

Project	<b>IEEE 802.16 Broadband Wireless Access Working Group</b> < <a href="http://ieee802.org/16">http://ieee802.org/16</a> >	
Title	<b>Fixes for Loss of Handover Messages</b>	
Date Submitted	<b>2008-01-16</b>	
Source(s)	Chi-Chen Lee, I-Kang Fu, Kelvin Chou, Paul Cheng MediaTek Inc. No. 1, Dusing Rd. 1 Science-Based Industrial Park, Hsinchu, Taiwan 300	<a href="mailto:chichen.lee@mediatek.com">chichen.lee@mediatek.com</a> <a href="mailto:ik.fu@mediatek.com">ik.fu@mediatek.com</a> <a href="mailto:kelvin.chou@mediatek.com">kelvin.chou@mediatek.com</a> <a href="mailto:paul.cheng@mediatek.com">paul.cheng@mediatek.com</a>
Re:	IEEE 802.16 Working Group Letter Ballot Recirc #26a	
Abstract	The behavior of MS/BS in response to the loss of MOB_HO-IND messages during a HO has not been defined in P802.16Rev/D2, which leads to asynchronization between MS and its Serving BS and potential insecurity. A remedy is proposed to address this issue.	
Purpose	Accept the proposed specification changes in IEEE P802.16Rev2/D2	
Notice	<i>This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups. It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who reserve(s) the right to add, amend or withdraw material contained herein.</i>	
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.	
Patent Policy	The contributor is familiar with the IEEE-SA Patent Policy and Procedures: < <a href="http://standards.ieee.org/guides/bylaws/sect6-7.html#6">http://standards.ieee.org/guides/bylaws/sect6-7.html#6</a> > and < <a href="http://standards.ieee.org/guides/opman/sect6.html#6.3">http://standards.ieee.org/guides/opman/sect6.html#6.3</a> >. Further information is located at < <a href="http://standards.ieee.org/board/pat/pat-material.html">http://standards.ieee.org/board/pat/pat-material.html</a> > and < <a href="http://standards.ieee.org/board/pat">http://standards.ieee.org/board/pat</a> >.	

## Fixes for Loss of Handover Cancellation Messages

Chi-Chen Lee, I-Kang Fu, Kelvin Chou and Paul Cheng  
MediaTek Inc.

### Problem Statement

According to IEEE Std 802.16Rev2/D2, an MS shall transmit a MOB\_HO-IND message for final indication that it is about to perform a HO. When the MS cancels or rejects the HO, the MS shall transmit a MOB\_HO-IND message with appropriate HO\_IND\_type field. However, the HO cancellation described in Section 6.3.22.2.3 or HO reject does not define the behavior of MS/BS in response to the loss of MOB\_HO-IND messages during a HO, which leads to asynchronization between MS and its Serving BS and potential insecurity. The loss of MOB\_BSHO-REQ message also leads to asynchronization between MS and BS.

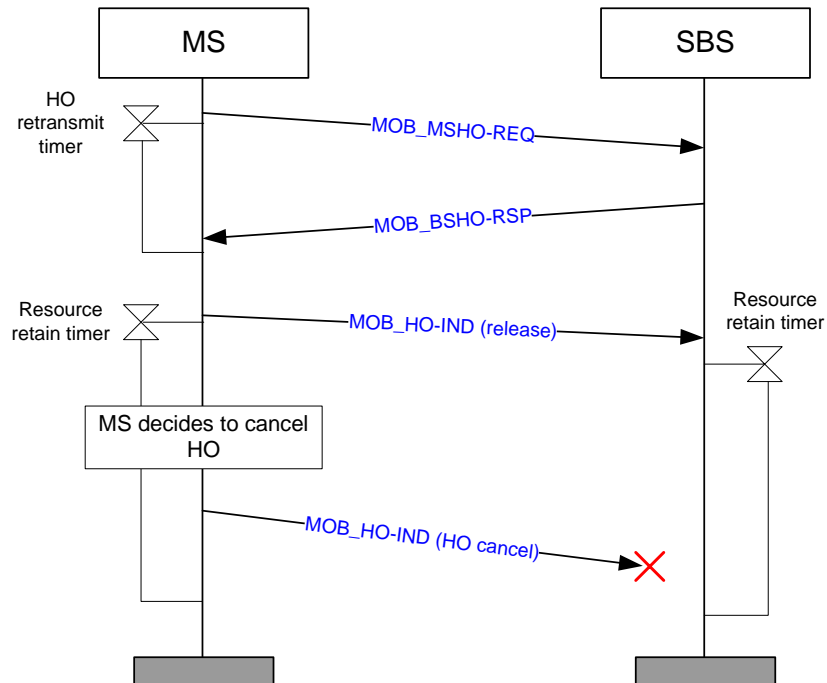


Figure 1 – Loss of MOB\_HO-IND messages during HO handshake

As shown in Figure 1, during the HO handshake, both MS and its SBS will not be notified the loss of MOB\_HO-IND message since there is no Ack for the MOB\_HO-IND message. If the MOB\_HO-IND message with HO\_IND\_type being *0b00* (SBS release) is lost, SBS may still learn the HO of MS through the notification from target BSs. However, the loss of MOB\_HO-IND message with HO\_IND\_type being *0b01* (HO cancel) makes MS and SBS have different perception of the MS status, i.e. MS considers the HO has been canceled while SBS considers the HO has been performed. Furthermore, if the MOB\_HO-IND with HO cancel, which contains the HMAC/CMAC Tuple, is lost and SBS still accepts subsequent BW requests, a malicious MS may attack or steal the BW from the SBS by sending BW requests to it.

Possible problematic scenarios are enumerated below:

**Scenario 1 (MS initiated HO):** MS decides to cancel HO right after it sent the MOB\_MSHO-REQ message, and the following MOB\_HO-IND with HO cancel is lost. MS will consider that the HO is canceled, while SBS will consider that MS continues HO and may stop DL&UL scheduling for the MS, as illustrated in Figure 2.

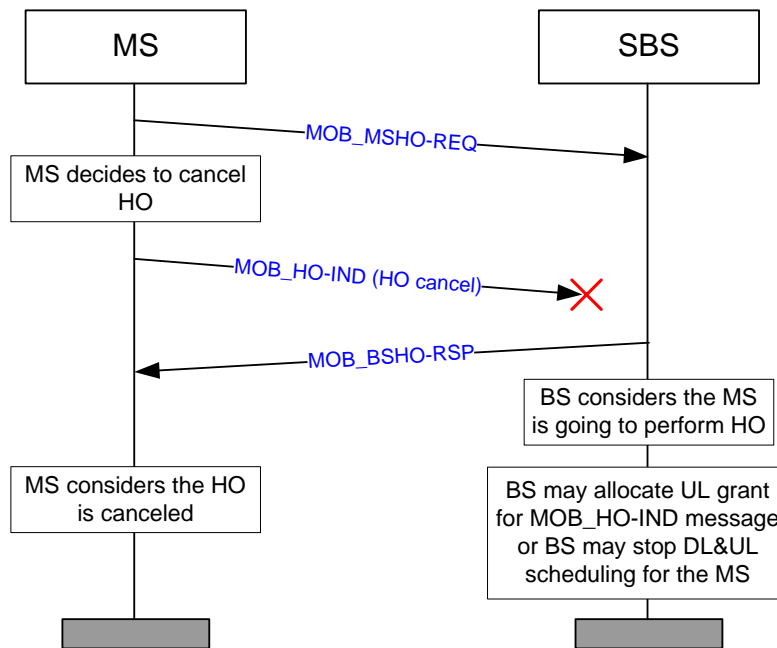


Figure 2 – Loss of HO cancel before MOB\_BSHO-RSP is sent by SBS

**Scenario 2 (MS initiated HO):** MS decides to cancel or reject HO right after it received the MOB\_BSHO-RSP message, and the following MOB\_HO-IND with HO cancel or HO reject is lost. MS will consider that the HO is canceled or rejected, while SBS will consider that MS continues HO and may stop DL&UL scheduling for the MS, as illustrated in Figure 3.

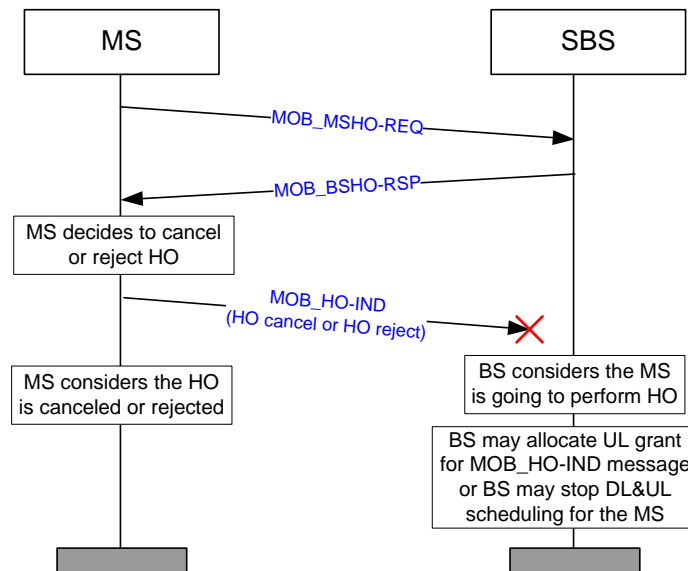


Figure 3 – Loss of HO cancel or HO reject after MOB\_BSHO-RSP is received by MS

**Scenario 3 (MS initiated HO):** MS decides to cancel HO right after it sent the MOB\_HO-IND message with SBS release, and the following MOB\_HO-IND with HO cancel is lost. MS will consider that the HO is canceled, while SBS will consider that MS continues HO and will stop DL&UL scheduling for the MS, as illustrated in Figure 4.

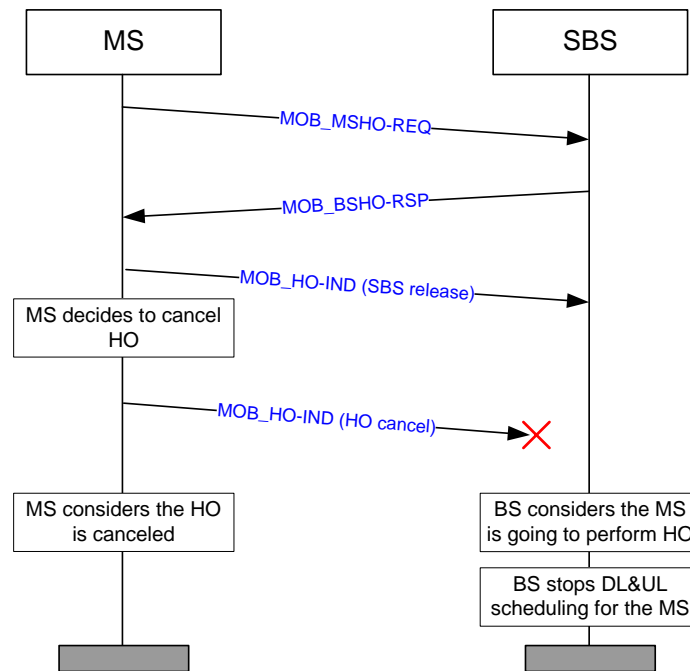


Figure 4 – Loss of HO cancel after MOB\_HO-IND with SBS release is sent by MS

**Scenario 4 (BS initiated HO):** MS decides to cancel or reject HO right after it received the MOB\_BSHO-REQ message from SBS, and the following MOB\_HO-IND with HO cancel or HO reject is lost. MS will consider that the HO is canceled or rejected, while SBS will consider that MS continues HO and may stop DL&UL scheduling for the MS, as illustrated in Figure 5.

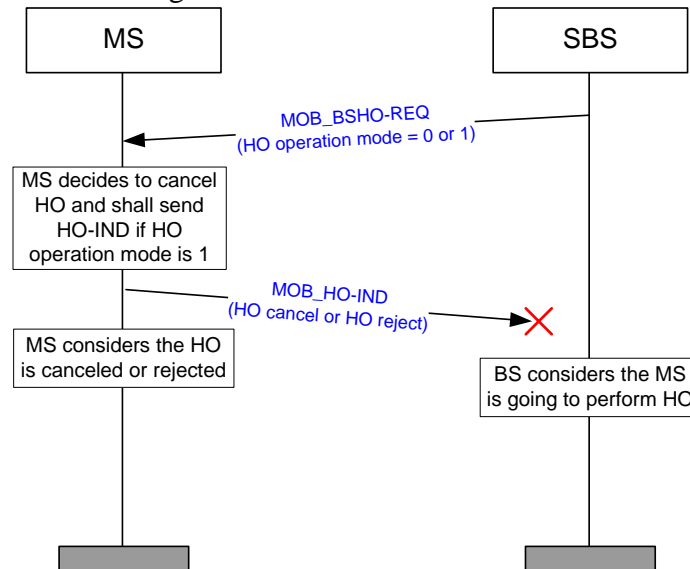


Figure 5 – Loss of HO cancel or HO reject after MOB\_BSHO-REQ is received by MS

**Scenario 5 (BS initiated HO):** MS decides to cancel HO right after it sent the MOB\_HO-IND message with SBS release, and the following MOB\_HO-IND with HO cancel is lost. MS will consider that the HO is canceled, while SBS will consider that MS continues HO and will stop DL&UL scheduling for the MS, as illustrated in Figure 6.

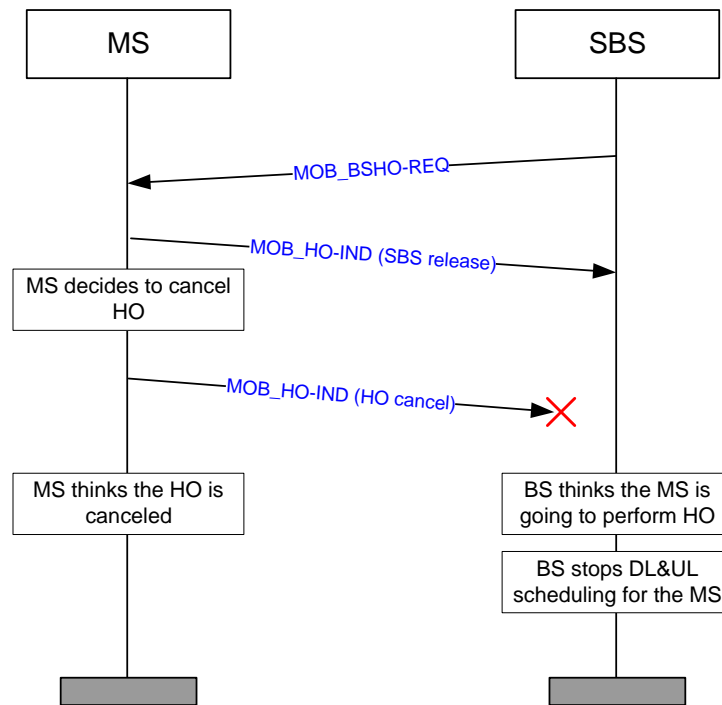


Figure 6 – Loss of HO cancel after MOB\_HO-IND with SBS release is sent by MS

**Scenario 6 (BS initiated HO):** MOB\_BSHO-REQ message is lost. In this case, MS will remain at normal operation, while SBS will consider that MS continues HO and may allocate unsolicited UL grant for MOB\_HO-IND message or may stop DL&UL scheduling for the MS, as illustrated in Figure 7.

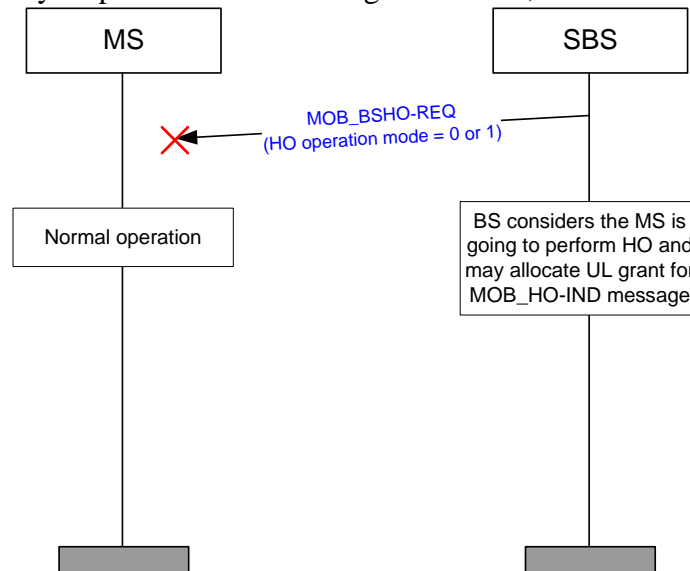


Figure 7 - Loss of MOB\_BSHO-REQ

### Suggested Remedy

The suggested remedies are illustrated in Figure 9 to Figure 13. First of all, after SBS sent MOB\_BSHO-REQ

or MOB\_BSHO-RSP message, it shall stop allocating UL allocations to the MS except the unsolicited grant or contention bandwidth request for the transmission of MOB\_HO-IND message. The allocation of unsolicited grant for ertPS and UGS services before the expiration of the HO indication readiness timer should be omitted since the duration between MOB\_BSHO-REQ/RSP message and MOB\_HO-IND message (2 by default) is very short. If the Serving BS receives MOB\_HO-IND message with HO\_IND\_type being HO cancel or HO reject from the MS, it shall allocate unicast grant to the MS as an acknowledge to the MOB\_HO-IND message. The BS shall resume UL scheduling for MS upon receiving one of the following messages: MOB\_HO-IND message with HO cancel/reject or MOB\_MSHO-REQ message.

Once MS decides to cancel or to reject HO after receiving the BSHO-REQ message or BSHO-RSP message, it shall start a HO-IND retry timer immediately after sending the MOB\_HO-IND message with HO cancel or HO reject, and then waits for the unicast grant from Serving BS. If MS does not receive any unicast grant before the expiration of the HO cancel retry timer, it shall retransmit the MOB\_HO-IND message to cancel or reject HO; otherwise MS considers that the HO cancellation is successful.

If the maximum retries exceeded on transmission of the HO cancel or HO reject message, the MS shall perform initial network entry or HO with other BS.

If MS sends MOB\_HO-IND message with HO cancel or HO reject right after sending MOB\_MSHO-REQ, but receives MOB\_BSHO-RSP from SBS, it shall consider that its HO cancel or HO reject message has been lost. In this case, it shall retransmit another MOB\_HO-IND message with HO cancel or HO reject and start HO-IND retry timer immediately.

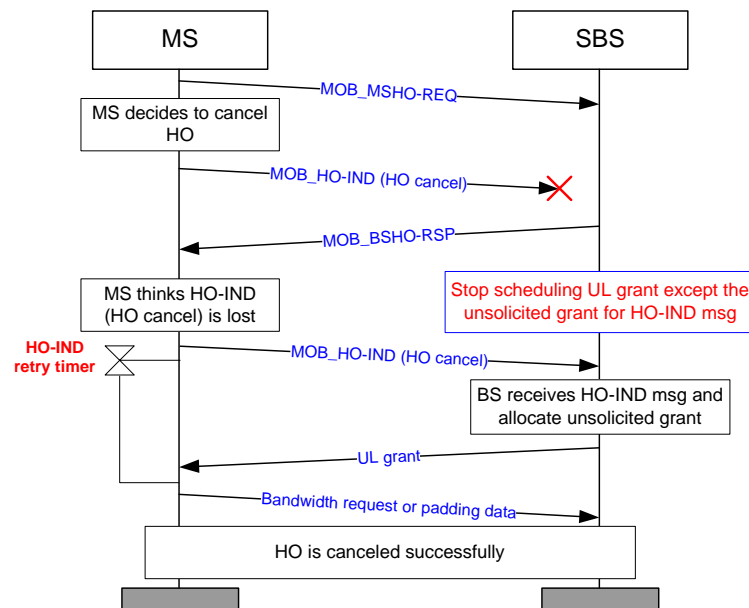


Figure 8 - Suggested remedy for scenario 1

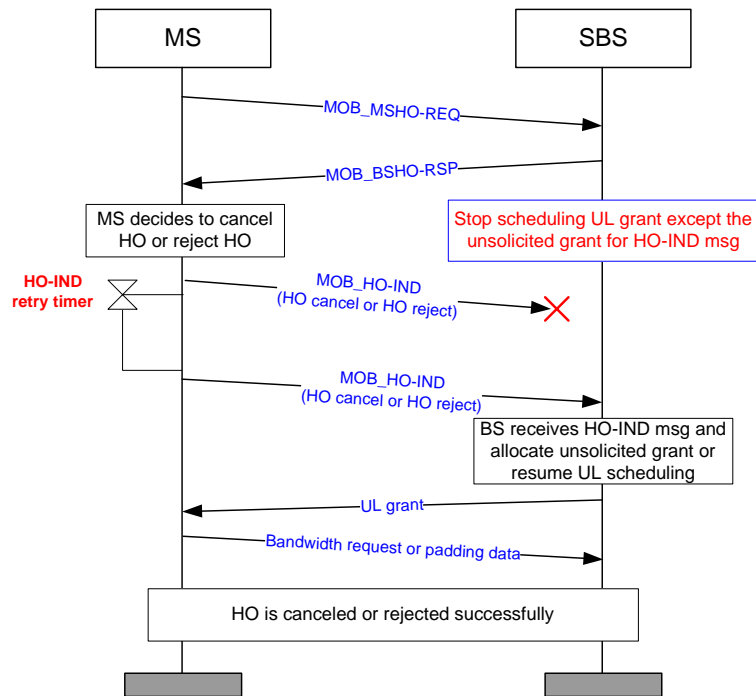


Figure 9 – Suggested remedy for scenario 2

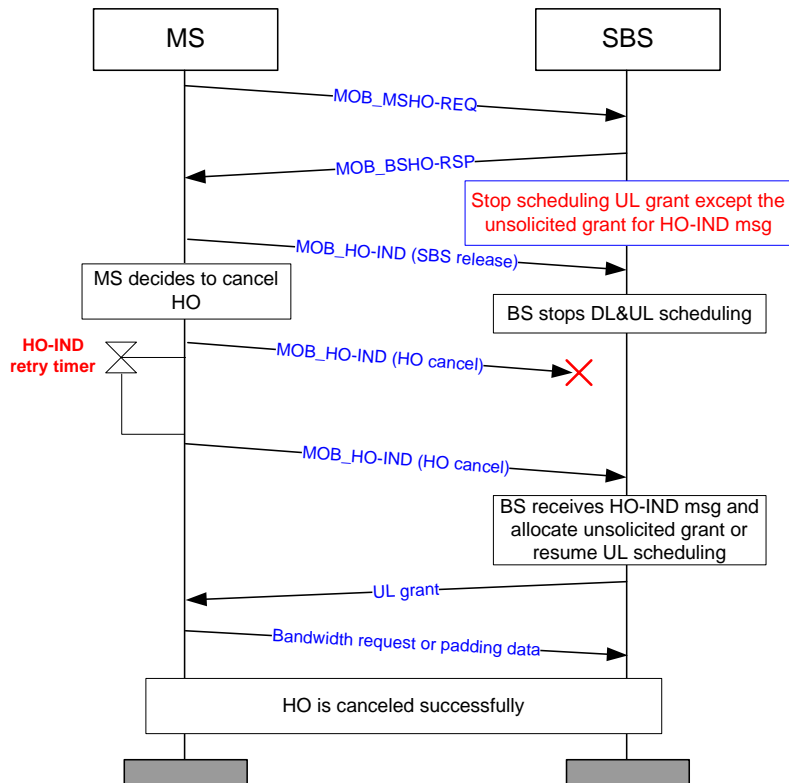


Figure 10 – Suggested remedy for scenario 3

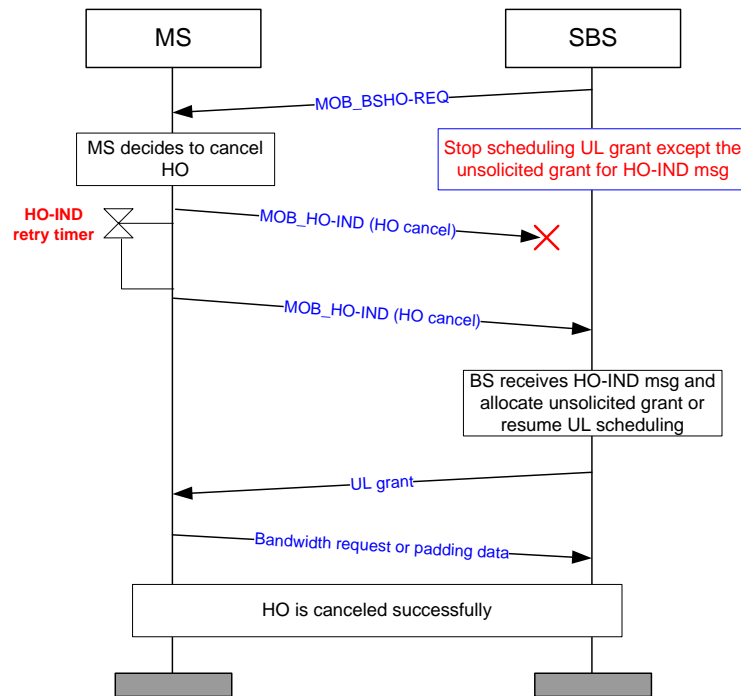


Figure 11 – Suggested remedy for scenario 4

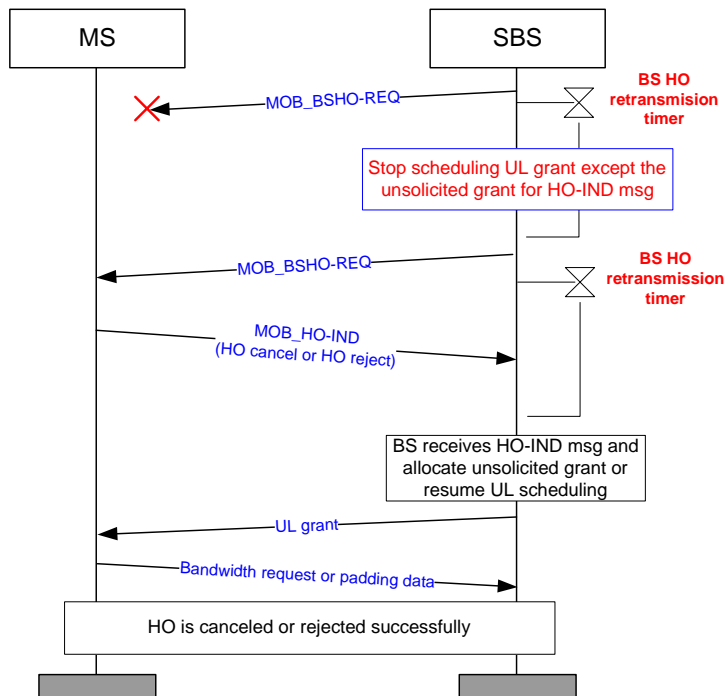


Figure 12 – Suggested remedy for scenario 5 and 6



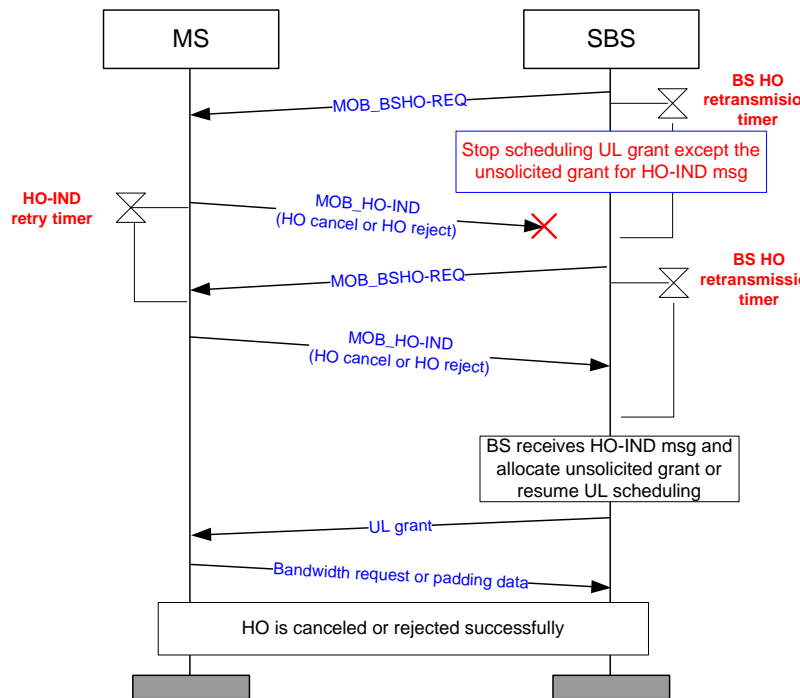


Figure 13 – Suggested remedy for scenario 5 and 6

## Suggested Changes in Rev2/D2

### Part 1

-----Start of the Text-----

[InRev2/D2, line 13 on page 437, section 6.3.22.2.2, insert the following text]

The serving BS shall stop issuing UL allocations to the MS expect the unsolicited grant for the transmission of MOB\_HO-IND message or bandwidth request for Basic CID after sending MOB\_BSHO-REQ/RSP message to the MS or after expiration of Handover Indication Readiness Timer if Unsolicited UL Grant for HO-IND flag is set to 1. If the Serving BS receives MOB\_HO-IND message from the MS and HO\_IND\_type field indicates the HO cancel or HO reject, it shall allocate UL allocation to the MS as an acknowledge of reception of MOB\_HO-IND message. The BS shall resume issuing DL and UL allocations for MS upon receiving one of the following messages: MOB\_HO-IND message that HO\_IND\_type field indicates HO cancel or HO reject or MOB\_MSHO-REQ message. The serving shall start BS HO request retransmission timer after sending MOB\_BSHO-REQ message and it shall retransmit the MOB\_BSHO-REQ message if it does not receive the MOB\_HO-IND message from the MS before the expiration of BS HO request retransmission timer. If the maximum retries exceeded on transmission of the MOB\_BSHO-REQ message, the serving BS shall start Resource Retain timer.

-----End of the Text-----

### Part 2

-----Start of the Text-----

[InRev2/D2, line 27 on page 437, section 6.3.22.2.3, insert the following text]

Once MS decides to cancel HO or reject HO after receiving the MOB\_BSHO-REQ/RSP message, it shall start a

HO-IND retry timer immediately after sending the MOB\_HO-IND message or after Handover Indication Readiness Timer if Unsolicited UL Grant for HO-IND flag is set to 1 in MOB\_BSHO-REQ/RSP message, then waits for the UL allocation as an acknowledge of reception of MOB\_HO-IND message. If MS does not receive the UL allocation before the expiration of the HO-IND retry timer, it shall retransmit the MOB\_HO-IND message to cancel HO or to reject HO, otherwise MS considers that the HO cancellation or rejection is successful. If the maximum retries exceeded on transmission of the MOB\_HO-IND message, the MS shall perform initial network entry or HO with other BS.

If MS sends MOB\_HO-IND message with HO cancel right after sending MOB\_MSHO-REQ message or MS sends MOB\_HO-IND message with HO cancel or HO reject after receiving MOB\_BSHO-REQ message, but receives MOB\_BSHO-REQ/RSP message from serving BS, it shall consider that the MOB\_HO-IND message has been lost. In this case, it shall retransmit the MOB\_HO-IND message to cancel HO and start HO-IND retry timer immediately or after Handover Indication Readiness Timer if Unsolicited UL Grant for HO-IND flag is set to 1 in MOB\_BSHO-REQ/RSP message.

-----End of the Text-----

### Part 3

-----Start of the Text-----

*[InRev2/D2, line 38 on page 438, section 6.3.22.2.6, change the third paragraph as]*

When the MS has detected a drop during network reentry with a target BS, it may attempt network reentry with its preferred target BS as through Cell Reselection (see 6.3.22.2.1), and may include resuming communication with the serving BS by sending MOB\_HO-IND message with HO\_IND type = 0b01 (HO cancel) **and start HO-IND retry timer immediately. If the maximum retries exceeded on contention-based bandwidth request or transmission of the MOB\_HO-IND message, the MS shall perform initial network entry or HO with other BS.** If the MS fails network reentry with its preferred target BS, the MS shall perform initial entry procedure.

-----End of the Text-----

### Part 4

-----Start of the Text-----

*[InRev2/D2, line 56 on page 438, section 6.3.22.2.6, add the sentence at the end of fourth paragraph]*

The serving BS shall ignore the bandwidth request from the MS that resources are not retained by serving BS any more.

-----End of the Text-----

### Part 5

-----Start of the Text-----

*[InRev2/D2, table 525, insert the following text]*

System	Name	Time reference	Minimum value	Default value	Maximum value
MS	HO-IND retry timer	Wait for UL allocation after sending the MOB_HO-IND message or after Handover Indication Readiness Timer if Unsolicited UL Grant for HO-IND flag is set to 1 in		Same as contention-based reservation timeout value specified in	

		MOB_BSHO-REQ/RSP message.		UCD.	
MS	Maximum MOB_HO-IND message retries	Number of timeout retries on MOB_HO-IND message		5	
BS	BS HO retransmission timer	Wait for MOB_HO-IND message from MS after sending MOB_BSHO-REQ message		70 ms or Handover Indication Readiness Timer if Unsolicited UL Grant for HO-IND flag is set to 1 in MOB_BSHO-REQ message	
BS	Maximum BSHO-REQ message retries	Number of timeout retries on MOB_BSHO-REQ message		5	

-----End of the Text-----