An Analysis of The Fast Handovers for Mobile IPv6 Protocol

Janne Lundberg
Helsinki University of Technology
Laboratory for Theoretical Computer Science

May 28, 2003

Abstract

Fast Handovers for Mobile IPv6 is an internet draft that gives a solution to the problem of packet loss during the handover procedure of Mobile IPv6. The draft attempts to solve the problem by establishing temporary tunnels between access routers. The tunnels are used to forward packets that would otherwise be sent to an address where the mobile node would not be able to receive them. The solution also allows access routers to temporarily store packets before they need to be delivered to the mobile node. In this paper we analyze the reasons why Mobile IPv6 experiences packet loss and what can be done to solve the problem. We also present the Fast Handovers for Mobile IPv6 draft, and analyze its suitability for solving the problem of packet loss during Mobile IPv6 handovers.

1 Introduction

Mobile IPv6 [3] is the current IETF proposal for a standard that enables a mobile computer to maintain its IPv6 address and transport layer connections while its point of attachment to the network changes. One of the fundamental principles in Mobile IPv6 design has always been, that mobility should never be visible to applications. The design principle has resulted in a very complex architecture and in a protocol which is extremely heavy. One problem in Mobile IPv6 is the amount of time it takes to register a mobile node to a new link. While a mobile host is registering itself to a new link, it can usually no longer communicate through its previous link. Since the registration delay is long, a significant number of packets will be lost, which may result in an unacceptable quality of service for the user.

The Fast Handovers for Mobile IPv6 draft attempts to mitigate the registration delay by acquiring information that is needed to join a new link before disconnecting communication at the old link. The system utilizes co-operating access routers which can request information from other access routers that are possible candidates for a handover. The mobile host uses the received information to prepare itself for the handover, which it can perform in many cases entirely without packet loss, even though connectivity to the network will be lost for a short period of time.

In this paper, we present the Fast Handovers for Mobile IPv6 draft and analyze the ability of the protocol to support seamless handovers between access routers. We assume that the reader has basic knowledge about Mobile IPv6, and we will only give introductions to topics that are added to the architecture by the Fast Handovers for Mobile IPv6 draft. The rest of this paper is organized as follows. In Section 2, we discuss the reasons for the latency in handovers and other possible solutions to the problem. In Section 3, we describe the operation of the fast handover protocol for Mobile IPv6. Section 4 analyzes the effectiveness of the suggested protocol. Finally, Section 5 concludes the paper.

2 Background

To understand the problem that is being solved by the Fast Handovers for Mobile IPv6 draft, we must first understand the problems in Mobile IPv6. The Mobile IP working group did not design the protocol to support frequent handovers, and if Mobile IP is to be used in an environment which may require handovers several times per second, the basic protocol becomes essentially useless. Any optimizations to the basic Mobile IP protocol need to be provided in separate drafts. The Fast Handovers for Mobile IPv6 draft is one such extension.

We assume that no link layer specific optimizations are used and the wireless networking interface in the mobile node can be connected to at most one link at any one time. That is, the mobile node is using a link technology which cannot receive data from other access points before it has terminated the link layer connection to its previous access router. We also assume that each mobile node has only one wireless interface, so it cannot use one interface to continue communicating with its current access point while it is searching for new access points using its other interface. The same implicit assumptions appear to have be used while writing the draft, although it has not been explicitly stated.

2.1 Sources of Delay

The delay in Mobile IPv6 handover is caused by a number of tasks that need to be performed. Some of the tasks can be performed in parallell, but some still require sequential processing. The basic Mobile IPv6 handover in a real life environment may proceed as follows.

1. **Change of link.** The handover starts when the mobile node either loses connection to its current access router or the mobile node otherwise determines that it should switch to another access router. In either case, the mobile node will lose its ability to communicate with the network before it can begin searching for a new access point. After a while, the mobile node reconnects to a new access point, and it can start to communicate using the new link.

2. **Movement detection.** The Mobile IPv6 draft calls to process of detecting arrival to a new link as movement detection. The primary movement detection mechanism in Mobile IPv6 is the IPv6 Neighbor Discovery protocol [5]. The mobile node listens for Router Advertisement messages and uses the received information to determine

that it has arrived to a new link. The original Neighbor Discovery specification allows routers to send unsolicited Neighbor Advertisements no more often than once every three seconds. The Mobile IPv6 specification changes the minimum delay between unsolicited advertisements to 50 milliseconds.

3. **Address acquisition.** When a mobile node has detected its movement to a new link, it needs to acquire a care of address from its new link before it can start to communicate with other nodes. The mobile node has two alternatives for acquiring an address. It can either use the Stateless Address Autoconfiguration protocol [6] or a stateful protocol, such as DHCPv6 [7], if it is available on the link. In the stateless address autoconfiguration protocol, the mobile node generates a tentative global address by combining an address prefix which has been received in a Router Advertisement message with a locally generated interface identifier. The tentative address is then sent to a link-local multicast group, to verify its uniqueness. If the request receives no reply, the tentative address is assumed to be unique and it is assigned to the interface.

   DHCPv6 can be used as a request-response protocol which immediately respond with an address. The DHCPv6 draft specifies that Duplicate Address Detection (DAD) should be performed even if the address has been generated using a stateful protocol. However, [6] states that DAD can be disabled if its overhead outweighs its benefits.

4. **Home agent update.** Next, a mobile host must update its home agent with the new care of address that it has acquired from the new link. The home agent is updated using a binding update (BU) message. The mobile node is required to receive an acknowledgement message from the home agent before proceeding to the next step in the handover. Thus, this step will add a delay the size of one round-trip-time tome the home agent.

5. **Return routability procedure.** After the home agent has been updated, the mobile node needs to send packets to ensure the return routability to its correspondent nodes. The mobile node sends two messages to its correspondent hosts simultaneously. One of the messages is tunneled through the mobile node's home agent, and the other message is sent directly to the correspondent node. Response messages to each of the messages are needed before the mobile node can continue to the next step in the handover. One of the answering messages is received via the tunnel from the home agent and the other one is received directly from the correspondent node. The actual contents of the messages are unimportant in this discussion.

6. **Binding updates.** Finally, after the return routability test has been completed, the mobile node can send the actual binding update message to its correspondent nodes, which completes the binding update.

Figure 1 illustrates performing a handover in Mobile IPv6. Current drafts are somewhat vague in describing what steps in the handover are absolutely required. In the figure, we have omitted completely the duplicate address discovery, as it is permitted when stateful address configuration is used. We also assume that no access control negotiations are needed before the access router on the target link allows the mobile node to start sending packets.

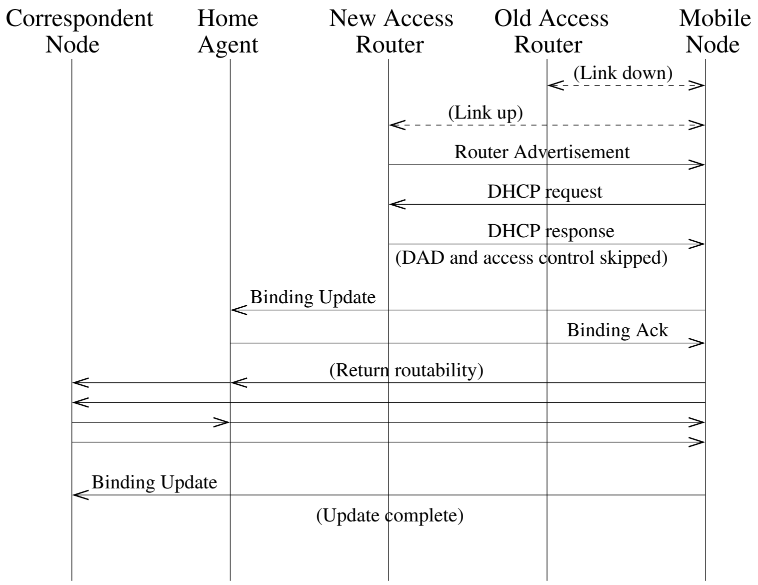

Figure 1: Mobile IPv6 handover.

If we consider the probable duration of each step in the handover process, we can see that a very large portion of the latency consists of only a few steps. The duration of step 1 is dependent on the properties of the link layer, and it is not discussed further in this paper. The duration of steps 2 and 3 depends on local settings of the new access point where the mobile node is being moved. Each one of steps 1-3 are operations that require communication only with devices that are located at the new access network, and will therefore not require communication with distant nodes with high propagation delays. A more serious source of delay is the communication required by steps 4-6. Each one of the steps requires communication with a node that may be physically very far away from the current location of the mobile node. Completing the handover requires a total of 3 round trips of messages to nodes which may be very far away from the mobile node. Even if we assume that all delay is a result of only signal propagation, the total latency can be as high 500ms if we are communicating with distant devices.

The total time of completing a Mobile IPv6 handover can be very substantial if the moving node is currently engaged in active communication with another host. The communication will be cut when the mobile node starts the handover procedure by disconnecting itself from its original access point. A new communication path is established only once the entire handover procedure has been completed, and every packet that was sent by the correspondent node during the handover signaling is lost.

2.2 Hierarchical Mobile IP

The Hierarchical Mobile IPv6 Mobility Management draft [1] suggests an alternative optimization for Mobile IPv6 which can be seen as complementing the Fast Handovers for Mobile IPv6 draft. The optimization can be used to reduce the latency of performing the Binding Update procedure by using a Mobility Anchor Point (MAP) that is located topologically near the current location of the mobile node. The MAP acts as a local home agent. A mobile node that needs to move to a new point of attachment in the network, only needs to register its new care of address at its current MAP. As the MAP should be topologically close to the mobile node, this update procedure can be performed rapidly. The mobile node may also benefit from a decreased number of signaling messages as route optimization may not be needed when Hierarchical Mobile IPv6 is used, and only the current MAP needs to be updated instead of a potentially large number of correspondent nodes.

3 Architecture

Fast Handovers for Mobile IPv6 is an extension to Mobile IPv6. Its goal is to reduce the number of packets that are lost during a handover by allowing the mobile node to use its previous Care of Address until the mobile node has completed the registration of its new Care of Address at the new access point. This is done by establishing a tunnel between the two access points that allows the mobile node to send packets as if it was connected to its old access point while it is completing its handover signaling at its new access point. The protocol consists of several improvements to Mobile IPv6, and the draft divides the protocol into three phases: handover initiation, tunnel establishment, and packet forwarding.

3.1 Terminology and Participating Components

The Fast Handovers for Mobile IPv6 draft introduces new terminology to Mobile IPv6. The most important new terminology that is required in this paper are the following.

Access Router (AR). The current default router of the mobile node. The mobile node uses its access router for communicating with nodes that are outside the current link of the mobile node.

Previous Access Router (PAR). The mobile node's default router before the handover. If the mobile node has established a care of address at its previous access router, the care of address at the PAR is called the Previous Care of Address (PCoA).

New Access Router (NAR). The mobile node's anticipated default router subsequent to its handover. Again, if the mobile node has established a new care of address at its NAR, the care of address at the NAR is called the New Care of Address (NCoA).

Bidirectional Tunnel (BT). A tunnel that is used by the PAR and the NAR to forward to a from the mobile node's Previous Care of Address.

Similar to the basic Mobile IPv6, the protocol requires signaling between mobile nodes and access routers. However, the protocol also has the requirement that access routers need to be able to communicate directly with each other to run the protocol. If the previous access router and the new access router are not able to communicated directly, a fast handover cannot be performed, and the mobile node will need to fall back to the basic Mobile IPv6 signaling.

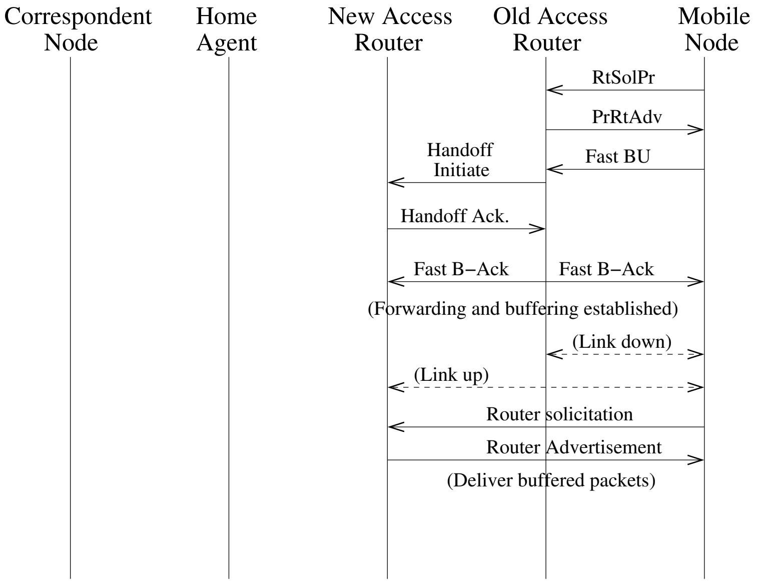

Figure 2: Handover in Fast Handovers for Mobile IPv6.

3.2 The Protocol

Figure 2 illustrates the fast handover protocol in the most basic case. A mobile node that anticipates the need to be moved to another access point, sends a Router Solicitation for Proxy message (RtSolPr) to its Old Access Router. In response to receiving the message, the router sends a Proxy Router Advertisement (PrRtAdv) to the mobile node. The PrRtAdv message contains all the information that the mobile node needs to connect to the NAR with only minimal delay. The information that is sent in the PrRtAdv message includes the new address that the mobile should start using on the new link, as well as the link layer address of the NAR. Once the mobile node has received the PrRtAdv message, it has all the information that it needs to connect to the NAR, and the mobile node is ready to perform the handover to the NAR. The mobile node can perform the RtSolPr - PrRtAdv exchange with a number of candidate access routers in preparation for handovers. The exchange by itself does not commit the mobile node to the handover.

When the mobile node decides to complete the handover, it sends a Fast Binding Update (Fast-BU) message to its Old Access Router (OAR). In response to receiving the Fast-BU message, the OAR sends a Handover Initiate message to the New Access Router (NAR) which the mobile node selected as the target for the handover. The New Access Router that receives the Handover Initiate message verifies the values that were included in the message, and sends a Handover Acknowledgement message back to the Old Access Router. When the Old Access Router receives the Handover Acknowledgement message, it completes its end of the bidirectional tunnel between the NAR and OAR, and sends a Fast Binding Acknowledgement (Fast B-Ack) message to both the mobile node and to the New Access Router.

When the New Access Router receives the Fast Binding Acknowledgement, it completes its end of the bidirectional tunnel, and starts buffering any packets that are received through the tunnel. The second Fast Binding Acknowledgement that is sent to the mobile node, informs the mobile node that it can leave the Old Access Router and start using the New Access Router. Once the mobile node has left the Old Access Router and established the link at the New Access Router, the mobile node sends a Router Solicitation message to the NAR, to inform it of the mobile nodes arrival on the link. As a result of receiving the Router Solicitation message, the NAR sends any buffered packets to the mobile node. Also, any packets that are received from the bidirectional tunnel from now on, are delivered directly to the mobile node without any buffering.

As can be seen from the figure, the protocol consists only of messages that are sent between nodes that are usually located topologically close to each other.

3.3 Network Initiated Handover

In the most basic form of the protocol, the handover is initiated by the mobile node. However, the protocol does not rely on the protocol being initiated by the mobile node. In the network initiated mode, the network initiates the handover by sending a gratuitous Proxy Router Solicitation (PrRtSol) message to the mobile node to be moved. Otherwise the protocol continues to operate as in the case of the mobile initiated handover.

Network initiated handovers have some advantages in comparison to mobile initiated handovers. The network may have topological information that it can use to select a target for the handover that is better suited for the mobile node. The network may also be able to collect and utilize other information, that is not available to a mobile node, to optimize handovers. Such information may include the level of congestion at different access points, or signal quality measurements from multiple access points. While such optimizations are possible, they are not discussed in the draft and will also therefore be omitted from this paper.

3.4 Three Party Handover

The three party handover occurs when a mobile node moves form its new access router (NAR) to another new access router (NAR') before it has registered a new care of address at the NAR and completed the Binding Update signaling with its Home Agent and all peers. In this case, the mobile node will need to update both the NAR and also the access router that the mobile mobile node was using prior to moving to the NAR. Both access routers will need to be informed about the access router which is the target of the handover, and new bidirectional tunnels will need to be established because packets may be arriving at both access routers simultaneously.

To complete a three party handover the mobile node sends the Fast Binding Update message to both the NAR and the PAR. In response to receiving the messages, both access routers will update their bidirectional tunnels to point at the NAR'. It is possible that a mobile node will need to perform a three party handover with an even larger set of access routers if the rate of handovers is temporarily very high and the mobile node has a large number of peers that need to be updated. In this case, all the previous access routers which may be registered in the binding caches of the peers need to be informed of the handover.

4 Analysis

In this section, we discuss the properties of the protocol. Our discussion consists of identifying and describing some fundamental properties and probable difficulties in the protocol.

4.1 Assumptions

The protocol makes some fundamental assumptions which must hold for the protocol to function. The draft describes the operation in an optimal environment with no obstacles to the protocol. In this section we identify some problems that have been bypassed in the draft, but which may become real problems that can hinder the implementation and deployment of the protocol.

Anticipated handovers. The mobile node must be able to anticipate link losses, as the mobile node must transmit the Fast Binding Update message prior to being disconnected from the current access router. If the mobile node has not been able to send the message prior to leaving the link, the bidirectional tunnel between the old access router and the new access router will not be established while the handover is in progress, and the packets that are sent to the old care of address will be lost.

Link discovery while communicating. If the mobile node is operating in the mobile initiated handover mode, the mobile node must be continuously looking for access points that may be potential targets for handovers. Whether or not this assumption is justified, depends on the underlying link technology. Even if the link technology does not allow this, it may be possible to install, for example, two wireless interface cards into a mobile device. In this case, one of the interfaces could be used for the actual communication while the other interface is only continuously looking for alternative access points.

Ability to select adequate access point. The draft offers no advice on selecting a suitable target router for the handover. Signal quality or strength do not usually give enough information to select the best candidate. For example, an access router that has very good signal quality can suddenly become completely invisible to the mobile node if the mobile node moves into a position that brings a heavy wall into the signal propagation path.

Trust between access routers. It is unrealistic to assume that access providers will allow their routers to respond to messages that are transmitted to them by another router from a network that belongs to some other access provider in another network. As the routers are able to automatically establish packet forwardings to arbitrary destination, this will open up a vulnerability which an attacker can exploit to forward packets to any destination in the Internet. Routers must therefore be able to trust one another to complete the handover. The routers must also be able to authenticate signaling messages to avoid forged messages. It is possible to protect signaling using IPsec, as fast handovers will usually be performed only between nodes that are physically close to each other, thus avoiding the problem of scalability. While authentication can be provided using a protocol, trust between access providers is inherently a political problem, and it is not clear whether or not fast handovers between access providers will be possible in practice.

No access negotiations. In its current form, the draft offers no way to perform access control negotiations. When a mobile node moves under a router that is administered by another organization than the previous access router, the mobile node will need to enter the link of the new acces router before it can begin negotiating for access rights into the new network. While the access negotiations are in progress, the network connectivity of the mobile node will not usually be possible.

4.2 Packet Loss

The protocol reduces packet loss by combining packet tunneling with buffering during the time the mobile node is switching between access routers. Before a mobile node detaches itself from its current access router, it has first established a tunnel between its current access router and the new access router where the mobile node will be transferred. When the tunnel is established, the new access router starts receiving packets that are destined to the mobile node. While the mobile node is establishing a connection to its new access router, the access router buffers the packets that it is receiving through the tunnel. When the mobile node announces its presence at the new access router by sending a Router Solicitation message, the buffered packets are transmitted to the mobile node.

If all the assumption in Section 4.1 hold, buffering at the NAR enables the mobile node to perform a handover without losing any packets.

4.3 Delay

Running the protocol results in two different forms of delay. First, the protocol requires time to prepare for handovers while the mobile node is still residing at its current access router. This can be done in the background, and the process can be initiated immediately when the mobile node enters a new link.

Another more important type of delay is caused by the actual handover between nodes. During the handover, the mobile node cannot send packets because it is not connected to an access router in any network. Since, as Figure 2 shows, the fast handover signaling consists of only messages that are sent to nodes that are topologically close to one another. Thus, the signaling delay can usually be expected to be relatively small. The actual delays that are required for the signaling to be completed will eventually depend on the efficiency of the protocol implementations and cannot be reliably estimated by only examining protocol specifications such as the Fast Handovers draft.

4.4 Discussion

The draft offers implementators great leeway in their implementation of the protocol. The draft does not offer any advice to many critical implementation issues. For example, the draft completely ignores describing ways in which the mobile node selects the best possible access router where it should be handed over. Nor does the draft attempt to give any insight into how to determine the need for handoffs, but only abstracts the issue behind concepts such as layer-2 triggers. Each implementor needs to interpret the abstractions in a way that is suitable to the environment and operating system that the implementor is using. It is also possible or even probable, that any particular implementation which will be suitable in one environment, will be completely unsuitable in another. Thus, any accurate analysis of the protocol would require focusing the analysis on some particular implementation and on its properties.

5 Conclusion

Fast Handovers for Mobile IPv6 is a protocol that can, in some situations, solve the problem of frequent and seamless handovers in Mobile IPv6. The protocol is based on building bidirectional tunnels between access routers, and on buffering data at access routers while the mobile node is completing its handover to a new link. In principle, the protocol can completely eliminate packet loss that would occur as a result of a mobile node moving to a new access point.

However, the protocol may be very sensitive to any anomalies in the network, and it will only work correctly when all its assumptions hold. For example, a mobile node must be able to determine, in advance, the access point where it should be handed over to receive the optimal connectivity. This is one example of a task that may not be possible in practice. Furthermore, as the draft currently specifies only the communication between the nodes and not the actual algorithms that are used to make the handover decisions, it is very difficult to make any reliable assesments about the effectivity of the protocol without focusing on the properties of some particular implementation of the protocol.

References

[1] Hesham Soliman, Claude Castelluccia, Karim El-Malki, Ludovic Bellier. Hierarchical Mobile IPv6 Mobility Management (work in progress). Internet draft, Internet Engineering Task Force, 2002.

[2] Rajeev Koodli. Fast Handovers for Mobile IPv6 (work in progress). Internet draft, Internet Engineering Task Force, 2002.

[3] David Johnson, Charles Perkins and Jari Arkko. Mobility Support in IPv6 (work in progress). Internet Draft, Internet Engineering Task Force, 2003.

[4] Thomas Narten and Richard Draves Privacy Extensions for Stateless Address Autoconfiguration in IPv6. Request for Comments 3041, Internet Engineering Task Force, January 2001.

[5] Thomas Narten, Eric Nordmark and William Simpson. Neighbor Discovery for IP Version 6 (IPv6). Request for Comments 2461, Internet Engineering Task Force, December 1998.

[6] Susan Thomson and Thomas Narten. IPv6 Stateless Address Autoconfiguration. Request for Comments 2462, Internet Engineering Task Force, December 1998.

[7] Ralph Droms, Jim Bound, Bernie Wolz, Ted Lemon, Charles Perkins and Mike Carney. Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (work in progress). Internet draft draft-ietf-dhc-dhcpv6-28.txt, Internet Draft, Internet Engineering Task Force, November 2002.