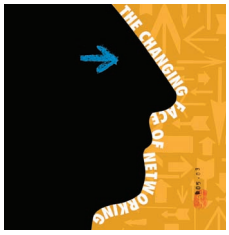
# Integrating Mobile IP with Ad Hoc Networks




**Extending traditional IEEE 802.11-based access points to incorporate the flexibility of mobile ad hoc networks would help make the dream of ubiquitous broadband wireless access a reality. The authors discuss several issues related to integrating the mobile Internet protocol with Manets.**

*Yu-Chee Tseng*
*Chia-Ching Shen*
National Chiao Tung University

*Wen-Tsuen Chen*
National Tsing Hua University

Ubiquitous computing has added a new feature, *mobility*, to the world of computing and communications. Many laptops, PDAs, handhelds, and other portable computing devices now include wireless connectivity as a standard feature, and more people are carrying computers when they travel to access the Internet anytime, anywhere.

The Internet Engineering Task Force's mobile Internet protocol[1] is a widely accepted standard that uses mobile agents to support seamless handoffs, making it possible for mobile hosts to roam from subnet to subnet without changing IP addresses. Another emerging wireless architecture, *mobile ad hoc networks*,[2-5] can be flexibly deployed in most environments without the need for infrastructure base stations. In most cases, Manets use IEEE 802.11 network interface cards. Manet applications include situations in which a network infrastructure is not available but immediate deployment of a network is required, such as a battlefield, outdoor assembly, or emergency rescue.

Integrating these two architectures will facilitate the current trend of moving to an all-IP wireless environment. We propose an architecture that extends the typical wireless access points to multiple Manets, each as a subnet of the Internet, to create an integrated environment that supports both macro and micro IP mobility. From the mobile IP perspective, foreign agents' service ranges are no longer limited to hosts within a single wireless hop; the use of Manets lets mobile hosts immediately utilize available Internet services without concern about disconnection.

## MOBILE IP AND MANETS

As Figure 1 shows, in a mobile IP environment, a mobile host or router can change its point of attachment from subnet to subnet. If a mobile host is away from home when a corresponding Internet host sends an IP datagram for delivery to the mobile host's home network, the datagram will be tunneled to the host's current foreign network. The home agent will encapsulate the datagram with an IP header carrying either the foreign agent's IP address or the mobile host's colocated care-of address. In our implementation, the foreign agent decapsulates the datagram and forwards it to the mobile host. Alternatively, if the care-of address is used, the mobile host serves as the endpoint of the tunnel and performs decapsulation locally.

Home and foreign agents advertise their services by periodically sending out Agent_Advertisement messages. A mobile host can send out an Agent_Solicitation message to look for local agents. From time to time, a mobile host must register its current care-of address with its home agent. The home agent keeps track of the mapping between each residential mobile host's permanent address and care-of address in a location dictionary.

Other mobile IP extensions include smooth handoff[6] and an extension for IPv6.[7] The "Related Work in Internet Computing" sidebar describes other protocols that support IP mobility.

In a Manet network, mobile hosts communicate with one another and roam at will. A routing path consists of a sequence of wireless links that do not


Published by the IEEE Computer Society
0018-9162/03/$17.00 © 2003 IEEE

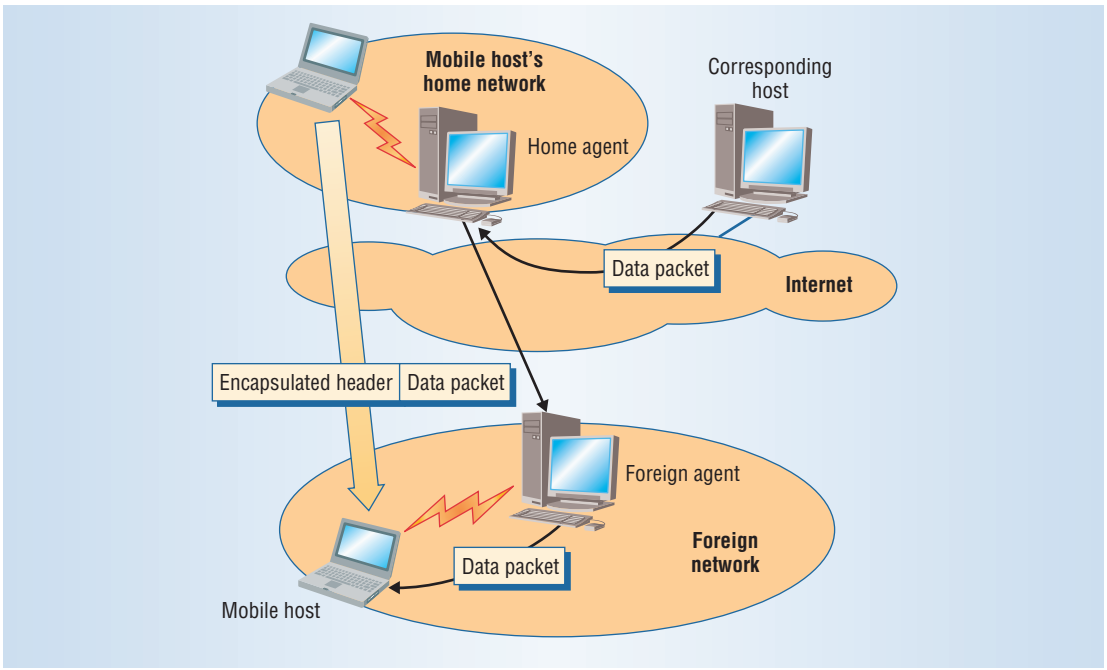



***Figure 1. Mobile IP transmission scenario. A corresponding host sends an IP data packet to a mobile host. If the mobile host is away, the packet is tunneled from the mobile host's home network to its current foreign network. The home agent encapsulates the packet with an IP header carrying the foreign agent's IP address or the mobile host's care-of address.***

## Related Work in Internet Computing

Mobile IP was originally designed to support macro mobility. Researchers have developed two other Internet protocols, cellular IP[1] and the handoff-aware wireless access Internet infrastructure (Hawaii),[2] to offer micro mobility.

Cellular IP uses a hierarchical approach to minimize registrations to home agents as a mobile host is roaming around. A foreign agent can provide services to multiple base stations. As long as the same foreign agent's base stations cover the mobile host, no reregistration is required, thereby significantly reducing handoff delay.

The Hawaii protocol adopts a domain-based approach in which base stations can be connected as a tree. It uses specialized path setup schemes that install host-based forwarding entries in specific routers to support intradomain routing. This offers the same advantage as cellular IP in supporting micro mobility and fast handoff. However, unlike cellular IP, Hawaii breaks the gateway-foreign-agent tie and thus is more tolerant to gateway failure, which simplifies gateway design.

Our framework supports micro as well as macro mobility. Instead of relying on hierarchical (wireline) routers, mobile hosts act as routers to extend the coverage of foreign agents. Cellular IP and Hawaii restrict mobile hosts to reside within one wireless hop from a base station, but our framework permits mobile hosts in multiple wireless hops from the base station.

Other research[3,4] has addressed using Manets to provide continuous Internet access via mobile IP. This includes extending mobile IP to let mobile hosts use a care-of address even if they are more than one hop away from a foreign agent. It also resolves the conflict between mobile IP and Manets in managing routing tables. Because mobile IP and Manets use two separate daemons, a route manager controls the system's routing table to coordinate the two daemons.

Our work is also compatible with current Manet design, and easily extends Manets to support IP mobility. Manet topologies can change dynamically, and foreign agents' service ranges can change accordingly, resulting in greater fault tolerance: If one foreign agent crashes, a mobile host can rely on Manet routing capabilities to connect to neighboring foreign agents.

Compared to earlier efforts that focused on only a single Manet, we consider the existence of multiple Manets in the same vicinity, with mobile agents and mobile hosts negotiating foreign agents' service ranges. The ability to dynamically adjust such service ranges greatly improves Manets' flexibility and reduces mobile agents' service overhead. In addition, Manets can overlap, supporting one another and offering higher fault tolerance in terms of Internet access. Direct communication between hosts covered by two different foreign agents, via Manet links, is also possible.

### References

1. A.G. Valkó, "Cellular IP: A New Approach to Internet Host Mobility," *ACM Computer Communication Rev.*, vol. 29, no. 1, 1999, pp. 50-65.
2. R. Ramjee et al., "HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks," *Proc. 7th Ann. Int'l Conf. Network Protocols* (ICNP 99), IEEE CS Press, 1999, pp. 283-292.
3. C.E. Perkins, "Mobile-IP, Ad-Hoc Networking, and Nomadicity," *Proc. 20th Int'l Computer Software and Applications Conf.* (Compsac 96), IEEE CS Press, 1996, pp. 472-476.
4. H. Lei and C.E. Perkins, "Ad Hoc Networking with Mobile IP," *Proc. 2nd European Personal Mobile Communications Conf.* (EPMCC 97), IEE, 1997, pp. 197-202.

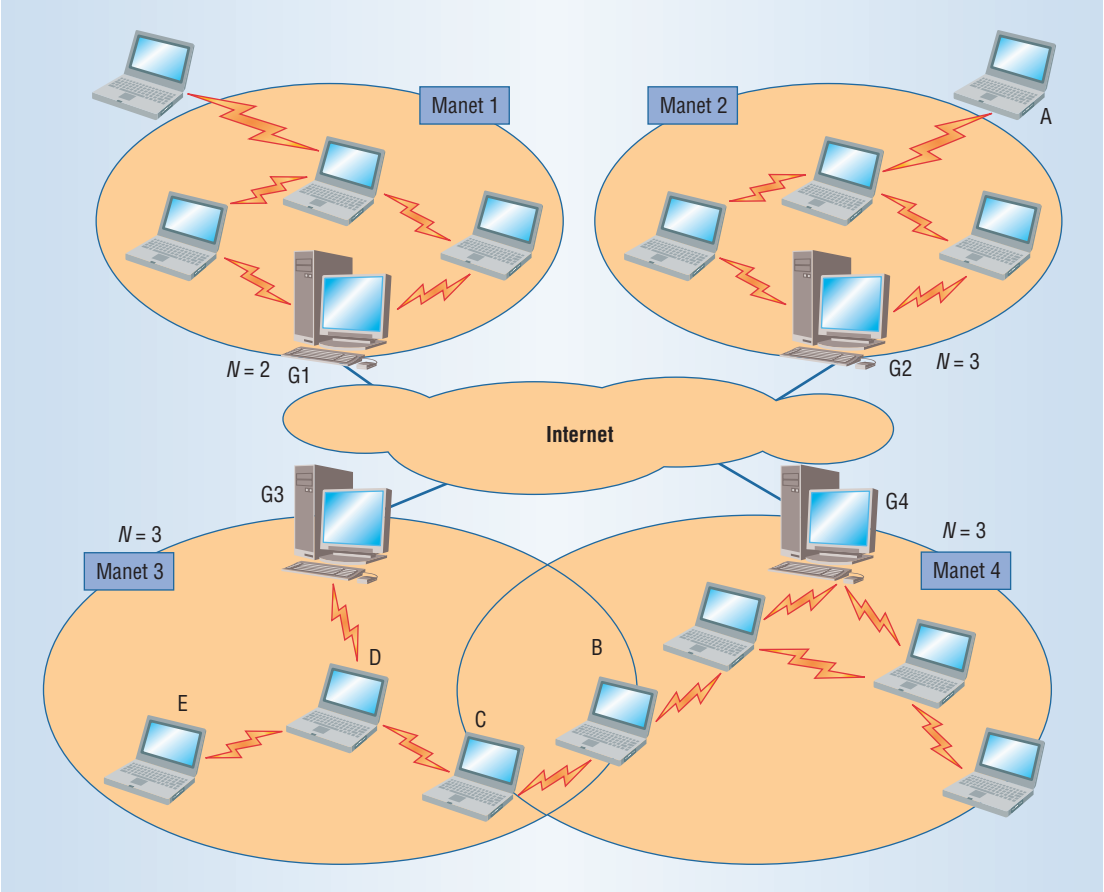



***Figure 2. Proposed network architecture. Each gateway (Gi) connects one Manet to the Internet and, to support mobile IP, also serves as the local foreign agent. Any mobile host within N wireless hops from the gateway can join the Manet the gateway serves.***

pass base stations. In this multihop configuration, each mobile host serves as a router.

Manet routing protocols can be classified as proactive and reactive. A *proactive* protocol such as the destination-sequenced distance-vector (DSDV) protocol[8] constantly updates routing information to maintain a near-global view of the network topology. In contrast, *reactive* protocols such as dynamic source routing (DSR),[9] the zone routing protocol (ZRP),[10] the constant bit-rate (CBR) protocol, and ad hoc on-demand distance vector (AODV) routing[5] conduct on-demand searches for a path. This approach may be less costly than a proactive protocol when host mobility is high. Other work has focused on unicast protocols,[6] multicast protocols, and broadcasting issues.[11]

## NETWORK ARCHITECTURE

As Figure 2 shows, our proposed architecture consists of multiple Manets attached to the backbone Internet. A *gateway,* the host that connects a Manet to the Internet, also defines a Manet's range. Each gateway has two network interface cards, one wireless and one wireline. Because they have fixed links, gateway hosts have no mobility. Gateways forward data packets and relay them between the Manet and the Internet. To support mobile IP, each gateway also serves as the foreign agent in its local Manet, periodically broadcasting Agent_Advertisement messages to announce its services.

Because Manets are mobile, networks can join and overlap one another. In such cases, the boundaries between Manets become vague, making foreign agents' service ranges unclear.

To precisely define a gateway's service range, we associate a parameter $N$ with each gateway. Any mobile host within $N$ wireless hops from the gateway can join the Manet the gateway serves. To accomplish this, we specify a time-to-live (TTL) equal to $N$ in each gateway's Agent_Advertisement message. For example, in Figure 2, even though it is connected to Manet 2, host A cannot be a part of Manet 2.

Any mobile host within the service ranges of multiple gateways can choose the closest one as its default gateway. This makes subnet boundaries clear even when Manets overlap. For example, in Figure 2, host C belongs to Manet 3 and host B belongs to Manet 4, and their home agents will accordingly tunnel IP datagrams to the proper gateways. Also, each gateway can define its own service range, $N$, independently based on its willingness and capability to provide services.

It is possible for a mobile host to disconnect from its gateway but remain connected to other Manets. For example, in Figure 2, if the link between gateway 3 and host D breaks, both host D's and host E's connections to the Internet will break because they are beyond gateway 4's service range.

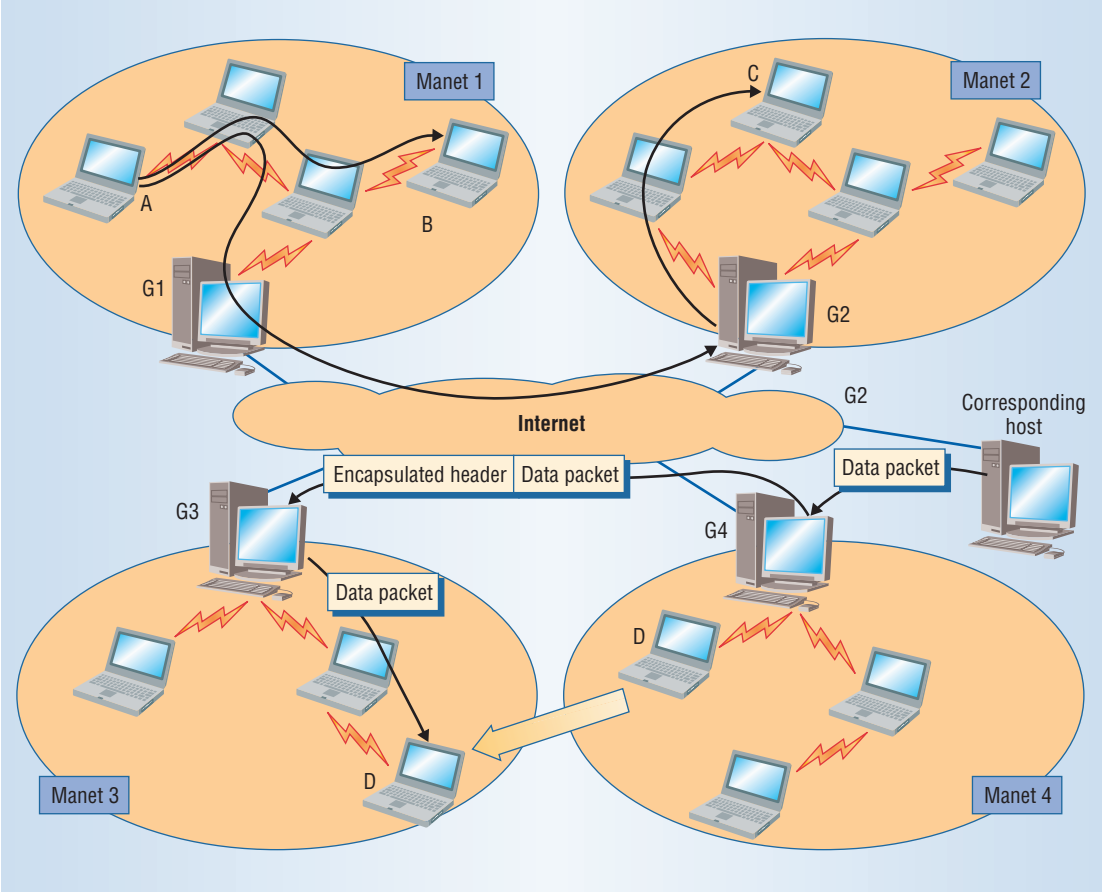



***Figure 3. Intra- and inter-Manet routing scenarios. Host A sends packets to host B through DSDV. It sends packets to host C first through DSDV, then by IP routing, and finally by DSDV again. The corresponding host sends packets to host D first through IP routing, then by tunneling, and finally by DSDV.***

To dynamically adjust a gateway's service range, and thereby solve the disconnection problem involving hosts D and E, a mobile host that does not receive an Agent_Advertisement message for a certain period can broadcast or multicast an Agent_Solicitation message with a TTL equal to $N'$. This value can gradually increase to avoid the *broadcast storm problem*[11] that flooding causes. If $N'$ is greater than or equal to $N$ and the Manet is connected, the gateway can hear the solicitation and decide whether to increase its $N$. For example, if host E's Agent_Solicitation has an $N'$ equal to 5, gateway 4 will receive the request and can increase its service range to cover both host D and host E.

## COMMUNICATION SCENARIOS

Our proposed network architecture can accommodate several different communication scenarios. In discussing the possible combinations, we assume that DSDV supports all corresponding Manet routings, although any proper routing protocol is applicable.

### Intra-Manet communication

DSDV supports intra-Manet communications. In the DSDV protocol, hosts exchange routing information periodically and compute the next hop to reach the destination with the least metric, such as hop count. DSDV will write proper route entries into the kernel routing table. To communicate with another host, a host first checks its routing table. If it finds a route entry leading to the destination, it forwards the packet directly to the next hop. The transmission from host A to host B shown in Figure 3 falls into this category.

### Inter-Manet communication

A host in a Manet will forward any packet whose destination is not listed in the kernel routing table to the local Manet's gateway. The gateway will then forward the packet to the Internet. The transmission from host A to host C in Figure 3 is an example of this packet transfer. Packets travel on Manet 1 based on DSDV, then on the Internet to gateway 2 based on IP routing, and then again by DSDV to host B on Manet 2.

When a mobile host roams away from its home network, mobile IP will forward packets between Manets. For example, in the transmission from the corresponding host to host D in Figure 3, packets arrive at gateway 4 via IP routing. Mobile IP encapsulates the packets and tunnels them to gateway 3, which then uses DSDV to forward them to mobile host D.

To support such a scenario, mobile hosts must follow mobile IP registration and deregistration procedures to monitor any existing Agent_Advertisement messages. DSDV routes these packets. Home agents maintain their mobile hosts' current locations and execute a proxy address resolution protocol (ARP)

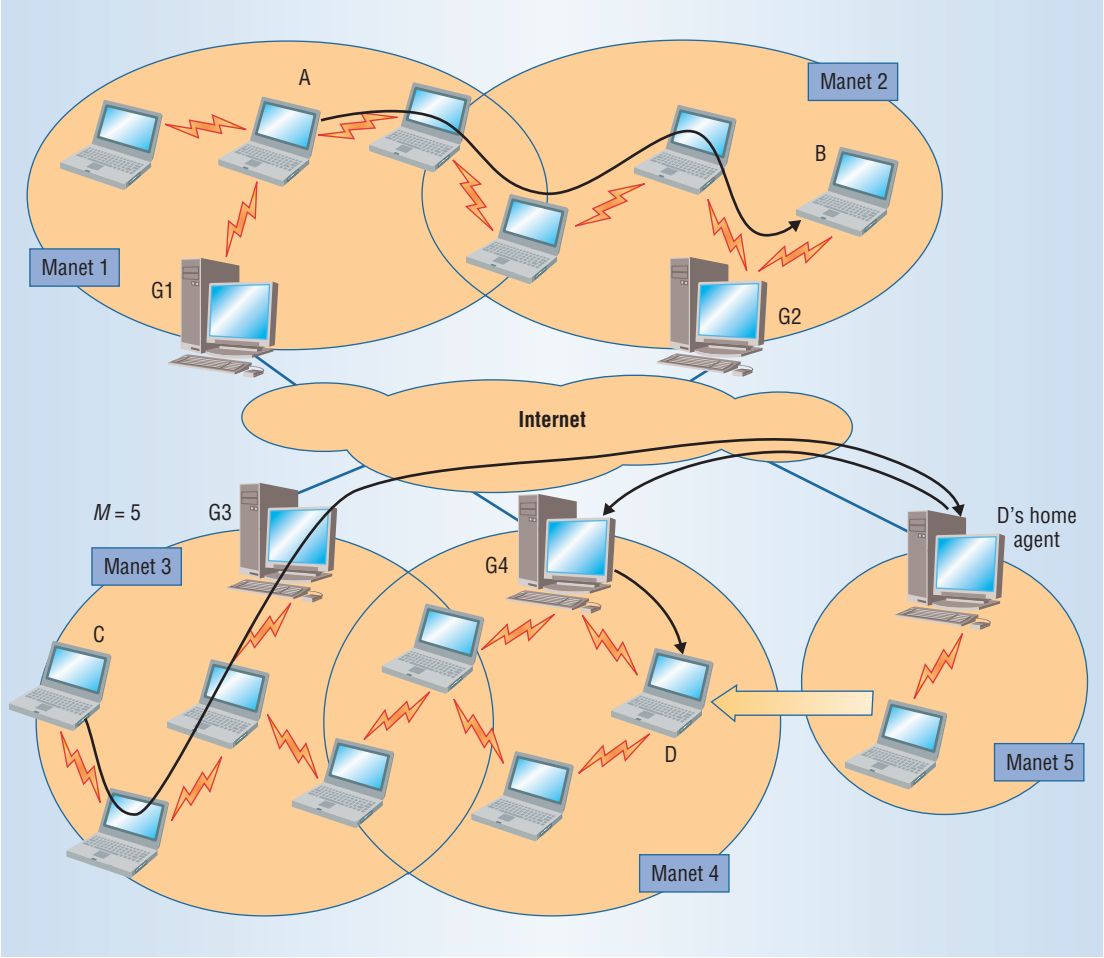



***Figure 4. Inter-Manet routing scenarios in overlaid Manets. Host A sends packets to host B directly via DSDV. Host C sends packets to host D first through DSDV, then by IP routing, followed by tunneling, and finally DSDV routing.***

for roaming mobile hosts, while foreign agents maintain visiting mobile hosts in their Manets.

When two Manets overlay, the frequent exchange of routing information by DSDV makes it possible for a mobile host to become aware of a route to another mobile host in a neighboring Manet. For example, in Figure 4, because host A has a route entry leading to host B, direct inter-Manet transmission is possible.

A mobile host always collects and propagates routing information for mobile hosts within $M$ wireless hops from itself. Therefore, we associate with DSDV a parameter $M$ that reflects the protocol's service range. Consequently, hosts in different but connected Manets can communicate with one another directly, if they are distanced by no more than $M$ hops. Such optimization reduces routing, tunneling, and encapsulation overhead. $M$ must be greater than or equal to $N$ so that a mobile host always knows a route to its local gateway.

When two mobile hosts reside in connected Manets but are more than $M$ hops away, the host should route their communications through the Internet. For example, in the transmission from host C to host D in Figure 4, assuming $M$ is equal to 5, host C will not be aware of the existing route leading to host D. Thus, DSDV forwards host C's IP datagrams to local gateway 3, and IP routing then forwards them to host D's home agent. Mobile IP will encapsulate the datagrams to host D's current foreign agent, and DSDV forwards the datagrams to host D. Properly tuning $N$ and $M$ will reduce overhead and improve efficiency.

## Broadcast

In wireline communication, a broadcast message is typically flooded around the physical range that a subnet covers. However, in wireless communication, because of the radio transmission property, the broadcast range is usually not well defined. This is particularly true for ad hoc networks, in which each mobile host has its own radio coverage. 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 define the broadcast coverage range as the service range that the issued broadcast's local gateway provides. Consequently, a subnet's range matches the Manet's range. When a mobile host sends a broadcast datagram, it first encapsulates the packet as a unicast by identifying the gateway as the destination host and then tunnels the unicast packet to the gateway. When the gateway decapsulates the packet and identifies it as a broadcast packet, it broadcasts the packet on behalf of the original source with a TTL equal to $N$.

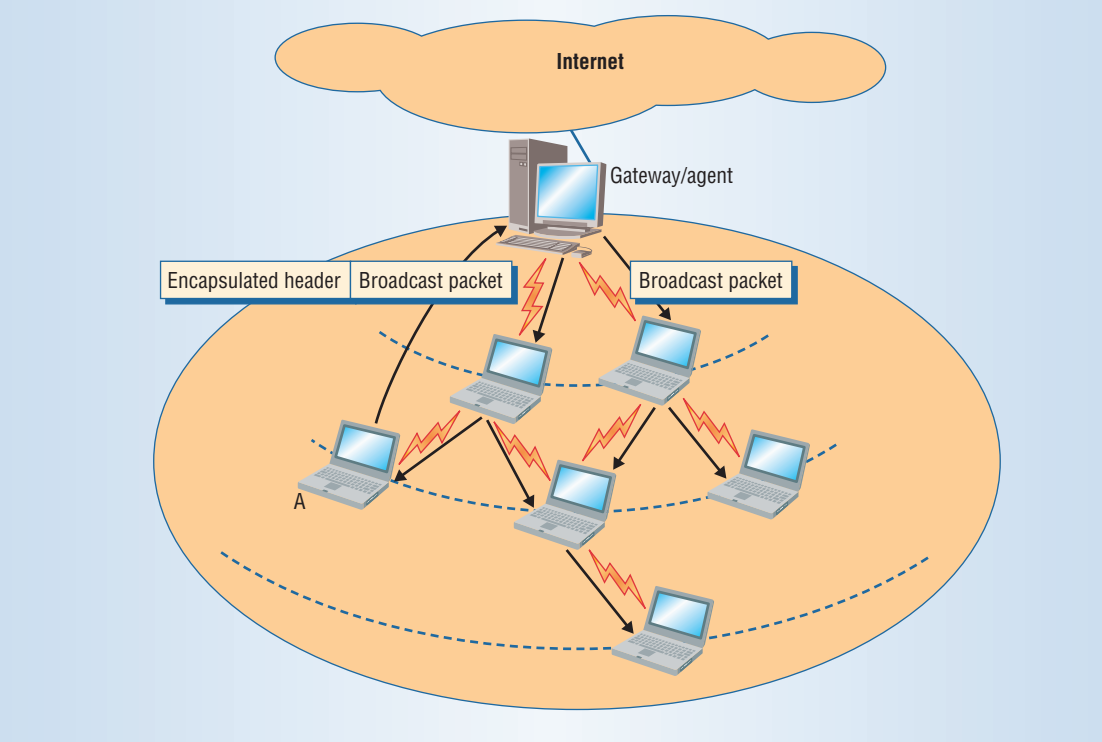



*Figure 5. Broadcast routing scenario. When a mobile host sends a broadcast datagram, it first encapsulates the packet as a unicast by identifying the gateway as the destination host. The gateway decapsulates the packet, determines that it is a broadcast packet, and broadcasts it on behalf of the original source with a TTL equal to N.*

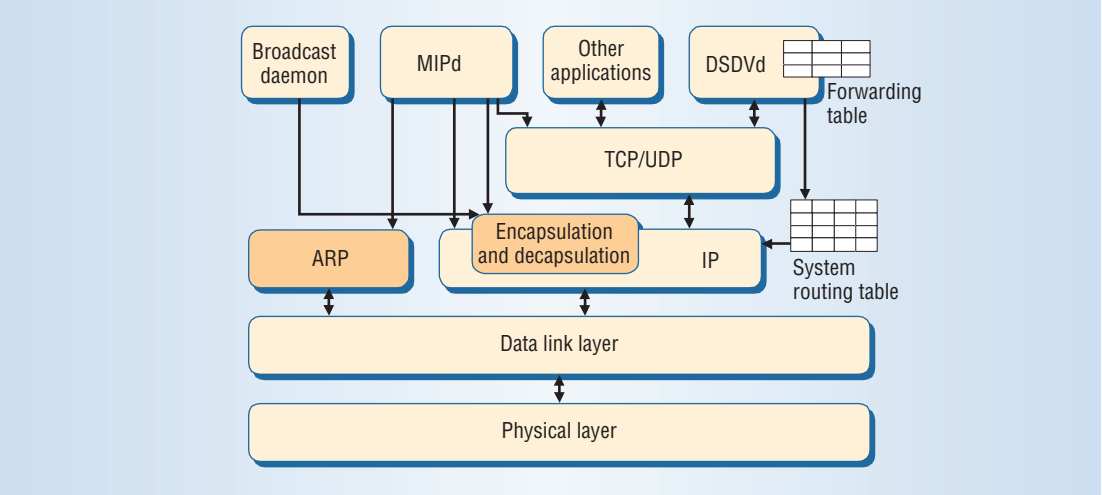



*Figure 6. System architecture of our implementation. The two daemons are network layer programs that are implemented on the application layer and interact with the system kernel through system calls.*

For example, Figure 5 shows how host A's broadcast datagram flows. To detect duplicate broadcasts, each mobile host maintains a list of broadcast IDs that it has received recently. The source IP address and IP identification fields in the IP header can serve as a unique identity.

## INTEGRATION AND IMPLEMENTATION

Our prototype network architecture, shown in Figure 6, integrates Mobile IP with Manets.

### TTL in IP packets

Each IP datagram has a TTL field to control its Internet lifetime. In Mobile IP, each Agent_Advertisement message should have a TTL equal to 1. We dynamically tune TTL to control our Agent_Advertisement, Agent_Solicitation, and broadcast packets.

### Routing inside Manets

Our implementation is based on the DSDV protocol.[8] Each host maintains a forwarding table that lists all available destinations along with the next hop leading to each destination. The forwarding table updates the kernel's routing table. Hosts in Manets use control packets to exchange information about distance vectors between neighboring hosts. Each route entry is associated with a sequence number originated by the destination host. The destination address for these control packets is 224.0.0.1 (the all-systems multicast address), with a TTL equal to 1 because there is no need to rebroadcast them.

Our prototype made some modifications to the DSDV protocol. Because Manets can overlap in our architecture, to avoid an overload in the amount of information being exchanged, the system only prop-

**Integrating mobile IP with Manets would realize the dream of broadband wireless Internet access.**

agates routing information within *M* hops. In addition, each gateway should broadcast its service range, *N*, through its control packets.

Further, each gateway should identify itself by associating a gateway bit in its control packets. Each mobile host should set its default router to be the host that leads to the gateway host with the least metric. Finally, if a mobile host also has a care-of address, it must advertise both its original IP address and the care-of address through DSDV's control packets. This is similar to a host having two IP addresses. Providing two entries in the control packets makes it possible to reach the mobile host directly at its permanent IP address in the Manet and also at its care-of address via mobile IP.

## Agent advertisement

In mobile IP, Agent_Advertisement messages have a TTL equal to 1. However, Manets' multihop nature requires setting the TTL to *N* and decreasing the value by one for each rebroadcast; no rebroadcast is necessary when the TTL is equal to 0. The destination field should be 255.255.255.255.

## Agent solicitation

A mobile host can multicast an Agent_Solicitation message to locate a nearby mobile agent. The destination field should be 224.0.0.2 (the all-routers multicast address).

Each time the solicitation process fails, the TTL can be doubled, making it possible to reach approximately four times as many hosts as in the previous round. Because the TTL value decreases 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 mobile host. By comparing this value to *N*, the gateway can then decide whether to enlarge its service range.

## ARP

In mobile IP, the address resolution protocol should be disabled when a mobile host visits a foreign network. Instead, the host registers the MAC (media access control)-to-IP address mapping when it receives an Agent_Advertisement message. However, to permit peer-to-peer communication inside a Manet, our network architecture requires enabling the address resolution protocol in foreign networks to send requests and replies as usual. Because many nomadic hosts can exist in a Manet, these networks should relay packets of any destination without using a subnet mask.

## Broadcast

We have designed a broadcast daemon to support the broadcast routing scenario shown in Figure 5. When a mobile host intercepts a broadcast datagram with the destination address 255.255.255.255 and a TTL of 1, and intercepts the source address "myself," the daemon encapsulates this packet as a unicast destined for the local gateway. When it receives the packet, the gateway decapsulates it and broadcasts it with a TTL equal to *N*. To prevent broadcast datagrams from looping back to the source host, the broadcast daemon also records broadcast datagrams that it has encapsulated recently.

## Destination address and TTL

In view of the fact that the *M* value that Manets use should be at least as large as the *N* value that mobile IP uses, it is possible to control the traffic flow into and out of a Manet by adjusting both parameters.

We recommend setting *M* equal to 2*N*, which guarantees that intra-Manet communication can always occur directly without encapsulation. In the worst case, a packet has to travel from a Manet's boundary to the gateway, and then to another end of the Manet, resulting in a hop count of 2*N*. In addition, communication between nearby Manets is likely to occur without going through mobile IP, thus the packet will not undergo encapsulation.

## Configuration of IEEE 802.11b NICs

Our implementation sets all wireless network interface cards to peer-to-peer (ad hoc) mode. All mobile hosts use the same extended service set identifier and channel number to communicate with one another. Foreign agents can use different channels to increase channel reuse and thus communication bandwidth.

In most current products, an NIC will automatically scan available channels only when its current connection is broken. Consequently, a host may not be able to discover all its neighbors if they are operating at different channels. In our framework, the network should function correctly, but some routes may not exist even if some hosts are physically neighbors.

Our system is based on Linux Redhat v2.2.16 and implements two daemons, DSDVd and MIPd. As Figure 6 shows, both daemons are implemented on the application layer and interact with the system kernel through socket interfaces. DSDVd periodically multicasts user datagram protocol packets to help maintain the hosts' forwarding tables.

System calls write proper entries from the forwarding table into the kernel's routing table. MIPd uses raw sockets for advertisement, encapsulation, and decapsulation, and it uses normal sockets for registration. Unix system calls perform proxy ARP. In addition, the IP forwarding option at each mobile host must be turned on.

By supporting greater roaming flexibility, our proposed integration of mobile IP with Manets would realize the dream of broadband wireless Internet access. Extending our work, which is based on IPv4, to the next-generation IPv6 environment, which will include mobile IP features as inherent functionality, deserves further study. Load-balance routing is another challenging issue, especially when running such an architecture in a crowded area. ■


## Acknowledgment

This work is cosponsored 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.E. Perkins, *Mobile IP: Design Principles and Practices,* Addison-Wesley, 1997.
2. J.P. Macker and M.S. Corson, "Mobile Ad Hoc Networking and the IETF," *ACM Mobile Computing and Communications Rev.,* vol. 2, no. 1, 1998, pp. 9-14.
3. C.E. Perkins, E. M. Royer, and S.R. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," IETF Internet draft, Manet working group, Jan. 2002, draft-ietf-manet-aodv-10.txt.
4. E. Royer and C-K. Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *IEEE Personal Communications,* vol. 6, no. 2, 1999, pp. 46-55.
5. Y-C. Tseng et al., "Location Awareness in Ad Hoc Wireless Mobile Networks," *Computer,* June 2001, pp. 46-52.
6. C.E. Perkins and K-Y. Wang, "Optimized Smooth Handoffs in Mobile IP," *Proc. 4th IEEE Symp. Computers and Communications* (ISCC 99), IEEE CS Press, 1999, pp. 340-346.
7. C.E. Perkins and D.B. Johnson, "Mobility support in IPv6," *Proc. 2nd Ann. Int'l Conf. Mobile Computing and Networking* (Mobicom 96), ACM Press, 1996, pp. 27-37.
8. C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector (DSDV) Routing for Mobile Computers," *Proc. ACM SIGCOMM '94 Conf. Communications Architectures, Protocols and Applications,* ACM Press, 1994, pp. 234-244.
9. D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," *Ad Hoc Networking,* C.E. Perkins, ed., Addison-Wesley, 2000, pp. 139-172.
10. Z.J. Haas and M.R. Pearlman, "ZRP: A Hybrid Framework for Routing in Ad Hoc Networks," *Ad Hoc Networking,* C.E. Perkins, ed., Addison-Wesley, 2000, pp. 221-253.
11. S-Y. Ni et al., "The Broadcast Storm Problem in a Mobile Ad Hoc Network," *Proc. 5th Ann. ACM/IEEE Int'l Conf. Mobile Computing and Networking* (Mobicom 99), ACM Press, 1999, pp. 151-162.



***Yu-Chee Tseng*** *is a professor in the Department of Computer Science and Information Engineering at National Chiao Tung University, Taiwan. His research interests include wireless networks and mobile computing, video-on-demand, parallel and distributed computing, and network security. Tseng received a PhD in computer and information science from Ohio State University. He is a senior member of the IEEE and a member of the ACM. Contact him at yctseng@csie.nctu.edu.tw.*

***Chia-Ching Shen*** *is an engineer at ZyXEL Communications Corp., based in Hsinchu, Taiwan. His research interests include wireless networks, mobile computing, and protocol design for ad hoc networks. Shen received an MS in computer science and information engineering from National Chiao Tung University. Contact him at jcsheen@csie.nctu.edu.tw.*

***Wen-Tsuen Chen*** *is a professor and dean of the College of Electrical Engineering and Computer Science at National Tsing Hua University, Taiwan. His research interests include computer networks, broadband networks, parallel systems, and algorithms. Chen received a PhD in electrical engineering and computer science from the University of California, Berkeley. He is an IEEE Fellow. Contact him at wtchen@cs.nthu.edu.tw.*