Mobile IP Extension to Ad Hoc Wireless Networks[*]

Li-Hsing Yen[†]
Dept. of Computer Science and Information Engineering
National University of Kaohsiung
Kaohsiung, Taiwan 81148, R.O.C.

Chih-Syuan Jian
Dept. of Computer Science and Information Engineering
Chung Hua University
Hsinchu, Taiwan 30067, R.O.C.

Abstract

Mobile IP has been proposed for providing mobility services for mobile nodes that have direct (fixed or wireless) links to the Internet. In this paper, we consider extending Mobile IP to accommodate mobility support for mobile nodes that are two or more wireless hops away from a fixed infrastructure. Our proposal differs from existing solutions in that we do not use ad hoc routing protocols to relay Mobile IP messages and data packets: standard IP routing is used instead. The advantages of our proposal are (1) Mobile IP foreign agents need not be modified. (2) legacy mobile nodes that do not implement the extension are still able to connect to the fixed infrastructure, and (3) mobile nodes behave the same, no matter they have a direct link to the infrastructure or not. The proposed protocol has been implemented and tested.

Index Terms: Mobile IP, Ad Hoc Networks, Wireless Network, Mobility

---

[*] This work was supported by the National Science Council, Taiwan, under Contract NSC-90-2213-E-216-020

[†] Correspondence author. E-mail: lhyen@ieee.org. Tel: +886-3-5186408, Fax: +886-3-5186416.

1 Introduction

Due to the advance in wireless technology and development of portable computing devices, more and more hosts become mobile, i.e., they can change their points of attachment to the Internet. Mobile IP [8] is an Internet standards-track protocol that enhances the existing Internet Protocol (IP) to accommodate host mobility. In Mobile IP, a special router called mobility agent (MA) maintains location information for mobile hosts. When a mobile node (MN) moves away from its home network, the MA located in MN's home network, or its home agent (HA), will tunnel packets for the MN. Tunneled packets are usually, though not always, handled by the MA on the MN's visiting network called foreign agent (FA). With the intervention of its HA and FA, an MN away from home network can continue its communication with the rest of the Internet.

Mobile ad-hoc wireless networks (MANETs), or multihop wireless networks, have drawn much researcher's attention recently. MANET differs from conventional infrastructured wireless networks in that MANET contains no fixed network devices (e.g., base stations), and therefore all MANET connections are wireless. Due to limited transmission range of wireless signal, other nodes may involve in the routing and forwarding tasks for an end-to-end packet delivery. For this reason, there is no distinction between hosts and routers in MANET. MANET can be setup for command and control purpose in battlefield or for emergency rescue in disaster area.

Mobile IP is intended to support nodes that have a direct wireless or wired link to the Internet. In this paper, we consider extending Mobile IP to hybrid wireless networks, where fixed infrastructure and multihop wireless network coexist. A hybrid wireless network differs from infrastructured or one-hop wireless network in that not all MNs are directly attached to a fixed

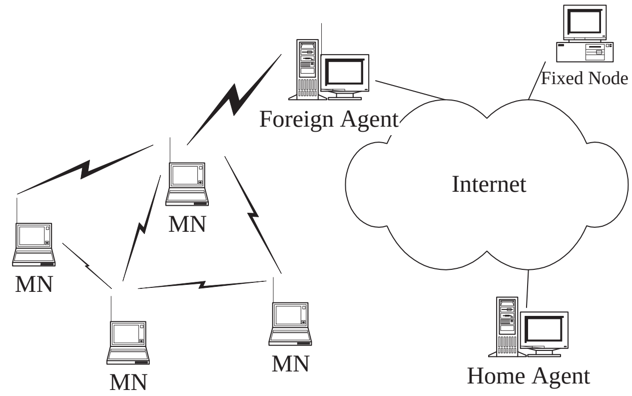


Figure 1: A hybrid wireless network

infrastructure. On the other hand, unlike MANET, not all communication links are wireless in a hybrid network. An example of hybrid wireless network is shown in Figure 1.

As MNs may not have a direct link with a fixed infrastructure, the following issues should be addressed when providing Mobile IP mobility services to all MNs. First, a mechanism is needed to relay packets between the end of the wired infrastructure (which could be an MA or router) and MNs. Up to date, all existing solutions [2, 4, 13, 16, 11, 15, 1, 6] assume the use of an ad hoc routing protocol in the MANET part of the hybrid network. An interworking function is therefore required in MAs or independent gateways. Second, an agent discovery scheme is needed for MNs that have no direct links with FA. Existing designs could be classified into three types: passive [4, 1], active [2], and hybrid [16, 11, 6]. Some schemes offer both options of passive and active approaches [13, 15]. Third, when an MN has a packet to send, the MN must determine a route to the destination. The routing is complicated by the fact that addressing in MANETs is “flat”—hierarchical IP routing is not applicable. Route discovery can be done by consulting the MN’s routing table [15], initiating a route discovery procedure

[2, 4, 13, 11, 6], or other means [2, 1].

All existing approaches assume the use of a MANET routing protocol, implying that MNs must implement two protocol suites (Mobile IP and a MANET routing protocol) to connect to the Internet. This requirement complicates the design of MNs and also imposes a heavy burden on MNs considering their limited storage space and computing power. Our research was motivated by the need not to use a MANET routing protocol in addition to standard IP routing. The proposed approach effectively extends Mobile IP to the whole wireless part of hybrid networks and demonstrates the possibility of not using MANET routing. Unlike the standard IP routing, this method demands no exchange of routing tables or ARP messages between hosts: all associated routing information is automatically and implicitly created as part of the process of delivering Mobile IP messages. The proposed approach also has the advantage of not modifying FAs.

Rest of this paper is organized as follows. Section 2 gives the background of the research and reviews related work. Section 3 describes the protocol in details. In Section 4, we compare the proposed approach with conventional ones and present implementation and experimental results. Section 5 concludes this paper.

2 Background and Related Work

Mobile IP offers two options on care-of address (CoA) which identifies an MN in the visiting network: foreign-agent CoA (FA-CoA) and co-located CoA (CCoA) [8]. If an MN uses an FA-CoA, which is usually an FA's IP address, all tunneled packets will be received and handled by the FA. The FA then delivers the packets to the MN with link-layer transmission, which does not work if the MN has no direct link to the FA. On the other hand, if

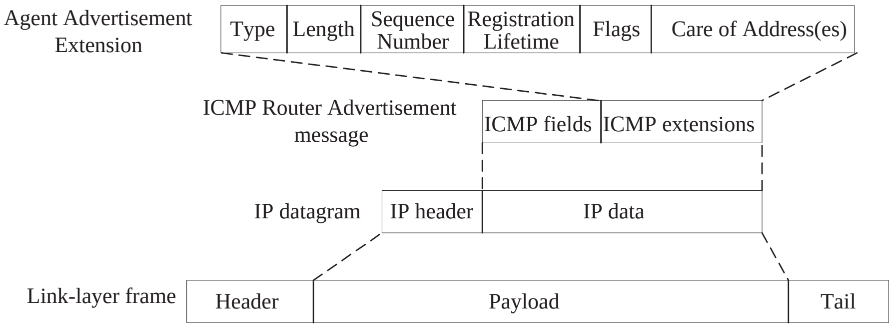


Figure 2: Agent Advertisement message

an MN uses a CCoA, which is a public IP address belonging to the visiting network, all tunneled packets are to be received and handled by the MN itself. However, if the access router (AR) on the visiting network has no direct link with the MN, the AR cannot deliver the packets to the MN with link-layer transmission.

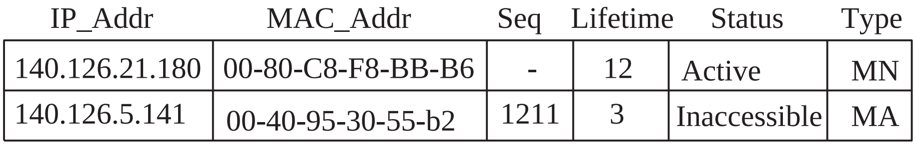
Ad hoc routing protocols are designed to deliver packets between hosts in MANET. Existing ad hoc routing protocols can be classified as table-driven (proactive routing) or on-demand (reactive routing) [12]. A table-driven routing protocol (such as DSDV [7]) attempts to maintain up-to-date routing information in MN's local routing table. On the other hand, on-demand routing protocols (such as DSR [5] or AODV [9]) create routes only when necessary.

As mentioned, all existing solutions assume the use of an ad hoc routing protocol in the MANET part of the hybrid network. These solutions, however, differ in how the following issues are addressed:

- Agent Discovery: This concerns how an MN is aware of the presence of an MA. Mobile IP extends ICMP [3] router discovery procedure by including an Agent Advertisement (*AgentAdv*) Extension in ICMP's Router Advertisement message, as illustrated in Figure 2. When appropriately configured, an MA periodically broadcasts *AgentAdv*. However, only MNs that are located within the MA's direct transmission range can receive the advertisement. There are several ways to let *AgentAdv* reach every MN in the hybrid wireless network. In passive agent discovery schemes [4, 1], an MA periodically broadcasts *AgentAdv* and all MNs receiving the advertisement rebroadcast it. In active agent discovery schemes [2], an MA does not broadcast advertisements periodically. Instead, an MN acquires agent information by broadcasting an AGENT SOLICITATION (*AgentSol*) and getting *AgentAdv* replied by the MA. Some schemes offer both passive and active options [13, 15]. Hybrid approach is also possible, where advertisements are sent only to the nodes within the direct transmission range [16, 6] or are flooded within a limited number of hops [11]. Other nodes acquire advertisements by an active method. Jung et al. [6] proposed using two types of advertisements, one having short lifetime is transmitted to MNs that are one hop away from the FA and the other having long lifetime is flooded to all MNs.

- Route Discovery: In Mobile IP, all MN-originated packets are first forwarded to FAs. In a hybrid wireless network, it is not efficient that all communications are through the FA (such as the scheme in [1] does). When the destination of an MN-originated packet is located within the MANET part, forwarding the packet to the FA and then to the destination inevitably incurs detour overhead. Therefore, when an MN has a packet to send, it should determine whether the destination node is within the ad hoc network or not. The method proposed by Broch et al. [2] demands that the MANET forms a single IP subnet, i.e., all MNs in the MANET share a common subnet address. In this way, whether the destination is located in the MANET can be determined by examining the IP address of the destination. In all other proposals, the IP address of the destination node no longer provides sufficient routing information, as addresses in the ad hoc network are considered “flat”. If a proactive routing protocol (such as DSDV) is used at the ad hoc network, the MN can consult its routing table for a route to the destination [16, 15]. If an on-demand routing protocol (such as DSR or AODV) is used instead [4, 13, 11, 6], the MN uses a route discovery procedure to find a route to the destination. In either way, if a route to the destination can be found, the MN can use ad-hoc routing protocol to deliver the packet. Otherwise, the destination node is assumed to be outside the ad hoc network, and the packet will be routed through the FA to the Internet.

- Move Detection: This concerns whether and when an MN should change its point of attachment to the Internet. Many proposals take hop-count based rule, where an MN registers to a new FA if the MN is at least N hop closer to the new FA than to the old FA. The value of N can be one [6] or two [4, 13, 11]. Some approaches take Euclidean distance between MN and FA as a metric to decide whether MN should change FA or not [15, 1]. Some even considers the load among FAs, trying to achieve load balance [1]. In the scheme proposed by Tseng et al. [15], the time-to-live (TTL) value of Agent Advertisement can be different for different FAs. This approach limits the range of advertisement broadcast, alleviating undesirable broadcast storm problems [14]. However, an MN is not guaranteed to receive advertisements from all reachable FAs.



IP_Addr	MAC_Addr	Seq	Lifetime	Status	Type
140.126.21.180	00-80-C8-F8-BB-B6	-	12	Active	MN
140.126.5.141	00-40-95-30-55-b2	1211	3	Inaccessible	MA

Figure 3: A sample binding cache

In Mobile IP specification [8], a mobile network is defined to be a network that moves as a unit with respect to the Internet. A node within a mobile network called mobile router takes the responsibility for the mobility of the mobile network, i.e., provides connectivity on behalf of other hosts and routers in the mobile network. These hosts and routers may themselves be fixed or mobile with respect to each other and with respect to the mobile router. In case that they are mobile, the mobile router may act as an FA and provide an FA-CoA to them.

Mobility router's functionality is quite complicated. Besides, mobile network has a hierarchical rather than flat architecture, which results in recursively tunneled packets to the destination host and wasting of scarce bandwidth. Most importantly, mobile router scheme is not applicable to cases where hosts' moving directions are diverse, the cases often found in MANETs.

3 The Proposed Scheme

In this section, we propose a scheme dealing with the case that MNs use FA-CoA. Our approach utilizes ARP cache that is used by Address Resolution Protocol (ARP) [10]. Unlike usual treatment, where cache contents are created as a result of making an explicit ARP request and getting the reply, cache contents in our approach are implicitly created and maintained as part of our Mobile IP extension. So ARP message exchange is not required. Our approach also utilizes host-specific routes and default routes. In fact, there is no route to any (sub)network in MN's routing table, as hierarchical IP routing cannot apply to MANETs.

Due to its limited use, the routing table actually can be integrated with ARP cache. We refer to the result of such integration as a *binding cache*. A sample binding cache is shown in Figure 3. When an MN receives a unicast datagram that is not destined for it, the MN looks up the binding cache to find the MAC address to be used for encapsulating the datagram in a data-link frame. If no such entry can be found, instead of submitting an ARP request for the destination's MAC address, the host forwards the datagram with the MAC address that corresponds to its default router, which is one of the MAs it has recognized.

We first introduce a basic scheme based on the assumption that MNs neither move nor disconnect from the network. Then, in Section 3.4, we shall discuss how to extend the basic scheme to deal with mobility and disconnection.

An MA in the following discussions refers to both HA and FA. The functions of a typical FA conform to those of an MA. However, a regular HA must be modified to accommodate the functionality of MA. Implementation details will be presented in the next section.

3.1 Agent Discovery

We offer both active and passive options of agent discovery approaches. The passive agent discovery floods *AgentAdv* over the MANET. Due to the nature of flooding, an MN may have received the same *AgentAdv* for several times, each time from a different neighbor. To avoid a costly "blind flooding", every MN intelligently rebroadcasts only the first received new adver-

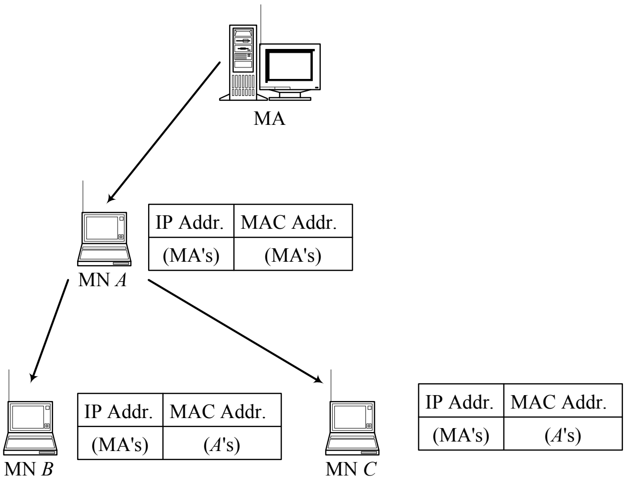


Figure 4: ARP cache contents after flooding AGENT ADVERTISEMENT

tisement. Duplicated and obsolete advertisements, identified by the same or lower sequence number from the same MA, will be discarded. Eventually, every MN will receive MA's new advertisement, provided that it is reachable from the MA.

The flooding of *AgentAdv* also sets up sufficient data-link and network layer information (i.e., address bindings) for MNs to send back packets to the MA. When an MN has recognized an MA (by *AgentAdv*), the MN creates (or updates, if the entry already exists) an entry in its ARP cache that maps the IP address of the MA to the MAC address of the host that forwards this message. In effect, the MAC address of the upstream node is considered that of the MA. Figure 4 shows the contents of every host's ARP cache after flooding *AgentAdv*.

Besides updating ARP cache, every MN also includes the MA's IP address in its routing table as a default route. Therefore, after flooding *AgentAdv*, IP packets issued by any MN will be delivered toward the MA, following a path determined by the link/network layer information that was created on propagating *AgentAdv*. This path is referred to as an upward path. Note that all upward paths together form a sink-tree rooted at the MA, and also that address bindings corresponding to upward paths are constantly refreshed by the MA's periodic flooding of *AgentAdv*.

An MN may optionally initiate active agent discovery by broadcasting *AgentSol*. This is one way by which an MN discovers MAs in case that MAs are configured not to periodically broadcast *AgentAdv*. Every other MN rebroadcasts the first received *AgentSol*, if it has not yet recognized any MA, or forwards the solicitation to its default router, otherwise.

As broadcasts are not synchronized, when a new *AgentAdv* is flooded and firstly arrives at an MN, it may come from a node different from the recorded upstream node. In that case, the MN must not update its address binding for MA provided that it can still receive *AgentAdv* from the recorded upstream node later. This rule avoids unnecessary topology renovation. We can achieve this by exploiting ICMP lifetime setting. Lifetime field in an ICMP message (i.e. *AgentAdv*) specifies the maximum amount of time that the advertisement is considered valid in the absence of further advertisement. We use it here to avoid unnecessary update of address binding for MA, which works as follows.

- When an *AgentAdv* is received and the MN has no recorded address binding for this MA, the MN creates an addressing binding for it, loads a lifetime timer with the value of the lifetime field, and starts the timer.
- If at any time before the lifetime timer expires a new advertisement is received from a different upstream node, the advertisement is ignored.
- If at any time before the lifetime timer expires a new advertisement is received from the same upstream node, the MN loads the lifetime

timer with the value of the lifetime field, and restarts the timer.

- If the lifetime timer expires, the MN removes the associated address binding.

In this way, until the lifetime of the current advertisement expires, advertisement messages received from different upstream node will be ignored.

According to the specification, the TTL field in the IP packet that carries *AgentAdv* or *AgentSol* must be one. MNs should ignore the TTL setting to let *AgentAdv* be broadcast. Alternatively, an MN can set an appropriate TTL value on sending *AgentSol*. The value sets up a maximal hop count between the MN and an MA to which the MN is willing to register.

3.2 Registration

After a roaming MN acquires an FA's information and its CoA from *AgentAdv*, it may issue a REGISTRATION REQUEST (*RegReq*) to inform its HA of the CoA. *RegReq* is to be relayed by the FA. Since the upward path from the MN toward the FA has been established, *RegReq* can be delivered to the FA without difficulty. In addition, any intermediate MN along the path (as well as the FA) receiving *RegReq* creates an ARP cache entry that maps the IP address of the message source to the MAC address of the node that forwards this *RegReq* (the downstream node). In effect, every intermediate MN as well as the FA views the downstream node's MAC address as that of the MN attempting registration. Figure 5 shows the ARP cache contents created on delivering *RegReq*'s from MNs B and C to the mobility agent.

Besides updating ARP cache, every MN and the FA also create in its routing table a host-specific route for the MN from which *RegReq* originates. This route together with ARP cache contents forces subsequent packets destined for the MN to be forwarded to the downstream node.

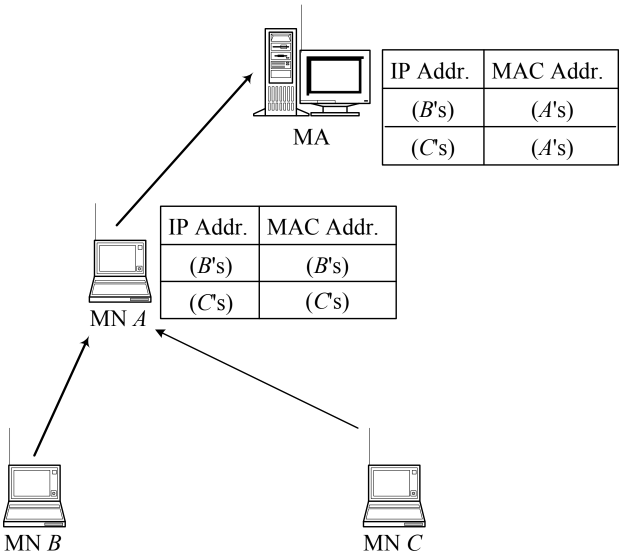


Figure 5: ARP cache contents after delivering *RegReq*'s from B and C.

After *RegReq* has been delivered to FA, all created address bindings have formed a path that suffices to deliver messages (e.g., REGISTRATION REPLY) from the FA to the MN attempting registration. This is referred to as a downward path. After both the upward and downward paths have been created, subsequent datagrams between the FA and the MN can be delivered with standard IP routing.

According to Mobile IP specification, when an MN is reachable from multiple MAs and receives *AgentAdv*'s from different sources, the MN may save all advertisements but selects only one of the MAs to register. After the registration successes, the MN will not register to any other MA as long as the registration lifetime (revealed in *AgentAdv*) does not expire. That is, a new *AgentAdv* does not necessarily cause an MN to change its point of attachment to the Internet.

3.3 Routing

As standard IP routing is used, there is no need to explicitly conduct a route discovery procedure to find a route to the destination. This is in contrast to other work [4, 13, 11, 6]. This scheme neither demands that the MANET forms a single IP subnet [2].

One property of the proposed scheme is that MN-originated packets are not always routed through an MA. The delivery of MN-originated packets is governed by the relative location of the destination. Four cases are possible:

- If the destination is located on the source's upward path toward the MA, the packet delivery will be terminated at the destination.
- If the destination's upward path overlaps with the source's, the MN that locates at the branch point of these two paths will redirect the packet toward the direction of the destination without routing the packet to the MA first (provided that the destination has registered to the same MA).
- If the source and the destination reside in the same MANET (i.e., they have registered to the same MA) but their upward paths do not overlap, the packet will be routed through the MA before it reaches the destination.
- If the destination is some node outside the source's hybrid network, the packet will be routed through the MA before it reaches the destination, as what occurs in original Mobile IP.

Consider the scenario shown in Figure 6 for an illustration. Suppose that MN C has registered to the MA and thus the binding cache in MN A has an entry that maps C's IP address to C's MAC address. If B issues a

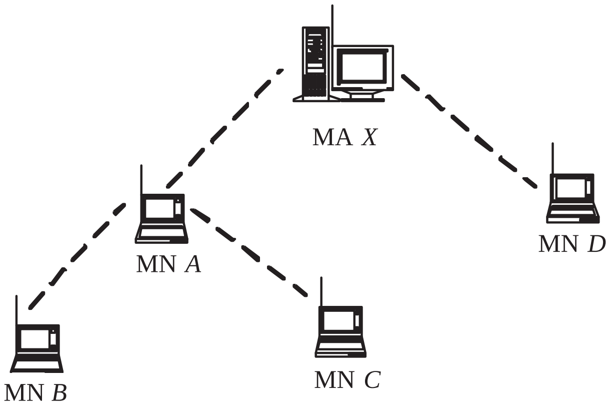


Figure 6: A hybrid network

packet that is destined for A, the packet will be delivered directly to A; if the packet is destined for C, it will be redirected by A to C without being routed through the MA first; if the packet is bounded for D or some node outside this hybrid network, the packet will be routed through the MA before it reaches the destination.

There deserves a note concerning the case that D is the destination. Suppose that D has already registered to the MA. According to the specification, the MA has a record in its visitor list that maps D's IP address to D's MAC address. So by consulting the visitor list, the MA can forward the packet to D directly without first directing the packet to D's HA and then getting the same packet tunneled back by the HA. This route optimization, however, is an implementation issue and has not been specified in Mobile IP.

3.4 Move Detection

When MNs move or disconnect from network, some upward and downward paths may become inaccessible, and the aforementioned scheme will fail. The MA may not be aware of that change. In fact, it considers packets being delivered successfully simply because these packets have been sent to an immediate downstream node. In addition, the destination MN may not be aware of the presence of these packets.

Fortunately, change of network topology or connectivity can be detected by the periodic flooding of *AgentAdv*. When a registered MN no longer receives advertisements from the same upstream node, even if it may still receive advertisements from other upstream nodes, the established downward path from an MA to it must be broken. When the lifetime of the last received advertisement eventually expires, the MN takes one of the following actions, depending on whether it can still receive the same MA's advertisements from other upstream nodes.

- If the MN does not receive the same MA's advertisements from another upstream node after lifetime expires, the MN must change its point of attachment to the Internet. In case that the MN has saved information about other MAs, it may issue *RegReq* toward one of them. Note that all address bindings corresponding to the new upward path have already been created due to the recent propagation of the new MA's advertisement, while processing the registration message will create all needed address bindings for the new downward path. If the MN has no knowledge of any other MA, it must broadcast *AgentSol*, trying to find another valid MA, and execute regular registration procedure accordingly.
- If the MN still receives the same MA's advertisement from a different upstream node after lifetime expires, the MN needs to change its upstream node but not its point of attachment to the Internet (i.e., the MN need not re-register to the same MA). However, the upward and

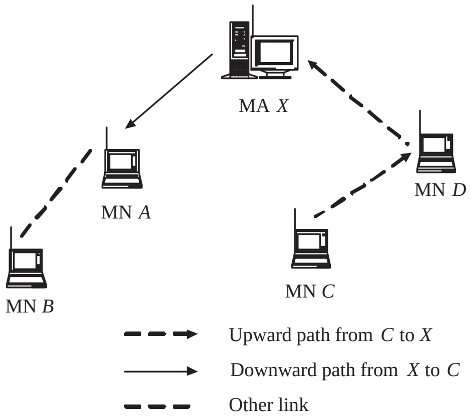


Figure 7: Inconsistent downward and upward paths

> downward paths become inconsistent. While the upward path has been renewed, the downward path is obsolete and needs an explicit renewal.

As an example of the inconsistency between upward and downward paths, consider the scenario shown in Figure 6. If MN C moves toward MN D and the wireless link between MNs A and C is broken, C's lifetime will expire eventually (C ignores advertisements forwarded by D during this period as D is not yet C's upstream node). After that, C changes its upstream node to D. While the upward path from C to the MA has been renewed, the downward path from the MA to C is obsolete and inaccessible (A cannot forward packets to C with C's MAC address). See Figure 7.

The MN initiates the renewal procedure by sending a unicast (rather than a regular broadcast as specified in Mobile IP) *AgentSol* message toward the MA. On receiving this message, every node creates or updates the address binding for the MN, similar to the way that *RegReq*'s are propagated. The issued *AgentSol* hence traverses the upward path, renewing all necessary address bindings for the downward path.

It is possible, though unlikely, that the current paths between a registered

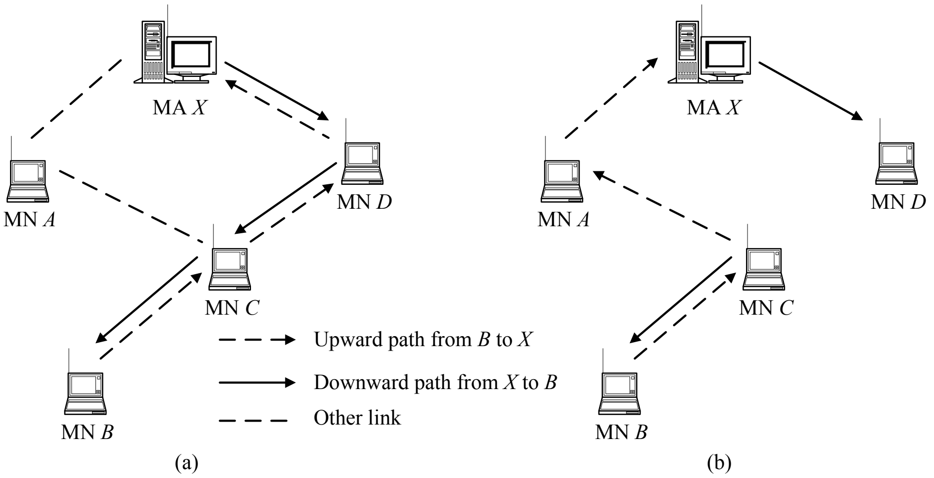


Figure 8: The downward path to MN B

MN and the MA become inaccessible but the advertisement lifetime does not expire, i.e., the MN continuously receives *AgentAdv* from the same upstream node. Consider the initial scenario in Figure 8a. Suppose later the link between MNs D and C is broken, causing the advertisement lifetime at C to expire. C may then receive subsequent advertisements from A and forward them to B before the advertisement lifetime at B expires. Although C will explicitly renew its downward path as it can discover the change of its upstream node, B would not do so since B's upstream node remains the same. Consequently, the downward path to B becomes inaccessible (Figure 8b).

As a remedy, whenever the advertisement lifetime expires at an MN, the MN will hold forwarding subsequent *AgentAdv* for some amount of time. In the previous example, this action would cause the expiration of the advertisement lifetime at B, forcing B to take appropriate action as stated above.

The aforementioned technique is a layer-3 approach, as it is based on the lifetime of *AgentAdv*'s. Unfortunately, an MN cannot use it to determine whether any of its downstream nodes has moved or disconnected. As a consequence, an MN may keep address bindings even for downstream nodes that have already moved away. This problem can be solved if MNs have the ability to detect link breakdown. Many wireless link-layer protocols such as IEEE 802.11 are reliable, implying that a failure in transmitting a frame can be detected. If such an event occurs repeatedly when an MN tries to send a packet to one of its neighbors, the neighbor is no longer considered available, and all information associated with that neighbor can be safely discarded.

4 Discussions and Evaluations

4.1 Qualitative Comparisons

Compared with other work, our solution for extending Mobile IP to hybrid wireless networks has the following advantages.

- The proposed approach need not modify FAs to support MNs that are multiple hops away from FAs. Besides, it needs no infrastructure devices other than MAs. In contrast, other proposals either require additional gateway devices [2, 16, 1, 6] or demand that MA must implement both Mobile IP and a MANET routing protocol [4, 13, 11, 15].

- All previous methods require that MNs must have two protocol suites (Mobile IP and a MANET routing protocol) to function correctly. In the proposed approach, MNs need not implement any MANET routing protocol in addition to the built-in IP routing.

- A legacy MN not implementing the extension is still able to connect to the Internet, provided that the MN has a direct wireless link with the fixed infrastructure. Even there are multiple hops in-between, the legacy MN may still connect to an MA, as long as all in-between MNs have implemented the extension. This is impossible in prior work.

There are, however, some performance issues in our protocol. The first is the cost of flooding *AgentAdv*'s. There are some general guidelines established for alleviating flooding cost [14]. One of the guidelines suggests that MN may selectively re-broadcast received messages (which are, in our case, advertisements). This may not cause problem since Mobile IP's design allows an MN to miss three successive advertisements before the last advertisement's lifetime expires.

One may suspect that, once downward paths have been constructed, the cost can be lowered if *AgentAdv*'s are propagated to every MN by end-to-end unicasts instead of a flooding. However, experimental result [4] has reported that the performance of flooding is better than that of multiple unicasts in propagating AGENT ADVERTISEMENT. The reason may be that flooding utilizes overlapped downward paths while unicasts do not. Flooding of advertisements could also be implemented as a multicast, where all downward paths jointly form a multicast tree. The cost of multicast, however, might not be lower than that of flooding.

Although the proposed approach is feasible, it does not always yield a shortest routing path between sources and destinations. As an example, packets sent from MN B to MN C in Figure 9 follow the upward path from B to MA X then the downward path from X to C. This path is not the shortest one as B in fact can send packets directly to C. However, the proposed approach yields non-optimal routing paths only when destinations reside in the hybrid network, a case of peer-to-peer communications. If optimal routing in such case is a need, MANET routing rather than the

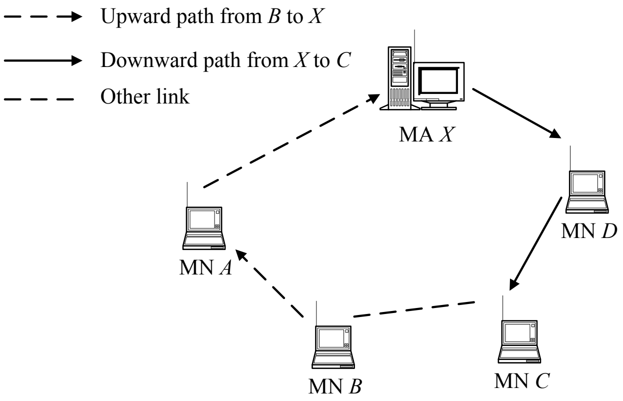


Figure 9: The routing path from B to C is not optimal.

proposed one should be used. If packet traffic is mostly from/to the fixed infrastructure, the proposed routing suffices as little traffic is peer-to-peer.

4.2 The Implementation

We implemented our proposal based on the source codes of Dynamics Mobile IP version 0.8.1 (http://dynamics.sourceforge.net), which was originally developed at Helsinki University of Technology. This software consists of three modules: one for MN, one for HA, and the other for FA. As the functionality of HA is separated with that of FA, both FA and HA modules must be running for a server to function as an MA to conform with Mobile IP specification.

We left the FA module intact and have modified both the MN and HA modules. In Dynamics Mobile IP implementation, an MN at home does not statically cache the MAC address of its HA. Similarly, an HA does not cache MAC addresses of MNs staying at home. Dynamic ARP caching is used instead, where records have a lifetime, and ARP request/reply is needed to acquire information not currently cached. The use of dynamic ARP causes a problem when the MN is two or more hops away from its HA: the HA cannot hear ARP requests issued by the MN and vise versa. For this reason, both the HA and MN modules have been modified so that MNs and HAs always use static ARP caching even when MNs stay at their home networks. This is also the only change to the HA module.

When an MN roams into another network, some of its ARP cache contents and host-specific routes in its routing table may no longer be valid. However, these contents will not disappear over time as they are all statically created. To determine which contents are to be removed to save space is a difficult task. Our current implementation erases these contents as long as it is detected that the MN has returned to its home network.

Other modifications on MN module are outlined as follows.

1. In Dynamics Mobile IP implementation, an MN module creates two ICMP sockets: one for sending *AgentSol* and the other for receiving *AgentAdv*. Our modification demands two additional ICMP sockets in every MN: one is for receiving *AgentSol* from and the other is for forwarding *AgentAdv* to other MNs.

2. After receiving *AgentAdv* but before processing it, the MN resets the TTL field in the IP header to 1 and sets the destination IP address to 255.255.255.255. This is to let the MN rebroadcast *AgentAdv*. Normally, when *AgentAdv* is received and passed on to the MN module, the TTL field has a value of zero and this *AgentAdv* therefore will not be rebroadcast. The change of the destination IP address also serves for the same purpose. The FA may occasionally send *AgentAdv* to an MN as a unicast (in response to an *AgentSol*, for example). If the MN does not change the destination IP address to a broadcast address, the *AgentAdv* will not be rebroadcast.

3. We have included codes that listen to *AgentSol* broadcasted by other

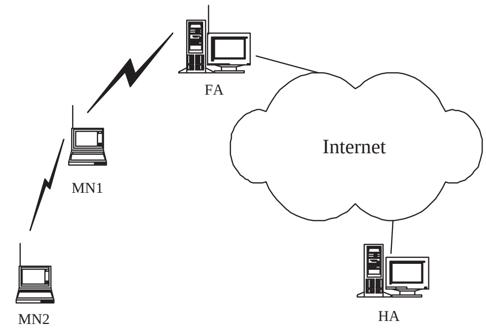


Figure 10: Experiment setup 1: Multihop routing in a visiting network

MNs. When an *AgentSol* issued by MN j is received by MN i, i puts j's IP address into i's routing table as a host-specific route, updates its ARP cache, and then issues a unicast *AgentSol* toward the MA. When a unicast *AgentAdv* that corresponds to the issued *AgentSol* is received by i, i forwards the *AgentAdv* to j.

4.3 Experiments

We also conducted experiments to evaluate the implementation. Four PCs, all installed with Linux kernel 2.4.20-8 (Redhat 9.0), are used in the experiments. These PCs play the roles of MN1, MN2, FA, and HA, respectively. The FA executed the original FA module of Dynamics Mobile IP, while MN1, MN2, and HA ran our modified codes. IP routing function is enabled in FA and HA. We used Iperf (http://dast.nlanr.net/Projects/ Iperf/) to measure UDP throughputs between two hosts. All results were averaged over 10 experiments.

Figure 10 shows the scenario for our first experiment. This is to demonstrate the correctness of our multi-hop routing function in hybrid wireless networks. As expected, both MN1 and MN2 connected to the Internet through the FA in this experiment. We measured the throughputs of MN1 and MN2 by the following three cases of experiments.

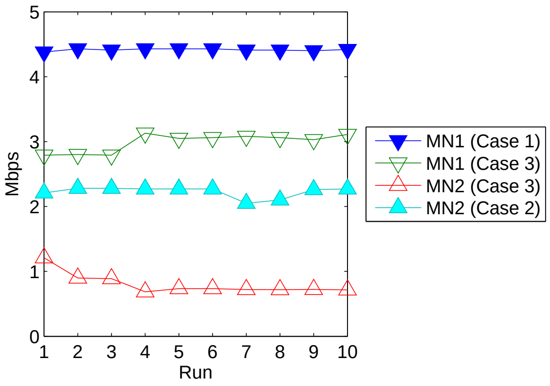


Figure 11: Throughputs with the first experiment setup

1. MN1 alone was tested with Iperf.
2. MN2 alone was tested with Iperf.
3. Both MN1 and MN2 were tested with Iperf.

Figure 11 shows the results. When MN1 alone was tested with Iperf, the average throughput is 4.42 Mbps; when MN2 alone was tested, the average throughput is 2.23 Mbps. In the latter case, MN1 must relay packets for MN2, so MN1 and MN2 contend channel usage. This explains why the throughput of MN2 is only half of that of MN1. When both MN1 and MN2 ran Iperf at the same time, channel contention happened more frequently and the average throughputs of MN1 and MN2 drop to 2.99 Mbps and 0.80 Mbps, respectively.

The next experimental setup follows the first, but MN2 was moved to some place that is within the radio communication range of HA. See Figure 12. MN2 successfully connects to the Internet through HA.

When both MN1 and MN2 were at home and MN2 was two hops away from HA, MN2 cannot connect to the Internet if HA ran the original HA module. With our modified HA module, HA successfully provided Internet

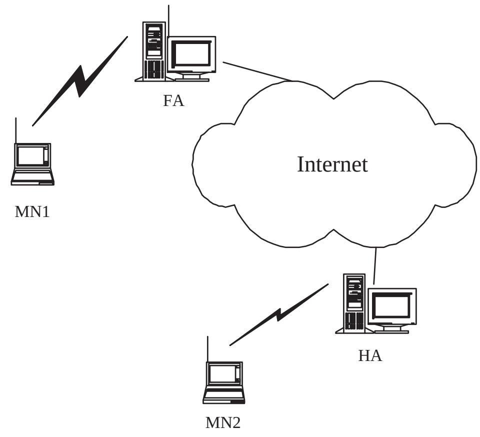


Figure 12: Experiment setup 2: MN2 returns home.

connectivity to MN2.

We also measured the performance impact of IP forwarding on throughput. We first placed MN2 in some place so that the distance between MN2 and FA is maximized while MN2 can still receive FA's advertisements. The measured UDP throughput from MN2 to FA was 3.53 Mbps on average. We then placed MN1 between FA and MN2 and moved MN2 further away from FA so that all traffic between FA and MN2 must now go through MN1. We found that the average throughput from MN2 to FA drops to 2.23 Mbps, a 36.8% performance degradation. See Figure 13. The results suggest that multi-hop transmissions should be avoided whenever a direct link can be utilized.

There are still some issues in our current implementation. First, the rule for avoiding unnecessary address binding update (Sec. 3.1) has not been implemented. As a result, an MN updates its address binding for an MA every time it receives the MA's *AgentAdv*. Second, we have not implemented any link-down detection technique. Consequently, an MN may keep address bindings even for downstream nodes that have already moved away. This wastes storage space but does not affect the functionality of our

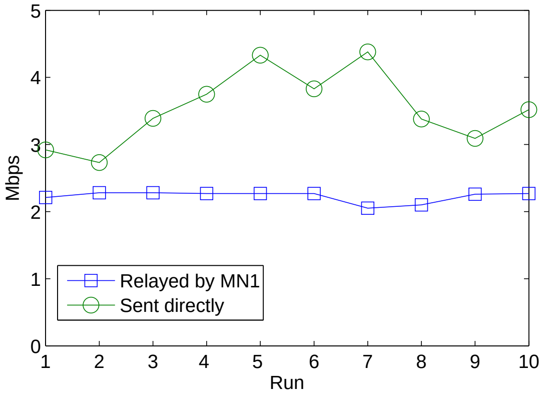


Figure 13: MN2's throughputs with and without the relay of MN1

implementation.

5 Conclusions

We have extended Mobile IP to accommodate mobility support for mobile nodes that are two or more wireless hops away from a fixed infrastructure. Unlike prior work, our extension does not employ any ad hoc routing protocols to relay Mobile IP messages and data packets. Instead, standard IP routing is used. Our approach utilizes ARP cache but ARP message exchanges are not needed. The cache contents are implicitly created and maintained as part of our Mobile IP extension. Our approach also utilizes host-specific routes and default routes in IP routing.

The advantages of our proposal are (1) Mobile IP foreign agents need not be modified, (2) legacy mobile nodes that do not implement the extension may be able to connect to the fixed infrastructure, and (3) mobile nodes behave the same, no matter they have a direct link to the infrastructure or not. The drawbacks of our protocol include the cost of flooding advertisements and the lack of an automatic way to clean up obsolete routes and cache contents.

References

[1] Habib Ammari and Hesham El-Rewini. Integration of mobile ad hoc networks and the Internet using mobile gateways. In *Proc. 18th Int'l Parallel and Distributed Processing Symposium*, 2004.

[2] Jose Broch, David A. Maltz, and David B. Johnson. Supporting hierarchy and heterogeneous interfaces in multi-hop wireless ad hoc networks. In *Proc. of Fourth International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN'99)*, pages 370–375, Los Alamitos, CA, USA, 1999.

[3] S. Deering. ICMP router discovery messages. Technical Report RFC 1256, IETF, September 1991.

[4] Ulf Jönsson, Fredrik Alriksson, Tony Larsson, Per Johansson, and Gerald Q. Maguire Jr. MIPMANET: Mobile IP for mobile ad hoc networks. In *Proc. of First Annual Workshop on Mobile and Ad Hoc Networking and Computing*, pages 75–85, Boston, Massachusetts, USA, August 2000.

[5] David B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. In Tomasz Imieliński and Henry F. Korth, editors, *Mobile Computing*, pages 153–181. Kluwer Academic Publishers, 1996.

[6] Jin-Woo Jung, Doug Montgomery, Kyungshik Lim, and Hyun-Kook Kahng. Dynamic agent advertisement of Mobile IP to provide connectivity between ad hoc networks and Internet. In H.-K. Kahng and S. Goto, editors, *Lecture Notes in Computer Science 3090*, pages 277–286. Springer-Verlag, 2004.

[7] C. E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing for mobile computers. In *ACM SIGCOMM Symposium on Communication, Architectures and Protocols*, pages 234–244, September 1994.

[8] Charles Perkins. IP mobility support. Technical Report RFC 2002, IETF, October 1996.

[9] Charles E. Perkins and Elizabeth M. Royer. Ad-hoc on-demand distance vector routing. In *Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications*, pages 90–100, Los Alamitos, California, USA, February 1999.

[10] David C. Plummer. An ethernet address resolution protocol. Technical Report RFC 826, IETF, November 1982.

[11] Prashant Ratanchandani and Robin Kravets. A hybrid approach to Internet connectivity for mobile ad hoc networks. In *IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1522–1527, 2003.

[12] Elizabeth M. Royer and Chai-Keong Toh. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Commun. Magazine*, pages 46–55, April 1999.

[13] Yuan Sun, Elizabeth M. Belding-Royer, and Charles E. Perkins. Internet connectivity for ad hoc mobile networks. *International Journal of Wireless Information Networks*, 9(2):75–88, 2002.

[14] Yu-Chee Tseng, Sze-Yao Ni, Yuh-Shyan Chen, and Jang-Ping Sheu. The broadcast storm problem in a mobile ad-hoc network. *Wireless Networks*, 8(2):153–167, March 2002.

[15] Yu-Chee Tseng, Chia-Ching Shen, and Wen-Tsuen Chen. Mobile IP and ad hoc networks: An integration and implementation experience. *IEEE Computer*, 36(5):48–55, May 2003.

[16] Jin Xi and Christian Bettstetter. Wireless multi-hop Internet access: Gateway discovery, routing, and addressing. In *Proc. World Wireless Congress*, San Francisco, USA, 2002.