International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 11 (2016) pp 7526-7531

Some Considerations for SCTP Handover Scheme in Mobile Network

Yong-Jin Lee

Department of Technology Education, Korea National University of Education,
250 Taesungtapyon-ro, Heungduk-ku, Cheongju, South Korea

Abstract
This paper presents some considerations on the performance improvement during the SCTP (stream control transmission protocol) handover. We first describe the related handover schemes in the mobile network including MIP (mobile IP) v4 and MIPv6. SCTP has multi-homing feature which can provide the mobile node with dual interfaces, so seamless data transfer between mobile node and correspondent node can be achieved. We suggest some performance improvement tips during IP address reconfiguration of the SCTP, especially in the ping pong behavior environment of the MN (mobile node). By manipulating the appropriate addition and deletion of IP address, we can reduce the handover latency during SCTP handover. In order to support our suggested scheme, we introduce the working set database and also discuss about the real environment application.

Keywords: MIPv4, MIPv6, fast handover, SCTP, working set

INTRODUCTION

Recent mobile application services have required the mobility management studies which can reduce the latency of end-user. The motivation of this paper is to study the mobility management in the computer network using IP address such as Internet, where many users move with the mobile device.
There have been a number of studies [1, 2, 3] on the mobility management schemes including handover latency. They have proposed a variety of handover mechanisms to be applied to the real network environment. Especially, mobile IPv4 and mobile IPv6 mechanism have been studied broadly. However, MIPv4 and MIPv6 cannot overcome the performance degradation problem such as latency since the packet loss mainly occurs during the handover. As an alternate solution, SCTP handover schemes with the IP address reconfiguration have been proposed [4, 5, 6].
This paper focuses on the IP address reconfiguration scheme during SCTP handover. The results reported in this paper can be used in the design and operation of mobile network. The objective of this study is to describe several mobility management schemes including IPv4 and IPv6 and propose the performance enhancement tips during SCTP handover. We achieve our objectives by proposing the working set model which provides the efficient IP address reconfiguration automatically.
The rest of the paper is organized as follows. In section 2, we describe several handover schemes in Mobile IPv4 and Mobile IPv6, respectively. Section 3 discusses some considerations for the performance improvement in SCTP handover scheme, followed by concluding remarks in section 4.

HANDOVER SCHEMES IN MOBILE IP

Mobile IPv4

In the micro mobility and the cellular IP approach [6], the mobility concept can be categorized in two classes: Macro mobility relates to movements of a MN (mobile node) among different IP domains or different wireless access networks; mobility management is held by a macro-mobility scheme, named MIP. Micro mobility relates to movements carried out among different micro-cells within the same IP domain. MIP is not appropriate to support fast, seamless handovers between
c
r

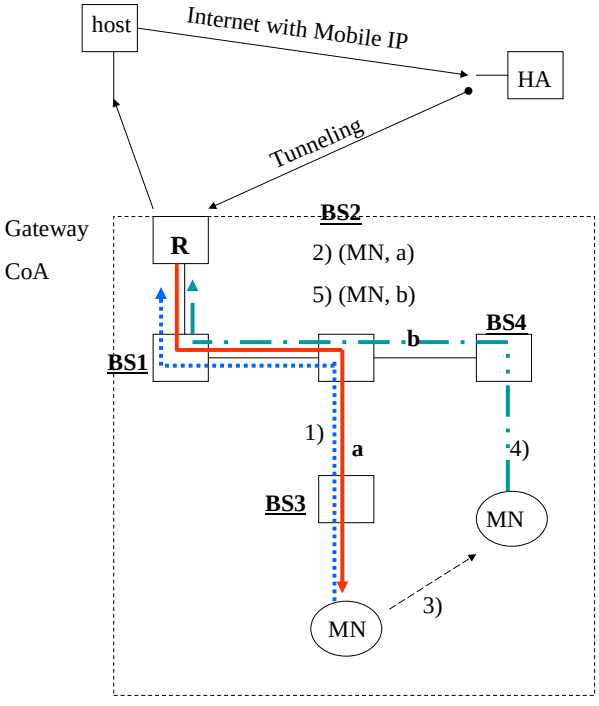


Figure 1: Micro mobility scheme

The micro mobility procedure in Figure 1 is as follows:
1) In the uplink routing, MN sends the data to the gateway.

2) After the data transmission of the MN, the routing cache in BS2 includes a mapping, (MN, a), which indicates that MN is reachable through interface "a". Cache entries are used to route the downlink packets (from the gateway to on the reverse path). Cache is refreshed by route-update packets (empty IP packets) that are periodically sent to the gateway by MN.
3) While moving from BS3 to BS4 during an active data session, the MN detects the stronger BS4 signal, tunes its radio to the channel used by BS4 (movement detection –handover initiated).
4) MN transmits a route-update packet (label "b" in the figure) that is cached by BSs along the path.
5) BS2 adds the new mapping, (MN, b) to its routing cache, thus keeping a double entry related to MN (the old and new route). Since the old mapping will be cleared only after the routing-cache timeout extinguishes, before this timeout both routers will coexist and packets addressed to MN will be delivered through both interfaces/path "a" and "b".

Fast handover in Mobile IPv4

There are two different mechanisms to obtain low handover latency in MIPv4. Firstly, the pro-registration handover procedure is as followings:

1) oFA (foreign agent) sends RS (router solicitation) to nFA.
2) nFA replies RA (router advertisement) to oFA. These procedures were performed before pre-registration handover. That is, oFA requests and caches RA's from neighbored nFA before handover.
3) PRS (proxy route solicitation) requests the advertisement from other routers excluding receiving router. This message is used only in the MN initiated handover.
4) When MN receives the PRS, it replies with PRA (proxy route advertisement).
5) MN sends the RR (register request) to nFA. Since MN has not been connected to nFA yet, this message is routed via oFA.
6) Register request and register reply are exchanged between HA (home agent) and nFA.

Secondly, Post-registration handover procedure is as followings:

1) Even if MN moves from oFA to nFA, it doesn't register with the nFA and defers the registration.
2) MN continues to use the oFA.
3) If MN moves to another nFA (nFA2) before registering the nFA (nFA1), the nFA2 sends signal to oFA while moving the one edge of tunnel to its own. That is, one edge of BET will remain in oFA until MN performs the MIP registration.

Especially, two-party post-registration handover scheme is represented in Figure 2.

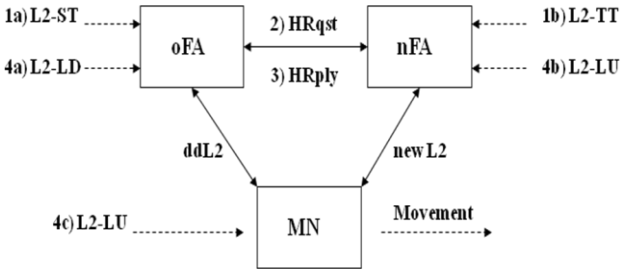


Figure 2: Two-party post-registration handover

Two party post-registration handover procedure is as the followings:

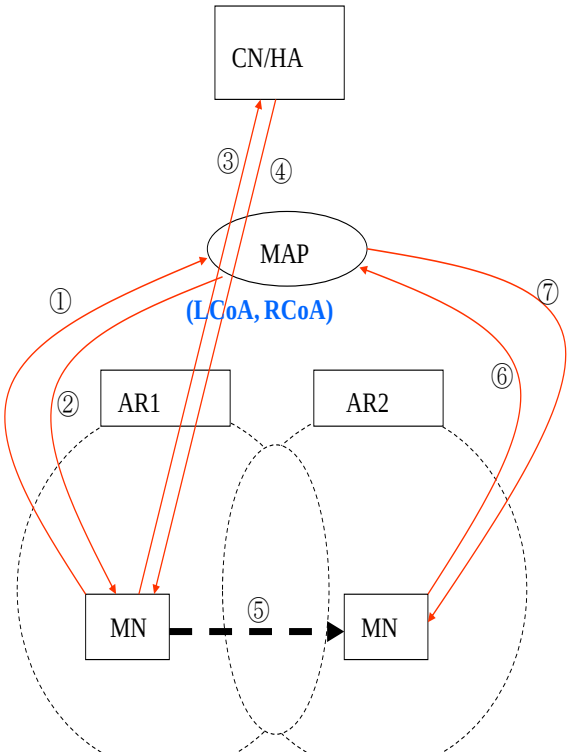
1a) ~ 1b) oFA or nFA receives L2 Trigger (L2-ST or L2-TT) which shows MN will move from oFA to nFA. 1a) When the oFA receives L2-ST, it contains L2 address of MN and ID (IP address or L2 address by which we can know IP address) of nFA.
1b) When the nFA receives L2-TT; it contains L2 address of MN and ID of oFA.
2) FA receiving L2 trigger sends the HRqst (handover request) message to other FA. For example, if oFA receives the L2 trigger, oFA sends HRqst to nFA. This message includes the lifetime of tunnel which oFA wishes to maintain, IP address of home network, home address of MN, L2 address options containing L2 address of MN.
3) FA receiving the HRqst sends the HRply (handover reply) to the other FA. For example, if oFA sends the HRply, this message includes the lifetime which oFA wishes to support, IP address of home subnet, and home address of MN and L2 address options containing L2 address of MN.
4) End of L2 handover is signaled by L2-LU trigger.
4a) When the oFA receives the L2-LD trigger, it forwards the data for MN by using the forwarding tunnel.
4b) When the nFA receives the L2-LU trigger, it starts to transfer data tunneled from oFA to the MN.
4c) Data from MN is forwarded to the next hop using the general routing method or through the reverse tunnel to oFA or nFA.

Mobile IPv6

The basic handover procedure in Mobile IPv6 [7, 8, 9, 10] is as follows:

1) MN detects the movement by using neighbor unreachable detection.
2) MN obtains a CoA using address auto-configuration.
3) MN performs the binding update.
4) CN sends binding acknowledges and binding is completed.
5) MN sends datagram to MN arrives on home network via standard IP routing.
6) The datagram is intercepted by the HA and is tunneled to the CoA.
7) MN sends the BU to CN.

8) Direct communication between MN and CN is accomplished.



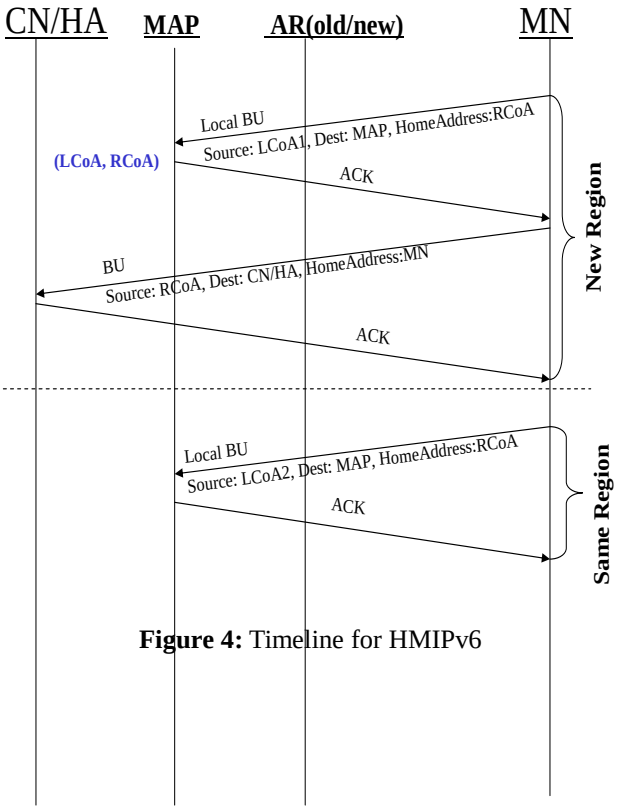


Figure 4: Timeline for HMIPv6

MN receives RA from AR1 (access router 1). RA contains the information that AR1 is included in MAP (mobility anchor point). MN configures LCoA and RCoA by using auto-configuration. HMIPv6 procedure is as followings:

① MN sends the local BU to MAP (source: LCoA based on the AR1 = LCoA1, destination: MAP, home address option: RCoA based on the MAP).
② MAP binds LCoA with RCoA and sends ACK to MN.
③ MN sends the BU to CN/HA (source: RCoA, destination: CN/HA, home address option: MN's home address).
④ MAP replies ACK.
⑤ MN moves from AR1 to AR2.
⑥ Since RCoA is the same as the previous address, BU/ACK is not necessary between MN and CN/HA. But, MN should send the local BU (LCoA2). At this time, if CN sends data to MN that arrives at MAP, data is forwarded to MN with the tunneling.
⑦ MAP replies ACK.

Fast handover in Mobile IPv6

There are two different mechanisms-anticipated handover and tunnel based handover to obtain low latency handover in MIPv6. Structure of anticipated handover for FMIPv6 is

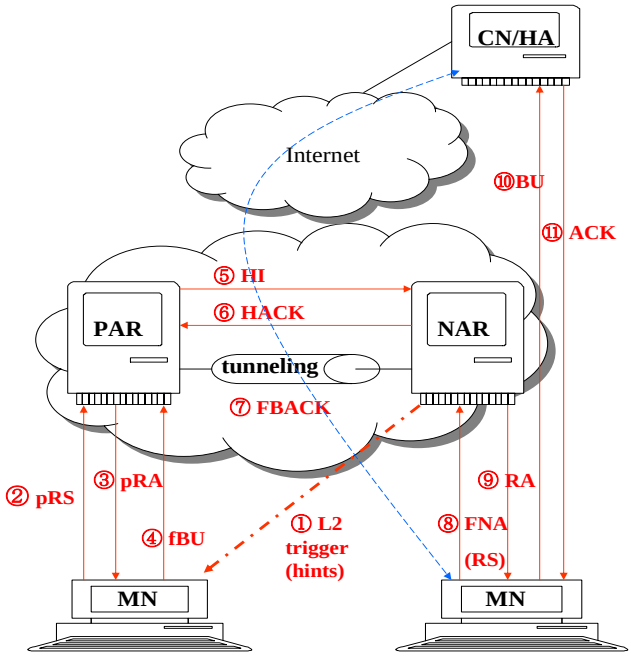


Figure 5: Structure of FMIPv6-anticipated handover

FMIPv6-anticipated handover procedure is as followings [13]:

① MN senses the movement to NAR by L2 trigger.
② MN sends pRS (proxy router solicitation) message for NAR to PAR. This message contains link-layer ID for NAR such as SSID of NAR in the wireless LAN.

③ PAR configures NCoA using the information of NAR which PAR already has. PAR sends pRA (proxy router advertisement) containing NCoA to MN.
④ MN sends fBU (fast binding update) request for binding the old CoA with NAR to PAR (old CoA→ NAR).
⑤ PAR sends HI (handover initiate) in order to setup the bi-directional tunneling with NAR. It also requests that NAR will verify the newly configured CoA.
⑥ NAR sends HACK (handover ACK) to PAR. It builds bi-directional tunnel and checks the new CoA.
⑦ PAR sends acknowledgement for NCoA to NAR through FBACK. It also intercepts data for the previous CoA of MN and forwards to NAR through tunneling.
⑧ After new link between NAR and MN is established, MN sends RS including fNA (fast neighbor advertisement) which represents MN itself.
⑨ NAR sends new CoA to MN through RA with NACCK option.
⑩ MN sends the BU to CN and HA.
⑪ CN and HA reply with ACK.

FMIPv6-tunnel based handover is represented in Figure 6. FMIPv6-tunnel based handover procedure is as followings [13]:

1) old AR senses the movement.
2) old AR initiates L2 trigger which includes MAC address of MN and IP address of new AR.
3) old AR sends HI (handover initiate) to new AR.
4) new AR replies with HIACK and establishes the bi-directional tunnel.
5) MN starts L2 handover.
6) old AR forwards the data from CN to MN or from MN to CN through bi-directional tunnel.
7) MN sends the BU to CN/HA and releases the tunnel.
8) CN and HA reply with the ACK.

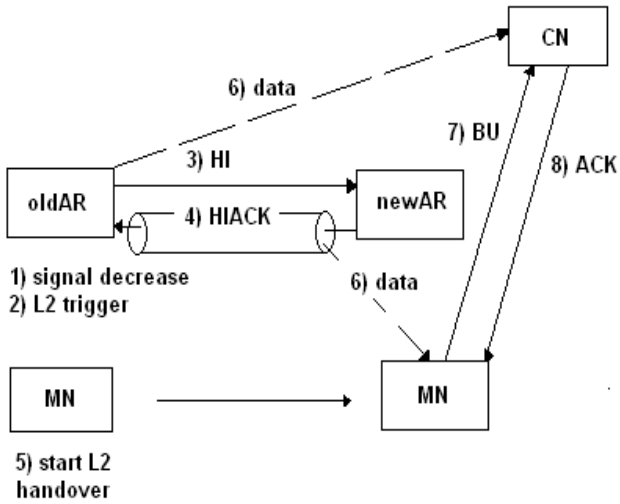


Figure 6: Structure of FMIPv6-tunnel based handover

Performance improvement in SCTP handover

Typical SCTP handover is performed according to the following procedures [11, 12, 13].

1) Physical layer detects radio signal from new subnet.
2) Physical layer receives router advertisements/beacons from AP (access point).
3) MN investigates IP address in the WS (working set) record and starts handover (SCTP layer).
4) If MN fails to find new IP address, it waits until auto-configuration or DHCP reply.
5) MN obtains new IP address and starts handover.
6) MN sends ASCONF: add_ip and set_primary chunk to CN.
7) MN receives ASCONF_ACK from CN with add_ip and set_primary.
8) Physical layer loses radio signal from the previous subnet.
9) Handover is completed.

To perform the SCTP handover, we need L2 and L3 handovers. L3 handover delay is composed of movement detection delay of MN and the new IP address configuration delay. Hence, in order to minimize the total delay for SCTP handover, we should reduce the delay such as movement detection delay and new IP configuration delay as well as the L2 handover delay.

In the mobile IP, we need the additional delay for registration. However, it is known that registration delay in the mobile IP environment can be optimized.

Now, we assume that MN returns to the cell frequently where it visited before. If we have no any handling scheme, we have to repeat the same configuration procedure for obtaining previously used IP address. This increases the L3 handover delay and the L4 handover delay simultaneously.

Improvement considerations

It is reasonable that we try to obtain the IPV6-address using stateless-auto-configuration, if we fail, then use the state full method such as DHCP. The reason to do this is why if the DHCP server is far away from the current location of MN, the time to send the DHCP request message and receive the DHCP_Reply can be longer than time to obtain the prefix from access router attached to MN. That is, as soon as we receive the RA from the attached router (prior to receiving the RA, we can send the RS), we obtain the IP-address using the stateless-auto-configuration of ipv6 (MIPv6). If this procedure fails, we use the state full method such as DHCP based on MAC address.

Assume that we use the FMIPV6 (fast handover for MIPv6) when we detect the signal from the physical layer. Then, we can get the CoA of new router (B) prior to the handover. Therefore, we can also obtain the new_ip address of host by using the stateless-auto-configuration.

Original SCTP packet format is represented in Figure 7. When the MN obtains new IP address, for example, (10.1.1.1), then MN sends the packet with the new_ip address given in Figure 8.

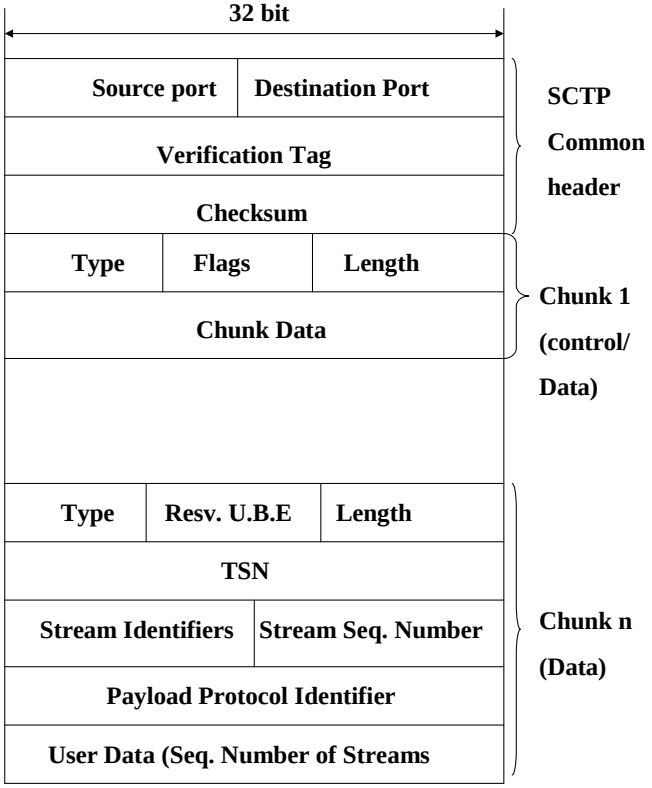


Figure 7: SCTP packet format

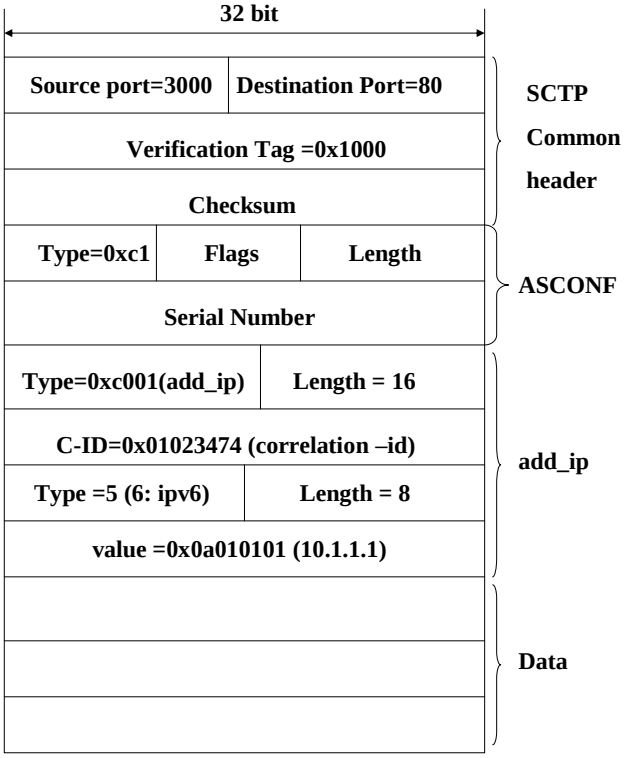


Figure 8: Example of add_IP SCTP chunk

Figure 9 shows the example of add_IP chuck transfer procedure. In the figure, the sender transmits the ASCONF request on the old IP address (9.1.1.1). If the request is accepted, the receiver (CN) can send the data on new IP a

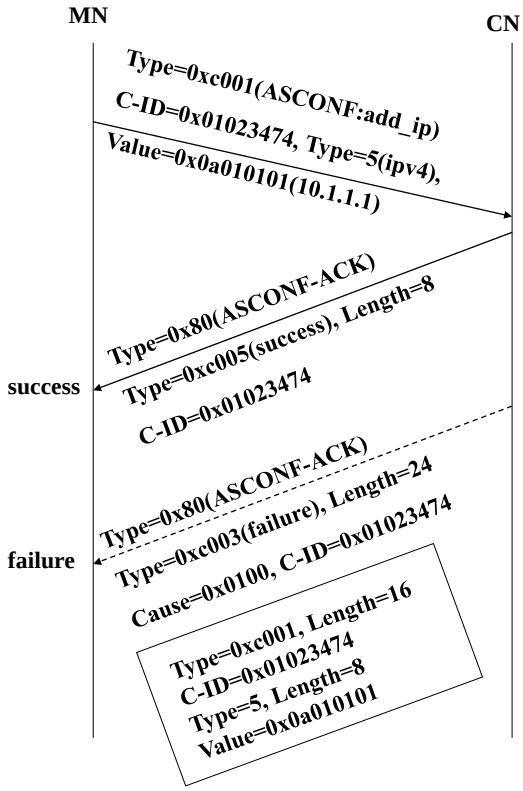


Figure 9: Example of add_IP SCTP chunk transfer

During the time interval between sending out the ASCONF:add_ip and receiving the ASCONF-ACK, it may be possible to receive DATA chunks out of order. The following examples illustrate these problems:

In the MN, the address (10.1.1.1) may be added after receiving the ASCONF-ACK. If the sender wants to send data by using the new IP address (10.1.1.1), it first should receive the ASCONF-ACK. However, due to packet re-ordering in the network, a new data chunk (destination: 10.1.1.1) may be sent and arrive at MN before the ASCONF-ACK confirming the adding of the address to the association. A similar problem exists in the deletion of an IP address.

For the add_ip case, an endpoint should consider the newly adding IP address valid for the association to receive data during the interval awaiting the ASCONF-ACK. The endpoint must not source data from this new IP address until the ASCONF-ACK arrives but it may receive out of order data. At this time, it may drop the data silently, however, it must not respond with an ABORT.

Our suggested solution

The sender inserts new_IP into the temporary WS database after sending ASCONF:add_ip. Before the ASCONF-ACK arrives, it receives data for the address in the temporary WS database. In the example, address (10.1.1.1) only can receive data. As soon as ASCONF-ACK arrives at MN, we move the new_IP from temporary WS to original WS. That is, we insert the feasible IP address capable to send and receive the data into the original WS and insert IP address capable to receive only into temporary WS. If we drop the out-of-order data, the data loss may occur during the handover. We send ASCONF-ACK and data on the new IP address simultaneously in order to send data.

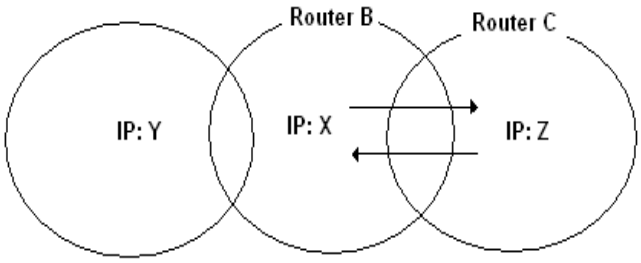


Figure 10: Example of revisiting the same region

For the delete_ip case, an endpoint may respond to the late arriving data packet or it may postpone the deleting IP address for a short period as still valid. If we handle the data packet, the peer will silently discard the ABORT. By the time the ABORT is sent, the peer will have removed the IP address from this association. If the endpoint decides to hold the IP address valid for a period of time, it should not hold it valid longer than two RTOs (retransmission time out) intervals for the destination being removed.

We store the delete_IP address on WS database. If ipv6 stateless-auto-configuration is used, then new IP address is configured by the prefix from router (B). We can bind the MAC address with new IP address and router's prefix, and store the record on the WS database. After then, we move into to the region (router C). If we return to B, packets we didn't receive may arrive. If we restore the previously assigned IP address while being in B, we may receive the out-of-data. In order to solve this problem, we maintain the association information such as [MAC_address, Router_pretix, IP_address] on WS database in MN.

CONCLUSIONS

Mobile network is one of the mostly used computer networks. Handover latency in the mobile network mainly occurs in the obtaining new IP address process. Especially, ping-pong behavior of mobile node increases the unnecessary latency remarkably. This paper presents several performance improvement tips applicable to the ping-pong environment by using the SCTP address reconfiguration. The multi-homing feature of SCTP supports our proposed mechanism. Future works to evaluate the proposed scheme will be expected.

REFERENCES

[1] Perkins, C. E., Mobile IP, Addison-Wesley, 1998, pp. 181-184.

[2] Lee, Y., 2014, "On the Layer based seamless handover schemes for mobile data network, " Advances in Computer Science, Vol. 3, Issue 6, No. 12, November, pp.92-99.

[3] Fu, S. and Atiquzzaman, M., "SCTP: State of the art in research, products, and technical challenges", IEEE Communications Magazine, Vol. 42, No. 4, 2004, pp. 64-76.

[4] Stewart, R., "Stream control transmission protocol (SCTP), RFC 4960, http://www.ietf.org/rfc/rfc4960.txt, 2007.

[5] Stewart, R. and Xie, Q., Stream Control Transmission Protocol (SCTP) A Reference Guide, Addison-Wesley, 2002.

[6] Andreadis, A., 2003, "Protocol for High-Efficiency Wireless Networks", Kluwer Academic Publishers, pp. 258-262.

[7] Montavont, N., "Analysis and Evaluation of Mobile IPV6 Handovers over wireless LAN", Mobile Networks and Applications, 8, 2003, pp. 643-653.

[8] Thomson, S., "IPv6 Stateless Address Auto configurations", RFC-2462, IETF, 1998.

[9] Narten, "Neighbor Discovery for IP Version 6 (IPv6)" RFC2461, December, 1998, IETF.

[10] Han, Y. et. als, "Advance Duplicate Address Detection", <draft-han-mobileip-adad-01.txt>, July, 2003.

[11] Stewart, R., "SCTP Dynamic Address Reconfiguration", <draft-ietf-tsvwg-addip-sctp-07.txt>, Feb., 2003.

[12] Lee, Y., 2015, "Location Management Broker Scheme for SCTP Handover, " International Journal of Engineering Innovation & Research, Vol.43, Issue 3, pp.424-427.

[13] Lee, Y., 2014, "History based Handover Broker Scheme for SCTP, " Advances in Computer Science, Vol. 4, Issue 3, No. 15, May, pp.91-96.