Multihomed Mobile Network Architecture

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*— IP mobility ensures network reachability and session continuity while IPv6 networks are on the move. In the Network Mobility (NEMO) model, the potential for NEMO Mobile Routers (MRs) to interconnect and extend Internet connectivity allows the formation Nested NEMO networks. With MANEMO, nested MRs can be efficiently interconnected in a tree-based structure with Internet access being maintained via a designated Gateway. However, this only supports single-homed Internet connectivity. With the span of wireless access technologies and the popularity of multi-interfaced devices, multihoming support in this scenario becomes critical. A Nested Mobile Network with heterogeneous available Internet access options would allow better overall network performance and optimal utilisation of available resources. In this paper, we present the Multihomed Mobile Network Architecture (MMNA), a comprehensive multihomed mobility solution. It provides a multihoming management mechanism for Gateway Discovery and Selection on top of a multihomed mobility model integrating different mobility and multihoming protocols. It enables a complex nested multihomed topology to be established with multiple gateways supporting heterogeneous Internet access. The results demonstrate that the proposed solution achieves better overall throughput, load sharing, and link failure recovery.**

Keywords—MIP; NEMO; MANEMO; Mobility; Multihoming;

I. Introduction

IP mobility ensures network reachability and session continuity while IPv6 nodes are on the move. This enables a mobile device such as a tablet or smart phone to maintain ongoing communication irrespective of its current point of attachment. This is not only applicable to individual IPv6 hosts but also to those interconnected into mobile IPv6 networks which can be formed in different environments. Personal Area Networks (PAN), Internet access on public transport such as trains and buses, and In-vehicle communication systems are examples of real-world use cases scenarios. However, the potential for theses mobile networks to interconnect allows the formation of more complex mobile network topologies. In public safety scenarios, mobile networks with co-located and connected first responder devices can be interconnected to extend Internet access provided by a designated gateway in a remote area. With the span of wireless access technologies such as WiFi, WiMax, and LTE and the popularity of multi-interfaced wireless devices, more Internet access options can become available in these sorts of scenarios but remain idle. Therefore, efficient multihoming support in such complex mobility scenarios becomes critical. Interconnected Mobile Networks, in a search and rescue scenario for example, can benefit from the availability of multiple gateways within the topology to maintain reliable and diverse connectivity with the mission control centre. A multihomed scenario would open the door for advanced mechanisms such as load sharing, traffic engineering, and failover recovery to be supported in mobility context. Eventually, this would allow better overall network performance, optimal utilisation of available resources, and the ability to project cost management.

In this paper, we address the need for efficient multihoming support in the context of nested mobility scenarios. We present the Multihomed Mobile Network Architecture (MMNA), a comprehensive multihomed mobility solution. It provides a multihoming management mechanism for Gateway Discovery and Selection on top of a multihomed mobility model integrating different mobility and multihoming protocols.

II. Background

A. Network Mobility Basic Support (NEMO)

The IETF has been working on the concept of network mobility and developed a basic mobility support solution, known as NEMO Basic Support (NEMO BS) [1]. It 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 to a Foreign Network after leaving its Home Network, it configures a temporary address, known as Care-of-Address (CoA), and initiates the Binding Update process. It sends a BU message to its Home Agent (HA) located at the Home Network in order to register the new CoA. The HA then installs a binding between the CoA, the MR's home address, and the Mobile Network Prefix (MNP) that is advertised by the MR. Upon a successful binding update, the HA sends a binding acknowledgement (BA) message back to the MR and a bi-directional IPv6-in-IPv6 tunnel is established between the two entities. The connectivity and reachability of the Mobile Network is then maintained over that tunnel while on the move. This is realised transparently to the communication of a MMN in the Mobile Network and a Correspondent Node (CN), a peer located on a different network.

In the NEMO model, each MR maintains Internet connectivity via its egress interfaces as a normal IPv6 host while providing a mobile subnet via its ingress interface. This would lead to a scenario where a remote MR connects to the mobile subnet of another MR and gains indirect Internet access. Once that happened, the remote MR carries out the

ISBN 978-3-901882-68-5 © 2015 IFIP

binding update process and establishes a tunnel with its HA over the existing tunnel of the MR to which it is connecting. The chain can also extend with multiple interconnected MRs in a similar way, resulting in topological structure known as Nested NEMO. With the NEMO-over-NEMO tunnelling model imposed by the underlying protocol, the communication of an interconnected MR needs to traverse a multi-tunnels path. This routing sub-optimality imposed by Nested NEMO is known as the Pinball Routing problem [2].

B. *MANET for NEMO (MANEMO)*

The concept of MANEMO is based on combining the properties of the Mobile Adhoc Network (MANET) and NEMO technologies. It is a broad concept illustrated in [3] which also defines that different NEMO and MANET related issues can be addressed within the MANEMO domain. This includes the Pinball Routing problem discussed earlier. The Unified MANEMO Architecture (UMA) [4] provides a comprehensive MANEMO-based solution. 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 networks.

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) and the Network In Node Advertisement (NINA) protocols, the interconnected MRs form a tree-based structure and establish routes over the tree. The tree formation process is initiated by the gateway MR (root-MR) that has direct Internet access, once it has successfully established a tunnel with its HA. It adds a Tree Information Option (TIO) containing tree information into its Router Advertisements. The tree information is then propagated further down by each connecting MR, after being received and processed to install a default route towards the gateway MR. Meanwhile, routing information is also exchanged over the tree. Each MR advertises its MNP into a Network In Node Option (NINO) attached to its Neighbour Advertisements. This information is propagated up the tree enabling the gateway MR to route inbound traffic over the tree and tunnel outbound traffic via its tunnel. The Binding Update process is then performed over the tree infrastructure. BU and BA messages are tunnelled via the gateway tunnel and routed over the tree to the respective MR. Upon a successful home registration, the HA ensures that the existing gateway NEMO tunnel is utilised for the communication of the registering MR. If the gateway and a MR within the tree belong to the same Home Network and HA, the scenario is called the Aggregated Roaming Scenario. On the other hand, if they are registered to different HAs then the MR needs to perform the binding process according to the Non-Aggregated Roaming Scenario. The HA of the gateway in this case performs the role of a Proxy-HA and carries out the MR binding process on its behalf. After receiving the BU message of the MR, it initiates the proxy binding process and sends a Proxy-BU, containing its address as the CoA, to the HA of the MRs (Target-HA). Upon a successful proxy binding, a HA-HA tunnel is established between the Proxy- and Target-HAs.

C. *Multihomed mobility*

The NEMO BS as well as the Mobile IPv6 protocols have no built-in 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. However, the MCoA protocol enables the maintenance of multiple communication paths over the multiple tunnels without defining how the traffic is forwarded among them.

A taxonomy classifying the possible multihoming configurations in the context of NEMO scenarios has been provided in [6]. Each possible configuration is identified by three tuples (*x*, *y*, *z*) where *x*, *y*, and *z* refer to the number of MRs, HAs, and MNPs being advertised in the NEMO network, respectively. For example, the (n, 1, *) configuration indicates a multihomed NEMO network of more than one MR registering one or more MNPs with only one HA.

III. Related Work

There have been ongoing efforts in the research community to provide multihoming support in the context of nested mobility scenarios. Reference [7] proposed a multihoming path discovery and selection solution on top of an optimised Nested NEMO model based on the Reverse Routing Header (RRH) protocol, multihomed using the MCoA protocol. In [8], a MR within a Nested NEMO network can select the best path among those available, using the proposed path selection algorithm. The decision is made according to the requirements of the current communication of a MMN connecting to it. The Hierarchical Path-Selection algorithm proposed in [9] addresses the loop avoidance and path selection issues in scenarios where multihomed MRs can connect to multiple MANEMO trees.

Other research efforts also address mobility and multihoming management in varying scenarios. In [10], the NeMo Gateway (NMG) entity is introduced to interconnect and manage multiple MRs in a multihomed Mobile Network. There have also been various efforts to address the different multihoming requirements, including load sharing/balancing and failure recovery, in the context of multihomed mobility. References [11] and [12] extend the underlying Neighbour Discovery Protocol (NDP) to divert ongoing NEMO communications seamlessly among multiple gateways in the case of link /device failure or for load sharing purposes. In [13], traffic redirection is managed and maintained via a central multihoming unit for instances where a failure has been detected in multihomed NEMO scenarios. Reference [14] proposes a dynamic load balancing mechanism based on calculated priorities of the available Mobile Routers.

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 on top of that a multihoming solution allowing for optimum utilization

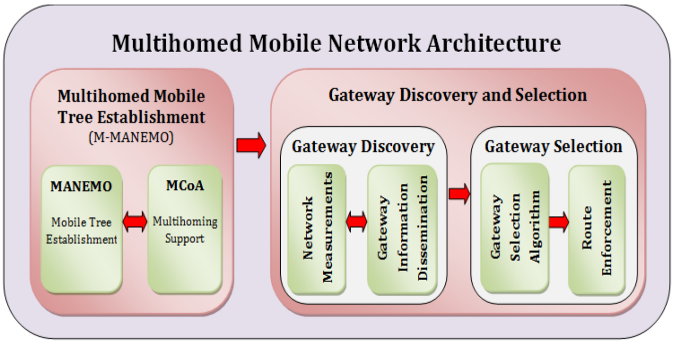

Multihomed Mobile Network Architecture
Multihomed Mobile Tree Establishment
(M-MANEMO)
MANEMO
Mobile Tree Establishment
MCoA
Multihoming Support
Gateway Discovery and Selection
Gateway Discovery
Network Measurements
Gateway Information Dissemination
Gateway Selection
Gateway Selection Algorithm
Route Enforcement

Fig. 1. MMNA Design Overview

and management of available network resources. Figure 1 presents an architectural overview of the design of the MMNA and shows the main components constructing the architecture. It is composed of two main processes, namely Multihomed Tree Establishment and Gateway Discovery and Selection. Establishing a multihomed tree topology provides the underlying infrastructure over which the Gateway Discovery and Selection process operates. A number of functional components are incorporated into the architecture to efficiently enable the discovery of and selection among the available gateways within a multihomed tree. This section describes the components of the MMNA.

A. *Multihomed Mobile Tree Establishment*

This process enables the establishment of a multihomed mobile tree with multiple gateways spanning across the tree providing heterogeneous Internet access. 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. This eliminates the routing sub-optimality and the overhead of multi-layered tunnelling imposed by the original NEMO-BS model. The MCoA protocol provides the multihoming functionality supporting the emergence of additional Gateways within the tree. Figure 2 shows a simple M-MANEMO tree of four mobile nodes having two gateways providing multihomed Internet access at GW1 (being the Main Gateway via a Wifi interface) and GW2 (as an Alternative Gateway via a cellular interface).

A potential gateway, a MR with multiple access interfaces, running M-MANEMO within a tree, can perform the home registration over an access interface and establish a NEMO tunnel with its HA while being registered over the tree interface. Once this happens, it becomes an Alternative Gateway providing an additional option to the tree nodes to access the Internet besides the tree's Main Gateway, i.e. the root-MR of the tree. M-MANEMO also enables a potential M-MANEMO gateway having a NEMO home registration and tunnel to join the tree over an additional egress interface, to become an Alternative Gateway to the tree. M-MANEMO also provides support for a more complex scenario in which the tree has multiple gateways each of which has multiple tunnels over heterogeneous points of attachment. For efficient management of the tunnelling across a M-MANEMO tree, each tunnel is assigned a unique identifier called a Tunnel ID (TID). For each tunnel established between a gateway and its HA or a Proxy-HA and Target-HA, a new TID is generated and assigned to that tunnel.

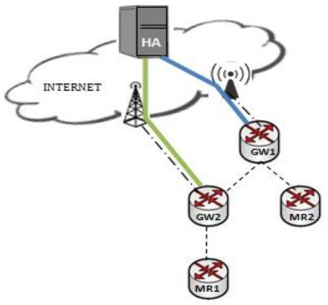


Fig. 2. A Simple M-MANEMO Tree

B. *Network Measurement*

The process of Network Measurements enables measurement collection of IP performance and capabilities metrics describing each Internet access option available within a M-MANEMO tree. After being disseminated, this information is fed into the Gateway Selection process as a series of inputs allowing informed decisions to be made. Considering the different requirements that could be imposed by different mobility and multihoming scenarios, it is important to design a customisable measurement collection process. In one scenario, for example, a comprehensive view of the performance of the entire communication path is required to discover the well performing and most reliable option. In this case, end-to-end measurement will be required. On the other hand, in a scenario where the deployed devices are of limited capability and Internet access incurs high costs, it is important to keep the measurement overhead to a minimum and adopt a lightweight approach. Figure 3 presents a design overview of the measurement process.

The measurement profile contains three main components that can be customised to meet the requirements of a particular scenario. The first enables the definition of the network path over which the measurements are collected and the collecting entity. The measurement could be performed for example by the end-host (MNN) for the end-to-end communication path, the MR entity for the MR-HA mobility path, or the Gateway entity over the mobility tunnels. The second component enables defining the measurement metrics that need to be collected in order to support the Gateway Selection process. There are a number of metrics that can be measured, with the most common being QoS metrics such as bandwidth, delay and packet loss. However, there could be scenarios where network reliability, security, cost, and load metrics are critical to making the decision. The third component provides the ability to apply the measurement mode applicable to a current deployment scenario. The measurement can be performed either in an *Active* or *Passive* mode. However, it could be feasible in some scenarios to run the process in a mode collaborating both passive and active measurements.

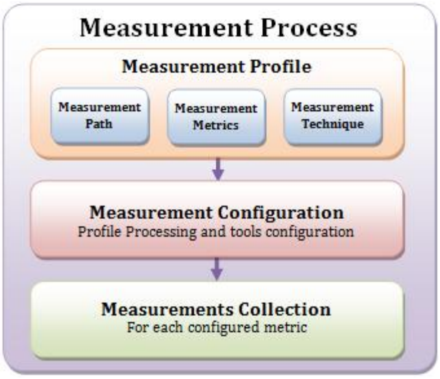


Fig. 3. Design Overview of the Measurement Process

In the next stage as shown in figure 3 the current profile describing the measurement configurations is processed. Accordingly, the applicable measurement tools to the profile are configured. There are a number of both passive and active tools that can be utilised and integrated into the process. For example, Netperf and UDPMon are active tools for measuring TCP and UDP throughput respectively. Another example is CapProp and PathChrip measuring the available bandwidth based on the packet pair estimation technique. The measurement collection is finally carried out once the relevant tools have been configured. The measurement profile and tools can be statically preconfigured whereas the measurement collection is a repetitive process that can be configured to run at a time interval suited to a given deployment.

C. *Gateway Information Dissemination*

The process of disseminating gateway information 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. To this aim, we developed a Gateway Discovery Protocol (GDP) defining how gateway information, once in place, is conveyed, propagated, and collected within the tree. Figure 4 illustrates these operations in a simple MMNA scenario where a M-MANEMO tree has only two gateways, GW1 and GW2, and a number of MRs interconnected within the tree. Each gateway advertises its capabilities and measurements to other MRs within the M-MANEMO tree. The gateway advertisement is performed on top of the underlying tree routing protocols. 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). As shown in figure 4, the recipients of the TIO advertisements within the tree also receive GISO messages providing information regarding GW1 and GW2. Gateway attributes such as the Home-of-Address, Home Agent IPv6 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. Figure 4 shows the one-way communication of GW2's advertisement.

During the Gateway discovery process, 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 contains its capabilities and measurements. This is frequently updated with the most up to date information.

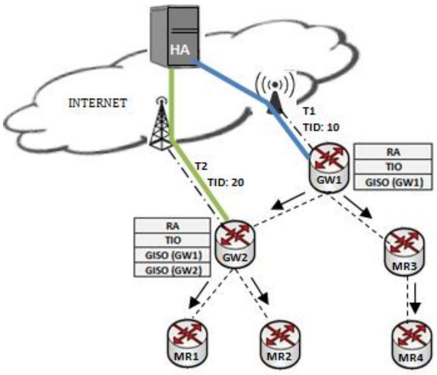


Fig. 4. Gateway Discovery Protocol (GDP) Overview

D. *Gateway Selection*

The process of gateway selection enables a selecting party to make the selection decision according to the selection policies defined for a given MMNA deployment, as well as real-time information being disseminated by the candidate gateways. Figure 5 presents a design overview of this process. It shows that the selection decision module takes two inputs. The first is the weights calculated for the selection criteria. The calculation is based on the importance rate given to each of the criteria by the applied policy. The second input is the gateway information after being collected from the Gateway Discovery List and then normalised. These inputs support making an informed decision for selecting the optimal gateway according to the policies of interest and the status of available gateways. 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 at different levels, such as flow- or network-based selection. Flow-based selection allows finer granular selection where the selection process is performed for every flow type or set of flows to be then mapped to a selected gateway. In the case of network-based selection the granularity level is coarser in a way that the decision is made for the traffic of a given mobile network. The more finer the selection granularity, the more control can be gained but with the cost of additional processing and signalling overhead.

The selection process is run by all the gateways within a M-MANEMO tree and each MR having more than a gateway available. The process in these nodes can be configured to run at a given time interval or based on specific events. For example, a selected gateway losing its access to the internet is a critical event to immediately act upon.

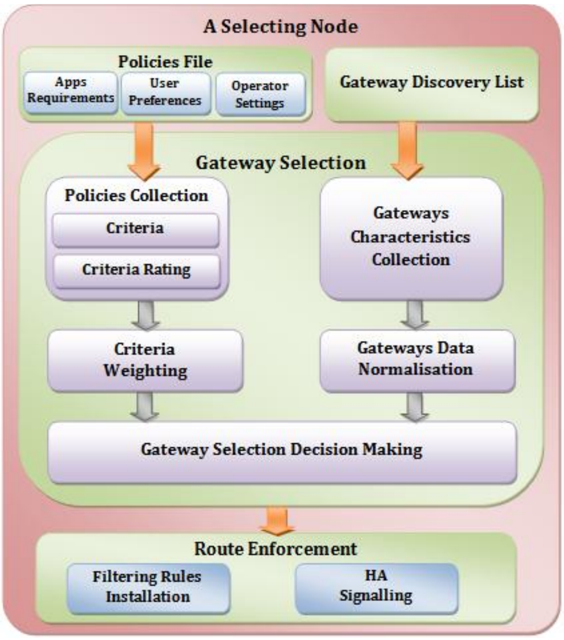


Fig. 5. Overview of the Gateway Selection Process

E. *Route Enforcement*

The process of route enforcement insures that outbound and inbound traffic of a Mobile Network within a M-MANEMO tree is always tunnelled via the currently selected gateway instead of traversing the default path. To enable this functionality, we developed a route enforcement mechanism on top of the M-MANEMO model. In this mechanism, the route enforcement process is realised upon collaborative operations performed at the different M-MANEMO entities namely Mobile Routers, Gateways, and Home Agents. Figure 6 demonstrates these operations in a simple MMNA scenario where tunnelling inbound and outbound traffic of MR1 is enforced via the selected gateway, GW2. Upon establishing a new NEMO tunnel with the corresponding HA, each gateway installs the necessary filtering and tunnelling rules to intercept and tunnel relevant outbound traffic via that tunnel. The HA also installs a tunnelling rule enabling relevant inbound traffic to be tunnelled via the established tunnel. This operation of filtering and tunnelling rules installation at the Gateway and HA entities is shown in figure 6 with number 1.

Once a MR has selected one of the available gateways, its HA is firstly notified of the newly selected gateway. To enable this functionality, the BU message is introduced with a new mobility option called the Selected Gateway Information Option (SGIO). Upon a new selection, an immediate BU+SGIO signaling message containing the information of the newly selected gateway is sent to the relevant HA as shown by number 2 in figure 6. Once received, the HA collects the information into its Traffic Forwarding List as shown in figure 6 with number 3, 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 carries on 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 to intercept and tunnel relevant outbound and inbound traffic respectively, the tunnel ID is also utilised by the MR entity for packet marking. The gateway selection process provides the tunnel ID of the selected gateway as an input to this process. Each packet generated by the MNNs connecting to the MR is marked with the tunnel ID of the currently selected gateway. As shown by number 4 in figure 6, packets sourced from the MNP1 prefix are marked by MR1 with the TID of the selected gateway, GW2. Meanwhile, the filtering and tunnelling rules installed at the HA upon signalling the selection help it to intercept and tunnel the inbound traffic destined to the MNNs.

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 a BU+SIGO signalling message has been sent by the MR, it is firstly received and processed by the Proxy-HA to install the relevant rules. The Proxy-HA then sends a Proxy BU+SIGO signalling message containing its IP address and the ID of the HA-HA tunnel established with the Target-HA. Once received, the Target-HA collects the information into its memory and installs the necessary filtering rules to intercept and route the corresponding inbound traffic via the HA-HA tunnel.

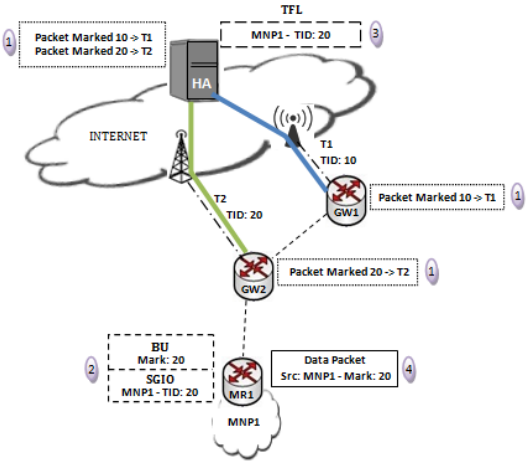


Fig. 6. Route Enforcement Mechanism Overview

V. MMNA Implementation

We experimentally implemented the MMNA solution in our lab at Lancaster University. This section provides an overview of the proof-of-concept implementation of the different MMNA processes described in the last section.

A. *M-MANEMO*

M-MANEMO was developed based on merging two main protocols, MANEMO and MCoA. These protocols have openly available Linux-based implementations providing the necessary functionality to support the different mobility and multihoming operations. Both were implemented on top of the original NEMO implementation. The MANEMO protocol implementation, known as UMA+, was developed at Lancaster University whereas the MCoA implementation is available as Linux kernel and userland patches to the original

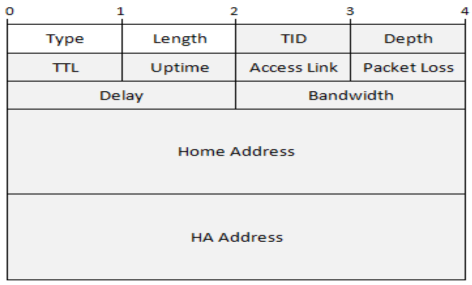
NEMO implementation. We integrated and modified accordingly these distinct implementations on top of umipv1.0 (the latest NEMO implementation by umip.org). We extended UMA+ to integrate the different MCoA functionality including BID mobility option processing, in addition to incorporating TID assignment and processing. M-MANEMO was developed using the 3.8.2 version of Linux kernel.

B. *Network Measurements profiles and tools*

Different measurement profiles can be created to fulfil varying MMNA deployment scenarios. In the current implementation, we defined two measurement profiles. The first is set as the default profile indicating the collection of measurements over tunnelled paths between the gateway and HA entities for metrics including bandwidth, delay, and packet loss, using an active mode. Accordingly, the Iperf and UDPMon active tools were incorporated to measure throughput, delay and packet loss at a given interval. The profile also indicates the collection of other metrics including gateway uptime that is computed periodically, and access cost that is supplied manually. The second profile enables lightweight measurement over the same tunnelled path for network bandwidth and load metrics using the passive mode. A simple passive monitoring tool was developed based on tcpdump and a Linux Perl script collecting the measurements of these metrics at a configurable interval. The measurement is performed at the gateway entity for both profiles.

C. *Gateway Discovery Protocol (GDP) Message Description*

Figure 7 illustrates the format of the Gateway Information Sub-Option (GISO) message. Being a sub-option to the base TIO option, it was formatted to be compliant with the generic TIO sub-option format allocating the first two bytes to indicate the Type and Length of the message. The TID, Home-of-Address, and HA Address indicates the ID of the tunnel the gateway is advertising, the HoA of the gateway, and the IPv6 address of its HA. The Depth and Time-To-Live (TTL) describe the number of hops the recipient is from the advertised gateway, and the advertisement is limited to during propagation, respectively. The Uptime provides the elapsed time since the advertised tunnel has been established and can serve as a reliability indicator. The message also provides measurement information indicating the throughput, delay, and packet loss over the advertised tunnel. The type of access link over which the tunnel is established is provided in the Access Link. This information would enable informed decisions to be made when selecting the preferred gateway according to criteria such as QoS.



0	1	2	3	4
Type	Length	TID	Depth	
TTL	Uptime	Access Link	Packet Loss	
Delay		Bandwidth		
Home Address				
HA Address				

Fig. 7. Gateway Information Sub-Option (GISO)

D. *Gateway Selection algorithm*

To experimentally enable the gateway selection functionality, a simple selection algorithm was developed. It enables a network-based selection as described in the previous section under sub-section D. 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. This method has been adopted related works such as [15] and [16]. The criteria are compared against each other to build a comparison matrix. Then, the geometric mean for each one is computed and the weights are then calculated as the ratio of its means to the sum of all the means. The normalization of the collected gateway data was implemented based on the min-max normalization method in which the normalized value (x') is calculated as follows:

$$x' = \frac{x - min(A)}{max(A) - min(A)} \qquad (1)$$

where x is the value to be normalized, and *min(A)* and *max(A)* is the minimum and maximum value among the gateway data of a given criterion. This would 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. Each normalized value is simply multiplied by the relevant criteria weight. Then the sum of the values of each gateway corresponding to the different criteria is calculated. Finally, the gateway with the maximum sum is selected.

E. *Route Enforcement Implementation*

The implementation of the route enforcement process is based on a number of functional components implemented at the different M-MANEMO entities in order to collaboratively enforce the new gateway selection. These components are 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. Each packet is marked with the ID of the preferred tunnel and this requires at least 8-bits. The Traffic Class (TC) field, that is large enough to accommodate this information, is utilised for packet marking. Since TC is developed for QoS classification and prioritization support, it has only local effect across the M-MANEMO tree in this implementation and is reset for each packet leaving the tree. This is a practical approach given the nature of the proof-of-concept experimental implementation. For HA signaling, the information of a newly selected gateway is carried into the Selected Gateway Information Option (SGIO) attached to a BU message. it enables a MR to communicate selection information such as the preferred tunnel ID and the IPv6 address of the corresponding gateway.

Furthermore, enforcing the new selection requires a number of traffic tunneling and filtering rules to be installed at each gateway and HA within a MMNA scenario. Since it was adopted to implement tunnel establishment in M-MANEMO, the Linux XFRM framework in conjunction with the Linux IP filtering framework "Netfilter" are adopted to enable the new selection to be enforced at the HA and Gateway entities. A Netfilter rule enables a gateway to intercept IPv6 packets with the TC value set to the ID of its tunnel and mark them locally within the kernel to then be intercepted and tunneled by the XFRM framework according to the installed XFRM policy.

VI. Evaluation

In order to evaluate the performance and capabilities of the MMNA solution, we built an in-lab experimental testbed enabling the running of our MMNA implementation on different mobility and multihoming setups. In this section, we describe the testbed setups and present the results of all the testing focused on the main aspects of multihoming, namely TCP throughput, load sharing, and link failure recovery.

A. *Testbed Description*

Different testbed setups were configured to conduct each of the different experiments, and figure 8 shows two of them. Setup (1) was configured to carry out the TCP throughput and load sharing experiments whereas setup (2) was configured for link failure recovery experiments. All the testbed setups were built 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 a couple of Ethernet interfaces. They are Linux machines with the 3.8.2 version of Linux kernel installed. As shown in figure 8, three of these PCs in setup (1) were configured to run as Access Routers (AR1, AR2, and AR3) and used to provide different Access Networks via Ethernet interfaces. Another two machines were configured to operate as a Correspondent Node and a MMNA-enabled HA. These different entities were interconnected via an Ethernet backbone network using a Netgear switch.

The other PCs were configured to run the MMNA implementation as Gateways (GW1, GW2, and GW3) and Mobile Routers (MR1, MR2, and MR3). They were configured with Software-based Access Points on the respective wireless interface to provide Mobile Networks over which they were wirelessly interconnected. The gateways were connected to the ARs over Ethernet interfaces configured to emulate connectivity to different access links. This is required to evaluate the behaviour of our solution on a more controlled environment and eliminate as much as possible the side effects of wireless properties. The GW1-AR1 link was configured to emulate a WiFi access link operating at 4.5Mbps whereas the GW2-AR2 and GW3-AR3 links were configured to emulate HSPA connections operating at 1.8Mbps. Additionally, the wired infrastructure was configured with a dynamically varying delay of approximately 80ms. Setup (2) in figure 8 was built and configured similarly with an additional HA (HA2) and only two gateways.

For each setup, we carried out two experiments, one for testing upstream traffic and the other for downstream traffic. The communication took place between the CN and virtual hosts configured on MR1,MR2, and MR3 to operate as MMNs. Each experiment was run ten times and the average result is taken for each experiment.

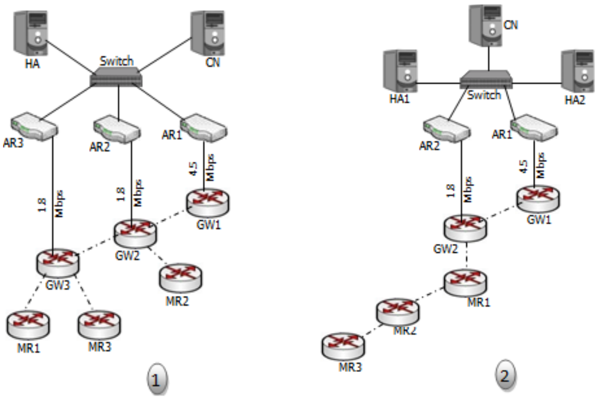


Fig. 8. Testbed Setups

B. *Overall TCP Throughput*

In order to examine the overall TCP throughput that can be achieved in an MMNA scenario, we conducted two experiments over setup (1) in figure 8. One for downstream TCP throughput in which a file was downloaded from the CN by each of the MMNs connected to the MRs. The other was for the upstream TCP throughput in which the file download was run by the CN node. In the both experiments, all the MRs were configured to run a basic selection policy dictating the selection of the gateway based on the access type. The experiments started with only the access of GW1 being available and selected by all the MRs. Then, MR2 selected GW2 when it advertised its 3G access after 70 seconds of the experiment. Once GW3 disseminated the advertisement of its 3G link, it was selected by MR3 after 100 seconds of the experiment.

Figure 9 and 10 show the results collected at the CN for the upstream TCP throughput and each of the MNNs for the downstream TCP throughputs. They show similar results regarding the overall TCP throughput in both of the experiments. With non-multihomed access using a single gateway (GW1) during the first 70 seconds of the experiment, TCP traffic of all the MMNs was tunnelled via the same tunnel (GW1-HA). This enabled an averaged overall throughput of about 3.9 Mbps to be achieved. Once the tree became multihomed with two gateways (GW1 and GW2) and MR1 traffic was sent via GW2, the TCP communications achieved better overall throughput. As illustrated in table I, the system was able to maintain about a 41% increase in the overall TCP throughput with multihomed access of two gateways. The additional access that became available at GW3 after 100 seconds of the experiment allowed further improvement. That is, an increase of about 67% was managed on the overall TCP throughout of the ongoing communications as illustrated in table I. These results demonstrate that TCP communication would achieve a good increase in the overall TCP throughput over a MMNA tree of multiple gateways with them being efficiently utilisation by the policies being applied.

C. *Load Sharing*

In order to examine the load sharing capability of the solution, setup (1) as shown in figure 8 was also used to carry out two additional experiments. The same configurations described in the previous section were applied but with UDP streaming among the MMNs and CN. In one experiment, The MMNs connecting to MR1, MR2, and MR3 were configured to receive 1.75, 3.75, and 1.5 Mbps UDP flows respectively. In the other, MMNs were configured similarly to send upstream UDP traffic.

Similar UDP throughput results were collected at the CN and each of the MMNs for the upstream and downstream communications, respectively. Figure 11 shows the result of the downstream UDP throughput. The WiFi access at GW1 was initially shared among the communications of all the MMNs and no one of them was able to receive the stream at the required bit rate. The situation improved when GW2 gained access via AR2 and the tree became multihomed. MR2 then selected GW2 based on its selection policy preferring a 3G connection over WiFi for (as an example) security reasons. The overall load was shared among the available gateways (GW1 and GW2), enabling the stream over MR1 to reach the required throughput of 1.75Mbps. Meanwhile, the throughput at MR2 and MR3 also showed an increase of about 20-30% but is still under the required throughput. Another gateway, GW3, established a tunnel via a 3G access network later on and the corresponding advertisement then triggered the selection process at MR3 to consider a closer gateway. Once MR3 selected it and the traffic tunnelled via the corresponding tunnel, the overall load of the tree was shared among the three gateways, enabling each of the MMNs to receive the corresponding UDP flow at the targeted throughput. The result shows the capability of the MMNA to enable load sharing among multiple gateways in order to improve the overall performance of ongoing communications.

Additionally, we calculated the handoff delay when redirecting the traffic from one gateway to another. This was calculated as the delay between the last packet being received via GW1 and the first packet received via GW2 and GW3 at MR1 and MR3 respectively. As table II illustrates, an average delay of about 110ms was experienced by the traffic over MR1 and a shorter delay in the case of MR3 traffic since it traversed less hops via GW3 within the tree. Such delays are due to the time required for enforcing the selection at the HA. On the other hand, no additional delay was experienced by MR2 traffic, which remained tunnelled via GW1.

D. *Link Failure Recovery*

We implemented a simple link failure recovery mechanism in order to examine the behaviour of the system in the case of a gateway losing its access to the Internet during operation. In this approach, receiving no more advertisements of a gateway signifies the loss of its access link. Then, those currently selecting that gateway would react upon this and reselect a different gateway. A policy was configured to enable the Main Gateway (GW1) once the failure has been detected. In order to evaluate the link failure recovery capability of the solution in different scenarios, setup (2) shown in figure 8 was used to configure different scenarios. In all of the experiments, a 1.5Mbps UDP flow was sent between one of the MRs and the CN over GW2. In scenario 1, 2, and 3 the stream was run by MR1, MR2, and MR3 respectively. Both of the gateways and MRs in these scenarios registered with HA1 only. In scenario 4, GW2 registered with HA2 and the stream was run between MR1 and the CN. The experiments ran for 200 seconds and after 110 seconds had elapsed the access link at GW2 (AR2-GW2) went down and the traffic was then redirect to GW1.

The results in table III show the delay between the last packet received via GW2 and the first packet received via GW1 at the communicating MR for each scenario. An average delay of 3.3 seconds was required by MR1 and HA to redirect the traffic to GW1. The delay increases at about 1.1 second the more the hops between the communicating MR and GW2. This can be attributed to the current failure detection mechanism that is based on each MR monitoring gateway advertisements being propagated over the TD protocol that need to be processed at each node. One approach to alleviate the problem and reduce the delay is to enable the failing gateway to send an immediate signalling message only processed by those currently selecting that gateway. On the other hand, the multiple HAs mobility in scenario 4 introduces a less than 300 ms delay on average compared to the average delay in scenario 1. This would explain that the HA-HA model with an additional tunnelling layer would cause less than 10% additional delay on average.

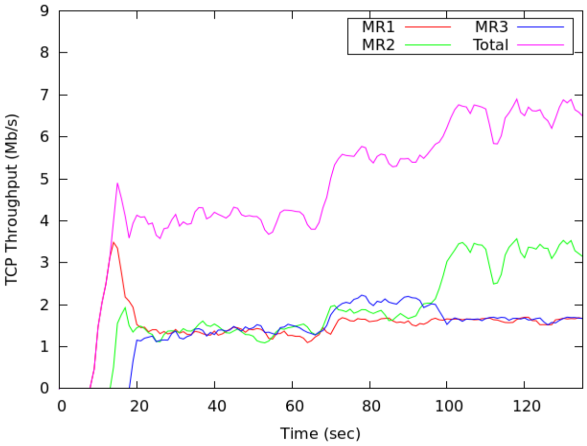


Fig. 9. Average Downstream TCP Throughput

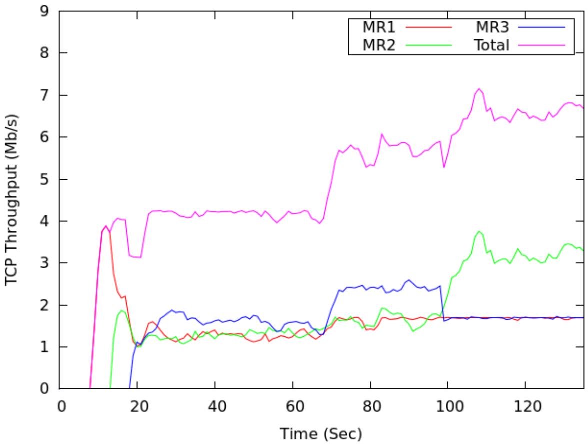


Fig. 10. Average Upstream TCP Throughput

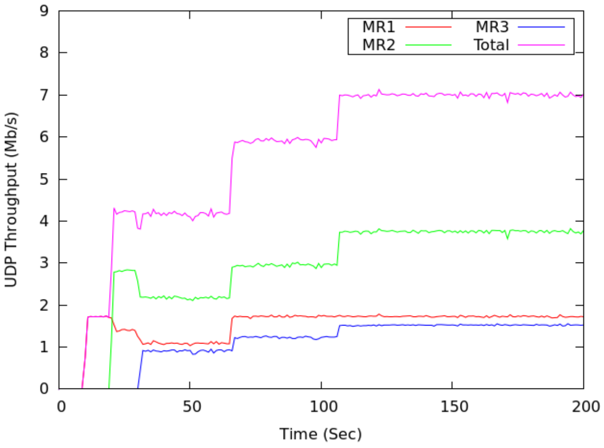


Fig. 11. Load Sharing

TABLE I. TCP THROUGHPUT IMPROVEEMNT

Experiment Time (sec)	Selected Gateways	Avg. Overall Throughput (Mb/s)		Improvement	
		Down stream	Up stream	Down stream	Up stream
10 - 70	GW1	3.892	4.004	-	-
70 - 100	GW1+GW2	5.516	5.643	41.7%	40.9%
> 100	GW1+GW2+GW3	6.534	6.651	67.9%	66.1%

TABLE II. HANDOFF DELAY (MS)

Node	Min	Max	Avg	Stdev
MR1	92.815	131.460	**109.403**	17.105
MR3	73.902	96.030	**85.986**	6.845

TABLE III. LINK FAILURE RECOVERY DELAY (SEC)

Scenario	Min	Max	Avg	Stdev
Scenario_1 (MR1)	2.989	4.579	**3.316**	0.493
Scenario_2 (MR2)	3.452	5.740	**4.581**	0.830
Scenario_3 (MR3)	4.483	7.196	**5.659**	0.974
Scenario_4 (MR1)	3.194	4.972	**3.611**	0.639

VII. CONCLUSION AND FUTURE WORK

In this paper, we have presented an overview of the Multihomed Mobile Network Architecture (MMNA) providing a comprehensive multihoming support for complex Nested mobility scenarios. The main components of the solution, namely the M-MANEMO model and the Gateway Discovery and Selection mechanism, have been introduced. The MMNA solution was experimentally implemented and evaluated over real-testbed setups, considering different multihomed mobility scenarios. As the results explained, the communications over the MMNA networks achieved better overall TCP throughput. The load sharing among multiple gateways allowed improved overall performance of ongoing communications. In the case of link failure, the solution enabled immediate reaction with varying delays in different scenarios. The present implementation considers a network-based selection. A flow-based implementation is also currently under development. This requires extending the gateway selection and the route enforcement processes.

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 2009)*, pp. 609-616, 2009.

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

[6] C. Ng, E. Paik, T. Ernst, and M. Bagnulo, *Analysis of multihoming in network mobility support*, IETF RFC 4980, October 2007.

[7] K. Ruoshan, F. Jing, and Z. Huaibei, "The Combination of Multiple Care-Of Addresses Registration and Reverse Routing Header in Nested Network Mobility", in *Proc. Of the International Conference on Internet Technology and Applications (iTAP 2011)*, pp. 1-5, 2011.

[8] S. Mitra, and S. Pyne, "Distributed Route Selection Algorithm in Nested Multihomed Mobile Networks", in *Proc. Of the International Conference on Advances in Computing, Control, & Telecommunication Technologies, (ACT '09)*, pp. 75-79, 2009.

[9] L. Long-Sheng, M. Jhu-Shyuan, T. Yao-Hui, and L. Gwo-Chuan, "The Lower Hops Selection Scheme for Constructing the Multihoming NEMO", in *Proc. Of the 9th International Conference on Hybrid Intelligent Systems (HIS '09)*, pp. 123-128, 2009.

[10] Z. Slimane, A. Abdelmalek and M. Feham, "Infrastructure Independent Mobility Support for Multiple Mobile Routers Multihomed NEMO Networks", *International Journal of Computer Science Issues, Vol. 10, Issue 2, No 3*, pp. 191-200, March 2013.

[11] R. Kuntz, J. Montavont, and T. Noel, "Multiple mobile routers in NEMO: How Neighbor Discovery can assist default router selection." In *Proc. Of the 19th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2008)*, pp. 1-6, 2008.

[12] R. Kuntz, J. Montavont and T. Noel: "*Multihoming in IPv6 Mobile Networks: Progress, Challenges, and Solutions*", IEEE Magazine, 2013.

[13] Z. Slimane, M. Feham, and A. Abdelmalek, "A seamless and transparent MN-proxy based mobility support for (n, n, 1) multihomed NEMO model," *International Journal of Computer Science and Network Security*, vol. 10, no. 4, pp. 306-313, 2010.

[14] Lei, Zhao, Li Xiaoping, Dong Qingkuan, and Tan Shuaishuai. "Priority based Dynamic Load Balancing for Multi-Homed Network Mobility." *International Journal of Advancements in Computing Technology*, 2013.

[15] T.Y. Chung, F.C. Yuan, Y.M. Chen, BJ. Liu and C.C. Hsu, "Extending Always Best Connected Paradigm for Voice Communications in Next Generation Wireless Network," In *Proc. of the 22nd International Conference on Advanced Information Networking and ApplicatiOns*, pp.803-81O, March 2008.

[16] M. Lahby, L. Cherkaoui, and A. Adib, "A Novel Ranking Algorithm Based Network Selection For Heterogeneous Wireless Access," Journal of Networks, vol. 8, pp. 263–272, Feb. 2013