

Dynamic Management of Multiple Mobile Routers

Manabu Tsukada[†], Thierry Ernst[†], Ryuji Wakikawa[†] and Koshiro Mitsuya[†]

[†] Graduate School of Media and Governance, Keio University
5322 Endo, Fujisawa-shi, Kanagawa 252-8520, Japan
{tu-ka, ernst, ryuji, mitsuya} @sfc.wide.ad.jp

Abstract—Network mobility (NEMO) support is used to maintain the Internet connectivity of a group of terminals located into a network that changes its point of attachment to the Internet. The Internet access is made through a number of interfaces on a Mobile Router acting as a gateway of the mobile network. The overall bandwidth can be increased and redundancy can be provided by serving the mobile network through multiple mobile routers. However, this raises a number of issues related to multihoming. We therefore propose a Multiple Mobile Router Management (MMRM) system which allows nodes in the mobile network to be connected transparently to the Internet through multiple mobile routers. Mobile routers can dynamically join and leave the mobile network. They cooperate in order to share their Internet access within the entire mobile network. The proposed system is implemented and evaluated. Evaluation results show that the overhead of our system is negligible while redundancy and the overall bandwidth for the nodes in the mobile network are increased.

Keyword: Network Mobility (NEMO), Multihoming, Multiple mobile routers, Load balancing

I. INTRODUCTION

Today, mobile terminals are able to access the Internet from anywhere using wireless technologies such as IEEE802.11a/b/g, GPRS or Bluetooth. Thanks to the back-drop, the demand for on-the-move and uninterrupted Internet connectivity is increasing. In order to fulfill such demand, protocols for host mobility (Mobile IPv6 [1]) and network mobility (NEMO Basic Support, or NEMO in short [2]) have been specified by the Internet Engineering Task Force (IETF).

Network mobility support is necessary for a group of computers moving together and requiring access to the Internet, such as a network of sensors or access networks deployed in vehicles. For example, NEMO Basic Support is considered by the InternetCAR project [3] within the WIDE project as a means to connect automobiles to the Internet. Motivations and requirements for doing so are discussed in [4].

The main purpose of the NEMO Basic Support protocol is to establish a bi-directional tunnel between the router in the vehicle known as the *mobile router* (MR) and a server in the fixed infrastructure known as the *home agent* (HA). The MR serves as a gateway between the nodes located inside the vehicle (*mobile network nodes* or MNNs) and the Internet whereas the HA is in charge of re-routing all packets to the current location of the vehicle. This current location is determined by the point of attachment of the vehicle within the Internet topology, i.e. by the temporary address acquired on the *egress interface* of the MR. This temporary address

is called the *Care-of Address* (CoA). A permanent address, called the *Home Address* (HoA) and obtained on the same link as the HA (home link), is also acquired on the same interface and used as an identifier. All MNNs in the mobile network have a permanent address taken from a permanent prefix assigned to the mobile network (*Mobile Network Prefix* or MNP) and allocated on the home link. All packets intended to or originated from the MNNs are encapsulated into the tunnel established between the MR and the HA.

Meanwhile, mobile terminals such as mobile phones, laptops or Personal Digital Assistants (PDA) are more and more often shipped with multiple network interfaces. If these interfaces can be maintained simultaneously, the node has multiple paths to the Internet and is said *multihomed* [5]. For a mobile network, multihoming translates into either the MR being multihomed or several MRs being used to attach the mobile network to the Internet [6]. In mobile environments, multihomed configurations are particularly motivated by scarce bandwidth, frequent failures and limited coverage areas. This brings a number of benefits including the possibility to face the lack of coverage of a particular technology, to augment the Internet connectivity and to choose the best path in terms of delay, bandwidth or price. The motivations and the benefits of multihoming are detailed and illustrated through a number of scenarios in [7].

In this paper, we propose a Multiple Mobile Router Management (MMRM) system which allows a mobile network to be served through multiple MRs and transparently to the MNNs. The proposed system allows MRs to dynamically join and leave the mobile network. The objectives of our work are detailed in Section II whereas our approach is discussed in Section III. The proposed MMRM system is then described in Section IV and implemented in Section V. Our implementation is evaluated in Section VI. Section VII concludes this paper.

II. OBJECTIVES

Usually, there are several MNNs in a mobile network and the mobile network is connected to the Internet via a single MR. Some nodes may dynamically join into the mobile network. Some of them may have their own Internet access, possibly through a distinct access network or access technology. In theory, such Internet access could be used to improve the overall Internet connectivity offered to the MNNs.

To demonstrate this, we consider the target scenario described in Fig. 1. Several computers such as PCs and sensors are located in a vehicle and connected to the Internet via

a GPRS interface on the in-vehicle MR. Now, a passenger carrying a PDA is entering the vehicle. This PDA has an IEEE802.11g interface. There is quite a lot of traffic on the GPRS access point and the transmission error rate has increased. However, the access on the IEEE802.11g access point remains good. So, some of the traffic should be diverted to the IEEE802.11g interface of the PDA. Sessions that were temporarily diverted to the IEEE802.11g interface are transferred back to the GPRS interface when the PDA is carried out of the vehicle.

However, in practice, this scenario cannot be realized. One of the reasons is that MNNs already in the mobile network do not know that an additional Internet connectivity, through another MR, is available, and they are not allowed to switch between MRs without breaking on-going sessions. Our objective is thus to allow MRs to dynamically join and leave a mobile network and to share their Internet access within the entire mobile network, transparently to the MNNs. This provides redundancy and allows to increase the bandwidth perceived by MNNs.

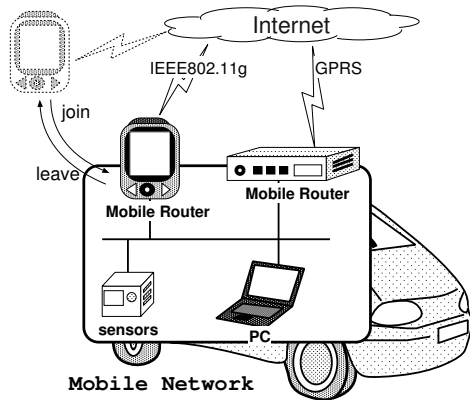


Fig. 1. Target scenario for MMRM

III. ISSUES AND APPROACH

[6] is a detailed analysis of the behavior of NEMO Basic Support under all the possible multihoming configurations. The configurations are classified according to three parameters, (x) the number of MRs connecting the mobile network to the Internet, (y) the number of HAs serving the mobile network, and (z) the number of MNPs advertised in the mobile network. This leaves us with eight cases. The configuration considered in this paper corresponds to "Multiple MRs, single HA and single MNP", referred to as case (n,1,1). The (n,1,1) configuration translates into multiple bidirectional tunnels being established between each pair of (HoA, CoA), and brings a number of issues which must be solved in order to realize our scenario outlined in the previous section. Below, for each issue we explain how they are going to be addressed:

a) Multiple Paths Establishment: The first issue is how the multiple bi-directional tunnels can be established. Our approach is to extend the use of the MCoA scheme [8] from registering multiple CoAs acquired by a single MR

to registering multiple CoAs acquired by several coordinated MRs. Originally, MCoA specifies a function to register multiple CoAs with a single HA. A *Binding Unique Identification number* (BID) is used to distinguish multiple bindings registered by a single mobile node and corresponding to the same HoA. The BID is stored in a *Binding Update List* (BUL) and is sent by the mobile node by means of a sub-option in the binding update. In our approach, the HoA of the MR already in the mobile network is provided to the MR joining the mobile network and the CoA acquired by the latter MR is provided to the former MR. The former MR associates this CoA to a virtual egress interface while the latter MR uses the former MR's HoA to establish a tunnel with the HA. This approach is illustrated on Fig. 2 as follows: when MR1 and MR3 join the mobile network already served by MR2, MR2 gets a total of three CoAs (one for the real interface and two for the virtual interfaces). MR1 registers CoA1 to HA using MR2's HoA and creates MR1-HA tunnel. MR3 also create MR3-HA tunnel the same way. In its *Binding Cache* (BC), HA keeps three bindings corresponding to the same HoA and distinguishes the bindings by means of the BID.

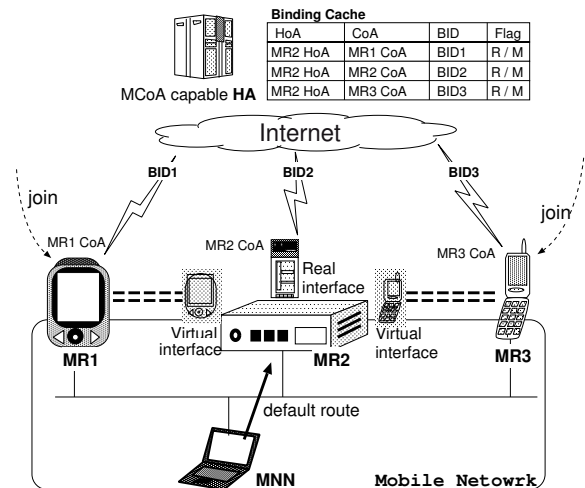


Fig. 2. Approach of MMRM

b) Path Selection: Now that there are multiple available bi-directional tunnels, they should be used simultaneously. The MR should be able to select the path for packets originated from the mobile network, and HA should be able to select the path for incoming packets bound to the mobile network. For doing so, some policies could be bound to a path. In MCoA, the user may be able to bind some policies to a BID. Policies can be used to divide flows to multiple network interfaces by flow type, port number, or destination address. However, the mechanism to distribute or configure policies is not within the scope of MMRM as is not in MCoA.

The usual approach for path selection is for MNNs to select the exit MR by means of [9]. This approach, however, would force all MNNs to be able to select the MR based on user policies. The replacement can be costly for low performance nodes such as sensors devices. However, the exit MR may

be treated as a default route of legacy IPv6 nodes. So, our approach is for the MNNs to send packets to the default router as normal IPv6 nodes do. In contrast with the usual approach, our approach doesn't require all MNNs to be extended with any special function. On the other hand it may introduce some overhead due to the encapsulation and decapsulation process. This overhead is negligible according to the results of our experimentation described in Section VI-A.

c) **Session Preservation:** In the event one tunnel fails, the path must be changed without breaking on-going sessions and transparently to the MNNs at layers above layer 3. Our approach is to establish a bi-directional tunnel between the MR already in the mobile network and the new MR brought into it. When an MNN wants to communicate with a CN, the packets from MNNs are routed to the default router, i.e. the former MR. Then, packets are redirected over this bi-directional tunnel. On Fig. 2, MR1-MR2 and MR2-MR3 bi-directional tunnels are established. MR2 treats these tunnels as virtual egress interfaces. MR2 refers to its policies and selects the interface from its three egress interfaces (one real and two virtual). When MR2 selects a virtual interface from MR3, the packets are encapsulated by MR2 to MR3. Then the packets are decapsulated by MR3 and transmitted to HA via the MR-HA tunnel. Since the source and destination addresses of the packets are not changed, sessions can be preserved.

d) **Dynamic State Sharing:** In order to allow MRs to join into and leave from the mobile network, a dynamic state sharing scheme is needed to detect MRs joining and leaving. At first, we define a list to keep the state of bindings on multiple MRs. All MRs in the mobile network maintain that list. MRs register the binding information to the list and advertise it to the mobile network when a binding is updated. By exchanging binding information with one another, each MR is able to get the state of bindings maintained by the other MRs. When an MR joins the mobile network, the other MRs detect it from such advertisements. In addition, each entry is associated with a lifetime, and entries from the list are deleted as the lifetime expires. When a MR leaves from the mobile network or shutdowns, corresponding entries are also deleted. The deletion allows other MRs to detect that a MR has left.

IV. OVERVIEW OF MMRM

In order for MNNs to benefit from a configuration with multiple MRs, MRs must collaborate and be synchronized with one another. To distinguish between an MR already in the mobile network and the joining MR, we consider two types of MRs. We, then, define a list to keep the state of bindings on multiple MRs, and all MRs in the mobile network should maintain the list. The MRs exchange information to synchronize the list maintained by each MR. We define message formats exchanged among the MRs. HAs are requested to be able to record multiple bindings by means of the MCoA scheme. The following terms are needed to describe MMRM:

- **Primary Mobile Router (PMR):** the MR acting as a default router for MNNs. The PMR is gathering policies and has the responsibility for path selection.

- **non-Primary Mobile Router (non-PMR):** all MRs not acting as a default router for MNNs. The non-PMR does not have policies for path selection and simply forwards packets from the PMR to HA.
- **Neighbor Egress interface List (NEL):** a list maintained by both the PMR and non-PMRs. The list contains an entry for every binding that the multiple MRs have. Table I shows the format of the NEL.

TABLE I
NEIGHBOR EGRESS INTERFACES LIST FORMAT

Element	Format
BID	Integer number
Mobile Router type	PMR / non-PMR
Home Address	IPv6 address
CoA	IPv6 address
Ingress interface Address	IPv6 address
Lifetime	Integer number (seconds)

- **NEL Advertisement:** a message to synchronize NELs between MRs. PMR and non-PMRs advertise all the NEL information to the mobile network from an ingress interface when a NEL entry is added, removed or updated.

The process of exchanging binding information among multiple MRs is illustrated on Fig. 3: (1) A non-PMR is brought to the mobile network and (2) receives NEL advertisement messages periodically sent by the PMR. (3) At the same time, the non-PMR adds to the NEL the PMR's binding information received from the NEL advertisement. After this, (4) the non-PMR sends a binding update to the HA which serves the mobile network. A *binding acknowledgment* is received back from the HA. At this time, the non-PMR specifies the same Home Address as the PMR and specifies the BID which is generated in a way it cannot be duplicated with another BID in binding update messages. The non-PMR adds an entry to the BUL as specified in NEMO Basic Support and (5) adds the binding information to the NEL. (6) At the same time, a NEL advertisement is sent to the mobile network from the ingress interface of the non-PMR. (7) Then, the PMR receives the NEL advertisement message from the non-PMR and adds in the NEL an entry which contains the binding information of the non-PMR. Next, (8) a bi-directional tunnel is established between the PMR and the non-PMR.

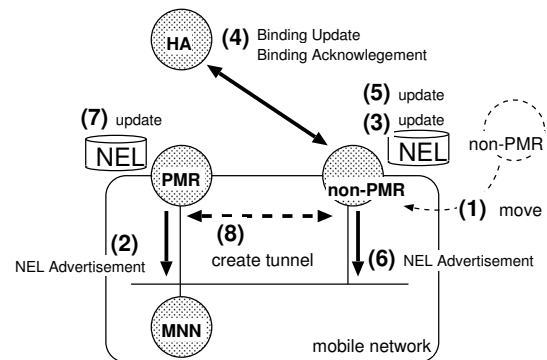


Fig. 3. Messaging between PMR and non-PMR

The routing process using MMRM is illustrated in Fig. 4. When an MNN wants to communicate with a CN, the packets from MNNs are routed via the PMR, because the PMR is always a default router on the link. For path selection, PMR refers to its policies and selects the route to the HA via the appropriate MR. In case policies advocate routing via the PMR-HA tunnel, the PMR transfers packets via its tunnel to the HA as specified by NEMO Basic Support and MCoA. In case policies are advocating routing via the non-PMR-HA tunnel, the PMR transfers packets via its tunnel to the non-PMR, as shown on Fig. 4. Packets are then transferred by the non-PMR to the HA via the non-PMR-HA tunnel. When packets are sent from the CN to the MNN, HA selects the route as specified in MCoA.

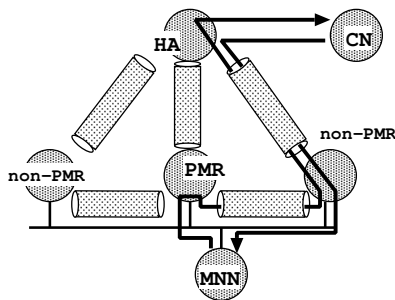


Fig. 4. Routing for MMRM

V. IMPLEMENTATION

We implemented MMRM on NetBSD-1.6.2-RELEASE [10] with SHISA snap-20041115 [11], [12]. First, let's briefly describe the SHISA implementation so that our MMRM extensions brought to the MR are better understood. In SHISA, three daemons are responsible of particular functions on the MR end. A special socket called *mobility socket* is used to exchange state among daemons:

- **Mobility socket:** a raw socket used to pass state related to mobility between kernel and userland. For example, a user daemon can set, delete, and update the binding information to the kernel.
- **Mobile Router Daemon (MRD):** it manages a BUL on the MR end, sends binding updates and receives binding acknowledgments. When the BUL is modified, the daemon sends a message to the kernel and the other daemons via the mobility socket.
- **Movement Detection Daemon (MDD):** it detects and notifies movements to the kernel and the other daemons via the mobility socket on the MR end.
- **NEMO Network Daemon (NEMONETD):** it configures MR-HA tunnels and the routing table on the MR end. When the BUL is modified, the daemon receives a message via the mobility socket and configures MR-HA tunnels and routes.

An instance of the MRD, the MDD and the NEMONETD operate on the MR as illustrated in Fig. 5. The MDD keeps

watching the routing socket. (1) MDD detects movements from the socket when the MR acquires a new CoA. (2) The movement information is notified to MRD via the mobility socket. (3) MRD sends a binding update to the HA which serves the mobile network. A binding acknowledgment is received back from the HA. After that, MRD updates the BUL and (4) notifies the BUL information to the kernel via the mobility socket. NEMONETD also listens to the mobility socket and receives the BUL information. (5) NEMONETD sets up the bi-directional tunnel to HA and sets up the route to the mobile network based on the BUL information. When a binding expires, MRD deletes the corresponding entry and (4) notifies the BUL information to the kernel via the mobility socket. NEMONETD also listens to the mobility socket. (5) The bi-directional tunnel to HA is deleted and the routing table is modified by NEMONETD.

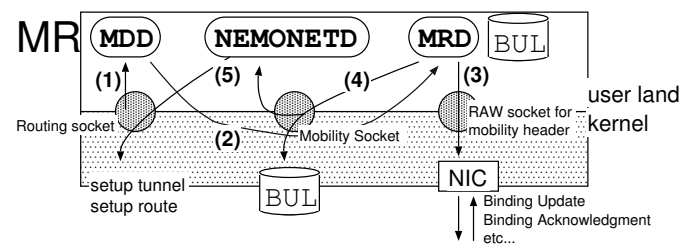


Fig. 5. Overview of SHISA implementation (on the MR end)

We added a new daemon named Multiple Mobile Routers Management Daemon (MMRMD) to perform the new MMRM function. This daemon is running on the MR end, manages the NEL, and collaborates with the other daemons running on the MR and other MMRMD running on other MRs. In order to synchronize the NELs managed by the other MRs serving the same mobile network, binding information are exchanged with the MMRMDs running on the other MRs. The daemon selects the path to the HA based on policies.

The implementation of MMRM is illustrated in Fig. 6. MMRMD checks two sockets and receives messages from them. One is the mobility socket which receives messages when the BUL is updated. The other is a raw socket for UDP port number 11233 on the ingress interface to exchange binding information with the other MRs.

In Fig. 6. (a) MMRMD receives the messages about a BUL information whenever a BUL entry is added, removed, or updated from the mobility socket. In case a BUL entry has been added or updated, MMRMD picks the HoA, the CoA and the BID up from the messages and updates the corresponding NEL entry. In case a BUL entry has been removed, the corresponding NEL entry is also removed. It is removed as well when the lifetime has expired. In both cases, (b) MMRMD sends a NEL advertisement on the ingress interface. (c) When an MMRMD receives a NEL Advertisement from other MRs, a new NEL entry is added, or the corresponding NEL entry is updated, or removed, according to the NEL advertisement. When the state of NELs is changed, (d) the

daemon sets up IP Filter [13]. IP Filter is software to set rules to distribute traffic to the network interfaces for passing packets through the MR. In this implementation, path selection and flow separation are performed by IP Filter.

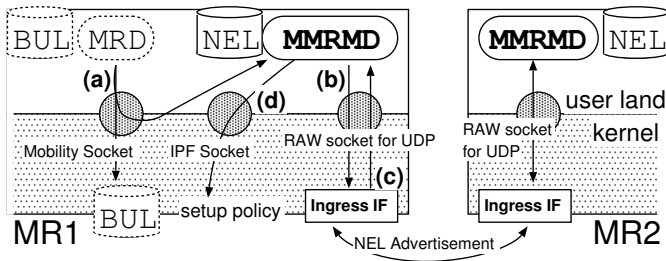


Fig. 6. Overview of MMRM implementation

VI. EVALUATION

Our system is designed to achieve the multihoming benefits described in [7]. The system aims at providing *Permanent and Ubiquitous Access*, *Redundancy/Fault-Recovery*, *Load Balancing*, and *Preference Settings*. *Increased Bandwidth* is also achieved according to the experimentation described in Section VI-B.

The performance of MMRM was evaluated by experimentation using the IPv6 local network illustrated on Fig. 7. The testbed was designed to minimize the influence of unexpected traffic. There are two routers between MRs and HA, and between HA and CN. MR1 is shipped with two egress interfaces and is connected to links (A) and (B). MR2 is shipped with one egress interface and is connected to link (C). Solid lines are Ethernet and dotted lines are Ethernet whose bandwidth is limited to 1200 Kbits/sec using [14]. This limitation is necessary in order to emulate a link with less bandwidth and to avoid HA being a bottleneck. MR1 is the PMR and MR2 is a non-PMR. *Router Advertisements* (RAs) are sent every five seconds on the links where MRs are connected to.

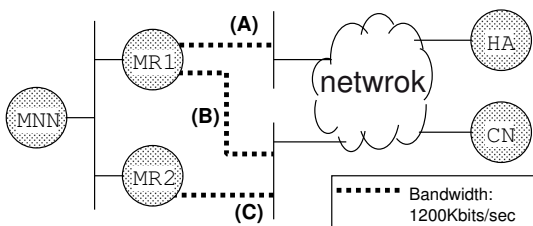


Fig. 7. Evaluation environment

The specification of each computer is listed in Table II. The ingress interfaces of MR1 and MR2 are 10BASE-T and the other network interfaces are 100BASE-T. This difference can be ignored because the performance of each MRs is equal.

A. Overhead measurement

The redirection may introduce some overhead due to the encapsulation process at the PMR, decapsulation process at the

TABLE II
PERFORMANCE OF EACH PCs

	CPU	Memory	OS
HA	PentiumIII 1.0GHz	256M	NetBSD 1.6.2-R
MR1	PentiumIII 1.0GHz	640M	NetBSD 1.6.2-R
MR2	PentiumIII 1.0GHz	640M	NetBSD 1.6.2-R
CN	Pentium M 1.0GHz	256M	FreeBSD 4.10-R
MNN1	PentiumIII 868.25MHz	256M	NetBSD 1.6.2-R
Routers	AMD Enhanced Am486X4	64M	FreeBSD 4.9-R

non-PMR, and the additional hop to the CN. Such overhead does not appear, when MNNs directly select a default router from multiple MRs. In fact, MMRM allows MNNs to use multiple paths transparently at the cost of the redirection overhead. This overhead was measured in terms of *Round Trip Time* (RTT) and throughput by comparing the case where PMR does not redirect the packets and the case where PMR redirects the packets. In the first case, MMRM is disabled and the MR1-HA tunnel is used. In the second case, MMRM is enabled and the MR2-HA tunnel is used. For the RTT measurement, MNN sends 56-Byte ICMPv6 Echo Request packets to CN 100 times. Results are shown on Fig. 8. The average RTT when MMRM was disabled is 2.381 ms, and 2.860 ms when MMRM was enabled. The redirection overhead adds 0.479 ms on RTT, an increase by 20%. For the throughput measurement, MNN sends TCP packets to CN for 5 minutes. The packet size is 1208 bytes. The average throughput when MMRM was disabled is 1071 Kbits/sec, and is 991 Kbits/sec when MMRM was enabled. The overhead is reduced by 80 Kbits/sec, a decrease by 7%.

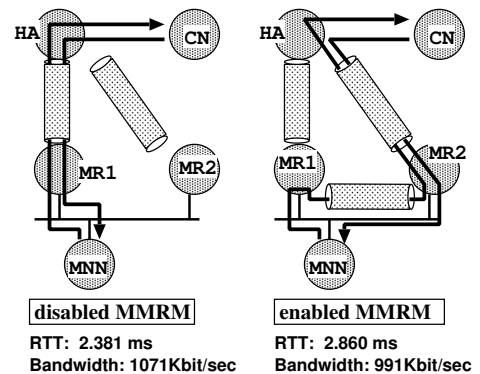


Fig. 8. Overhead measurement

This overhead must be balanced against the complexity and cost to extend all MNNs with path selection mechanisms as this would require a replacement of all nodes in the mobile network. The cost can be particularly high for low performance nodes such as sensor devices, or for nodes temporally carried into the mobile network. Also, in a situation where a PDA with an IEEE802.11b interface joins, the available bandwidth for MNNs can be increased by 11Mbps. The redirection overhead (0.479 ms on RTT and 80Kbits/sec on throughput) is negligible in this case.

B. Flow distribution

We checked if MMRM increases the throughput by flow distribution. The change of throughput was measured when three sessions go through the same MR-HA tunnel and when three sessions go through separate tunnels using MMRM redirection. MNN establishes three TCP sessions to CN, according to policies specifying port numbers 5001, 5002 and 5003 for Ethernet links (A), (B) and (C) respectively. The throughput was measured every 3 seconds for 600 seconds.

From time $t=0$ to $t=300$ second, link (B) and (C) were disconnected and all the three sessions from MNN to CN pass through the same link (A) in Fig. 7. From $t=300$ to $t=600$ second, all three links (A), (B) and (C) were connected. According to policies, all the three sessions from MNN to CN pass through three distinct links.

Fig.9 shows the total throughput of three sessions from MNN to CN. The average throughput is 1086 Kbits/sec from $t=0$ to 300 second. On the other hand, the average throughput is 2586 Kbits/sec from $t=300$ to 600 second. By using MMRM, the throughput for MNNs is increased by 1500 Kbits/sec, which represents a 238% improvement. In addition, Fig.9 shows that MMRM is able to change the path without breaking on-going sessions and to distribute traffic as soon as multiple paths become available. In fact, the overall connectivity is shared dynamically.

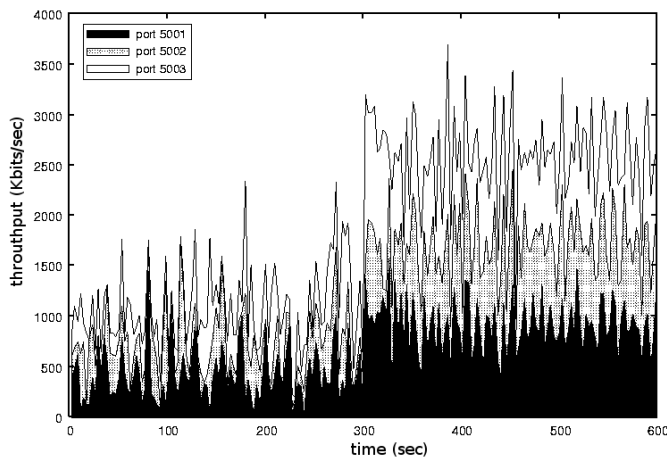


Fig. 9. Throughput measurement

VII. CONCLUSION

We proposed the Multiple Mobile Routers Management (MMRM) system to allow MRs to dynamically join into and leave from a mobile network. When MMRM-enabled MRs such as mobile phones are brought by passengers to a mobile network such as an in-vehicle network, MNNs are able to access the Internet through multiple MRs. MMRM increases the redundancy and the bandwidth for MNNs by separating the traffic to multiple paths.

Three features are proposed, (1) multiple CoAs registration from MRs, (2) cooperation between MRs through information

exchange, and (3) traffic separation from MNNs to CNs. Extensions of MCoA were proposed to register multiple CoAs from multiple MRs. We, then, defined a packet format to exchange information between multiple MRs. A primary MR allows traffic separation using multiple bi-directional tunnels between several MRs and the HA. The MMRM extensions were implemented on SHISA with NetBSD by adding a new daemon.

The overhead of MMRM comes from the packet redirection over a tunnel between MRs. Our evaluation shows the redirection overhead is negligible in our scenario. It also shows MMRM is able to transparently change the path for applications on MNNs, to dynamically share the Internet connectivity, and to increase the overall bandwidth.

As for the open issues that will be considered for future work, the MMRM system does not yet allow MNNs to communicate with CNs when PMR is down. For this issue, a mechanism allowing a non-PMR to replace a PMR can be considered. A non-PMR does not know if a PMR is down, or leaves from the mobile network by removing a corresponding NEL entry, but HA knows it from the binding update. This could allow the HA to select an alternative PMR. Security considerations will also have to be dealt with in future work. Security between HA and MRs will be provided by the Security Association (SA) pairs between the PMR and the HA. For security between MRs, transport mode IPsec can be used to protect NEL advertisements. Secure Neighbor Discovery (SEND) can provide security between MRs and MNNs.

REFERENCES

- [1] D. Johnson, C. Perkins, and J. Arkko. *Mobility Support in IPv6*, June 2004. IETF RFC 3775.
- [2] Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu, and Pascal Thubert. *Network Mobility (NEMO) Basic Support Protocol*, January 2005. IETF RFC3963.
- [3] Thierry Ernst, Koshiro Mitsuya, and Keisuke Uehara. Network Mobility from the InternetCAR Perspective. *JOIN: Journal on Interconnection Networks*, 4(3), September 2003.
- [4] Thierry Ernst and Keisuke Uehara. Connecting Automobiles to the Internet. In *ITST: 3rd International Workshop on ITS Telecommunications*, Seoul, South Korea, November 2002.
- [5] Nicolas Montavont, Ryuji Wakikawa, Thierry Ernst, Chan. Wah Ng, and Koojana Kuladinitthi. Analysis of Multihoming in Mobile IPv6. Internet Draft draft-montavont-mobileip-multihoming-pb-statement-04.txt, IETF, June 2005. Work in progress.
- [6] C. Ng, E. Paik, T. Ernst, and M. Bagnulo. *Analysis of Multihoming in Network Mobility Support*, July 18 2005. IETF work in progress, draft-ietf-nemo-multihoming-issues-03.txt.
- [7] T. Ernst. *Goals and Benefits of Multihoming*, February 21 2005. IETF work in progress, draft-ernst-generic-goals-and-benefits-01.txt.
- [8] Wakikawa Ryuji, Uehara Keisuke, Ernst Thierry, and Nagami Kenichi. *Multiple Care-of Addresses Registration*, January 20 2005. IETF work in progress, draft-wakikawa-mobileip-multiplecoa-04.txt.
- [9] R.Draves and D.Thaler. *Default Router Preferences and More-Specific Routes*, January 17 2005. IETF work in progress, draft-ietf-ipv6-router-selection-07.txt.
- [10] The NetBSD Project, June 2005. <http://www.netbsd.org/>.
- [11] SHISA, June 2005. <http://www.mobileip.jp/>.
- [12] Nautilus6 project, June 2005. <http://www.nautilus6.org/>.
- [13] IP Filter, June 2005. <http://coombs.anu.edu.au/avalon/>.
- [14] QoS Layer 2 Switch with Media Converter CX2510-MC, September 2005. <http://www.nec-globalnet.com/products/cx2510mc.html>.