ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 3, No.15 , May 2015
ISSN : 2322-5157
www.ACSIJ.org

History based Handover Broker Scheme for SCTP

Y. –J. Lee

Department of Technology Education, Korea National University of Education
Cheongju, 363-791, South Korea
lyj@knue.ac.kr

Abstract

This paper presents history based broker handover scheme for SCTP (stream control transmission protocol) in order to minimize the handover latency by the ping pong behavior of mobile node. SCTP is alternate protocol to TCP in the transport layer. It has multi-homing feature which provides the mobile node with dual interfaces to minimize the packet loss during handover in the overlapped region. L4 handover scheme using the multi-homing of SCTP is well known to reduce the latency more than handover schemes using other protocols. This paper presents an efficient handover scheme for IPv6 and IPv4 by utilizing the visiting history of MN (mobile node) and the broker instead of the CN (correspondent node). The considerations to implement this scheme in the real environment are also discussed.

Keywords: *Handover scheme, SCTP, History based broker scheme.*

1. Introduction

Handover is one of very important mechanisms in communication networks. Handover is classified into four handovers with respect to the layer: Layer 1(L1), Layer 2(L2), Layer 3(L3), and Layer 4 (L4) handover.

The physical layer carries out the L1 handover by detecting the signal power degradation. The data link layer performs the L2 handover. L3 handover is performed in the network layer. Transport layer carries out the L4 handover.

Layer 2 handover depends on how to detect the change of signal power and is performed by using hardware. The performance of Layer 3 handover scheme is affected by how to exchange old IP address with new IP address promptly and how to obtain new IP address fast. MIPv4 (mobile IPv4) and MIPv6 provide MN with the mobility. L4 handover scheme using SCTP is known to show better performance than TCP based handover schemes [1,2,3].

This paper focuses on the history based broker scheme in order to minimize the handover latency. We deploy the working set maintaining the previously obtained IP address and the broker computing the new IP address with new prefix instead of CN.

In this paper, we present the logical model to describe the novel procedure instead of the experimental results, which is the another research topic.

We discuss the handover latency of SCTP in the next section. History based broker scheme for IPv6 and IPv4 will be discussed in sections 3 and 4, respectively. We conclude this paper in section 5.

2. Handover latency of SCTP

Fig. 1 depicts the typical handover latencies on the timeline.

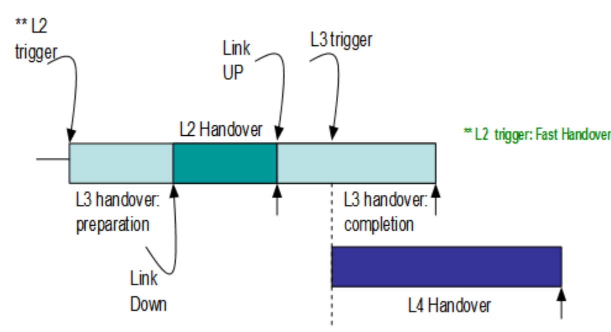

Fig. 1 handover latency

To perform the SCTP handover, we need also L2 and L3 handover. In Fig. 1, L3 handover delay is composed of movement detection delay of MN and the new IP address configuration delay. In the Mobile IP [4], we need the additional delay for registration. But, it is known that registration delay in the mobile IP environment can be optimized.

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.

Now, we assume that MN returns to the cell 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. In this paper, we suggest the broker scheme to reduce the time to acquire new IP address. We first present the broker scheme for IPv6 in the next section, and then for IPv4 in section 4.

Fig. 2 shows typical SCTP handover timeline [2,5].

(1) PHY: Physical layer detects radio signal from subnet B
(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 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 & set_primary chunk to CN.
(7) MN receives ASCONF_ACK from CN with add_ip & set_primary.
(8) PHY: Physical layer loses radio signal from subnet A.
(9) Handover is completed.

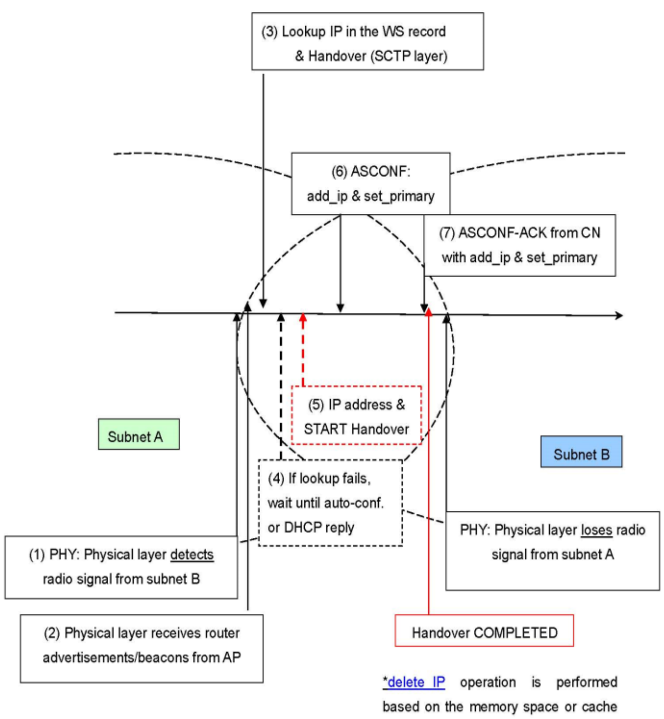

Fig. 2 SCTP handover timeline

3. History based broker scheme for IPV6

Fig. 3 and Fig. 4 depict the handover procedure and the broker scheme for IPv6 using stateless auto-configuration [6], respectively. In Fig. 3 and Fig. 4, AR represents access router. NS and NA show the network solicitation and network acknowledgement, respectively [7]. DAD means duplicate address detection in IPv6 [8,9].

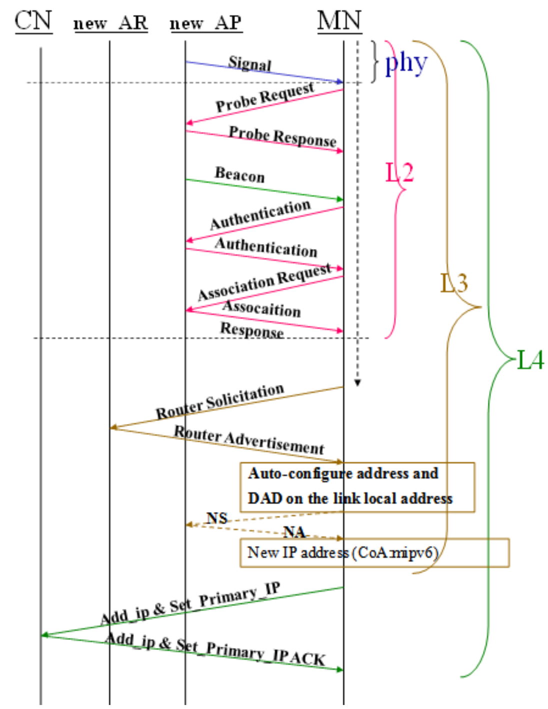

Fig. 3. Handover for IPv6 using stateless auto-configuration

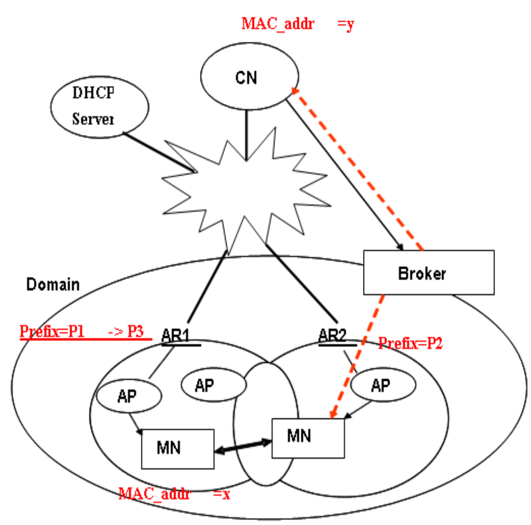

Fig. 4. Broker scheme for new IP configuration

3.1 Invariable router prefixes

(1) Physical layer of MN detects the signal power from the new AP when MN enters into the overlapped region.

(2) Physical layer receives router advertisements/beacons from AP. Link layer passes the association information record (its own MAC_address, the prefix of router) to the upper layer. Here, MAC_address is assumed to be unique address and starts the link layer handover (performs (4)).

(3) SCTP layer of MN looks up the WS. If it finds the IP_address matching with (MAC_address, the prefix of router) received from the link layer, then proceeds to step (5). Otherwise, it waits until (4) is completed.

(4) IP layer of MN performs the stateless-auto-configuration using the prefix from AR. If MN fails this configuration, then it sends the DHCP_request to DHCP server located in somewhere in the network. Since it might take long time before receiving the DHCP_reply, to use the stateless-auto-configuration is recommended. If stateless-auto-configuration is impossible, we proceed to the DHCP request and reply. IP layer passes the new IP address to the upper layer.

(5) SCTP layer of MN adds the new association information record to the WS. The association information record is composed of {(MAC_address, the prefix_of_router, new_IP_address), visit_count, visit_time (timestamp)}. Here, MAC_address of the peer might not be bound if we don't use the INIT or INIT-ACK for this purpose. If so, it'll be bound when receiving ASCONF or ASCONF-ACK from the peer. WS record is constituted by supplementing MAC_address, prefix, visit_count, visit_time to the existing data structure of IP_list.

(6) SCTP layer of MN sends the packet combining ASCONF(add_ip) and ASCONF(set_primary) to the CN. The slightly modified ASCONF (add_ip) and ASCONF (set_primary) format to meet our goals are presented in Fig. 5 and Fig. 6, respectively.

When the layer of CN receives the packet, it checks the feasibility for adding and setting primary IP and adds the association information record to its WS. At this time, the add_ip operation must be performed prior to the set_primary operation. Then, it sends the extended ASCONF-ACK containing both add_ip and set_primary _IP.

(7) When the MN receives the ASCONF-ACK from CN, it binds the (MAC_address, visit_count, visit_time) on the WS.

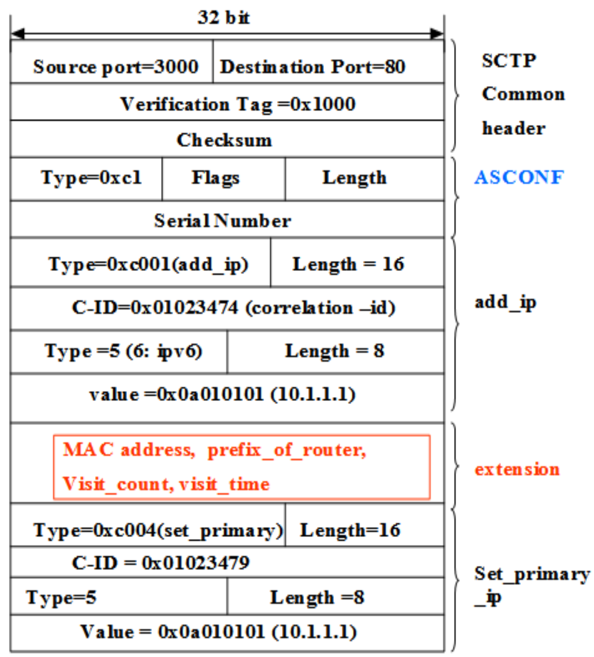

Fig. 5. Modified ASCONF chunk with add_ip and set_primary

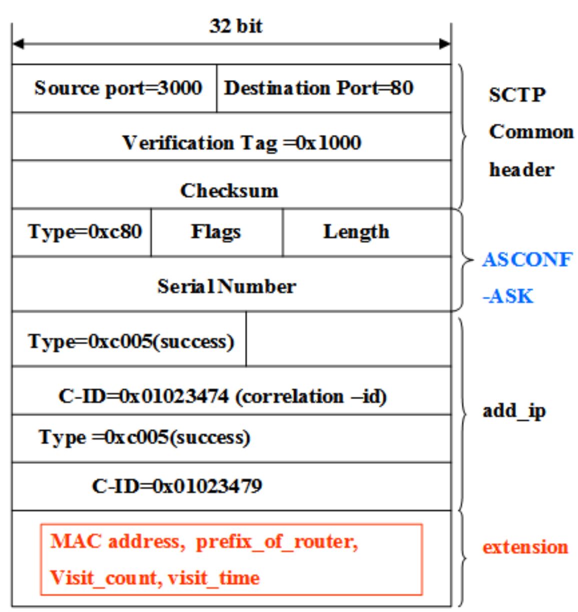

Fig. 6. Modified ASCONF_ACK chunk with add_ip and set_primary

ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 3, No.15 , May 2015
ISSN : 2322-5157
www.ACSIJ.org

3.2 Variable router prefixes

If some prefixes of routers are changed during some times, they may be inconsistent with the prefix of the association information record in WS.

(1) High priority

If we make new IP address computed in the IP layer to have higher priority than old IP address in WS for the same association, the inconsistency problem can be solved because WS is updated with the new IP address. However, this is not always useful in the environment where little changes of prefixes occur. The reason is why waiting for the IP layer to finish configuring new IP_address is unnecessary since it is already in the WS.

(2) Introduction of the broker

Step 1. Broker can be installed in the CN, although it can be anywhere in the network. It is also located in the domain covering the certain area or routers.

Step 2. Whenever CN receives or sends the association information record from/to MN, it also sends the record to the broker.

Step 3. Broker collects prefixes from routers that it covers the domain and compares the prefixes of the routers collected with the prefix stored in its own WS periodically.

Step 4. If the specific prefix of router is changed, broker first finds the relevant WS record. Such a record can be searched by using the MAC address in the WS record.

Step 5. Broker replaces the existing prefix with the new prefix and updates the IP_address based on the newly obtained prefix and MAC address.

Step 6. Broker sends the update record to the relevant MN and CN. This message format is same as ASCONF add_IP extension presented in Fig. 5 and Fig. 6.

3.3 Space of WS

When the SCTP layer of MN tries to add the new association information record to the WS, and the WS space is not enough to store the record, the record with the victim mark can be deleted. Here, marking operation as victim might be performed earlier. If such a victim record doesn't exist, SCTP layer calls the victim selection procedure based on some criteria. At this time, ASCONF (with delete_IP chunk) can be sent with the ASCONF(add_ip & set_primary_IP) simultaneously.

We can also use cache memory to select the victim for delete_IP. We can preserve the WS records for the specific time.

3.4 Flow of the history based broker scheme

Fig. 7 depicts the procedure of the history based handover broker scheme in the SCTP environment.

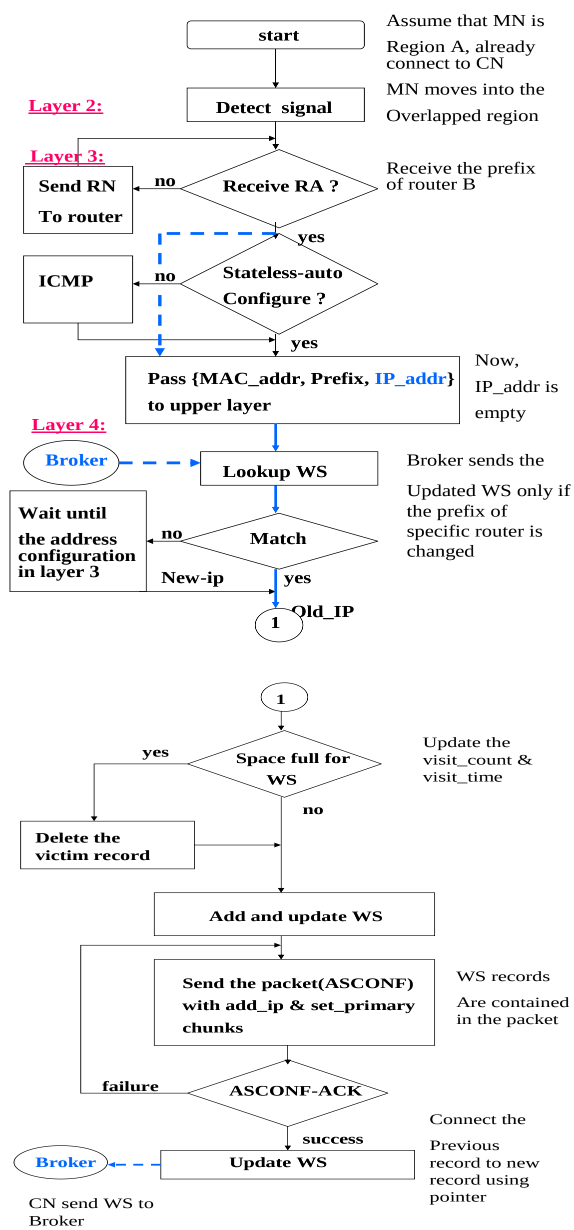

Fig. 7 Flow diagram of history based broker scheme

4. History based broker scheme for IPV4

Fig. 8 shows the handover procedure for IPv4 by using DHCP IPv4 [10].

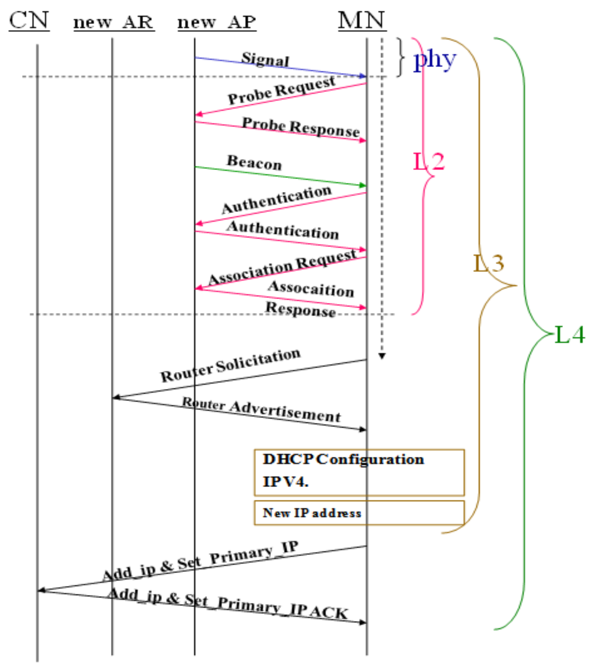

Fig. 8 Handover for IPv4 by using DHCP IPv4

In Fig. 8, we assume that new IPv4 address is obtained by using DHCPv4 server. We first describe our scheme in the case of using the DHCP server. We then explain another scheme utilizing the link-local-IPv4 address.

Assume that MN is located on the subnet A, the router prefix of which is prefix_A. MN moves into the overlapped region and hears the RA from subnet B's router. The prefix of router B is prefix_B. Currently, MN uses the DHCP IPv4 to acquire the new IP address. Normal DHCP IP4 procedure is presented in Fig. 9.

In the procedure, single failure of DHCP server can cause the entire communication failure. However, in the state-auto-configuration, DHCP server is unnecessary and is used as only the supplementary. DHCP request can be retransmitted four times, for total delay of 60 seconds. Delay becomes larger in the overlapped region. It is reported that time to obtain new IP address takes longer than the handover time.

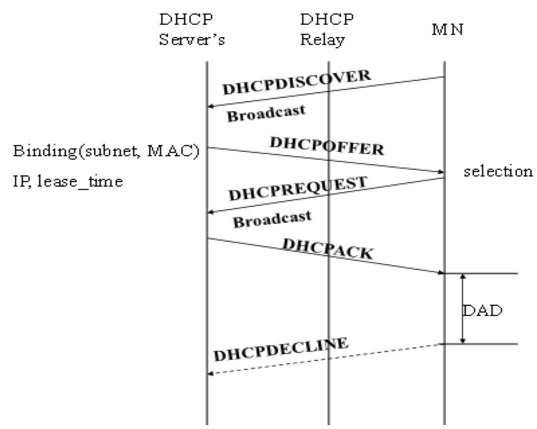

Fig. 9 Normal procedure for DHCP IPv4

4.1 Abridged procedure for DHCP IPV4 by the broker scheme

(1) When we enter the new region, we use the normal procedure for new IP acquisition in Fig. 9. At this time, the client may ask for a permanent assignment by asking for an infinite lease. (But, it is not guaranteed.). If so, we need not consider any more.

(2) SCTP layer of MN stores the following information (we call WS) in its own memory. {MAC, prefix, new_IP, visit_count, visit_time, lease_time, DHCP_server_IP} (We interchangeably use prefix and subnet number).

(3) SCTP of MN sends the ASCONF with add_IP & set_IP_primary with WS to CN.

(4) CN receives the ASCONF and extracts the WS and stores it (add_ip list is stored separately). CN sends WS to broker.

(5) Broker periodically checks if the router's prefix (subnet number) is changed. It also checks whether DHCP server's IP address is changed. If any change occurs, it marks the relevant WS and informs the relevant MN's and CN.

(6) When MN returns to the previously visited subnet, it can know its returning by comparing the prefix from new router with the prefix stored on its WS. Of course, the prefix of previously visited subnet was changed, it can't know where it visited before. In this case, the broker might inform the change to MN and CN.

The operation procedure is presented in Fig. 10. If the subnet number is changed (by information from broker), MN uses the normal DHCP procedure. But, even in this case, MN doesn't have to use the broadcast address if the DHCP server's IP address is not changed. That is, MN can send the DHCPDISCOVER message by using the unicast.

If the subnet number is unchanged, MN uses the abridged DHCP procedure. That is, it sends the DHCPREQUEST message with the requested IP address option by using the unicast. At this time, DHCP server's IP address is assumed not to be changed. The request IP option allows the MN to reuse the previously allocated network address. We stored already the visited IP address on WS of MN.

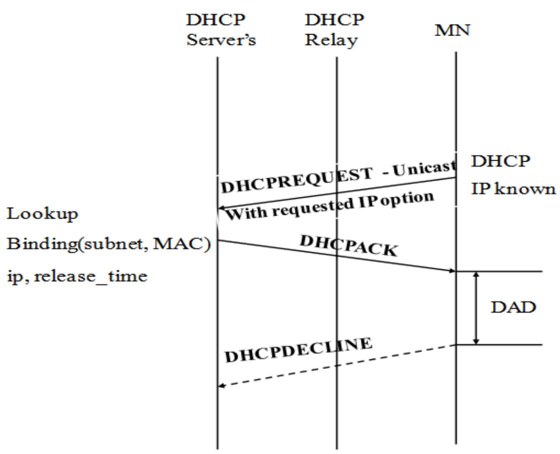

Fig. 10. Abridged procedure for DHCP IPv4

4.2 Link-local-IPv4 address

When the DHCP server doesn't exist or fails, we use the following scheme [11,12]. We assume that router supports NAT (network address translator) and MN uses the dynamic link-local IPV4 address configuration.

MN obtains new link-local IPV4 address by using auto-configuration. Let the link-local address be *X* (*X* is one of 169.254/16). SCTP of MN sends the ASCONF add_ip containing *X* to the router. Meanwhile, MN sends the query to DHCP server.
Since router has NAT, it replaces link-local address (*X*) with its address (*Y*) or encapsulates and forwards to CN (address: *E*). The reason is why link-local address cannot be routable. In this case, *X* in add_ip chunk remains in unchanged because *X* is included in the transport layer.

CN which receives the ASCONF_add_ip finds that *X* is the link-local address. CN adds the router address (*Y*) to its add_ip list instead of link-local address (*X*). If the set_primary_IP chunk combined in the packet, then CN can send data over router address (*Y*).

If MN obtains the routable IP address from DHCP server during the above procedure, it sends the ASCONF with add_ip & set_primary_IP immediately.

5. Conclusions

Handover latency is one of the important factors which affect the communication performance. Especially, the obtaining time of new IP address affects the handover latency. In the ping pong environment, the re-computation of IP address is very frequent. The reuse of previously computed IP address is expected to reduce the handover latency. This paper presents history based broker handover scheme for stream control transmission protocol in order to reduce the handover latency by the ping pong behavior of mobile node. By using the SCTP's multi-homing feature in the overlapped region, we propose the efficient handover scheme for IPv6 and IPv4 by using the visiting history of MN and the broker. We also discuss some considerations necessary to implement the proposed scheme.

References

[1] Y. Lee, "On the Layer based Seamless Handover Schemes for Mobile Data Network," Advances in Computer Science: International Journal, Vol. 3, Issue. 6, 2014, pp. 92-99.
[2] S. Fu and M. Atiquzzaman, "SCTP: State of the art in research, products, and technical challenges", IEEE Communications Magazine, Vol. 42, No. 4, 2004, pp. 64-76.
[3] R. Stewart, "Stream control transmission protocol (SCTP), RFC 4960, http://www.ietf.org/rfc/rfc4960.txt , 2007.
[4] C. E. Perkins, Mobile IP, Addison-Wesley, 1998, pp. 181-184.
[5] R. Stewart, "SCTP Dynamic Address Reconfiguration", <draft-ietf-tsvwg-addip-sctp-07.txt>, Feb., 2003.
[6] S. Thomson, "IPv6 Stateless Address Auto configurations", RFC-2462, IETF, 1998.
[7] Narten, "Neighbor Discovery for IP Version 6 (IPv6)" RFC2461, December, 1998, IETF.
[8] N. Moore, "Optimistic Duplicate Address Detection", <draft-moore-optimistic-dad-03.txt>, September, 2003.
[9] Y. Han et. als, "Advance Duplicate Address Detection", <draft-han-mobileip-adad-01.txt>, July, 2003.
[10] R. Droms, "Dynamic Host Configuration Protocol", RFC-2131, IETF, 1997.
[11] Aboba "Detection of Network Attachment(DNA) in IPV4", <draft-ietf-dhc-dna-ipv4-02.txt>.
[12] S. Cheshire, "Dynamic Configuration of Link-local IPV4 address", <draft-ietf-zeroconf-ipv4-link-local-10.txt>.