# The ADAMO project : architecture to support communication for emergency services

# The ADAMO Project: Architecture to Support Communication for Emergency Services

Johan Bergs*, Dries Naudts†, Nik Van den Wijngaert*, Chris Blondia*, Ingrid Moerman†, Piet Demeester†, Jerome Paquay‡, Frank De Reymaeker‡ and John Baekelmans‡
* IBBT - PATS, Dept. of Mathematics and Computer Science, University of Antwerp, Antwerpen, Belgium
Email: {johan.bergs,nik.vandenwijngaert,chris.blondia}@ua.ac.be
†IBBT - IBCN, Dept. of Information Technology (INTEC), Ghent University, Gent, Belgium
Email: {dries.naudts,ingrid.moerman,piet.demeester}@intec.ugent.be
‡Cisco Systems, Diegem, Belgium
Email: {jepaquay,fdereyma,jbaekelm}@cisco.com

***Abstract*—When emergency services are in a crisis situation, one of their major needs is to have efficient communication. Every person involved needs to have the most up-to-date and relevant information at all times and needs to be able to communicate with his colleagues effectively. In order to support this, it is important that the network used by the emergency services supports all necessary communication flows to make this communication as smooth as possible. In this paper, we will describe the end-to-end system architecture we developed and implemented in the IBBT[1] project ADAMO - Advanced Disaster Architecture with Mobility Optimizations.**

## I. Introduction

In recent years, it has become clear that emergency services need to be able to communicate efficiently during a crisis. Many different research projects on crisis management and mobile emergency networks can be identified, such as:

- IST SHARE[1], a project intended to offer an information and communication system to support emergency teams during large-scale rescue operations.
- ICIS[2], aimed to develop better techniques for making complex information systems more intelligent and supportive in decision making situations.
- Calahan (Calamiteitenbeheer haven van Antwerpen - Calamity Management of the Port of Antwerp)

Many other projects, e.g. on information exchange standards, exist, but the three listed above are examples of projects that are closely related to ADAMO. The ADAMO project, however, does not only focus on information flows and decision support systems, but it also has a strong focus on the deployment of an ad-hoc emergency network, enabling these supportive technologies. Furthermore, the architecture developed tries to be complementary to existing technologies instead of replacing them completely. An example of this is the TETRA[3]-to-VoIP coupling offering compatibility between the existing TETRA system and the ad-hoc ADAMO system. This will be further explained in section IV.

The communication needs of the emergency services encompasses the availability of a reliable voice communication system that can be used at any time, at any place. In many European countries, the TETRA system is currently used as primary communication system for emergency services. TETRA has some advantages over GSM: (1) it is faster to set up a call, (2) grouping of many persons in one call is one of the design features of the system, (3) since the TETRA network is not publicly available, the risk of network saturation is reduced. TETRA, however, has one major disadvantage over other technologies: its very low bit rate of only a few kbps. This low bit rate does not allow large amounts of data to be transmitted over the TETRA network, limiting it in practice to voice traffic only. Another disadvantage of TETRA, at least in Belgium, is the lack of coverage inside buildings. This is especially disadvantageous for the fire departments, as they frequently have to enter buildings to fight fires. The loss of all communications is unacceptable in these situations.

To tackle the problem of insufficient indoor coverage, the IBBT GeoBIPS[4] project and its successor ADAMO[5] defined and tested an architecture that supports local communication using IEEE 802.11[6] technology and Voice-over-IP (VoIP), both indoor and outdoor. The details of the ADAMO network architecture will be discussed in section III-A. While GeoBIPS focused only on the on-site communication aspects, ADAMO also focused on the entire end-to-end communication and information flows between a crisis center and the incident site. These aspects will be discussed in section II. A general overview of the ADAMO architecture can be seen in figure 1.

In this figure, the backend is depicted in the lower right corner. Typically, the back end in the ADAMO concept would be a remote crisis center. This backend has a link to the Internet. The entire incident location (outside) is covered by a locally deployed outdoor network, which will also be further discussed in section III-A. One or more of the vehicles present at the incident area are connected to the Internet (see III-C), which enables broadband communication between the incident site and the crisis center. In section IV, we will describe the steps we took to bridge the existing TETRA network with the VoIP network deployed locally at the incident site. This enables the coupling of existing TETRA groups to Virtual Private Ad-Hoc networking (VPAN) (III-D) groups on the Wi-Fi network.

[1]Interdisciplinary institute for BroadBand Technology

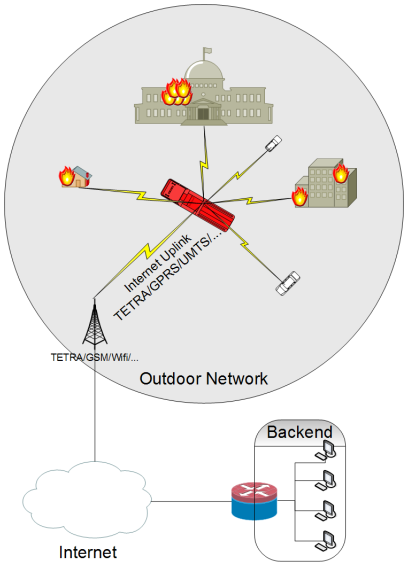


Fig. 1. ADAMO Architecture Overview

## II. Information Provisioning

Receiving correct, up-to-date information is essential for the different emergency services to perform their tasks[7]. During an emergency, there are different problems to tackle to ensure that everybody has access to this information. Firstly, the amount of information available can be enormous. If the scale of the incident is large, a lot of different sources of information need to be consulted in order to get a good overview of the entire incident. An emergency worker has no time to search all information sources for those pieces of data that are relevant for him at a certain time during the intervention. Secondly, it is important to ensure that the information used by the emergency workers is correct and up-to-date. This means that continuously changing information, originating from gas detectors for example, needs to be transmitted over the network in real-time. This also has as a consequence that all data preferably has a common data format for all disciplines. Each emergency discipline can have its own, specific view on the information. It should be avoided, however, that each discipline individually stores the information that is important to them, as this leads to data duplication and holds the risk that not all data sources are kept up to date. Thirdly, the information needs to be presented in such a manner that the end-user is able to interpret the supplied information easily. As many different end users are involved during a crisis situation, ranging from the fire fighter in the field to the coordinator in a crisis center, information representation is a factor that should not be ignored.

Two seemingly contradictory requirements can be identified for the information provisioning: on the one hand, as much information as possible is needed to give an overview of the incident, which is very useful in the crisis center as it needs to coordinate the different emergency services. An individual fire fighter, on the other hand, needs to be able to access only very specific, but very detailed and up-to-date, information on the task at hand. The level of detail required by a fire fighter in the field is much greater than the level of detail required in the crisis center. In section II-A, the information provisioning on-site will be discussed. In section II-B, we will describe the information provisioning in the crisis center.

### A. At the Intervention Site

On the incident site, we deployed an ad-hoc wireless mesh network, which will be described in more detail in section III-A. This network allows voice communication and the transmission of sensor data. This sensor data can, for example, be live data captured from fire fighters, such as amount of air left, temperature, etc. All sensor data can be visualized on a tablet PC used by the commanding officer (CO) of the fire fighter team. The CO can follow the status of each of his men and is notified of dangerous events, such as when the air pressure gets too low or a gas detector detects a potentially hazardous situation. Air pressure monitoring is one example of very detailed information, that is only useful for the CO. Therefore, it is not shared with the crisis center.

In the most optimistic situation, the local network, which is incident-wide, is coupled to the Internet. This allows us to combine local (dynamic and real-time) data with online (static) data such as intervention plans or maps of the surroundings. This also enables high-level data sharing with the crisis center. If a commanding officer of the police who is on site, for example, decides to block certain roads, he can share this information with the coordinating crisis center by making annotations on a shared map making them aware of this situation. This is more efficient than making telephone calls back and forth between the incident site and the crisis center. This also enables the crisis center to closely monitor the overall intervention as all information is immediately available for all interested parties.

### B. In the Crisis Center

In the crisis center, a multi-user multi-touch table was used. This enabled the decision makers of the different disciplines involved (police, fire department, medics and possibly civil defense) to share and pass information to each other. The fact that the table is truly multi-user means that each user can access only that information he is allowed to access, and that each user owns his windows displayed on the table surface. Only the owner can move, modify or close his windows.

In addition to the table, the crisis center can also use a large display or smartboard. This can be used to project information that is important for all disciplines, such as a map of the incident area.

## III. Communication

### A. Local Communication

When emergency teams arrive at an incident site, it is clear that they cannot rely on existing infrastructure. Therefore, it is essential that, whenever necessary, the rescuers can deploy their own network infrastructure to allow voice and data communication. In order to provide outdoor broadband

network connectivity at the disaster scene, different approaches could be taken.

In the first approach, short range hotspots are created at the different emergency vehicles by using a Mobile Access Router (MAR). The CO, equipped with a tablet PC and other emergency responders that are in the vicinity of such a hotspot will have wireless broadband access to the network at the scene. These hotspots are based on the IEEE 802.11a/b/g standard. Depending on the environment and the type of hardware (wireless radio chips and antenna's), they have a range of maximum $\pm$300m. Remark that at higher distance, throughput significantly decreases from a theoretical maximum of 54 Mbps to 1 Mbps. For smaller areas, one MAR could offer total outdoor connectivity [4]. In a larger area, when multiple vehicles are considered, no direct interconnectivity between them is provided in this architecture. In case multiple vehicles have uplink connectivity, it is be possible to interconnect them over the Internet. However, this may reduce possible bandwidth, depending on the Internet access technology that is used. Moreover, when there is no uplink available, no interconnection between the vehicles is possible. Another way to interconnect the different vehicles is the use of implementing a Wireless Distribution System (WDS). A WDS must be preconfigured and is, as such, not feasible at a disaster scene.

In the second approach the Command Post Operations vehicle (CP-OPS) acts as a central access point equipped with a long range network device (e.g. WiMAX). Every other vehicle will connect as a client to this access point. Even emergency responders who are outside the range of their nearest hotspot can connect with the central CP-OPS access point when there are equipped with a compatible client interface. In this situation all the network load is centralized, and, as a consequence, there is a single point of failure. The deployment of a long range technology at a command vehicle leads to practical problems and high expenses.

Third, to provide redundancy in the network, we might opt to use long range mesh technology (e.g. WiMAX) . Each individual vehicle will be equipped with a long range wireless base station, which can dynamically form some kind of mesh network. Currently, such a solution is not feasible.

A last network solution to provide full outdoor coverage is to make use of short range mesh technology [8] . In this use case, we assume that each vehicle is equipped with a short range wireless device (e.g. Wi-Fi). These nodes will dynamically form a wireless mesh network (WMN). Still, it may occur that a vehicle or emergency responder is outside the range of any other node and cannot integrate into the network. To solve this, extra mesh nodes could be deployed at the crisis area.

In ADAMO, the system architecture that we implemented was based on the first and last approach. In our final demonstrator we showed the first solution. The other approaches were included in our study but seemed currently not feasible in real-life situations due to practical and cost issues.

Due to a lack of good indoor coverage for voice and data communication, emergency teams are exposed to extra risks when entering buildings or other constructions. In order to provide communication between the CO and the teams inside, the outdoor network coverage should be extended to an indoor environment where strong signal degradation occurs (due to walls, ceilings, obstructions...) by deploying an ad-hoc self-organizing, highly redundant, self healing broadband wireless network. The indoor WMN that is described in this paper is based on IEEE 802.11 technology.

To provide a full WMN for indoor coverage, two approaches could be used.

- Single interface, single channel setup
- Multiple interface, dynamic channel algorithm

The former approach has following advantages:

- rapid deployment
- fast recovery
- small form factor
- low energy consumption

This approach does not work well if the nodes have a high density due to the fact that the interference increases with the number of nodes. Because of the increased interference, the overall throughput in the network could drop dramatically [9].

In the other approach, the mesh nodes could be equipped with more than one wireless interface, allowing us to deploy a multi-channel wireless mesh network [10]. When using multiple interfaces and different channels, the overall throughput of the system can be optimized, however, this is at a cost of less rapid auto-configuration and recovery and higher energy consumption [11].

The general indoor network architecture is shown in Figure 2 and consists of three network components which will form the mesh network: Mesh routers (MR), Mesh gateways (MG) and Portable mesh routers (PMR). The core of the network is the WMN, which is mainly formed by the MR. The MG will interconnect the WMN with the outdoor network. At the edges of the WMN, the PMR will connect to the network.

The MR are small, light-weight, battery powered devices that will be deployed during an exploration of a building. The devices are static, auto-configuring and will automatically integrate into the network after booting. Each MR consists of at least one wireless 802.11a/g interface that is tuned to a default channel. Other Wi-Fi interfaces can be added to provide more redundancy and bandwidth in the WMN. These interfaces are configured to other channels according to a Dynamic Channel Selection algorithm. The MG are to be deployed near the entrance of the building the rescue team wants to explore. These battery powered devices act as a gateway between the indoor WMN and the outdoor network that is set-up at the disaster scene. The MG has one or more 802.11 interfaces that will be part of the WMN. One of these interfaces must be tuned to the default channel. The Dynamic Channel Selection protocol will assign channels to the other 802.11 interfaces. Furthermore, the MG will have an uplink interface to the outdoor network. Several technologies are possible, such as 802.11, 3G client, WiMax client, Ethernet.

The members of the rescue teams are equipped with the PMR. This device will provide access to the WMN that is

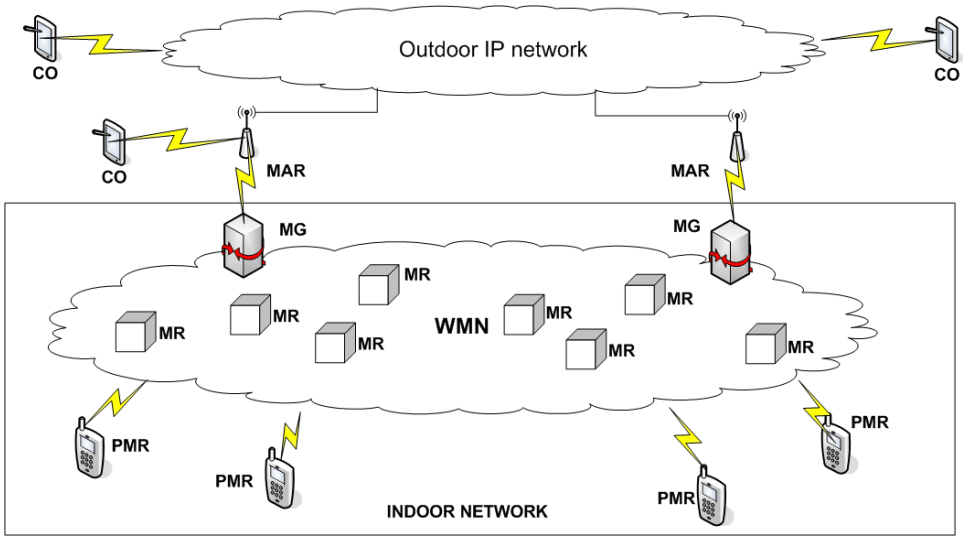


Fig. 2. Local network architecture

deployed in the building. In essence, the PMR is a part of the WMN and has similar functionality as the MR, except that they are mobile. In addition, the PMR could be connected to other sensor equipment that is carried by the rescue team. The sensor data then can be sent over the WMN. VoIP functionality can also be integrated in the device, to allow voice communication over the WMN. The device must be battery-powered and self-configuring.

The outdoor MAR is linked to the MG, which functions as a connection point between the indoor and the outdoor network. When the indoor network is deployed, several MG can be installed to keep the connection to the outdoor network and to avoid single point of failure. The WMN consists of one large range of IP addresses. The indoor network is dynamically configured, so it is not known in advance through which MAR each host is reachable. Initially, the WMN could be disjoint when two or more teams enter a building. At a certain point, it is possible that the separate networks merge, and will form a larger ad-hoc network. Thus, a mechanism is provided to dynamically learn routes towards the indoor hosts and vice versa.

For the indoor WMN, the OLSR routing protocol is used [12], which is a derivation of the OSPF routing protocol and is optimized for mobile ad-hoc networks. Because of the extensive support, stable implementation and several extensions, we preferred the use of the OLSR protocol [14]. Following requirements were important in our choice for OLSR: open source, pushed by IETF, multicast support, IPv4 based, gateways supported.

As the proposed outdoor routing protocol is OSPF, a OSPF-OLSR bridge is installed on the MG. That way, the indoor OLSR routes can be distributed in OSPF and vice versa. Thus, as OLSR is proactive, the MG will learn the routes to each host, and pass these routes to the MARs, which will distribute these routes in its OSPF area. The OSPF area covers the whole network, up to the home network at the crisis centre. As the secure uplink is multicast enabled, OSPF control traffic is sent towards the home network, so each node in the network has an overview of the whole topology.

This is necessary: because of the dynamic and mobile character of the whole network architecture, several routes could exist toward each device. Three possible routes could exist:

1) Route via backend
2) Route via on-site outdoor network
3) Route via on-site indoor network

This introduces extra challenges on the network design and the routing mechanism that run on the several network components. The VPAN, desired in section III-D, can be a good alternative to provide the necessary routing mechanisms between the network segments.

### *B. IEEE 802.11*

We chose to use IEEE 802.11 hardware because of the fact that it is a cheap, ubiquitous technology. In small-scale tests in the underground parking of IBBT in Ghent, Belgium, an office building and in different subway stations of Brussels, Belgium, the throughput and range of the IEEE 802.11 were deemed to be sufficient for realizing the goals of ADAMO.

In figure 3, a map of the office building is shown. The black line indicates the path we took during the exploration of the building. The dotted black line is the return path via a different floor. During the entire walk, we had a communication link between the person indoor and the one who was standing outside. The link was lost for a few moments when we entered a dead-spot (behind some metal racks). This is indicated by the black ellipse.

A major drawback of using IEEE 802.11 is the high risk of interference from external sources. As IEEE 802.11 hotspots are quite common, and as other technologies can use the

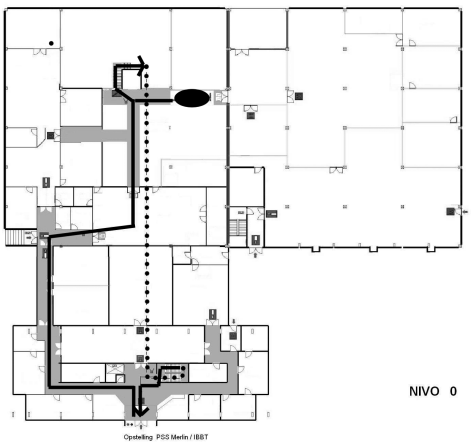


Fig. 3. Small-scale test in office building

same band, it is very likely that some other devices near the emergency site will cause interference. If the amount of interference is too high, it could degrade the performance of the emergency network to such an extent that it becomes unusable. It should however be noted that IEEE 802.11 causes no interference with the technologies currently used by rescue workers, such as TETRA. In a worst-case scenario with a lot of interference, the existing technologies and protocols can be used unmodified and considered to be a minimum service. The added value of ADAMO is lost, however. To tackle this problem of IEEE 802.11 interference, we recommend that a dedicated band should be defined in Europe that can only be used by the emergency services. However, the price of the equipment needed by the emergency services may be a little higher. Note that in America, the 4.9Ghz Public Safety band is already reserved for emergency services.

### C. Long Distance Communication

To enable connectivity between the incident area and the crisis center, an Internet connection is required. As the emergency workers at the incident area cannot rely on existing infrastructure, they need to set up their own Internet uplink. This is done by using the MAR mentioned above. One or more MARs at the incident area can be equipped with, for example, a 3G uplink technology. Any form of uplink is possible, however. In ADAMO, we considered 3G and WiMAX, but a satellite uplink is also one of the possibilities. Irrespective of the uplink technology, the connection to the crisis center is set up using a secure Mobile IP uplink. A second uplink to the crisis center is realized using the existing TETRA network. This uplink will only be used for voice traffic as TETRA bandwidth is very limited. It should be noted that the TETRA and IP networks are not two disjunct networks. Voice on the TETRA network is coupled to voice on the IP network (VoIP), as will be further discussed in section IV. This allows the emergency workers to use their VoIP equipment on places where TETRA coverage is insufficient, and still be connected to the country-wide TETRA network, even in the absence of a (broadband) Internet uplink.

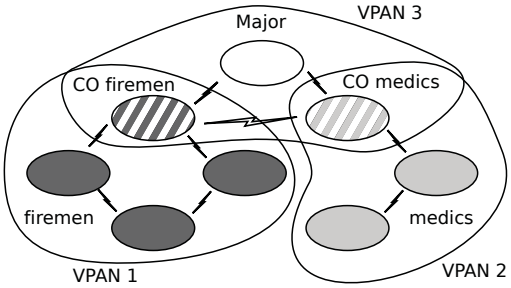


Fig. 4. VPAN partitioning

### D. Virtual Private Ad-hoc networking (VPAN)

In the VPAN concept, a logical overlay network of both local and distributed nodes is set-up on top of an existing infrastructure [13]. For local connectivity, VPAN is deployed over the communication links at the link layer. For distributed connectivity, IP connectivity is required, typically over the Internet. VPAN features security and self-organization towards the end user. Security is performed both in terms of networking and applications and service. The VPAN concept is based on ad hoc network techniques and private addressing. Local and distributed nodes will organize themselves in logical virtual networks, providing a secure and transparent overlay.

As the VPAN solution is based on the creation of clusters of nearby nodes, we use the interdisciplinary character of disaster management to define the several clusters [14]. As depicted in Figure 4, each of the disciplines will generate a VPAN cluster on site. End devices can automatically set-up secure communication within a cluster, based on ad-hoc networking techniques. The crisis centre at the backend could form a cluster of the network as well.

Each of the clusters will have one or more VPAN gateways. Every separate VPAN gateway will register itself with the VPAN agent, which must be reachable over an interconnecting structure (e.g. the Internet). This way, the different gateways will be informed about the location of other clusters that can be reached within the overlay. Secure tunnels will be set up between the VPAN gateways and routing information between the clusters is exchanged. Now, each client device will be able to securely and transparently connect to any other member of the overlay network, regardless of the physical location of the devices.

VPAN gateways will connect to the Internet via different uplink connections, for example UMTS, GRPS, WiMax or IEEE 802.11. Inter-cluster connectivity is only achievable if the VPAN agent can be reached. Intra-cluster communication is possible, regardless of the VPAN agent.

Each of the members of an overlay must run the VPAN protocol. Because the ad-hoc routing protocol is integrated in the VPAN solution, no mesh routing protocol is needed at

the on site mesh. However the current intra cluster routing protocols that are supported, which are a modified version of WRP and a very basic implementation of AODV, are not optimized for dynamic mobile networks like the ADAMO indoor network. However, integrating the OLSR routing protocol, which has been proven to suffice for the on site network, could be done with rather minor effort. For the inter-cluster routing, extensions are written based on tunnel identifiers instead of next hop info.

### *E. Security issues*

As emergency networks are vulnerable to different attacks, it is of the utmost importance that the communication network is completely secure and shielded from unauthorized people and malicious hackers to prevent intrusion and information leaks. Only trusted nodes are allowed to join the network and encryption is used when transferring data over the network and the Internet. AAA mechanisms and encryption techniques are integrated in the VPAN solution. All nodes that want to participate in an overlay network must share a common cryptographic trust relationship.

## IV. TETRA to VoIP Coupling

As explained in the introduction, TETRA is the primary communication system for emergency services in Belgium, but it lacks indoor coverage. Since a local ad-hoc IEEE 802.11 network, used for communication using VoIP, is already deployed in the ADAMO system, it would be very beneficial if the gap between the VoIP communication network and the TETRA network is bridged. We were able to do so by mapping a TETRA voice group to a VoIP group and vice versa. This was achieved by combining a few existing state-of-the art technologies. The first is the Cisco CME (Call Manager Express), a system that offers a sophisticated set of key system and PBX telephony features. The idea is to install the CME in one of the vehicles present at the disaster site. Any SIP client can connect with the CME and create a conference call. Preferably, all SIP enabled radios used by the different intervention teams are configured to connect to the CME automatically. Every team at the intervention site uses its own conference call group. Note that the CME only provides a conference call service and is not able to group calls.

The second and third technologies we used to allow for intercommunication, not only between different VoIP groups on the CME, but also between the TETRA network and the CME groups, were a standard mobile TETRA radio that we coupled to a Cisco IPICS + LMR (IP Interoperability and Collaboration System - Land Mobile Radio). The IPICS was originally developed for emergency services that are in need of inter- and intra-communication during chaotic situations. It offers communication interoperability between many different technologies, such as telephones, cell phones, IP or non-IP networks, etc. The IPICS also offers push-to-talk facilities to any connected device by using Virtual Talk Groups and Combined Channels. In this concept, one channel would be one TETRA group, coming from the TETRA radio connected to the LMR, or one VoIP conference group, coming from the CME, which is also connected to the IPICS. Using this PTT functionality, it is possible to interconnect the TETRA network with the VoIP clients. This enabled us to have bi-directional push-to-talk communication between the existing TETRA system and the ad-hoc ADAMO VoIP system. The VoIP clients register with the CME and are added to the correct (TETRA) groups via the IPICS channel of the LMR.

This TETRA to VoIP coupling has been implemented and was successfully demonstrated at the ADAMO closing event.

## Acknowledgement

This research is partly funded by the Flemish Interdisciplinary institute for BroadBand Technology (IBBT) through the GeoBIPS and ADAMO projects. The authors would like to thank all academic and industrial partners of these projects, and more specifically IBBT - EDM - UHasselt, AbiWare, Astrid NV and Dräger Safety for their valuable contributions to the ADAMO project.

## References

[1] IST. (2007, Dec.) Mobile support for rescue forces, integrating multiple modes of interaction. [Online]. Available: http://www.ist-share.org/

[2] BSIK. (2003) Interactive collaborative information systems. [Online]. Available: http://www.icis.decis.nl/

[3] *Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)*, European Telecommunications Standards Institute Std. EN 300 392-2, Rev. 2.5.2, Nov. 2005, work item reference: REN/TETRA-03129.

[4] GeoBIPS. (2006, Dec.) Geographical broadband integration for public services. [Online]. Available: https://projects.ibbt.be/geobips/

[5] ADAMO. (2007, Jan.) Advanced disaster architecture with mobility optimizations. [Online]. Available: https://projects.ibbt.be/adamo/

[6] *Part 11: Wireless LAN Medium Access Control (MAC) and Phsyical Layer (PHY) specifications*
*Amendment 4: Further Higher Data Rate Extension in the 2.4GHz band*, IEEE Computer Society Std., Jun. 2003.

[7] K. Luyten, F. Winters, K. Coninx, D. Naudts, and I. Moerman, "A situation-aware mobile system to support fire brigades in emergency situations," in *CAMS 2006, the 2nd International Workshop on context-aware mobile systems*, 2006.

[8] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[9] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Transactions on Information Theory*, vol. IT-46, no. 2, pp. 388–404, Mar. 2000.

[10] B.-J. Ko, V. Misra, J. Padhye, and D. Rubenstein, "Distributed channel assignment in multi-radio 802.11 mesh networks," in *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*, March 2007, pp. 3978–3983.

[11] J. Robinson, K. Papagiannaki, C. Diot, X. Guo, and L. Krishnamurthy, "Experimenting with a multi-radio mesh networking testbed," in *Proc. First Workshop on Wireless Network Measurements*, Apr. 2005.

[12] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)," RFC 3626, experimental. [Online]. Available: http://hipercom.inria.fr/olsr/

[13] J. Hoebeke, G. Holderbeke, I. Moerman, B. Dhoedt, and P. Demeester, "Virtual private ad hoc networking," *Wirel. Pers. Commun.*, vol. 38, no. 1, pp. 125–141, 2006.

[14] P. Dedecker, J. Hoebeke, D. Naudts, I. Moerman, J. Moreau, and P. Demeester, "Fast and safe emergency communication through network virtualization," in *IWCMC '09: Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing*. New York, NY, USA: ACM, 2009, pp. 42–46.