



**LANCASTER UNIVERSITY
COMPUTING DEPARTMENT**

Developing a Portable Wireless LAN Kit

Panagiotis Georgopoulos, Ben McCarthy, Christopher Edwards
{ panos, b.mccarthy, ce } @comp.lancs.ac.uk

Under the Portable WLAN Trial JANET Programme

<http://www.ja.net/development/portablewlan.html>



June 2010

Table of Contents

1	Introduction	4
2	Case Study Requirements	5
3	Portable WLAN Kit Description	8
3.1	Hardware	9
3.2	Software	17
3.2.1	Supporting Mobility	17
3.2.2	Supporting Handovers	19
4	Evaluation	24
4.1	In-field Operation.....	24
4.2	Battery Lifetime and Software Reliability Testing.....	25
4.3	Effective Range Testing	26
4.3.1	Handheld Device to Backpack Router Range Testing	26
4.3.2	Backpack Router to Backpack Router Range Testing.....	27
4.3.3	Dense Woodland Range Testing	28
4.4	Software Testing	29
4.4.1	UMA Testing.....	30
4.4.2	Handover Manager Testing.....	30
5	Conclusion.....	35
	References.....	38

Table of Figures

Figure 1 : Backpack and Router	8
Figure 2 : Backpack Router worn in a field study	8
Figure 3 : The Backpack Router	9
Figure 4 : Ubiquiti Routerstation Board - Front	10
Figure 5 : Ubiquiti Routerstation Board - Back	11
Figure 6 : Closer look on the inside of the Backpack Router	12
Figure 7 : Simple operation with the use of an "ON-OFF" switch	13
Figure 8 : Side view of the Backpack Router (3G modem, Sensor gateway and USB hub visible)	14
Figure 9 : Dimensions of the Backpack Router	15
Figure 10 : Connectivity Option Example	20
Figure 11 : Access Point Information	21
Figure 12 : Range Tests between Backpacks and Individual Device	27
Figure 13 : Range Tests between Backpack Routers	28
Figure 14 : Range Tests between Backpack Routers in Dense Woodland	29
Figure 15 : Handover Manager Testbed Configuration	31

Table of Tables

Table 1 : UBIQUITI ROUTERSTATION BOARD : HARDWARE SPECIFICATIONS	16
Table 2 : PORTABLE WLAK KIT : HARDWARE COMPONENTS COSTING	16
Table 3 : HANDOVER MANAGER TESTING RESULTS	33

1 Introduction

It is without doubt that outdoor academic studies, usually but not limited to biology, geology or physics students/researchers, can be greatly benefited from Internet connectivity. Nowadays, during the course of an outdoor study module, individuals do not just carry their science specific tools, but have also a range of network enabled devices, such as laptops, netbooks, sensor nodes, cameras, GPS devices to aid them during their study. Being able to provide Internet connectivity to this range of devices as individuals move outdoors in regions with harsh morphology, is not an easy task.

The goal of this JANET trial programme [1] is to be able to develop a portable and easily carried Wireless LAN kit (WLAN) that should provide local and global connectivity to the devices individuals carry during an academic outdoors study. In simple terms, local connectivity should be offered to devices in the form of a 802.11b/g wireless network and global connectivity should be offered by the portable WLAN kit with the aid of a backhaul connectivity option, such as a Satellite, 3G/UMTS or WiMAX link or by establishing its own connection to the Internet if that is feasible.

In our view the portable WLAN kit should also try to accommodate the mobility of the end users' devices and bring the advantages of MANEMO [3] to this challenging application domain. Furthermore, careful consideration should be taken when the portable WLAN kit is able to provide Internet connectivity via more than one backhaul connectivity links, as choosing one with the correct characteristics (e.g. bandwidth, latency, cost) is an important decision. The portable WLAN kit should be able to proliferate the coverage of the best available backhaul connectivity link in an efficient way, despite the mobility of the users and the physical characteristics of the area, which might be mountainous or full of dense woodland, foliage and other plants. Finally, supporting all the above in a simple and trouble-free manner to avoid having dedicated network staff on hand is a really challenging endeavor.

The rest of the report describes our development of a portable WLAN Kit. Section 2 that follows, discusses a specific outdoor case study as it would be undertaken for an academic module. This allows us to draw some definite networking and design requirements that we would like our solution to satisfy. Section 3 describes the hardware and software components of the in-house developed portable WLAN prototype. Section 4 evaluates our prototype with a thorough range of tests varying from in-field operation, to battery lifetime and effective range testing. In addition, this section describes the strenuous testing on the software that we implemented to run on our portable WLAN prototype. Finally, Section 5 concludes this report by mentioning the strengths and weaknesses of our solution and discussing future work.

2 Case Study Requirements

The basic motivation behind this work is the development of a **lightweight and mobile WLAN kit**, which would be able to **bring network connectivity “in the field”** as required in a real module academic course. In an effort to provide the best suited portable wireless kit solution for the required case study, let’s try to describe a scenario as it would evolve around the course of an academic study. This would enable us to identify the high and low level requirements the scenario reveals, and target to satisfy those with a designated solution.

Let’s suppose that for a module of the Biological Sciences undergraduate course of the Lancaster Environment Centre (LEC) at Lancaster University, students are supposed to form 10 teams, each comprised of 2 groups of 5 people, which should walk around the Derwent water lake of the Lake District and collect information about the flora and fauna of the region over the duration of daylight of two consecutive days. The aim of each team is to be able to identify as many different plants, trees and animals as possible and collect information about them in an accurate way on an online wiki (or collaborative google wave document) that should be edited during these two days of the outdoor activity. High marks for this academic exercise are given to the students of the teams that find as many different “items” (being plants, flowers, trees, animals, bugs, etc) as possible, but which are also described accurately on the wiki. The accuracy of their description is based on whether the “item” has a photo, a proper description of what it is, a location of where it was found on the region and the environmental conditions (e.g. temperature, light, humidity) that the “item” lives in. As described, each team is comprised of two groups that move independently in the region so that they can cover as much ground as possible and collect information from different parts around the lake. It would be highly advantageous if the groups of a team are communicating during the day, so that they won’t collect information for the same “items” and thus put overlapping information on the wiki. Each team has its own password protected online area on the wiki that should be edited directly as students walk around the region, so that they won’t lose track of what they found.

From the described scenario, it is clear that the students of each team would have multiple and different devices varying from laptops, netbooks, cameras, sensors and many others, which should be supported -connectivity wise- from the portable WLAN kit. It is without doubt that a basic primary requirement of this case study, is to get Internet connectivity for the devices that students carry whilst they move from one place to another during their exercise. Internet connectivity would enable students with laptops/netbooks to post “items” on the wiki in an ad-hoc manner and also help them to look information up for plants or animals they don’t know (e.g. on Wikipedia or their departmental website) so that they will describe them accurately on the wiki. Furthermore, Internet connectivity would enable groups of the same team to communicate using instant messaging or VoIP, so that they can collaborate more effectively. Wireless Internet connectivity should be provided not only for netbooks and laptops, but also for wireless network IP cameras so that students can post photos or videos directly to the wiki (instead of having to download them to a laptop from a storage card and then upload them to the wiki). In addition, students might be carrying GPS devices so that they can create an online map with the coordinates of the location of each “item” they found. The portable WLAN kit should also be able to support wireless sensor nodes which will collect temperature, humidity and other readings from the area the students explore, so that they can record the environmental conditions around the “items” they found.

In order to be able to support the networking needs of the case study that we described above we have identified specific networking requirements (NR) the portable WLAN kit should be able to satisfy. These are as follows :

NR1) Provide a wireless network to all the devices that students carry as they move. Ideally, this network should support a variety of devices (e.g. netbooks, laptops, IP cameras, sensors etc) via different access network technologies (e.g. 802.11a/b/g, 802.15.4 etc)

NR2) Provide Internet connectivity to the wireless network's end devices, ideally, via the best suited and available connectivity option. The portable WLAN kit should be able to get Internet access via different Access Networks (either directly or indirectly) such as 3G/UMTS, Satellite link or via long-range 802.16 links giving it backhaul access to the Internet¹. In addition, it would be very advantageous if the portable WLAN kit would be able to identify all the available connectivity options and use them according to certain criteria needed each time, such as cost, bandwidth, delay or other application requirements.

NR3) Maintain efficient local and global communication of users when they are roaming. An important consideration on the networking needs of a field study is that the end devices tend to move independently or as a group and thus a portable WLAN kit should be able to maintain connectivity for them as they roam. Therefore, an efficient networking solution for these mobile devices could be optimized with the support of host and network mobility protocols that are specifically designed to provide seamless connectivity for mobile hosts (such as Mobile IPv6 [13]) or mobile networks (such as NEMO BS [14]) as they roam. In addition, MANET protocols might be able to bring additional advantages when local communication is taking place. In fact, the combination of both the aforementioned protocols, which has given birth to the newly emerging MANEMO protocols, seems to be the most efficient solution for the networking needs of a field study which is comprised of students roaming from one region to another and they are interested in both local and Internet communication. Therefore, a portable WLAN kit should try to run a MANEMO protocol that is especially designed to support the mobility of users' end devices when the move independently or as part of a mobile network.

On the other hand, the portable WLAN kit should be able to satisfy more "practical" requirements that an outdoor academic study has. These requirements are mainly related to its design and its feasibility for every-day. Therefore, ideally, we would like our portable WLAN solution to satisfy the following design requirements (DR) :

DR1) Size : Should be small and fit easily inside a backpack compartment.

DR2) Weight : Should be mobile, portable and lightweight, easily carried by a person for a reasonable amount of hours.

¹ One way this can be accomplished is by identifying Internet Points of Presence (PoP) of the National Education Network (NEN) around the region an academic study is to be undertaken and get the portable WLAN kit to reach those via 802.16 long range links. For example, the Cumbria and Lancashire Education Online (CLEO) network interconnects all the schools around the area of Cumbria and Lancashire and thus a PoP might be just a few miles away from a study field [4, 30].

DR3) Weather resistant : Should be resistant to weather conditions such as wind, rain, frost and sunshine. Ideally the kit should be enclosed in a waterproof and robust enclosure.

DR4) Easy to use : Should require no or minimal networking setup, establish network connections rapidly and boot up quickly. Users should require little or no training to use it.

DR5) Battery lifetime : Should have a reasonable operation lifetime .

DR6) Reliability : Should be able to withstand vibration and shock (i.e. not reset nor hang) from walking, running and climbing. In addition, its software should be as much bug free as possible so that the router will not reset nor hang during operation.

DR7) Effective range : Should be able to provide a reasonable network coverage for individuals roaming in an outdoor area.

With the aforementioned networking and design requirements into account we have designed a portable WLAN prototype that is described in detail in the next Section.

3 Portable WLAN Kit Description

This Section describes the portable WLAN Kit that was designed at the Computing Department at Lancaster University. Our prototype is based on the idea of using an embedded Linux board with multiple wireless interfaces to run as a Mobile Router (MR) in a small and simple enclosure that fits in a backpack (see Figure 1), thus we also refer to it as backpack router (term interchangeably used onwards with Portable WLAN kit). The idea is that a member of each group of individuals wondering around the fields is carrying a backpack with the mobile router (see Figure 2), thus providing connectivity to all the devices around him.

This portable WLAN kit should satisfy as many of the networking and design requirements that we described in the previous section as possible. Therefore, the kit should be easily carried in a backpack from a person walking in the field, and its main purpose should be to find the best available Internet connectivity option and offer it via one or more wireless interfaces to all the mobile devices around it. If the mobile router is not able to establish Internet connectivity via an externally offered backhaul option (e.g. Satellite or WiMAX link), then it should try to establish its own 3G/2G connection or connect via its ad-hoc interface with another backpack router in its vicinity (explained in detail in the following Subsections). This would enable backpack routers to create some sort of a mesh network in the field and thus proliferate Internet connectivity to other backpack routers and end devices carried by individuals (students or researches in our scenario) roaming in the field, leading to better connectivity coverage to more end user mobile devices.

The following sections describe the hardware, software, design and implementation decisions that we have taken for our portable WLAN prototype.



Figure 1 : Backpack and Router



Figure 2 : Backpack Router worn in a field study

3.1 Hardware

The portable WLAN kit prototype is a small, lightweight, multi-interfaced mobile router enclosed in a compact waterproof enclosure (see Figure 3). The primary role of the mobile router is to run the MANEMO protocol suite (described in the following Section) to maintain connectivity between the mobile devices around it (the devices that students carry) and provide Internet connectivity to them via a backhaul option usually provided externally via, for example, a Satellite, WiMAX or 3G/UMTS link. In situations where no Internet connection could be established using a backhaul option, the backpack router can provide its own Internet gateway if suitable 3G/2G coverage is available, as it is equipped with a USB 3G modem [19]. The portable WLAN kit is able to provide both an 802.11b/g wireless network for devices to connect to it and also play the role of a sensor gateway and collect sensor readings from surrounding sensors, as it is equipped with an 802.15.4 TmoteB sensor board.



Figure 3 : The Backpack Router

The main boards we are currently using for the portable WLAN kit are Ubiquiti Routerstations [2, 12, 21] (see Figure 4 and Figure 5). After much analysis and testing, this was considered the best board for all our requirements (size, weight, performance, radio capability and Linux-compatibility). There are other board possibilities (e.g. Gumstix, mini-ITX, ALIX, Gateworks) but they are inferior to Ubiquiti boards with respect to one or more of our requirements. We only considered single-board computers (SBCs) and ruled out PC-104 based boards due to their size and layout resulting in a relatively large enclosure.

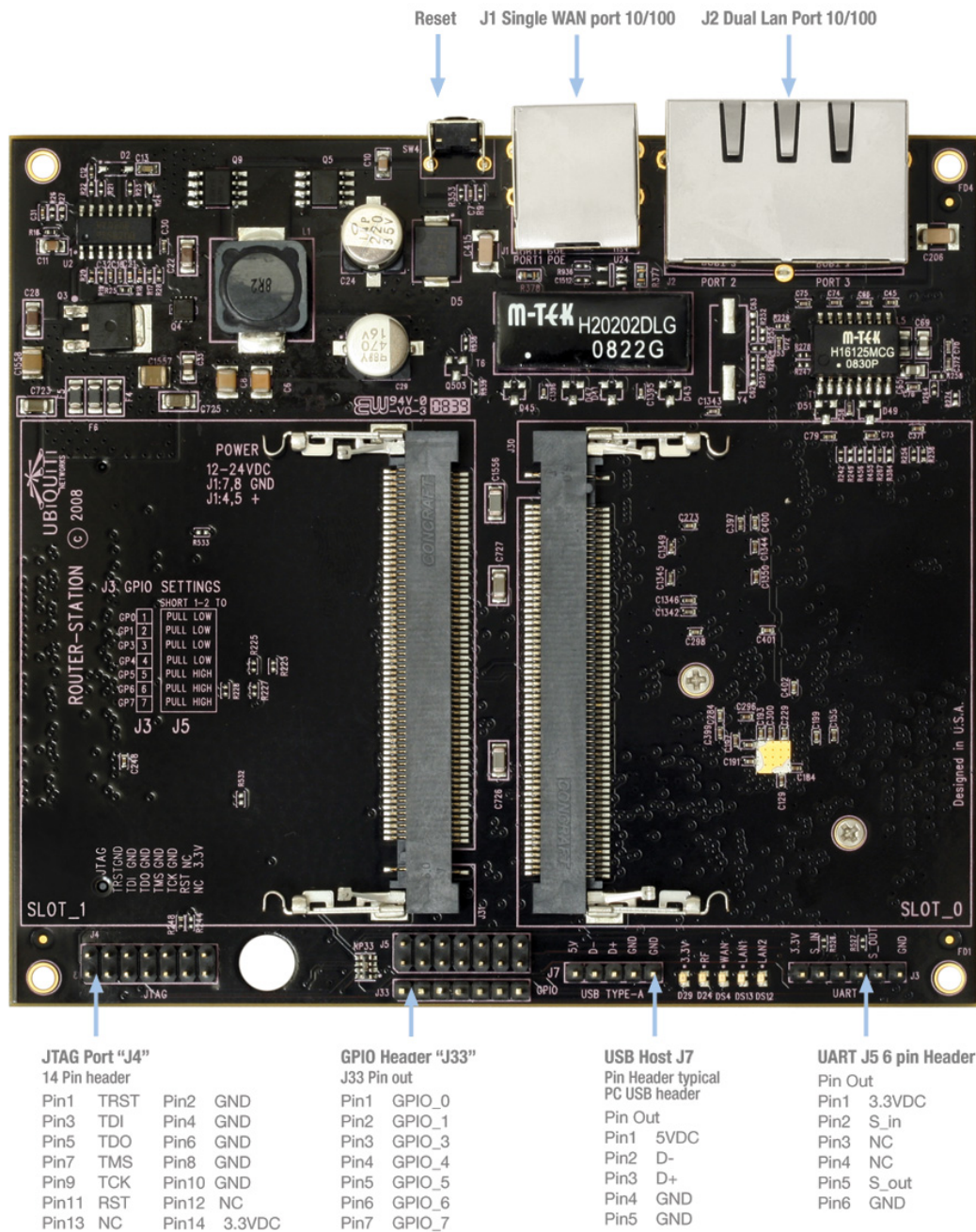


Figure 4 : Ubiquiti Routerstation Board - Front

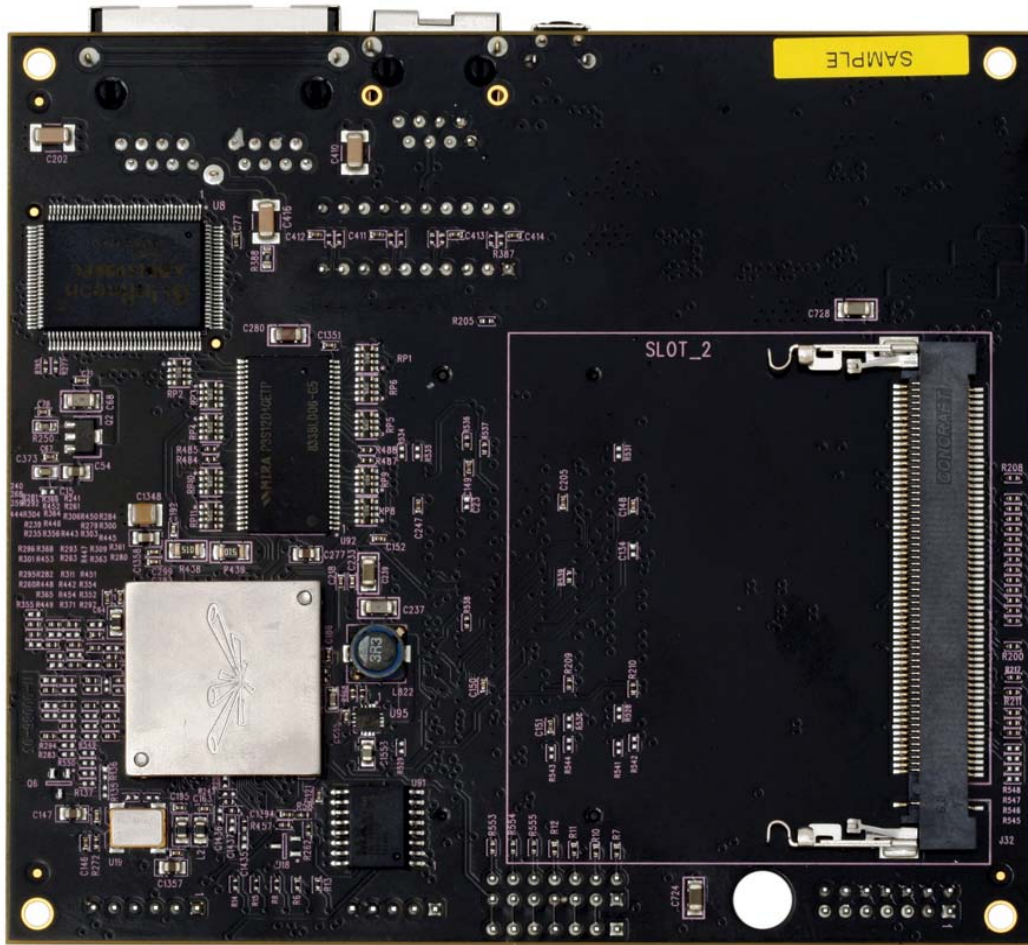


Figure 5 : Ubiquiti Routerstation Board - Back

The Routerstation board [2] can only be powered via the power-over-Ethernet (PoE) port so inside the router enclosure we have a simple circuit that connects a Lithium-Ion battery to the PoE port (seen at the top of Figure 6). The board accepts anything between 12-24V, although our tests with numerous 12V batteries were unsuccessful as they would sometimes drop their supply below 12V. The Lithium-Ion batteries we use are 15V and supplied by Enix Energies [15]; anything higher than 15V and the batteries we found were too big and heavy for a backpack router.

The Ubiquiti Routerstation boards have three mini-PCI slots (two at the front and one at the back) and so each backpack router contains three Wi-Fi modules. These Wi-Fi modules are Ubiquiti XtremeRange2 (2.4 GHz) [16] (two of them are visible on Figure 6) which can be exchanged according to requirements. We use one Wi-Fi module to create an 802.11b/g access point that provides wireless connectivity to end-devices around the backpack router (laptops, netbooks, IP cameras etc). The second Wi-Fi module is used for MANET (ad-hoc) connections with other backpack routers and thus create some sort of a mesh network in an effort to further extend their wireless coverage and provide more efficient local communication. Finally, the third Wi-Fi module is for the backpack router to connect to other access points and get Internet connectivity from them. For example either via an access point connected to a backhaul Internet connectivity link or an access point of another backpack router that has Internet connectivity. Each Wi-Fi module is connected to a 2.4 GHz omnidirectional antenna giving 5dBi gain [18] (see Figure 3).

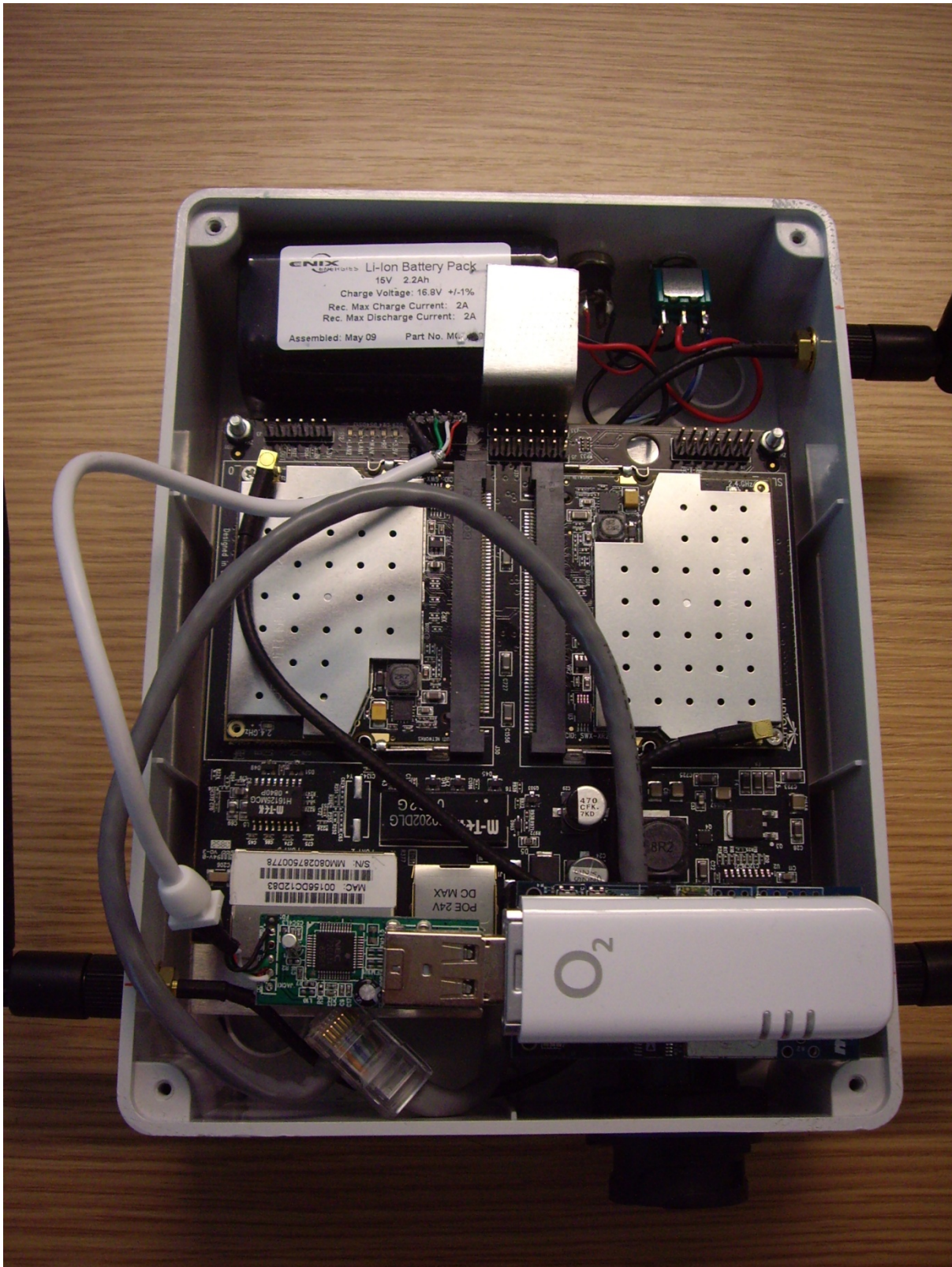


Figure 6 : Closer look on the inside of the Backpack Router

On the outside of the enclosure, there is a bare minimum of features in order to simplify user operation. An on/off switch is accompanied by a charger socket on the one side (see Figure 7) and an Ethernet connection is provided on the other side (see Figure 8) to allow the backpack router to be connected to other devices across a wired LAN if that is required.

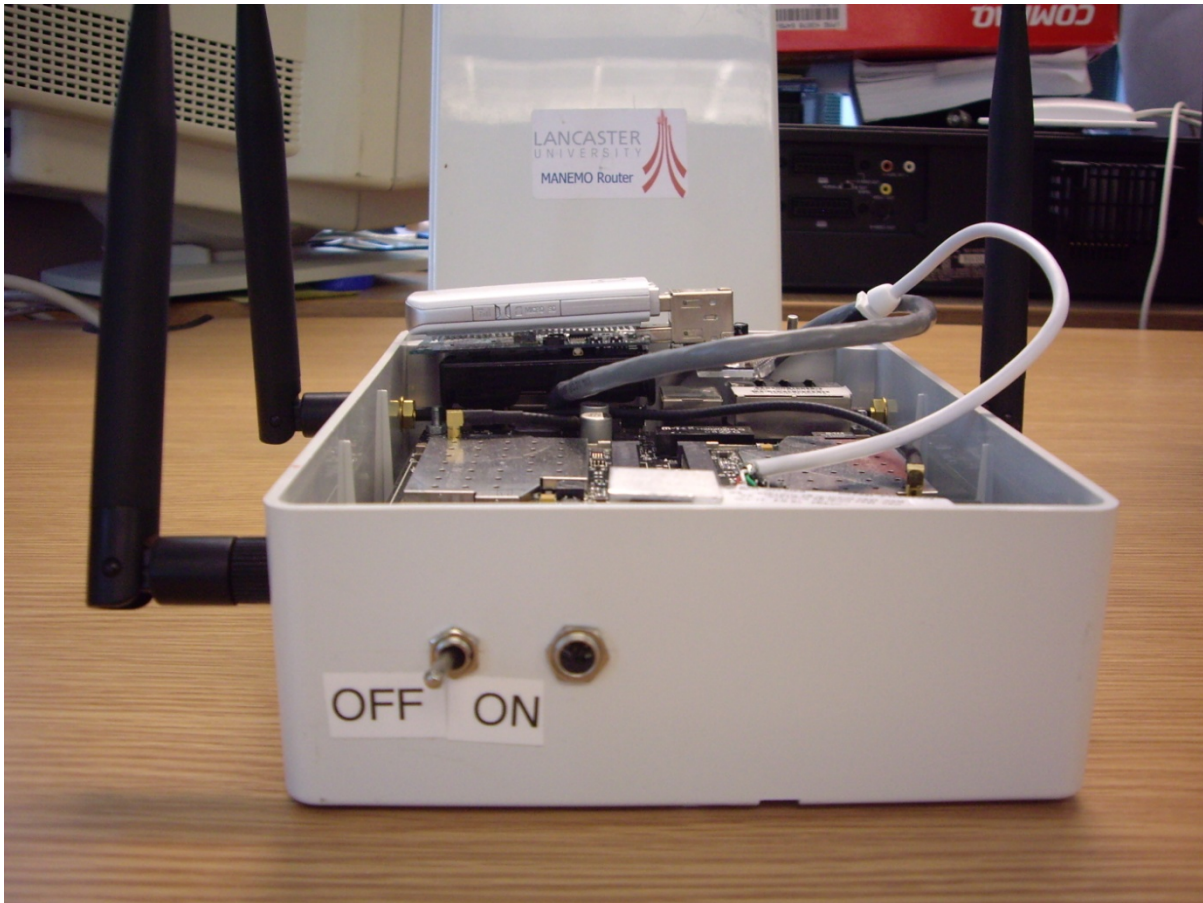


Figure 7 : Simple operation with the use of an “ON-OFF” switch

To allow the portable WLAN kit to establish its own direct connection to the Internet if no other backhaul option is provided, we have also integrated a 3G/2G (UMTS/GPRS) module (see Figure 8) [19] via a small form-factor USB hub that is soldered to the USB pins of the Ubiquiti main board. The 3G/2G capability (depending on the Operator and the coverage) is important for maintaining global Internet connectivity when there is no global route via any of the 802.11 interfaces. An intelligent software module for handover management (described in the Section 3.2.2) is able to determine when this interface should be used.

Augmenting the capabilities of the portable WLAN kit with sensor networking was an important decision of ours, as we believe that sensor nodes are much needed in outdoor academic studies for recording light, humidity, temperature, atmospheric pressure and a variety of other readings. For this reason, we connected a TelosB TPR2400CA sensor board [20] on the USB hub (see Figure 8) to allow the backpack router to also function as an 802.15.4 gateway and thus provide seamless sensor networking in a mobile environment. Network wise supporting the transmission and reception of sensor readings requires instructing all the sensor nodes around the portable WLAN kit to send their readings to the IP address of the sensor gateway of the backpack router over 802.15.4. In turn, the backpack router sensor gateway is seamlessly translating these readings to IP packets and forwards them to a globally reachable sensor sink server over the Internet being accessed via the backhaul link the portable WLAN kit is using at the moment of transmission. To test this sensor capability we have implemented the client and gateway sensor node applications, in addition to the sensor readings sink server that perform this communication successfully.

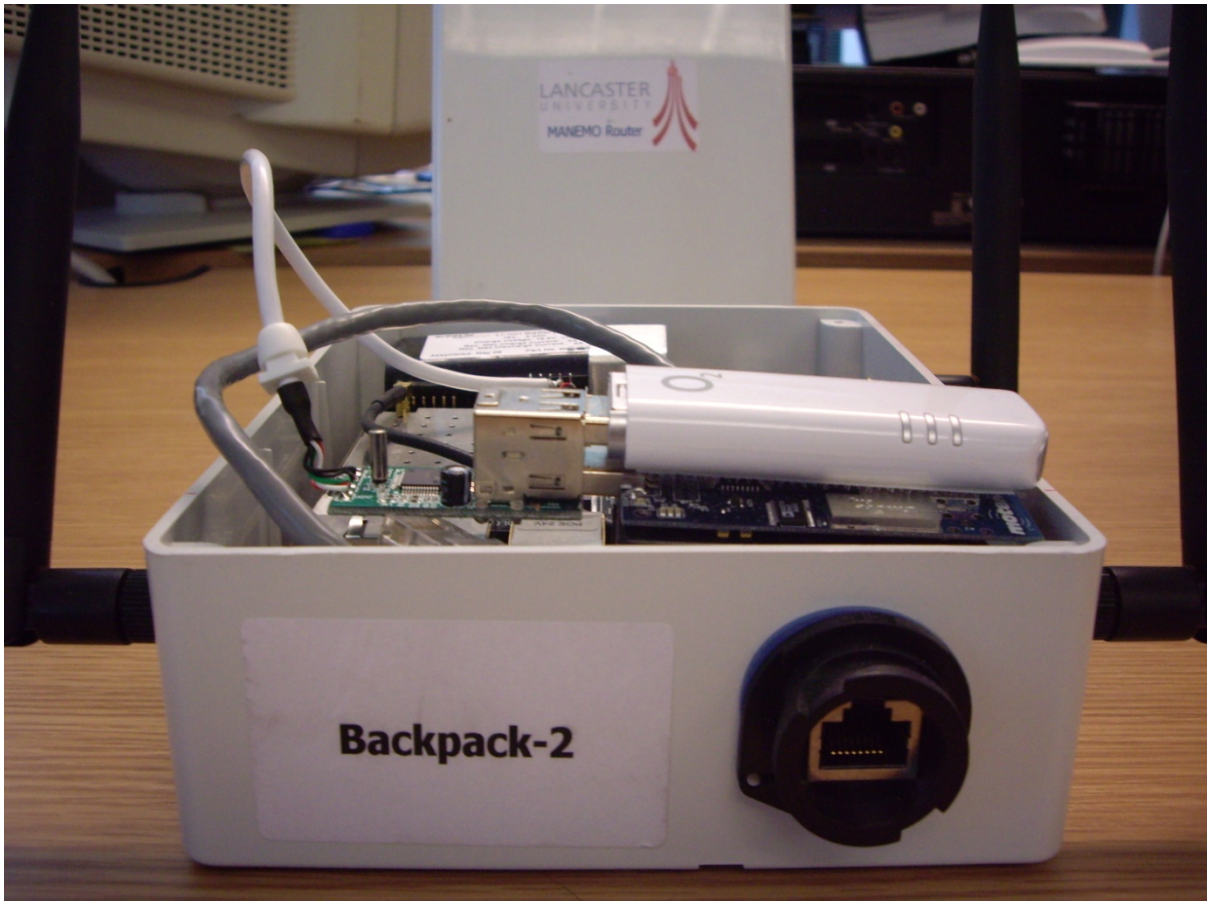


Figure 8 : Side view of the Backpack Router (3G modem, Sensor gateway and USB hub visible)

The enclosure of the backpack router is a plain sided IP56 rated box [17], made of thermoplastic and is resistant to water, heat and minor shocks. The dimensions of the backpack router (excluding antennae) are 190mm x 140mm x 70mm (length x width x depth) (Figure 9). For detailed dimensions and schematics of just the Ubiquiti Routerstation board the reader is referred to [12]

The total weight of the backpack router (including the 3G module and TelosB sensor gateway) is only 1.2Kg, much less than an average laptop (circa. 2.5Kg) and around 8% less than typical netbooks such as the Samsung NC10 (1.33Kg) and the Asus Eee PC (1.3Kg). Since it is high likely that the students will carry their usual (and often heavy) academic related equipment, the added size and weight of a mobile router could be extremely unwelcome. Therefore, we feel that the 1.2Kg weight of our portable WLAN prototype is considered ideal.

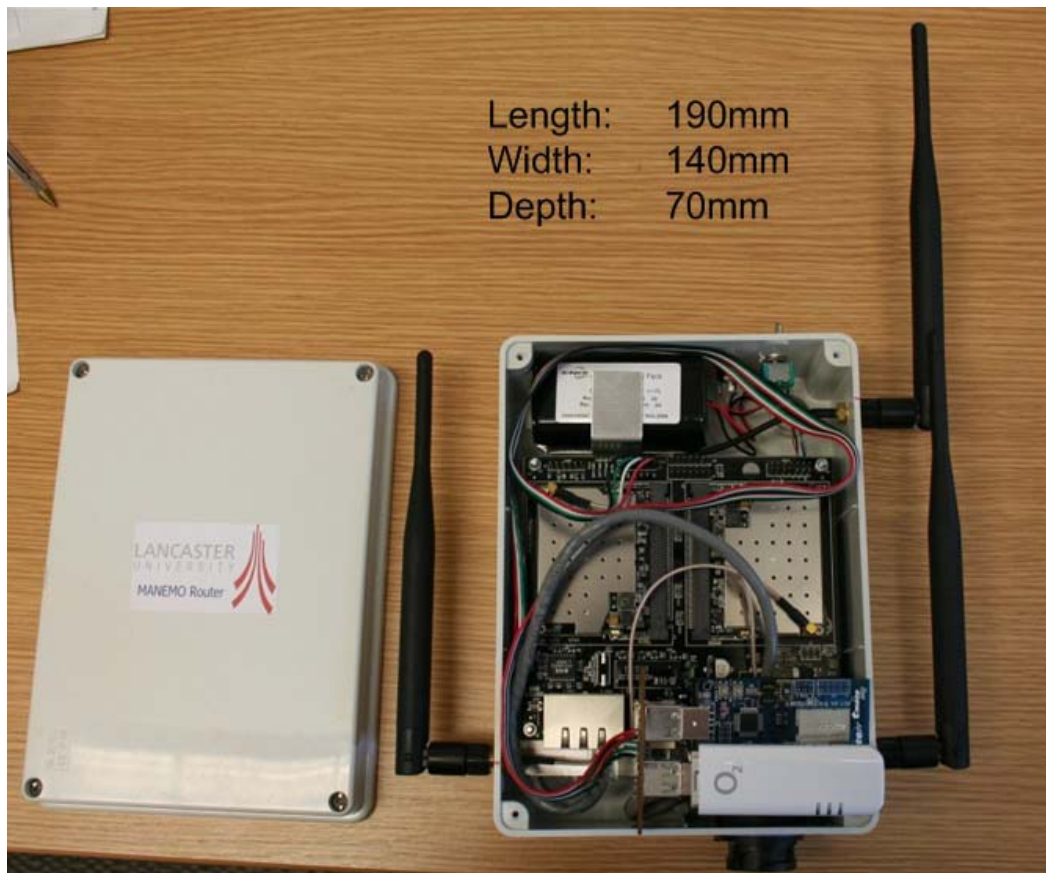


Figure 9 : Dimensions of the Backpack Router

Fortunately, the relatively small size and light weight of the enclosure (Figure 9) means that it can easily fit inside the pouch of a backpack. The enclosure was designed so that the omnidirectional antennae would be vertical when placed inside the backpack (see Figure 2) to maximise the efficiency of the antennae's horizontal polarisation.

Finally, Table 1 below presents the hardware specification of the Ubiquiti Routerstation board itself, whereas Table 2 presents all the hardware components that comprise our portable WLAN kit prototype with their approximate costing. The approximate cost of the portable WLAN kit as a whole (including its charger and mains lead) is 511.57 pounds (VAT inclusive), but can be reduced according to the specific needs of the application that needs to be supported. For, example if sensor networking is not required, then the TelosB sensor gateway board is unnecessary, which reduces the aforementioned price by 118 pounds, bringing down the cost of the prototype to 393.57 pounds. On the other hand, the described portable WLAN kit is our first complete prototype and maybe our next advanced effort might cost a bit more due to more specialized hardware.

Table 1 : UBIQUITI ROUTERSTATION BOARD : HARDWARE SPECIFICATIONS [2]	
Processor Specs	Atheros AR7161 MIPS 24K, 680MHz
Memory Information	64MB SDRAM, 16MB SPI Flash
Networking Interface	3X 10/100 BASE-TX (Cat. 5, RJ-45) Ethernet Interface
PCI Support	3X 32-bit mini-PCI
Approvals	FCC,CE
RoHS Compliance	YES
Power Supply	From 12V to 24V
Power Method	Passive Power over Ethernet (pairs 4,5+; 7,8 return)
Operating Temperature	-30C to +75C
Weight	0.21 kg

Table 2 : PORTABLE WLAK KIT : HARDWARE COMPONENTS COSTING			
COMPONENT	SUPPLIER	QUANTITY	APPROX. COST (£) (inc. VAT, excl. delivery)
Ubiquiti RouterStation board	Microcom.us	1	46.90 (69.95\$)
Ubiquiti XTREMERANGE2, MINI-PCI Wireless Adapter 802.11b/g (600mW)	Microcom.us	3	(3x) 67.00 (99.95\$)
2.4GHz, 5dBi gain SMA Male internal knuckle antenna	Siretta.co.uk	3	(3x) 4.65
MMCX to Re-SMA Chassis Socket - 18cm	Linitx.com	3	(3x) 3.15
USB 2.0 Hub, Mini 2 Port (white)	Farnell.com	1	5.18
O2 MF100 (Qualcomm MSM6280) White USB Modem	O2.co.uk	1	19.99
TelosB (TPR2400CA) Sensor mote	Willow.co.uk	1	118
IP65, 190X140X70MM, Plain Sided Enclosure	Farnell.com	1	4.68
Enix Energies Battery, LI-ION, 15V, 2.2AH, PK.	Farnell.com	1	40.26
Mascot Charger, LI-ION, 3 Step 4 Cell	Farnell.com	1	25.39
Ubiquiti Networks POE-15-EU	Microcom.us	1	8.68 (12.95\$)
Mains lead 2.5A to 13A plug (2M)	Farnell.com	1	3.09
Misc (switches, cables, screws, battery holder, fuses, plugs, soldering, etc.)	-	-	15
Total Approximate Cost for a Portable WLAN kit (£) :			511.57

3.2 Software

The Ubiquiti Routerstation boards that we are using in our portable WLAN solution ship with OpenWRT Kamikazee [6], which is one of the most popular Linux distributions for embedded devices and especially open-source based wireless routers. OpenWrt provides a “fully writable filesystem with package management”, which for the developer means “a framework to build any application without having to build a complete firmware around it”, and for the user means that “full customization is provided” and therefore he has the flexibility to use the device in whatever way he wants [6]. In other words, as we build our Portable WLAN solution using Routerstation boards, OpenWrt allows us to compile and configure our mobility related protocols (described in the following subsections) with their complementary packages, and also provides the flexibility to the end users to setup scripts and customize the router in whatever way they want to suit their network setup.

To support our mobility protocols we had to rebuild the OpenWRT kernel with the core UMA protocols, OLSRd [22], RADVD [23] and OpenVPN [24] packages. This process required checking out the latest OpenWRT version, installing the required packages, inserting them into the kernel, selecting the appropriate kernel options and finally compiling this UMA enabled version of OpenWRT. The reader can find detailed information about these on our wiki [9, 10] as well as the OpenWRT wiki and configuration guide at [7, 8] .

In addition we created scripts to set up the network interfaces of the kit and scripts to run our mobility protocols. OpenWRT provides a very useful utility for automatically running software when it is booting up. Therefore we took advantage of this and added our scripts so that every time the portable WLAN kit boots up, all the networking interfaces are set up automatically and our mobility protocols start running without any additional intervention from the user. IPv6 autoconfiguration feature is our advocate in this process as by using RADVD to correctly advertising network prefixes in Router Advertisements, the backpack routers can configure topologically correct addresses without any further network setup. The reader is referred to [11, 8] for detailed information on setting the aforementioned scripts to run when the router boots up.

3.2.1 Supporting Mobility

An academic field study evolving around the scenario we described in Section 2, unavoidably includes multiple different wireless devices experiencing mobility and network roaming. If we consider carefully the scenario we described, we realize that it involves groups of mobile devices with networking needs, moving as a whole and experiencing network mobility (as opposed to host mobility). Therefore, our portable WLAN router should be running the Network Mobility Support Protocol [14, 25] to support the mobility of the end devices that students carry, as they explore a region individually or as a group. The advantages of constant Internet connectivity for all the end devices as they move, without them being aware of their mobility and no matter where the point of attachment of the network is, are very significant in our scenario and thus the router of the portable WLAN kit should be able to run NEMO BS [14, 28].

On the other end we realized that groups of students are in need of communication with other students in the vicinity in an optimal fashion. Using NEMO BS in a VoIP communication scenario where a student from a group wants to talk with another student from another group, would mean that all the VoIP packets would have to be routed out of the local network to the Internet and then be routed back in the other group's network even though the two groups are possibly located very near to each other. It is apparent that this imposes a very suboptimal routing path that introduces delay and overhead to the communication, which should be avoided at the networking level. In this "local" communication scenario, a MANET protocol such as OLSR [26], optimized for local ad-hoc routing of packets, would bring substantial benefits and thus we would strongly want our portable WLAN kit to support it.

One approach to support the two aforementioned networking requirements (Internet connectivity for mobile networks and optimized local communication) would be to be running NEMO BS and OLSR in parallel in our portable WLAN router. However, our approach is a significant research step forward, as it builds on the fact that both the aforementioned networking protocols (NEMO BS and OLSR) have individually some clear disadvantages, but if they are integrated carefully they can benefit each other. The research community as a whole has captured and tried to encounter these disadvantages in one optimized solution under the umbrella of the MANEMO (MANET + NEMO) research work [3]. The motivation behind the MANEMO research work is based on the following observations.

NEMO BS can provide a realistic and relatively efficient solution to mobility scenarios which incorporate single, distinct mobile networks. However, in nested NEMO scenarios, NEMO BS introduces an unacceptable level of routing inefficiency that makes its real-life use unfeasible [3, 5]. In nested NEMO scenarios, NEMO BS needs to route packets out of the NEMO networks' topology using tunnelling, which leads to inefficient routing and imposes processing and delay overhead even in cases where networks are in very close proximity. In addition, NEMO BS introduces a level of indirection in local communication among devices of mobile networks that are directly connected, because they must rely on the reachability of an external entity, namely, the Home Agent or Home Agents of the communicating networks. These NEMO BS protocol inefficiencies could be very well benefited from a MANET-style routing protocol that could be engaged to facilitate the local routing of packets between mobile hosts and mobile routers, without them losing their public external reachability from the Internet, that NEMO BS offers.

On the other hand, MANET protocols are implemented to optimize local communication between mobile hosts and mobile routers without a predeployed infrastructure. However, although a MANET node can have optimized local communication with other MANET nodes and get Internet connectivity from designated Gateways, it cannot register any change in its point of attachment to the Internet, and the MANET protocol itself cannot be allowed to leak routes into the Internet. This means that nodes within a MANET are not directly reachable externally, that is from a Correspondent Node located on the Internet, and in turn, whilst a MANET node can communicate with a CN if it initiates the communication, packet transfer cannot continue if the MANET node's attachment to the Internet changes. Therefore, the NEMO BS properties of continuous external reachability of a mobile node despite its network's mobility, can greatly benefit a scenario where the disadvantages of a MANEMO protocol are apparent.

As we discussed previously, in an attempt to produce a suitable solution to the aforementioned problems of both NEMO BS and MANET research domains, work has begun on integrating the efficient, localised, multihop routing provided by MANET protocols with the transparent network mobility support offered by the NEMO BS protocol in an area dubbed as MANEMO (MANET+NEMO) [3, 5]. This research is trying to use the efficient, local routing model of MANET protocols to solve many of the problems experienced in nested NEMO networks. In addition, the globally reachable Home Agent-based properties of NEMO can also provide advantages to MANET scenarios. MANETs could use a Home Agent to provide them with a permanently reachable location on the Internet without flooding their changing routing information into the infrastructure. Moreover, in certain scenarios where a MANET node is disconnected from a MANET but manages to have its own direct connection to the Internet, it may be feasible to route packets to another MANET node via the Internet this time, using its communication with a HA. It goes without saying, that the MANEMO research work can greatly benefit both the MANET and NEMO technologies and solve the problems of their respective domains creating a unified solution.

The Unified MANEMO Architecture (UMA) is the first MANEMO implementation of a protocol architecture that has been designed at the Computing Department, Lancaster University. UMA integrates and augments the MANET and NEMO technologies in one unified solution with two facets, in an effect to bring mutual benefits to both problem domains. By using protocols with MANET based properties, the communication model of a nested NEMO network can be optimised in a manner that best suits the characteristics of scenarios that form the nested NEMOs, which is implemented with the “**NEMO-Centric MANEMO (NCM)**” facet of UMA. Conversely, the globally reachable properties provided by the NEMO BS protocol can be used to bring additional functionality to MANET configurations, which corresponds to the “**MANET-Centric MANEMO (MCM)**” facet of UMA.

Having designed and implemented such an innovative and state of the art MANEMO protocol ourselves, at Lancaster University, it would be unfortunate not to apply it in the Portable WLAN context where it could be bring great benefits. Therefore we have compiled and build our C code for the Routerstation board of our Portable WLAN kit and configured it to run automatically and take advantage of the three Wi-Fi module the router has, when it boots up. To avoid repeating detailed information on the birth of UMA, the way it operates and its testing, the reader is referred to our JANET deliverable document “The progression from IPv6 to MANEMO” of the Mobile IP Trial project [5] and also to our related research papers [27, 28].

3.2.2 Supporting Handovers

The router that comprises the portable WLAN kit should be an autonomous entity, capable of operating continuously without any manual interaction from an end user. A Mobile Router (MR) (i.e. backpack router) running UMA can conceivably adapt to the changing topologies of the network setup and ensure that the best possible network layer routing is always utilised. However, whilst the network protocols running on the MR are able to adapt to such changes in the network, they do not actually *trigger* any changes (i.e. network handovers) to occur in the first place. The types of changes we refer to are those related to utilising the best possible connection to the Internet at any given

time. For example, during the course of an outdoor field study, the portable WLAN router might be given three backhaul connectivity options, for example via an access point to a WiMAX link, via an access point to a Satellite link or via its own UMTS connection, and it should be able to decide which one to use based on certain criteria. For this reason, we have implemented a utility that is auxiliary yet complementary to the UMA network protocol suite, which we call the Handover Manager [29]. The Handover Manager's role is to constantly monitor all of the available backhaul connectivity options and intelligently decide the most appropriate connection to the Internet to utilise.

Figure 10 illustrates a typical scenario the Handover Manager may be presented with during the course of an outdoors study. In this diagram, the Mobile Router is currently connected to the Internet via the Wi-Fi access point AR5, which could be getting Internet connectivity from, for example, a long-range WiMAX Link. As an alternative, it can also choose to communicate with nodes in the Internet via a UMTS connection it has in place via its USB UMTS gateway, or via its ad-hoc interface connection with MANET 1 (let us consider that this is the MANET network of all the backpack routers), or it could choose to establish its Wi-Fi connection with another alternative access point (AR1, AR2, etc). If the connection that the MR has in place with AR_5 is satisfactory, then it will continue to be utilised. However, if the MR's connection with this access point becomes weak and its throughput drops below a satisfactory level, then the Handover Manager will intervene by establishing a connection with a more suitable alternative.

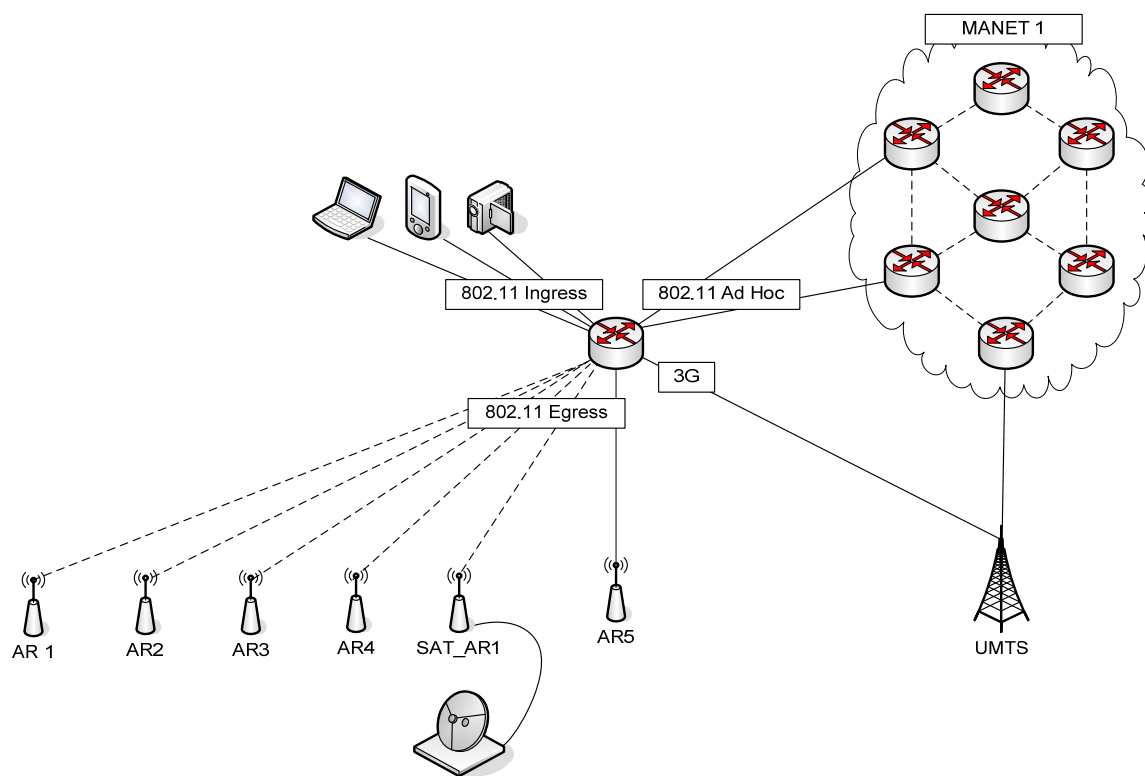


Figure 10 : Connectivity Option Example

In order to determine the most suitable alternative from the backhaul connectivity options, the Handover Manager accurately gathers information about the surrounding networking environment, and simultaneously monitors a number of parameters, they are:

- Signal strength of current Wi-Fi connection with access network.
- Signal strength of cellular base station.
- Signal strength of all other Wi-Fi access points within range.
- Layer 3 connectivity of current Wi-Fi connection.
- Layer 3 connectivity of cellular (3G/2G) connection.
- Capability of any available MANET Gateway's Internet connection.
- Network characteristics of any available iMANET connection.

The process of monitoring each of these parameters is handled by separate threads that each update a centrally stored database which holds relevant information about every available connection. Of the network parameters monitored, the signal strength of the MR's current Wi-Fi connection and of its cellular network interface are the most straightforward pieces of information to ascertain as both values can be requested from the respective interface drivers. To ascertain the signal strength of all other available access points the MR periodically performs a scan of its surrounding environment and stores the results it gathers along with the previous n results in a sub table (where n is a value that is configurable via a configuration file). An example of the resulting information records are illustrated in Figure 11. This allows the Handover Manager to derive the average signal strength and ignore potentially erroneous information caused by temporary obscurities in the radio environment.

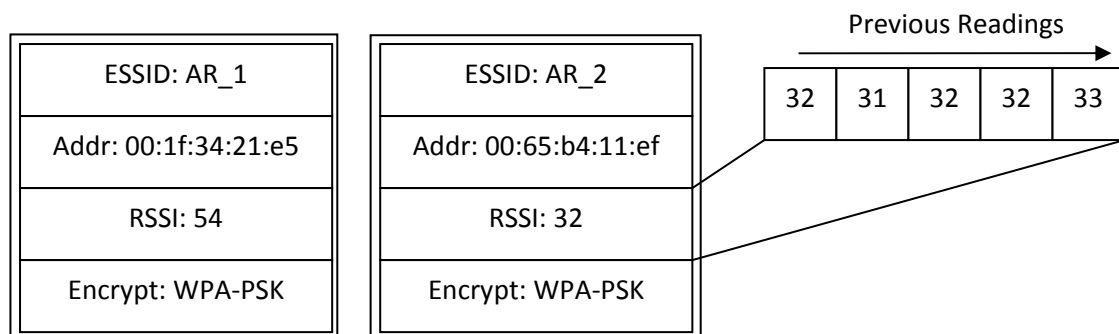


Figure 11 : Access Point Information

In addition to monitoring the physical signal strength of the direct access network connections, the Handover Manager also monitors the network layer availability of its direct connections (if a connection is present) by periodically performing ICMP echo request/reply transactions with the access router of the network it is getting access from. This process is performed between the IPv6 link local addresses associated with the MRs interfaces and the appropriate access routers. Using the link local scope addresses in this manner ensures that any change in the global routing table caused by network topology alterations and subsequent handovers does not affect this local communication check. Obviously the most important information this reveals is whether network layer connectivity is actually available over a given connection, since many situations can arise where an access

network maybe physically visible at the radio layer but it is not possible to actually establish Internet access over the connection. Another important network characteristic this process exposes is the network latency times experienced. This is particularly useful in current deployments because as IPv6 adoption is not massively prevalent yet, IPv6 transitioning mechanisms (typically tunneling) are routinely utilised to provide access over existing IPv4 networks. In these situations the access router that the Handover Manager communicates with when performing an ICMP echo request is therefore located at the IPv6 transitioning tunnel endpoint. Determining the latency experienced between the MR and the tunnel endpoint gives the Handover Manager a good indication of the overall network characteristics including the overhead imposed by the IPv6 transitioning technique.

As well as monitoring the interfaces that the MR can establish its own direct connection with, the Handover Manager also monitors the network characteristics of the path to the Internet achievable via any MANET that the MR is currently connected to via its ad-hoc interface (i.e. the rest of the backpack routers carried in the field of our scenario). This comprises of two steps, firstly the Handover Manager takes into account the latency that each available MANET Gateway advertises it is currently experiencing and secondly it considers the link quality metrics associated with the multihop path between itself and any specific Gateway. In order to achieve the first step the OLSR component of UMA had to be augmented to accept the latency information about the Gateway's Internet access and then include it into one of the existing OLSR messages. The ability to carry information related to a Gateway's connection is not possible in OLSR so to introduce this capability we included it into the OLSR Host and Network Association (HNA) message format. HNA messages are used by Gateway's in OLSR to advertise their ability to reach the Internet and so by including the connection latency information of the Gateways within their actual Gateway advertisement message it means that this related information is collocated in one message. Upon receiving these messages OLSR then forwards their content (Gateway address and its current latency experienced) on to the Handover Manager for it to store and process. On the other hand, OLSR does inherently provide the MR with information related to the quality of the multihop path up to any particular Gateway, so this too is provided to the Handover Manager. In both of these cases the information flow is different for the Handover Manager than it is with the direct access network connections it forms. Rather than having to proactively probe or transmit traffic into a connection, in the indirect case of MANET communication, information about the available network connections is sent to the Handover Manger.

All of the aforementioned information is gathered and periodically updated for the entire duration that the Handover Manager is operational. After completing all of its monitoring processes once, the Handover Manger has effectively developed a network connectivity map of its local environment which it then strives to keep up-to-date as the backpack router's mobility causes network infrastructure to come into and out of range. This network map is then utilised by the Handover Manager's decision engine, which constantly cycles through all the available information in order to maintain an accurate and prioritised list of connection alternatives.

At present, the Handover Manager uses a simple connection preference model:

1. Wi-Fi Internet access network
2. UMTS
3. Wi-Fi extension of satellite connectivity

4. MANET with visible Gateway

Any appropriate Wi-Fi network that provides a direct connection to the Internet is selected first. If no access points matching this criterion are available, the Handover Manager first checks the current status of the Layer 3 connectivity of the UMTS connection via its modem (this information is immediately available to the Handover Manager because it periodically checks the UMTS connection at all times in parallel to its other operations). If the UMTS connection is unavailable, the next connection the Handover Manager will consider is an access point that offers an indirect link to a satellite access network. Finally, if no satellite connection is available either then the connection with a MANET will be utilised if a suitable Gateway is present. Finally, if no connectivity options are available at all, the Handover Manager will not perform any handover and will instead continue to monitor all interfaces for the first available connection.

4 Evaluation

The portable WLAN kit is designed to be carried easily by individuals (as well installed into a vehicle if required) and is the key component in the proliferation of the mobile network that is projected in the field of operation, eventually providing network connectivity for all the devices that students/researchers use for their academic needs outdoors. It is therefore important to ascertain the capabilities of the kit we designed and determine its suitability for use in everyday outdoors academic exercises.

In this section we detail the testing we performed specifically to evaluate the capabilities of the backpack router and see if the designed prototype satisfies the original objectives of this project. Our thorough testing spans from evaluation the satisfaction of the networking requirements of the portable WLAN kit, to evaluating the satisfaction of its design and in-field operation requirements which were all detailed in Section 0. Therefore, to verify the networking requirements of our portable WLAN solution we performed thorough testing on our innovative mobility protocol suite, namely UMA, and our intelligent Handover Manager software. On the other end, to verify the design and practical requirements of our solution, we performed a number of in-field operation testing, varying from battery lifetime and reliability testing to effective range testing. The range testing was performed outdoors in a field with both end user devices and other backpack routers being interconnected and thus forming a connectivity chain, essentially extending network coverage. The results from our tests are reported in the following subsections.

4.1 In-field Operation

One of the primary requirements for the backpack router is to be unobtrusive in the students/researchers operations out in the field, which ultimately means it must be very straightforward for them to use and require very little input during operations. The portable WLAN kit was designed from the beginning with this very requirement in mind and is therefore almost as simple to use and unobtrusive as it can possibly be. The physical device simply has one switch which can either be set to "On" or "Off" (see Figure 7), after switching the router on it can then be dropped into a backpack and doesn't require any further interaction. From a cold start, once the router is switched on it automatically boots up all of its appropriate system resources and then starts to automatically configure its networking interfaces. Once all hardware configurations are completed the backpack router then initialises our MANEMO protocol (i.e. UMA) and its intelligent Handover Manager software, which immediately starts scanning the surrounding area for appropriate external connections to the Internet. This handover software then continues to run autonomously for the duration of an operation, constantly updating the router's understanding of its surrounding wireless networking environment and making handover decisions as and when it is necessary, as explained in Section 3.2.2.

It is unlikely that the boot time of the backpack router would be of that significant importance to a student/researcher undertaking an outdoors academic study (as the router could easily be started in a vehicle on the way to the field). However, in our effort to thoroughly test every aspect of the portable WLAN kit we wanted to determine the overall time it takes for the backpack router to complete its boot phase, configure its interfaces and be fully operational. For this reason, we developed a simple application that recorded the router's system time at the moment data is able to be successfully transmitted to the Internet. By configuring the router to reset its system clock and therefore begin its start up phase with a system time of zero, we were then able to obtain an accurate boot up time (full OS load and initial hardware configuration), which on average took 26 seconds to complete. At this point the router is ready to start trying to establish a global connection, then the MANEMO protocol and the handover software's start up process were seen to add a further 10 seconds to this value.

After starting up the router and placing it into a backpack, the next important in-field considerations become its resilience to the environment conditions it will encounter. For this purpose the device needs to be fully water resistant and also be able to resist shocks and vibrations. Our backpack router hardware is contained inside a water resistant plastic enclosure that ordinarily would be sufficiently weatherproof, apart from our current switch mechanism. At present we use a metal power switch mechanism that protrudes from the enclosure and could therefore facilitate water to enter. In future iterations of the enclosure we will attempt to solve this problem by have incorporating a completely seamless, waterproof method of switching the router on and off. The backpack router's shock and vibration resistance is good mainly because there are no moving parts used anywhere in its design. This ensures that even persistent vibrations and knocks will not affect the operation of the routers main board and interfaces, however the main concern in this respect is the stability of the internal cabling and fixings. As the router we currently use is still in the prototype stage the cabling and fixings we use are unspecialised, off the shelf computer components. In order to properly fulfill this requirement however we would probably need to use more robust, better secured cabling and stronger internal fixings.

4.2 Battery Lifetime and Software Reliability Testing

Once operational, the router in the portable WLAN kit must continue to operate autonomously for as long as possible. The operational time of the backpack router is therefore inextricably linked to the lifetime of its internal battery and also to the reliability of the software running on the router. To test the battery life of the router we produced a simple application that constantly transmits traffic over each of the router's wireless interfaces for as long as it can. The application was started at the end of the boot phase and recorded the exact time that every packet was transmitted until the point it powered down. On average the current battery we use gave us 3hrs 30mins operating time under these strenuous circumstances. This might be long enough to support some short outdoor field studies and is also perfectly suitable for performing academic demonstrations and trials outdoors, but for prolonged studies this would not be long enough. In addition to the operational time, the time it takes to then recharge the Li-ion batteries was also recorded to take an average of 3hrs 30mins. The battery that we currently use is again only a non-specialist, inexpensive, off-the-shelf

product. If the backpack router were to be taken beyond the prototype stage then this power solution would be given further consideration.

In addition to determining the operating time of the backpack routers, we also tested the reliability of the MANEMO protocol that runs on the routers by transmitting prolonged data streams and recording whether the data was lost or temporarily broken at any point. In each of the tests we performed, with varying different MANEMO network topologies the data stream was seen to continue unbroken for over 48hrs. These tests were performed with the Handover Manager running on the background and triggering handovers according to changes in the connectivity options that the portable WLAN kit was discovering. This 48 hours of unbroken data transmission is sufficiently long enough to support any possible academic study (and more likely, any possible battery technology we can obtain).

4.3 Effective Range Testing

The backpack router can be considered as both a node in the wider mobile network and also as a hub to which individual devices connect. In an academic outdoor field study scenario this equates to the backpack router allowing persons' laptops, streaming webcams, PDA devices, GPS devices and others to connect directly to it, and at the same time being able to connect to other backpack routers carried by other people within range. Since the backpack routers interconnect with each other in order to expand the reach of the mobile network effectively when it is projected onto an outdoor area usually with a rough physical morphology, a fundamental consideration is the wireless range that each individual router can add to the network. The more backpack routers that can be deployed in a field the better, as each one will further proliferate the level of network connectivity available at any given time. However, it is important to note that since coverage is extended in this efficient way by allowing routers to connect back to back to each other, this may arise situations where there is no need for a person of each team (e.g. in the scenario discussed in Section 0) to carry his "own" backpack router. In this case, the backpack routers deployed will provide connectivity to the individual devices carried by the members of a team and at the same time, it may also provide connectivity to devices of members of another team in the vicinity. For these reasons, it is important to determine both the range capabilities for individual devices connecting to a backpack router and for backpack routers connecting to other backpack routers.

4.3.1 Handheld Device to Backpack Router Range Testing

Measuring the capability of an individual device to remain connected to a backpack router's Wi-Fi Access Point effectively indicates the range of coverage of a Mobile Network provided by a backpack router. To test this capability we connected Windows Mobile Smart Phones (HP iPaqs & HTC Touch Cruises) to the backpack router and recorded the distances that could be roamed before the connection began to break up. To allow us to gather accurate measurements we developed a simple application that recorded a GPS coordinate log of all the area covered whilst the handheld device

was able to remain connected the backpack router and also, log exactly when and where that coverage was lost. In Figure 12 we present some of the testing we did in this area (illustrated in the familiar Google Maps interface, which was chosen to provide us with accurate distances between waypoints). What Figure 12 shows is the ability for a handheld device to remain connected to a backpack router at up to over 320 metres away from the backpack router. It is also important to point out that in this specific test illustrated there was no clear line of sight either, as there are significantly tall buildings present in this area pictured (which were not present when the satellite image of Figure 12 was taken). Overall the results in these tests were very encouraging, as we had initially expected the handheld device to only be able to transmit to the backpack router over much smaller ranges because they are relatively low power devices.

Router Coverage Test

-  [Starting Point](#)
+54° 0' 21.59", -2° 47' 1.49"
-  [PDA lost coverage](#)
+54° 0' 31.53", -2° 46' 56.73"
-  [Distance in straight line](#)
Distance in straight line is approximately 1050 feet that



Figure 12 : Range Tests between Backpacks and Individual Device

4.3.2 Backpack Router to Backpack Router Range Testing

In addition to testing the range of the Mobile Network coverage projected around an individual backpack router, it is also important to understand their range capabilities when interconnecting to other backpack routers to form the on-field wireless network infrastructure. In this case the routers connect to each other using their onboard Wi-Fi interfaces through a 5dBi omni directional antenna. Figure 13 again shows an image reconstruction of the effective Wi-Fi coverage test range, but this time for the backpack router to backpack router connection. On average we have been able to establish communication between two backpack routers at up to 400 metres with near line of sight. This level of coverage, combined with the additional range achievable by handheld devices and the proliferation of network coverage that interconnecting the Backpack routers can provide is

considered very positive overall. With the MANEMO approach and these levels of effective range, large areas could be provided with high throughput wireless network infrastructure.

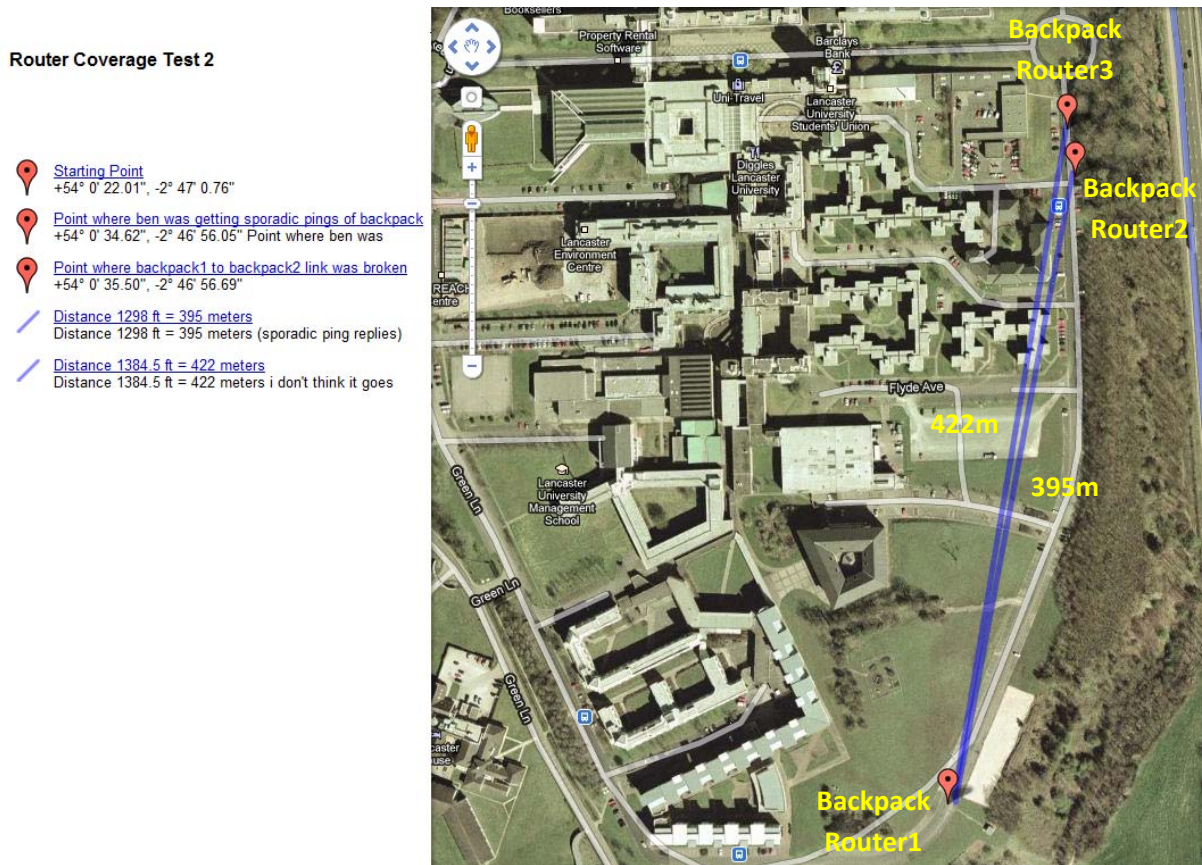










Figure 13 : Range Tests between Backpack Routers

4.3.3 Dense Woodland Range Testing

As well as straight forward, line-of-sight and near line-of-sight testing, we also carried out tests in densely wooded areas. It is obviously of importance that for any solution that is designed to operate in an outdoor field, and possibly an area with harsh morphology (such as mountains, cliffs or dense woodland), tests should be performed over this type of terrain. For this reason, we performed various range tests in dense woodland on campus at Lancaster University. During these tests, we witnessed that the range of the backpack routers is reduced to a certain degree (as it was expected) but overall we were again very impressed with the actual results we achieved. In our tests we observed an average connection distance between Backpack routers of around 170 metres and an average connection distance between the handheld devices and the Backpack routers of around 100 metres. An example test configuration is shown here in Figure 14, in this area tree density was such that people become no longer visible after only around 20 – 30 metres and yet whilst out of visible range, communication could still continue over our networking infrastructure. In addition to the individual range of a backpack router, this particular test area very succinctly highlighted the

strengths of the connectivity chaining approach of MANEMO. In this area the forest very steeply drops away (this is the point at which the first backpack router would start to go out of range. However, since one backpack router (depicted as Backpack Router 2 in Figure 14) remained at the top of this land feature it meant that another Backpack router (depicted as Backpack Router 4) and thus its connected devices, could continue to communicate back to the Backpack router 1 at the starting point, at the most southern point of the woodland. In particular, in this test we also carried 2-way Motorola personal radios for comparison and whilst the 2-Way radio signal broke up, the MANEMO connection stayed in place, because of its ability to forward data through the intermediary Backpack router.

Router Coverage Test 3 (dense foliage testing)

-  [Starting point - Ben with Backpack 1](#)
+54° 0' 27.43", -2° 46' 55.41"
-  [Martin acting as Relay point with Backpack 2](#)
+54° 0' 33.31", -2° 46' 55.60"
-  [PDA lost connection with backpack 2](#)
+54° 0' 36.41", -2° 46' 54.36"
-  [Lost B2-B4 \(router to router\) link](#)
+54° 0' 38.29", -2° 46' 54.51"
-  [Backpack1 to Backpack 2 Link - Distance 600 ft = 183](#)
Distance 600 ft = 183 metres
-  [Backpack 2 to Backpack 4 link : Distance 513 ft = 156](#)
Distance 513 ft = 156 meters Notice though that there is
-  [PDA to Backpack 2 link = Distance 325 ft = 99 meters](#)
Distance 325 ft = 99 meters Quite fair for a pda in
-  [Distance between a pda and an endpoint being](#)
Distance covered with one relay: 919 feet = 280 meters

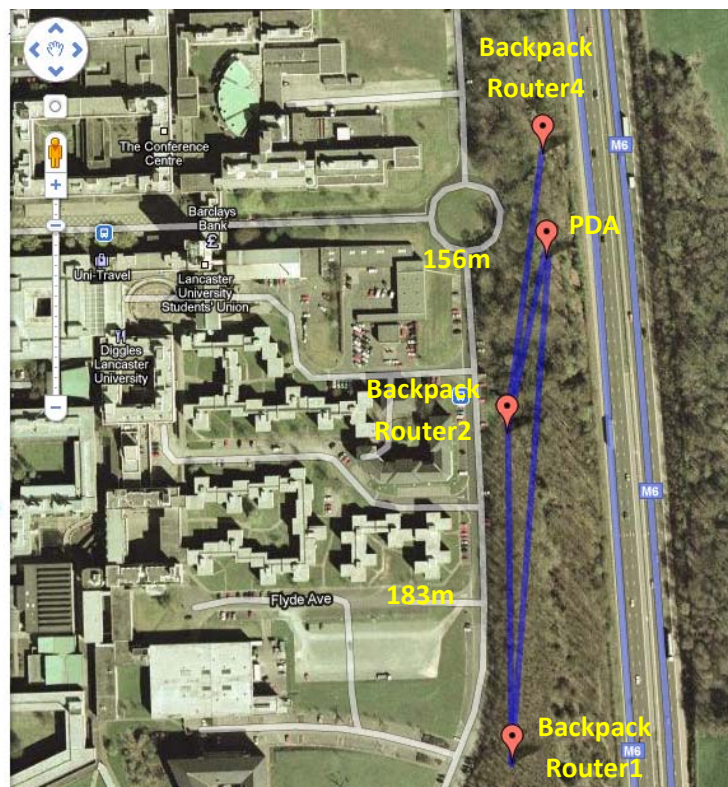


Figure 14 : Range Tests between Backpack Routers in Dense Woodland

4.4 Software Testing

In addition to all the previous tests that we have undertaken to evaluate the design decisions and characteristics of our portable WLAN solution, its software should also be thoroughly tested. Undertaking software tests is very important, especially because we have implemented ourselves the software that runs on the backpack router, in an effort to enrich its functionality and make its operation much more efficient. UMA and Handover Manager tests are reported in the following subsections.

4.4.1 UMA Testing

Section 3.2.1 described that in order to support communication in a mobile network context without losing efficient local communication, we have designed an innovative protocol suite dubbed UMA which runs on our portable WLAN solution. Thoroughly testing all the mobility scenarios that can arise with UMA while it supports mobile end devices is essential for the runtime operation of our portable Wireless LAN kit. For this reason we have performed various tests on UMA, which have been reported in our lengthy JANET deliverable report “The progression from IPv6 to MANEMO” of the Mobile IP Trial project [5] and thus reader is referred to that document for full testing discussion, result analysis and evaluation of UMA. Overall UMA is in a very stable state and can support efficiently complex networking scenarios that can arise due to the mobility of the MR or the end devices.

4.4.2 Handover Manager Testing

Section 3.2.2 described that the router in our portable WLAN kit has to be able to operate autonomously and be able to find the best available connection to the Internet. For this reason, we have developed the Handover Manager software that runs complimentary to the UMA protocol, in order to record the characteristics of all the backhaul options presented to the router at each moment and establish a connection via the best suited option amongst them.

To determine the capabilities of our approach we need a number of criteria that would help us identify the overall performance and responsiveness of the Handover Manager. Those criteria are as follows:

- Length of time taken to establish full initial connectivity map.
- Length of time taken to recognize a change in the existing connectivity map.
 - Change to Wi-Fi access network availability.
 - Change to Cellular Network availability.
 - Change to MANET Gateway availability.
- Length of time taken to recognise a lost connection.
 - Loss of connection via Wi-Fi access network.
 - Loss of connection via Cellular Network.
 - Loss of connection via MANET Gateway.

To record the length of time taken for the Handover Manager to establish information about its surrounding network environment and see how well it performs running on our portable WLAN kit, we began by producing a testbed which represented a typical networking landscape that a Mobile Router could be presented with in an outdoors study. Illustrated in Figure 15, the setup comprised of 4 Wi-Fi access points (each connected to different IPv6 subnets of the Lancaster University network), 1 UMTS connection (provided by the UK cellular network operator O2) and a MANET consisting of 3 UMA enabled MRs (2 of which were acting as Gateways), representing essentially other backpack routers in the vicinity. From the moment it was activated, we then recorded the length of time the

Handover Manager took to establish one complete connectivity map detailing all of the relevant information about each of the different possible access networks.

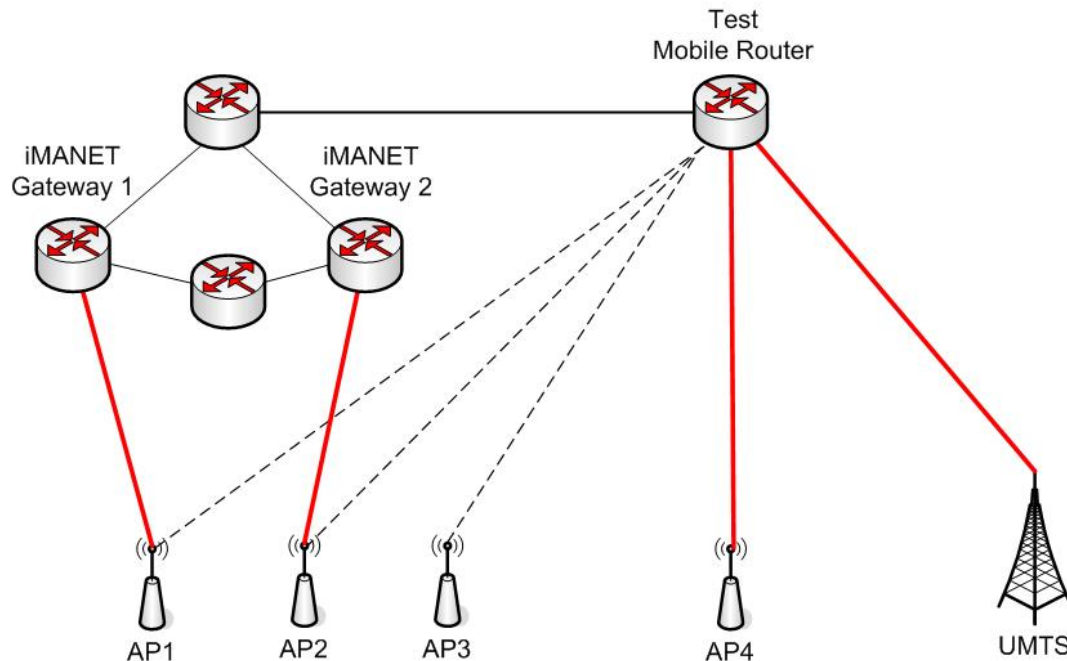


Figure 15 : Handover Manager Testbed Configuration

Once the Handover Manager had established its connectivity map and begun periodically updating its information, we analysed its responsiveness to alterations in the surrounding environment by then subsequently shutting down network infrastructure (and in the case of the cellular connection, reducing the 3G modem's signal quality). For this phase of testing the main connection to the Internet was established via AP4 which remained untouched and always available. This in turn meant that all changes to other networks were peripheral to the main Internet connection and would not therefore cause the MR to handover at anytime, but instead would only affect the potential ordering of networks in the Handover Manager's prioritised list of connection alternatives. To record the responsiveness to changes in the Wi-Fi availability we shut down AP1 and AP2 simultaneously, this ultimately left only AP3 as a viable alternative and therefore we recorded the point from when the APs were shutdown to the point at which AP3 became the highest ranked (and only available Wi-Fi connection alternative). To test the Handover Manager's responsiveness to change on the cellular interface we chose to manipulate the connection by reducing the modem's received signal strength. We did this by placing the modem into a Faraday cage. Using this approach was not enough to remove all trace of signal quality but it was enough to dramatically reduce the reported signal strength and subsequently disrupted the network layer data connection. For the test of responsiveness to change in the MANET network conditions we simply forced MANET to stop advertising it was a Gateway in its HNA messages, as this is what would happen in a real scenario if a MANET Gateway lost its own direct connection to the Internet.

After performing the tests to measure the responsiveness of the Handover Manager to changes in the surrounding network environment we also wanted to see how quickly it responded to losing its main point of connection to the Internet (and therefore subsequently utilising the best possible alternative connection available at that time). For these tests Wi-Fi AP1, AP2 and AP3 remained

permanently deactivated and AP4 was only activated for the first test where the Wi-Fi connection was established and then lost. This was to prevent the Handover Manager from immediately preferring the other Wi-Fi APs over the cellular or MANET Gateway connection as it is designed to do. This meant that for each of the three connection types tested we first setup the main connection to the Internet via the appropriate network and then upon dropping the connection a subsequent handover was performed via the cellular network (except when we tested the loss of the cellular network connection, in which case a handover was performed via the MANET as no Wi-Fi AP was available).

Finally, for each test performed we set the rate at which each monitoring process performed its sampling to one of four settings (0.5 seconds, 2 Seconds, 5 Seconds and 10 Seconds). All of the separate individual scanning and monitoring processes that the Handover Manager performs are carried out periodically, and therefore it is obvious that the frequency that these processes are carried out will have a significant effect on its responsiveness. Setting the interval between the time each process is run to be relatively high (e.g. 10 seconds) will result in a lot of dead time where the Handover Manager will be oblivious to potentially large scale changes to the surrounding network connectivity options. However, setting the sampling rates to be extremely low (e.g 0.01 seconds) will ultimately utilise more power and CPU resources.

The results from our lab based testing are presented in Table 3. One of the most obvious trends we observed and that is evident in our results was the obvious significance of the periodic interval utilised by the monitoring processes. However, the length of the interval period did not have any effect on the first set of results because the Handover Manager immediately starts its monitoring processes when it is activated in order to populate its network connectivity map as quickly as possible. Once completed, the interval period is then only adhered to as the monitoring processes begin to update the network map information with the changing status of access networks around them. One significant factor that we observed to have added to the time the Handover Manager took to complete its tasks or respond to a change was the network layer probing it performs and the overhead that introduces. This was evident to us during testing because our output data would show that all of the signal strength scans (of both the directly connect Wi-Fi AP and cellular connection and the peripheral Wi-Fi APs) were completed relatively quickly (depending on the interval rate). However, the subsequent information gathered from determining the latency experienced at the network layer would often arrive significantly later. This is mainly because of the number of processes that must complete beforehand in order for the network layer information to be gathered. Specifically the Handover Manager must wait firstly for the connection with the appropriate network to be established, then once in place it must then wait for the IPv6 Neighbour Discovery process to complete (namely a Router Advertisement / Neighbour Advertisement transaction must take place). This then allows the Handover Manager to ascertain the IPv6 Link Local address of the network access router and finally an ICMP echo request can be sent.

Once the Handover Manager has established its connections and built its initial network connectivity map these network layer delays are no longer a problem because the appropriate addresses have been established and recorded. In the tests measuring the Handover Manager's responsiveness to change in the surrounding network environment, the deactivation of two of the Wi-Fi APs was quickly detected because the AP signal strength scanning process is very fast. With the MANET connection, the loss of a Gateway causes UMA to proactively alert the Handover Manager,

whilst this means that the issues imposed by the sampling interval do not affect this test, the responsiveness is still somewhat sluggish because OLSR must first timeout the Gateway to ensure it has definitely stopped transmitting HNA messages, this process in itself was observed to take over 3 seconds.

Table 3 : HANDOVER MANAGER TESTING RESULTS							
Interval Period	Establish Full Connectivity Map	Recognition of Change in Connectivity Map			Recognition of Change in Connection State		
		Wi-Fi	Cellular	MANET	Wi-Fi	Cellular	MANET
0.5 s	5.4 s	0.6 s	1.9 s	3.3 s	1.5 s	2.9 s	4.1 s
2.0 s	5.8 s	1.0 s	2.3 s	3.4 s	2.8 s	4.9 s	4.2 s
5.0 s	5.7 s	2.8 s	4.1 s	3.3 s	4.4 s	6.7 s	3.9 s
10.0 s	5.5 s	5.5 s	5.9 s	3.2 s	6.7 s	8.3 s	4.4 s

The Handover Manager's ability to detect lost connections is of particular importance since the sooner a completely unusable connection is detected the sooner a usable alternative can be supplied. With the Handover Manager a lot of emphasis is placed on a dramatic loss in signal strength, or the network layer connectivity being reported as lost when detecting connection losses. In the first tests where the Wi-Fi and cellular connection were lost the handover was triggered relatively quickly because the loss of the network was detected from the immediate loss of signal strength reported by the interface (although the reaction with the cellular link was a little more sluggish because our method of dropping the signal strength was not as definitive as deactivating the Wi-Fi AP). For the MANET Gateway, the bottleneck is again the time taken by OLSR to determine that the Gateway is no longer present. In this case the MR waits for a set period of time (i.e. this is another potentially configurable interval value) after it received its last advertisement from an MANET Gateway before it decides that the Gateway is no longer present. This process could potentially be speeded up by forcing the Gateway to proactively advertise the fact that it is no longer a Gateway. This approach would make sense because Gateways can often still be connected to the same MANET but they lose their own direct connection to the Internet. In which case they must no longer advertise that they are a Gateway, but at the same situation should not necessarily be treated in the same that a MANET node disconnection is (as it is treated now).

One important advantage that the use of the Handover Manager provides is the ability to benefit from the use of "Make-before-break" handovers in Vertical Handover situations. This is because the Handover Manager is able to establish a connection simultaneously with a different heterogeneous access network (getting advantage of the multiple network interfaces the backpack router has) to the one that is currently utilized as the main connection to the Internet and then crucially the Handover Manager can step in at any moment and force UMA to perform a Binding Update over any interface it specifies. This ability means that the large overhead attributed to establishing connections at Layer 2 can be avoided in some circumstances. For instance if a MR has a connection to the Internet via its cellular interface and a Wi-Fi network subsequently moves into range, the Handover Manager can establish a connection to the Wi-Fi network and first check it for Network Layer connectivity before triggering UMA to switch over its connection to the Internet. By using this approach the Handover Manager ensures that the only delay in setting up a session is imposed by

the time it takes to communicate with a MR's HA over the Internet. This means that in low latency networks the whole registration process can be achieved in under 0.5 seconds.

5 Conclusion

The design of our portable WLAN kit is aimed to provide connectivity for mobile devices for outdoor academic studies and support the connectivity requirements of devices individuals may carry. The main objective of the kit is to provide both local and global Internet connectivity to all the devices that students/researchers use as part of a scenario that takes place in an environment with usually harsh terrain characteristics. The portable WLAN kit is able to find out and utilize the best-suited backhaul Internet connection and share this connection with all the devices around it despite them experiencing mobility. Our solution not only provides an 802.11b/g wireless network for devices to connect to, but also supports wireless sensor networking with the use of an 802.15.4 sensor gateway that collects readings from sensor devices that are in its vicinity. Furthermore, our portable WLAN kit has the ability to form an on-field MANET network with other portable WLAN kits in its vicinity to make local communication much more efficient and to further extend and proliferate connectivity if required. In addition, our prototype has the ability to establish its own 3G connection to the global Internet if no other backhaul option is available. Running our UMA protocol suite on the portable WLAN router brings additional advantages to this scenario as mobile devices experience uninterrupted and seamless connectivity no matter where the point of attachment of the mobile network is. In addition, UMA brings to end-user mobile devices efficient local communication by using a MANET protocol (OLSR) to optimize backpack router to backpack router communication, without having to run any additional protocols on the end devices.

We have performed extensive tests to determine the portable WLAN prototype's suitability for use in outdoors studies and, in conclusion, believe that it is suitable for use for a few hour long academic studies (limited just by the run time of our batteries). It has to be noted that further work is needed on the hardware components of our prototype, to realise a product ready for full deployment. In particular, for further revisions of the hardware design we will specifically aim to reduce the footprint of the device, to improve the waterproofing in general and to make the internal cabling and fixings neater and more robust.

Reducing the size of the router board in particular and the whole WLAN kit in general, will make it more suitable for use in the backpacks that individuals use on a study. In its current form the backpack router is housed in a weatherproof thermoplastic container that is 190mm long by 140mm wide by 70mm deep. To better suit the requirements of an outdoor study (i.e. fit in a backpack more easily) the footprint of the backpack router should ideally be reduced. As the footprint of the main board in the current prototype is almost 140mm wide, the width of the housing would not be changeable, however both the length and the depth of the housing could be greatly reduced through the use of a better designed battery and cabling set up within the housing. The use of a flat Li-ion battery with a similar footprint to the main board, layered on top of it would allow us to drastically reduce the length of the housing (this extra space houses the rectangular battery currently used). Layering a new battery in this manner would then add to the depth of the device, but the current unused space in this dimension is significant and the space could be used even more efficiently with a better cabling solution. Improving the cabling and fixings will also make the router more resistant to long term, sustained vibration and shock. It is important to note that we have managed to keep the weight of our prototype in remarkably low levels (only 1.2kg) which is very important as individuals would have to carry the kit in a backpack for quite a few hours. Finally,

there is a need for further waterproofing which stems from an unsuitable switch design that we chose to incorporate into our enclosure early on in our research. For this particular item, we would need to go back and reconsider our switch options in general and take more consideration of the intricate properties of the material the switch itself is made of and not just the way the switch is installed. Overall, we are happy with this outcome, especially since the provisioning of hardware for continuous use in these environments is an extremely specialised field in which we have little previous experience.

In addition to the physical attributes of the backpack router itself, we found the effective wireless communication range, that was achievable, to be better than expected, and therefore very positive overall. Wireless signal propagation is again a very specialised subject and so far have only used simple, generic 5Dbi omni-directional antennas with the backpack router. These are inexpensive, off-the-shelf antennas that are used in everyday indoor wireless scenarios and we have found them to perform much better than originally expected. We believe that through the use of more specialised and higher quality equipment, hopefully, we will be able to increase the effective wireless communication range of the backpack routers to be significantly better than the already satisfactory levels we are currently achieving. This is another area where potentially we expect to be able to make further gains in the future.

It is very important to emphasize that the strength of our portable WLAN kit does not only lie on our delicate hardware design. We have paid particular attention to the software that the Routerstation board inside the portable WLAN kit runs to satisfy the networking requirements of our scenario. Not only is the operating system that the router runs an open source specialized embedded Linux based distribution, ideal for our purpose, but we have also implemented specific networking protocols to further support the mobility of the kit and the networking requirements of the devices around it. Our MANEMO based protocol suite (i.e. UMA) incorporates the best of two research areas, network mobility and ad-hoc networking, and brings a unified solution that substantially benefits our mobile scenario. With UMA, end-devices enjoy seamless and uninterrupted global connectivity, no matter where the backpack router is getting connectivity from, but they also get efficient local communication with mobile devices in their vicinity. Complementary to UMA, our Handover Manager software is able to fully discover all the backhaul connectivity options and build a prioritized list of these options based on certain network criteria. This enables the portable WLAN kit to use the most efficient backhaul option each time, by taking into account characteristics such as signal strength, network connectivity or delay. Overall, we feel that the innovative software components of our portable WLAN prototype complement successfully its delicate hardware design and increase the strengths of our solution.

In general, one of the major benefits of developing a solution for the difficult environments that an outdoor study may take place in, is that our solution is applicable to many other applications and scenarios. For example, our portable WLAN kit could be used in mountain rescue missions where it can support the communication needs of the rescuers' personal area network (comprised of possibly a camera, a PDA, biomedical sensors etc) or it could benefit less taxing scenarios. For example everyday emergency services scenarios where the router can be expected to be housed in a relatively stable vehicle or a backpack that is infrequently exposed to heavy rain or persistent vibration, then our solution can already be seen to be potentially suitable. This means that by initially setting out to solve the clearly scoped mobile networking requirements of a specific and

challenging scenario, as an outdoor academic study is, we have simultaneously developed a solution that could be suitable for use in many other important and demanding use case scenarios with similar design and networking requirements.

References

- [1] **Portable WLAN Trial JANET Programme** : <http://www.ja.net/development/portablewlan.html>
- [2] **Ubiquiti Routerstation homepage** : <http://www.ubnt.com/products/rs.php>
- [3] R. Wakikawa, P. Thubert, T. Boot, J. Bound and B. McCarthy. “**Problem Statement and Requirements for MANEMO**”. Internet Draft (Work In Progress), July 2007.
- [4] **Cumbria & Lancashire Education Online** : http://www.cleo.net.uk/index.php?category_id=113
- [5] Lancaster University. “**The Progression from Mobile IPv6 to MANEMO**”. Investigations in Mobile IP under the JANET Network Access Programme.
<http://www.ja.net/documents/development/network-access/mobile-ip/investigations/C4-the-progression-from-ipv6-to-manemo.pdf>
- [6] **OpenWrt**, Linux distribution for embedded devices. <http://openwrt.org/>
- [7] **OpenWrt Wiki** : <http://wiki.openwrt.org/>
- [8] **OpenWrt Configuration Guide** : <http://kamikaze.openwrt.org/docs/openwrt.html>
- [9] **Network Mobility Research Group’s Webpage**. OpenWrt – Installation Instructions : <http://uma-wiki.network-mobility.org/index.php5?title=OpenWRT - Installation Instructions>
- [10] **Network Mobility Research Group’s Webpage**. OpenWrt – Routerstation Kernel Settings : <http://uma-wiki.network-mobility.org/index.php5?title=Ubiquiti Router Station Kernel Settings>
- [11] **Network Mobility Research Group’s Webpage**. OpenWrt – Configuration Instructions : <http://uma-wiki.network-mobility.org/index.php5?title=OpenWRT - Configuration Instructions>
- [12] **Ubiquiti Routerstation Schematics** : http://www.ubnt.com/downloads/ROUTER_STATION_DWG.pdf
- [13] D. Johnson, C. Perkins and J. Arkko. “**Mobility Support in IPv6**”. RFC 3775, June 2004.
- [14] V. Devarapalli, R. Wakikawa, A. Petrescu and P. Thubert. “**Network Mobility (NEMO) Basic Support Protocol**”. RFC 3963, January 2005.
- [15] **Enix Energies Battery** : <http://onecall.farnell.com/enix-energies/800055/battery-li-ion-15v-2-2ah-pk/dp/1290997>
- [16] **Ubiquiti XtremeRange2 Mini-PCI, Wireless Adapter** : <http://www.microcom.us/xr2.html>
- [17] **IP56 Rated, Plain Sided Enclosure** : http://onecall.farnell.com/_/ol20023/ip65-190x140x70mm-plain-sided-box/dp/EN81301
- [18] **2.4 GHz, 5dBi gain SMA Knuckle Antenna** : http://www.siretta.co.uk/search_box.php?mcatid=219

- [19] **O2 MF100, Qualcomm MSM 6280 USB Modem** : http://shop.o2.co.uk/promo/o2mobilebroadband/tab/Pay_and_Go
- [20] **TelosB (TPR2400CA) Sensor Mote Datasheet** : http://www.willow.co.uk/TelosB_Datasheet.pdf
- [21] **Network Mobility Research Group's Webpage**. OpenWrt – Routerstation Board Specification : http://uma-wiki.network-mobility.org/index.php5?title=%3D%3D%3D_Ubiquiti_Routerstation_%3D%3D%3D
- [22] **Optimized Link State Routing Daemon (OLSRD)**. <http://www.olsr.org/>.
- [23] Linux IPv6 **Router Advertisement Daemon (RADVD)**. <http://www.litech.org/radvd/>.
- [24] **OpenVPN** <http://openvpn.net/>
- [25] T. Ernst. “**Network Mobility Support in IPv6**”. PhD Thesis, Universite Joseph Fourier, Grenoble, France, September 2008.
- [26] T. Clausen and P. Jacquet. “**Optimized Link State Routing Protocol (OLSR)**”. IETF Request For Comments 3626, October 2003.
- [27] Ben McCarthy, C. Edwards and M. Dunmore. “**Using NEMO to Support the Global Reachability of MANET Nodes**”. In Proceedings of the 28th Conference on Computer Communications, IEEE INFOCOM 2009, April 19 -25, Rio de Janeiro, Brazil.
- [28] Ben McCarthy, Christopher Edwards and Matthew Jakeman. “**Supporting Nested NEMO Networks with the Unified MANEMO Architecture**”. In Proceedings of the 34th IEEE Conference on Local Computer Networks (LCN 2009), Zurich, 20-23 October 2009.
- [29] McCarthy, Ben and Georgopoulos, Panagiotis and Edwards, Christopher. “**Intelligent Autonomous Handover in iMANETs**”. In: Second ACM/SIGMOBILE International Workshop on Mobile Opportunistic Networking (MobiOpp 2010), February 22-23, 2010, Pisa, Italy.
- [30] The **National Education Network (NEN)**. <http://www.nen.gov.uk/>