

Multiple Access Interfaces for Mobile Nodes and Networks

Chan-Wah Ng

Panasonic Singapore Laboratories
Blk 1022 Tai Seng Ave #06-3530
Singapore 534415
Email: cwng@psl.com.sg

Thierry Ernst

Keio University, Jun Murai Lab
5322 Endo, Fujisawa-shi
Kanagawa 252-8520, Japan
Email: ernst@sfc.wide.ad.jp

Abstract—With the progress of wireless technologies today, mobile terminals with multiple access interfaces are emerging (e.g. laptops, Personal Digital Assistants). However, multiple interfaces cannot yet be used simultaneously; nor can they be switched without breaking ongoing connections. This paper explores the benefits and issues of having multiple access interfaces when mobile nodes and networks employ layer-3 mobility protocols of Internet Protocol version 6 (IPv6) to access the Internet while changing their points of attachment to the Internet. To overcome some of the identified problems, we propose a tunnel re-establishment technique. Simulation results show that this technique would allow mobile nodes and networks to benefit from permanent (and even uninterrupted) access to the Internet using different access technologies, without requiring special services provided by the access routers.

I. INTRODUCTION

Nowadays, more and more portable terminals have the ability to connect to the Internet using a wide range of access technologies, such as Third Generation (3G) cellular networks, General Packet Radio Service (GPRS), IEEE 802.11a/b/g, and Bluetooth. It is foreseen that the Internet Protocol (IP), particularly IP version 6 (IPv6), will be the convergent layer when these terminals (i.e. *nodes* with respect to the IPv6 terminology [1]) connect to the Internet. In order for these portable nodes to become truly *mobile* and to be reached no matter where in the Internet topology they are currently attached to, Host Mobility Support in IPv6 (or MIPv6 in short) [2] is developed by the Internet Engineering Task Force (IETF). In addition, as progress in wireless technologies continues to accelerate and gain widespread acceptance and adoption, a new form of mobility is starting to emerge: network mobility. Network mobility occurs when an entire network of IPv6 nodes moves as an entity and changes its point of attachment to the Internet topology. Examples of this include access network and sensors networks deployed in vehicles [3], [4] and wireless personal area networks. Network Mobility Support (i.e. NEMO Basic Support [5]) is being looked into by the Network Mobility (NEMO) Working Group [6] at the IETF.

At the same time, with the wide range of wireless access technologies available, portable terminals fitted with multiple access interfaces (which we hereafter refer to as *multi-mode nodes*) are starting to appear. These include dual-mode handphones, laptops, and Personal Digital Assistants.

The usefulness of attaching to the Internet using different access technologies at different time, or even simultaneously, has been described in various documents, including [7], [8]. However, protocols embedded in multi-mode nodes available in today's consumers market do not allow switching between interfaces without breaking on-going sessions. There are some issues to be resolved when doing so. In [8]–[10], the need for multiple address bindings in MIPv6 is addressed. [11] and [12] analyze the deployment of NEMO Basic Support in a mobile network with multiple access interfaces.

Building upon these previous work the current paper focuses on the implications of using multiple access interfaces while operating mobility support protocols (such as MIPv6 and NEMO Basic Support) that are designed originally with single-mode devices in mind. We first give an overview of MIPv6 and NEMO Basic Support in Section II. Then we look at the benefits of multi-mode nodes operating these mobility protocols in Section III. Following that, we explore into the potential problems and issues that one might face with such operations in Section IV. In Section V, we turn our attention to techniques that can be used to overcome some of these problems. Section VI presents preliminary results obtained from the simulation of these techniques. Finally, Section VII concludes this paper.

II. MIPv6 AND NEMO BASIC SUPPORT PRIMER

In essence, MIPv6 [2], [13] aims at enabling a mobile host to be reached by its global address, no matter where on the Internet topology the host is currently attached to. Each mobile host has a permanent home domain in MIPv6. When the mobile host is attached to its home network, it is assigned a permanent global address known as a home address (HoA). When the mobile host is away, i.e. attached to some other foreign networks, it is usually assigned a temporary global address known as a care-of address (CoA). The idea of mobility support is such that the mobile host can be reached at the home address even when it is attached to other foreign networks. This is done by means of IP-in-IP Tunneling [14]. A *bi-directional tunnel* is established between the mobile host and its home agent (HA), an entity residing in the mobile host's home domain. The tunnel is set up with the mobile host registering its care-of address with its HA

using messages known as Binding Updates (BU). From then on, the HA is responsible for intercepting packets intended to the mobile host's home address and encapsulating them to the corresponding care-of address. In the other direction, packet sent to other nodes using the mobile node's home address are also tunneled to the HA for further forwarding.

Extending the concept of mobility support for individual hosts to mobility support for a network of nodes, the objective of network mobility support [6], [15], [16] is to provide a means for nodes in a mobile network (MNNs) to be reached by their permanent address, no matter where on the Internet the mobile network is attached to. In essence, a mobile network is a network of nodes where the entire network changes its point of attachment to the Internet. This usually entails a mobile router (which bridge the mobile network to the Internet) in the mobile network that changes its point of attachment to the Internet.

In NEMO Basic Support [5], the mobile router controlling a mobile network performs routing of packets to and from the mobile network using some routing protocols when it is in its home domain. When the mobile router and its attached nodes move to a foreign domain, the mobile router registers its care-of address with its HA. An IP-in-IP *bi-directional tunnel* is then set up between the mobile router and the HA. The routing protocol used when the mobile router is at its home domain is again performed over the bi-directional tunnel. This means that every packet intended to the mobile network will be intercepted by the HA and forwarded to the mobile router through the bi-directional tunnel. The mobile router then forwards the packet to a host in its mobile network. When a packet is sent from a mobile network node, it transits via the mobile router which forwards it to the HA through the bi-directional tunnel. The HA then forwards the packet to the intended recipient.

Hereafter, the term mobile node is used to refer to either a mobile host (operating MIPv6) or a mobile router (operating NEMO Basic Support). In addition, the term *ingress interface* is used to refer to the network interface that connects the mobile router to the mobile network, as opposed to an *egress interface* that refers to an access interface that a mobile node uses to connect to the Internet. A multi-mode mobile node has several such egress interfaces.

III. ADVANTAGES OF USING MULTIPLE INTERFACES

Using multiple access interfaces, either in fixed or mobile nodes and networks, can bring various benefits [8]. These includes (a) Permanent and Uninterrupted Access, (b) Load Sharing and Load Balancing, (c) Redundancy and Fault Tolerance, and (d) Bi-Casting. In the following paragraphs, we detail each of these benefits for mobile nodes and networks.

A. Permanent and Uninterrupted Access

Different wireless technologies have different range and area of coverage. For instance, IEEE 802.11b has a typical coverage of 100m, whereas a GPRS base station can usually cover a radius of over 1 km. On the extreme, a mobile node with

satellite connection can retain connectivity even when it roams across an entire continent. Thus, it is possible for a multi-mode node or a mobile network with multiple mobile routers to make use of different access technologies at different time to ensure continuous connectivity. As an illustration, consider a node equipped with GPRS and IEEE 802.11b. When this mobile node is within a IEEE 802.11b hot-spot, it can connect to the Internet using its IEEE 802.11b interface. As it moves out of range from the IEEE 802.11b access point, it can switch over to use GPRS to maintain its Internet connection (albeit at a much lower speed). The mobile node can in fact alternate between these access interfaces to achieve handover with little or no disruption to its ongoing traffic sessions.

B. Load Sharing and Load Balancing

With multiple simultaneous connections to the Internet, a mobile node or a mobile network can receive and send data via multiple paths. This paves the way for achieving load sharing and load balancing. Load sharing occurs where a traffic flow is distributed among the available connections to achieve lower latency and increase robustness to network failures. Load balancing, on the other hand, is to spread different traffic flows to different connections. The available bandwidth and congestion condition at each connection is usually considered while doing so.

C. Redundancy and Fault Tolerance

A mobile node or a mobile network with more than one access interfaces can possess more than one independent connections to the Internet, thus attaining a level of redundancy that enables the mobile node or mobile network to maintain a greater resilience against network failures. For instance, a mobile network with more than one mobile router can switch all outgoing sessions from the failed primary mobile router to the secondary mobile router. Another example is a mobile node which activates a stand-by link when the primary link it is using fails.

D. Bi-Casting

Bi-Casting is to duplicate packets in a flow to be routed through alternate paths to its destination. With multiple simultaneous connections to the Internet, bi-casting can be used with a mobile node or a mobile network to increase the resilience of a traffic flow to packet drops and possibly reducing packet delays.

IV. ISSUES WITH MULTIPLE INTERFACES

Although multi-mode nodes would bring the benefits described in the previous section, there exists several issues in their deployment [9]–[12], [17]. Most significant of all is the problem of ingress filtering and failure detection.

A. Ingress Filtering

Ingress filtering refers to the filtering of packets by a router when forwarding packets received from an ingress subnet. This is done to check if the source address of the packet is valid in the said subnet, and is usually carried out to prevent address

snooping and diversion attacks [18]. Typically, this involves comparing the source address field of a packet with a list of valid address prefixes associated with the subnet.

To benefit from multi-mode nodes, it is often necessary to split packets originating from the same session between multiple bi-directional tunnels. This is especially true when we consider *fault tolerance* where packets must be diverted from a failed bi-directional tunnel to other alternative (perhaps newly established) bi-directional tunnel(s).

When doing so, care has to be taken to prevent ingress filtering from dropping the outgoing packets when the two tunnels end at different home agents. Ingress filtering occurs when these different home agents are configured to accept packets from different source prefixes. For example, consider the case when a mobile network has two tunnel connections to home agents HA1 and HA2. The mobile network prefix P1 is registered to HA1, and mobile network prefix P2 is registered to HA2. Mobile network nodes are free to auto-configure their addresses based on any of P1 or P2. When the tunnel to HA1 is broken, packets usually sent through the tunnel to HA1 are diverted through the tunnel to HA2. If HA2 (or some border gateway in the domain of HA2) performs ingress filtering, packets with a source address prefix of P1 may be discarded.

To avoid ingress filtering for such cases, the mobile router(s) can stop advertising the network prefix P1. This will stop mobile network nodes from using source address auto-configured from prefix P1. However, switching the source address suffers from the following two limitations:

- The process is long since nodes have to wait for source address to get deprecated [19].
- This forces transport sessions without multihoming capabilities (such as Transmission Control Protocol, TCP) to terminate, and be re-established using the new source address. Transport sessions with multihoming capabilities (such as Stream Control Transmission Protocol, SCTP) may be able to continue without disruption.

A similar situation may happen when a multi-mode mobile node subscribes simultaneously to different service providers using different access technologies (eg 802.11b and satellite). In such cases, each service provider might assign a different home address and home agent to the mobile node. When the mobile node wants to switch interfaces, ingress filtering will occur if the mobile node wished to use the same home address. The mobile node is now forced to use a different home address, which may cause on-going transport sessions to terminate.

B. Failure Detection

In order for fault recovery to work, the mobile nodes and home agents must first possess a means to detect failures. It is expected for faults to occur more readily at the edge of the network (i.e. at the mobile nodes), due to the use of wireless connections. The mobile node can then rely on router advertisements from access routers, or other layer-2 trigger mechanisms to detect faults [20] [21] [22]. In comparison, it is more difficult for home agents to detect tunnel failures. Home agents and mobile nodes can use proprietary methods

(such as constant transmission of heartbeat signals) to detect failures and check tunnel liveness. However, a lack of standardized "tunnel liveness" protocol means that it is harder to detect failures when mobile nodes and home agents belong to different administrations.

A possible method is for the mobile nodes to send binding updates more regularly with shorter Lifetime values. Similarly the home agents can return binding acknowledgment messages with smaller Lifetime values as well, thus forcing the mobile nodes to send binding updates more frequently. These binding updates can be used to emulate "tunnel heartbeats". This however may lead to more traffic and processing overhead, since binding updates sent to home agents must be protected (and possibly encrypted) with security associations.

V. TECHNIQUES FOR TUNNEL RE-ESTABLISHMENT WITH MULTIPLE ACCESS INTERFACES

In order to utilize the additional robustness provided by multiple access interfaces, mobile nodes that employ bi-directional tunneling with their home agents should dynamically change their tunnel exit points depending on the link status. For instance, if a mobile node detects that one of its egress interface is down, it should detect if any other alternate route to the global Internet exists. This alternate route may be provided by any other mobile router in the case of a mobile network, or by another access interface the mobile node itself possesses. If such an alternate route exists, the mobile router should re-establish the bi-directional tunnel using this alternate route.

A. Detecting Presence of Alternate Routes

To do so, a mobile node must first be capable of detecting alternate routes. The case where a mobile node possesses multiple access interfaces (bound to the same home agent or otherwise) should be trivial, since the mobile node should be able to "realize" it has multiple routes to the global Internet.

In the case where multiple mobile routers are on a mobile network, each mobile router has to detect the presence of other mobile routers. A mobile router can do so by listening to *Router Advertisement* (RA) message on its *ingress* interface(s). When a mobile router receives a RA message with a non-zero *Router Lifetime* field on one of its ingress interface(s), it knows that another mobile router which can provide an alternate route to the global Internet is present in the mobile network.

B. Re-Establishment of Bi-Directional Tunnels

When a mobile node detects that its current bi-directional tunnel with its home agent is down, a new bi-directional tunnel must be established over the alternate route. We consider two separate cases here: firstly, the alternate route is provided by another access interface that belongs to the mobile node; secondly, in the case of a mobile network, the alternate route is provided by another mobile router connected to the mobile network. We refer to the former case as an alternate route provided by an alternate egress interface, and the latter case as an alternate route provided by an alternate mobile router.

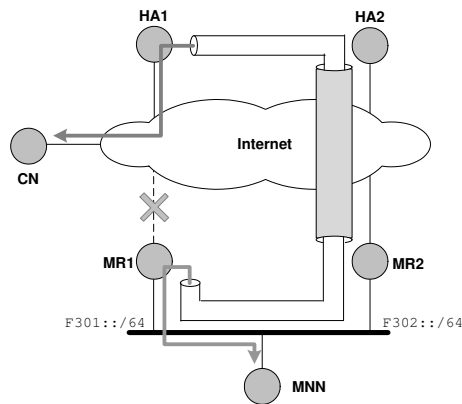


Fig. 1. Re-Establishment of Tunnel

1) *Using Alternate Egress Interface:* When the mobile node loses the connection over an egress interface, an alternate egress interface can be used should the mobile node possess multiple egress interfaces. The idea is to use the global address (most likely a care-of address) assigned to an alternate egress interface as the new (back-up) care-of address of the mobile node to re-establish the bi-directional tunneling with its home agent. The most direct way to do so is for the mobile node to send a binding update to the home agent of the failed interface using the care-of address assigned to the alternate interface. After a successful binding update, the mobile node encapsulates outgoing packets through the bi-directional tunneling using the alternate egress interface. This way, there is no need for the mobile node to switch home address and on-going sessions are not disrupted. It can continue to send packets using the home address of the failed interface.

2) *Using Alternate Mobile Router:* When the mobile router loses a connection to the global Internet, the mobile router can utilize a route provided by an alternate mobile router (if one exists) to re-establish the bi-directional tunnel with its home agent. First, the mobile router has to obtain on its ingress interface a care-of address with the prefix announced by the alternate mobile router. Next, it sends a binding update to its home agent using the new care-of address. From then on, the mobile router can encapsulate outgoing packets through the bi-directional tunnel via the alternate mobile router.

Fig. 1 illustrates the configuration. Here, mobile router MR1 and MR2 are advertising prefixes F301::/64 and F302::/64 respectively. When MR1's link to the Internet is broken, MR1 re-establishes the tunnel with its home agent HA1 through a care-of address configured from F302::/64, via MR2. By doing so, the mobile network node MNN can continue to use an address configured from F301::/64 to communicate with a correspondent node CN.

Note that every packet sent from/to mobile network nodes to/from their correspondent nodes will experience two levels of encapsulation. The first level of tunneling is done between the mobile router which the mobile network node uses as its default router and this mobile router's home agent. The second

level of tunneling is done between the alternate mobile router and its own home agent. By doing so, there is no need for the mobile router to stop advertising itself as a default router, thereby avoiding the need for mobile network nodes to change their address.

The mechanism described above uses bi-directional tunnel to overcome the problem of ingress filtering. Since binding updates are used to establish the bi-directional tunnel (and binding updates between a mobile node and its home agent must be protected with security associations), the mechanism does not expose the nodes performing ingress filtering to any new threats other than those possibly introduced by MIPv6 or NEMO Basic Support.

C. Avoiding Loops

The method to re-establish the bi-directional tunnel as described above may lead to infinite loops of tunneling. This could happen when two mobile routers on a mobile network lose connection to the global Internet at the same time and each mobile router tries to re-establish its bi-directional tunnel using the other mobile router. We refer to this phenomenon as *tunneling loop*.

One approach to avoid tunneling loop is for a mobile router that has lost connection to the global Internet to insert an option into the RA message it broadcasts periodically. This option serves to notify other mobile routers on the link that the sender no longer provides global connection. Note that setting a zero Router Lifetime field would not work well since it would cause mobile network nodes that are attached to the mobile router to stop using the mobile router as an access router too (in which case, the mobile network nodes would be forced to change their addresses which is what we are trying to avoid). A similar approach is investigated in [17].

D. Predictive Re-Establishment for Seamless Handover

The tunnel re-establishment technique as described above can be extended to achieve seamless handovers when the access interfaces can send warning notifications on pending lost of connection, such as those described in [21] [22]. Upon receiving such notifications, the mobile node can start to establish a new tunnel using alternative routes even before the bi-directional tunnel it is currently using breaks down. This allow the mobile node to handover with as little disruption as possible. To achieve true seamless handover, it is required that the layer-2 trigger be sent t_{pred} amount of time before the connection breakdown occurs, where t_{pred} is given by:

$$t_{pred} \geq t_{bu} + t_{pkt} \quad (1)$$

In (1), t_{bu} is the time taken for a binding update packet sent from the mobile node to reach the home agent, and t_{pkt} is the time taken for a data packet encapsulated by the home agent to reach the mobile node. In general, it is difficult for the mobile node to estimate the values of t_{bu} and t_{pkt} separately. It is relatively easier for the mobile node to estimate the round trip time, t_{rtt} , to the home agent. We can approximate $t_{bu} + t_{pkt}$ to be t_{rtt} , then (1) becomes

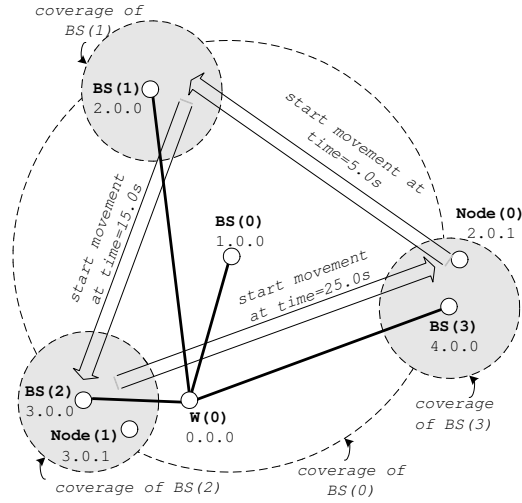


Fig. 2. Simulation Scenario

$$t_{pred} \geq t_{rtt} \quad (2)$$

A multi-mode mobile node may, for reasons of saving power, activate only one interface while other interface(s) is(are) put on standby. An early notification of impending lost of connection can then be used to activate a backup interface. For such cases, (2) needs to factor in the time taken to activate this backup interface, t_{wake} . Thus, we have

$$t_{pred} \geq t_{wake} + t_{rtt} \quad (3)$$

VI. SIMULATION RESULTS

Using the Network Simulator 2 (NS-2) [23] simulation package, we simulated a mobile node with multiple interfaces actively re-establishing bi-directional tunnel depending on the interface which has an available connection as described in Section V. Fig. 2 shows the simulation scenario we used. In Fig. 2, *Node(0)* is the mobile node with two interfaces, one tuned to channel 1 (which offer wide operating range but a meager bandwidth of 64kbps), and the other tuned to channel 2 (which offer high bandwidth but limited access range). Whenever both channels are available, *Node(0)* always use the one that offers higher bandwidth (i.e. channel 2). This scenario emulates a mobile node roaming in an area with three 802.11 hotspots and covered by a GPRS base station. Different home addresses are assigned to the two interfaces. There are 4 base stations spread across the map: *BS(0)* is tuned to channel 1, and *BS(1)*, *BS(2)*, and *BS(3)* tuned to channel 2. The four base stations are connected to a single wired node *W(0)*. In addition, *BS(1)* is the home agent for *Node(0)*.

In the scenario, *Node(0)* is sending a constant bitrate traffic to *Node(1)* using TCP. During the 40 seconds simulation, *Node(0)* moves from *BS(3)* to *BS(1)* at time=5s, to *BS(2)* at time=15s, and finally back to its original position at time=25s. We monitored the received traffic throughput at *Node(1)*, and

plotted the received throughput against simulation time in Fig. 3.

Three different simulations were carried out using the same scenario settings. In the first simulation, *Node(0)* did not employ the tunnel re-establishment technique described in Section V. This effectively means that *Node(0)* would stick with the interface it was using when a transport session first started (in this case, *Node(0)* would always use the interface tuned to channel 2, since the TCP session started when *Node(0)* was within operating range of *BS(3)*, which operated in channel 2). The throughput obtained for this simulation is labeled **Normal** in Fig. 3.

As *Node(0)* moved out of the operating range of *BS(3)*, we see that the throughput dropped to 0 (at time=8s), even though an alternative connection was available with channel 1. The connection was resumed only when *Node(0)* moved within range of *BS(1)*, at time=11s. The same session disruption can be observed for time=18s to 22s, and time=28s to 35s.

In the second simulation, *Node(0)* used the tunnel re-establishment technique described in Section V. This means that *Node(0)* would re-establish the bi-directional tunnel after detecting channel 2 is no longer available. It would do so by using the care-of address of the interface tuned to channel 1 as a care-of address for the interface tuned to channel 2. In this simulation, we assumed there was no layer-2 notifications of channel breakdown, so *Node(0)* can only detect that connection is broken when it can no longer receive router advertisements on the current channel.

The throughput obtained for the second simulation is shown in Fig. 3 labeled **Re-Est**. As we can see, there is a small throughput of 50kbps during the interval of time where a zero throughput was observed in the first simulation (i.e. time=10s to 12s, time=20s to 23s, and time=30s to 35s). This is due to *Node(0)* switching over to channel 1, and re-establishing the bi-directional tunnel with the same home address. However, we still observed a narrow gap of zero throughput during the switch of channels. This is the period when *Node(0)* had just left the operating range of channel 2, and has yet to re-establish the tunnel. During this time period, *Node(0)* was still sending data out to channel 2, until the expiration of a timer for the reception of router advertisements.

For the third simulation, *Node(0)* used predictive re-establishment as described in Section V-D. Here, we pre-programmed the locations of the base stations and the operating range of each channel into *Node(0)* so that *Node(0)* can calculate its distance from a base station thereby deducing if connection is about to break. *Node(0)* changed in advance its current end-point to the care-of address of the interface tuned to channel 1 after deducing the current connection is about to break.

The graph labeled **Pre-Est** in Fig. 3 shows the throughput obtained for the third simulation. Now, we notice that the narrow gaps of zero throughput as observed in the second simulation were eliminated by predictive re-establishment of tunnel. This is indeed a seamless handover, without any special services provided by the base stations.

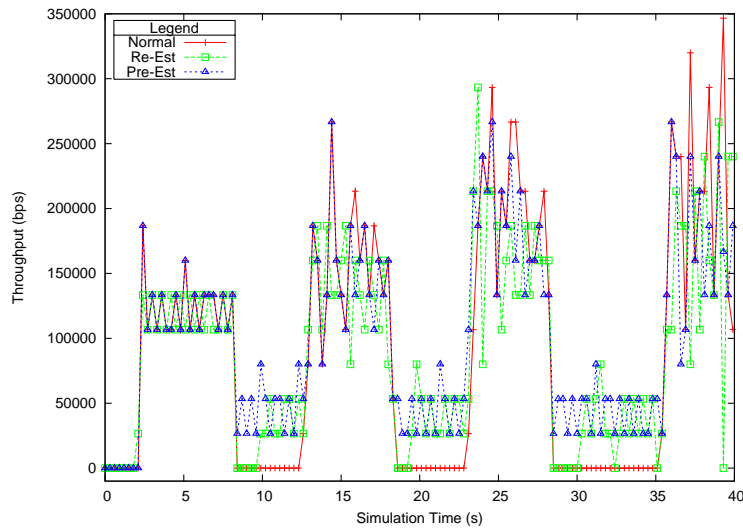


Fig. 3. Comparison of throughputs in 3 simulations.

VII. CONCLUSION

With the advent of wireless technologies, mobile nodes with multiple access interfaces will be a commodity in the near future. This paper explored the benefits of having multiple access interfaces when these nodes employ layer-3 protocols such as Mobile IP or Network Mobility Basic Support to gain persistent access to the Internet while changing their points of attachment to the Internet. Though advantages such as ubiquitous access, seamless handover and fault tolerance are generally desirable, there are issues such as ingress filtering to be addressed before the benefits can be fully enjoyed. A technique for tunnel re-establishment is proposed, and simulation results showed that this technique can be employed to allow mobile nodes ubiquitous access to the Internet, and possibly even to achieve seamless handovers. We will continue to explore other potential issues that might arise in using multiple access interfaces with host and network mobility as our further research focus.

REFERENCES

- [1] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," *IETF RFC 2460*, December 1998.
- [2] D. B. Johnson and C. E. Perkins, "Mobility Support in IPv6," *IETF RFC 3775*, June 2004.
- [3] T. Ernst, K. Mitsuya, and K. Uehara, "Network Mobility from the InternetCAR Perspective," *JOIN: Journal on Interconnection Networks*, September 2003.
- [4] T. Ernst and K. Uehara, "Connecting Automobiles to the Internet," in *ITST: 3rd International Workshop on ITS Telecommunications*, Seoul, South Korea, November 2002.
- [5] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," *IETF Internet Draft: draft-ietf-nemo-basic-support-03.txt*, June 2004, work in progress.
- [6] IETF, "NEMO Working Group Charter," March 2003. [Online]. Available: <http://www.ietf.org/html.charters/nemo-charter.html>
- [7] R. Stemm and R. Katz, "Vertical Handoffs in Wireless Overlay Networks," *Journal on Mobile Networks and Applications*, vol. 3, no. 4, pp. 335–350, 1998.

- [8] T. Ernst, N. Montavont, R. Wakikawa, E. K. Paik, C. W. Ng, and T. Noel, "Goals and Benefits of Multihoming," *IETF Internet Draft: draft-ernst-generic-goals-and-benefits-00.txt*, July 2004, work in progress.
- [9] N. Montavont, R. Wakikawa, T. Ernst, and T. Noel, "Analysis of Multihoming in Mobile IPv6," *IETF Internet Draft: draft-montavont-mobileip-multihoming-pb-statement-01.txt*, July 2004, work in progress.
- [10] R. Wakikawa, K. Uehara, and T. Ernst, "Multiple Care-of Address Registration on Mobile IPv6," *IETF Internet Draft: draft-wakikawa-mobileip-multiplecoa-00.txt*, February 2003, expired.
- [11] T. Ernst and J. Charbon, "Multihoming with NEMO Basic Support," in *First International Conference on Mobile Computing and Ubiquitous Computing (ICMU)*, Yokosuka, Japan, January 2004.
- [12] C. W. Ng, E. K. Paik, and T. Ernst, "Analysis of Multihoming in Network Mobility Support," *IETF Internet Draft: draft-ietf-nemo-multihoming-issues-00.txt*, July 2004, work in progress.
- [13] C. E. Perkins and D. B. Johnson, "Mobility Support in IPv6," in *Proc. of the 2nd Mobile Computing and Networking (MobiCom)*, November 1996, pp. 27–37.
- [14] A. Conta and S. Deering, "Generic Packet Tunneling in IPv6," *IETF RFC 2473*, December 1998.
- [15] T. Ernst and H.-Y. Lach, "Network Mobility Support Terminology," *IETF Internet Draft: draft-ietf-nemo-terminology-01.txt*, February 2004, work in progress.
- [16] T. Ernst, "Network Mobility Support Requirements," *IETF Internet Draft: draft-ietf-nemo-requirements-02.txt*, February 2004, work in progress.
- [17] N. Montavont, T. Ernst, and T. Noel, "Multihoming in Nested Mobile Networks," in *International Symposium on Applications and the Internet - IPv6: Technology and Deployment Workshop*, Tokyo, Japan, January 2004.
- [18] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," *IETF RFC 2827 BCP 38*, May 2000.
- [19] R. Draves, "Default Address Selection for Internet Protocol version 6 (IPv6)," *IETF RFC 3484*, February 2003.
- [20] N. Montavont, T. Noel, and P. Bertin, "Parameters Abstraction to Optimize Mobility Control," *The 6th International Conference on Advance Communication Technology (ICACT 2004)*, February 2004.
- [21] A. Yegin et al., "Supporting Optimized Handover for IP Mobility - Requirements for Underlying Systems," *IETF Internet Draft: draft-manyfolks-l2-mobilereq-02.txt*, February 2003, expired.
- [22] A. Yegin, E. Njedjou, S. Veerepalli, N. Montavont, and T. Noel, "Link-layer Hints for Detecting Network Attachments," *IETF Internet Draft: draft-yegin-dna-l2-hints-01.txt*, February 2004, work in progress.
- [23] K. Fall and K. Varadhan, "NS notes and documentation," The Vint Project, UC Berkeley, LBL, USC/ISI, Xerox PARC, Tech. Rep., 2000, "http://www.isi.edu/nsnam/ns/index.html".