https://doi.org/10.54361/ajmas.269721

Original article

Fast Handover for Mobile in Major Optimization Algorithms: IPv4 Mobility

Mohamed Hmadi[1,2], Mouemer Elriheemi[3], Muntaser Fraj[4]

[1]*Department of Computer Science, Faculty of Science, Azzaytuna University, Tarhuna, Libya*
[2]*Department of Cyber Security, University of Darence Ahlahlia, Libya*
[3]*Department of Computer Science, Faculty of Science, Azzaytuna University, Tarhuna, Libya*
[4]*Department of Computer Engineering, Bright Star University-Brega, Libya*
Corresponding Email. *m.hmadi@azu.edu.ly*

Abstract
This paper presents a predictive handover algorithm that relies on pre-configuring the new access router before a disconnection occurs. The mechanism establishes a temporary tunnel between the previous router (PAR) and the new router (NAR) during the handover period, utilizing enhanced techniques such as pre-registration, packet buffering, and rerouting. These enhancements demonstrate a significant ability to reduce both handover latency and packet loss. This paper also explains the workings of the Mobile IPv4 (MIPv4) protocol, outlining its main challenges and proposing key optimization methods. Furthermore, it compares the most prominent handover optimization algorithms in Mobile IP and proposes two fast handover schemes, analyzing various factors that influence IP-layer handover performance through extensive simulations.
Keywords. Mobile Node (MN) IP Address, Mobile Ipv4 (MIPv4), Fast Handover, Optimization Algorithms.

Introduction

Mobile IPv4 (RFC 5944) enables devices (Mobile Nodes) to roam across networks while maintaining active connections using a dual-addressing strategy: a permanent Home Address (HoA) for identification and a temporary Care-of Address (CoA) reflecting current location. The Home Agent (HA) on the home network tracks the MN's CoA, intercepts packets sent to the HoA, and tunnels them to the MN's current location, while Foreign Agents can optionally assist with CoA assignment and packet forwarding. Through Agent Discovery, Registration, and Tunneling, the MN updates its location with the HA, enabling seamless packet delivery via triangular routing (CN→HA→MN) without disrupting ongoing TCP/UDP sessions. This mechanism supports uninterrupted mobility across Wi-Fi and cellular networks, allowing video calls, file transfers, and gaming sessions to continue seamlessly as the MN changes attachment points.

Problems

Providing mobility within the existing internet infrastructure is challenging because IP addresses tied to fixed network locations, while mobile devices constantly change attachment points; higher-layer connections cannot tolerate address changes without breaking connectivity, and additional concerns like cybersecurity and QoS further complicate protocol design [1]. To address this, Mobile IPv4 (RFC 5944) establishes fundamental requirements: enabling continuous communication without changing the original IP address, ensuring backward compatibility with non-MIPv4 nodes, avoiding new security vulnerabilities, minimizing signaling overhead on bandwidth-constrained wireless links, and maintaining independence from underlying access technologies [2]. The protocol introduces key entities—Home Agent (HA) and Foreign Agent (FA)—and dual addressing: a permanent Home Address (HoA) for node identification and a temporary Care-of Address (CoA) reflecting current topological location. A Mobile Node's home network matches its HoA prefix, while any other network is considered foreign; the HA tracks the MN's location and forwards packets, while the FA assists with routing on visited networks. MIPv4 operates through three core functions: Agent Discovery (locating mobility agents), Registration (binding CoA to HoA at the HA) [3], and Tunneling (forwarding packets from HA to CoA). This triangular routing approach (CN→HA→MN) preserves ongoing TCP/UDP sessions despite mobility, enabling seamless roaming across Wi-Fi and cellular networks for uninterrupted services like video calls, file transfers, and gaming.

Results

Tunnel-based handover

Tunnel-based handover belongs to the smooth handover category. The basic operation is to redirect misrouted packets from the previous MA to the current MA of an MN. The Internet draft “Route Optimization in Mobile IP” [10] provides a basic way to realize packet redirections, in which the MN utilizes the *Previous FA Notification Extension* (PFANE) in a Registration Request message to guide its current FA to set up a tunnel with its previous FA after a handover. Thus, the misrouted packets were retrieved from the previous FA. Nevertheless, merely redirecting packets does not recover all the lost packets in many cases. According to [11], the old FA will only begin to redirect packets after it gets the defined Binding Update message from the new FA. Therefore, those misrouted packets coming before the Binding Update message would be retrieved. Several researchers proposed using an FIFO (First In First Out) buffer at each FA to save the most recent packets destined for an

Received*: 07-05-2026 -* ***Accepted****: 05-07-2026 -* ***Published****: 12-07-2026*

https://doi.org/10.54361/ajmas.269721

MN. FAs not only decapsulate tunnelled packets and deliver them to the specific MN, but also buffer these packets. When it receives a Binding Update message for the MN from another FA, it re-tunnels the buffered packets as well as any future packets destined for the MN, to the new FA. By this means, packet loss during a handover can be eliminated if the buffer size is large enough to accommodate all the incoming packets during the period from the moment when the MN loses contact with the old FA to the moment when the old FA gets a Binding Update message for the MN. However, since this period can be variable, there is a tradeoff when determining the optimal buffer size. If the buffer size is made large enough to guarantee that there is no packet loss during a handover, in many cases, some of the redirected buffered packets could already be received by the MN. As a result, a major side effect of handing over buffered packets is packet duplication. Duplicated packets are a waste of the bandwidth resource, especially on wireless links, and they cause duplicated packet acknowledgments so that the retransmission mechanisms of upper layers (TCP) are invoked. The relationships between the number of lost packets and the buffer size, and between the number of duplicated packets and the buffer size, are shown in the simulation results.

Multicast-based handover

Multicast-based handover belongs to the fast handover category. In fact, basic MIPv4 already offers an option to use the concept of multicast-based handover. That is, an MN can set the 'S' bit in its Registration Request message to require its HA to provide the simultaneous binding function [12]. The HA then copies the datagrams and tunnels them to all the mobility bindings of the MN. In this way, when the MN moves back to one of its previous FAs, it will get its datagrams immediately. However, this is not quite feasible, since the global network traffic load would significantly increase if there were many MNs requesting the simultaneous binding service. However, benefiting from the partition of macro-mobility and micro-mobility, multicast-based handover could work much better inside a domain, because in this case, all duplicated datagrams are kept inside the domain without affecting other parts of the Internet. Since usually an MN cannot predict its next FA, merely using the simultaneous binding function can never guarantee fast handovers. Consequently, a number of multicast-based schemes have been proposed (for example, [13] and [14]), and all of them more or less rely on a certain mechanism of the local network to provide multicast position information, so that it can be guaranteed that the next FA of the MN has received the multicast datagrams before the MN moves to its area. Note that most of the multicast-based handover schemes also deploy a buffer at each FA to smooth handovers. This is because an MN needs time to switch its link-layer connectivity from the old FA to the new FA. During this time, the incoming packets can be stored in the new FA's buffer. The new FA then forwards the buffered packets to the MN after the MN connects to it. The deployment of buffers has the same side effect as that in the tunnel-based approach. A comparison between the tunnel-based approach and the multicast-based approach was made by showing the simulation results on handover performance.
Standard MIPv4, datagrams destined for an MN are always intercepted by the HA and then tunnelled to the current access location of the MN. However, datagrams sent by the MN are forwarded directly to its CNs in normal cases [15]. As a result, the triangle routing problem arises (Figure 2). In this case, datagrams to the MN are routed along paths that are significantly longer than optimal, especially when the MN is near its CNs but far from its HA. MIPv4 route optimization [16] was proposed by Perkins to address the triangle routing problem. The proposal provides a means for CNs to maintain a binding cache for MNs for use in tunneling datagrams directly to them, bypassing their HA. In [17], four message-layered to manage the binding cache in CNs: Binding Warning, Binding Request, Binding Update, and Binding Acknowledgement. A Binding Warning message is used to send a suggestion that certain CNs or FAs need a Binding Update. A Binding Request message is used to send a request for the current mobility binding of an MN from the MN or its HA. A Binding Update message is used to send a notification.

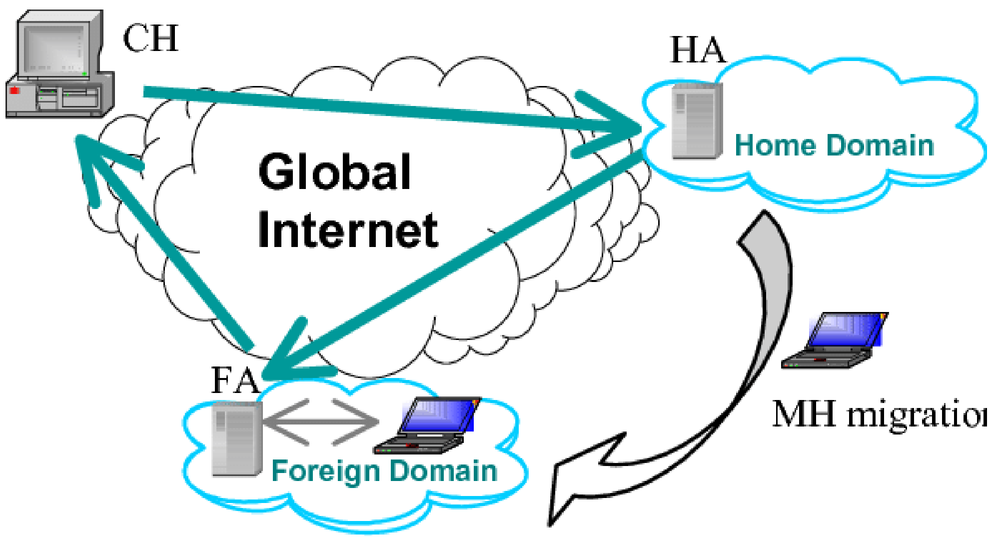

Figure 3. Mobile IPv4 Triangle Routing

Received*: 07-05-2026 -* ***Accepted****: 05-07-2026 -* ***Published****: 12-07-2026*

OF an MN's current mobility binding. A Binding Acknowledgment message is used to send a response to a Binding Update message. Any node may utilize these four messages to maintain a binding cache in order to optimize the routing of its datagram that is destined for an MN. The protocol details are referred to [18]. Obviously, to support the basic MIPv4 route optimization scheme, CNs were modified to understand the protocol. Moreover, since the Binding Update message needs to be authenticated to prevent it from introducing extra security vulnerability, a preconfigured SA is needed between an MN's HA and a CN. These cause great difficulties for this scheme to be widely deployed. More recently, Vidalia et al. designed an agent-based MIPv4 Optimization scheme [19], whose key idea is to introduce Correspondent Agents (CAs) in networks to maintain binding caches, and tunnel datagrams to MNs on behalf of each CN. In this way, the route optimization function is transparent to end nodes, and hence no modifications are required in CNs. In addition, a CA may manage the binding caches for several end nodes in the same subnet. When multiple CNs in the same subnet are communicating with an MN, only one Binding Update message is required to be sent to the CA, which reduces signaling traffic. Therefore, the agent-based scheme is more easily deployable than the basic route optimization extension for MIPv4. However, the security challenge still exists since it is hard to guarantee that an MN's HA shares an SA with any CA that the MN will communicate with. A new route optimization solution for MIPv4 is proposed, which adapts the default Mobile IPv6 route optimization scheme for MIPv4 based on the agent-based architecture.

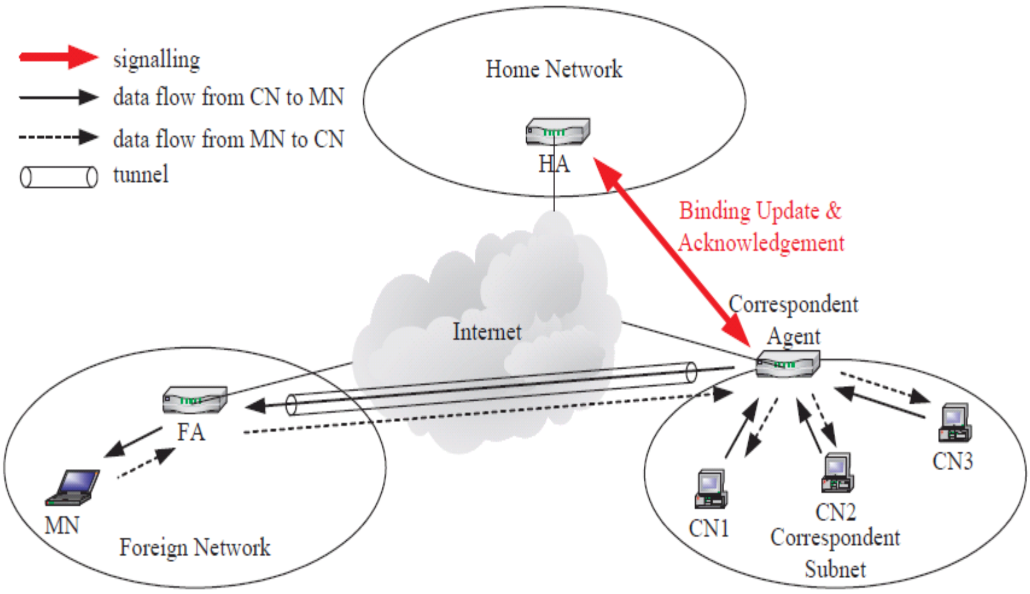

Figure 4. Mobile IPv4 Agent-Based Route Optimization

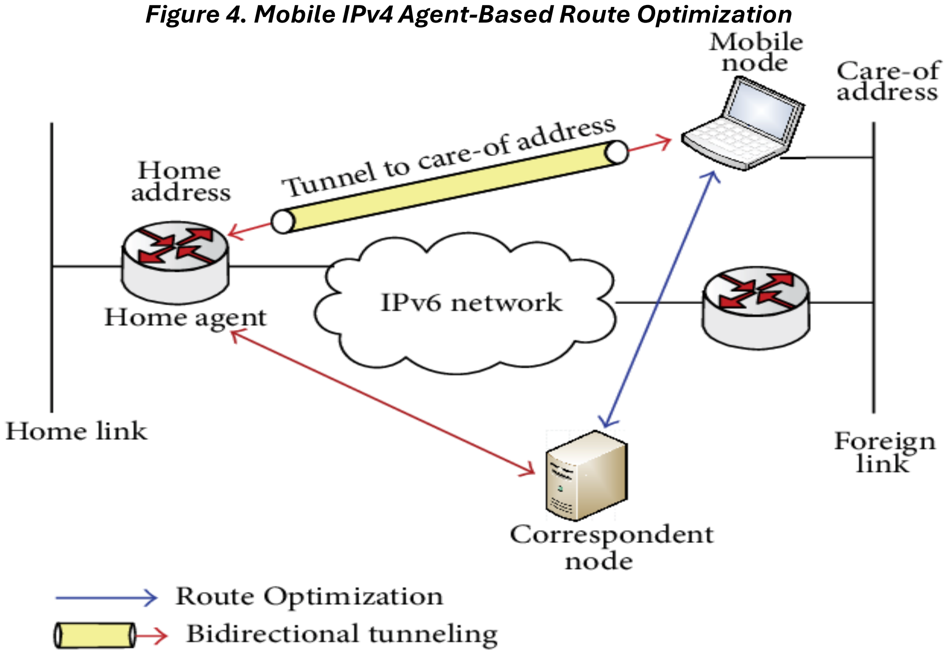

Figure 5. Mobile IPv6 bidirectional tunnelling and Route Optimization

***Received**: 07-05-2026 - **Accepted**: 05-07-2026 - **Published**: 12-07-2026*

https://doi.org/10.54361/ajmas.269721

Discussion

Agent discovery is the process of an MN detecting an MA either on the home network or on a foreign network, which is quite similar to the ICMP Router Discovery protocol [4] that is used by Internet nodes to detect routers. An MN utilizes the agent discovery process to decide whether it is in the home network or a foreign network, check whether a handover occurs, and obtain a new CoA if it decides to register to a new foreign network. The basic operation of agent discovery involves two types of messages: Agent Advertisement and Agent Solicitation. The Agent Advertisement message is sent by MAs periodically announcing their presence on a link. On the other hand, the Agent Solicitation message sent by MNs actively solicits an MA's advertisement in the absence of periodic Agent Advertisements expected. These two messages help MNs to find an MA initially on startup and perform movement detections in the case of handovers. On receipt of an Agent Advertisement, an MN determines whether it is in its home network or a foreign network. If the MN is in its home network, it operates as normal without using any mobility support functions. If it detects that it is located in a foreign network, or it has just returned home from a foreign network, a registration process is needed. Registration is the process by which an MN notifies its HA of its current location of attachment to the Internet. The registration process involves two messages, Registration Request and Registration Reply. In a foreign network, the MN first acquires a CoA from an FA or through other address allocation mechanisms, such as DHCP (Dynamic Host Configuration Protocol) [5], and then it composes a Registration Request message containing the obtained CoA and sends it to the HA. After processing the Registration Request, the HA returns a Registration Reply message to the MN indicating the registration status. If the registration is successful, the HA keeps a binding entry in its binding table to associate the MN's current CoA with its HoA. In a special case, when the MN returns to its home network from a foreign network, it sends a special Registration Request message (with the CoA set to its HoA) to notify its HA of its return home. This process is called de-registration, in which the HA also returns a Registration Reply to indicate the de-registration status, and deletes the binding entry for the MN. Tunneling is a special routing strategy that enables datagrams to reach an MN even when it is away from home. In MIPv4, HoA always recognizes an MN. When it is away from home and has successfully registered with its HA, the HA is responsible for capturing all datagrams destined for the MN and redirecting them to the MN's current CoA. The tunneling techniques enable this datagram redirection without changing the original IP datagrams. IP-in-IP encapsulation [6] is the default tunneling scheme used by MIPv4. The tunnel end could be the MN's FA or the MN itself, depending on the type of CoA the MN is using. A CoA obtained from an FA is called an FA CoA; while a CoA obtained through a local address, configuration mechanism is called a co-located CoA. A binding, or mobility binding, refers to the association between an MN's home address and care-of address. In MIPv4, registration messages are authenticated to prevent malicious nodes from spuriously generating these messages to embezzle mobility services or disrupt the normal routing of MIPv4. Three registration authentication extensions defined in MIPv4 for security considerations. They are:

- Mobile-home authentication extension
- Mobile-foreign authentication extension
- Foreign-home authentication extension

To compose and verify these authentication extensions, three mobility *Security Associations* (SAs) are required:

- Mobile-home (MN-HA) mobility SA
- Mobile-foreign (MN-FA) mobility SA
- Foreign-home (FA-HA) mobility SA

An SA is the combination containing both the necessary cryptographic key information and a way to identify the cryptographic transform. According to [6], these mobility SAs are derived from the basic AAA (Authentication, Authorization, and Accounting) SA shared between an MN and its HA or home AAA server (AAAH). After the description of each mechanism, this section gives a general review of the operations of MIPv4. Suppose an MN originally stays in its home network, and then moves to a foreign network, and finally returns to its home network again. MAs advertise their existence periodically on their local network. On receipt of an Agent Advertisement from its HA, the MN determines that it is in the home network and operates like a fixed host. When the MN moves to a foreign network, it actively solicits Agent Advertisements by sending Agent Solicitations or waits for a periodical Agent Advertisement. The MN obtains an FA CoA on receipt of an FA advertisement or a co-located CoA through other address configuration mechanisms such as DHCP. The MN sent registration request message (srr) with its current CoA and the necessary authentication extensions to its HA directly or via an FA. On the assumption that the HA accepts the Registration Request, it generates a Registration Reply message to the MN, as well as updating its binding table for the MN. When the MN receives the successful Registration Reply, the registration process finishes. The HA starts to announce the availability of the MN to other routers to intercept datagrams destined for the MN. When HA tunnels the intercepted datagrams to the MN according to its binding table. Encapsulated (tunnelled) datagrams are decapsulated (detunnelled) by the FA or the MN itself, and finally reach the MN's upper layers. IN normal cases, the MN sends datagrams directly to its communicating nodes, or Correspondent Nodes (CNs), without tunneling. When the MN detects that it has returned home, it deregisters with HA and announces its availability on its own. The HA deletes the binding entry for the MN and stops tunneling datagrams destined for the MN. From then on, the MN acts as a normal host without mobility support again. In this way, MIPv4 completely hides the MN's mobility from upper-layer applications [7]. When the MN is in a foreign domain, this architecture provides the possibility that, in most cases, the MN's movements are very transparent to its HA. That is, the location update messages caused by the MN's movements inside a

Received*: 07-05-2026 -* ***Accepted****: 05-07-2026 -* ***Published****: 12-07-2026*

https://doi.org/10.54361/ajmas.269721

domain are handled by the gateway router of the domain without notifying the HA. As a result, signaling messages are processed locally and do not need to travel all the way back to the HA. Therefore, the handover latency is reduced, and signaling traffic load is limited inside the domain. The partition of macro-mobility and micro-mobility automatically brings different types of mobility management. Several micro-mobility management protocols for IPv4 have arisen, among which Mobile IP Regional Registration [8], which is also called *Hierarchical Mobile IPv4* (HMIPv4), is the most promising one to be standardized by the IETF. In [9], a few extensions were added to the original MIPv4 protocol to provide regional registration functions. Specifically, two regional registration messages are proposed (Regional Registration Request and Regional.

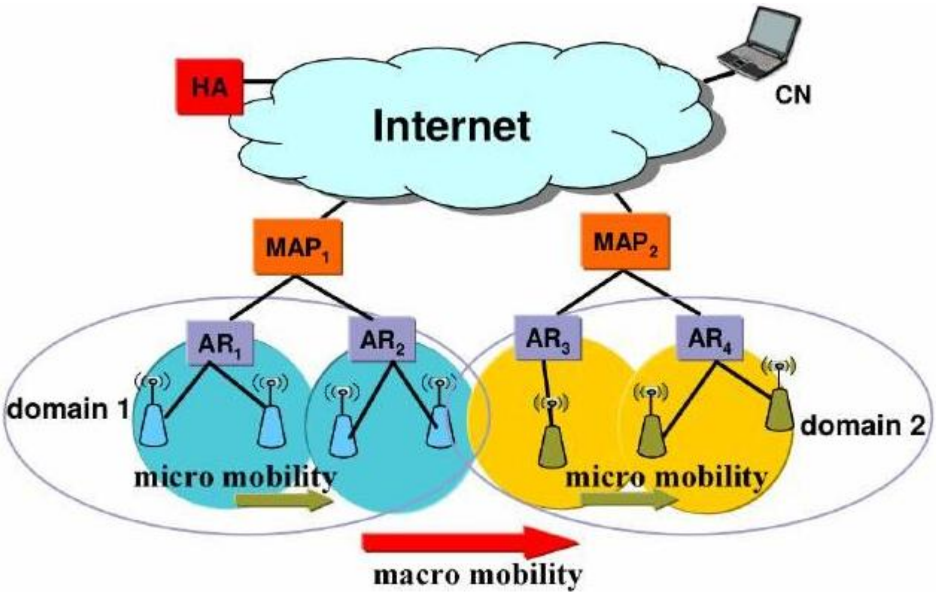

Figure 1. Macro-Mobility and Micro-Mobility

Registration Reply) And two new mobility entities were introduced. The *Gateway Foreign Agent* (GFA) and *Regional Foreign Agent* (RFA). A GFA is a special FA usually placed at the edge of an administrative domain with a globally routable IP address. It is able to generate a reply message in response to a request message for a regional registration. An RFA is an FA with the capability of a GFA located in a multi-level hierarchical system, which may be the target of a request message for a regional registration. (Figure 2) shows a typical network model for the Overview of the Mobile IP registration process protocol.

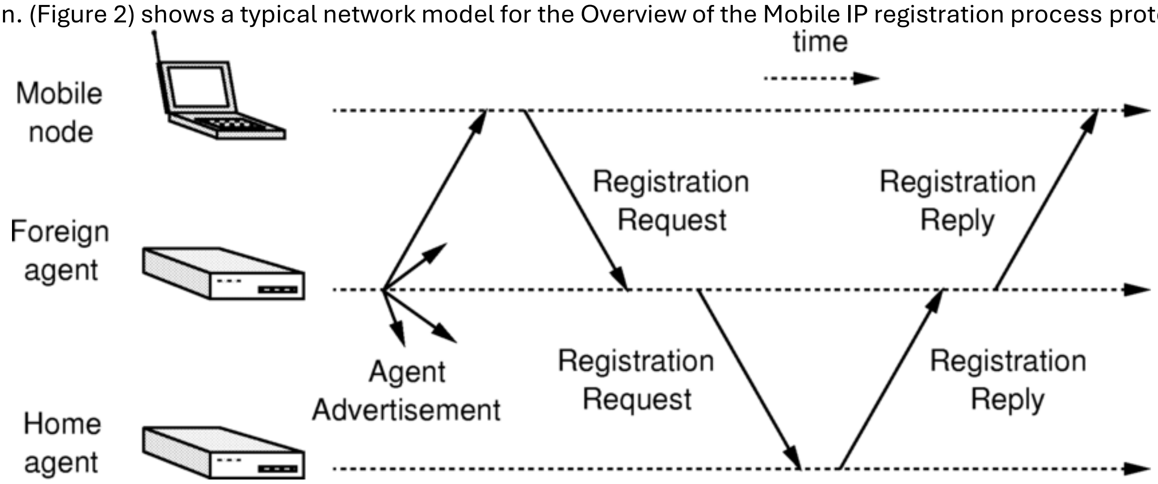

Figure 2. Overview of the Mobile IP registration process

When an MN first enters a foreign domain, it performs a registration with HA (home registration). The HA registers the CoA of the MN. If the foreign domain supports regional registrations, the CoA should be a globally routable address of a GFA. When the MN changes its access FA under the same GFA or RFA, it may perform a regional registration addressed to the GFA or RFA, which is transparent to the HA. Note that if the regional registration destination is an RFA, the MN's movement may even be transparent to the GFA and any higher-level RFAs. Outside the domain, the GFA's address is thought of as the MN's CoA. Datagrams destined for the MN are tunnelled to the GFA first by the HA. The GFA reroutes (decapsulates and re-encapsulates) them to the next level of the hierarchy towards the MN, and thus repeats by each RFA in the hierarchy, until the datagrams reach the MN. Datagrams from the MN are sent directly to its CNs in normal cases. Mobile IP handovers incur a period of packet misrouting to the previous CoA. In basic MIPv4, the misrouted packets can be retrieved by the higher layer's retransmission mechanisms (if retransmissions are needed). The number of misrouted packets largely depends on

***Received**: 07-05-2026 - **Accepted**: 05-07-2026 - **Published**: 12-07-2026*

the total time required to complete a handover. Efforts have been made by researchers to minimize the Mobile IP handover disruption. In general, there are two categories of methods: smooth handover and fast handover. Smooth handover and fast handover are two different concepts. "Smooth" means the number of packets lost caused by a handover should be none or negligible. "Fast" means the period of performing a handover should be as short as possible. However, these two different concepts are linked. A smooth handover should be fast enough for any packet delays not to trigger higher-layer retransmissions or cause too much disruption for delay-sensitive services; a fast handover in turn makes the handover smoother, and a fast handover scheme combined with a smooth handover scheme, since some packet loss can be inevitable under any fast handover scheme. A great number of proposals have been brought forward with regard to the Mobile IP fast and smooth handover issue. They summarized into three basic approaches: tunnel-based handover, multicast-based handover, and link-layer assisted handover. The link-layer assisted handover solutions of IP layer solutions are implemented and discussed.

Conclusion

Based on the analysis of the major Mobile IP handover optimization algorithms (IPv4 Mobility), an algorithm based on a Mobile IP proposed. First of all, we established constraints to ensure network connectivity, under the premise of meeting the constraints, by controlling the transmission power to establish an effective transmission link and reduce unnecessary connections; secondly, based on ensuring network connectivity, the use of planar geometry to draw auxiliary lines, and geometric cutting, the location of the node is divided into different regions, for different regions of the topology of the link. Finally, according to the remaining IP mobility sending data, an adaptation function is established, and different neighboring nodes are selected for data transmission by the adaptation function so that the energy consumption of shared to optimize the enhancement efficiency. Mobile IP related protocols (e.g. MIPv4 LLH, HMIPv4 and FMIPv4) to accelerate the deliveries of signaling or urgent data without introducing new security vulnerabilities. The Two-Way Registration scheme was further developed. Many enhancement schemes to optimize the agent-based Return Routability test for the MIPv4 route optimization proposal are implemented for performance evaluation.

Conflict of interest. Nil

References

1) Gao Q, Acampora A. A virtual home agent based route optimization for mobile IP. In: 2000 IEEE Wireless Communications and Networking Conference; 2000 Aug 6; Chicago, IL. New York: IEEE; 2002.
2) [Author unknown]. Topology Control and Medium Access Control (MAC) Protocol for Wireless Sensor Networks (WSNs) in Cyber-Physical System. [Publication details missing in original text].
3) Wang H, Zhou G, Bhatia L, Zhu Z, Li W, McCann JA. Energy-neutral and QoS-aware protocol in wireless sensor networks for health monitoring of hosting systems. IEEE Trans Ind Inform. 2020;16(8):5543–5553.
4) Wang H, Li J, Gao H, Zheng X. Gateway bandwidth arrangement of data transmission in cyber-physical system. Int J Sens Netw. 2018;27(1):14–25.
5) Yazdi FR, Hosseinzadeh M, Jabbehdari S. A priority-based MAC protocol for energy consumption and delay guaranteed in Wireless Body Area Networks. Wirel Pers Commun. 2019;108(3):1677–1696.
6) Bharghavan V, Demers A, Shenker S, Zhang L. MACAW: A media access protocol for wireless LANs. In: Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM); 1994 Aug 31-Sep 2; London, UK. New York: ACM Press; 1994. p. 212–225.
7) Bolch G, Greiner S, de Meer H, Trivedi KS. Queueing Networks and Markov Chains. 1st ed. New York: John Wiley and Sons; 1998. Chapter 10; p. 423–430.
8) Gamal AE, Mammen J, Prabhakar B, Shah D. Throughput-delay trade-off in wireless networks. In: Proceedings of IEEE INFOCOM; 2004 Mar 7-11; Hong Kong. New York: IEEE; 2004.
9) Gupta P, Kumar PR. Capacity of wireless networks. IEEE Trans Inf Theory. 2000 Mar;46(2):388–404.
10) Karn P. MACA: a new channel access method for packet radio. In: Proceedings of the 9th Computer Networking Conference; 1990 Sep 22; London, Ontario. 1990. p. 134–140.
11) Kumar A, Manjunath D, Kuri J. Communication Networking: An Analytical Approach. San Francisco: Morgan Kaufmann Publishers; 2004. Chapter 8; p. 456–476.
12) Caceres R, Padmanabhan V. Fast and scalable wireless handoffs in support of mobile Internet audio. ACM J Mob Netw Appl. 1998 Dec;3(4):351-363.
13) Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460. 1998 Dec.
14) Droms R, Bound J, Volz B, Lemon T, Perkins C, Carney M. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3315. 2003 Jul.
15) Thomson S, Narten T. IPv6 Stateless Address Autoconfiguration. RFC 2462. 1998 Dec.
16) Narten T, Nordmark E, Simpson W. Neighbor Discovery for IP Version 6 (IPv6). RFC 2461. 1998 Dec.
17) Conta A, Deering S. Generic Packet Tunneling in IPv6 Specification. RFC 2473. 1998 Dec.

***Received**: 07-05-2026 - **Accepted**: 05-07-2026 - **Published**: 12-07-2026*

18) Plummer D. An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware. RFC 826. 1982 Nov.
19) Nikander P, Aura T, Arkko J, Montenegro G, Nordmark E. Mobile IP version 6 Route Optimization Security Design Background. Internet-Draft [draft-nikandermobileip-v6-ro-sec-00.txt]. 2003 Apr.

Received*: 07-05-2026 -* ***Accepted****: 05-07-2026 -* ***Published****: 12-07-2026*