and in addition we wanted not to influence the production system by letting some clients connect directly to this infrastructure. For this first demonstration we have chosen the Windows Media 9 format, because encoders already exist on the market for some time and are heavily used in other projects. This made it possible to quickly set up a working system. A second reason was the possibility to encode multiple bitrates, and the ability for the terminal to switch dynamically between them according to the available bandwidth. This switching is possible without interruption of the video streaming, which fits very well our requirements. During the demonstration we encountered some problems with the Windows Media format due to incompatibilities of some devices to stream dynamic bit rates. This issue needs to be analyzed in more details. The encoder server was using an Osprey capture card. This card was chosen because of good references, and Linux compatibility. Even though we have used an Windows XP machine for the demonstration, it is still possible to use it at a later point in time with other encoding software under Linux.

4.1. Data flows

The video data flow came from the media encoder at the CITA headquarter over the VPN connection back to the u-2010 hosting center. The streaming server took as input, the newly formatted video from the encoder. It then distributed one of the video streams over the Mobile IP [11] tunnel of the Mobile Access Router (MAR) [12] at the tunnel to the different video clients. For the video part, there was no direct connection from a mobile terminal to the encoder PC in the CITA headquarter. The switching of the video was made using an XML-RPC [13] connection directly to the media encoder running a switcher gateway.

4.2. Functional management

The operator switching the video to be shown in the fire engine was at the tunnel during the demo. In a real deployment, this will most probably be a CITA operator, or a trained operator at the fire brigade headquarters. In an emergency situation firemen have no time to operate the video terminal and switch between cameras to find out which one gives the best information.

4.3. Server and network node usage and distribution

The encoder server was located at the CITA headquarter. For the demonstration we set up a VPN tunnel to our private U-2010 network, to be able to reach the streaming server, and for the clients to be able to reach the camera switcher gateway. The encoder server was also connected to the CITA network to be able to switch the cameras, if requested by the video terminal. A streaming server (Windows Server 2003) was located in the backbone of the Hosting Center. At the tunnel, a normal laptop and two ultra mobile PCs (UMPC) were used to show the video. One UMPC device and the laptop were mounted in the fire engine, together with the networking equipment. The second one was used as portable terminal outside of the fire engine.

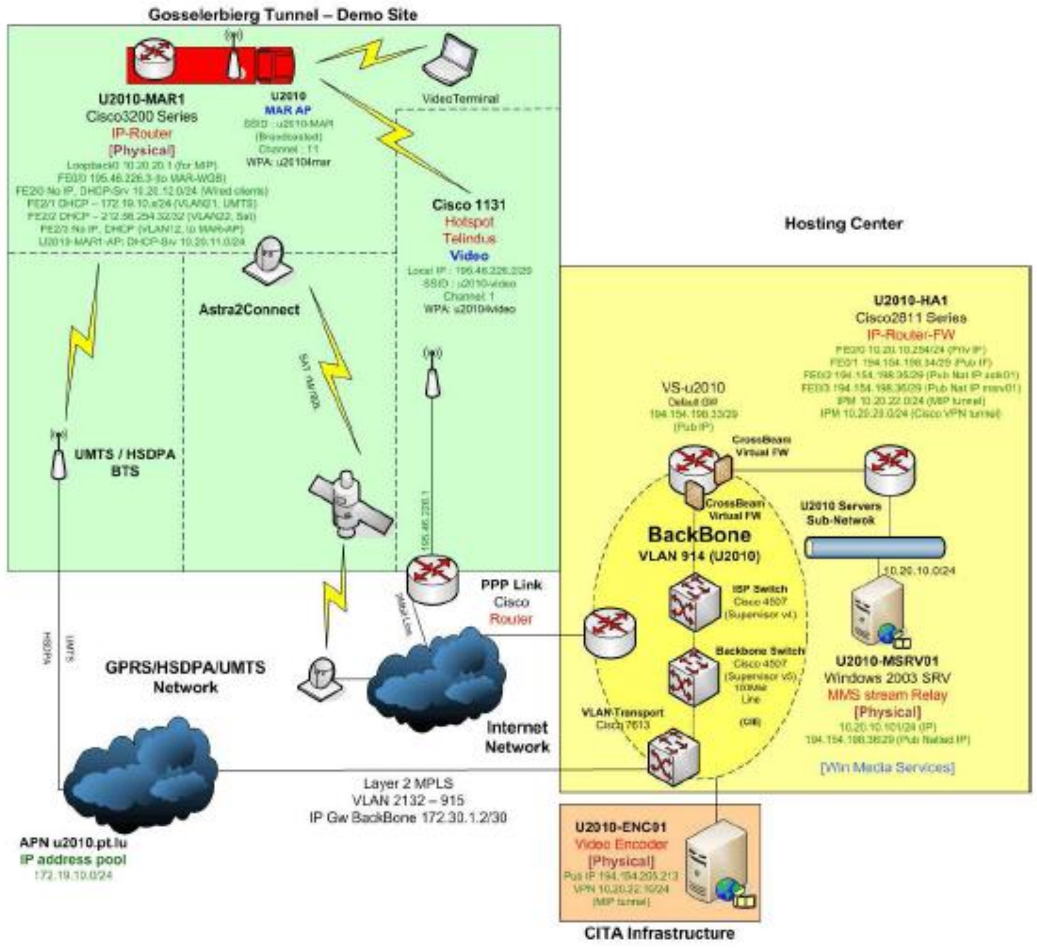


Figure 5. Video Architecture

To be able to connect the mobile video equipment to the streaming server, a Mobile Access Router (MAR) was set in the fire engine. This MAR set up a Mobile IP tunnel to the Home Agent, located in the same network as the streaming server in the Hosting Center. The following network technologies were used by the MAR:

• **802.11g wireless LAN:** Used to simulate the fire brigade headquarter, or an urban area where public hotspots are available. In general this technology should have the highest priority (i.e., it should be used first whenever available). During the demo, the priority was changed to have a lower priority as the satellite; otherwise the satellite would not have been used by the MAR, because during the demo at the location where the satellite terminal was installed, there was also wireless LAN coverage.

• **3G UMTS/HSDPA:** Used for the video transmission while the fire engine was on the road. It was configured in the MAR to have the lowest priority, meaning that it is used when no other network connection is available.

• **Satellite connection:** Used on the tunnel location to have a high bandwidth connection, even when local systems are unavailable because of damage of the base stations (e.g. fire), or when overloaded because too many people are using them at the location of the incident. The micro-VSAT was configured in the MAR to have the highest priority, meaning that as soon as the fire engine arrived at location, and the Ethernet cable was plugged into the router, the MAR switched to this connection. The MAR provided network access to its clients using a wired Ethernet connection (Ethernet switch mounted in the fire engine) and using a Wireless LAN 802.11g connection.

4.4. Video devices

As video device with camera switching capabilities a normal Windows XP based laptop was used in the fire engine during the demonstration. This laptop showed the video in high resolution and a map with available cameras that could be selected by an operator. In addition, a Windows CE based UMPC was used to show the video. On this device it was not possible to switch the cameras; it always showed the video selected by the laptop computer. The used mobile devices were two Gotive H42 [14]. One device was mounted with the corresponding docking station in the fire engine and was connected with an Ethernet adapter (USB over docking station) to the MAR. The second device was used outside of the fire engine for demonstration purposes to the public. It was connected with a wireless LAN connection to the access point provided by the MAR.

5. Lessons learned

In this section we will evaluate the outcome of the demonstration and propose solution that can be used to improve the system. First of all, for both applications using a VPN to enable the communication between the remote sites introduced an enormous overhead in terms of processing time and configuration effort. Using IPv6 as addressing protocol will solve this and other issues. More information on IPv6 and how it will be used will be given in subsection 6.1. For the video demonstration, most features worked as planned. The only noticeable issue was that some mobile client devices did support dynamic bitrates streaming. For the audio demonstration, one of the major problems was the inadequate end-devices carried by the firefighters for the audio communication. Small buttons and a sensible touch screens are not suitable for firefighters wearing big gloves. One possibility to overcome this problem is to interface the TETRA [3] radio system with the group call application or to use ruggedized devices such as the ones used for the video demonstration. The second problem came from the full-duplex property of the voice communications. Every participant was able to use the communication channel simultaneously which often resulted in confusion. To guarantee an acceptable level of Quality of Service (QoS), parameters like the right voice codec need to be chosen carefully. In our setup the voice communication need to be propagated through different networks with different properties (bandwidth, delay, jitter, etc.). A compromise need to be made between bitrates and processing time. End-devices need more time to process highly compressed audio codecs. An additional delay is introduced by the VPN Gateway. All together results in a unacceptable delay of the voice communication. On the other hand choosing a codec with a high bitrates may result in bandwidth insufficiency if too many users participate to the group call. The previously described problems often result in communication echoes. Using the hardware echo canceller of the VoIP server helps to improve the quality of the communications but in some cases it remained insufficient. One solution to overcome most of the previous problems is to use a Push-To-Talk (PTT) like communication system on top of the group call application. This would allow to conduct a structured conversation between the group call participants, reduce the network load as only one voice stream is propagated trough the network at the time and reduce the echoes as every participant is muted by default. The difficulty is to provide a system that can be used over the different network technologies. One solution is to use Dual-Tone Multi-Frequency tones (DTMF) [15]. It specifies a set of standardized analog tones that can be used as control messages over multiple network technologies A prototype has been implemented and is currently being tested. Another problem is the single point of failure (SPOF) of the centralized architecture. If the link to the central server fails, the current group call system will stop working. In order to avoid such a situation an *offline model* needs to be conceived to provide a minimum of communication capabilities. In this mode it should still be able to use local IP voice services. This can be realized using SIP as signaling protocol. Local IP clients would still be able to participate to a group call using multicast or broadcast as transmission method. A practical limitation of this concept is the transmission range of the WiFi AP. In order to increase the coverage of wireless networks, so called wireless multi-hop networks can be used. They are composed of multiple wireless nodes which are used as routers to propagate data through the network. Concepts like [16], [17] and [18] can be used to efficiently spread audio streams through such kind of wireless networks. Such a system could then be used in areas where no communication technology is available or was destroyed. This research topic is currently being analyzed and further results will follow soon.

6. Future improvements

In addition to the enhancement described in the previous section, two major features will be added to the next version of the group call application. The first is to use IPv6 as addressing protocol for audio and video. The second is to interface the TETRA radio system with the VoIP server. Those features will be shown in the next public demonstration which is planned for mid 2009. 6.1 Global connectivity using IPv6 The network setup remarkably showed the need for IPv6 for interoperable public safety communication. The absence of sufficient amount of globally routable IP addresses requires the usage of a VPN tunnel to bridge networks. This not only has a negative influence on the overall QoS, it also reduces the ability to adapt to changing network situations fast. For instance, one may conceive that a mobile end-devices migrates to a different network but still should be available. Additionally IPv6 natively supports many useful features like:

• **Stateless auto configuration** - IPv6 provides an elegant mechanism to provide automatic address configuration without the need of a DHCP server.

• **IP Security -** IPv6 natively supports IPSec which can be used to authenticate and encrypt IP packets.

- **Mobile IPv6 -** MIPv6 offers a mechanism that allows a mobile node to change its network while it still keeps it IP address.

- **Quality of Service -** The IPv6 header contains different fields in order to guarantee a certain level of QoS.

More in depth details concerning the different IPv6 features can be found in [19], [20]. Currently, the central Asterisk server has been updated to support IPv6 connectivity. The server is connected through the European research network GEANT2 [21] to the IPv6 Internet. The remaining task is to find the appropriate client devices which support IPv6. More and more software and hardware clients provide this feature by default. In order to furthermore support IPv4 devices, a tunnel will be used.

6.2 Interface to TETRA

One solution to overcome the problem of the inappropriate end-devices for the firefighters is to interconnect the TETRA radio system with the group call application. The TETRA end-devices were designed to be used by emergency services and fulfill all the user requirements. As there is currently no TETRA IP gateway available, the idea is to connect the system the same way as it was done for the circuit switched end-devices namely via the PRI card of the VoIP server. The current scenario is the following: A mobile TETRA BTS will be deployed at the demonstration site to provide the needed coverage. An dedicated E1 line will be used to connect the BTS to the telecommunication provider hosting the additional TETRA components and the VoIP server. This setup allows routing the traffic from the end-devices to the VoIP server where the communications can be managed. The practical feasibility of this concept needs to be proven. First tests are planned beginning of 2009.

7. Conclusion

The primary communication method used by public safety services is voice. Video provides additional information that allow to take preliminary decisions. A harmonization of the different communication systems is required in order to enhance the cooperation of the different rescue units. The applications described in this work provide such a tool. Using different existing communication technologies allow creating group calls between a given set of first responders. The central VoIP server provides the interoperability between packet switched and circuit switched networks. The call coordinator application allows to manage the group call and if needed add or remove users. Using Mobile IP allows keeping alive communication sessions over different IP networks. This is especially useful for unidirectional real time services such as video streaming. Using IP as central transmission protocol has many advantages. Application layer protocols such as SIP can be used to exchange information between the different components. The resulting architecture provides a flexible framework that can easily be extended to support additional services. Future developments will promote the use of IPv6 as it provides many novelties that can be used to extend the system. The resulting application allows a better organization of the different emergency services. The response time should be significantly improved which might save lives. Not all of the previously presented procedures (spatial & technical) are realistic in real emergency situations. However it provides an overview of the different technical possibilities that could be used by emergency services in near future.

References

[1] U-2010: Ubiquitous IP-Centric Government & Enterprise Next Generation Networks. Online-Reference: http://www.u2010.eu/, (Last accessed in Mar 2008).
[2] R. Frank, T. Scherer, C. Simon, and T. Engel. A GovernmentalVision on Public Safety Group Calls and Object Tracing. In *TIEMS 2007 14th Annual Conference - Disaster Recovery And Relief - Current & Future Approaches*, volume 14. TIEMS, Hydrographic Institute of the Republic of Croatia, June 2007.
[3] Terrestial Trunked Radio. Online-Reference: http://www.tetra-association.com/, (Last accessed in Mar 2008).
[4] Cisco IPICS. Online-Reference: http://www.nps.edu/Cebrowski/Docs/IPICS%20Solution%20Overview.pdf, 2005 (Last accessed in Jan 2009).
[5] B. McCarthy, C. Edwards, and D. M. Dunmore. The Integration of Ad-hoc (MANET) and Mobile Networking (NEMO): Principles to Support Rescue Team Communication. In *ICMU 2006 Proceedings*, pages 284–289, London, UK, 2006. IEEE Computer Society.
[6] Asterisk - The Open Source PBX & Telephony Platform. Online-Reference: http://www.asteriks.org/, (Last accessed in Mar 2008).
[7] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol, 2002.
[8] D. Willis and B. Hoeneisen. Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts. RFC Editor: RFC3327, 2002.
[9] Asterisk AGI. Online-Reference: http://www.voip-info.org/wiki-Asterisk+AGI, (Last accessed in Mar 2008).
[10] CITA - Controle et Information du Trafic sur les Autoroutes. Online-Reference: http://www.cita.lu/, (Last accessed in Oct 2008).
[11] E. C. Perkins. IP Mobility Support for IPv4. RFC Editor: RFC3344, 2002.
[12] CISCOMobileAccess Router. Online-Reference: http://www.cisco.com/univercd/cc/td/doc/product/access/mar 3200/, (Last accessed in Oct 2008).
[13] XML-RPC Home Page. Online-Reference: http://www.xmlrpc.com/, (Last accessed in Oct 2008).
[14] GOTIVE - Communicators for Mobile Enterprise. Online-Reference: http://www.gotive.com/products/h42.htm, (Last accessed in Oct 2008).
[15] ITU-T Recommendation Q.23 - Technical features of push-button telephone sets. Online-Reference: http://eu.sabotage.org/www/ITU/Q/Q0023e1.pdf, 1988 (Last accessed in Mar 2008).
[16] T. J. Kwon and M. Gerla. Efficient flooding with Passive Clustering (PC) in ad hoc networks. *SIGCOMM Comput.Commun. Rev.*, 32(1):44–56, 2002.
[17] J. Macker, I. Downard, J. Dean, and B. Adamson. Evaluation of distributed cover set algorithms in mobile ad hoc network for simplified multicast forwarding. *SIGMOBILE Mob. Comput. Commun. Rev.*, 11(3):1–11, 2007.
[18] A. Qayyum, L. Viennot, and A. Laouiti. Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks. In *HICSS '02: Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 9*, page 298,Washington, DC, USA, 2002. IEEE Computer Society.
[19] S. Hagen. *IPv6 Grundlangen - Funktionalitt - Integration*. Sunny Publishing AG, Maur, Schweiz, 2004.
[20] B. Stockebrand. *IPv6 in Practice*. Springer, Berlin, Germany, 2007.
[21] GEANT 2. Online-Reference: http://www.geant2.net/, (Last accessed in Mar 2008).