MOBILITY SUPPORT AND SOFT HANDOVER PROTOCOL FOR IP-NETWORKS

Jukka Mäkelä, Timo Hämäläinen
University of Jyväskylä, Department of Mathematical Information Technology, P.O. Box 35, FIN-40100 Jyväskylä, FINLAND

Gábor Fekete, Jorma Narikka, Anna-Maija Virkki
Jyväskylä Polytechnic, School of Information Technology, Piippukatu 2, FIN-40100 Jyväskylä, FINLAND

Keywords: Handover, routing, wireless communications, mobility.

Abstract: In this paper, a handover mechanism that offers soft handover support between two different IP subnets for mobile clients is introduced. This handover is a part of a whole mobility support protocol consisting of several components. The handover is based on a protocol that introduces new methods for updating the location of mobile nodes. The handover is designed to cause no or minimal packet loss and be fast. It uses two different interfaces for achieving it.

1 INTRODUCTION

The number of mobile devices used has been increased in the past few years and they are expected to be widely used in the near future. The evolution of mobile devices has increased the use of IP based applications through wireless links. The normal routing mechanisms cannot meet the requirements of mobility and new protocols for handling the movement of mobile devices are needed. At present IPv4 is the most commonly used protocol in IP networks and Mobile IPv4 (Perkins C., 2002) is the introduced protocol to handle mobility in those networks. IPv6 is already introduced to be the next generation of IP and Mobile IPv6 (Johnson D., 2003), (Perkins and Johnson, 1996), Hierarchical Mobile IPv6 (HMIPv6) (Soliman et al., 2004), (Castelluccia, 2000) and (Castelluccia, 1998) are proposals of techniques to handle mobility in IPv6 networks.

When moving between two access routers which reside in different subnets a mechanism called handover is needed and the time this handover needs to happen should be minimized. The location of the mobile node is also required to know because it won't locate anymore in its home network during its movement. In mobile IP the location of a mobile node is known at least by one of the routers in the home network. This router is acting as a home agent for the mobile node. In Mobile IP it is needed to send the binding update messages to the home agent when doing the handover for updating the mobile node's location. The distance between the home agent and the mobile node can be quite far and the time needed for the updating might increase because of this distance. There has been a lot of research about handover to handle the movement. It is proposed that the mobile node can update the information first with the access routers to increase the speed of the handover (Perkins and Johnson, 1996). The same kind of mechanism is also used in the handover mechanism introduced in this paper. The current IETF draft about fast handover (Koodli, 2003) develops the idea further so that handover latency could be minimized and the handover would be more beneficial and efficient. In (Sulander, 2004) a flow based method is introduced to decrease the handover time. In that method the data flow is directed to the mobile node from the first crossover router during the update mechanism.

A proposed extension, Hierarchical Mobile IPv6 (HMIPv6) to Mobile IPv6, introduces a new local home agent called mobility anchor point (MAP). The MAP is supposed to be closer to the mobile node than to its original home agent. The mobile node can do the updating first with this local MAP

Mäkelä J., Hämäläinen T., Fekete G., Narikka J. and Virkki A. (2004).
MOBILITY SUPPORT AND SOFT HANDOVER PROTOCOL FOR IP-NETWORKS.
In *Proceedings of the First International Conference on E-Business and Telecommunication Networks*, pages 121-126
DOI: 10.5220/0001385401210126

and after that with its own home agent. So the signaling latency during the handover can be reduced. Mechanisms where the mobile node can receive packets during signaling the update are also introduced. However, these protocols still cannot meet the requirements for applications, which are delay sensitive, such as voice, especially in macro mobility management (Vivaldi et al., 2003).

In this paper, we present a handover mechanism based on the idea presented in (Mäkelä, 2003), (Fekete, 2003). The brief description of the whole protocol functionality with new ideas of routing is going to be published in (Mäkelä et al., 2004). This presented protocol has a handover mechanism, which achieves soft handover. The idea is based on the fact that mobile node have several possible Layer 2 technologies available (network interface cards) when doing a vertical handover for IP based connection (e.g. WLAN and GPRS). When a mobile node has at least two interfaces for two different technologies the interfaces can be used simultaneously during the handover. The handover is made only between the access routers. The mobile node does not have to register its new location with the HA all the time. This handover is based on the idea that introduces mechanisms, similar to routing protocols, for updating the location of mobile nodes. The basic idea is that every router that takes part in the routing must know the current location of the mobile node. The use of these mechanisms offers ways to increase the speed of the handover and offers a way to accomplish soft handover.

2 NEW ROUTING PROTOCOL

The idea about handling the movement in IP-networks called DRiWE (Dynamic Routing in Wireless Environment) protocol (Mäkelä, 2003), (Fekete, 2003) introduces the mechanisms for handling the problems of routing for the mobile devices. The protocol considers only the mechanisms to handle the OSI Layer 3 movements.

The main idea of the protocol is that the routing decisions take place only in routers. Those routers, which participate in routing data flows for the mobile node, know the location of the mobile node. The routers use host specified information about mobile nodes in their routing tables besides the normal network based routing information. The protocol also introduces mechanisms to avoid the gratuitous growth of the routing tables. The routing table's growth is controlled by allowing the dropping of the routing information of the mobile node and getting it by a dedicated mechanism if needed. The protocol also includes an advertising mechanism so that routers can propagate the information about the location of mobile nodes to other routers.

To achieve soft handover, the mobile node uses two interfaces and communicates with both access routers (AR1 and AR2, in Fig. 1) at the same time during the handover. The connection to the new access router (AR2, in Fig.1) is formed before the old connection breaks. During the handover, the mobile node accepts incoming packets from both of its interfaces. Therefore, there is no need to stop the data flow at any time. The decision when the handover should happen is not concerned and is the one interesting topic for further research, see Chapter 6. Both interfaces are used only during the handover so that the current connection is used until the new connection is totally established and ready for the data flow. For solving all problems the protocol still needs more research. (Mäkelä et al., 2004).

3 HANDOVER

The handover mechanism must be supported by the access routers, mobile nodes and also by the intermediate routers between access routers. The correspondent node that communicates with the mobile node does not need any support for the protocol or for the handover mechanism. The intermediate routers need to support it because of the behaviour of the introduced update mechanism.

In the example scenario in Figure 1, the mobile node is attached to AR1 and it’s moving to the AR2's access network. When the mobile node is going to connect to the other access network it has to complete a Layer 3 handover for enabling the IP traffic. For enabling the connection in the foreign network the mobile node needs a temporary IP-address (care-of address) from the new access router (AR2, in Fig. 1). The care-of address query takes place through the current access router (AR1, in Fig. 1).

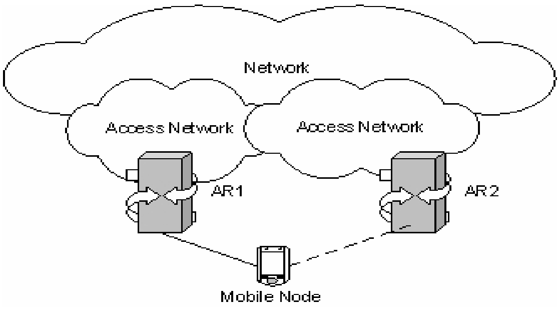

Figure 1: The handover.

For enabling the use of the HoA (the Home Address) of the mobile node as a source address for the outgoing packets tunneling is used between the mobile node and the access router. The packets go tunneled to the access router by using the care-of address as the source and the IP address of the access router as the destination for the tunnel (outer) packet. The access router decapsulates the packet and sends the original packet to the destination with source address being that of the mobile node's HoA. Packets destined to the mobile node are routed to their destination by using the HoA as the destination and will be routed to the current access router. The access router knows all the mobile nodes that are currently attached to its network and will deliver the packets to them.

After the mobile node is correctly attached to the access network of the new access router (AR2, in Fig. 1) the updating of the new location of the mobile node at the previous access router (AR1, in Fig. 1) starts. When the previous access router (AR1, in Fig. 1) gets the information about the new location of the mobile node it starts to forward packets destined to the mobile node to the new access router (AR2, in Fig. 1). After the successful update of the location between access routers the mobile node changes its default outgoing route to go through the tunnel towards the new access router (AR2, in Fig. 1) and the handover has successfully finished. Figure 2 presents the needed messages for getting the care-of address (CoA) an updating the location in a successful handover.

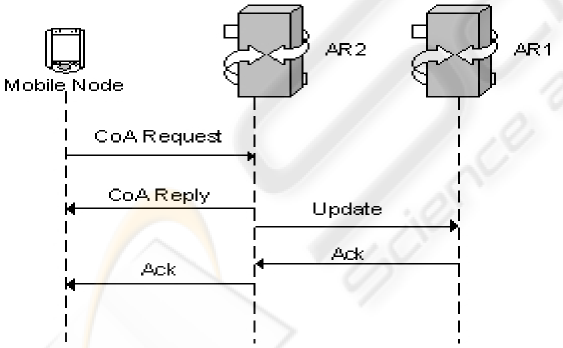

Figure 2: Handover messaging.

The DRiWE protocol introduces a mechanism for keeping the connections up between mobile nodes and access routers even when there are no packets to send or receive. It is done by the exchanging of timely Keep-Alive messages. The mechanism gives the information about link breaks to the mobile node. Without this, when there are packets to send, the broken connection may not be detected for quite a long time e.g. when using UDP. The mobile node can also be prepared for situations when it is ping ponging between two access routers or needs to use the older connection again especially when the current connection is lost and the older connection is still available. The use of this mechanism should be very carefully chosen not to cause extra traffic to the network or extra power consumption to the mobile node when trying to keep the interfaces up.

3.1 Update mechanism

The behavior of the mechanism used to update the location of the mobile node between access routers needs the update message to be handled at every router between the access routers. This is necessary because those intermediate routers have to update their information about the location of the mobile node accordingly. Other solution for sending the update messages is to use tunneling between the old and new access routers to forward the packets between them (AR1 and AR2, in Fig. 1). The DRiWE protocol introduces mechanisms, which allow routers to acquire the location of mobile nodes when needed to track down its current position for routing purposes.

The Update message is sent to the next router on the route to the destination (AR1, in Fig. 1). The first intermediate router adds the HoA of the mobile node included in the message to its routing table and the next hop will be the router from which this message was received. Every intermediate router between the access routers will do the same. When the update message reaches its destination (AR1, in Fig. 1) this access router changes its routing table and starts forwarding the packets to the mobile node through the new access router (AR2, in Fig. 1).

The update message is also acknowledged to the sender and to the mobile node. If the sender (AR2, in Fig. 1) doesn’t get the acknowledgement it sends the info about erroneous updating to the mobile node and the recovery mechanism will be started. The recovery mechanism is for recovering the location information in the affected routers back to the form it was before the update. The recovery works like the update mechanism but will be started also from both access routers (AR1 and AR2, in Fig. 1). So the recovery will propagate from both directions and will recover the situation back even when there is a link break between the access routers.

4 IMPLEMENTATION

A proof-of-concept version of the protocol has been implemented under Linux fully in user space. The implementation covers the entire fast handover mechanism and is based on IPv4. The implementation works with IPv4 but at this stage it is easy to port it to IPv6 since it does not use any IP specific things except for IP addresses.

The software was tested in a small Ethernet test network consisting of four routers, a workstation working as the MN and another as the CN. During the tests no TCP connections were lost between the MN and the CN while handing over, even when the handover failed (the update recovery mechanism corrected the paths).

This early draft implementation showed that the idea is workable. Even though no comparisons were made to other protocols, such as MIPv6, in the sense of practical testing but a theoretical comparison can be seen in the next chapter.

5 COMPARISON TO OTHER PROTOCOLS

The DRiWE protocol was designed with tools existing for user space protocol implementation and because of this there are some shortcomings which could be solved by redesigning the protocol to work more tightly in Layer 3 (now only routing table and interface address modifications are done using netlink sockets and ioctl calls in Linux).

MIPv6 is known (thought) to not being able to satisfy seamless handovers due to the procedures it has to accomplish during its handover phase. Besides Duplicate Address Detection (DAD) and authorizations, it needs to send BU messages to each of its CNs in order to update their knowledge of the actual location of MNs. Until the CNs are not updated they continue sending packets to the old CoA of the MN, thus resulting in possible packet losses if that CoA is not used by the MN any longer (e.g. it has only one interface). Plus, the MN has to register with its HA too. In the DRiWE protocol, during a handover only one Update message is sent out from the new AR to the old AR. This allows the MN to be accessible at the new AR immediately. It is because it can be assumed that it was reachable at the old AR and what the Update message did was that it updated the routing information of the old AR to forward packets for the MN towards the new AR.

Because of the update mechanism of the DRiWE handover, the MN may not be accessible on the best path from a CN. In MIPv6 it is accessible because every CN knows the CoA of the MN, so they can send packets to it using the best path (according to their and subsequent router's routing tables). In DRiWE, traffic is not routed to the MN by its CoA but by its HoA. It means that after a handover the MN is accessible through its old AR (and the routers between the old AR and the new AR, because they became updated by the update mechanism). For the MN to be accessible on optimised routes it is necessary to update the routers that store information about its previous (or older) location. For this a routing protocol can be used which is initiated by the MN through its current AR. A simple and fast routing protocol could do the job (like RIP).

In MIPv6 the HA is acting as a Proxy for Neighbour Discovery messages destined to the MN. It is used to make the local nodes in the home network to send packets destined to the MN to the HA's MAC address instead. The same mechanism is also needed for DRiWE for the same reason.

Timers for bindings in CNs and HAs are used by MIPv6 to drop unused bindings from their binding caches. In DRiWE, routers can drop unused routing table entries that correspond to MNs. It can be done either when the routing table size reaches a certain size or by maintaining a timer for unused entries (or both). Although, there are Keep-Alive messages exchanged between MNs and ARs to keep alive MN registrations. If the MN does not get Keep-Alive messages from the current AR for a specific amount of time it tries to change its AR back to the previous one. It is possible because the MN keeps alive its registration to the previous AR.

MIPv6 supports the discovering of the HA by a MN by means of Dynamic Home Agent Address Discovery (DHAAD). This mechanism can be used to DRiWE too.

The Home Address Destination Option (HoADO) is used by MIPv6 to avoid using tunneling of packets from the MN to CNs. If tunneling were used then the destination address in both the inner and outer IP headers would be the same, thus resulting in wasting bytes. For traffic from CNs to MNs the type 2 routing header is used. In DRiWE tunneling is used to send packets from the MN to CNs. The current implementation of the protocol uses a tunnel between the MN and the AR when sending packets to CNs outside the visited network. It means that these packets will have the MN's HoA as their source when reaching the CN. There is an issue when sending packets to CNs in the visited network, because in that case the MN would send them using its CoA as the source address even though the CN might be waiting for a packet from the HoA of the MN (in the case when the CN wants to talk to the MN at its HoA). Therefore, it is assumed that CNs should not use the CoA of the

MN, what's more, they should not even know it. There is no really need for a CN to send packets to the MN using its CoA in DRiWE. The CoA is considered to be known only by the respective access router and the MN. Another assumption is that all the packets sent by the MN have the HoA as the source (they go through the tunnel between the MN and the access router) and the MN is allowed to use its CoA for communication only with the access router. This way CNs always talk to the MN at its HoA.

In MIPv6 this is solved by manipulating packets in Layer 3 of the network stack and using HoADO and the type 2 routing header. Resulting in all the packets sent to CNs with bindings being seen at their destination as coming from the HoA of the MN. But when a CN has no binding for the MN it is not clear in MIPv6 which address will be used by the MN when sending packets to this CN (e.g for long term UDP connections established inside the visited network).

In FMIPv6 for the protocol to work there must be a router in the currently visited network that may work as a proxy for the MN. This proxy router is used to tunnel packets arriving to the MN's CoA in its network to the new AR in the new visited network. As mentioned in Chapter 3, the update mechanism can be implemented by using tunneling between the old AR and the new AR, thus making the old AR to tunnel packets destined to the MN's HoA to the new AR. This mechanism is more or less equal to the FMIPv6 way. Both protocols have to tear off the tunnel after some time. FMIPv6 when the MN has finished with updating the CNs, and DRiWE after the normal update mechanism (modifying/adding location information of the MN in the old AR and the routers towards the new AR).

The MIPv6 L3 handover starts after the MN has detected movement (already moved) to a new network (by receiving Routing Advertisements with unknown prefixes). For a DRiWE-handover to start the MN has to know the IP address of the AR beforehand. The same applies to FMIPv6.

MIPv6 by default supports MNs with one interface. DRiWE needs at least two interfaces of the same type. These two interfaces must be of the same type to provide smooth handover (one is used while the other is being configured). FMIPv6 also supports one interface by default, although to receive L2 information about the new AR while still connected to the old one it may need a second interface.

DRiWE implements fast and smooth handovers. Fast means that the handover needs less signalling than handovers for MIPv6, and smooth means that no or minimal number of packets get lost during the handover thanks to the use of multiple interfaces. Even though the handover is faster than of MIPv6's, the routes for reaching the MN after a handover may not be the optimal ones. For this an additional location advertisement is necessary (MN routing advertisement). In MIPv6 CNs have knowledge about the exact location of MNs by BU messages. In DRiWE, the knowledge in routers about MNs may not be direct. This is caused by the way the MN's location is updated during handovers. That is, to provide routers with exact location information of a MN, the MN has to advertise its location (MN routing advertisement). This advertisement can be matched with the sending of BU messages in MIPv6.

FMIPv6 provides fast handover for MIPv6 by reducing the necessary number of signalling during the handover process until the MN regains IP connectivity at the new AR. But after the fast handover the MN needs to send BU messages to CNs in order to use optimised routes. Therefore, it has a similar kind handover style as DRiWE. It has two phases, the first phase is to provide fast establishment of IP connectivity and the next is to “build “ optimised routes to the MN. Even though the second phase of FMIPv6's handover may be faster in large networks (with lots of routers) then that of DRiWE's, DRiWE may need less signalling in small networks with lots of CNs.

In FMIPv6, when the new AR receives the Handover Initiate (HI) message from the old AR, it starts to defend the new CoA of the MN until the MN arrives at the new network. The same kind of mechanism is needed in DRiWE for the same purposes as for FMIPv6. That is, to defend the new CoA from being used by another node in the network of the new AR until the MN arrives there. This defending means that the new AR must work as a proxy for neighbour discoveries for the MN for the new CoA.

Security was not designed into DRiWE yet, though it is obviously needed. For example only authenticated MNs must be allowed to register to ARs and to instruct them to start e.g. the update mechanism. For protocol messages sent between ARs and routers the same security considerations may apply as for normal routing protocols.

6 CONCLUSION AND FUTURE WORK

By the current design of the DRiWE protocol it can be seen that it may be useful in small networks where fast handover is necessary for MNs and the number of CNs the MN is communicating with is high. The maximum size of the networks in which the protocol could be used depends on the advertisement method of location information of MNs, which part of the protocol needs further research.

Even though there are a few issues remained to solve, the protocol is usable and the issues can be dealt with by moving some of the protocol mechanisms to lower layers (e.g. Layer 3).

Further research is needed to incorporate movement detection. There are several projects working in this interesting area, because it is needed by all the mobility support protocols as well (e.g. MIPv6).

It is also planned to make the protocol able to intelligently choose between various available access technologies (which also involves handover), that is to support vertical handover.

REFERENCES

Castelluccia C., 2000. HMIPv6: A Hierarchical Mobile IPv6 Proposal, *ACM Mobile Computing and Communications Review, vol.4, no.1, January 2000, Pages 48-59.*

Castelluccia C., 1998. A Hierarchical Mobility Management Scheme for IPv6. *Proceedings of the Third IEEE Symposium on Computers and Communications 1998 (ISCC '98), 30 June-2 July 1998, Page(s): 305-309.*

Fekete G., 2003. The implementation of the DRiWE Mobility Support Protocol. *Bachelor's Thesis, Jyväskylä Polytechnic*.

Johnson D., Perkins C. and Arkko J., 2003. Mobility Support in IPv6. *IETF draft, work in progress*.

Koodli R., 2003. Fast Handovers for Mobile IPv6. *IETF draft, work in progress*.

Mäkelä J., 2003. Dynamic routing for the wireless devices in IP-networks. *Master's Thesis, University of Jyväskylä, in finnish.* 2003.

Mäkelä J., Fekete G., Narikka J., Hämäläinen T., Virkki A-M.,2004. Soft handover and routing mechanisms for mobile devices. *To be published in The 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, September 2004, Barcelona, Spain*.

Perkins C., 2002. IP Mobility Support for IPv4, *IETF RFC 3344, August 2002.*

Perkins C. and Johnson D., 1996. Mobility support in IPv6. *Proceedings of the Second Annual International Conference on Mobile Computing and Networking (MobiCom'96), Rye, New York, USA, November 1996.*

Soliman H., Castelluccia C., El-Malki K., Bellier L., 2004. Hierarchical Mobile IPv6 mobility management (HMIPv6). *IETF draft, work in progress*.

Sulander M., Hämäläinen T., Viinikainen A., Puttonen J., 2004. Flow-Based Fast Handover Method for Mobile IPv6 Network. *Proceedings of the 59th Semi Annual Vehicular Technology Conference Spring 2004.*

Vivaldi I., Ali B.M., Habaebi H., Prakash V., Sali A., 2003. Routing scheme for macro mobility handover in hierarchical mobile IPv6 network. *Proceedings of the 4th National Conference on Telecommunication Technology 2003 (NCTT 2003), 14-15 Jan. 2003, Page(s): 88-92.*