Mobile IPv6 Protocols

Khaled Mahmood Al-Adhal,
Department of CSE, Faculty of Engineering & Technology
MANAV RACHNA INTERNATIONAL UNNIVERSITY

Dr. S. S. Tyagi
Professor& HoD,
CSE, FET, MRIU

***Abstract*:To work out the quandary of packet loss for theperiod of the handover procedure of Mobile IPv6, an internet draft referred to as Fast Handovers for Mobile IPv6, stretches a crack Mobile IPv6. The draft endeavors to solve the glitch by establishing transitory tunnels amid the access routers.**

The tunnels are used to onward the packets that would else be sent to an address where the mobile node would not be able to receive them. The way out also countenances access routers to momentarily store packets before they are ceded to the mobile node. This paper analyzes the grounds why Mobile IPv6 is subjected to packet loss and gets a hold of the keys to this lock. We also present the Fast Handovers for Mobile IPv6 draft, and analyze its appropriateness for solving this problem of packet loss during the handovers.

1. INTRODUCTION

Mobile IPv6 [2] is the current IETF proposal for a touchstone that empowers a mobile computer to uphold its IPv6 address and transport layer connections while its point of attachment to the network deviates. Invisibility of mobility is one of the major concerns of Mobile IPv6's design. The design has resulted in a very complex architecture and in a protocol which is tremendously heavy.

The expanse of time Mobile IPv6 takes to register a mobile node to a new link is an added problem. While a mobile host registers itself to a fresh link, it usually loses communication to its aforementioned link. Since the registration lag is protracted, a hefty number of packets are lost, which may result in an objectionable quality of service for the punter.

The outline for the Fast Handovers for Mobile IPv6 bids to mitigate the registration delay by procuring information that is obligatory to seam a new link before disconnecting the interaction with the erstwhile link. The system exploits the co-operating access routers to call information from other access routers that are probable entrants for a handover. The mobile host primes itself for the handover by using the received information. This can be performed in many cases utterly without packet loss, even though connectivity to the network will be absent for a fleeting period of time.

In this paper, we expound the Fast Handovers for Mobile IPv6 draft and analyze the ability of the protocol to support seamless handovers between access routers. We take for granted that the reader has the rudimentary knowledge about Mobile IPv6, and we will only impart taster to topics that are appended to the architecture through 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 apprehend the problem that is being unrivalled by the Fast Handovers for Mobile IPv6 draft, we must first twig 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 environment they require handovers several times per second, the basic protocol becomes entirely useless. Any optimizations to the basic Mobile IP protocol have 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 exercised and the wireless networking interface in the mobile node can be connected to at most one link at a time. The mobile node uses a link technology that does not receive data from other access points before it has terminated the link layer connection to its previous access router. We also presuppose that each mobile node has a solitary wireless interface, so it cannot use that interface to continue communicating with its current access point while it searches for new access points using its supplementary interface. The same implicit assumptions appear to have been used while writing this draft, although it has not been unambiguously stated.

2.1 Analysis 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 parallel, but some still require sequential processing. The basic Mobile IPv6 handover in a real life environment may ensue as follows.

1) Movement detection. The handover starts when themobile node either loses connection to its current access router or the mobile node requires a switch to another access router. In either case, the mobile node will lose its ability to communicate with the network before it may embark on hunting 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) Configuration Time. The Mobile IPv6 draft is thedetecting of arrival to a new link as movement detection. The principal movement detection mechanism in Mobile IPv6 is the IPv6 Neighbor Discovery protocol [1]. The mobile node listens for Router Advertisement messages and uses the received information to ascertain its arrival at a new link. The newfangled Neighbor Discovery specification consents the routers to send unsolicited Neighbor Advertisements not more than once in every three seconds. The Mobile IPv6 speciation reduces the minimum delay between the unsolicited advertisements to 50 milliseconds.

3) Registration. A care of address is required when amobile node has to move to a new link, before it tends to start communicating with other nodes. The mobile node has two discretions to get hold of an address. It can either use the Stateless Address Auto configuration protocol [2] or a tasteful protocol, such as DHCPv6, if it is available on the link. In the stateless address auto-configuration 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 projected 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 responds with an address. The DHCPv6 draft stipulates that Duplicate Address Detection (DAD) should be performed even if the address has been generated using a tasteful protocol. However [1], states that DAD can be disabled if its overhead outweighs its benefits.

4) Home agent update. A mobile host must update its homeagent with the new care of address that it has acquired from the new link. A binding update (BU) message is used to update the home agent. The mobile node receives an acknowledgement message from the home agent before proceeding to the next step in the handover. Thus, this step will add an impediment to the size of one round-trip-time to the home agent.

5) Return rout-ability procedure. After the home agent hasbeen updated, the mobile node sends packets to ensure the return rout-ability to its correspondent nodes.

The mobile node sends two messages to its correspondent hosts in chorus. One of the messages is tunneled through the mobile node's home agent, and the other message is sent directly to the correspondent node. Rejoinders 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 no great shakes in this confab.

6) Binding updates. Finally, after the return rout-ability testhas 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 categorically required. In the fig, we have omitted completely the duplicate address discovery, as it is admissible when stateful address configuration is used. We also assume that no access control negotiations are needed before the access router on the target link countenances the mobile node to start sending packets.

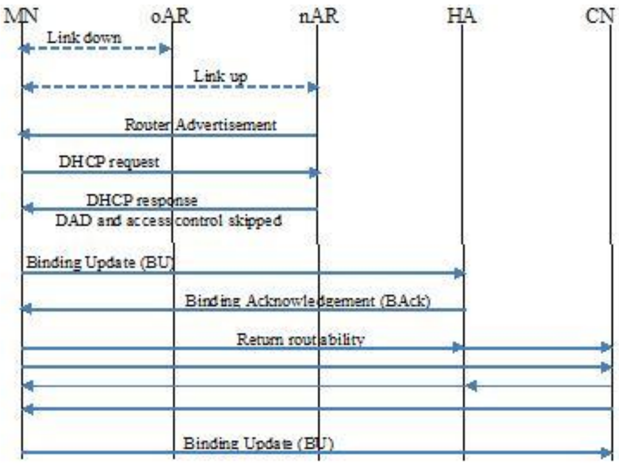

Fig.1 Handoff of Mobile IPv6

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, which is not discussed further in this paper. The duration of steps 2 and 3 depends on local settings of the neoteric access point to where the mobile node is being moved. Each of steps are operations that require communication only with devices that are ferret out at the new access network, and will therefore not require communication with distant nodes with high propagation delays. A more sombre 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 circuits 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 far-flung devices. The total time of completing a Mobile IPv6 handover can be very abundant if the moving node is currently employed in active communication with another host. The communication will be cut when the mobile node starts the handover procedure by disconnecting itself from its fundamental access point. A new communication path is established 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 [6] suggests an another course of action for the optimization of Mobile IPv6, which can be seen as a round out of 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 topo-logically in the radar of the current location of the mobile node. The MAP deeds a local Home Agent. A mobile node that needs to move to a new point of attachment in the network needs to register its new care of address at its current MAP. This update is quick as the MAP is topologically close to the mobile node. The mobile node may also benefit from a decreased number of signaling messages as route optimization may not be call for when Hierarchical Mobile IPv6 is used. Only the current MAP needs to be updated instead of a bulky number of correspondent nodes.

3. ARCHITECTURE

Fast Handovers for Mobile IPv6 is basically an extension to Mobile IPv6. Its end is to shrink the number of packets that are mislaid during a handover by countenancing the mobile node to use its forgoing Care of Address until the mobile node has completed the registration of its new Care of Address at the new access point. This is thru by establishing a tunnel between the two access points that allows the mobile node to despatch packets as if it was connected to its old access point while it is completing its handover pointing at its new access point. The modus operandi consists of several improvements to Mobile IPv6, and the draft rifts the protocol into three phases: handover initiation, tunnel establishment, and packet forwarding.

3.1 Terminology and Participating Components [1]

The Fast Handovers for Mobile IPv6 draft announces new terminology to Mobile IPv6. The latest lexis that is of utmost prominence in this paper is as follows.

- Access Router (AR): The current default router ofthe mobile node is the AR. The mobile node uses its access router for communicating with nodes that are free-standing to the current link of the mobile node.
- Previous Access Router (PAR): It is the mobilenode'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 baptized as the Previous Care of Address (PCoA).
- New Access Router (NAR): The mobile nodesanticipated 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 christened the New Care of Address (NCoA).
- Bidirectional Tunnel (BT). It is a tunnel that is usedby the PAR and the NAR to headlong from the mobile node's Previous to a Care of Address.

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

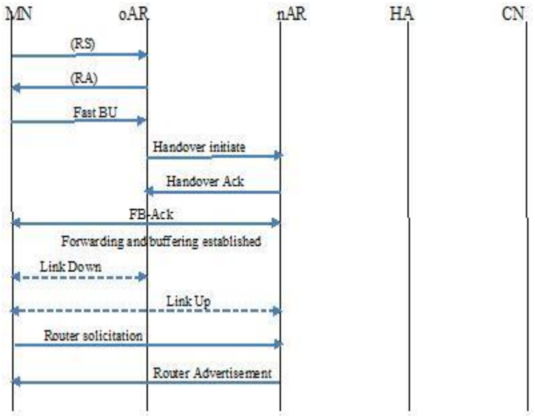

Fig 2: Fast Handover Mobile IPv6.

The Protocol [5]

Figure 2 exemplifies 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 bond to the NAR with 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 retort to receiving the Fast-BU message, the OAR sends a Handover Initiate message to the New Access Router (NAR) which the mobile node plumped 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 shoots 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 appraises the mobile node that it can leave the Old Access Router and onset 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 influx on the link. As an upshot of grasping the Router Solicitation message, the NAR sends buffered packets to the mobile node[4].

Also, any packets that are received from the bidirectional tunnel afterwards are delivered directly to the mobile node without any buffering.

As can be seen from the fig, 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 [3]

In the most basic form of the protocol, the handover is initiated by the mobile node. However, this protocol does not bank 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 redeployed. Otherwise the protocol endures to manoeuvre as in the case of the mobile initiated handover.

Network initiated handovers have some plusses in comparison to mobile initiated handovers.

The network may have topological information that can aid in target selection for the handover that is well-matched for the mobile node. The network may also be able to amass and employ other information that is not accessible 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 in the cards, they are not chewed over 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 pears [7].

In this case, the mobile node will need to update both the NAR and the access router that the mobile node was using prior to moving to the NAR. Both access routers will have to be updated about the access router which is the target of the handover, and new bidirectional tunnels will be set up because packets may be arriving at both access routers simultaneously.

To meet the ends of a three party handover the mobile node sends the Fast Binding Update message to both the NAR and the PAR. In rejoinder to receiving the messages, both access routers will update their bidirectional tunnels to direction at the NAR'. It is possible that a mobile node will have 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 associates 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 central conjectures which must be held for the protocol to function. The draft portrays the operation in a peak environment with no stumbling block to carry out the protocol. In this section we identified 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 toanticipate link losses, as the mobile node must transmit the Fast Binding Update message prior to being disconnected from the in progress access router. If the mobile node has not been able to send the message before 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 isoperating in the mobile initiated handover mode, the mobile node must be unremittingly scrutinizing 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 nocounsel 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 thataccess 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 forwarding's 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 on-going form, the draft offersno 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 pass into the link of the new access 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 disengages itself from its current access router, it has already 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 holds true, buffering at the NAR enables the mobile node to perform a handover without losing any packets.

4.3 Delay

Running the protocols 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 important type of impediment is caused by the actual handover between nodes.

During the handover, the mobile node cannot send packets if it is not connected to an access router belonging to any network. 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 adjournment 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 the users great leeway in their implementation of the protocol. The draft does not offer any advice to several critical implementation issues. For example, the draft completely ignores the ways in which the mobile node selects the best possible access router as its destination. Nor does the draft attempt to give any insight into how to determine the need for handoffs, but only sketches the issue behind concepts such as layer-2 triggers. Each user needs to interpret the abstractions in a way that is apposite to the environment and operating system that the user is using. It is also possible or even probable, that any particular implementation which will be suitable in one environment will be completely inappropriate 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 selective state of affairs, solve the problem of frequent and seamless handovers in Mobile IPv6. The protocol is grounded 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 transpire as an effect 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 are sustained. 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 assessments about the affectivity of the protocol without focusing on the properties of some particular implementation of the protocol

REFERENCES

[1] Cong Hung. TRAN a, Van T.T DUONG Mobile IPv6 Fast Handover Techniques Published in: Advanced Communication Technology (ICACT), 2011 13th International Conference Page(s): 1304 – 1308, year 2008

[2] Charles E. Perkins, "Mobile IP" (publisher: prentic hall] (Feb.2008), second edition.

[3] D.R.W.Holton, "A Cross-Layer Decision for Mobile IP Handover", Published in: Advanced Information Networking and Applications (AINA), 2010 24th IEEE International, Page(s): 641 – 646, 20-23 April 2010. HA

[4] Fayza nada "performance analysis of Mobile IPv4 and Mobile IPv6" The international Arab journal of information technology, vol 4, No 2, April 2007.

[5] Reza Farahbakhsh, "Smooth Handover by Synchronizing Context Transfer Protocol and Fast Mobile IPv6", Published in: Internet Multimedia Services Architecture and Applications (IMSAA), 2009 IEEE International Conference, Date of Conference: 9-11 Dec. 2009, Page(s): 1 – 5.

[6] Vivaldi, I, Habaebi, M.H. Ali, B.M. and Prakesh, V, " Fast handover algorithm for hierarchical mobile IPv6 macro-mobility management", Published in Communications, 2003, APCC 2003. The 9th Asia-Pacific Conference, (Volume: 2), Page(s): 630 - 634 Vol.2, Date of Conference: 21-24 Sept. 2003

[7] Yong-Geun Hong, Myung-Ki Shin, Hyoung-Jun Kim, " Fast Handover for Mobile IPv6 using Access Router Based Movement Detection and CoA Configuration", Published in: Vehicular Technology Conference, 2004. VTC 2004-Spring, 2004 IEEE 59th, (Volume:4), Page(s): 2442 - 2446 Vol.4, Date of Conference: 17-19 May 2004