# Ad hoc networking and ambient intelligence to support future disaster response

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

*Abstract*— **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. A futuristic scenario is presented where, for each of the emergency services, Ambient Intelligence (AmI) technologies are used to support communication amongst the members of a virtual team. AmI is further used to enable cross service communication and coordination, e.g., between police, firefighters and ambulance teams, which may include transborder and transnational cooperation. The application therefore is an example of extended enterprise computing systems incorporating inter-organisational and international dimensions. It therefore addresses the themes of (AmI enabled) Information and Communication Technologies (ICT) to support inter-enterprise collaboration and collaboration between virtual teams. We examine the future and emerging technologies needed to realize this vision of ambient intelligent support for the rescue services. One of the emerging technologies is ad hoc networking. In this paper we focus on the possibilities and challenges raised by combining fixed infrastructure networks with ad hoc networks to support ambient intelligent services for major incident management.**

*Index Terms*— **Disaster response, ad hoc networking, ambient intelligence, Body Area Networks, telemonitoring.**

## I. Introduction

In this paper we present a futuristic vision of how ambient intelligent environments may be used in future to support the emergency services during first response to a major incident.

A major incident is defined in the MIMMS (Major Incident Medical Management and Support) standard thus: “as any incident where the location, number, severity, or type of live casualties requires extraordinary resources”. Major incidents may arise through natural disasters such as earthquakes, volcanic eruptions or floods, or may be man made. Man made causes may be accidental (such as major transportation accidents) or deliberate (such as large scale acts of terrorism). Experience from around the world shows that communication and coordination are among the main challenges experienced during the first response to major incidents e.g., [2], [3], [4], [5], [6], [7], [8]. Communication and coordination are prerequisites for effective collaboration. “The initial response to a major emergency aims to deal with the first effects. Collaboration, co-ordination and communication are vital” [8]. According to [9], very many casualties of major incidents die because of lack of organization. The 9/11 commission reported that “Effective decision making in New York was hampered by problems in command and control and in internal communications” [2]. Severe communication difficulties were experienced especially following the second attack on the Twin Towers in New York. In this very difficult working situation “incident commanders from responding agencies lacked knowledge of what other agencies and, in some cases, their own responders were doing” [5].

In the first response to a major incident, emergency teams may be drawn from different administrative regions and from neighboring or even distant countries. The communication problems may be further complicated because the incident itself may cause destruction of infrastructure including communications infrastructure. Destruction may be ongoing so the communications landscape may itself be rapidly changing, deteriorating through loss of nodes and reduction in bandwidth at the same time as demand increases. In this dynamic situation we envision a future scenario where the emergency vehicles and the Ambient Intelligence (AmI) suits of the emergency workers can provide the basis for mobile ad hoc networking to support intra- and inter-organizational communications, thereby facilitating smooth C3 (Command, Control and Communication).

In section II below the futuristic scenario is elaborated. For each of the emergency services, AmI technologies are used to support communication amongst the members of a virtual team. Moreover AmI is used to enable cross service communication and coordination, for example between local government emergency coordinators, police, firefighters and ambulance teams from different regions. In this hypothetical case transborder cooperation is also needed.

In section III we examine some of the future and emerging technologies needed to realize this vision of ambient intelligent support for the rescue services. In section IV we look at networking issues raised in the context of infrastructure networks and, then examine the possibilities and challenges raised by the use of ad hoc networks in major incident

Manuscript received April 4, 2005. The Major Incident Scenario was developed as part of the work of the MOSAIC project (FP6-IST-2003-2 004341) and under the AMI _AT _WORK [1] initiative of the New Working Environments Unit of the European Commission’s Information Society Technologies programme. Part of the work discussed in this paper was funded by the European Commission under the IST project MAGNET [37].

[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

management. In section V we present discussion and conclusions. First we present the illustrative scenario.

## II. MAJOR INCIDENT SCENARIO

This section elaborates the Major Incident scenario, which is a hypothetical futuristic scenario set in a fictional European location. The scenario draws on existing European disaster plans and on experience from actual incidents in Europe, Asia and the United States. The scenario projects one possible future under the assumption that certain Information and Communication Technologies (ICT) will be available and sufficiently mature to support ambient intelligent (mobile) applications. Some of the enabling technologies implied are indicated in angle brackets.

*At 5.02 am a loud bang wakes the city of Dorpstadt. The Mayor gets up and looks out of the bedroom window. He sees an orange glow and a plume of smoke beginning to rise from somewhere close to the centre of the city. He receives an audio call on his home AmIE (Ambient Intelligent Environment); it is a call from Anna - the city council official who is nominated as the emergency coordinator. It seems that a big explosion has occurred (cause unknown) which rates at least as a serious incident, possibly a major incident. The Mayor gets dressed and sets off for the town hall, which is outside the affected zone. If the town hall was affected the mayor would use one of the secondary control centres located outside the town. The town hall is to act as the regional control centre and emergency communications centre according to the regional Emergency Plan. As he drives the half a kilometer to the town hall he continues his conversation with Anna via his car AmIE <Personal Area Network (PAN)-PAN seamless handover, Personal Networks (PNs)> with Anna, who is also on her way to the town hall. The mayor is not surprised to see people appearing on the streets and traffic going in all directions at an hour when the streets are usually empty. As the mayor arrives he sees Anna and other members of staff arriving.*

*The mayor takes the decision to activate the regional emergency plan. As a first priority the Mayor and Anna need information about the current situation on the ground. Situation assessment must include an assessment of location and extent of the affected area, assessment of casualties and also an assessment of any further threat, which depends on knowing the location and cause of the explosion and awareness of any additional risk factors such as chemical- or bio-hazards in the proximity. The mayor asks the office AmIE (the ambient intelligent office environment) to call the chief constable and at the same time asks the AmIE to punch up the traffic cam outputs to the wall display screens in his office. On another screen the AmIE flips through national and local TV channels to check for news bulletins and live broadcasts but it seems no TV crews have arrived at the scene yet. The traffic cams show traffic beginning to build up at junctions. Some cams are out – their distribution on the electronic map <Geographical Information Systems (GISs)> on another of the AmIE wall displays shows the location and extent of the worst affected area. Anna is meanwhile enacting the emergency protocol. The protocol activates the emergency command and control arrangements, the emergency communication centre and the setting up of a public information line and emergency centres for the public. Under this protocol the town hall AmIE connects to the shared emergency services communication network (a secure network routed over the Euro GRID high performance ICT facility <Virtual Private Networks (VPNs), GRID computing>). According to the protocol, the emergency response coordination function is distributed across the local government officers, central government, and the emergency services' control centres, with clear lines of command for overall control and for on-the-ground operations. As the protocol is activated, the AmIE wall display of the city at each centre is automatically augmented with the combined displays of the other services <information sharing>. All of them show the area that is most badly affected (it soon becomes known by the locals as The Zone) as a 'dark' area where their respective communication systems have been knocked out.*

*Meanwhile the fire service's regional control centre has dispatched all available on-call fire fighting teams from the district and the ambulance control centre is dispatching (road) ambulances to the scene and has requested the air ambulance service based 120 km away in the capital to supply all available air ambulances. These will be used to ferry in traumatologists and anaesthesiologists, also extra paramedics from other regions, and to evacuate casualties.*

*At the main police station the officers of the night watch view the police surveillance cams in the city centre as soon as they hear the first explosion. Like the traffic cams, some of the police cams are not sending (they have been damaged or destroyed in the explosion). The officers get a further view by calling up high resolution satellite images <Galileo> onto one of their AmIE walls. According to the plan, police units are moving into the area and military units are on alert in case they are needed. The police units' movements are superimposed on the satellite picture <augmented reality>.*

*Elsewhere in the city barriers are being broken out of storage and transported to the scene. A cordon will be needed to control access in and out of the affected zone, to ensure that emergency service can get access.*

*The explosion has affected a half kilometer radius from the epicenter, destroying a factory, many shops and two hundred homes. It has also taken out the communications infrastructure in the area. This includes fixed telephone lines, surveillance and traffic cameras and cellphone antennas.*

*At 5.43 there is another loud bang. Another massive explosion has occurred. More police surveillance cams and traffic cams go black.*

*The police are coordinating access to the Zone for emergency vehicles whilst trying to control the public who are now converging on the Zone: some desperately trying to get into the Zone to check on their homes or to find missing* *friends or family members, others drawn by curiosity and the drama of the situation to view the spectacle. Press photographers and TV crews have arrived and are broadcasting live footage. Some 'walking wounded' are stumbling away from the Zone.*

*The positions of the police units are tracked on the AmIE walls at the police station superimposed on the satellite pictures and the city GIS map, as are the locations of the ambulances and firefighting teams who are converging on the scene. Vehicles show up as moving squares and individual team members as moving dots.*

*Michelle and Paul were one of the first ambulance teams to arrive at the scene. The paramedics know that more serious casualties await them closer to the epicentre of the explosion. They have audio communications built into their headsets and are talking with ambulance control and to the surgical team at the local hospital as they drive into the Zone. They can see burning buildings and thick black smoke. They are also talking to the police who are coordinating the emergency services at the scene. They also talk to the fire service control who tell them that it is not safe for the ambulance to proceed further. They stop the ambulance. Casualties are being brought out of burning buildings by the firefighters. The paramedics begin triage and treatment. (Triage is the assessment of casualties' injuries in order to prioritise and target help most effectively.)*

*Staff at the ambulance control centre and at the hospital are viewing the scene through 6 cameras mounted on the exterior of the ambulance and also through the paramedics' head mounted cameras; they can zoom and pan the cameras remotely to get a better view without the paramedics having to do anything. The hospital staff can give advice if requested and can make some clinical assessment to help to prepare the A&E departments to receive the casualties.*

*As the emergency vehicles move into the Zone the communication blackspot begins to disappear on the AmIE displays. The AmIE systems of the emergency vehicles and of the emergency staff themselves are automatically connecting to each other forming a mobile communications network <mobile ad hoc networking>, thus plugging some of the gaps in the damaged fixed infrastructure.*

*As they begin to help their first casualty the paramedics continue to talk to the hospital staff and have an open link to receive messages from the police and fire services coordinators. The coordinators may need to advise them to pull out because of imminent threat of further explosion. At the same time the paramedics' AmI-suits are querying the casualty's wearables and implanted devices <ad hoc networking, resource discovery> to see if they can get ID and emergency dataset and link to the casualty's Electronic Medical Record (EMR) at the hospital. With luck the casualty may be wearing their own sensors <wireless sensor networks> which also can provide vital signs data. If not (or if damaged) the paramedics can apply a stick-on vital signs monitoring system <Body Area Network (BAN)> to the casualty. Now they can see a transparent visualisation of the vital signs as a moving holo head-up display The vital signs are also superimposed on the hospital staff's display, showing each casualty's vital signs readouts hovering transparently over their video image <augmented reality, mixed realities>. Stretchers, neck braces and spinal boards also have built in sensors which can transmit vital signs. The paramedics' own biosignals including stress indicators are being continuously monitored by the sensors in their AmI-suits < wearable computing, smart fabrics, interactive textiles>.*

*Firefighter and police AmI-suits are similarly equipped with sensors and built in audio-visual communication devices. Firefighters' AmI suits also monitor their air supply and measure environmental factors including external temperature, Carbon Monoxide (CO) and Carbon Dioxide ($CO_2$), and can warn firefighters to get out of a building when flashover signs are detected for example. High resolution positioning devices in the firefighter AmI suits help remote coordination of search of smoke-filled buildings for victims and improve chances of finding and rescuing injured firefighters as well as casualties.*

*Off duty paramedics living close by are arriving at the scene on foot. Their body-worn AmI devices register them with the ambulance control centre <ad hoc networking, identification and authentication> and they are directed to the place they can be of most use. Traumatologists and anaesthesiologists are now in route to the scene in a variety of transports including cars, ambulances and air ambulances. They will operate on patients who are trapped at the scene or too unstable to be moved. In each of the transports the emergency medical staff can communicate via the in-vehicle AmIE with other members of the virtual trauma team via ad hoc networking, the highway AmI infrastructure and the Euro GRID backbone.*

*During eventual transfer of a casualty to hospital the AmI ambulance maintains communication between the ambulance paramedics and the distant members of the trauma team. The AmI ambulance connects <mobile ad hoc networks, Beyond 3rd Generation (B3G)> with the AmI highway networks or via other AmI infrastructures (such as AmI homes) as it passes through urban or rural environments. Video of the patient can be transmitted to the hospital from the 6 cameras inside the ambulance and the patient's vital signs continue to be transmitted during the transfer.*

*Because of the number of casualties some patients are taken to a hospital over the border in the neighbouring country, which has also sent its own ambulances and air ambulances. Fortunately language is no difficulty since the AmIEs can detect and simultaneously translate all European Union (EU) languages (and some others).*

Our scenario covers Phase One only, but the AmI systems must ensure that information collected in Phase One is made accessible, with appropriate access controls, to the professionals involved in the subsequent phases of the operation.

Fig. 1 illustrates some of the possibilities for ad hoc networking between mobile nodes (emergency vehicles and emergency personnel) and thence to fixed nodes such as hospitals and emergency services control centres.

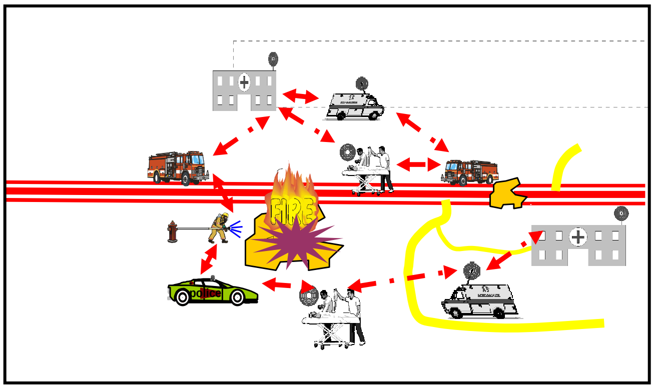

Fig. 1: Ad hoc networking between emergency services: logical view

## III. TECHNOLOGIES INVOLVED

First we offer a definition of ambient intelligence, then we describe some of the specific technologies needed to support ambient intelligence.

### A. *Ambient Intelligence*

Ambient Intelligence (AmI) refers to intelligent processing and communication services distributed transparently throughout the surrounding (physical) environment. The purpose is to provide various functionalities to users, by making the environment act in a smartly adaptive, assistive and anticipatory way. AmI services must have properties of persistence, pervasiveness, adaptability, transparency and seamlessness, and above all be human-centric.

### B. *AmI technologies*

The AmI vision in general assumes a large number of interoperating devices, including sensors, actuators and devices performing information storage, processing and communication, embedded in the surrounding physical environment. The devices may be embedded in intelligent surfaces and materials or worn on the body (e.g., embedded in smart fabrics and interactive textiles) or even within the body (smart implants). The very density of devices requires that they be low power, low cost, miniature (down to nano scale), and characterized by redundancy in order to offset failure of individual devices. The (huge number of) devices must cooperate together to provide services characterised by intelligence and context sensitivity, requiring novel service, application and networking functions. Devices may communicate via wireless or wired technologies (or a combination) and subnetworks may be organized according to advanced networking concepts such as BANs, Intra Body Networks (IBNs), PANs and PNs. Network mechanisms and protocols will need to support highly dynamic network (re)configuration, such as self-organising networks and ad hoc networking.

In the following section we focus in on some of the networking issues raised by the major incident scenario of Section II.

## IV. NETWORKING ISSUES IN MAJOR INCIDENT MANAGEMENT

The emergency services have traditionally used fixed infrastructure support for emergency communications (eg TETRA, public cellular systems or other access systems which allow access to internet). Mobile phones were found to be invaluable in the Asian Tsunami disaster as a means of voice communications and location: “mobile phone networks turned out to the best and most non-vulnerable methods of communication in the face of the terrible earthquake-tsunami. The disaster points out the new communication and location capabilities of mobile networks while at the same time it cries out for even more robust and disaster hardened systems and special emergency abilities and organizations. The cost of global emergency preparedness would be negligible compared to totally fixed systems or to the savings in human and material costs in large scale crisis” [6].

However cellular networks depend on infrastructure (antennas) remaining intact. When infrastructure is destroyed in a large scale incident, ad hoc networks may provide the only communication possibility for the emergency services by providing islands of communication whereby the professionals at the scene may communicate with each other. Further, ad hoc networks may also be able to connect to nodes in the surviving infrastructure, thereby bridging to, and plugging the gaps in, the infrastructure networks. We expect that future emergency networks will use such a combination of infrastructure and ad hoc networks; however since they have different properties the possibility of combining the two brings new technical challenges. In the following sections we discuss some of the end-to-end issues associated with infrastructure networking for emergency telecommunications services and then look at the consequences of introducing ad hoc networking into the picture.

### A. *End-to-end networking issues*

Many end-to-end networking issues which have a special bearing on disaster and major incident management can be identified, see [10], [11], [12], but the most significant ones are related to end-to-end addressing, resilience in the wired infrastructure, mobility, quality of service and security. We designate the communication service which has to be supported in this scenario as the *emergency telecommunications service* and the supported communication traffic as the *emergency traffic*.

Before discussing end-to-end networking issues and solutions for emergency telecommunications services we have to consider that these solutions cannot rely on ubiquitous or typical inter-domain communication solutions along the path between the end points. This is due to the fact that there may exist islands that are realized in the form of overlay networks or where these solutions will be constrained and used only by the entities which are supporting the transport and application layers. Another consideration is related to the fact that the emergency telecommunications services might have to use existing architectures and protocols from different standardization bodies, such as International Telecommunication Union (ITU) and Internet Engineering Task Force (IETF). A more extended list of such requirements and considerations can be found in [13].

### *1) End-to-end addressing*

A device can only participate in a data/voice communication if other devices can reach it. This can be accomplished by using Internet Protocol (IP) addresses that are either globally unique or unique within a local/private domain. Devices using the former type of IP addressing can be reached by any device located anywhere in the Internet. In the latter type of IP addressing, devices that are located outside the local/private domain cannot directly reach devices using the latter type of IP addressing. This problem can however be solved by using certain methods such as the Network Address Translation (NAT) [14]. The main disadvantage of using methods such as NAT is that NAT elements become critical infrastructure elements: if they fail, all communication through them fails, and, unless great care is taken to assure consistent, stable storage of their states, even when they recover, the communication that was passing through them will still fail. In major incident scenarios this disadvantage is of huge significance and therefore the former type of IP addressing would be more appropriate.

Due to the large numbers of embedded devices involved in provisioning Ambient Intelligent services, very large IP address spaces are needed. IPv6 [15], [16] provides a giant leap in this direction but at some point even this larger address space will be flooded if AmI were to be deployed on a large scale throughout Europe or worldwide.

### *2) End-to-end mobility*

This networking issue is associated with how the end-to-end connectivity and routing are affected by the mobility of the mobile devices and the mechanisms used in mobility solutions. The interaction between mobility management solutions and routing protocols has to be engineered with consideration of the requirements imposed by the emergency telecommunications services.

A mobile device should be able to continue using its IP address as it moves among different IP sub-networks, (e.g., when a mobile device is moving from a WLAN technology coverage into a cellular technology coverage). The required networking functionality should support transparency above the IP layer, including maintenance of active TCP connections and UDP port bindings. This could for example be accomplished by using the Mobile IP protocol ([17]).

### *3) Resilience in the wired infrastructure*

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 have to be developed.

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. 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. [18]). The discovery process should be accomplished rapidly and if possible prior to the need arising.

### *4) End-to-end fault tolerance*

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. An example of such mechanism is specified in [19].

In the latter mechanism, an original data packet is followed by one or more redundant packets. An example of such mechanism is specified in [20].

### *5) End-to-end Quality of Service*

QoS is defined as the performance level of a service offered by the network to the user. Different applications have different requirements and therefore different QoS requirements. For multimedia applications, throughput, delay, and delay jitter are the most significant QoS parameters, while for military applications security is an essential issue. In the case of emergency management, network availability is the most important parameter.

QoS provisioning requires special measures to be taken in the network in order to guarantee a service, negotiation between host and network, call admission control, resource reservation, and priority scheduling of packets. QoS provisioning mechanisms are classified into hard QoS and soft QoS. In hard QoS, the requirements must be guaranteed to be met for the complete duration of the session. In soft QoS, guarantees are given within certain statistical bounds.

There are situations where a communication network is fully used by typical (existing) traffic at the moment that an emergency telecommunications service needs to use this network. Therefore, the QoS provisioning supporting the emergency traffic must be distinguished from the QoS provisioning supporting other typical traffic. A general requirement is that in all major incident scenarios the emergency traffic should be assigned a higher priority than the existing, typical traffic.

In some circumstances both types of traffic, typical and emergency, have to be treated as non-preemptive in nature. In some situations national regulations or legislation may prohibit preemptive actions (e.g., dropping existing ongoing flows, such as the telephony flows). In this situation QoS signaling and/or QoS provisioning architectures have to be applied. Examples of QoS signaling protocols are the Resource Reservation Protocol (RSVP) [21] and the protocols that are being developed within the IETF NSIS working group [22]. Examples of QoS architectures are the Integrated Services [23] and the Differentiated Services [24] architectures.

In other situations national legislation and/or regulations allow or even *require* the preemption of the emergency telecommunications services. In this case new signaling and provisioning mechanisms have to be developed to ensure that the emergency traffic is always pre-empted in relation to ongoing typical flows, such as dropping on-going telephony calls, e.g. [61].

The above disparity could be managed using a local policy that determines the level at which the emergency traffic is preempted and affects the existing typical traffic load in a communication network. This policy could be maintained in centralized gateways, or distributed at several network entities. Furthermore, this policy could be configured statically or dynamically using a signaling protocol such as COPS [15].

#### 6) *End-to-end security*

The most significant security threats raised by the support of the emergency telecommunications services are described in the following subsections.

***Denial of Service.*** As mentioned in Section IV.A.5, emergency traffic may get a higher priority than existing typical traffic. A network which supports such emergency telecommunications services could be abused to enhance the effectiveness of denial of service attacks. The priority feature could severely magnify the threat of attacks on bandwidth availability in lower capacity links and on reserving and using resources on an end-to-end basis. Therefore, any network provider who supports a priority mechanism must carefully apply the associated access control and security mechanisms.

***User authorization.*** In order to prevent the theft of service and to reduce the threat of denial of service attacks, it is crucial that the network provider verifies the authorization of the emergency telecommunications service request before accepting the request and providing the service with priority facilities.

***Confidentiality and integrity.*** When emergency telecommunications services are being used it is very important that communication is protected such that the information carried cannot be intercepted and/or altered to exacerbate the disaster situation. This could for example occur in the situation where orders are deliberately intercepted and altered by third persons to cause further damage. Therefore, the confidentiality and integrity of such communications should be protected using as far as possible end-to-end security protocols, such as IPSec [26].

### B. *Ad hoc networks for emergency management*

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.

Fig. 2 shows an example of a combination of fixed infrastructure networks with several forms of ad-hoc networking for supporting emergency services. Different forms of ad hoc communication take place, involving rescue workers, emergency vehicles, personal networks, devices, etc. Many different radio technologies are likely to be involved. In addition, the ad-hoc network may communicate with the fixed infrastructure using a variety of systems and radio interfaces. Service continuity needs to be supported in presence of mobility and unreliable channels.

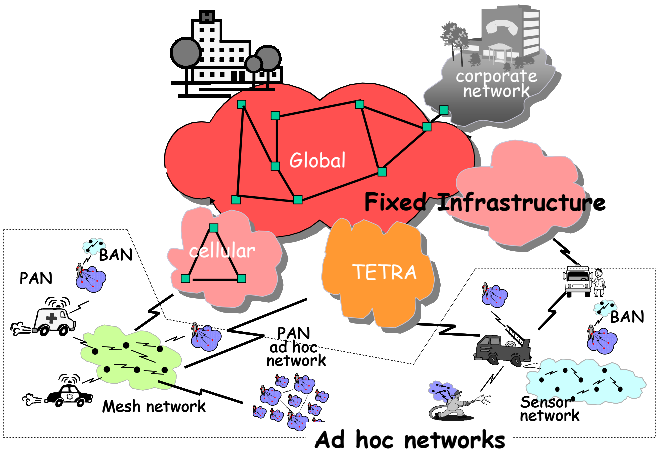

Fig. 2: Ad-hoc and infrastructure-based networking for emergency support.

Extensive research in ad hoc networks has taken place in the last years leading to a better understanding of the problem and to substantial progress in the field. However, many research issues need still to be solved in order to be able to able to meet the requirements posed by emergency scenarios. The rest of this section is devoted to the discussion of some of the most important challenges in ad hoc emergency networks, as well as to emerging technologies that will influence developments in this area.

#### 1) *Address Autoconfiguration*

Address configuration is an important issue in ad hoc networking. Assigning a unique address to each device in a network is a prerequisite for participation in the network. It is the first essential parameter that must be configured to enable the participation of a host in a network. In fixed networks, hosts rely on centralized servers like Dynamic Host Configuration Protocol (DHCP) [27]. However, in general this approach cannot be extended to mobile ad-hoc networks due to their highly dynamic topology. As a consequence, an autoconfiguration protocol is required to enable dynamic assignment of network addresses.

The main task of an address autoconfiguration protocol is to efficiently manage the address space by selecting, allocating and assigning a unique network address to an unconfigured node. In addition, it should take care of de-allocating addresses when nodes leave the network. One of the major challenges is the merging and splitting of networks. Address conflicts may arise when networks merge, requiring some nodes to acquire new addresses. In addition, autoconfiguration protocols need to take into account the particular properties of ad hoc networks such as dynamic topology, unreliability of wireless links, multihop topology, bandwidth scarcity as well as the computational and energy limitations of some of the nodes.

Several methods have been proposed for dealing with this problem in ad hoc networks (see [28] for a survey). The approaches can be classified as statefull and stateless. Statefull protocols maintain an address allocation table in either a centralized or distributed manner. Centralized protocols relay on a permanent reachable node for configuration. Distributed approaches in contrast allow every node to select addresses for unconfigured nodes; synchronization measures need to be taken to avoid assignment of duplicate addresses. In stateless protocols, unconfigured nodes self-assign addresses and rely on a Duplicate Address Detection (DAD) procedure to verify uniqueness. The DAD is the most important component of these protocols. DAD procedures may be either independent or integrated with the routing protocol. Hybrid approaches that combine some elements of statefull and stateless have also been proposed.

Although many of the presented solutions are promising, there are still many limitations that need to be overcome. More research is needed in order to find scalable and robust solutions that are able to deal with the limited computational resources of some of the devices that compose an emergency network.

### *2) Routing*

Routing protocols for ad hoc networks has been the subject of extensive research over the past several years. A mobile ad hoc networking (MANET) activity [29] was formed within IETF to develop a routing framework for IP-based protocols in ad hoc networks. Although this work resulted in very many algorithms, still many issues are open, including multiparameter optimization, multimode (reactive-proactive) behaviour, context awareness and scalability.

Another issue in ad hoc routing is the protection against routing-disruption attacks. Conventional ad hoc routing protocols lack mechanisms to protect them from disruptions from malicious nodes. Examples of attacks are the intentional modification or falsification of routing information. Protection measures are in many cases specific to the routing algorithm. Although various security extensions have been proposed for existing protocols (see for example [30]), many of these extensions remove important performance optimizations. A major challenge is the design of efficient routing protocols that have both strong security and high network performance.

### *3) Quality of Service*

Hard QoS is very difficult to provide in ad-hoc networks. Most of the reported work on QoS for ad hoc networks provides soft QoS solutions.

QoS support in wireless ad hoc networks is an active area of research with many challenges due to the lack of central coordination, mobility of the hosts and limited availability of resources. An excellent survey of challenges and solutions for QoS in ad hoc networks can be found in [31].

### *4) Security*

The use of wireless links together with their ad hoc nature makes emergency networks considerably more vulnerable to attacks than wired fixed networks. Possible attacks in emergency networks range from *denial of service* or *passive eavesdropping* to *impersonation* and *corruption of messages*. Eavesdropping might give an adversary access to secret information, thus violating confidentiality. Active attacks might allow the adversary to *delete messages*, to *inject erroneous messages*, to *modify messages* and to *impersonate a node*, thus violating availability, integrity, authentication and non-repudiation.

In addition, nodes roaming in a hostile environment with relatively poor physical protection may easily be compromised. Malicious attacks may not only come from outside the network, but they may originate from within the network by compromised nodes.

Entity authentication can be sufficient to verify the trust level of each node in the network so that correct execution of critical network functions is assured. Such an a priori trust can only exist in a few special scenarios, where a common, trusted authority manages the network. However, this is mostly not the case for emergency networks operating in ad-hoc mode. With lack of a-priori trust, classical network security mechanisms based on authentication and access control cannot cope with the security problems on the ad hoc networking level. Cooperative schemes which try to avoid the need of centralized authorities have been proposed. Examples of authentication approaches for ad hoc networks are threshold cryptography [32], re-arranged shared secret [33], self-organized infrastructure [34], and progressive authorization [35].

### *5) Personal networks*

A new person-centred concept which is expected to play an important role in spontaneous networking for emergency applications is PN [36]. PN is a new concept related to pervasive computing with a strong user-focused view as developed within the IST MAGNET project [37]. PNs are distributed personal environments where people interact with a variety of devices not only in their close vicinity but potentially anywhere. PNs are configured in an ad hoc fashion, as the opportunity and the demand arise, to support personal applications. The heart of the PN is a PAN, which is physically associated with the owner of the PN. Unlike present PANs, which have limited coverage, the span of a PN does not have geographic restrictions, incorporating devices regardless of their geographic location. The extension of the PAN with remote devices will physically be made via infrastructure-based networks, e.g., the Internet, an organization's intranet, or via ad hoc networks such as other persons' PNs, a vehicle area network or a home network.

Short range technologies, as those being standardized by the Institute of Electrical and Electronics Engineers (IEEE) 802.15 Working Group on Wireless PANs (WPANs) [38], play an important role in PNs. IEEE802.15.1 defines the lower transport layers of the Bluetooth™ wireless technology while Bluetooth SIG [39] takes care of the upper layers. Similarly, for low data rates, IEEE802.15.4 focuses on the standardization of the lower layers and the Zigbee Alliance [40] concentrates on the higher layers. The IEEEP802.15.3 high rate task group [41] is working on new standards for data rates above 200 Mbps.

#### *6) Wireless mesh networks*

Mesh networking is a relatively new technology based on ad hoc networking that is undergoing rapid progress. Wireless mesh networks (WMN) [42] consist of mesh routers and mesh clients. Mesh routers usually have minimal mobility while mesh clients can be stationary or mobile nodes. Mesh routers form the backbone of the WMN providing network access for both mesh and conventional clients. Integration with other networks, such as e.g., Internet, cellular, Wireless-Fidelity (Wi-Fi) or sensor networks, can be accomplished via gateway or bridging functionality present in the mesh routers. The attractive capabilities of WMN such as self-configuration, self-organization, robustness, low-cost and ease of deployment makes this technology very promising for many applications including emergency networks.

There are already several companies offering mesh networking products. However, there are many issues that need to be solved to make full use of this concept, in particular scalability and performance. This has triggered many academic and industrial activities dedicated to enhancements of existing technologies as well as to the definition of new specifications for mesh networks.

#### *7) Wireless sensor networks*

Sensor networks is another field which is developing very rapidly, enabling many diverse applications such as environmental monitoring, monitoring of biological signals, sensing and diagnostics, security, surveillance and monitoring of structures. Networks of sensors and actuators are essential underlying technologies for enabling AmI. The design of sensor networks is influenced by many factors, including fault tolerance, scalability, cost, operating environment, topology, hardware constraints, transmission media and, in particular, power consumption. Each of these enforces specific requirements not found in traditional networking on all layers of a sensor node protocol stack. Although many results have already been published, research in sensor networking is still in its infancy. Fundamental technical advances are needed for the large scale deployment of sensors that is envisaged in fully fledged AmI for emergency situations.

## V. DISCUSSION AND CONCLUSIONS

Out of all the technological developments implied by the future vision of AmI for disaster management, we have focused here on networking issues. In particular we examined some possibilities and challenges raised by combining fixed infrastructure networks with ad hoc networks and examined some possible current and emerging technical solutions.

Some of the requirements for coordination and interoperability between emergency services are already being addressed. For example, in the Netherlands, in 1997 the C2000 [43] project began implementing a digital two-way radio network supporting voice, data and paging, using the TETRA standard. C2000 provides interoperability between police, fire brigade, ambulance service and military police and offers cross-border 'Schengen' interoperability with Belguim and Germany. The Twente Region of the Netherlands, which suffered a major incident in 2002, is currently rewriting its disaster plan according to the MIMMS standard, which integrates the procedures of the three emergency services.

At time of writing the Netherlands is one of 30 countries to ratify the Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations. The convention came into force on 8 January 2005 and “calls on States to facilitate the provision of prompt telecommunication assistance to mitigate the impact of a disaster, and covers both the installation and operation of reliable, flexible telecommunication services” [44]. It also makes provision for waiving of regulatory barriers relating to importation and use of telecommunications resources in the context of (international) disaster response operations. Signatory states must develop a telecommunication action plan as part of disaster preparedness planning.

Work at the University of Twente on Body Area Networks in the European project MobiHealth [45-59] and the Dutch project Awareness [60] lays the foundation for future ambient intelligent BANs, such as the AmI suits for emergency service workers described in this paper.

These developments can be seen as the start of a trajectory leading towards future ICT support based on sophisticated AmI technologies. Clearly, similar principles are relevant to all kinds of large scale (natural or man-made) accidents or disasters including large scale terrorist attacks and the potentially much larger scale natural disasters such as the 2004 Asian Tsunami. Some of the principles and ideas relating to ICT/AmI support for emergency and disaster response can also be extrapolated into routine scenarios such as homecare for chronically ill, elderly or disabled, or self-care and wellness management for today’s highly mobile citizens.

## ACKNOWLEDGMENT

The Major Incident Scenario was developed as part of the work of the MOSAIC project (FP6-IST-2003-2 004341) and under the AMI _AT _WORK [1] initiative of the New Working Environments Unit of the European Commission's Information Society Technologies programme. Our grateful thanks go to the following domain experts who kindly gave their expertise in validation of the scenario: Ralph de Wit, surgeon, Medisch Spectrum Twente, The Netherlands; Theo Dohmen, former director of the Information Centre "Vuurwerkramp Enschede"; and Alastair Norman, of Leeds University Business School.

Some of the ideas discussed in this paper have been elaborated within the European IST project MAGNET [37]. We would like to express our gratitude to the European Commission for funding this project.

## REFERENCES

[1] AMI _AT _WORK http://www.amiatwork.com

[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] BBC News: world edition, "Failures in NY attack response", August 3rd (2002), http://news.bbc.co.uk/2/hi/Americas/2170907.stm;

[4] Enschede Ramp dossier, Tubantia http://www.tctubantia.nl/krant/tc/ramp/index2.html

[5] THE 9/11 COMMISSION REPORT: Extracts of Report Relating to First Responder and Other Emergency Communications, Information Sharing, Emergency Preparedness and Response. MESA project report http://www.projectmesa.org/ftp/SC/SC09_Sophia_2004/

[6] Tsunami communications, MobileMonday Weekly, January 4, 2004, http://www.mobilemonday.net/mm/

[7] 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

[8] Dealing with Disaster, HTTP://WWW.UKRESILIENCE.INFO/CONTINGENCIES/DWD/C2A MANAGEMENT.HTM**]**.

[9] MIMMS Major Incident Medical Management and Support, Advanced Life Support Group, BMJ Books, ISBN 0727913913, 2002.

[10] Internet Emergency Preparedness (ieprep), IETF Working Group: http://www.ietf.org/html.charters/ieprep-charter.html

[11] Carlberg, K., Brown, I., Beard, C., "Framework for Supporting Emergency Telecommunications Service", IETF Internet draft, draft-ietf-ieprep-framework-10.txt, Oct. 2004.

[12] ITU, "International Emergency Preparedness Scheme", ITU Recommendation, E.106, March 2000.

[13] Carlberg, K., Atkinson, R., "General Requirements for Emergency Telecommunications Service", Informational, RFC 3689, Feb 2004

[14] Egevang, K., Srisuresh, P., "Traditional IP Network Address Translator (Traditional NAT)", Informational, RFC 3022, January 2001.

[15] Deering, S., Hinden, R., "Internet Protocol, Version 6 (IPv6) Specification", Proposed Standard, RFC 2460, Dec., 1998.

[16] Hinden, R., Deering, S., "Internet Protocol Version 6 (IPv6) Addressing Architecture", Proposed Standard, RFC 3513, April, 2003.

[17] Johnson, D., Perkins, C., Arkko, J., "Mobility Support in IPv6", Proposed Standard, RFC 3775, June, 2004.

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

[19] Rosenburg, J., Schulzrinne, H., "An RTP Payload Format for Generic Forward Error Correction", Standards Track, RFC 2733, December, 1999.

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

[21] Braden, R., et. al., "Resource Reservation Protocol (RSVP) Version 1, Functional Specification", Proposed Standard, RFC 2205, Sept. 1997.

[22] Next Steps in Signaling (nsis), IETF Working Group: http://www.ietf.org/html.charters/nsis-charter.html

[23] Braden, R., et. al., "Integrated Services in the Internet Architecture: An Overview", Informational, RFC 1633, June 1994.

[24] Blake, S., et. al., "An Architecture for Differentiated Service", Proposed Standard, RFC 2475, Dec. 1998.

[25] Durham, D., Boyle, J., Cohen, R., Herzog, S., Rajan, R., Sastry, A., "The COPS (Common Open Policy Service) Protocol", Proposed Standard, RFC 2748, Jan., 2000.

[26] Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", Proposed Standard, RFC 2401, Nov., 1998.

[27] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., Carney, M., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Standards Track, RFC 3315, July 2003.

[28] K. Weniger and M. Zitterbart, "Address Autoconfiguration in Mobile Ad Hoc networks: Current Approaches and Future Directions", IEEE Network, July 2004, Vol.18. No.4, PP-6-14.

[29] IETF WG Charter. http://www.ietf.org/html.charters/manet-charter.html

[30] P. Papadimitratos and Z. Haas, "secure Routing for Mobile Ad hoc Networks, Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonia, USA, January 2002.

[31] T. Bheemarjuna Reddy, I. Karhigeyan, B.Y. Majo, C. Silva Ram Murthy, "Quality of service in ad hoc wireless networks: a survey of issues and solutions", Elsevier journal on Ad Hoc Networks, 2004.

[32] L. Zou and Z.J. Haas, "Securing Ad Hoc Networks", IEEE Network Magazine" , Vol13, No 6, Nov 1999.

[33] B. DeCleene et al, "Secure Group Communications for Wireless Networks, MILCOM 2001.

[34] J.P. Hubaux, L. Buttyan, and S. Capkun, "The Quest for Secity in Mobile Ad Hoc Networks", Proc. Of the ACM MobiHoc 2001, Long Beach, USA, October 2001.

[35] R.R.S. Verma, D. O'Mahony and H. Tewari, "Progressive Authentication in Ad Hoc Networks," in Proceedings of the Fifth European Wireless Conference, Barcelona, Spain, February 24-24, 2004, pp. 511-517.

[36] Ignas G. M. M. Niemegeers, Sonia M. Heemstra de Groot, "Research Issues in Ad-Hoc Distributed Personal Networking", Wireless Personal Communications: An International Journal, Volume 26, Issue 2-3, Pages 149-167, Kluwer Academic Publishers, August 2003.

[37] IST MAGNET, http://www.ist-magnet.org/.

[38] IEEE 802.15 WG for WPAN http://grouper.ieee.org/groups/802/15/

[39] Bluetooth the official website http://www.bluetooth.com/

[40] Zigbee Alliance homepage http://www.zigbee.org/

[41] IEEE802.15.3 TG http://www.ieee802.org/15/pub/TG3.html

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

[43] C2000 project
http://www.mobilecomms-technology.com/projects/dutch/
http://www.tetraturkey.com/english/frm_index/ref.html

[44] ITU Press Release: Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations http://www.itu.int/newsroom/press_releases/2005/01.html

[45] Jones, Val, Rob Kleissen, Victor V. Goldman (1999), Mobile applications in the health sector, Presentation at Mobile Minded Symposium, 22 September 1999, University of Twente.

[46] Jones, V. M., Bults, R. A. G., Konstantas, D., Vierhout, P. A. M., 2001a, Healthcare PANs: Personal Area Networks for trauma care and home care, Proceedings Fourth International Symposium on Wireless Personal Multimedia Communications (WPMC), Sept. 9-12, 2001, Aalborg, Denmark, http://wpmc01.org/, ISBN 87-988568-0-4

[47] Val Jones, Richard Bults, Dimitri Konstantas, Pieter Vierhout, Body Area Networks for Healthcare, Proceedings Wireless World Research Forum meeting, Stockholm, 17-18 September 2001. http://www.wireless-world-research.org/

[48] Jones, Val, Richard Bults, Pieter AM Vierhout, Virtual Trauma Team, 2001c, Wireless World Research Forum meeting, Helsinki, 10-11 May 2001; http://www.wireless-world-research.org/

[49] Jones, Val, Mobile applications in future healthcare, Presented at CTIT Workshop, University of Twente, 8 February 2001.

[50] Wireless World Research Forum, 2001, The Book of Visions 2001: Visions of the Wireless World, Version 1.0, December 2001; http://www.wireless-world-research.org/

[51] Konstantas, Dimitri, Val Jones, Richard Bults and Rainer Herzog, 2002a, MobiHealth - Wireless mobile services and applications for healthcare, International Conference On Telemedicine - Integration of Health Telematics into Medical Practice, Sept. 22nd-25th, 2002, Regensburg, Germany.

[52] Konstantas, Dimitri, Val Jones, Richard Bults, Rainer Herzog, 2002b, MobiHealth – innovative 2.5 / 3G mobile services and applications for healthcare, Thessaloniki, 2002.

[53] Dokovsky, N., A.T. van Halteren, I.A. Widya, "BANip: enabling remote healthcare monitoring with Body Area Networks", In proceedings of IEEE Conference on scientiFic engIneering of Distributed Java applIcations (FIDJI 2003), Luxemburg, November 2003.

[54] Widya, A. van Halteren, V. Jones, R. Bults, D. Konstantas, P. Vierhout, J. Peuscher, 2003a. Telematic Requirements for a Mobile and Wireless Healthcare System derived from Enterprise Models. Proceedings IEEE ConTel 2003: 7th International Conference on Telecommunications, June 11-13, 2003, Zagreb, Croatia.

[55] A. van Halteren, R.G.A. Bults, I.A. Widya, V.M. Jones, D.M. Konstantas, "Mobihealth-Wireless body area networks for healthcare", Proc. New generation of wearable systems for ehealth: towards a revolution of citizens' health and life style. December 11-14, 2003, Il Ciocco Castelvecchio Pascoli Lucca, Tuscany. Pag. 121-126 (geen ISSN/ISBN)(feb 2004)

[56] Halteren A.T. van, Konstantas D., Bults R., Wac K., Dokovski N., Koprinkov G., Jones V., Widya I., MobiHealth: Ambulant Patient Monitoring Over Next Generation Public Wireless Networks IN e-Health: Current Status and Future Trends Volume 106 Studies in Health Technology and Informatics Edited by: G. Demiris 2004, 156 pp., hardcover, ISBN: 1 58603 442 1

[57] A. van Halteren, R.G.A. Bults, I.A. Widya, V.M. Jones, D.M. Konstantas, "Mobihealth-Wireless body area networks for healthcare" Wearable eHealth Systems for Personalised Health Management: State of the Art and Future Challenges. Volume 108 Studies in Health Technology and Informatics, Edited by: A. Lymberis and D. de Rossi, 2004, 360 pp., hardcover, ISBN: 1 58603 449 9, http://www.iospress.nl/html/boek1143885731.html

[58] Halteren A, Bults R, Wac K, Konstantas D, Widya I, Dokovsky N, Koprinkov G, Jones V, Herzog R. Mobile Patient Monitoring: The Mobihealth System, The Journal on Information Technology in Healthcare (JITH ) 2004.

[59] Val Jones, Arend Rensink, Theo Ruys, Ed Brinksma and Aart van Halteren (2004). A formal MDA approach for mobile health systems, Proc. EWMDA-2, Second European Workshop on Model Driven Architecture (MDA) with an emphasis on Methodologies and Transformations September 7th-8th 2004, Canterbury, England.

[60] Freeband Awareness project, http://awareness.freeband.nl

[61] Xu, Y., Westhead, M., Baker, F., "An Investigation of Multilevel Service Provision for Voice over IP Under Catastrophic Congestion", IEEE Communications Magazine, June 2004.

This Technical Report is also published in the proceedings of

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.

as

Val Jones, Georgios Karagiannis, Sonia Heemstra de Groot,
Ad hoc networking and ambient intelligence to support future disaster response.