Efficient Mobility and Multihoming Support for Mountain Rescue

Ibrahim S. Alsukayti
School of Computing and Communication
Lancaster University
Lancaster, United Kingdom
i.alsukayti@lancaster.ac.uk

Christopher Edwards
School of Computing and Communication
Lancaster University
Lancaster, United Kingdom
c.edwards@lancaster.ac.uk

***Abstract*— Introducing an IP-based communication system into the mountain rescue domain would enable carrying out search and rescue missions in an effective way. With efficient mobility and multihoming support, a Mountain Rescue Team would be able to establish more effective and reliable Internet communication. In this paper, we present the Multihomed Mobile Network Architecture (MMNA), a comprehensive multihomed mobility solution for complex nested mobility scenarios. It provides a multihoming management mechanism for gateway discovery and selection, on top of an efficient multihomed mobility model integrating different mobility and multihoming protocols. The design of the MMNA solution is first presented. We then describe how the MMNA was experimentally implemented and evaluated in a testbed setup to examine its effectiveness and feasibility considering a use case example of a mountain rescue scenario. The results highlight the practicality and advantages of deploying the MMNA into such a critical real-world scenario.**

Keywords— NEMO; MANEMO; Mobility; Multihoming; Mountain Rescue;

I. INTRODUCTION

Enabling dynamic communication in a search and rescue domain is of critical importance. Instant and permanent access to information is vital, particularly in life-saving scenarios. In mountain rescue, effective and reliable communication between in-field parties and the mission controller at the respective headquarters supports making informed decisions. However, providing a data networking solution in this domain requires the consideration of different demanding requirements in such mobile and dynamic environments. These include the need for efficient support of IP mobility to ensure network reachability and session continuity while the members of search groups are on the move. When Personal Area Networks and Vehicular Area Networks are established in such scenarios, adequate mobility support can be provided by basic mobility solutions. However, the potential for these mobile networks to interconnect and extend Internet access of a designated gateway to remote search areas, leads to the formation of more complex mobile network topologies. In order to keep network disruption at a minimum in these sorts of scenarios, it is important to ensure optimised mobility support. Moreover, there is high potential in such scenarios for a number of Internet access options to emerge within a certain search location and provide diverse connectivity to the Internet. For in-field rescue workers, enabling the connectivity to, and allowing the sharing of, multiple access options over their Personal Area Mobile Routers would enhance the performance of their communication and have positive impact on their missions. Therefore, optimised mobility support with efficient multihoming management in such complex scenarios becomes important. Homogeneous and heterogeneous connectivity needs to be considered in these sorts of scenarios to increase resource utilisation in addition to allowing the convergence of multiple topologies. It is also important in this context to provide efficient multihoming management enabling informed and policy-based decisions to be made when having multiple access options to the Internet. Consideration should also be given to enable efficient use of available resources and allow concurrent access to multiple gateways within one topology. For a symmetric and consistent view, traffic forwarding should be ensured for both inbound and outbound communication. Per-flow access management would enable traffic engineering at a fine-grained granularity. In this paper, we address these requirements for efficient multihomed mobility support in the context of complex scenarios. Although the focus here is on mountain rescue, we designed a solution that can fit other applications such as vehicular-based communications. We present the Multihomed Mobile Network Architecture (MMNA), a comprehensive multihomed mobility solution, and detail a thorough evaluation in the context of mountain rescue.

II. BACKGROUND

A. Network Mobility

NEMO Basic Support (NEMO BS) [1] provides a roaming Mobile Network of a group of nodes, referred to as Mobile Network Nodes (MNNs), with mobility support managed by its Mobile Router (MR). Once the MR connects and configures a Care-of-Address (CoA), it performs the Binding Update process with its Home Agent (HA). The HA then installs a binding between the CoA, home address, and the Mobile Network Prefix (MNP) of the MR. Upon a successful binding update, a bi-directional tunnel is established between them. The reachability of the Mobile Network is then maintained over the tunnel, transparently to the communication of its MMNs and Correspondent Node (CN).

In NEMO, a remote MR can connect to the mobile subnet of another MR and gain indirect Internet access. However, this requires the remote MR to register and establish a tunnel with its HA over the tunnel of the MR to which it is connecting. The chain can extend resulting in topological structure known as Nested NEMO. In this model, MR communication traverses sub-optimal routes over a multi-tunnel path, resulting in the Nested NEMO problem of Pinball Routing [2].

B. MANET for NEMO (MANEMO)

The concept of MANET for NEMO (MANEMO) is based on combining the properties of the Mobile Adhoc Network (MANET) and NEMO technologies [3]. It defines two different models, the NEMO-Centric MANEMO (NCM) model, addressing the Nested mobility issues, and the MANET-Centric MANEMO (MCM) model, addressing mobility support for MANET. An example of a comprehensive MANEMO-based solution is the Unified MANEMO Architecture (UMA) [4].

The NCM model provides a Route Optimisation solution for the Nested NEMO scenario. It is based on enabling a MANET-like routing model within the nested infrastructure to allow only a single tunnelling layer via its gateway-MR. Using the Tree Discovery (TD) protocol, interconnected MRs form a tree-based structure and establish default routes towards the gateway MR. The Network In Node Advertisement (NINA) protocol is also used to exchange routing information over the tree, by each MR advertising its MNP up the tree. The Binding Update process is then performed over the tree infrastructure. Upon a successful home registration, the existing tunnel of the gateway is utilised for the MRs communication. If the gateway and a MR within the tree belong to the same HA, the scenario is called the Aggregated Roaming Scenario. Otherwise, the binding process is performed as a Non-Aggregated Roaming Scenario in which the gateway's HA becomes a Proxy-HA and carries out the MR binding process to establish a tunnel with the Target-HA.

C. Multihomed mobility

NEMO BS and Mobile IPv6 do not have any multihoming support. However, they were extended with the Multiple CoA Registration (MCoA) [5] protocol enabling a multi-interfaced MR to register multiple CoAs and establish multiple tunnels with its HA. Each CoA is assigned a unique Binding Identifier (BID), which is then used to identify the different bindings of the MR. The MCoA protocol enables the maintenance of multiple communication paths over the multiple tunnels without defining how the traffic is forwarded among them.

III. MOUNTAIN RESCUE

A. Mountain Rescue Overview

Search And Rescue (SAR) refers to the process of locating and rescuing people in different types of incidents such as collapsed bridges, cave accidents and natural disasters. a common SAR type is the mountain rescue service mainly focusing on incidents within mountainous terrain. The basic operations in a mountain rescue mission include locating, first aiding and evacuating casualties being in terrain-located incidents. For example, a mission can commence in response to a lost person, fallen climber, or mountain hiking accident.

The mountain rescue service in England and Wales is structured in a number of Mountain Rescue Teams (MRTs) distributed across nine geographical areas [6]. Each of those teams is an autonomous charity run by volunteers and covering a distinct search area. The necessary coordination among the teams within one area is provided by an organisational body that also supports cooperation among different teams, among members of distinct teams, and between teams and other parties such as a police force. The Lake District Search and Mountain Rescue Association (LDSAMRA) [7] is one example that coordinates the mountain rescue service among twelve rescue teams covering the Lake District and Cumbria regions. Each team consists of a number of trained members and a designated leader. Each team would also have all-terrain rescue vehicles and search dogs, and be equipped with specialist mountaineering and medical equipment. If air support is needed, a helicopter can be provided by the Royal Air Force Mountain Rescue. For example, the Cockermouth Mountain Rescue Team [7] has 40 members, one of them is a base controller in charge of monitoring and controlling rescue operations at a Headquarter.

A mountain rescue mission commences in response to a received callout requesting help for locating and rescuing a casualty. Once enough members have responded to the call and become ready to initiate the operation, an initial search and rescue plan is discussed after they are briefed on the incident. The team is then divided into separate search groups, each of which is assigned a leader, and taken to the search location in rescue vehicles. The team controller stays at the Headquarters in order to monitor and control the search and rescue operation in addition to arranging for any necessary support from other parties in cases such as the need for an airlift to the hospital. The communication among the different search and rescue members is vital during the operation and would allow more informed decisions to be made. The controller ideally maintains communication with all the search groups in the field. The search groups can also communicate with each other in addition to direct communication between individual search workers.

B. Use Case Description and Assumptions

In order to evaluate the MMNA solution in a mountain rescue scenario, we developed a use case example around mountain rescue. The focus was on a multi-team operation involving three search groups. Two of the search groups, SG1 and SG2, belong to the same Mountain Rescue Team and each one consists of four rescue workers. The third search group, SG3, came from a different Mountain Rescue Team, supporting the operation with three rescue workers. The search and rescue operation commenced upon a call out for a lost and injured elderly person in a remote mountainous area with the exact location being vaguely known, and moderate access to the area.

The communication among the different in-field parties and the Headquarters was realised over the Internet. In-field parties are interconnected over wireless network infrastructures to form MMNA structures with Internet access over different access technologies. Each of the rescue vehicles and rescue workers are equipped with a MMNA-enabled multi-interfaced Mobile Router. The Mobile Router at each of the vehicles operates as a MMNA Main Gateway with multiple interfaces enabling connectivity to public Wi-Fi hotspots and satellite based Internet access. In addition, it projects a long range 802.11a wireless hotspot to which other Mobile Routers can connect. Each Mobile Router has an 802.11a/b wireless access interface allowing connectivity to the Mobile Router of a rescue vehicle or another rescue worker. It also provides a short range 802.11b wireless hotspot via a portable Access Point to which carried IP devices and other Mobile Routers can connect. Mobile Routers are also fitted with additional cellular access interfaces enabling connectivity to different cellular access technologies.

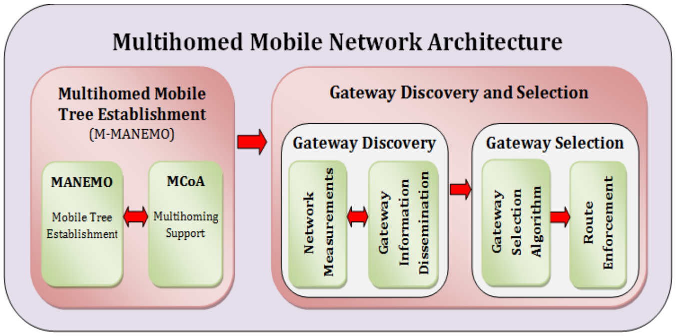


Fig. 1. MMNA Design Overview

Management and control of the mountain rescue operation is based on a number of services integrated into a command and control system. These include location tracking, telemedicine, voice communication, video steaming, and image sharing. Location (GPS coordinates) and biomedical (e.g. body temperature and heart rate) information are periodically collected and transmitted by a GPS device and biomedical sensors connected to the Mobile Router of each member. Medical sensors are also attached to the casualty in order to relay medical information to the medical team. Voice communication is realised using a VoIP system allowing one-to-one and group calls. Additionally, the helmet of each member has a mounted camera enabling a live video stream and sending images of the casualty or the search location

IV. MMNA DESIGN

The Multihomed Mobile Network Architecture (MMNA) is a comprehensive multihoming solution for nested mobility scenarios. It enables the establishment of a multihomed mobile tree of heterogeneous Internet access, and provides an efficient solution for multihoming management. Figure 1 presents an architectural overview of the MMNA design. It shows the two main MMNA processes, namely Multihomed Tree Establishment and Gateway Discovery and Selection. This section briefly describes these main components (for more details see [8]).

A. *Multihomed Mobile Tree Establishment*

This process enables the establishment of a multihomed mobile tree with multiple gateways spanning across the tree. To achieve this, we extended the MANEMO architecture by integrating the MCoA protocol to enable efficient support of nested mobility and multihoming. We called this collection the Multihomed-MANEMO (M-MANEMO) protocol. Adopting MANEMO enables the establishment of an optimised tree-based routing model using the TD and NINA protocols in addition to performing an enhanced home binding process. The MCoA protocol provides the multihoming functionality supporting the emergence of additional gateways within the tree. Figure 2 shows an example of a simple M-MANEMO tree formed by a number of Mobile Routers, with GW1, GW2, and GW3 are the available Gateways providing Internet access via different access technologies. M-MANEMO also enables a gateway to join another tree over an additional egress interface, to become an Alternative Gateway to the combined tree. For efficient tunnel management, each tunnel in a M-MANEMO tree is assigned a unique identifier called a Tunnel ID (TID).

B. *Gateway Discovery*

The process of Gateway Discovery enables the MRs in a M-MANEMO tree to discover and learn the capabilities and performance of the available gateways within the tree. This would enable the nodes to make informed decisions when selecting the optimal gateway to access the Internet. We developed a Gateway Discovery Protocol (GDP) defining how gateway information is conveyed, propagated, and collected within the tree. We also backed this up with the Network Measurement process to enable the collection of IP performance and capabilities metrics describing each Internet access option available within a M-MANEMO tree.

Considering the different requirements that could be imposed by different scenarios, we designed a customisable measurement collection process. It contains a measurement profile enabling the definition of three main parameters to meet the requirements of a particular scenario. The first is the network path over which the measurements are collected. The second is the measurement metrics that need to be collected in order to support the Gateway Selection process. The third enables selecting the measurement mode, *Active* or *Passive*, applicable to a deployment scenario. The next stage is processing the created profile to configure the applicable measurement tools. There are a number of passive and active tools that can be utilised and integrated into the process (Netperf and UDPMon for example). At the final stage, the measurement collection is carried out and repeated according to a configured time interval suited to a given deployment.

Each gateway advertises its capabilities and measurements to other MRs within the M-MANEMO tree. The TD protocol advertisements are extended to carry gateway information over the tree. The base TIO option is amended with a new sub-option, called the Gateway Information Sub-Option (GISO). Gateway attributes such as the Home-of-Address, HA address, and the current depth within the tree are included into the gateway advertisement in addition to the ID of the tunnel being advertised. The advertisement also contains network measurements collected during the network measurement process. The gateway advertisement is then propagated down the tree enabling each gateway to disseminate its information to the sub-tree of MRs branching off its ingress interface. Each MR receiving gateway advertisements collects the disseminated gateway information into a list, called the Gateway Discovery List. Each entry in the list corresponds to an available gateway and is frequently updated with the most up to date information.

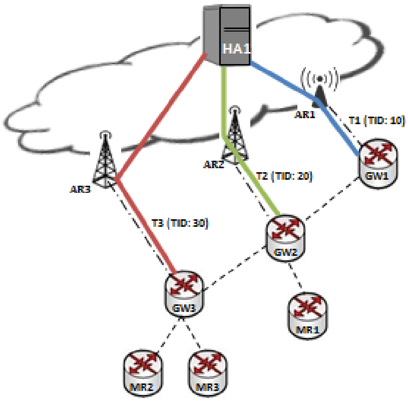


Fig. 2. M-MANEMO tree

C. Gateway Selection

The process of gateway selection enables making a decision according to the selection policies defined for a given MMNA deployment, as well as real-time information being disseminated by the candidate gateways. In order to insure that outbound and inbound traffic of a Mobile Network within a tree is always tunnelled via the selected gateway instead of traversing a default path, this process also contains a route enforcement mechanism.

The gateway selection process is run by all the gateways of a tree and each MR having more than one gateway available. The design of this process is based on the decision-making module which takes two inputs. The first are the weights calculated for the selection criteria. The calculation is based on the importance rate given to each of the criteria according to the applied policy. The second input is the gateway information after being collected from the Gateway Discovery List and then normalised. Once the decision has been made, the selected gateway is provided as an input to the route enforcement process. The gateway selection process could be implemented either as a flow- or network-based selection. Flow-based selection allows finer granular selection where every flow type or set of flows is mapped to a selected gateway. In the case of network-based selection, the granularity level is coarser in that the decision is made for the traffic of a given mobile network. The process can be configured to run at a given time interval or based on specific events (link failure at a gateway, for example).

Additionally, we developed a mechanism whereby route enforcement is realised upon collaborative operations performed at the different M-MANEMO entities. Each gateway installs the necessary filtering and tunnelling rules to intercept and tunnel relevant outbound traffic via its tunnel. The respective HA also installs a tunnelling rule enabling inbound traffic to be tunnelled via the relevant tunnel. Once a MR has made a selection, it notifies its HA of the newly selected gateway. It sends an immediate BU message to its HA after attaching a new mobility option, called the Selected Gateway Information Option (SGIO), to contain the information of the newly selected gateway. Once received, the HA collects the information into its Traffic Forwarding List and installs the necessary filtering rules to intercept and route corresponding inbound traffic via the selected gateway. Upon receiving a successful acknowledgement from the HA, the MR continues the process of enforcing the selection, and applies a marking to the outgoing traffic of its Mobile Network. Given that the gateways and HA associate the tunnelling and filtering rules for each tunnel with its ID, the tunnel ID of the selected gateway is also utilised for packet marking. Each packet generated by the MNNs connecting to the MR is marked with the relevant tunnel ID. In a scenario where a MR selects a gateway belonging to a different HA, the Proxy-HA in this case also performs the role of Proxy-Gateway. Once it receives a BU+SIGO message, the Proxy-HA sends a Proxy BU+SIGO message to the Target-HA containing the ID of their HA-HA tunnel. This indicates to the Target-HA to route the corresponding inbound traffic via the HA-HA tunnel.

V. MMNA IMPLEMENTATION

We experimentally implemented the MMNA solution (using Linux kernel version 3.8.2) and this section provides an overview of the proof-of-concept implementation.

M-MANEMO was developed based on merging two main protocols, MANEMO and MCoA. These protocols have openly available Linux-based implementations on top of the original NEMO implementation. The MANEMO implementation (known as UMA+) was developed at Lancaster University, and the MCoA implementation is available as Linux kernel and userland patches. We extended UMA+ to integrate the different MCoA functionality including BID mobility option processing. It also incorporates other functionality such as TID processing.

In the current implementation, we defined two measurement profiles. The first is set as the default profile indicating the collection of measurements for metrics including bandwidth, delay, and packet loss, using an active mode. Accordingly, the Iperf and UDPMon active tools were incorporated to collect such measurements at a given interval. The profile also includes the collection of gateway uptime that is computed periodically, and access cost that is supplied manually. The second profile enables lightweight measurement to collect network bandwidth and load metrics using a simple passive monitoring tool that was developed based on tcpdump. For both profiles, the measurement is performed at the gateway entity for the tunnelling path between the gateway and HA entities.

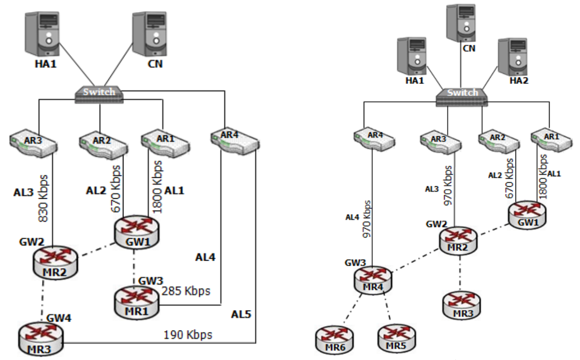
For information dissemination, the Gateway Information Sub-Option (GISO) message was implemented containing attributes such as the HoA of the gateway and its HA's IPv6 address. It also includes the TID of the advertised tunnel. The GISO also indicates the number of hops the recipient is from the advertising gateway (Depth), and hop number to which the advertisement is limited during propagation (Time-To-Live). It also contains metrics such as the Uptime to provide the elapsed time since establishing the advertised tunnel. In addition, the GISO provides measurement information such as throughput, RTT, and packet loss over the advertised tunnel. It also indicates the type of access link over which the tunnel is established.

To experimentally enable gateway selection functionality, we developed a simple selection algorithm. For criteria rating, a numerical scale of [1-5] is adapted to apply the relevant importance to each of the criteria of interest according to a static policy. Calculating the criteria weights based on the rating data was implemented using the Pairwise Comparison method. The criteria are compared against each other to build a comparison matrix in order to calculate the criteria weights based on the calculation of the geometric mean for each one. The normalization of the collected gateway data was implemented based on the min-max normalization method to map the data to values ranging from 0 to 1. Once the gateway data has been normalized and the criteria weights are in place, the decision is made using the Simple Additive Weighting method to select the gateway with the maximum sum.

The implementation of the route enforcement process was based on a number of functional components including packet marking, HA signaling, and tunneling and filtering rules installation. To enable in-line route enforcement for outbound traffic, the main IPv6 header is utilised to mark outgoing packets at the MR entity with the ID of the preferred tunnel. The Traffic Class (TC) field is utilised for packet marking. Since TC was mainly developed for QoS support, it has only local effect across the M-MANEMO tree in this implementation and is reset for each packet leaving the tree. For HA signaling, a selecting MR communicates selection information, such as the preferred tunnel ID and the IPv6 address of the corresponding gateway, into a SGIO that is attached to an immediate BU message. Furthermore, the Linux XFRM framework in conjunction with the Linux IP filtering framework "Netfilter" were adopted for enabling each gateway and HA to install traffic tunneling and filtering rules allowing the new selection to be enforced. A Netfilter rule enables a gateway to intercept IPv6 packets with the TC set to the ID of its tunnel and mark them locally within the kernel to then be matched and tunneled by the XFRM framework according to installed XFRM policies.

VI. EVALUATION

The evaluation of the MMNA solution was based on the mountain rescue use case described in Section III. In this section, we detail the evaluation process and discuss the results.



(a) (b)

Fig. 3. Testbed Setups: (a): Setup-1, (b): Setup-2

A. *Testbed Description*

The evaluation of the MMNA in our use case example was carried out on an experimental testbed. Two different testbed setups, shown in Figure 3, were developed using a collection of Linux desktop PCs (2.9GHz CPU and 6GB RAM), fitted with Atheros Chipset 802.11a/b/g wireless interfaces in addition to two Ethernet interfaces. The PCs are running Linux Ubuntu 12.04 with Linux kernel version 3.8.2. In both of the setups, four of the PCs were configured to run as Access Routers (AR1, AR2, AR3, and AR4), and two machines were configured to operate as a MMNA-enabled HA (HA1) and a Correspondent Node (CN). The second setup has an additional HA (HA2) as shown in Figure 3(b). These entities were interconnected via an Ethernet backbone network using a Netgear network switch. The other PCs were configured to run as MMNA-enabled Gateways and Mobile Routers. They were also configured with Software-based Access Points and RADVD to establish connectivity to each other. The gateways were connected to the ARs over wired Ethernet links configured to emulate connectivity to different access links. In both of the setups, AL1 and AL2 were configured to emulate a Wi-Fi access link (at 1800 Kbps) and a satellite access link (at 670Kbps), respectively. The HSPA cellular connections were emulated over GW2-AR3 and GW3-AR4 links (at 970Kbps). AL4 and AL5 emulated UMTS (at 285 Kbps) and EDGE (at 190Kbps) cellular connectivity respectively. Additionally, the wired infrastructure was configured with a dynamically varying delay (≈ 60ms) in order to emulate the approximate delay of Internet paths.

The communication among the different search parties in our use case was represented using a suite of different applications that were implemented with particular configurations over the testbed. The communications of the location and biomedical information were both implemented as a single text file transfer over a client-server TCP-socket (every 5 seconds). Similarly, the communication of the medical information concerning the casualty condition was implemented as a text file transfer with an interval of a second. For VoIP communication, a Linux version of the Linphone application was installed and configured to make G.711 VoIP calls delivered at a bit rate of 64 kbps over the RTP/UDP protocols. The communication of live video was represented as an adaptive video streaming of pre-recorded and pre-encoded video contents. A basic video streaming implementation of the Dynamic Adaptive Streaming over HTTP (DASH) standard was developed to run over the HTTP/TCP protocols. It was configured to monitor the recently achieved network TCP throughput and accordingly adapt the video streaming bit rate with values ranging from 100 to 4500 kbps. Finally, a TCP application was implemented to realise the sharing of search areas and casualty images with the Headquarters on the testbed (every 5 seconds).

TABLE I. BRIEF DESCRIPTION OF THE EXPERIMENTAL STAGES

Stage	**Event Summary**		**Communication**					**Testbed**	**Duration (Sec)**
			GPS & Sensor	**VoIP**	**Video Streaming**	**Image**	**Other**		
S.1	GW1	Additional access Link	ALL	MR2	MR1	-	-	a	120
S.2	MR2	Internet access via HSPA link	ALL	MR1 MR2	MR2	MR3	-	a	120
S.3	MR1	Internet access via UMTS link	ALL	ALL	MR3	MR1	-	a	240
	MR3	Internet access via EDGE link							
	GW1	Disconnection at the Satellite access link							
S.4	MR1	MR1 was shut down	ALL	MR2	MR3	MR2	-	a	120
	MR3	Cellular link is down							
	GW1	Satellite access link was re-established							
S.5	MR4	Two trees were merging	ALL	MR2 MR3 MR4	MR2 MR5	MR6	-	b	120
S.6	MR4	The converged tree split into two trees	ALL	MR2 MR4	MR6	MR2	MR3-MR5 Intra-Comm	b	180
S.7	MR2	Link failure at the HSPA access link	ALL	MR2	MR3	MR2	-	a	180
S.8	MR4	Two trees of different HA merged	ALL	ALL	MR2 MR5	MR3	-	b	180
S.9	MR1	Re-attached to the tree	ALL	ALL	MR3 MR5	MR2 MR1	Med-Sensor (MR3)	b	300
	-	Policies changed after casualty was found							

B. *Experiment Setup*

The performance of the different communications over the MMNA infrastructure was evaluated in varying MMNA scenarios of the use case example. This was accomplished in an experiment of nine stages carried out with different configurations and considerations. Table I provides a description of these experimental stages and explains for each one the main considered events, the entities performing the different types of communication, the utilised testbed setup, and the test duration. The main focus was on the different activities of the search group SG1 and their interaction with SG2 and SG3. For each of the nine stages, a test of ten runs was carried out over the relevant testbed setup. The results were then collected for each run and the average result was presented. The following section provides results analysis of each of the experiment stages.

C. Results Analysis

In this subsection, we present and discuss the results for each stage. Table 1 presents details of the ongoing communications for each stage. The test in each stage was carried out separately on one of the testbeds shown in Figure 3 (see Table 1). Please note that each stage was built on its previous one.

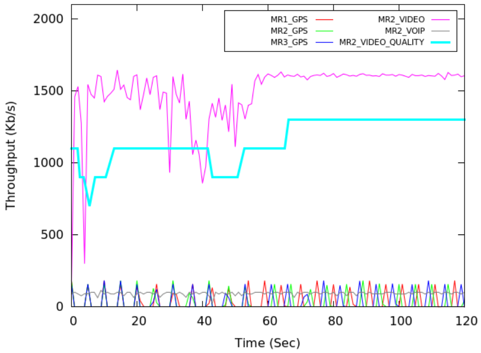


Fig. 4. Stage 1 Results - Traffic Throughputs

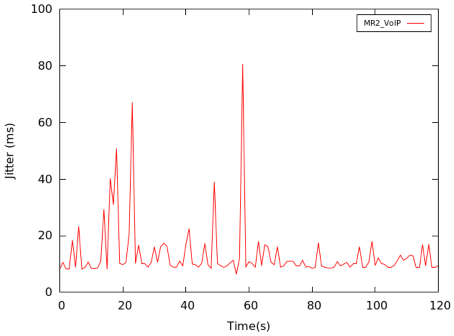


Fig. 5. Stage 1 Results - VoIP Jitter

In stage 1 (S.1), the experiment shows the advantages of having multihomed Internet access over the Main Gateway compared to a single-homed access. It started with the only available access being AL1 over GW1 for the entire tree. After 60 seconds, AL2 became available as an additional access option and the traffic of the GPS-Sensor applications was then handed off to it. During the first 60 seconds, the TCP throughput of MR1 video traffic fluctuated and experienced some drops, with a streaming rate of 1100kbps (with some drops) as shown in Figure 4. MR2 VoIP also experienced some increases above 50ms on its jitter as shown in Figure 5. These frequent reductions were due to the contention of all the communications over the only available access link (AL1).The overall situation improved once AL2 became available enabling the video streaming to achieve consistent TCP throughput (with a 20% increase on its streaming rate). MR2 VoIP traffic also achieved better jitter with a reduction of about 24% as shown in figure 5. It can also be noticed that once the GSP-Sensor traffic had been redirected over the newly emerging access link, it achieved relatively better network performance. For example, MR3 GPS-Sensor traffic was able to transmit 12 updates over AL2 compared to only 10 updates with non-multihomed access.

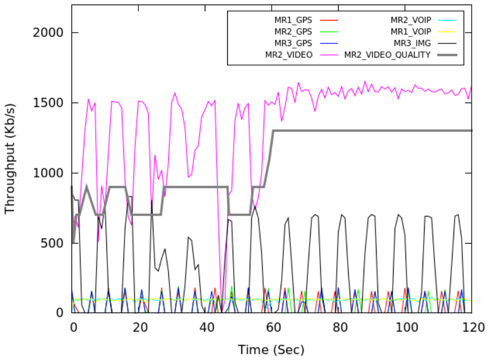


Fig. 6. Stage 2 Results - Traffic Throughputs

In stage 2 (S.2), we highlight the further improvement on the overall performance the solution can achieve with additional access option. The test started with AL1 and AL2 being available while AL3 then emerged at GW2 after 60 seconds and MR3 images and MR2 VoIP traffic were then redirected via AL3. Figure 6 shows frequent reductions of the TCP throughput achieved by MR2 video when the image relay took place every 5 seconds during the initial 60 seconds. As a result, the video was streamed at a rate that fluctuated between 900 and 700 Kbps. However, the throughput of the video stream and its streaming rate noticeably improved once the MMNA tree became triple-homed. The video streaming rate increased by 44% and the MR3 image transfer maintained a more consistent throughput.

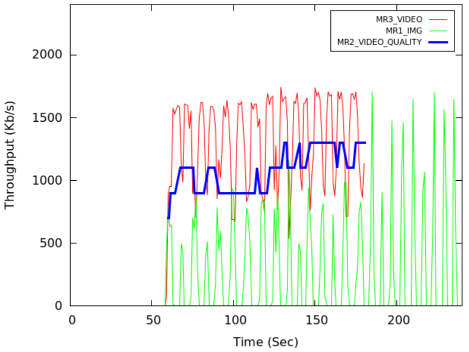


Fig. 7. Stage 3 Results - Video Streaming and Image Transfer

Stage 3 (S.3) shows the capability of the MMNA solution to support all-gateways scenarios. The test started with the three access options of S.2 being available. AL4 and AL5 then became available at 120 seconds and a link failure on AL2 then occurred. Figure 7 shows that the video and image communications started at 60 seconds. At that point, AL1 had to contend with MR3 video traffic and the frequent transfer of MR1 images, in addition to the MR1 VoIP call. This resulted in frequent TCP throughput drops for the video stream and the respective rates being fluctuated. Even after all the MRs served as Alternative Gateways at 120 seconds, the situation continued with slight improvement on the TCP throughputs since the MR1 VoIP call was redirected via AL4. Consequently, an increase of about 20% was achieved on the video streaming rate. The link failure at AL2 occurred when location and biomedical updates were due from MR1 and MR2 which then tried to communicate with the server but failed. This resulted in these updates being missed and an average delay of 2.994 seconds before the following update was then received. MR3 was sending an update when the failure happened, resulting in an average delay of 4.819 seconds before the communication recovered.

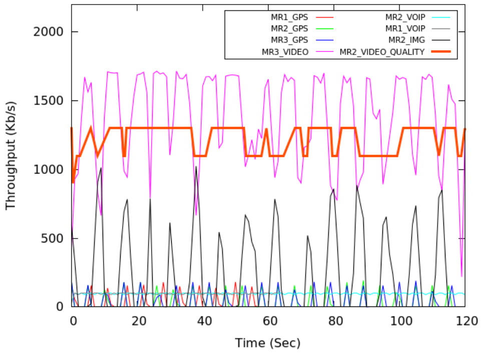


Fig. 8. Stage 4 Results - Traffic Throughputs

In stage 4 (S.4), we highlight the flexibility of the solution in the context of a dynamic situation. The test started with all-Gateway as described in S.3. After 60 seconds, MR1 was disconnected and shutdown while a link failure on AL5 occurred. AL2 then became available at GW1 and the location and biomedical updates of MR2 and MR3 was redirected via it. However, Figure 8 shows that each of them was able to transmit 12 location and biomedical updates over its access link during the first 60 seconds compared to 11 updates over AL2 during the final 60 seconds. The MR3 video and MR2 image TCP communications were competing for the available bandwidth over AL1. As shown in Figure 8, the throughput of the video streaming experienced frequent reductions due to the image relay every 5 seconds.. However, this was maintained during the entire test duration despite those events took place at 60 seconds.

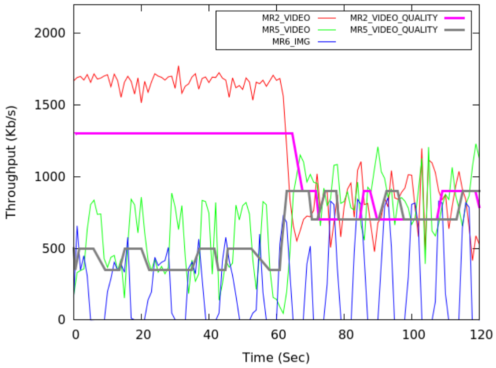


Fig. 9. Stage 5 Results - Video Streaming and Image Transfer

Stage 5 (S.5) shows the capability of the solution to support the convergence of multiple trees and enable resource sharing among them. The test started with two distinct MMNA trees during the initial 60 seconds. The first tree (GW1, GW2, and MR3) had multiple access options whereas the second tree (GW3, MR5, and MR6) was single-homed. As shown in Figure 9, MR5's video stream achieved low TCP throughput with frequent reductions resulting in a fluctuating streaming rate. After 60 seconds, the two trees merged and GW3 operated as an Alternative Gateway for the combined tree. Consequently, MR5's video stream and MR6 image transfer achieved better TCP throughputs. Figure 9 shows an increase of about 28% on the video streaming rate. However, the TCP throughput and streaming rate of MR2 video streaming dropped via GW1, which can be adhered to the applied selection policies. Additionally, we examined VoIP jitter and found that a decrease of about 13% was achieved by GW3 VoIP communication on the experienced jitter after the tree convergence.

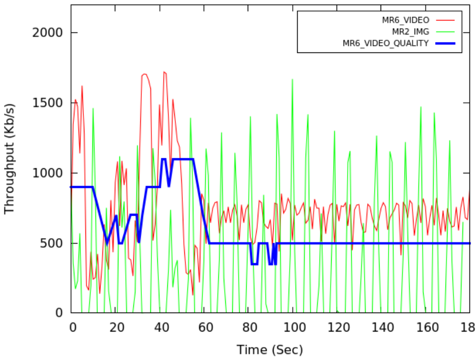


Fig. 10. Stage 6 Results - Video Streaming and Image Transfer

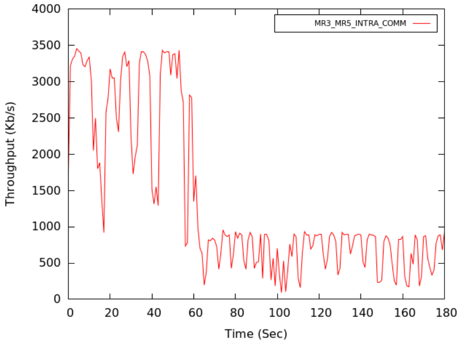


Fig. 11. Stage 6 Results - MR3-MR4 Intra-communication

Stage 6 (S.6) highlights the flexibility of the approach to sustain ongoing communication in the case of tree split. The test started with the two trees of S.5 being still merged for the initial 60 seconds. After that, the two trees split again and the traffic of each tree was then redirected via the respective available gateways. MR3 and MR5 were internally communicating over the tree during the initial 60 seconds. This enabled high TCP throughput to be achieved as shown in Figure 10. After the two trees split, MR3-MR5 communication was maintained as inter-tree communication over GW1 and GW3 (via HA1), with the frequent reductions due to overlapping with MR2 image transfer. Figure 11 shows that MR6 then continued receiving the video stream with a more stable TCP throughput and streaming rate. The TCP throughput of MR2 image traffic also improved, enabling more images to be transferred. However, the jitter experienced by MR4 VoIP traffic showed a noticeable increase due to the resulting single-homed access.

Stage 7 (S.7) shows how the efficient multihoming support provided by our solution can help in link failure recovery. The test carried out over setup (a) of Figure 3. It started with AL1, AL2, and AL3 being the only available access links. The failure occurred on AL3 at 60 seconds and the respective traffic was redirected via GW1. the MMNA enabled the Mobile Routers to maintain their respective communications when the failure occurred with some experienced delay. MR2 location and biomedical updates experienced an average delay of about 3.993 seconds when the traffic was being redirect via AL2. The link failure occurred when MR2 image transfer was due, but failed. This resulted in an average delay of about 1.995 seconds.

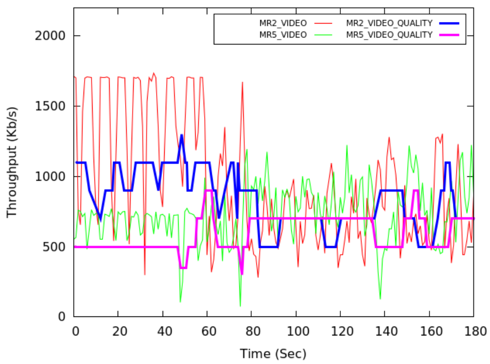


Fig. 12. Stage 8 Results - Video Streaming

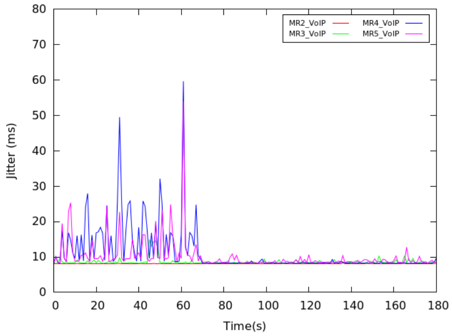


Fig. 13. Stage 8 Results - VoIP Jitter

stage 8 (S.8) shows the capability of the solution to support the convergence of multiple trees belonging to different Home Networks. The test started with two distinct MMNA trees during the initial 60 seconds. The first tree (GW1, GW2, MR3) registered with HA1, whereas the other tree (GW3 and MR5) registered with HA2. At 60 seconds, the two trees converged, and MR5 video traffic and the location and biomedical updates were redirected via AL1 and AL2, respectively. Figure 12 shows that MR5 video stream then achieved a better throughput with an increase of about 20% on its streaming rate. Figure 13 shows a reduction of about 39% and 17% on the jitter experienced by the VoIP traffic of MR4 and MR5, respectively. However, the TCP throughput of MR2 video streaming also declined after 60 seconds. This can be attributed to the applied selection policies which caused an increase in traffic contention at GW1.

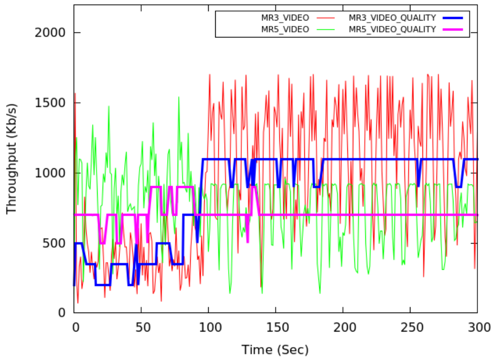


Fig. 14. Stage 9 Results - Video Streaming

In critical events such as when a casualty has been found, it is important to dynamically apply the selection policies that can ensure high performance of critical communications. The last stage (S.9) highlights the flexibility of the approach to support dynamic policy-based gateway selection. The test started with the converged tree having four access options (AL1, AL2, AL3, and AL4). At 100 second, new policies dedicating AL1 for those communications critical to the casualty was applied. These were the medical data, MR3 video streaming, and MR2 image transfer. This required redirecting MR5 video traffic via AL4. As a result, Figure 14 shows that MR3 video stream achieved a noticeable increase in its throughput and rate. The throughput of MR2 image traffic also improved by 30%, enabling the transfer of 12 images compared to 9 images before. The new decisions also allowed an increase of 9% on the throughput of the medical data traffic. We also examined the average jitter experienced by MR4 and MR5 VoIP calls which showed a decrease of 18%.

VII. CONCLUSION

In this paper, we have presented an overview of the Multihomed Mobile Network Architecture (MMNA) providing comprehensive multihoming support for complex mobility scenarios. The MMNA was experimentally implemented and evaluated in a Linux environment. Through designing a nine-stage experiment, we were able to envisage nine snapshots representing varying realistic events that could happen in a typical mountain rescue scenario. The results highlight the effectiveness and feasibility of the MMNA approach considering a Mountain Rescue use case. It was evident that the emergence of an additional gateway within a MMNA topology resulted in improving overall performance, while having an all-Gateways model of connectivity allowed for effective management of multihomed access. In addition, the ability of the MMNA to cope with multiple events at the same time goes along with the potential of such scenarios to be dynamic in reality. The support of the convergence of multiple trees and sharing Internet access even between those originating from different Home Networks demonstrated another practical dimension to the approach. While the focus has been mainly on Internet accessibility across an MMNA tree, local communication is of great importance in such scenarios. The ability to sustain communication between different nodes within a tree, even when they become separated after a tree split, demonstrates the applicability of the solution to such failure-prone environments. The ability to apply policies in a dynamic manner provides a more flexible and functional approach to potentially suit realistic requirements.

REFERENCES

[1] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, *Network mobility basic support protocol*, IETF RFC 3963, January 2005.

[2] C. Ng, P. Thubert, M. Watari, and F. Zhao, *Network mobility route optimization problem statement*, IETF RFC 4888, July 2007.

[3] 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.

[4] B. McCarthy, M. Jakeman, and C. Edwards, "Supporting Nested NEMO networks with the Unified MANEMO Architecture", In *Proc. Of the 34th IEEE Conference on Local Computer Networks (LCN)*, pp. 609-616, 2009.

[5] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, *Multiple Care-of Addresses Registration*, IETF RFC 5648, 2009.

[6] Mountain Rescue England and Wales Homepage. Available: http://www.mountain.rescue.org.uk/

[7] The Lake District Search and Mountain Rescue Association Homepage. Available: http://www.ldsamra.org.uk/

[8] I. Alsukayti and C. Edwards, "Multihomed Mobile Network Architecture," *Networking Conference, 2015 IFIP* , pp.195-203, 2015.