Easy Wireless: broadband ad-hoc networking for emergency services

Maurits de Graaf, Hans van den Berg, Richard J. Boucherie, Frank Brouwer, Irene de Bruin, Herman Elfrink, Irene Fernandez-Diaz, Sonia Heemstra de Groot, Roland de Haan, Jan de Jongh, Sindo Nunez, Jan–Kees van Ommeren, Frank Roijers, Jan Stemerdink, Erik Tromp

Abstract— Wireless ad-hoc networks will enable emergency services to continuously overview and act upon the actual status of the situation by retrieving and exchanging detailed up-to-date information between the rescue workers. Deployment of high-bandwidth, robust, self-organising ad-hoc networks will enable quicker response to typical what/where/when questions, than the more vulnerable low-bandwidth communication networks currently in use. This paper addresses a number of results of the Easy Wireless project that enable high bandwidth robust ad-hoc networking. Most of the concepts presented here have been experimentally verified and/or prototyped.

***Index Terms*—ad-hoc networks, disaster recovery, quality of service, routing**

I. Introduction

IN emergency situations, it is of vital importance for rescue personnel to obtain an accurate and consistent picture of the situation, and to regain control and co-ordination on the shortest possible notice. This prevents further escalation, minimises the number of casualties and restricts the damage. The communication systems that are available now for rescue services lack crucial functionalities. They suffer from high vulnerability due to the fact that they rely on a fixed infrastructure and lack of self-organization capabilities, do not support multimedia applications asking for high quality communications and/or high bandwidth.

A. *Emergency networks*

In the case of a disaster, public networks generally are not reliable enough for communication between relief workers. These networks easily get overloaded or become unusable. For example, in the S.E. fireworks disaster, Enschede, the Netherlands (May 2000), a fireworks depot exploded and destroyed a large part of the city. The GSM network became unusable within a few minutes. During the metro incident in London the authorities considered to turn off the GSM network because bombs exploded via GSM in Madrid. Shortly after the Katrina disaster, messages on the internet indicated a "desperate need to re-establish communications in the disaster … volunteers from the tech community willing to travel to the area affected by Katrina are sought" [1]. The conventional solution for communication in disaster relief operations is largely based on TETRA, designed for speech and status messaging, reaching data rates between 2.4 and 7.2 kbps. These data rate limits are insufficient to give firemen access to the construction details of a building or to transport video images. While these constraints are somewhat relaxed with the advent of TETRA-II, it remains a severe constraint that TETRA relies on a fixed network infrastructure of base stations, and is therefore susceptible to the type of big disasters we have in mind. An ad-hoc networking approach will allow the relief workers to enter the disaster area and communicate with each other quickly.

B. *Easy Wireless*

This paper presents some of the results of the ITEA Easy Wireless project [2]. The general goal of ITEA Easy Wireless is **service continuity** for mobile users. Participating countries are Belgium, Finland, Norway, Spain and the Netherlands. Several use cases are addressed in the project: home/office, public transport and emergency services. In this paper we focus on ad-hoc networking for emergency services. Within this project solutions have been designed for the support of real-time and broadband (voice, video, high-speed data) applications via wireless ad-hoc networks. The majority

Manuscript received March 5, 2007. This work was supported by Easy Wireless – Ministry of Economic Affairs, Department of Commerce, under Grant IS043014.

Maurits de Graaf and Erik Tromp are with Thales Divion Land & Joint systems in the Netherlands, P.O. Box 88, 1270 AB Huizen, Netherlands, +31 35 5248 149; fax +31 35 5248 343, Maurits.deGraaf@nl.thalesgroup.com.

Frank Brouwer, Irene de Bruin, Herman Elfrink, Sonia Heemstra de Groot, Jan Stemerdink are with WMC (Twente Institute for Wireless and Mobile Communications), sonia.heemstra.de.groot@ti-wmc.nl.

Richard Boucherie, Roland de Haan, Jan–Kees van Ommeren are with the University of Twente, R.J.Boucherie@utwente.nl.

Hans van den Berg, Irene Fernandez Diaz, Jan de Jongh, Sindo Nunez and Frank Roijers are with TNO, J.L.vandenBerg@tno.nl.

of the algorithms have been experimentally validated in prototypes and test beds.

C. *This paper*

The remainder of this paper is structured as follows. Section II provides the overall view on the network and presents the general scenario and the communication services that need to be supported. Section III provides the high level requirements of the emergency ad-hoc network. Section IV discusses the various Easy Wireless results. Section V concludes the paper by presenting test beds, prototypes and simulation environments.

II. Scenario and Services

The projects MESA [3] and SAFECOM [4] have provided valuable input in discussing the characteristics of user scenarios. Figure 1 shows a high level picture of a disaster site. Vehicles and personnel of various rescue organisations are on the scene of the incident. Besides the fire department, the police department and the emergency medical services, these include e.g. hospitals, public utilities and the general public. The communication system provides various services. These include voice, short text/status messages/sensor information (e.g. GIS information), database access (medical data), remote control, real-time video, streaming video, still pictures. Terminals of individual rescue workers and rescue vehicles form an ad-hoc mesh network. These terminals connect to peers in their vicinity. This mesh network connects to the existing infrastructure through several gateways. First responder vehicles create gateways towards TETRA and UMTS, whereas special vehicles, like commander vehicles or communication units, may have gateways to satellite or microwave links.

III. Requirements & Architecture

In the project a disaster-relief network requirements analysis was undertaken, partly based on literature. Here, only a limited set of requirements is identified pertaining to the emergency ad-hoc network on the disaster site.

Emergency deployment. The network must be suitable for deployment at major emergencies, using vehicle-mounted antenna masts and small mobile units carried or worn by users. It should coexist and provide access to public and other emergency network systems (e.g. TETRA-based). The network must also support sufficient quality of service to support the services mentioned before. This implies broadband communications.

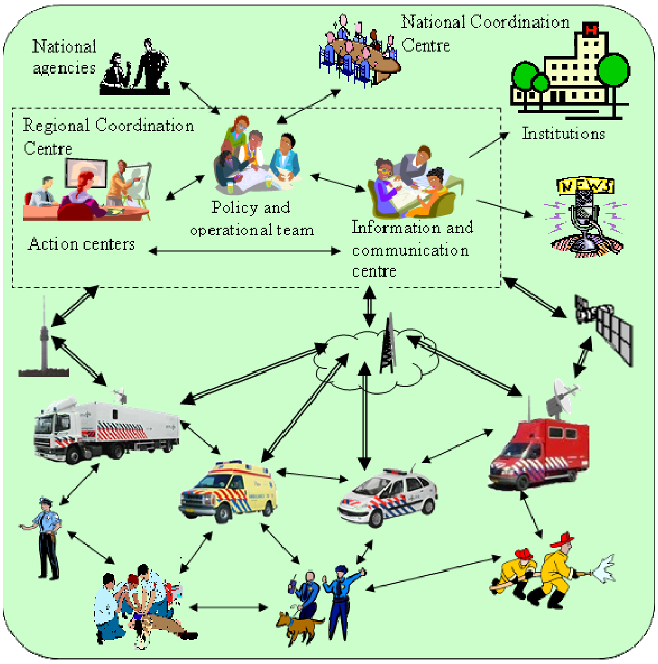
National agencies
National Coordination Centre
Institutions
Regional Coordination Centre
Policy and operational team
Information and communication centre
Action centers
NEWS

Figure 1 Communication at disaster site

Self organization. The network should be deployed easily and quick with little human maintenance. Devices have to be capable of configuring themselves into a network. Procedures involved in self-organization include ad-hoc network creation, ad-hoc device discovery, connection establishment, scheduling, address allocation, routing and topology management.

Reliability. Reliability is fundamental. First, the system architecture must be so that within a network there are no network elements whose failure will impact large parts of the network (in particular, there will be no single points of failure). Second, disruptions of communication paths (due to link failures, node failures or node mobility) need to be automatically detected. If the network topology is such that alternative communication paths exist, reconfiguration of paths shall take place. Third, the communication network equipment must be resistant to extreme temperatures, shock and vibration, salt and dust, radiation, rain, snow, etc.

Multicast. The network must support efficient multicasting in the sense that data shall not be duplicated unnecessarily.

Security. Security is a critical aspect during deployment of a wireless network, since the broadcast nature of wireless signals is vulnerable to attacks in various protocol layers.

The architecture of the emergency network consist of two ad-hoc, mesh network planes: one for communication between end points (typically rescue workers, but also e.g. robots) and one plane acting as communication backbone (typically rescue vehicles) between clusters of endpoint and gateway nodes to external networks. As is illustrated in Figure 2, the emergency network contains *personal nodes*, *vehicle nodes* and *gateways*. Personal nodes provide networking facilities to persons. Typically they are of small size, lightweight and make use of battery power. Vehicle nodes are installed in a vehicle (or in another platform), are of larger size, have less constraints on weight, and on power consumption. A gateway is a vehicle node with the capability to provide interfaces to other types of networks. Figure 2 shows two networks that consist of personal nodes that are connected via the network of vehicle nodes. In the vehicle node network one of the nodes functions as a gateway to the infrastructure network.

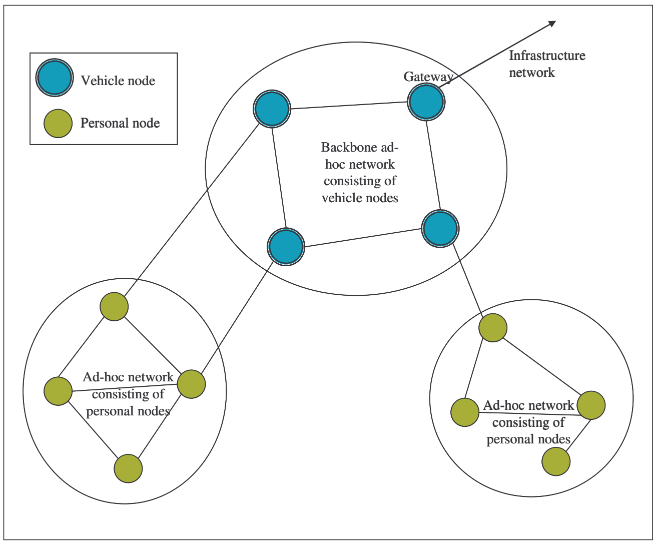
Vehicle node
Personal node
Gateway
Infrastructure network
Backbone ad-hoc network consisting of vehicle nodes
Ad-hoc network consisting of personal nodes
Ad-hoc network consisting of personal nodes

Figure 2.The Emergency Network

IV. Easy Wireless Results

In order to support the services and meet the other critical requirements, optimisations on multiple protocol layers are necessary. In the rest of this paper we address the project results on the application layer (service discovery), the network layer (new mechanisms for path computation and dynamic cost measurement and multicast forwarding), the meshing layer ('Layer 2.5' forwarding), the datalink layer (analysis of IEEE 802.11e), and the physical layer (transmit power control). The transport layer has not been the topic of our research activities, as this topic was addressed by other partners in the ITEA Easy Wireless project [5].

A. Service discovery

As no infrastructure is available in disaster relief operations, it is important that at each point in time every person in the disaster-relief team offers its services to the rest of the team and that he is aware of the services that the rest can offer to him. The mechanism that allows automatic detection of devices and services offered by these devices in the network is called service discovery (SD). The idea behind service discovery is to enable a dynamic service architecture. Within Easy Wireless we have experimented with JXTA [6] and Service Location Protocol (SLP) [7], [8] as SD protocols. JXTA is a frame-work which offers many features, among which (1) a combination of a distributed directory based architecture and a hybrid directory based architecture, where storage of service information is done at each node but where special nodes also act as directory; (2) the possibility to define groups of peers and to restrict the share of services to this peer group; The downside of extensive functionality provided by JXTA is a rather heavyweight and difficult to use implementation. In contrast, IETF-defined SLP provides a comparatively simple and lightweight alternative service discovery protocol for distributed (as well as centralized) environments. SLP does not provide anything similar to JXTA's "group" concept, nor to its generic service access mechanisms.

B. Path computation and cost measurement adaptations to routing protocols

1) Extensions to OLSR

The Optimised Link State Routing (OLSR) [9] protocol is one of the MANET route discovery protocols. OLSR optimises the flooding of link state information through the network by using multipoint relays (MPRs). Only nodes selected as MPRs are responsible for forwarding control traffic, thus providing an efficient mechanism for flooding. This makes OLSR particularly suitable for large and dense networks, with medium mobility of the nodes which is the situation in an emergency. A standard, RFC-compliant OLSR implementation is maintained by [10]. OLSR, like most of the other MANET routing protocols, simply minimize the number of hops between source and destination in their path computation. In practical experiments [11] it has appeared that this does not provide stable network routes. The route discovery process gets fooled by transient link availability with neighbour nodes that are too distant for reliable communication. The ETX extension to OLSR provides a partial solution to this problem: the link error ratio is estimated by measuring the packet loss for OLSR HELLO packets that a node receives from its neighbours. However, this does not take into account bandwidth, user preferences or other link characteristics. In the project we have enhanced OLSR – ETX in two ways:

◊ In addition to measuring the link error ratio, also link speed and type of link (wired or wireless) are taken into account in the determination of the best route from source to destination.

◊ To meet the self-organization requirement, a probing mechanism has been implemented to automatically detect the link speed and link type (whether wired or wireless). The probing mechanism is based on the CapProbe implementation [12] and on the packet-pair – mechanism [13].

2) *Multicast*

Although one-to-many communications can be achieved using unicast, the aggregate throughput of the network can be improved by using multicast forwarding. The particularities of ad-hoc networks have motivated the development of multicast routing protocols specific for these networks. Multicast ad-hoc routing protocols can be classified in two categories: tree-based and meshed based. Multicast Ad-hoc On Demand Distance Vector (MAODV) is a popular example of the first group and flooding and On-Demand Multicast Routing Protocol (ODMRP) are typical examples of the second. In emergency situations, the group reliability of the protocol (ability to deliver the packets to all members of the rescue team) is of vital importance. Previous studies ([14], [15], [16]) showed that in situations with mobility, like emergency situations, ODMRP and flooding are more reliable than MAODV at the cost of some more overhead. The simplicity of flooding (no routing overhead) and its performance (reliability, overhead) which is similar or better than that of ODMRP, has motivated the recent research on flooding-based routing protocols by the IETF. This resulted in the IETF specification of the Simplified Multicast Forwarding (SMF) protocol [17]. SMF is an improved flooding mechanism which can work together with relay set selection algorithms (like OLSR). The SMF-mechanism seems a good solution because of its high reliability and efficiency compared to other algorithms.

3) *Basic Multicast Forwarding (BMF)*

Based on the results of the previous section, in the Easy Wireless project, an OLSR plug-in for Basic Multicast Forwarding has been made available to the open source community [18]. This mechanism floods IP multicast and IP local-broadcast traffic over an OLSR network, where the MPRs identified by OLSR are used to optimise the flooding. Compared to the SMF implementation by NRL (Naval Research Laboratory) there are a number of differences: BMF uses encapsulation (instead of the IP packet identification field), to prevent duplicate reception of forwarded packets, and BMF supports forwarding of packets between multiple network interfaces

4) *Multi-path routing*

Multi-path routing enhances single-path routing by distributing traffic over multiple paths to increase the effective bandwidth. In wireless environments, nodes that are located close together may interfere, even though these belong to different paths. Most of the proposed multi-path protocols aim at finding link- or node-independent paths and do not explicitly take signal interference between paths into account. On the contrary, we have developed a generic mathematical model to assess network capacity in a multi-path environment under interference [19], [20]. The model explicitly captures interference and considers typical characteristics of wireless networks, such as different ranges and multiple source-destination pairs. The inherently complex model is solved via a heuristic greedy technique. This technique provides a fast approximate solution, so that it is practically feasible. Numerical evaluations give insight into the impact of the network characteristics on the capacity. In situations with limited interference, using many paths improves the capacity significantly. However, in disaster areas, where the radio network is typically quite dense, only few paths must be used.

C. *Layer 2.5 mechanisms*

A common solution for creating meshed networks is to do Layer 3 (L3) meshing, i.e. use a dedicated MANET routing protocol (see section IV) to solve meshing at the IP layer. Result of this is that the meshed network architecturally becomes an IP routing domain. This may work fine in many situations, but also poses some problems, because several standard 'subnet-based' IP mechanisms like IP address assignment, multicasting and IPv6 router discovery do not work on a routing domain. As a consequence, several efforts have been and are being undertaken in the MANET area to invent mesh supporting alternatives to the standard mechanisms. A totally different way of solving this issue is to implement meshing *below* the IP layer (L2 or L2.5 meshing). In this way the meshed network architecturally becomes a 'normal' subnet. Additionally, this approach allows having one meshing solution independent of the used network layer (IPv4, IPv6).

1) *FLAME*

In order to experiment with L2/L2.5 meshing the Forwarding Layer For Meshing (FLAME, [21]) protocol has been developed. The FLAME protocol runs as an intermediate layer between IP and the 'real' L2 MAC layer, without affecting either of them: to the network layer FLAME is an Ethernet-type MAC layer, and for the 'real' MAC layer FLAME is just another network layer protocol. All operation is entirely based on L2 (MAC) addresses and mechanisms, so FLAME runs under any type of network layer. A FLAME entity exchanges information with other FLAME entities through an 18-byte header that is prepended to the network layer payload whenever the network layer transmits a packet. FLAME uses this 'in-band' data to build and maintain its forwarding tables. FLAME's basic mechanism to build its forwarding table is to use the last hop through which a message from node A was received as the first hop to send a packet to A. When a packet is broadcasted the same packet may arrive over multiple paths. To enable the receiver to detect this, each packet contains a sequence number that is unique within the scope of the originating node. More elaborate forwarding mechanisms incorporating bandwidth are currently under investigation.

2) *Multihoming*

Multihoming as a general term refers to a network or node with multiple egress paths. We concentrated on the case where several gateways may be available to access the Internet from an ad-hoc network, but availability changes over time due to changing connectivity conditions. So the issues are gateway discovery and gateway selection. When using a L3 MANET protocol, gateway discovery and selection can be integrated (as has been done for OLSR in the form of its so-called HNA messages). When using L2/L2.5 meshing a separate mechanism must be used. For this purpose the protocol ARIADNE (Adaptive Routing in Ad-hoc Networks) was developed for use with IPv6. ARIADNE incorporates a mechanism that monitors incoming IPv6 Router Advertisement messages before they reach the IP layer, and only lets them pass if they are from the currently "best" gateway. To determine which is best, ARIADNE uses path cost information that is provided by the FLAME protocol.

D. *Layer 2 mechanisms*

Currently, IEEE 802.11 wireless LAN [22] is the most popular technology used for wireless ad-hoc networks due to the distributed mechanism of acquiring access to the wireless medium. The IEEE 802.11E [23] standard, is an enhancement which provides QoS differentiation. Unfortunately, the QoS-mechanisms only provide per-hop differentiation and the resulting end-to-end QoS depends on many variables such as the number of active neighbouring nodes and the number of intermediate hops. Performance studies show that IEEE 802.11E improves the QoS with respect to IEEE 802.11B, although in ad-hoc networks resulting end-to-end QoS is only sufficient for a limited number of mildly loaded hops. To give an impression, we present the results of a relatively simple ad-hoc network, a so-called chain topology, giving insight into the benefits of QoS-differentiation of IEEE 802.11E. In this scenario the first node initiates two flows, which traverse the entire chain, that have different QoS requirements and are treated with different priorities by the nodes. Figure 3 presents the throughputs, for different number of hops. For a single hop we see that the throughput of the high priority flows is three times higher than the low priority flow. For longer chains the differentiation becomes less. Currently we are investigating the performance of multi-hop flows in more complex topologies.

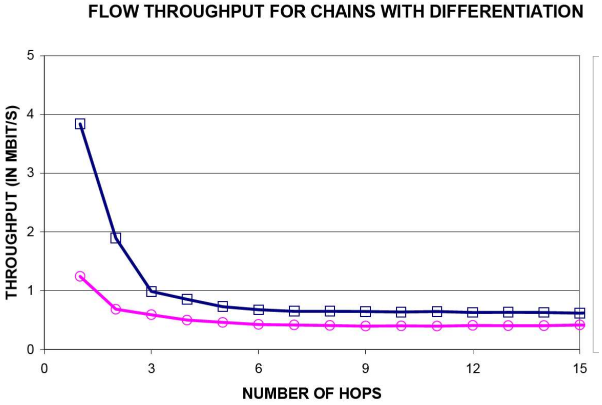

Figure 3 Flow throughput for chain ad-hoc network of different lengths with service differentiation.

E. *Layer 1 mechanisms*

1) *MultiRadio nodes*

In a traditional ad-hoc mesh network the capacity is severely limited by the fact that all communications take place through the same frequency channel. This problem can be mitigated by using multiple frequency channels. One convenient way to realize multi-channel mesh networks is to equip nodes with multiple off-the-shelf 802.11 network interface cards (NICs) using existing standards. These multiple radio interfaces can each be tuned independently to different channels, selected from a pre-defined channel set. A major research topic is how to design a (dynamic) channel assignment algorithm that optimises the network capacity by minimizing the internal interference and congestion through the proper selection of the channels. A simulation program of layers 1 and 2 was created to facilitate the design and evaluation of various channel assignment algorithms (see Figure 4).

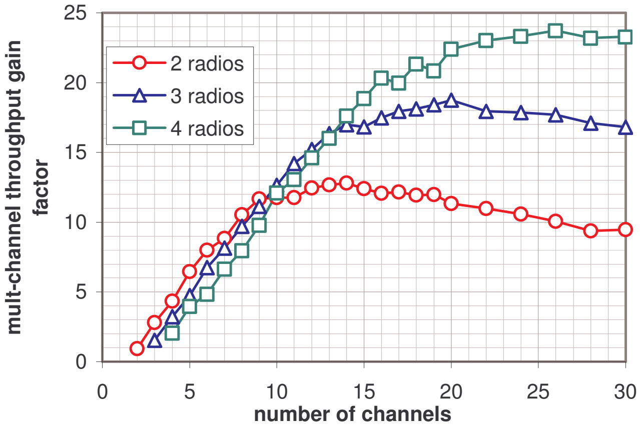

Figure 4. Multi-channel capacity gain

The gain factor by which the throughput of the network can be improved with respect to the (single-radio) single-channel network was assessed by means of simulations with 100 nodes. Figure 4 shows this gain factor as a function of the number of channels, for 2, 3 and 4 radios per node, where the channel assignment was performed at random. The decline at a high number of channels is caused by the loss of connectivity as the probability of nodes lacking a common channel increases with the number of channels.

2) Transmit Power control

Transmit Power Control (TPC) is defined as the ensemble of mechanisms and policies for controlling the transmission power of nodes in a wireless network. Depending on the application type of the ad-hoc network, TPC serves one or more of the following objectives: (1) Increasing the network capacity through spatial reuse; (2) Decreasing the energy consumption of battery-powered nodes; (3) Decreasing the electromagnetic signature of the ad-hoc network. Simulation studies and test bed experiments show that: Reducing the transmit powers in each single hop (i.e., at the *link* level) increases the potential for spatial reuse of the wireless medium, and therefore increases the effective capacity of the network.

Although transmit power control at the link level generally improves network capacity, decreasing the transmission footprint via multihop relaying in the presence of transmit power control (i.e., at the *network* level) often has a negative impact on the network capacity. Even though TPC is a physical-layer mechanism, its introduction affects the MAC or even the routing layers as well. Therefore, in studying TPC, one needs to think in *cross-layer* solutions.

F. Bottleneck node analysis

In wireless ad-hoc networks, nodes at central positions in the network tend to have disproportional larger traffic load since they are more likely to be selected as relay nodes. Since all nodes contend equally for the wireless medium, transmission bottlenecks tend to occur at central relay nodes. In particular, the buffer of the relay node fills whenever two or more neighbouring nodes transmit simultaneously. The impact on network performance was analytically studied for two different scenarios. Focusing on data traffic, the transmission time of data flows was determined. Then, including voice traffic into the consideration, simple priority mechanisms turned out to considerably reduce packet delays for voice traffic while only marginally increasing data flow transmission times. These mechanisms rely on prioritisation of voice packets over data packets at relay nodes. Such prioritisation can either be strict or through packet differentiation such as implemented in the 802.11E version. Comparisons with non-prioritised hybrid voice-data scenarios suggest that prioritisation/differentiation is imperative in order to support delay critical voice applications.

G. Connection to infrastructure networks

Ad-hoc networks can be stand-alone groups of mobile terminals, but typically need connectivity to an existing infra-structure. UMTS with High-Speed Downlink Packet Access (HSDPA) is a logical choice as wide area radio technology to fulfil this role. HSDPA increases the systems capacity and the users' peak data-rate for packet switched services. Network level simulations show that both the Quality of Service experienced by the end-user as well as the system resources strongly depend on user characteristics (speed, location, load, burstiness) and system parameters (packet scheduler, flow control, several timers) [24]. The handover performance is important for real-time services over HSDPA because it is the hard handover type with 'break before make'. The Easy Wireless project created a multi-cell network simulator for HSDPA to study service continuity during handovers. The handover threshold, delay and discard timers have a strong impact on the performance [25]. The initial scope of HSDPA is on best effort services. Upcoming services will be multimedia in nature. This requires the development of techniques, protocols and algorithms that fulfil the broadband high-speed, high-capacity and high-reliability requirements [26]. In order to satisfy similar constraints on the reversed direction, also the uplink equivalent (HSUPA) has recently been deployed [27].

V. EXPERIMENTAL TESTBEDS / PROTOTYPES

A. *Test bed for Layer 2.5 mechanisms*

In order to evaluate and do experiments with L2.5 meshing as part of the project a dedicated test bed was built around the FLAME L2.5 meshing protocol as presented in Section IV.C. The test bed consists of 5 Linux based laptops, representing 2 Vehicle Nodes (VNs), 2 Personal Nodes (PNs), and 1 Backoffice Node (BN). The VNs and PNs form an ad-hoc wireless subnet using 802.11a @ 54 Mbps. Both VNs are also connected to the BN, through OpenVPN [28] based Virtual Private Network (VPN) tunnels over a backbone connection. FLAME runs on the PNs over the 802.11a interface, on the VNs over both VPN and 802.11a interface (thus bridging these interfaces), and on the BN over the VPN.

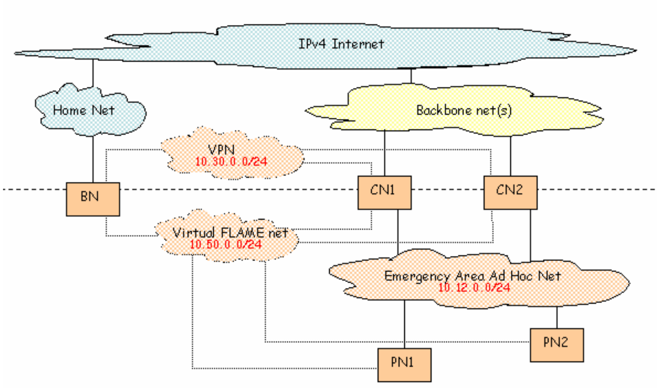

Figure 5. FLAME L2.5 testbed.

The result of this setup is that all nodes logically appear to be connected to one single broadcast domain. A separate test control application allows to enable/disable the VN's and PN's network interfaces underneath FLAME, in order to test the ability of FLAME to adapt its forwarding paths according to currently available connectivity options. Over this network a location tracking and video imaging application is run, which uses ad-hoc service discovery based on SLP [7]. The server side of this application runs on the VNs and the PNs, delivering (simulated) location information, and, for PNs only, a video stream from a connected webcam. The client side runs on BN and both VNs, and displays, on a map, the location, and, when available, the video images of server nodes.

B. *MultiRadio Nodes*

A prototype multi-radio node was developed that can be equipped with up to 4 NICs. Apart from FLAME, it includes a Multi-Channel MAC (MCM) layer to multiplex the transmissions through the different NICs. It optionally includes a scanning radio that is in fact one of the NICs which is dedicated to the task of scanning the neighbourhood for other nodes and the channels they are using.

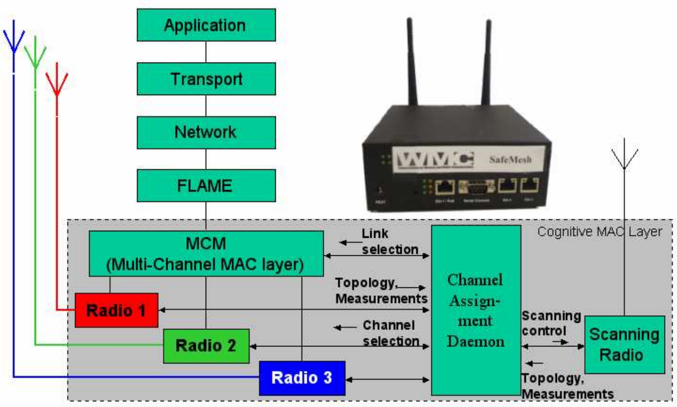

Figure 6. Prototype multiradio node

C. *Prototype for Layer 3 mechanisms*

The OLSR protocol together with its extensions on multicast and on Quality of Service described in Section IV.B have been implemented in a prototype network node. The node is suitable for installation emergency vehicles. Together with the services that were already available a complete system is formed, providing all vehicle communication services on a single node. The prototype integrates vehicle intercom, Ethernet LAN, IP router, serial data links in a rugged, reliable system that can be used to interconnect vehicles in any order and in any topology, which is designed to be used in harsh environments

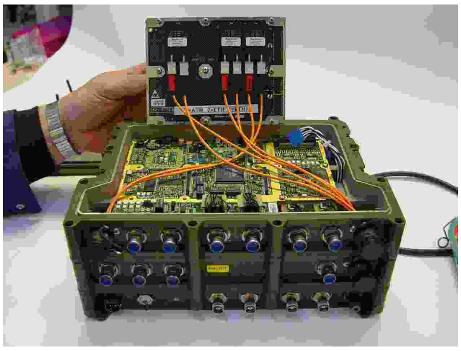

Figure 7. Protoype network node

D. *Layer 1 testbed*

An important tool in the Easy Wireless test bed used for the evaluation of policies and mechanisms in ad-hoc networks is a 9-port fully-meshed wireless-medium emulator. The *TNO Ad-hoc Network Emulator* allows its users to build and test networks between radio devices with channel conditions that resemble real life scenario's in a controlled laboratory environment. The specific characteristics of the type of radio link deployed can be applied to the links and various scenarios of usage can be run. Various levels of attenuation and distortion (for instance due to multi-path interference and obstructing buildings) can be applied; either per use case or from a pre-written scenario. With the emulator, operators and users can assess the behaviours of an envisaged ad-hoc radio network in a controlled, reproducible environment at much lower cost than with real-life experiments.

E. Simulation tooling

The simulation-tool is an own-developed tool written in the general-purpose programming language Delphi. The simulator is divided into multiple modules according to the OSI-layers to provide independency between the different layers. The highest layer represent mobile users that can enter and leave the system start and finish applications, e.g. voice services, streaming video and file transfers. The IP-layer forwards the data packets by using an underlying WLAN-station that transmits the data traffic over a wireless medium; in case the destination user cannot be reached directly, the packets are sent via intermediate WLANs. The MAC-layer contains all the details of CSMA/CA contention of the EDCA [23], e.g., the back-off mechanism, physical and virtual carrier sensing, and collision handling. The PHY-layer includes propagation- and fading-models and a clear channel assessment (CCA) procedure that results in limited ranges for successfully transmitting and receiving packets and sensing transmissions of other nodes.

VI. Conclusion

To support situational awareness in emergency rapid deployment of unplanned networks in the disaster site is required. A natural candidate for this type of networks is ad-hoc communications. The inherent lack of centralised control and the variability of the network topology call for optimisations on many layers of the protocol stack. TNO, WMC, University of Twente and Thales L&J Systems NL participate in the ITEA Easy Wireless consortium to research such solutions. This paper presents a number of Easy Wireless results that enhance the quality of service and support autonomous operation in emergency command posts.

References

[1] Message of Sun 4 sept 2005. Victor Bahl, mobicom@listserv.acm.org, subject: “Helping the victims of Katrina - Technology & Cash Assistance Sought”.

[2] http://easywireless.telecom.tno.nl

[3] MESA TX 70.0001, Service Specification Group Services and Applications, Statement of Requirements V 3.11, October 2000, Available at http://www.projectmesa.org.

[4] The SAFECOM program. “Statement of requirements for Public Safety wireless Communications and interoperability”. Report, SAFECOM, March 2004.

[5] University of Cantabría, “*End-to-End Quality of Service for Mobile Heterogeneous Networks – A Generic Architecture Proposal*”, in the 9th International Symposium on Wireless Personal Multimedia Communications (WPMC 2006), San Diego (USA), 17 Sept, 2006.

[6] Brendon Wilson, “JXTA”, New Riders Publishing, First Edition 2002.

[7] E. Guttman et al., “IETF RFC2608: Service Location Protocol, Version 2”, [online]. Available: http://ietf.org/rfc/rfc2608.txt

[8] E. Guttman et al., “IETF RFC2609: Service Templates and Service: Schemes”, [online]. Available: http://ietf.org/rfc/rfc2609.txt

[9] Optimized Link State Routing Protocol, Request For Comments (RFC) 3626

[10] http://www.olsr.org

[11] “Implementation Experience with MANET routing protocols”, K.-W. Chin, J. Judge, A. Williams and R. Kermode In ACM SIGCOMM Computer Communications Review, Volume 32, Number 5, November 2002

[12] CapProbe - Ling-Jyh Chen e.a , ww.cs.ucla.edu/NRL/CapProbe/ CapProbe: A Simple and Accurate Capacity Estimation Technique.”ACM SIGCOMM 2004, Portland, USA, 2004

[13] “Packet-Pair Rate Control - Buffer Requirements and Overload Performance”, S. P. Morgan, S. Keshav, Technical Memorandum, AT&T Bell Laboratories, October 1994.

[14] K. Viswanath, K. Obraczka and G. Tsudik; Exploring Mesh- and Tree Based Multicast Routing Protocols for MANETs; IEEE Transactions on Mobile Computing; 2005

[15] T. Kunz and E. Cheng; Multicasting in Ad hoc Networks: Comparing MAODV and ODMRP; Proceedings of Workshop on Ad hoc Communications; Germany; September 2001.

[16] S-J. Lee, W. Su, J. Hsu, M. Gerla and R. Bagrodia; A Performance Comparison Study of Ad hoc Wireless Multicast Protocols; Proceedings of INFOCOM; 2000.

[17] Simplified Multicast Forwarding for MANET; IETF MANET WG; draft-ietf-manet-smf-03, work in progress; October 2006.

[18] http://sourceforge.net/projects/olsr-bmf

[19] Roland de Haan, Richard J. Boucherie and Jan-Kees van Ommeren, “The Impact of Interference on Optimal Multi-path Routing in Ad Hoc Networks”, in Proc. of ITC, Ottawa, Canada, 2007.

[20] Tom Coenen, Maurits de Graaf, Richard Boucherie, “An upper bound onmulti-hop wireless network performance”, in Proc. of ITC, Ottawa, Canada, 2007.

[21] H.G.Elfrink, “FLAME white paper”, [online]. Available: http://www.ti-wmc.nl/downloads/Flame-wp-3.1.pdf

[22] IEEE p802.11b/D7.0, Supplement: higher speed physical layer extension in the 2.4 GHz band, 1999

[23] IEEE p802.11e-2005, Amendment 8: Medium Access Control (mac) Quality of Service Enhancements. November 2005.

[24] I.C.C. de Bruin e.a., Performance analysis of Hybrid-ARQ characteristics in HSDPA, *Wireless Personal Communications*, Springer, 2006.

[25] Irene de Bruin e.a., Performance evaluation of VoIP over HSDPA in a multi-cell environment, accepted for the *Fifth International Conference on Wired/Wireless Internet Communications,* Coimbra, Portugal, 2007.

[26] F. Brouwer e.a., Broadband multimedia over HSDPA, book chapter accepted for publication in "*Broadband Mobile Multimedia Techniques and Applications*", to be published by Auerbach Publications, Taylor & Francis Group.

[27] Camilo Orejuela Mesa, WCDMA – Enhanced Uplink performance evaluation, MSc thesis University of Twente, the Netherlands, 2006.

[28] OpenVPN website, [online]. Available: http://openvpn.net/