Mobile IP and Ad Hoc Networks: An Integration and Implementation Experience

Yu-Chee Tseng†, Chia-Ching Shen†, and Wen-Tsuen Chen‡
†Department of Computer Science and Information Engineering
National Chiao Tung University
Hsin-Chu, 30050, Taiwan
Email: {yctseng, jcsheen}@csie.nctu.edu.tw
‡Department of Computer Science
National Tsing Hua University
Hsin-Chu, 30050, Taiwan
Email: wtchen@cs.nthu.edu.tw

***Abstract*—*Mobile IP* has been widely accepted as a standard to support IP mobility in a wireless Internet environment to keep a session connected when a mobile host roams from subnet to subnet. Another emerging wireless network architecture that is gaining more and more popularity is the *mobile ad hoc network (MANET)*, which can be flexibly deployed in almost any environment without the need of infrastructure base stations. In order to move to an all-IP environment, there seems to be a growing demand to integrate these two architectures together.**

Typically, mobile hosts are served by access points that can connect to them directly (in one hop). In this paper, we propose to extend access points to multiple MANETs, each as a subnet of the Internet, and discuss how to support Mobile IP in such environment. Such integration is beneficial to both societies. From Mobile IP's prospective, Foreign Agents' service areas are not limited to hosts within a single (wireless) hop any more. From MANET's prospective, mobile hosts can immediately enjoy tremendous services already existing on the Internet through Mobile IP. This article reports our integration and implementation experience based on IEEE 802.11b wireless LANs. Issues such as overlapping of MANETs, dynamic adjustment of mobile agents' service coverages, support of local broadcast and various communication scenarios are addressed. Discussion also covers required adjustments of Mobile IP to support such architecture.

***Index Terms*— ad hoc network, mobile computing, Mobile IP, mobility management, routing, wireless Internet.**

I. Introduction

Wireless communications and mobile computing are gaining more popularity in recent years. Wireless communication devices have become standard features in most portable computing devices, such as laptops, PDAs, and handsets. People are becoming used to carrying computers while traveling around to enjoy the tremendous services on the Internet. Ubiquitous computing has added a new feature, *mobility*, to the world of computing and communications.

We have observed two strong growths of interests related to this trend. The first one is Mobile IP [15], which supports mobile hosts roaming from subnet to subnet without need of changing IP addresses. Mobile (home and foreign) agents are used to support seamless handoffs. The next generation IPv6 will include features of Mobile IP as inherent functionality. Another emerging wireless network architecture is the *mobile ad hoc network (MANET)*, which can be flexibly and conveniently deployed in almost any environment without the need of infrastructure base stations. MANETs have received intensive attentions recently [6], [11], [18], [20]. In the literature, most works are based on IEEE 802.11-like network interface cards to build a MANET. The recently proposed wireless sensor networks also have a similar architecture to the ad hoc networks.

In the trend of moving to an all-IP environment, there seems to be growing demand to integrate these two architectures together. In this paper, we propose to extend the typical *wireless access points* to multiple MANETs, each as a subnet of the Internet, and discuss how to support Mobile IP in such environment. Such integration is beneficial to both societies. From Mobile IP's prospective, Foreign Agents' service areas are not limited to hosts within a single wireless hop any more. From MANET's prospective, mobile hosts can immediately enjoy tremendous services already existing on the Internet without worrying about disconnection due to mobility. With such combination, macro mobility is supported by the former, while micro mobility is supported by the latter.

This article reports our integration and implementation experience based on IEEE 802.11b wireless LANs. Various routing scenarios involving Mobile IP and MANET are discussed. One fuzzy area is the possibility of some MANETs overlapping with each other to form a larger MANET (which is sometimes inevitable), making the service boundaries of home/foreign agents vague. The dynamics of MANETs also necessitates redefining the service coverage of AGENT_ADVERTISEMENT and AGENT_SOLICITATION messages in Mobile IP so as to adapt to constant topology changes of MANETs. The support of local broadcast and various communication scenarios and issues like TTL, ARP, and registration, are addressed. Discussions also cover required adjustments of Mobile IP to support such architecture.

II. Preliminaries

A. Mobile Ad Hoc Networks (MANETs)

A MANET is a network consisting of a set of mobile hosts which may communicate with one another and roam around at their will. A routing path may consist of a sequence of wireless links without passing base stations (i.e., in a *multi-hop* manner). This requires each mobile host to serve as a router. Applications of MANETs occur in situations like battlefields, outdoor assemblies, and emergency rescues, where base stations or fixed network infrastructures are not available, but networks need to be deployed immediately.

Extensive efforts have been devoted to the routing issues on MANET. Routing protocols can be classified as *proactive* and *reactive*. A proactive protocol (such as the DSDV protocol [12]) constantly updates routing information so as to maintain a (close to) global view on the network topology. On the contrary, a reactive protocol searches for a path in an on-demand manner. This may be less costly than a proactive protocol when host mobility is high. Representative reactive protocols include DSR [5], ZRP [3], CBR [4], and AODV [11]. A review of unicast routing protocols for MANET is in [18]. Multicast is studied in [1], [2]. Broadcasting issues are studied in [7], [8], [9].

B. Mobile IP

The Mobile IP is defined by IETF to support IP mobility [15]. Transparent to TCP and UDP, it allows sessions to remain connected when mobile hosts roam from subnet to subnet without the need of changing IP addresses.

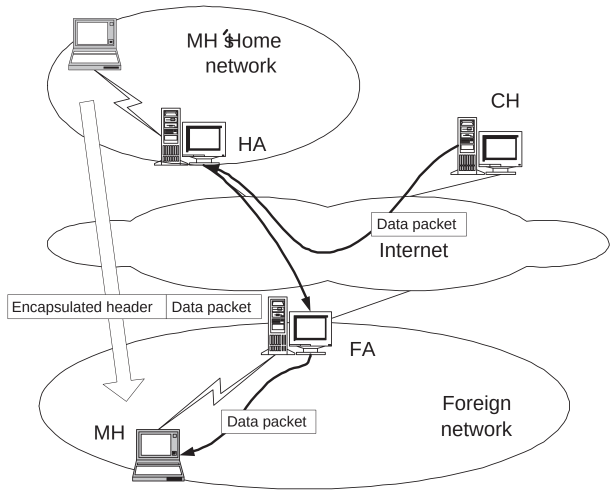

Fig. 1. The transmission scenario of Mobile IP.

Four roles are defined in Mobile IP: mobile host (MH), corresponding host (CH), home agent (HA), and foreign agent (FA), as illustrated in Fig. 1. A MH is a host or a router that may change its point of attachment from subnet to subnet. When a CH, which is a host in the Internet, sends an IP datagram to a MH, it will be delivered to the MH's home network. When the MH is away from home, the datagram will be *tunneled* to the foreign network. The HA will encapsulate the datagram with an IP header carrying FA's IP address or the MH's co-located CoA (care-of-address). In case of using FA's address, the FA should de-capsulate the datagram and forward it to MH. CoA can be dynamically obtained as a temporary address, through such as DHCP address configuration procedure. If the co-located CoA is used, the MH itself serves as the endpoint of the tunnel and performs decapsulation locally. In our implementation, we follow the former solution.

HA and FA need to advertise their services by periodically sending AGENT_ADVERTISEMENT. A MH unaware of any local mobile agent may inquire by sending AGENT_SOLICITATION. From time to time, MH needs to register with its HA its current CoA. HA keeps track of the mapping between each residential MH's permanent address and its CoA in a location dictionary (LD). Further extensions of Mobile IP also exist, such as smooth handoff [14] and extension for IPv6 [16].

C. Related Work

Cellular IP [21] and HAWAII [17] are two Internet protocols to support IP mobility. Cellular IP separates *macro* mobility from *micro* mobility. Originally, mobile IP is to support macro mobility. To reduce frequent registrations to HA as a MH is roaming around, Cellular IP adopts a hierarchical approach. A FA can provide services to multiple base stations. As long as a MH is covered by base stations belonging to the same FA, no re-registration is required. In this case, handoff delay may be significantly reduced. As such, micro mobility to support seamless handoff is achieved. HAWAII (Handoff-Aware Wireless Access Internet Infrastructure) adopts a domain-based approach to support mobility. Base stations can be connected as a tree. It uses specialized path setup schemes which install host-based forwarding entries in specific routers to support intra-domain routing. This results in the same advantage of supporting micro mobility and fast handoff as in Cellular IP. Compared to Cellular IP, HAWAII breaks the tie between gateway and FA, and thus is more tolerant to failure of gateways and simplifies the design of gateways.

References [10], [13] also address the construction of MANET by providing continuous Internet access based on Mobile IP. How to extend Mobile IP to allow MHs to use CoA even if they are more than one hop away from FAs is addressed. The conflict between the management of routing tables in Mobile IP and MANET is resolved. Implementations on both OS/2 and AIX are reported. In particular, two separate daemons are used by Mobile IP and MANET. To coordinate these two daemons, a route manager is used to control the system's routing table.

Compared to [21], [17], our network architecture does not rely on hierarchical (wireline) routers. Instead, following the basic idea of ad hoc networks, mobile hosts are used as routers to extend the coverage of FAs. Thus, our framework also support micro mobility as well as macro mobility. While Cellular IP and HAWAII restrict mobile hosts be resident in one (wireless) hop from the base stations, our framework allows mobile hosts in multiple (wireless) hops from the base station. Also, our work is compatible with current design of MANET, thus easily extending MANET for IP mobility support. In addition, since the topologies of MANETs may change dynamically, the service ranges of FAs may also change accordingly. An advantage is a higher fault-tolerant capability — if one FA crashes, a mobile host may rely on MANET's routing capability to connect to neighboring FAs. Compared to [10], [13], which considers only one single MANET, we consider the existence of multiple MANETs in a vicinity area. Specified by the local FA, the service range of a FA may be dynamically adjusted. Negotiation between mobile agents and mobile hosts on FAs' service ranges is possible. This may greatly improve the flexibility of MANETs and reduce the service overhead of mobile agents. Also, MANETs may overlap with each other, and thus can support each other and offer a higher fault-tolerant capability in terms of Internet access. Further, to enjoy the flexibility of MANETs, direct communications between hosts under two FA's coverages, through MANETs' links, are possible.

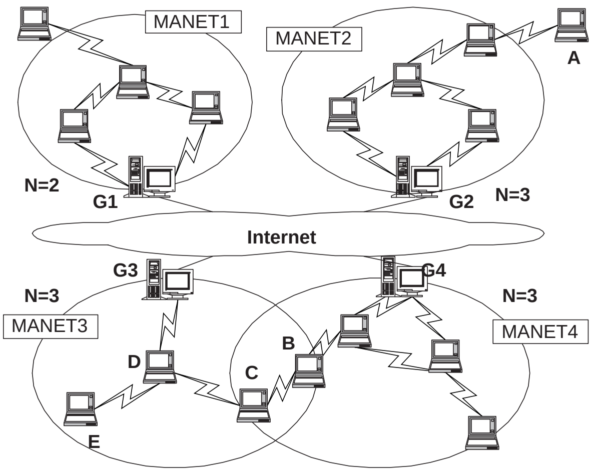

Fig. 2. The proposed network architecture, which extends each access point to a MANET.

III. Network Architecture and Communication Scenarios

A. Network Model

We consider the network consisting of multiple MANETs, each of which has a point of attachment to the backbone Internet. The host connecting a MANET to the Internet is called the *gateway*. We use gateways to define the ranges of MANETs. Each gateway has two network interface cards (NICs), one wireless and one wireline. Gateway hosts have no mobility since they have fixed links. However, non-gateway hosts can roam around freely, and thus the definition of MANETs actually changes by time. Several MANETs are shown in Fig. 2. Gateways are responsible of intertworking MANETs with the Internet by forwarding/relaying packets. To support Mobile IP, each gateway also serves as the FA in its local MANET. So it should periodically broadcast AGENT_ADVERTISEMENT messages to announce its service to members of its MANET. (In our discussion, we may interchangeably use gateway and FA according to the context.)

Since members of MANETs are mobile, it is likely that a MANET is partitioned into multiple MANETs, or some MANETs may join and overlap with each other. In such cases, the boundaries between MANETs become vague, making the service ranges of FAs unclear. We propose to define the service ranges of gateways by associating with each gateway a parameter N. Any mobile host within N wireless hops from the gateway can join the MANET served by the gateway. This is achieved by specifying a TTL = N in each gateway's AGENT_ADVERTISEMENT. For example, in Fig. 2, host A, though connected to MANET2, can not be a part of the network.

In case that a host is within the service ranges of multiple gateways, it can choose the shortest-distance one as its default gateway. By so doing, the boundaries of subnets are clearly defined even if MANETs are overlapping with each another. For example, in Fig. 2, host C belongs to MANET3, while host B belongs to MANET4, and their HAs will tunnel IP datagrams accordingly from the proper gateways. Also, note that each gateway can define its own N independently based on its willingness/capability to provide services.

When MHs move around, it is even possible that a MH is disconnected from its gateway, but still remains connected to other MANETs. For instance, in Fig. 2, if the link between G3 and D breaks, hosts D's and E's connections to the Internet will become broken because they are beyond the service range of G4. To dynamically adjust a gateway's service range, we propose that a MH, on missing AGENT_ADVERTISEMENT for a certain period, may broadcast or multicast an AGENT_SOLICITATION message with a TTL = N'. The value of N' can be gradually increased to avoid the *broadcast storm* problem [7] caused by flooding. The solicitation can be heard if $N' \geq N$ and the MANET is connected. On receiving the AGENT_SOLICITATION, the gateway may decide, based on its willingness, whether to increase its N or not. In the above example, if host E's AGENT_SOLICITATION has an $N' = 5$, G4 will receive the request, and may increase its service range to cover D and E.

B. Some Communication Scenarios

Based on the above network architecture, several different communication scenarios may exist. In the following, we discuss the possible combinations and the corresponding routings. In the discussion, we assume that routing in MANETs is supported by DSDV (however, any proper routing protocol for MANETs is applicable).

- *Intra-MANET communication:* The communications are supported by DSDV. In the DSDV protocol, hosts will exchange routing information periodically and compute the next hop to reach the destination with the least metric (such as hop count). Proper route entries will be written into the kernel routing table by system calls. So whenever a route entry leading to the destination is found, the packet is directly forwarded to the next hop. The transmission from A to B in Fig. 3 fits into this category.

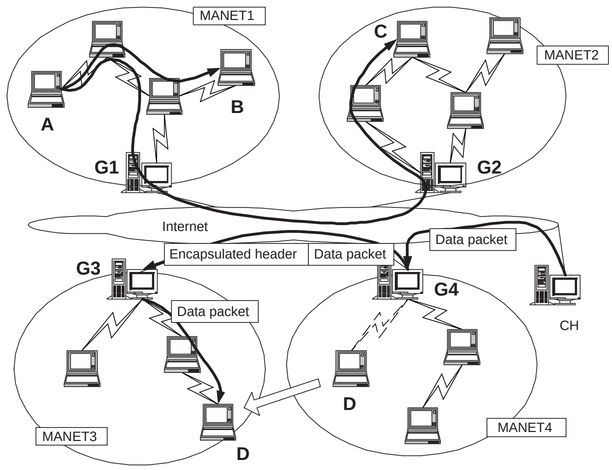

Fig. 3. Intra- and inter-MANET routing scenarios.

- *Inter-MANET communication (direct):* For any packet whose destination is not listed in the kernel routing table, it will be forwarded to the gateway of the local MANET. The gateway will then forward the packet to the Internet. The transmission from A to C in Fig. 3 is such an example. Packets travel on MANET1 based on DSDV, then on the Internet to G2 based on IP routing, and then on MANET2 to B by DSDV again.
- *Inter-MANET communication (with Mobile IP):* A MH may roam away from its home network. In this case, Mobile IP will be involved to forward packets between MANETs. In the transmission from CH to D in Fig. 3, packets will arrive at G4 by IP routing. These packets will be encapsulated and tunneled, by Mobile IP, to G3, which will then forward them to D by DSDV.

  To support such scenario, MHs have to monitor any existing AGENT_ADVERTISEMENT. Registration and deregistration procedures in Mobile IP should be followed. The routing of these packets will be supported by DSDV. HAs should maintain the current locations of its MHs. FAs should maintain the visiting MHs in their MANETs. HAs should execute proxy ARP for roaming MHs.
- *Inter-MANET communication in overlaid MANETs (direct):* When two MANETs overlay with each other, a MH may be aware of a route to another MH that belongs to a neighboring MANET. This is made possible by the frequent exchange of routing information by DSDV. In this case, directly routing between these MANETs is allowed. For example, in Fig. 4, since A has a route entry leading to B, direct inter-MANET transmission is possible.

  To support such scenario, we propose to associate

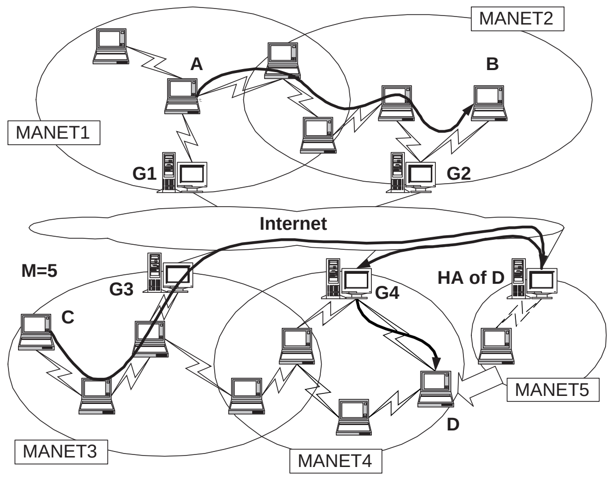

Fig. 4. Inter-MANET routing scenarios in overlaid MANETs.

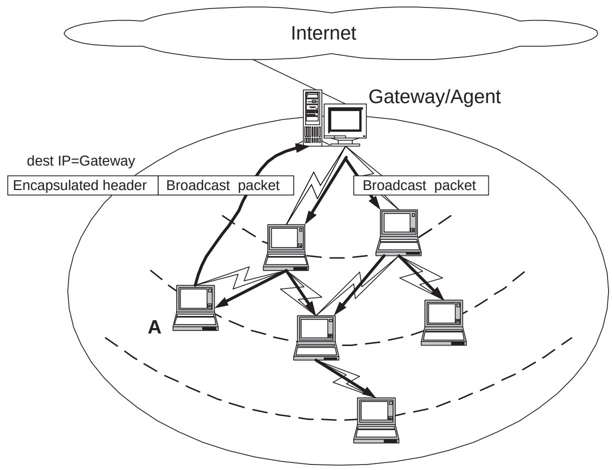

Fig. 5. Routing scenario of broadcasting.

with DSDV a parameter M, which reflects the service range of DSDV. I.e., a MH always collects/propagates routing information for MHs that are within M wireless hops from itself. As a result, hosts in different, but connected, MANETs may communicate with each other directly. The routing, tunneling, and encapsulating overheads can be reduced by such optimization. Note that it is mandatory that $M \geq N$ so that routing information leading to the local gateway is always known by a MH.

- *Inter-MANET communication in overlaid MANETs (with Mobile IP):* Contrary to the above scenario, when two MHs are resident in connected MANETs but away by more than M hops, their communications should be routed through the Internet. In the transmission from C to D in Fig. 4, assuming $M = 5$, host C will not be aware of any route (although existing) leading to D. In this case, its IP datagrams will be forwarded to the local gateway G3 (by DSDV), which will in turn forward the datagrams to D's HA (by IP routing), which will encapsulate the datagrams to D's current FA (by Mobile IP), which will forward the datagrams to D (by DSDV). As can be expected, the values of N and M should be properly tuned to reduce overheads and improve efficiency, which may be directed to an interesting research problem.
- *Broadcast:* Broadcasting is useful in many circumstances. In wireline communication, the scope of broadcast is well defined — a broadcast message is typically flooded to the physical range covered by a subnet. In wireless communication, due to the radio transmission property, the range that should be covered by a broadcast is usually not well defined. This is particularly true for ad hoc networks, where each MH has its own radio coverage. Note that if we directly adopt a TTL value to a broadcast packet, each mobile host's broadcast range will be distinct (depending on its current location).
  We propose to define the coverage range of a broadcast as the service range provided by the local gateway where the broadcast is issued. As a result, the range of a subnet matches with the range of a MANET. The detailed routing is conducted as follows. When a MH wants to send a broadcast datagram, it first encapsulates the packet as a unicast by identifying the gateway as the destination host. When the unicast packet is tunneled to the gateway, the gateway will decapsulate the packet and find that it is a broadcast packet. Then the gateway broadcasts this packet on behalf of the original source with a TTL = N. For example, Fig. 5 shows how A's broadcast datagram flows. Note that to detect duplicate broadcasts, each MH should maintain a list of broadcast IDs that it has received recently. The "source IP address" and the "IP identification" fields in the IP header can serve as a unique identity.

IV. Integration and Implementation Issues

Based on the proposed network architecture, we have developed a prototype which integrates Mobile IP and MANET together. Below, we report our integration and implementation experiences. The following modifications are required:

- *TTL in IP Packets:* Each IP datagram has a TTL field to control its lifetime on the Internet. In the original Mobile IP, each AGENT_ADVERTISEMENT should have TTL = 1. We dynamically tune TTL to control our AGENT_ADVERTISEMENT, AGEN_SOLICITATION, and broadcast packets.

- *Routing inside MANET:* Our implementation is based on the DSDV protocol [12]. Each host maintains a *forwarding table* containing a list of all available destinations together with the next hop leading to each destination. This forwarding table is used to update the kernel's routing table. Control packets are used to exchanges distance vectors between neighboring hosts. Each route entry is tagged with a sequence number originated by the destination host. These control packets have a destination address of 224.0.0.1 (all-systems multicast address) with TTL = 1 because they need not to be rebroadcast.
  In our protocol, several modifications are required. First, since we allow MANETs to overlap with each other, to avoid the amount of information being exchanged becoming too large, only route information that is within M hops is registered and propagated. Second, recall that M should be at least as large as N used by the local gateway; the value of N should be broadcast together with the gateway's control packets. Third, each gateway should identify itself as a gateway by associating a gateway bit in its control packets. Each MH should set its *default router* to be the host that leads to the gateway host with the least metric. Forth, if a MH also has a CoA, it has to advertise through DSDV's control packets its original IP address as well as its CoA. This is similar to having two IP addresses by a host. This can be easily achieved by providing two entries in the control packets. So the MH can be reached both by its permanent IP address directly (in the MANET sense) and by its CoA (in the Mobile IP sense).
- *Agent Advertisement:* In the original Mobile IP, AGENT_ADVERTISMENT has TTL = 1. Due to the multi-hop nature of MANETs, the TTL should be set to N, and the value is decreased by one each time it is rebroadcast. No rebroadcast is needed when TTL = 0. The destination field should be 255.255.255.255.
- *Agent Solicitation:* A MH can multicast AGENT_SOLICITATION to find a nearby mobile agent. The destination field should be the all-routers multicast address 224.0.0.2. We recommend that its TTL field be doubled each time when the solicitation process fails. Intuitively, doubling the TTL can reach approximately four times the hosts that can be reached in the previous round. In addition, since the value of TTL will be decreased as the packet travels more hops, the original TTL value should be recorded in the packet's payload so that when the gateway receives the packet, it can recover its distance to the requesting MH. By comparing this value to N, the gateway can decide whether it needs to enlarge its service range N or not.
- *ARP:* In the original Mobile IP, ARP should be disabled when a MH visits a foreign network. The MAC-to-IP address mapping is registered when AGENT_ADVERTISEMENT is received. Under our network architecture, to allow peer-to-peer communication inside a MANET, ARP still needs to be enabled in foreign networks. ARP requests and replies should be sent as usual. Since many nomadic hosts may exist in a MANET, the concept of subnet mask should not be used and packets of any destination should be relayed.
- *Broadcast:* We design a broadcast daemon to support the scenario in Fig. 5. Whenever a broadcast datagram with destination address = 255.255.255.255 and TTL = 1, source address = myself is intercepted, the daemon will encapsulate this packet as a unicast destined for the local gateway. On receiving the packet, the gateway will decapsulate and broadcast it with TTL = N. However, one potential problem is that the broadcast datagram may loop back to the source host. To resolve this problem, the broadcast daemon should also record the recent broadcast datagrams that it has encapsulated recently.
- *Destination address and TTL:* Recall that the M used by MANETs should be at least as large as N used by Mobile IP. By adjusting M and N, we can control the amount of traffic flowing into and out of a MANET. We recommend that $M = 2N$, which guarantees that intra-MANET communication can always be done directly without encapsulation (in the worst case, an intra-MANET packet may need to be sent to the gateway first and then forwarded to the destination). Also, inter-MANET communication between nearby MANETs are likely to be done without going through Mobile IP (and thus the encapsulation procedure).
- *Configuration of IEEE 802.11b NICs:* In our implementation, all wireless NICs are set to the peer-to-peer (ad hoc) mode. All mobile hosts use the same ESSID and the same channel number so as to communicate with each other. To increase channel reuse (and thus communication bandwidth), it is possible that FAs can use different channels. In most current products, a NIC will automatically scan the available channels only when its current connection is broken (i.e., active scanning). So a host may not be able to discover all its neighbors if they are operating at different channels. Under our framework, the network should function correctly, except that some

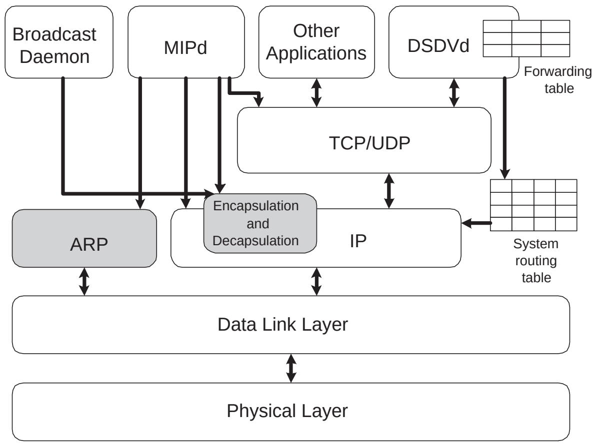

Fig. 6. System architecture of our implementation.

routes may not exist even if some hosts are physically neighbors.

Our system is developed based on Linux Redhat 2.2.16. Two daemons, namely *DSDVd* and *MIPd*, are implemented. Conceptually, both daemons are network-layer programs. However, they are actually implemented on the application layer and interact with system kernel through socket interfaces. The concept is shown in Fig. 6. *DSDVd* periodically multicast UDP packets to help maintain hosts' forwarding tables. Proper entries from the forwarding table are written into the kernel's routing table by system calls. In *MIPd*, we use RAW sockets for advertisement, encapsulation, and decapsulation, and normal sockets for registration. Proxy ARP is done by UNIX system calls. Also, the IP forwarding option at each mobile host must be turned on.

V. CONCLUSIONS

In this paper, we have investigated the related issues to integrate MANETs with Mobile IP. Hence, traditional access points can directly enjoy the flexibility of MANETs and widen their coverage ranges. In view of the worldwide explosive deployments of IEEE 802.11-based access points, such extension would help make our dream of ubiquitous broadband wireless access come true. Details of our prototyping and implementation experiences are reported. Some performance test results are available in [19]. The discussion in this paper is based on IP version 4; it will be interesting to investigate the related issues on IP version 6.

ACKNOWLEDGEMENTS

This work is co-sponsored by the MOE Program for Promoting Academic Excellence of Universities under grant numbers A-91-H-FA07-1-4 and 89-E-FA04-1-4.

REFERENCES

[1] C.-C. Chiang, M. Gerla, and L. Zhang. Forwarding group multicast protocol (fgmp) for multihop, mobile wireless networks. *ACM-Baltzer Journal of Cluster Computing*, 1(2), 1998.

[2] J. J. Garcia-Luna-Aceves and E. L. Madruga. A multicast routing protocol for ad-hoc networks. In *INFOCOM*, 1999.

[3] Z. Haas and M. Pearlman. *ZRP: A Hybrid Framework for Routing in Ad Hoc Networks (a book chapter in Ad Hoc Networking, Ed. C. E. Perkins, Chapter 7)*. Addison-Wesley, 2000.

[4] M. Jiang, J. Li, and Y. Tay. Cluster based routing protocol (CBRP) functional specification (internet draft), 1998.

[5] D. B. Johnson, D. Maltz, and J. Broch. *DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks (a book chapter in Ad Hoc Networking, Ed. C. E. Perkins, Chapter 5)*. Addison-Wesley, 2000.

[6] J. Macker and M. Corson. Mobile ad hoc networking and the IETF. *ACM Mobile Computing and Communications Review*, 2(1):9–14, Oct. 1998.

[7] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu. The Broadcast Storm Problem in a Mobile Ad Hoc Network. In *MobiCom*, pages 151–162, 1999.

[8] E. Pagani and G. P. Rossi. Reliable broadcast in mobile multihop packet networks. In *MobiCom*, pages 34–42, 1997.

[9] E. Pagani and G. P. Rossi. Providing reliable and fault tolerant broadcast delivery in mobile ad-hoc networks. *Mobile Networks and Applications*, 4:175–192, 1999.

[10] C. Perkins. Mobile-IP, ad-hoc networking, and nomadicity. In *COMPSAC*, 1996.

[11] C. Perkins. Ad-hoc on-demand distance vector routing. In *MILCOM*, 1997.

[12] C. Perkins and P. Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector (DSDV) Routing for Mobile Computers. In *ACM SIGCOMM Symposium on Communications, Architectures and Protocols*, pages 234–244, Sep. 1994.

[13] C. Perkins and H. Lei. Ad hoc networking with mobile IP. In *EPMCC*, 1997.

[14] C. Perkins and K. Wang. Optimized smooth handoffs in mobile IP. In *IEEE Symp. on Computers and Communications*, 1999.

[15] C. E. Perkins. *Mobile IP Design Principles and Practices.* Addison-Wesley, 1997.

[16] C. E. Perkins and D. B. Johnson. Mobility support in IPv6. In *Mobile Computing and Networking*, pages 27–37, 1996.

[17] R. Ramjee, T. F. L. Porta, S. Thuel, K. Varadhan, and S. Y. Wang. HAWAII: A domain-based approach for supporting mobility in wide-area wireless networks. In *ICNP*, pages 283–292, 1999.

[18] E. Royer and C. Toh. A review of current routing protocols for ad-hoc mobile wireless networks. *IEEE Personal Communications*, Apr. 1999.

[19] C.-C. Sheng. Mobile IP and ad hoc networks: An integration and implementation experience. Master Thesis, National Chiao Tung University, Dept. of Computer Science and Information Engineering, 2002.

[20] Y.-C. Tseng, S.-L. Wu, W.-H. Liao, and C.-M. Chao. Location awareness in ad hoc wireless mobile networks. *IEEE Computer*, 34(6):46–52, June 2001.

[21] A. G. Valko. Cellular IP - a new approach to internet host mobility. In *ACM Computer Communication Review*, 1999.