Varakliotis, S.; Stephan, N.; Kirstein, P.T., "Open Multi-Purpose Gateway for Emergency Services Internetworking," Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference on , vol., no., pp.1,6, 14-18 June 2009 doi: 10.1109/ICCW.2009.5208005

PROCEEDINGS PAPER

Open Multi-Purpose Gateway for Emergency Services Internetworking

Socrates Varakliotis, Nikolas Stephan, Peter T. Kirstein
Dept. of Computer Science
University College London
{s.varakliotis, n.stephan, p.kirstein}@cs.ucl.ac.uk

Abstract

Access to a variety of Networks will be a central part of technologies employed by future emergency responders. Incompatibilities are often introduced as a result of widely disparate uses and varying capabilities of devices, which must be resolved through internetworking. This requires devices such as gateways to connect these networks and enable communication to the furthest extent possible.

This paper outlines a number of specific cases in which gateways may be used as well as the capabilities different available devices offer and how they can be used for multiple purposes in an Emergency Services context.

I. Introduction

Emergency responders increasingly rely on state-of-the-art communication technologies to carry out critical monitoring, response, rescue and recovery operations. These technologies can be tailored to emergency scenarios such as tunnel fires, mountain rescue and hazardous material contamination and broadly fall into the following classes:

- Special devices borne or worn by the first responders (e.g. palm terminals, vital or environmental sensors, light wearable equipment).
- Local systems already at the site as part of the monitoring or communications infrastructure (e.g. fixed cameras and other sensors, cable infrastructure, base stations).
- Systems that are deployed during the response operation in the area surrounding the crisis (e.g. access points, enhanced tracking and tracing sensors, wireless probes).
- Remote systems that help notify, manage and control the response operation from an operations centre.

In this setting, the resources, human or otherwise, are usually administered by different government or public authorities. A multitude of technologies are used to interconnect them, ranging from sensing devices to personal and group communication equipment. The outcome of an operation largely depends on the efficacy of communication and information exchange. Furthermore, the success of future operations relies on appropriate training; improved through the study and review of data, gathered during a real operation or readiness exercise.

In this context, the Internet Protocol (IP) can play the core role in interconnecting existing communication networks formed by the devices mentioned above. The benefits arise from the already large base of deployment and interconnectivity options offered by IPv4 (and even more by its successor, IPv6). These benefits are highlighted below. The paper introduces technology available for interworking of first responders. It is centred on IP-based interconnection and discusses technologies that enable this interoperation, such as Wireless Sensor Networks (WSNs), and their associated protocols.

We introduce a prototype multi-purpose gateway, built using open-standards. It is work-in-progress under a multinational, EC-funded project called U-2010 (EU/ICT no. 035003) aiming to improve the means of communication and access to information available to rescuers in emergency situations. While it is general-purpose, its enhanced network and application layer functionality is considered in the emergency services context, in particular those scenarios envisaged by the U-2010 project.

II. Background

A. Wireless Sensor Networks

Despite being powerful when deployed in large numbers, wireless sensors are very limited individually. They often have limited connectivity, radio range and maximum throughput. A typical wireless sensor network (WSN) node has a nominal radio range of less than 100m in line-of-sight and fairly low data rates. In practice, these figures are even lower in busy outdoor or enclosed, environments, such as road tunnels and buildings, where thick concrete and various metals introduce radio interference, multi-path fading symptoms, etc.

In spite of these limitations, WSNs can add great value to applications for first responders, providing flexible platforms for monitoring and surveillance. Their wireless ad-hoc nature requires little prior infrastructural investment, with an ad-hoc routing technology that is resilient to individual node failures. During the crises, various quantities of the physical world around the crisis site need to be constantly measured in order to maintain public safety.

Traditionally first responders used either proprietary or closed industry standards. This led to expensive and isolated sensor network islands that were not directly interoperable. More recently WSNs use IP, or adaptation layers to IP networks. Additionally, the wide adoption of IPv6 will allow large numbers of small nodes to easily be controlled easily and monitored remotely via the Internet [11]. This means emergency respone teams can be monitored continuously for their well-being and guided during their operation.

Page -->

B. Gateways

As both the needs and technology evolve in the Emergency Services environment, the deployment of flexible and extensible gateways would greatly simplify the introduction of additional services. Such a gateway is an interesting extension to existing WSNs as it enables a number of more advanced uses. Most importantly these include facilities to connect to other incompatible networks by acting as an access point to a wired network, or incompatible wireless technology. In addition it can enable entirely new functionality such as advanced computation on data collected by the sensor nodes, or even limited video streaming.

The gateway resides on communication vehicles of first responders or could be statically deployed in certain high- risk environments. A future possibility, as miniaturisation of hardware progresses, is that it could be carried, as part of a Personal Area Network (PAN), by rescuers.

C. Scenarios

An interesting scenario, involves emergency response teams operating in a road tunnel during a fire incident. The rescue operation is aided by both fixed and dynamically deployed WSN infrastructure, wireless ad-hoc networks, and backhaul terrestrial and satellite links, all interconnected by the multipurpose gateway. By increasing the amount of information available to rescuers, which is usually limited yet extremely valuable, situation awareness can be improved significantly. Many of the issues that arise in tunnel fires result from the extreme hostility of the environment, including bad visibility and limited communication. The simple addition, for example, of heat and location sensors to the equipment carried by rescue workers, would be a huge improvement. Data from these sensors can be transferred to other rescue staff involved on-site and to control rooms near-site, or off-site. Communication to a local or remote mission control room is also provided.

The general setup would usually consist of a vehicle, such as a fire engine, with advanced communication equipment including data displays. This vehicle can be positioned outside the tunnel and act as a base station, providing other devices inside the tunnel with connectivity. Data gathered by statically deployed sensor networks, as well as those carried by rescuers or robots, can then be collected in this location and relayed to anyone requiring access to it.

Additional scenarios not considered here are mountain rescue, nuclear incidents and flu pandemics.

III. Network heterogeneity

A variety of networking technologies are available to first responders. We examine below how this heterogeneity is exhibited at different layers of the OSI model.

A. Link-Layer Heterogeneity

A broad range of wireless communications technologies should work together to assist first responders. The widely varying capabilities of the devices however result in a hierarchy, as defined by range, between which gateways enable connectivity.

- The IEEE 802.15.4 [5] standard is well suited to short range communications, with Bluetooth being a less common choice due to its unusual architecture and other limitations.
- For medium range communications IEEE 802.11 [4] is most widely deployed and understood.
- Long range communications are somewhat different in that they are usually deployed as point-to-point links shared with others, rather than multiple devices using them directly. This simplifies interoperability with other technologies. Likely systems to be employed are WiMAX [6], satellite links and cellular networks such as GPRS, UMTS and HSPA.

It is not advisable to use all these technologies simultaneously, as a number of issues, such as interference, may arise. However, for different situations the best technology may vary and some are generally more suited to emergency responders than others.

B. Gateway Heterogeneity

A number of systems that allow operation of various technologies are used for internetworking in U-2010 and are described below.

1) *Open-source General-purpose Sensor Gateway:* Sensor network gateways are required to perform protocol translation where the ad-hoc sensor mesh network is not directly compatible with the core IP network of an infrastructure. This protocol translation, for example, can be done in a sub-IP layer, in order to adapt IPv6 packets appropriately for transport to and from the WSN and a larger IP core network. 6LoWPAN is such an adaptation layer (see description in Section IV-D).

The **Cool MoteMaster (CMM)** [7] is a basic WSN gateway developed during the RUNES project by LiPPERT. It is a small-form-factor Linux-based board with an Alchemy Au1550 500 MHz MIPS-architecture CPU with low power consumption, 128MB flash RAM, an 802.15.4 Freescale transceiver and Ethernet, USB, RS-232 serial and general purpose digital and analogue I/O ports in the basic configuration. Expansion boards provide support for 802.11 wireless connectivity and in the same way other PCI- 104 compatible boards can be used to extend the gateways hardware capabilities.

The CMM gateway has evolved into a versatile, open- source, multi-purpose gateway under U-2010, with the following capabilities (the building blocks of the system are depicted in Figure 1):

- Serve the U-2010 tunnel and wearable WSNs in 6LoWPAN protocol adaptation (IPv6).
- Cache sensor measurements for off-line use (down-links, training purposes, etc.).
- Stream low frame-rate, low-resolution video from the WSNs physical environment.
- Act as the mobile router of a roaming wearable PAN (with NEMO support, cf. Section VII).

Page -->

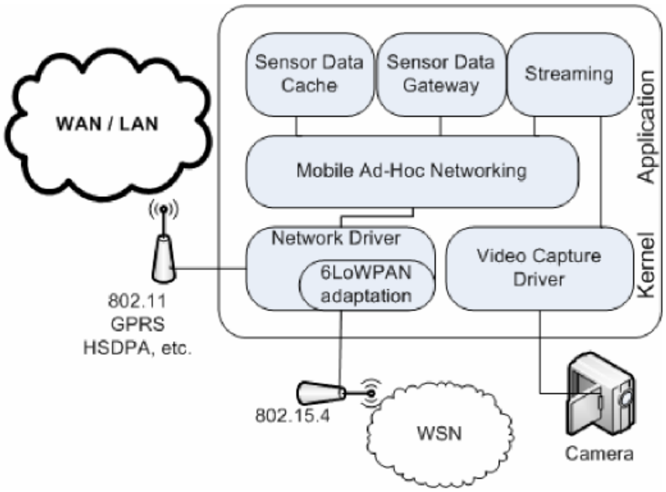

Fig. 1. Building blocks of an open-source multi-purpose gateway.

Each of these services and how they have been tailored to the gateway, is described in turn in later sections. It is important to note that the functionality of the multi-purpose gateway is not limited to the above services.

2*) Other gateways:* The **Arch Rock PhyNet** [1] router is an IP-based 802.15.4 WSN device that connects 6LoWPAN mesh networks via Wi-Fi and Ethernet interfaces to diverse WAN links. It is used to eliminate the need to co-locate individual WSNs with the server-based management functions that control them, allowing data aggregation on a potentially remote WSN management server.
The PhyNet routers are core parts of the U-2010 WSN infrastructure. There can be several routers in an Arch Rock WSN deployment for scalability and resilience to failures.
In U-2010 the **IABG Highly Mobile Network Node (HiMoNN)** [3] and the **Cisco Mobile Access Router (MAR)** [2] are used mainly for wide-area connectivity and to provide other gateways and nodes with up-links.

The MAR is capable also of NEMO Basic Support [9] described in Section VII, with further proprietary extensions for network mobility. It combines interoperability with the full range of commercial Cisco router offerings; its ruggedized form and resilient enclosure, as well as extensive integration options with other modular boards for other access networks, allow surveillance and video analytics and beyond.
The HiMoNN is more focused on the formation and support of mobile ad-hoc wireless networks (MANETs) with associated open standards.
Unfortunately, both gateways above are of a closed nature; they are commercial offerings, and are restricted in terms of what is possible for outside groups like ours to do with them to test new technologies. Novel uses are therefore limited only to their designers and more open architectures are usually a better choice when working in research environments with experimental protocols and applications.

C. Compatibility Issues

There are a large number of compatibility issues with these gateways due to the fact that they vary greatly both in respect to hardware and software. The software on the devices spans from the entirely open-source CMM (Linux operating system), to the completely closed and proprietary MAR (Cisco IOS operating system). Compatibility for open-source parts of the system is not usually a big issue as the openness allows any required changes to be made. But only being able to modify one side of an infrastructure is not always sufficient; certain interactions are not possible due to one side being closed.
Some gateways (among the CMM, HiMoNN, MAR, and the Arch Rock router) can co-operate to provide internetworking functionality to a WSN, or MANET functionality and remote access to first responders. But this can only be achieved by further integration of these gateways at a system level, which can be costly and may lead to more complex network configurations.

III. Network types, properties and standards

A. Basic Networks

Basic networks are permanently attached to some communications infrastructure at an emergency site. One example could be a vehicle specially modified for emergency services communications (fire engine, police car, communications truck, etc.). Their networking infrastructure is mobile in that it travels to the location in question and can be used while doing so. However, these networks are likely to remain static once there, unless an escalating situation necessitates a move.

When stationary, a gateway can more easily establish reliable up-links to allow remote access to collected data. These up-links could, for example, utilise a satellite dish (set up upon arrival of first responders) or a wireless wide-area data network. This allows mobile gateways to make short- range connections to the basic gateway, rather than having to establish long-range connections. The gains from this are significant, as energy is severely limited on truly mobile networks and long-range connections are likely to consume significantly more energy.

In addition to this there is likely to be a LAN inside the communications vehicle; the basic gateway can take advantage of wired or high-reliability wireless connections to other devices on this vehicle in order to provide connectivity or other services.

B. Mobile Networks

A second class of network is the truly mobile network and examples include mobile robots or wearable PANs. Mobile gateways have the ability to provide more long-range connectivity for sensor nodes attached to, or dynamically deployed by, first responders. This means that a sensor node, for example, with very limited range can simply connect to a mobile gateway that acts as a backhaul link to a more remote basic gateway. Furthermore, sensors placed within the operational environment either permanently or temporarily can use the gateway carried by a responder to make connections.

Page -->

This has the advantages that it enables increased miniaturisation of nodes, allows the mobile gateway to act as a 6LoWPAN gateway for WSNs, and enables mobile networking standards to be deployed in the operations field (Section VII).

C. Static Networks

The last category are the truly static networks that are usually fixed on some solid infrastructure. These fixed networks are mainly used for surveillance and daily monitoring of environmental or traffic conditions. Examples include the CITA traffic management system for the Luxembourg highway network, which features car counting alarm strips, messaging boards, traffic cameras and tunnel supervision equipment. Of course technical developments may require that even these networks have further extensions, such as adding RFID sensors to monitor dangerous cargo entering a tunnel.

In order to interconnect static networks, their gateways also have to be permanently deployed on-site. Although traditionally this category of fixed infrastructure networks was based on analogue set-ups, it is now becoming increasingly digital, and IP-based. This means that IP gateways are likely to be present in areas such as tunnels and bridges leading to enormous benefits for Public Safety applications.

Static networks are interesting in Public Safety management because of their potential to be wired rather than wireless, which results in additional reliability and bandwidth. In the case of a tunnel infrastructure, for example, they could be implemented in such a way that large portions should survive a catastrophy, and could then act as a backhaul for IP datagrams coming from inside the tunnel to the endpoints. This can be useful when mobile wireless gateways need to operate within range of the fixed infrastructure.

D. 6LoWPAN

Until recently, it was not technically possible to use IPv6 over Low-Power Wireless Personal Area Networks based on IEEE 802.15.4. The three main issues being the low throughput rate, limited space for buffering and an MTU that is one- tenth of the minimum required by IPv6 (128 compared to 1280 bytes).

Fortunately, these issues have now been addressed by the IETF 6LoWPAN group in the recently published RFC4944 standard [13] that proposes three primary alterations:

- The use of stateless header compression reducing the general packet overhead to a minimum.
- Fragmentation, allowing IPv6 packets to be transmitted using a frame size of only 128 bytes.
- Layer-two forwarding of IPv6 datagrams.

V. Application services

Further to internetworking, emergency services benefit from a number of applications that can use the network technologies described in the previous section. While these application- level services are vital, they may run on relatively resource- constrained devices, such as the gateways themselves. This section focuses only on applications that can be accommodated by gateways with limited resources, which are primarily used for internetworking purposes; these application services may therefore be hosted on a best-effort basis in tandem with their primary tasks.

A. Video Streaming

For the proposed open gateway architecture for first responders (depicted in Figure 1), a light-weight video-streaming service has been implemented. It is based on commodity USB cameras (Logitech QuickCam family), aided by open-source video software and includes two basic modules:

- **The capture driver module:** In reality, this involves multiple popular video drivers, which have been built into a Linux kernel. This ensures support for a large choice of commercially available webcams and rapid deployment.
- **The streaming service:** This involves development of a light-weight streaming server module, based on HTTP.

The server runs as a daemon with trivial camera control (pan, tilt, zoom), if supported by the camera hardware.

The simple video-streaming service can make use of hardware JPEG or MJPEG compression on webcams, in order to reduce CPU cycles. This makes it a light solution for embedded devices, such as portable gateways carried by first responders. Typical performance is less than 10% CPU utilisation on a 500 MHz MIPS board when streaming VGA 640x480 video frames. The achieved frame-rate is as low as 2-6 frames per second, which is a good trade-off to the CPU utilisation. The service has been built for the MIPS architecture and deployed on the CMM running Linux kernel 2.6.24.

B. Local Data Cache

Slow and unreliable wide area connectivity may cause gateways operating in an emergency scenario to occasionally lose their connection, in which case it is anticipated that they continue their operation in local scope. WSN measurement data could be vital information once the connectivity is restored and can provide immediate assessment of the situation and fast access to resources that are currently deployed on-site.

To accomplish continuity in service and no loss of data measurements, the gateways need local data caches. This can be any sort of storage method that can be hosted on the gateway. Examples range from log-files (including appropriately organised sensor measurement data for later processing), special file-system partitions reserved for caching, removable flash memories (sticks, or discs) to larger hard-disks.

The multi-purpose gateway architecture for first responders has been further enhanced under U-2010 to accommodate this local data cache (see Figure 1). It is provided as temporary log files that are initially stored in a small ram-disk area of the file-system. This allows fast processing, for temporary short- lived network outages. When this area fills up (few minutes to a couple of hours), measurement logs are transferred to flash memory for medium-term storage (one day). If network connectivity is restored within this time, a remotely initiated service can retrieve the data from the gateway. If these time limits are exceeded, the logs are rotated; older logs will be deleted first when the limits are reached. It is noted that all

Page -->

processing (data parsing and upload to a database) is left to the system that initiated the remote

transfer.
Caching on the multi-purpose gateway architecture also extends to the video-streaming service which is capable of caching still image sequences in JPEG format. These are captured and stored at regular user-specified intervals on the gateway even when no HTTP-streaming connection is active.

C. WSN Node Heterogeneity and Integration

Node heterogeneity in the U-2010 scenario refers to the availability of a number of sensor node devices to the infrastructure of the tunnel. These sensor devices may vary in hardware (the sensor controller board), software (operating system and other software components running on the board and in the ad-hoc network), or in the network (the communications technology and stacks used, routing protocols, etc.). In the following paragraphs we review basic features of popular sensor nodes that are available in U-2010. We then describe a way of integrating measurements from different WSN platforms into a unified U-2010 WSN measurement database to which the open general-purpose gateway is key.

1) *RUNES sensor nodes:* The RUNES nodes are based on the Telos hardware platform and run the Contiki open- source OS, as well as the RUNES middleware. The RUNES middleware and Contiki OS make full use of the sensing devices, periodically taking light, humidity and temperature measurements. These data are transmitted to a remote UDP sink, which could be the data management system of the tunnel control room, or a remote control room in a crisis situation.
RUNES sensor nodes are used in U-2010 to emulate the wearable and dynamically deployable sensors used by first responders as they arrive at the disaster scene.

2) *Arch Rock sensor nodes:* Arch Rock makes available two basic types of sensor boards, or nodes. The IPsensor node and the IPserial node. Both types run proprietary binary images of the PhyNet software (based on TinyOS), which powers their PhyNet product line.

The Arch Rock nodes are 802.15.4-compatible wireless battery-powered devices with integrated temperature, humidity and light sensors. The main board is identical to the Telos platform and comes in a rigid enclosure with battery compartment and shouldered expansion ports. Available expansion ports and generic sensor and serial drivers allow users to easily augment the nodes with numerous different external switches, sensors, and relays to create customised wireless sensor networks.
The WSN application-level protocol is closed, with only a programmatic interface, based on web-services, available to the user, via the PhyNet “gateway server”.

3) *Integration:* Two different types of WSN nodes based on the Tmote/Sky hardware are available in the Fire-in-Tunnel scenario of U-2010; one is running TinyOS and the other is running Contiki OS - but both are measuring the same physical quantities (temperature, humidity and light). The deployments belong to two independent types of WSNs. One commercially acquired is from Arch Rock based on RFC 4944/6LoWPAN and deployed as fixed infrastructure by the tunnel operators.
The other RUNES-based WSN is deployed dynamically by the firemen for monitoring, research and training purposes.

In the above situation, the two deployments are not able to interoperate at the network layer, and appropriate translation at the application layer is required. This entails running software translation on the gateway, which parses and extracts measurements from both types of WSN and stores them in a common format. Alternatively encapsulation in the appropriate packet format and forwarding to a common U-2010 data sink, where appropriate processing takes place, is possible. From there, sensor measurement data is uniformly rendered over a web-based GUI (the U-2010 portal).

VI. Related work

There is plenty of literature in the area of internetworking of WSNs. However, published work mostly describes bridging between different access media or custom WSN applications, with data collection, processing and caching capabilities individually. There is also some reference on additional services such as video streaming, but little literature has been identified on combinations of the above in the same gateway.

Bridging has been done in a number of commercial implementations [10][1]. While the problem is largely solved, there are a number of aspects that are still in the process of being standardised by different organisations. For example, the Compact Application Protocol (CAP) [14] proposes the execution of ZigBee Application Profiles over a standard IP stack, thus enabling application-level internetworking between industry-strength legacy ZigBee WSNs and IP-based ones.

Using a gateway for additional services is less common. However, the Cisco Mobile Access Router (MAR) [2] is a powerful and ruggedized small form-factor router platform with multiple additional capabilities if extended with purpose- built boards, such as video-analytics for military and surveillance applications [8]. Furthermore, the IABG Highly Mobile Network Node (HiMoNN) [3] has been designed to satisfy ad-hoc mobile networking requirements.

VII. Current developments

Network mobility is an important topic in the context of Emergency Services networks. There are numerous cases in which networks as a whole, such as Vehicle Area Networks or Personal Area Networks, are required to move.

One approach to network mobility, put forward by the IETF Network Mobility (NEMO) [9] working group, allows an entire network to roam by utilising a mobile access router. This has the advantage that a large number of nodes can be mobile, while requiring only a single device to go through the actual address re-acquisition. Unfortunately, the fact that a Home Agent is used means that triangular routing occurs; this is not always a major issue, but can become a significant overhead when nested routes are formed. Fortunately the problem can be alleviated by what has been termed MANEMO, a system in which a MANET protocol is employed in nested NEMO topologies [12]. This allows nodes from different nested mobile networks that are within range of each other

Page -->

to communicate directly, rather than requiring data to traverse long paths via a Home Agent. This is a very powerful mechanism in scenarios where large numbers of individual WSNs, some or all of which are mobile, are in one place and must communicate.

One issue with using MANEMO in the above scenario is that it is not directly applicable to IPv6-enabled WSNs running the 6LoWPAN adaptation layer; this is due to the fact that sensor nodes do not use global IPv6 addresses, but a short 16-bit address drawn from a local space instead. This means that direct ad-hoc communication with sensor nodes from other 6LoWPAN networks is not possible and employing MANEMO on gateways, rather than sensor nodes is therefore the most sensible setup in this situation.

NEMO has successfully been deployed and tested on the CMM in a simulated mobility environment; work to also allow MANEMO is ongoing.

VIII. Validation

We have been doing tests with the equipment and software described above in quasi-realistic environments. In addition to new technologies such as MANEMO, further considerations are important when evaluating the use of the interconnecting devices. We list below some key issues from our experiences in U-2010. This is not an exhaustive list of evaluation results, but rather an overview of important notes. A more detailed assessment with measurements is underway, and due for completion with the U-2010 project.

It is desirable to avoid having both an enhanced CMM and a HiMoNN gateway operating back-to-back in the same locality. This is mainly for radio interference; only 2 of the 15 radio channels available to 802.15.4 are on non-overlapping frequencies to 802.11 interfaces, which are primarily used by the HiMoNN for the WAN connections. Furthermore, only 3 of the 11 channels of 802.11 are non-overlapping within its frequency domain. This requires good a-priori management and tuning of these resources in Public Safety communications.

The concept of having a single function MAR and separate application-oriented CMM and HiMoNN routers is desirable in configurations where the MAR offers multiple reliable WAN connections and the other nodes support WSN applications (enhanced CMM) and MANETs (HiMoNN). They can cooperate locally, even if wide-area connectivity is down.

In addition, as mentioned earlier, the general-purpose CMM seems to be the only gateway that runs in low-power mode at the moment, and which could easily support a battery-powered wearable outfit for PANs, suitable for multiple scenarios beyond the Fire-in-a-Tunnel. Furthermore, the general-purpose CMM-based gateway provides the flexibility for enhanced services, such as MANEMO and video, as described earlier in Sections V and VII.

IX. Conclusions

The Internet Protocol can have a complementary, if not core, role in emergency response operations. We have identified and described different types of IP-based networks that are available to first responders, as a result of tailoring their communications solutions to exemplary operational scenarios.

Furthermore, a number of ways in which systems have been employed as gateways, to offer additional functionality and increase flexibility, have been outlined and evaluated.

In addition, an interesting area in which work is ongoing has been put forward in the form of simple network mobility (NEMO) and more advanced mesh-based ad-hoc network mobility (MANEMO). Technologies that can benefit most first response operational environments.

It is hoped that the open nature of the proposed gateway architecture, will invite more experimental features by other parties. These can now be evaluated and show-cased in quasi- realistic emerging Public Safety lab environments, hosted by many research institutions and the industry (UCL, Univ. of Luxembourg, Cisco, to name a few).

X. Acknowledgements

We would like to thank the partners of the U-2010 project (EU/ICT no. 035003) for their continuing co-operation and support relating to this work.

References

[1] ArchRock Corp. PhyNet Router. http://www.archrock.com/products/ phynet router.php.

[2] Cisco Systems Inc. Rugged outdoor wireless network routers 3200 series. http://www.cisco.com/en/US/products/hw/routers/ps272/index. html.

[3] IABG mbH. Highly Mobile Network Node. http://www.iabg.de/ infokom/fachthemen/himonn en.php.

[4] IEEE 802.11 Group. http://www.ieee802.org/11/.

[5] IEEE 802. 15.4 Group. http://www.ieee802.org/15/pub/TG4.html.

[6] IEEE 802.16 Group. http://www.ieee802.org/16/.

[7] LiPPERT Cool Mote Master. http://www.lippert-at.com/index.php? motemaster.

[8] Western Datacomm. Intelligent Video Server board. http://www. western-data.com/products/ivs.php.

[9] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. RFC3963: Network Mobility (NEMO) Basic Support Protocol. *IETF: Network Working Group*, August 2005.

[10] P. Dutta, J. Hui, J. Jeong, S. Kim, C. Sharp, J. Taneja, G. Tolle, K. Whitehouse, and D. Culler. Trio: Enabling Sustainable and Scalable Outdoor Wireless Sensor Network Deployments. *IPSN06*, pages 407– 415, April 2006.

[11] K. Mayer and W. Fritsche. IP-enabled Wireless Sensor Networks and their integration into the Internet. *Proceedings of the first international conference on Integrated internet ad hoc and sensor networks*, 2006.

[12] B. McCarthy, C. Edwards, and M. Dunmore. Advances in MANEMO: Denition of the Problem Domain and the Design of a NEMO-Centric Approach. *2007 International Symposium on Applications and the Internet Workshops (SAINTW'07)*, September 2007.

[13] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. RFC4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks. *IETF: Network Working Group*, September 2007.

[14] G. Tolle. A UDP/IP Adaptation of the ZigBee Application Protocol. *IETF Internet-Draft*, http://www.ietf.org/internet-drafts/draft-tolle-cap00.txt, October 2008.