EAU: Efficient Address Updating for Seamless Handover in Multi-homed Mobile Environments

Yuansong Qiao, Shuaijun Zhang, Adrian Matthews, Gregory Hayes, Enda Fallon

EAU: Efficient Address Updating for Seamless Handover in Multi-homed Mobile Environments[†]

Yuansong Qiao[1,2], Shuaijun Zhang[1], Adrian Matthews[1]
Gregory Hayes[1], Enda Fallon[1]

[1] Software Research Institute, Athlone Institute of Technology, Ireland
[2] Institute of Software, Chinese Academy of Sciences, China
{ysqiao, szhang, amatthews, ghayes, efallon}@ait.ie

Abstract. Dynamic address configuration is essential when maintaining seamless communication sessions in heterogeneous mobile environments. This paper identifies some significant problems when using the Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration (SCTP-DAR) extension. We illustrate that SCTP-DAR can enter a deadlock state during the handover phase, ultimately resulting in communication failure. Deadlock arises as a result of the basic design rationale of SCTP-DAR, i.e. using a data oriented transmission scheme to transmit address update messages. This paper proposes a new transmission control mechanism for efficiently exchanging up-to-date address information between association endpoints. In particular we introduce an address operation consolidation algorithm which eliminates address operation redundancy. In addition, a priority based transmission re-scheduling algorithm for address updating operations is proposed to detect and remove potential deadlock situations. The above schemes have been verified through experiments.

Keywords: Multi-homing, Heterogeneous Networks, Mobility, Dynamic Address Configuration

1 Introduction

Current mobile communication systems involve a substantial number of multi-homed mobile devices interacting with a pervasive heterogeneous network environment. For example: Wi-Fi, 3G and WiMax are widely deployed in the Internet, and, simultaneously, most smart phones support multiple network connections, such as 3G, Wi-Fi and Bluetooth. Wireless technologies will probably continue to diversify in future. Thus, there has been a significant research and standardization effort focusing on providing general support for multi-homing and mobility, e.g. 4G networks [1], IEEE 802.21 [2], Site Multi-homing by IPv6 Intermediation (SHIM6) [3], Host Identity Protocol (HIP) [4] and Stream Control Transmission Protocol (SCTP) [5].

[†] This Research Programme is supported by Enterprise Ireland through its Applied Research Enhancement fund.

When a multi-homed mobile node (MN) is roaming across heterogeneous networks, its IP addresses can change frequently. Both mobility and wireless network fluctuations can cause network connections to be disconnected and re-numbered. Even in fixed scenarios, the host addresses may change during network failures if Dynamic Host Configuration Protocol (DHCP) is used to configure IP addresses. The up-to-date IP addresses should be transmitted to the correspondent node (CN) immediately so that communication interruptions can be avoided or reduced. Furthermore, a multi-homed mobile node probably needs to inform the correspondent node of its preferred primary IP address for communication according to its local policies or network conditions.

When the set of addresses in a node is changed, address updating messages can be sent to the correspondent node through the following schemes:

- Transmitting all current addresses of the node to the correspondent node in one message, such as in SHIM6 [3]. This scheme cannot guarantee that Network Address Translation (NAT) middleboxes are traversed correctly. Packets originating from different network addresses of a multi-homed host may pass through different NAT middleboxes on different paths. If a multi-homed host transmits all its addresses in one message, it requires that all NAT middleboxes are synchronized, i.e. one middlebox should translate an address which may pass through other middleboxes in the future. This is difficult to achieve in the current Internet.
- Sending address updating operations (AUOs) to the correspondent node to modify the set of addresses saved in the correspondent node, such as in the SCTP Dynamic Address Reconfiguration (SCTP-DAR) extension [6]. If AUOs are transmitted in separate packets, the protocol can traverse NAT middleboxes correctly [7] [8].

This paper will consider the second address updating scheme as it has broader usage scenarios than the first scheme. The SCTP-DAR standard is an extension for SCTP and therefore it was originally designed for network fault tolerance scenarios. However, researchers immediately found that it provided an ideal way to implement seamless vertical handover between heterogeneous networks. Consequently, there has been much effort to improve the handover performance based on SCTP-DAR, such as in [9] [10] [11].

Most of the current work concentrates on employing some auxiliary functions, such as using link signal strength [11], to enhance SCTP handover performance. SCTP-DAR is used as a fundamental function and it is presumed that it can operate properly.

This paper abandons this assumption and studies the address updating mechanism while using SCTP-DAR in mobile scenarios.

SCTP-DAR defines three AUOs: (1) ADD-IP – Add an address to an association; (2) DELETE-IP – Delete an address from an association; (3) SET-PRIMARY – Request the peer to use the suggested address as the primary address for sending data.

As the received sequence of AUOs can affect the address updating result, the AUOs are reliably transmitted through a First-In-First-Out (FIFO) mechanism which is typically used for data transmission. However AUOs are normally not equally important. Some newly generated operations can override earlier operations. For example, for a specific address, if a DELETE-IP operation is generated after an ADD-

IP operation, the final result is that the address is deleted from the SCTP association. If the ADD-IP operation is in the transmission queue, it is not required to be transmitted. Therefore the current SCTP-DAR is not optimized.

This paper will firstly present two scenarios where two SCTP endpoints enter a deadlock state during the handover phase. The association between two SCTP endpoints is finally broken even though there are active IP addresses available for communications. Through analyzing the problems, this paper proposes an efficient address updating scheme (named EAU) which consists of three parts: (1) An ordered & partially reliable transmission scheme for AUOs, which removes the FIFO constraint in SCTP-DAR; (2) An AUO consolidation algorithm, which can merge AUOs to remove redundancy; (3) An AUO re-scheduling algorithm, which can detect and remove potential deadlock situations.

The rest of the paper is organized as follows. Section 2 introduces SCTP-DAR and summarizes related work. Section 3 illustrates the SCTP-DAR performance degradation issues in detail. Section 4 describes the detailed design of the EAU address updating scheme. Section 5 presents test results for the proposed scheme. Conclusions and future work are presented in Section 6.

2 Related Work

SCTP Dynamic Address Reconfiguration (SCTP-DAR) Extension

SCTP [5] is a reliable TCP-friendly transport layer protocol supporting multi-homing and multi-streaming. Two SCTP endpoints can exchange their addresses at the initial stage, but the set of addresses cannot be changed thereafter. Therefore the SCTP-DAR extension [6] was proposed. A new SCTP chunk type called ASCONF (Address Configuration Change Chunk) is defined to convey three AUOs: ADD-IP, DELETE-IP and SET-PRIMARY. In the normal case, only one single ASCONF chunk is transmitted in a packet. During retransmissions, it is allowed to bundle additional ASCONF chunks in a packet. However, only one outstanding packet is allowed. SCTP-DAR defines that the transmission of ASCONF and ASCONF-ACK chunks must be protected by the authentication mechanism defined in [12]. More detailed security considerations are described in [6].

Other Related Work

Various mobile schemes based on SCTP-DAR have been proposed, such as in [9] [10] [11]. SCTP NAT traversing problems are studied in [7] [8]. In [13], two SCTP stall scenarios are presented. The authors identify that the stalls occur as a result of SCTP coupling the logic for data acknowledgment and path monitoring. SCTP Concurrent Multi-path Transfer (CMT-SCTP) is studied in [14].

Apart from SCTP in the transport layer, research has been performed in other layers of the OSI stack in support of multi-homing & mobility. IEEE 802.21 [2] encapsulates the heterogeneity of the underlying networks and provides a unified layer 2 handover support for upper layers. SHIM6 [3] provides multi-homing support in the Network Layer for IPv6. As SHIM6 is designed for IPv6 networks, NAT traversing is not considered in the design. HIP [4] suggests adding a Host Identity Layer into the OSI stack – consequently, a host is identified by its identity no matter

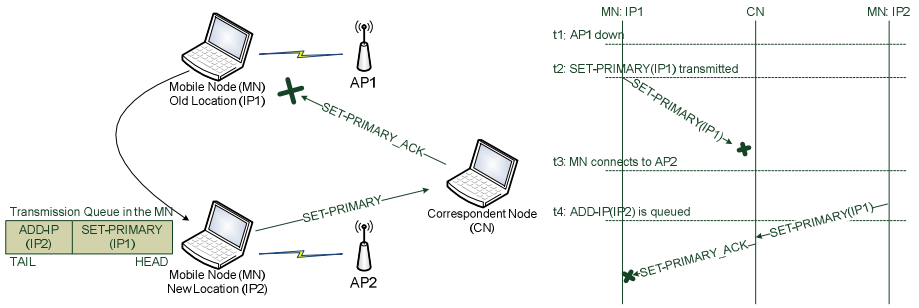
where it is located. In 4G systems, current research [1] is trying to provide integrated support for Multi-homing and Mobility.

3 Two SCTP-DAR Deadlock Scenarios

This section demonstrates two scenarios where the two SCTP endpoints cease to communicate despite there being IP addresses actually available for communications. The scenarios are not deduced from conjectured tests but are observed from real experiments while using Linux to test SCTP mobile functions.

In all the tests of the paper, the address updating policies are set to the same for testing purposes: when the SCTP application receives an interface/address UP event, it sends an ADD-IP and a SET-PRIMARY operation for the new address to its peer; when the application gets an interface/address DOWN event, it sends a DELETE-IP operation to its peer. An unusual phenomenon is observed in the experiments, i.e. an address UP event is always generated when the attached access point is turned off. This is caused by the implementation mechanism in the Linux wireless device drivers. Consequently, an ADD-IP and a SET-PRIMARY operation request are generated by the application. The ADD-IP request is rejected because the address is already in the association. The SET-PRIMARY operation is generated and transmitted to the peer.

3.1 Deadlock Scenario 1: All Addresses Are Changed



(a) Experiment setup (b) Event sequence

Fig. 1. Problem 1 – ADD-IP blocked by other ASCONF chunks.

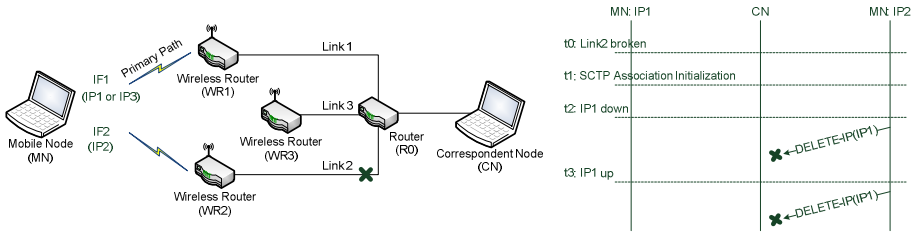
When all the IP addresses of an SCTP node are changed and the new addresses are unable to be transmitted to its peer, the association will be broken. An example is where a mobile node has only one network connection and that connection is renumbered (Fig. 1a). In the test, the MN has only one network connection which connects to a Wi-Fi network (AP1). When AP1 is down, the MN connects to AP2 (the network connection is renumbered). The sequence of the events in this experiment is shown in Fig. 1b. A SET-PRIMARY operation for IP1 is generated just after AP1 is turned off. An ADD-IP operation for IP2 is generated after the MN connects to AP2.

In current SCTP-DAR, an ASCONF chunk can be sent to the peer from a new IP address which currently is not in the association. Therefore, the ASCONF chunk with

the SET-PRIMARY operation (Fig. 1a) can be sent to the CN through the new IP address (IP2). However, the CN can only send an acknowledgement to an IP address which is already in the association. Consequently the acknowledgement is sent to the old IP address (IP1). The process continues until the SCTP association is broken.

In the experiment, if the ADD-IP(IP2) operation could be sent to the peer, the communication could be recovered. Unfortunately ADD-IP(IP2) is blocked by SET-PRIMARY(IP1) (Fig. 1a). SCTP-DAR defines that only one outstanding ASCONF chunk is allowed in normal situations. Nevertheless, ASCONF chunks can be bundled into one packet during retransmissions according to SCTP-DAR. Apparently, if SET-PRIMARY(IP1) and ADD-IP(IP2) could be bundled in one packet, the communication could be recovered. However, this scheme has two drawbacks: (1) It is not guaranteed that all ASCONF chunks can be allocated to one packet. Path Maximum Transmission Unit (PMTU) varies for different network types. The number of ASCONF chunks is also uncertain; (2) It can cause problems when there are NAT middleboxes between the two SCTP endpoints.

3.2 Deadlock Scenario 2: The Same Address is Down & Up



(a) Experiment setup (b) Event sequence

Fig. 2. Problem 2 – The ADD-IP operation cannot be generated after IP1 is up at time t3 because IP1 is still in the association (under deletion). (Acronyms in the figure: ***IP*** – IP Address; ***IF*** – Interface; ***WR*** – Wireless Router)

This section shows a scenario where an ADD-IP operation cannot be generated when an IP interface goes down and then comes back up. The experiment setup is shown in Fig. 2a. The MN has two IP addresses. The CN has one IP address. The default route in the MN is set to WR1 originally. The link between WR2 and R0 is broken at time t0 in Fig. 2b. Note that the MN cannot detect that Link 2 is broken because SCTP only detects whether peer addresses are active.

The sequence of events in the experiment is shown in Fig. 2b. IP1 goes down at time t2. A DELETE-IP chunk is generated to delete IP1. The MN sends the DELETE-IP chunk through IP2 to the CN. The DELETE-IP chunk or the DELETE-IP_ACK chunk is lost because Path2 is broken.

After a transmission timeout occurs, the DELETE-IP chunk should be retransmitted. According to SCTP-DAR, when an IP address is under deletion, it can be used for the reception of SCTP packets but cannot be used as a source address. Therefore, the DELETE-IP has to be retransmitted via IP2 even though IP1 has become available (time t3). The retransmitted DELETE-IP chunk is consequently lost again. Finally the SCTP association is broken.

The experiment shows three problems in SCTP-DAR: (1) the MN has to transmit an obsolete DELETE-IP operation which cannot reflect the current address status of the MN; (2) the DELETE-IP operation is transmitted on a broken path (Link2). It cannot use the current active address (IP1) because the address is under deletion; (3) the MN cannot create an ADD-IP operation to add IP1 into the association when IP1 is up again (time t2) because IP1 is still in the association (under deletion).

4 Design of EAU

4.1 Design Overview

In the above experiments, the communications are broken because the mobile node fails to send the ADD-IP operations to the peer. In current SCTP-DAR, ASCONF chunks are transmitted in sequence. If the ASCONF chunk at the head of the transmission queue cannot be transmitted successfully, all other ASCONF chunks are blocked. In addition, as SCTP-DAR is designed to transmit the oldest ASCONF chunk first, the internal state in the protocol refuses to generate new AUOs in some circumstances (Problem 2 in Section 3), which can further worsen the situation.

The essential problem in the SCTP-DAR design is that all AUOs are treated equally. In fact, a new operation can obsolete some previous operations. Furthermore, the different types of operations are not of the same priority. The ADD-IP operation is more important than others because it can increase the reachability of the node.

In order to overcome the above problems, the newly generated AUOs, especially ADD-IP operations, should be transmitted as soon as possible. This paper proposes to improve the current SCTP-DAR scheme using the following three steps: (1) Change ordered/reliable transmission to ordered/partially reliable transmission. (Section 4.2); (2) Use a consolidation algorithm to delete obsolete AUOs. (Section 4.3); (3) Use a transmission re-scheduling algorithm to select an AUO with the highest priority for transmission. (Section 4.4)

4.2 ADD-IP/DELETE-IP/SET-PRIMARY Procedure

4.2.1 Ordered/Partially Reliable Transmission Control

As mentioned before, the AUOs have two important characteristics: (1) The transmission sequence can affect the address operation results. Therefore, the AUOs should be transmitted in order; (2) A new AUO can obsolete some old operations. Therefore, these obsolete operations are not required to be transmitted reliably.

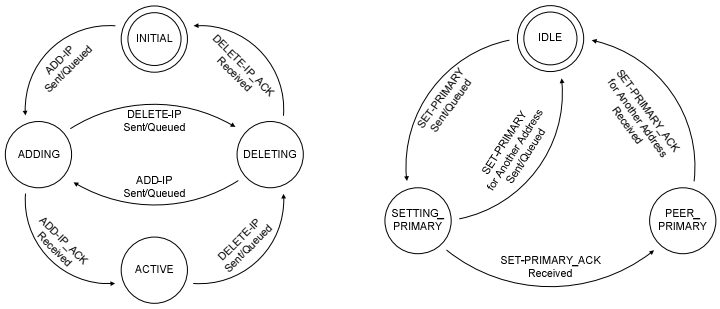
Based on these two characteristics, this paper proposes an ordered/partially reliable transmission scheme for transmitting AUOs. The idea is similar to the Partial-Reliability extension for SCTP (PR-SCTP) [15]. As only one ASCONF chunk is outstanding, the transmission control process is much simpler than PR-SCTP.

In the sender side, every ASCONF chunk is assigned a sequence number which is incremented by 1 after being assigned. The sender guarantees that all transmitted ASCONF chunks have consecutive sequence numbers. In normal situations, the sender transmits one ASCONF chunk after the acknowledgement for the previous

ASCONF chunk is received (the same as current SCTP-DAR). However, the sender can choose to transmit the next ASCONF chunk without waiting for the acknowledgement when it decides that the outstanding ASCONF chunk should be abandoned (Section 4.3) or should be re-scheduled after another ASCONF chunk (Section 4.4).

On the receiver side, the receiver should be able to receive ASCONF chunks with non-consecutive sequence numbers because the sender may abandon some ASCONF chunks. However, the received sequence number must be in ascending order, i.e. the current receiving sequence number must be greater than the last received sequence number.

4.2.2 Local Address States Definition



(a) Addition/Deletion (b) Set peer primary

Fig. 3. State transition diagram for local addresses.

In deadlock scenario 2 (Section 3.2), the SCTP node refuses to generate an ADD-IP operation because the address is still in the association. In order to overcome this problem, four new address states are defined for local addresses in the SCTP node (Fig. 3a):

- ***INITIAL***. The address is not in the SCTP association.
- ***ACTIVE***. The address has been added into the association and is ready for sending and receiving packets.
- ***ADDING***. The last operation for the address is ADD-IP. The ADD-IP chunk has been transmitted or queued and has not been acknowledged.
- ***DELETING***. The last operation for the address is DELETE-IP. The DELETE-IP chunk has been transmitted or queued and has not been acknowledged.

An IP address can only be in one of these four states. Whenever an IP address goes UP or DOWN, an ADD-IP or DELETE-IP is generated and the address state is set to ADDING or DELETING respectively. Therefore, the address state represents the current status of the address. It ensures an address status change is immediately reflected in the address state.

Furthermore, three states for setting the peer primary address are defined as follows (Fig. 3b):

- ***SETTING_PRIMARY***. The last SET-PRIMARY was sent for this address and has not yet been acknowledged.

- ***PEER_PRIMARY***. The acknowledgment of the SET-PRIMARY has been received.
- ***IDLE***. The address is in neither of the above two states.

Before changing an address to the SETTING_PRIMARY or PEER_PRIMARY state, the same state for other addresses must be cleared, i.e. only one address can be in the SETTING_PRIMARY or PEER_PRIMARY state.

4.2.3 Address Manipulation Process

Address Addition/Deletion Process

The address adding/deleting process on the sender side is shown in Fig. 3a. When an IP address comes UP, if the address is not in the association or is in the DELETING state, an ADD-IP chunk is generated. The address state is set to ADDING. Conversely, when an IP address goes DOWN, if the address is in the ACTIVE or ADDING state, a DELETE-IP chunk is generated. The address state is set to DELETING.

When the sender receives an acknowledgement for an ADD-IP/DELETE-IP operation, if the address is in the ADDING or DELETING state, an addition or deletion operation is performed respectively. Otherwise the acknowledgement is ignored because it is acknowledging an obsolete operation.

When the receiver receives an ADD-IP/DELETE-IP chunk, it performs the addition/deletion operation if the specified address is not/is in the SCTP association.

Setting Peer Primary Process

The process for setting peer primary in the sender side is shown in Fig. 3b. A SET-PRIMARY operation can be generated only when the IP address is both in the ACTIVE or ADDING state and is not in the SETTING_PRIMARY or PEER_PRIMARY state. The IP address should be set to the SETTING_PRIMARY state subsequently.

When the sender receives an acknowledgement for a SET-PRIMARY, if the address is in the SETTING_PRIMARY state, the address state is changed to PEER_PRIMARY. Otherwise, neglect the acknowledgement because it is acknowledging an obsolete SET-PRIMARY chunk.

When the receiver receives the SET-PRIMARY chunk, it sets the specified address as peer primary if the address is in the SCTP association.

SCTP Endpoint Synchronization

As the sender of AUOs only saves the latest address updating status, the synchronization between the sender and the receiver should be considered.

An SCTP endpoint saves two sets of addresses, i.e. local address set and peer address set. The states of local addresses are defined in Section 4.2.2. The states of peer addresses are defined as follows:

- ***INITIAL***. The address is not in the SCTP association.
- ***ACTIVE***. The address is in the SCTP association and has been verified, i.e. a HEARTBEAT chunk has been sent to the address and the HEARTBEAT_ACK has been received.

- ***UNCONFIRMED***. The address has been added into the association but has not been verified.

When a local address is in the ADDING or DELETING state, the address saved in the peer side could be in any state amongst INITIAL, ACTIVE and UNCONFIRMED. Therefore the address should not be used as a source address. However, it should be used for receiving data from the peer.

4.3 Address Operation Consolidation Algorithm

The aim of the algorithm is to delete obsolete AUOs in order to increase the transmission efficiency. The algorithm can be triggered before sending an AUO or just after an AUO is generated.

For each IP address, the last ASCONF chunk contains the final operation for that address. Therefore all previous related ASCONF chunks can possibly be deleted. The general steps to consolidate operations are defined as follows (starting from the tail and working towards the head of the queue): (1) A DELETE-IP operation obsoletes previous ADD-IP, DELETE-IP and SET-PRIMARY operations for that IP address; (2) An ADD-IP operation obsoletes previous ADD-IP and DELETE-IP operations for that IP address; (3) A SET-PRIMARY operation obsoletes any previous SET-PRIMARY operations.

If an outstanding ASCONF chunk is obsolete and should be deleted, the new ASCONF chunk should be transmitted according to the rules of congestion control, i.e. the new ASCONF chunk should be sent when the acknowledgement of the outstanding ASCONF chunk is received or the transmission timer expires.

The essential idea of the algorithm is to transmit the last operation reliably but to transmit previous operations partially reliably. Irrespective of whether the previous operations have been transmitted or not, the last operation should be kept for transmission to make sure that both SCTP endpoints have the same view of the address set. For example, for a specific address, if a DELETE-IP operation is generated after an ADD-IP operation which is still in the transmission queue, some may think both operations can be deleted. Actually, the DELETE-IP should be kept for transmission. The reason is that there might be a previous DELETE-IP operation which was transmitted unreliably before the ADD-IP operation. Therefore the sender is not sure if the specified address has been deleted in the peer by the unreliably transmitted DELETED-IP operation.

4.4 Address Operation Re-Scheduling Algorithm

This section describes the algorithm for detecting potential deadlock situations and removing the deadlocks by selecting an appropriate ADD-IP chunk to transmit.

The Re-Scheduling algorithm can be triggered by the following two conditions: (1) All the addresses in the association are not available in the system, e.g. the addresses in the system have been re-numbered; (2) All paths between the two SCTP endpoints are broken, i.e. the ASCONF chunk cannot be sent to the peer successfully. A threshold value called ASCONF_MAX_RTX is defined to detect ASCONF transmission failures. If the number of consecutive transmission timeouts for an

ASCONF chunk exceeds the threshold, the Re-Scheduling algorithm is triggered. The threshold is set to 3 in the paper. If it is set to 1, the Re-Scheduling algorithm is triggered for every ASCONF transmission timeout.

In order to maximize the reachability of a mobile node, the priorities of the AUOs are defined as follows:

$$Priority_{ADD\text{-}IP} > Priority_{SET\text{-}PRIMARY} > Priority_{DELETE\text{-}IP}. \quad (1)$$

When the re-ordering algorithm is triggered, it uses inequality (1) to select an ASCONF chunk to transmit. If there are multiple ADD-IP chunks in the transmission queue, the ADD-IP chunk is selected according to the following descending priorities: (1) The address in the ADD-IP chunk is an active address in the system, i.e. the IP address belongs to a network interface at the SCTP endpoint. (2) The ADD-IP chunk has not been transmitted. (3) The address in the ADD-IP chunk is in SETTING_PRIMARY state.

5 Implementation & Verification

The proposed scheme has been implemented in Ubuntu 9.04 (with a revised Linux-2.6.27.28 Kernel). Various tests have been executed to cover different network disconnection and interface renumbering scenarios (Six of these tests are listed in Table 1). The main purpose of the tests is to discover whether the proposed scheme can recover the communication when the connections between the MN and the CN experience total disconnection during the handover phase. The experimental network setup is shown in Fig. 2a. The MN and CN keep transmitting data to each other in the tests. All SCTP parameters are set to default. The detailed test setup, physical disconnection time, data interrupt time, and analysis are listed in Table 1. TEST 2 and TEST 3 repeat the experiments in Section 3. The results show that the deadlock situations are avoided effectively.

In these tests, after physical connections recover, the MN needs to wait for one transmission timeout of the outstanding ASCONF before sending an ADDIP for the new active address. The waiting time is from 0s to 60s according to the SCTP default configuration. The delay can be reduced by adjusting SCTP parameters.

Table 1. Experiment setup and results for verifying the function of the proposed scheme. "***PDT***" is the ***Physical Disconnection Time*** in seconds, which is the duration from the attached ***Wireless Router*** (***WR***) of an ***interface*** (***IF***) being turned off to the interface being attached to a new wireless router. "***DIT***" is the ***Data Interruption Time*** in seconds, which is the duration from the attached wireless router being turned off to data transmission being recovered.

No	IF1 Behaviour	IF2 Behaviour	PDT	DIT
1	IF1 connects to WR1; WR1 is restarted; IF1 re-connects to WR1.	IF2 is always Down.	IF1:53s	53s
2	IF1 connects to WR1; WR1 goes down; IF1 connects to WR3 (IF1 is renumbered).	IF2 is always Down.	IF1:38s	86s

3	IF1 connects to WR1; WR1 is restarted; IF1 re-connects to WR1.	IF2 always connects to WR2. Link2 is broken.	IF1:63s	108s
4	IF1 connects to WR1; WR1 goes down; IF1 connects to WR3 (IF1 is renumbered).	IF2 always connects to WR2. Link2 is broken.	IF1:36s	84s
5	IF1 connects to WR1; WR1 is restarted; : IF1 connects to WR1.	IF2 connects to WR2; : WR2 is restarted; : IF2 connects to WR2.	IF1:57s IF2:136s	85s
6	IF1 connects to WR1; WR1 is restarted; : IF1 connects to WR3 (IF1 is renumbered).	IF2 connects to WR2; : WR2 is restarted; : IF2 connects to WR2.	IF1:38s IF2:132s	84s

Note:

- In **TEST 1**, no ASCONFs are generated because only one IP address is in the association and it cannot be deleted from the association. Data transmission recovers immediately after WR1 goes up.
- In **TEST 2 (The same test as Section 3.1)**, it takes 48s (86-38) for the MN to recover the communication after IF1 connects to WR3. When IF1 connects to WR3, an ADD-IP(IP3) is generated and queued. When the transmission timer of the outstanding SET-PRIMARY(IP1) expires, the re-scheduling algorithm is executed and the ADD-IP(IP3) is arranged to the head of the queue. The queuing time of the ADD-IP(IP3) is 48s.
- In **TEST 3 (The same test as Section 3.2)**, it takes 45s (108-63) for the MN to recover the communication after IF1 re-connects to WR1. When WR1 goes down, a DELETE-IP(IP1) is sent via IF2, which is lost because Link2 is broken. Simultaneously, MN sets IP1 to the DELETING state. When IF1 re-connects to WR1, the default route is set to WR1 and therefore packets are sent through WR1. However, the MN cannot use IP1 as a source address at current stage because IP1 is not in ***ACTIVE*** state. An ADD-IP(IP1) is generated and queued in the MN. The ADD-IP(IP1) obsoletes the outstanding DELETE-IP(IP1). However, it is not allowed to be sent out until the timeout of the outstanding DELETE-IP(IP1) occurs. The queuing time for the ADD-IP(IP1) is 45s.
- In **TEST 4**, it takes 48s (84-36) for the MN to recover the communication after IF1 connects to WR3. The event procedure is similar to that in TEST 3. The difference is that MN sends ADD-IP(IP3) via WR3 after IF1 connects to WR3.
- In **TEST 5**, it takes 28s (85-57) for the MN to recover the communication after IF1 connects to WR1. The event procedure is similar to that in TEST 3.
- In **TEST 6**, it takes 46s (84-38) for the MN to recover the communication after IF1 connects to WR3. The event procedure is similar to that in TEST 4.

6 Conclusions & Future Work

This paper studies address updating mechanisms for multi-homed mobile scenarios. It identifies that the design rationale of current SCTP-DAR cannot reflect the characteristics of address updating operations (AUOs). SCTP-DAR uses a data oriented transmission mechanism (First-In-First-Out & Reliable) to transmit AUOs,

which significantly degrades handover performance and can cause communication to be broken in certain circumstances.

In order to overcome these problems, this paper proposes a novel address updating mechanism (named EAU) as follows. An ordered/partially reliable transmission scheme is proposed based on the observation that AUOs should be delivered in order but some obsolete operations are not necessary to be transmitted reliably. A set of new address states is defined to reflect the up-to-date address status. A consolidation algorithm is proposed to remove obsolete AUOs. Finally, a re-scheduling algorithm is proposed to detect and remove the deadlock situations presented in the paper.

The proposed address updating mechanism is implemented and verified based on the SCTP module in Linux. However, the mechanism can be used in more general situations because address updating management is a crucial function in many multi-homed mobile applications.

Future work is to test the proposed scheme in more complicated environments, such as in NAT enabled environments.

References

1. Vidales, P., Baliosion, J., Serrat, J., Mapp, G., Stejano, F., and Hopper, A., "Autonomic system for mobility support in 4G networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 12, pp. 2288–2304 (2005)
2. IEEE P802.21/D14.0 Media Independent Handover Services (2008)
3. Nordmark, E., Bagnulo, M., "Shim6: Level 3 Multihoming Shim Protocol for IPv6", IETF RFC 5533 (2009)
4. Moskowitz, R., Nikander, P., "Host Identity Protocol (HIP) Architecture", IETF RFC 4423 (2006)
5. Stewart, R., Ed., "Stream Control Transmission Protocol", IETF RFC 4960 (2007)
6. Stewart, R., Xie, Q., Tuexen, M., Maruyama, S., Kozuka, M., "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", IETF RFC 5061 (2007)
7. Tüxen, M., Rüngeler, I., Stewart, R., Rathgeb, E. P., "Network Address Translation for the Stream Control Transmission Protocol", IEEE Network, vol. 22, Issue 5, Page 26-32 (2008)
8. Hayes, D. A., But, J., Armitage, G., "Issues with Network Address Translation for SCTP", ACM SIGCOMM Computer Communication Review, vol. 39, no. 1 (2009)
9. Ma, L., Yu, F. R., Leung V. C. M., "Performance Improvements of Mobile SCTP in Integrated Heterogeneous Wireless Networks", IEEE Transactions on Wireless Communications, vol. 6, no. 10 (2007)
10. Fu, S., Ma, L., Atiquzzaman, M., Lee Y., "Architecture and Performance of SIGMA: A Seamless Mobility Architecture for Data Networks", Proc. ICC'05, Seoul, Korea (2005)
11. Chang, m., Lee, M., Koh, S., "Transport Layer Mobility Support Utilizing Link Signal Strength Information", IEICE Transactions on Communications, vol. E87-B, no. 9 (2004)
12. Tuexen, M., Stewart, R., Lei, P., Rescorla, E., "Authenticated Chunks for the Stream Control Transmission Protocol (SCTP)", IETF RFC 4895 (2007)
13. Noonan, J., Perry, P., Murphy, S., Murphy, J., "Stall and Path Monitoring Issues in SCTP", Proc. of IEEE Infocom, Barcelona (2006)
14. Natarajan, P., Ekiz, N., Amer, P., Iyengar, J., Stewart, R., "Concurrent multipath transfer using SCTP multihoming: Introducing the potentially-failed destination state", Proc. IFIP Networking, Singapore (2008)
15. Stewart, R., Ramalho, M., Xie, Q., Tuexen, M., Conrad, P., "Stream Control Transmission Protocol (SCTP) Partial Reliability Extension", IETF RFC 3758 (2004)