Support of Future Disaster Response Using Generalized Access Networks (GANs)

Georgios Karagiannis[1], Val Jones[1], Sonia Heemstra de Groot[2]

***Abstract*— Efficient communication and coordination are major challenges experienced by the emergency services (fire-brigade, police, ambulance) during the first response to a major incident. A major incident can happen anywhere and at any time, hence support for emergency communications services should be ubiquitous and independent of communication technologies and infrastructure used. We present a vision of how ambient intelligent environments may be used in the future to support the emergency services during first response to a major incident. Support includes enabling emergency communications and biomedical monitoring for front line personnel. In this paper we focus on the possibilities and challenges raised by using the GAN (Generalized Access Network) infrastructure to support ambient intelligent services and emergency services (fire-brigade, police, ambulance) for major incident management.**

I. Emergency Communications for Major Incident Management

Efficient communication between, and coordination amongst, different agencies and teams are amongst the major challenges experienced by the emergency and rescue services during the first response to a major incident. This observation holds for many different types of major incident; whether it be a large scale natural disaster in a remote area (such as earthquake, flood or volcanic eruption) or a major accident in an urban setting caused by human error or system failure (such as major transportation or industrial accidents) [1] or an incident resulting from deliberate action (e.g. an act of war, terrorism or sabotage) [2].

In all cases, management of the first response involves coordination of teams from a number of different agencies, which may include emergency medical services, fire services, police and security services, local and national government agencies and Non-Governmental Organisations (NGOs) as well as the specially convened disaster coordination team.

Large incidents may be spread across national boundaries, or may overwhelm the response capability of one country, thus requiring international cooperation in first (and subsequent) response phases, further complicating this very challenging coordination task. The communication problem is further exacerbated if telecommunications are disrupted through destruction of communications infrastructure.

Depending on the circumstances such incidents are sometimes complicated by environmental risk factors such as the possibility of chemical, biological or radiological pollution. These risk factors have to be recognised, monitored, contained and managed as part of the response.

A major incident can happen anywhere any time, therefore the support for emergency communication services should be ubiquitous and should be independent of the communication technologies and infrastructure used.

In this paper we focus on the possibilities and challenges raised by using the GAN (Generalized Access Network) infrastructure to support ambient intelligent services and emergency services (fire-brigade, police, ambulance) for major incident management. A GAN is a common fourth generation mobile and wireless access network, including different types of air interfaces, based on a flexible and seamless All-IP (Internet Protocol) infrastructure. The solution should be able to provide the following:

Security support: Security is a most critical issue, especially in case of deliberate attacks such as terrorist incidents, since the emergency communication systems themselves will become a high-tech target for terrorists in order to increase confusion and disruption of the rescue effort.

Resilience support: When a major incident occurs, one or more nodes and links in the wired network infrastructure may be damaged or destroyed. It is crucial to develop resilience mechanisms that provide fast connectivity restoration to minimize disruption of the prevailing Quality of Service (QoS) requirements as well as efficient node protection mechanisms. The quality of resilience mechanisms need to be judged by appropriate QoS-based criteria that differentiate between various QoS models, and the type of network in which they should apply. In conjunction with this, link state discovery mechanisms have to be developed that can be used for the immediate discovery of efficient end-to-end paths.

Mobility and load distribution support: The end-to-end connectivity and routing are affected by the mobility of mobile devices and the mechanisms used in mobility solutions. Solutions have to be provided to support the mobility, routing and load distribution within ad-hoc networks and the GAN.

Network management support: For automated network management integrated across diverse network environments, an overlay network management scheme is

[1] University of Twente/CTIT/ The Netherlands. v.m.jones@utwente.nl, g.karagiannis@utwente.nl

[2] Twente Institute for Wireless and Mobile Communications/ University of Twente Sonia.Heemstra.de.Groot@ti-wmc.nl

required. One of the drivers for this network scenario is to produce straightforward, scalable and stable management of the network, compared to current management schemes.

Ad hoc networks for emergency management support: In the vision presented here ad hoc networking plays an important role. It allows fast set up of a communication structure when the communications infrastructure is not available. In addition, it may extend the coverage of the global area to locations with no support of communication facilities.

This paper is organised as follows. Section 2 describes the proposed solution, section 3 initiates a discussion and section 4 describes the conclusions and the future work.

II. PROPOSED SOLUTION

We envision a future scenario where the emergency services' vehicles and personnel are equipped respectively with Vehicle and Body Area Networks (VANs and BANs). The ambulance service, for example, would have ambulance Vehicle Area Networks which communicate with the Paramedic's Body Area Networks and the firefighters would have another kind of specialised professional BAN, and so on. The VANs and BANs of the different emergency services themselves comprise nodes that may connect to form (hierarchical) mobile ad hoc networks to support intra- and inter-service communications, thereby facilitating smooth C3 (Command, Control and Communication) at the disaster scene. Ad hoc networking may provide the only communication possibility for the emergency services by providing islands of communication whereby the professionals at the scene may communicate. Further, ad hoc networks used by the emergency services should be able to discover and communicate with any surviving *in situ* environmental sensor networks and any surviving telecommunication infrastructure, thereby connecting over the damaged infrastructure networks with the disaster and emergency services coordination centres. Such an infrastructure will support resilience mechanisms providing fast connectivity restoration, resulting in a self-healing communication environment.

Over the past few years, overlay networks have emerged as an alternative for introducing new functionality that is too cumbersome to deploy in the underlying IP infrastructure. Overlays allow third-party entities, other than traditional ISPs, to offer enhanced communication services to clients. Similarly, overlay mechanisms with QoS support enable enterprises or third parties to build their own Virtual Private Networks (VPNs).

VPN technology is based on a tunnelled architecture where most of the traffic is fixed. However, a significant part of the traffic that is supported by the GAN is mobile. Therefore, the already existing VPN tunnelling solutions, which require specific edge-routers that perform tunnelling and forwarding, cannot be used for the GAN. On the other hand, MPLS solutions are not economical, since they require specific solutions for forwarding tunnelled packets.

Data Networks, especially in mobile and wireless environments, must be able to maintain an effective operability even when they are partially dysfunctional. Current Layer 3 mechanisms fail to provide resilience of sufficient quality to support real-time traffic. Fast restoration is included into the design objectives of MPLS, but its scalability is limited. Most of the current work in Traffic Engineering (TE) [3] has focused on load balancing to minimize congestion. However, QoS support and resilience have been treated, if at all, as a bi-product.

Research on ad-hoc networks has mainly focused on stand-alone sets of terminals. When attached to access networks, security concerns become a very relevant issue. Also, the dynamic routing algorithms designed for isolated networks are far from being adequate for attached ad-hoc networks. Besides, most of the work towards QoS support has concentrated on isolated ad-hoc networks.

Additionally, advances in computing, wireless and sensing technology have enabled sensor networking. Every environment can be surrounded with sensors [4], which allows to create Smart Spaces where users/devices roam and dynamic service provisioning is supported [5]. These systems are quite beneficial regarding security, cost reduction, remote control of areas at risk or areas that are not possible to wire. Moreover, advances in networking technologies now allow the transfer of sensor data to systems which have the capacity to store a large amount of information.

The innovative networking technologies involved in realising this solution are as follows.

A. Body Area Networks

We define a BAN as a body worn network of communicating devices, which may also communicate wirelessly with other networks via a communication gateway which we term a Mobile Base Unit (MBU). In 2001 Jones, Bults and Vierhout proposed the use of Body Area Networks to support Virtual Trauma Teams [6]. The vision was that casualties attended by ambulance teams would be fitted with trauma patient BANs to measure vital signs and transmit them to the hospital. At the same time the paramedics would each be equipped with a specialized health professional BAN effecting audio and video communication with colleagues in the Accident and Emergency Department at the hospital.

The vision was developed further in [7] and since 2002 the University of Twente and partners have been developing Body Area Networks (BANs) during the IST Mobihealth [8], FREEBAND Awareness [9] and eTEN HealthService24 [10] projects. In Mobihealth one of several clinical settings addressed was trauma care; patient and paramedic BANs were developed and trialled with the regional trauma centre (Medisch Spectrum Twente) and the ambulance service in Enschede in the Netherlands. Data was transmitted to the

hospital via GPRS and UMTS. Subsequently the MobiHealth trauma BAN was trialled in Bremen, Germany, during the IST XMOTION project [11] using the XMOTION platform and transmitting data over UMTS.

In the MobiHealth trauma setting we dealt with a single casualty and one ambulance and its paramedic team. In the IST MOSAIC project [12] we extended this scenario to cover a major incident, where multiple teams from the different emergency services cooperate together to provide first response in case of a major accident, disaster or terrorist attack. A detailed Major Incident scenario illustrating a possible future use of advanced BANs interacting with AmiEs (ambient intelligent environments) was developed for MOSAIC and for the Wellbeing_service@work community of the European Commission's AMI@work initiative [13] and is reported in [14], ASWN]. Figure 1 illustrates the MOSAIC vision of future BANs for emergency services personnel realised as wearable microelectronics incorporated into the uniforms.

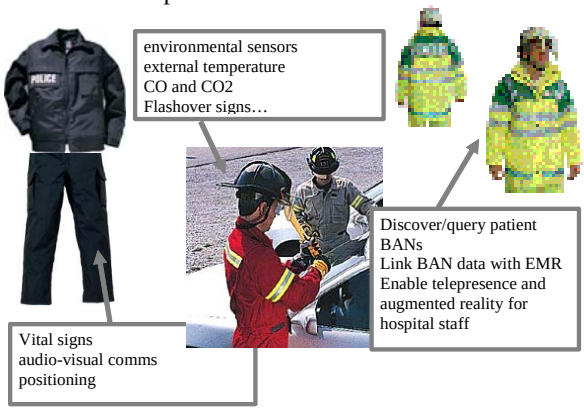

Figure 1 BANs for emergency services personnel

For police, the BAN will support vital signs monitoring and positioning as well as audio-visual communications with police command and control centres. In addition, firefighters' BANs would incorporate environmental sensors measuring for example, external temperature, carbon monoxide and carbon dioxide and possibly detecting flashover signs. Additionally to these services, paramedic BANS might also have the capability to discover/ and query patient BANs and link BAN data with the EMR. By means of audio, data visualization and video they would also enable emergency room staff at the hospital to experience the scene remotely through telepresence and augmented reality.

Figure 2 illustrates ad hoc networking at the disaster scene between emergency workers' BANs and the emergency vehicles' vehicle area networks, within and between the services.

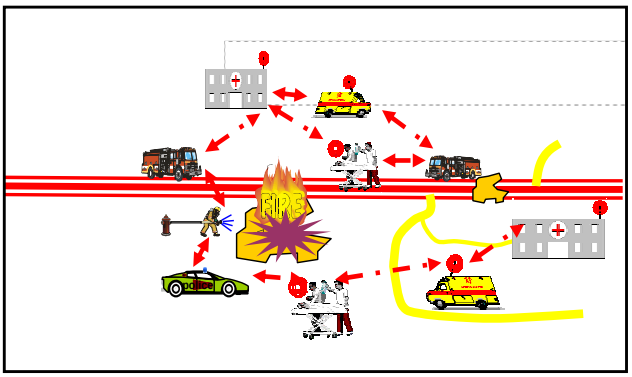

Figure 2 ad hoc networking at the scene

B. *GANs*

Generalized Access Networks (GANs), see Figure 3, provide a promising solution for support of Emergency Services (fire-brigade, police, ambulance etc) by allowing ubiquitous connectivity to ad-hoc networks. A GAN can be considered as a common fourth generation architecture, including mobile and wireless access networks, based on a flexible and seamless All-IP (Internet Protocol) infrastructure with enhanced interworking features and global roaming for all access technologies. GANs can share the same network infrastructure among different operators, supporting appropriate levels of security and QoS. The approach is based on separating physical networks into a number of overlay networks to support, for example,, the separation of multiple mobile virtual operators, the formation of service networks and emergency services Virtual Private Networks (VPNs). A new approach toward overlay network provisioning, without requiring special lower-layer solutions (such a those below Layer 3, e.g., MPLS), can be investigated and applied (i.e., a "pure IPv6" solution).

Figure 3 illustrates the architecture that is supporting the aforementioned emergency scenario, which incorporates:

A GAN operator which has a common infrastructure supporting multiple radio interface technologies through which mobile hosts and several forms of ad-hoc networks for supporting emergency services are attached, such as Mesh networks, Wireless Sensor networks, BAN (Body Area Networks) and PAN (Personal Area Networks).

Different forms of ad hoc communication, involving emergency services personnel (paramedics, police, fire fighters, disaster coordinator at the scene) and emergency vehicles. The edge of the wired infrastructure is shown as ED (Edge Device) and the wireless edge as WED (Wireless Edge Device). The WED is a sophisticated device with air-interface functionality (e.g. base-stations and access points) as well as edge-router functionality.

Many different radio technologies for communication with remote centres (e.g., hospitals, police and fire brigade headquarters, disaster coordinator) using the different GAN

system and radio interfaces.

Support of service reliability in presence of mobility and unreliable channels.

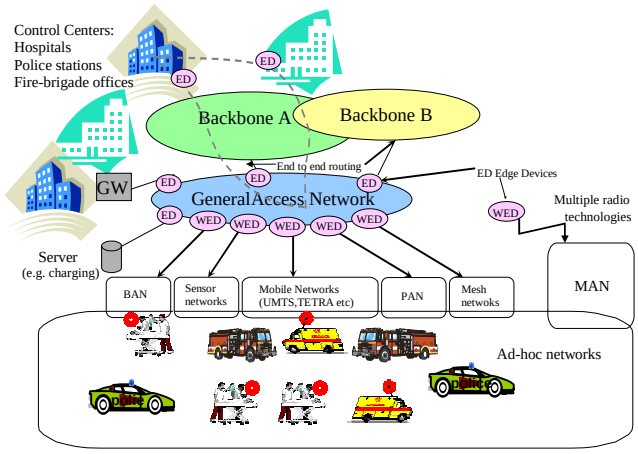

Figure 3: Architecture of proposed solution

III. IMPLEMENTATION ISSUES

This section emphasizes the issues that need to be addressed in order to meet the requirements given in Section 1.

Resilience mechanisms

When a major incident occurs, one or more nodes and links in the wired network infrastructure may be damaged or destroyed. Resilience mechanisms need to be developed to provide fast connectivity restoration to minimize disruption of the prevailing Quality of Service (QoS) requirements. In addition, efficient and stable protection mechanisms as well as QoS-based criteria to judge the quality of resilience mechanisms have to be developed. The criteria may differentiate between the different QoS models, and the network (ad-hoc and wired infrastructure) in which they should apply. Parameters such as network convergence time, allowed packet loss and delay for different applications (voice, streaming video, etc.), are strict related to resilience. In conjunction with this, link state discovery mechanisms have to be developed that can be used to discover running (not failed and not congested) end-to-end paths. This involves the ability to find and use an alternate path to route the emergency traffic around failed points or congestion (see e.g. [17]). The discovery process should be accomplished rapidly and if possible prior to the need arising.

Furthermore, in the special circumstances of a major incident, different mechanisms are needed to compensate for lost data packets. Such mechanisms could be based on Forward Error Correction (FEC), or on redundant transmissions. In the former mechanism, additional FEC data packets could be constructed from a set of original data packets and inserted into the emergency traffic. In the latter mechanism, an original data packet is followed by one or more redundant packets. An example of such mechanism is specified in [18].

Resilience also extends to consideration of redundant access to WED/ED entities. This provides a means of giving emergency users access to multiple points-of-presence, where possible. If a particular WED/ED becomes unduly congested or even fails, transparent handovers to adjacent devices are supported. This requires inter-WED/ED signaling In the case of congestion, priority and/or pre-emption will be given to emergency communication traffic.

The resilience capabilities of the terminal need to be addressed. Terminals will be multi-mode, with access to multiple Medium Access layers. One of these layers is an ad-hoc access capability that exists between various suitably capable terminals and the WED(s) - without recourse to other infrastructure. With ad-hoc operation, the terminal has the ability to forego the use of existing alternative forms of transport, assuming they are even available at a given location, and make the terminal itself act as a logical router.

Mobility and interoperability between GAN and ad-hoc networks and load balancing

The overall objective is to define how the overlay network and the routing are affected by mobility and the mechanisms used in mobility solutions, when emergency telecommunication services have to be supported by the network infrastructure.

The interaction between classical mobility management solutions has been engineered with a single routing-layer in mind, and without consideration of the requirements imposed by emergency telecommunication services and real-time services like voice and video, necessary under many critical circumstances. Therefore this interaction has to be re-engineered with consideration of the requirements imposed by the emergency telecommunications services. The existing mobility support mechanisms may not integrate efficiently and naturally in the layered architecture formed by the introduction of the overlay layer

The solution has to develop scalable mechanisms for an efficient allocation of the resources in a network, particularly as far as link bandwidth and end-edges capacity is concerned. In scenarios with sudden changes in traffic demand (e.g. a moving network in a handover process), these mechanisms should dynamically distribute traffic to benefit from idle resources.

Moreover a GAN aims at providing connectivity for multihop ad-hoc networks, such as VANs and BANs anywhere and anytime. A self-configuring network of mobile hosts (MANET) extends this connectivity in such a manner that a mobile node is able to remain connected to the GAN, even if it is out of the range of a wireless access point (where a WED is located). In this way, mobile nodes have more chances for reaching the GAN. Furthermore, MANETs allow nodes to maintain various routes making more resilient the routing as well as the end-to-end QoS

requirements. New multi-hop ad-hoc network protocols will be developed, that improve the performance of the network in this context, solving several challenges both in the GAN and the ad-hoc network. Such challenges are related to addressing, routing, seamless, resilience, mobility support, security and QoS support.

Several mobility protocols and various mechanisms that achieve performance optimizations on these protocols have been or under development. Concerning the GAN there is a different aspect that should be addressed, namely the interconnection of mobile networks or hosts to various overlay networks. Current mobility management protocols, e.g. in the Internet, rely on a set of basic mechanisms for support of mobile hosts. These are typically terminating the routing at a mobility server in the access domain called the anchor point. Tunnelling is often used from the wireless access router, in the access domain, to a home agent or a local anchor point. The enumerated mobility servers and tunnelling are overlaid the basic routing, creating a strong dependence on the performance of the routing protocols, regarded as "classical" ones. However, these classical protocols were not designed to support emergency telecommunications traffic, real-time and QoS-aware traffic (e.g., voice and video), nor a dynamic network management.

One of the tasks, related to routing and mobility in Overlay Networks, is the identification/inventory of the mechanisms used by the mobility protocols and QoS signaling protocols. The impact of the layered architecture on the functionality of these mechanisms and signaling protocols has to be investigated. Particularly, the need for information at the overlay layer for coordination and decision-making related to mobility management, routing and QoS should be identified. Also a requirement list regarding the layered architecture should be drawn.

Furthermore, descriptions of interactions between mobility functions (mobile anchor point and tunnelling functions) and overlay network within the wired network should be provided. This will implicitly describe an interface between the GAN and the global IP backbones.

The new routing mechanisms, for deployment in the wired domains should smoothly interoperate with the native routing in the various wireless domains. Therefore the challenge of interconnecting mobile hosts, ad-hoc networks, Moving networks, VANs and BANs with the GAN, based on the layered routing approach (from the routing perspective) should be analysed.

Network management

Due to the fast expansion of the existing networks in conjunction with the emergence of many different network technologies, network management proves to be a very difficult task. In order to cope with this task, it is essential to create a logical network for automated network management integrated across diverse environments of heterogeneous networks. Thus, among the key issues to be addressed are management automation and management integration. Automation is needed to ease the task of the manager, thereby lowering operational costs. Integration is needed to reduce response times, despite the dynamic changes that are expected within the future GAN. To smooth the processes of integration and automation, it is important to bridge the traditional gap between network and service management. One promising approach to accomplish this is to adapt to a common middleware technology for management, based on XML and web-services [16].

Security aspects

During the design and deployment of any form of routing protocol, security has to be taken into consideration. Recently the IETF Routing Protocol Security working group (RPSEC) is active on producing an early draft on a generic threat analysis for standard network routing protocols. This is a systematic approach to identify routing-specific threats and vulnerabilities, without attempting to explore the problems of specific routing protocols, but the presumption is that the routing protocols under examination are those of the network and internetworking layers.

Many of these security problems have arisen as a consequence of the prioritization of functionality over security, and the lack of a considered approach to the identification and rectification of generic security threats. An analysis that identifies the actual security requirements in logical networks that are supporting emergency telecommunication services is required. Whilst the analysis that has been carried out for general networks can be educational, there are significant differences between such an environment and the one that we propose to study: in an overlay network, the concept of scalability typically has a rather different meaning than when it is applied to the Internet as a whole. In particular, the number of nodes involved is typically rather small as compared to the size of the general Internet, but the distances between nodes can be large, and the models of network interconnectivity assumed for the Internet may well not apply for such networks. Consequently, completely different routing metrics may apply. Likewise, the overlay nature of the network means that processing costs per message are likely to be relatively high, so the use of more sophisticated metrics, and more complexity and delay in configuring the network is not only tolerable but is often also a wise investment of resources. In addition to performance enhancement, the necessary configuration may also be constrained by primary security requirements – thus, for routed VPNs, the configuration of routing is partly dependent on performance, but can also depend both positively and negatively on whether routes should traverse certain links or pass through certain intermediate nodes.

The problem with a purely generic approach to security service provision is that it would be possible to discuss, practically indefinitely, the need for and nature of such services, the relevant parameters, and the adaptation of their dynamic behavior in response to changing conditions.

Security mechanisms, parameters, and policies change on timescales down to the relatively short term. Consequently, there is a need to investigate mechanisms that allow the definition of various policy issues such as: how routing and forwarding are to be accomplished within a hierarchy; how security associations may be established between links; and, indeed, how, by whom, and under what circumstances the update and management of the various policies may be done. Consequently, a crucial matter is how best the management aspects of security can be captured within a generic toolkit.

For the type of wireless networks that allow multihop communication (ad hoc networks), security issues are rather difficult. The new opportunities that the GAN concept provides in this context need to be analyzed, which basically arise from the possibility of authenticating terminals that are ad-hoc connected to the infrastructure and have an agreement with different operators or service providers but make use of the same GAN.

IV. Conclusions and Future Work

In this paper we present a vision of how ambient intelligent environments may be used in future to support the emergency services during first response to a major incident. We envision a future where emergency workers' Vehicle and Body Area Networks will be nodes connecting to form mobile ad-hoc networks to support intra- and inter-service communications at the scene and to enable health and wellbeing monitoring for the emergency workers and for casualties at the scene. These ad-hoc networks should also be able to communicate to remote nodes, e.g., receiving hospitals and emergency control centres, via the discovered surviving communication infrastructure. We believe the solution proposed above supports the requirements by enabling

- ubiquitous connectivity to ad-hoc networks;
- resilience in face of damaged infrastructure;
- mobility and load distribution;
- adaptive network management.

Amongst the major challenges are

- ensuring security of the emergency telecommunications services especially in terrorist incidents;
- quality assuring the correct operation of services in such dynamic adaptive distributed systems.

The next step is to establish detailed end-user requirements and begin to design and prototype the elements of the solution described in this paper.

Acknowledgment

We would like to acknowledge the consortium that contributed to writing the IST project proposal MAJESTI. Some ideas presented in this paper have been discussed with members of this consortium. The application scenario was first developed with EC support under the IST MOSAIC project and the Ami@Work initiative. We are grateful to Ralph de Wit from the regional trauma centre Medisch Spectrum Twente for his expert inputs as an internist, surgeon and expert on major incident management from the medical perspective.

References

[1] Oosting, "De Vuurwerkramp: Eindrapport", Commissie Onderzoek Vuurwerkramp, Enschede/den Haag, Feb. 28th (2001), ISBN: 90-71082-67-9, (in Dutch, including an English version of the summary "Final Consideration"), http://www.minbzk.nl/contents/pages/00001947/eindrapport_oosting_2-01.pdf

[2] The 9/11 COMMISSION REPORT: Final Report of the National Commission on Terrorist Attacks upon the United States. Executive summary. http://www.9-11commission.gov/report/index.htm http://www.9-11commission.gov/report/index.htm

[3] "Overview and Principles of Internet Traffic Engineering", IETF request for Comments 3272, located at: http://www.ietf.org/rfc/rfc3272.txt?number=3272

[4] I.F. Akyyildiz, X. Wang and W. Wang, Wireless mesh networks: a survey, Elsevier Computer Networks, 2005.

[5] http://www.m-zones.org/

[6] Jones, V.M., Bults, R.A.G., Vierhout, P. A. M., Virtual Trauma Team, 2001c, Wireless World Research Forum meeting, Helsinki, 10-11 May 2001; http://www.wireless-world-research.org/

[7] Jones, V. M., Bults, R. A. G., Konstantas, D., Vierhout, P. A. M,. 2001b, Body Area Networks for Healthcare, Wireless World Research Forum meeting, Stockholm, 17-18 September 2001; http://www.wireless-world-research.org/

[8] MobiHelath project, see: http://www.mobihealth.org

[9] Awareness project, see: http://awareness.freeband.nl

[10] Health service, see: http://www.healthservice24.com

[11] Timm-Giel, A., Amadou, Aust, S., Goerg, C., Ehrichs, L., Kus, M., Wischnewski, M. B., UMTS Application Trials: Teleambulance in the IST project xMOTION, IST Mobile Summit 2003, Aveiro Portugal, June 2003.

[12] Mosaic Project, see: http://www.mosaic-network.org/

[13] AMI@Work Family of Communities, see: http://www.mosaic-network.org/amiatwork/

[14] Jones, V., and Saranummi, N., MOSAIC vision and scenarios for mobile collaborative work related to health and wellbeing. ICE 2005, 11th International Conference on Concurrent Enterprising, University BW Munich, Germany, 20-22 June 2005, AMI@Work Forum Day: Towards Ambient Intelligence at Work, Vision 2010. Proceedings of the 1st AMI@work communities Forum Day 2005, 'Towards Ambient Intelligence at Work 2010', Munich, Germany, 22 June 2005, Marc Pallot & Kulwant S Pawar eds.), ISBN 13 978 0 85358 225 0.

[15] Jones, V. Karagiannis, G., Heemstra de Groot, S., Ad hoc networking and ambient intelligence to support future disaster response, Proc. ASWN 2005, 5th Workshop on Applications and Services in Wireless Networks, June 29 - July 1st, 2005, Paris, pp. 137-146, Hossam Afifi and Djamal Zeghlache (eds.), Institut National de Telecommunications, Groups des Ecoles des Telecommunications 9, rue Charles Fourier, 91011 Evry Cedex, France, (c) 2005 IEEE. ISBN 2-9156-18-08-9

[16] Schonwalder, J., Pras, A., Martin-Flatin, J.P., "On the future of Internet Management Technologies", IEEE Communications Magazine, Vol. 41, No. 10, October 2003, ISSN: 0163-6804, pp. 90-97.

[17] Sharma, V., Hellstrand, F., "Framework for MPLS-Based Recovery", Informational, RFC 3469, February 2003.

[18] Perkins, C., et al., "RTP Payload for Redundant Audio Data", Standards Track, RFC 2198, September, 1997.