Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>	
Title	**HO Latency Reduction**	
Date Submitted	**2008-05-14**	
Source(s)	Brian Shim, Sungjin Lee, Geunhwi Lim, Samsung Electronics	Voice: +82-31-279-5248 E-mail: steve.lee@samsung.com
	Xiangying Yang Intel	E-mail: xiangying.yang@intel.com
	Vladimir Yanover, Nadav Lavi Alvarion	E-mail : vladimir.yanover@alvarion.com
	Tzavidas Stavros Motorola	E-mail : stavros.tzavidas@motorola.com
	Kiseon Ryu LGE	E-mail : ksryu@lge.com
	Yerang Hur Posdata	E-mail : yehur@posdata-usa.com
Re:	LB26c	
Abstract	This proposal proposes a method to reduce handover latency.	
Purpose	Review and adopt.	
Notice	*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.	
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: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.	

Handover Latency Reduction

Brian Shim, Sungjin Lee, Geunhwi Lim
Samsung Electronics

Hyunjeong Hannah Lee, Xiangying Yang
Intel

Vladimir Yanover, Nadav Lavi
Alvarion

Tzavidas Stavros
Motorola

Yerang Hur
Posdata

Kiseon Ryu
LGE

Erik Colban
Nextwave

Phillip Barber
Huawei

1.Problem Overview

When an MS moves toward a target cell performing a hard handover (HHO), it disconnects with the current serving base station (BS) and performs network re-entry procedure in order to connect with the target BS. During HHO, there then exists a service interruption time for which the MS cannot send/receive data traffic to/from any BS. Thereby, it is essential to maintain the service interruption time short enough so that during HHO the performance degradation of delay sensitive applications such as VoIP can be unnoticeable. According to the current IEEE 802.16e, the service interruption time begins right after the MS sends the MOB_HO-IND message and lasts until the network re-entry completes..

Once the MS moves to the target cell, the MS must achieve PHY synchronization first, and then update MAC context information to connect to the target BS by exchanging MAC management messages. The MAC context update procedure includes RNG-REQ/RSP, SBC-REQ/RSP, Authorization, and REG-REQ/RSP message exchanges. In order to reduce the service interruption time, the current IEEE 802.16e protocol employed HO optimization. Especially for the fully optimized HO, all the MAC context update steps can be combined into one step and thus the MS is required to exchanges only RNG-REQ/RSP with the target BS before resuming data transmission/reception at the target BS.

Furthermore, in the current system, during handoff, new TEKs are generated and sent to MS through SA-TEK-Update TLV in RNG-RSP or PKMv2 SA-TEK-Response messages, which increases the latency of the Handover- process.

If new TEKs are not included in the handover procedure, the TEKs used in S-BS continue to be used in T-BS,

but it is less secure than using new TEKs at the T-BS.

In addition, establishment of secure connections during the Handover is further delayed by the ranging transaction (RNG-REQ – RNG-RSP). This adds additional delay to the Handover process.

This contribution proposes a way to further reduce the service interruption time for the fully optimized HO by allowing data to flow before the RNG-REQ/RSP exchange procedure is completed at Target BS. In order to achieve this the authors have consensus on that CID allocation update and security procedures should be performed in other way rather than Ranging message exchange.

2. Proposed Solution

In the up-front negotiations procedure, both MS and BS shall clearly identify their capabilities to support the TEK Generation mechanism and the CID update mechanism described here.

When the serving BS contacts the potential target BSs for a HO, the potential target BSs actually assign the connection IDs and then respond the serving BS with these pre-assigned CIDs for the MS performing HO. Then, the pre-allocated CID update information is delivered to the MS prior to HO execution, i.e., during HO preparation, via the serving BS through MOB_BSHO-REQ or MOB_BSHO-RSP messages. Resultantly, the size of these messages becomes larger. Because MOB_BSHO-REQ or MOB_BSHO-RSP messages are usually transmitted when the MS is located in the cell edge, it is desirable to reduce their sizes as much as possible.

As RNG-REQ/RSP is omitted, authentication and TEK updates are an additional issue to be resolved.

We propose a TEK generation mechanism for handover. Based on this mechanism, the MS and T-BS generate TEKs respectively without any extra message exchange during handover.

In the proposed TEK generation algorithm, new TEKs at the T-BS are computed by

TEK*i* = Dot16KDF (KEK', CMAC_KEY_COUNT_T, SA-ID, "TEK*i* Generation")

…… (1)

In the above formula KEK' is a simple transformation of KEK in order to to cryptographically isolate the KEK used for encrypting the TEK (legacy) from KEK' used for generating the TEKs during HO. KEK' is computed as follows: KEK' = Dot16KDF(KEK).

The main idea behind this proposal is to use CMAC_KEY_COUNT to guarantee freshness when generating TEKs after the MS has successfully accessed a new BS. In equation (1) , CMAC_KEY_COUNT_T is the expected value of the CMAC_KEY_COUNT to be used for generating the CMAC_KEY_* keys. After the exchange of RNG-REQ and RNG-RSP messages that is used to establish a value for the CMAC_KEY_COUNT at the MS and the BS, CMAC_KEY_COUNT_T is simply the established value. During handover, however, we propose to allow for the generation of TEKs before the exchange of RNG-REQ and RNG-RSP messages. In this case, CMAC_KEY_COUNT_T_M = CMAC_KEY_$COUNT_M$ + 1 and CMAC_KEY_COUNT_T_B = CMAC_KEY_$COUNT_N$.

The label "TEK*i* Generation" differentiates between TEK0 and TEK1 keys generated for the same SAID. Specifically the labels will be "TEK0 Generation" and "TEK1 Generation"

Initially, TEK0 and TEK1 Lifetimes are set to 1/8 and ½ of the PMK Lifetime respectively. PN0, PN1, RxPN0,

and RxPN1 are initialized to 0 at the time when fresh TEK0 and TEK1 are generated.

TEK update during handover

(1) Before access to the T-BS, the MS computes the TEKs by using the value of CMAC_KEY_COUNT_T_M = CMAC_KEY_COUNT$_M$ +1, KEK, T-BS ID, etc. Then, it sends MOB-MSHO-REQ to indicate the S-BS of the handover intention.

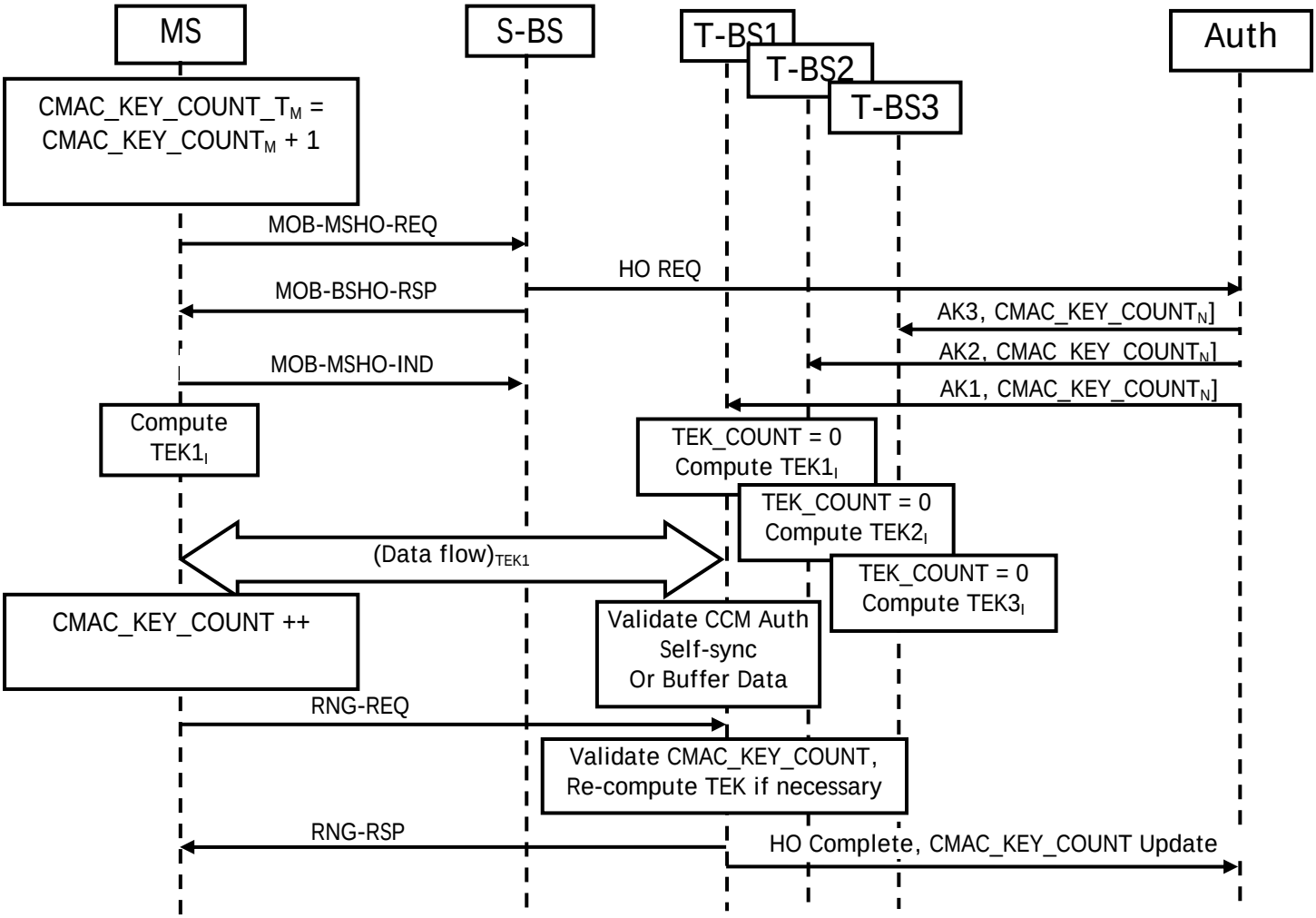
(2) All potential T-BS's are pre-populated with AK Context, including AK and CMAC_KEY_COUNT$_N$. To prevent potential replay attacks, all T-BS(s) shall retain received AK Context and PNs until an explicit indication of HO completion is received from the Authenticator – consistent with current NWG specifications.

(3) The T-BS computes the TEK once the CMAC_KEY_COUNT$_N$ is received. If CMAC_KEY_COUNT$_N$ is received before CMAC_KEY_COUNT$_M$, the TEKs are computed with CMAC_KEY_COUNT_T_B = CMAC_KEY_COUNT$_N$.

There is a potential of CMAC_KEY_COUNT_T_B < CMAC_KEY_COUNT_T_M, and it leads to the inconsistent TEKs in MS and T-BS. To handle this error, the following conditions are considered in TBS

- CMAC_KEY_COUNT_T_B = CMAC_KEY_COUNT_T_M
  - Normal valid case. Its validity can be determined early by verifying AUTH of UL Data if AES/CCM is used.
- CMAC_KEY_COUNT_T_B < CMAC_KEY_COUNT_T_M
  - This is a mis-synchronization case, which gets resolved when the T-BS receives the updated value of CMAC_KEY_COUNT$_M$ later during the handover process.
  - If AES/CCM is used, and the T-BS receives UL data, then the T-BS can apply a classic self-synchronization method:
    - CMAC_KEY_COUNT_T_B is force-incremented by the T-BS, and AUTH of UL Data is checked again.
    - This procedure is optional and is left to implementation
- CMAC_KEY_COUNT_T_B > CMAC_KEY_COUNT_T_M
  - This is a replay attempt. Self-sync will not succeed. The data from MS has to be discarded.
  - Once the CMAC_KEY_COUNT$_M$ is received and found to be smaller than expected, the connection is released.

Note that the since CMAC_KEY_COUNT$_N$ does not get incremented until after the MS successfully completes a handover and the MS may cancel handover, the Authenticator may pass the same value of CMAC_KEY_COUNT$_N$ to the T-BS in a subsequent handover. Therefore, the T-BS should cache the TEK context (including PNs) associated with the value of CMAC_KEY_COUNT_T_B until CMAC_KEY_COUNT$_N$ has been incremented beyond that value. Likewise, the MS should cache all TEK contexts associated with a value of CMAC_KEY_COUNT_T_M until it increments CMAC_KEY_COUNT$_M$.



Optimization HO with No Additional Signaling

Normal TEK Refresh

- In order to minimize the changes needed to implement the proposed algorithm, all TEK update and generation procedures other than TEK update during HO are left unchanged. As currently defined, TEK can be requested by MS and returned to MS under encryption by KEK.

3. Proposed Text Changes

Remedy 1:

[Adopt the following changes in section 6.3.1.1 Point-to-multipoint (PMP):]

Each air interface in an SS shall have a 48-bit universal MAC address, as defined in IEEE Std 802®-2001. This address uniquely defines the air interface of the SS. It is used during the initial ranging process to establish the

appropriate connections for an SS. It is also used as part of the authentication process by which the BS and SS each verify the identity of the other.

Connections are identified by a 16-bit CID. At SS initialization, two pairs of management connections, basic connections (UL and DL) and primary management connections (UL and DL), shall be established between the SS and the BS, and a third pair of management connections (secondary management, DL and UL) may be optionally generated. The three pairs of management connections reflect the fact that there are inherently three different levels of QoS for management traffic between an SS and the BS. The basic connection is used by the BS MAC and SS MAC to exchange short, time-urgent MAC management messages. The primary management connection is used by the BS MAC and SS MAC to exchange longer, more delay-tolerant MAC management messages. Table 36 specifies which MAC management messages are transferred on which of these two connections. In addition, it also specifies which MAC management messages are transported on the broadcast connection. Finally, the secondary management connection is used by the BS and SS to transfer delay-tolerant, standards-based [Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), SNMP, etc.] messages. Messages carried on the secondary management connection may be packed and/or fragmented. For the OFDM, and OFDMA PHYs, management messages shall have CRC. Use of the secondary management connection is required only for managed SS.

The CIDs for these connections shall be assigned in the RNG-RSP, ~~ and~~ REG-RSP, ~~messages~~or MOB_BSHO-REQ/RSP for pre-allocation in handover. When CID pre-allocation is used during HO, ~~A~~a primary management CID may be derived based on Basic CID without assignment in the messages (see 6.3.22.2.11). The message dialogs provide three CID values. The same CID value is assigned to both members (UL and DL) of each connection pair.

For bearer services, the BS and the SS may initiate the set-up of service flows based upon the provisioning information. The registration of an SS, or the modification of the services contracted at an SS, stimulates the higher layers of the BS and/or the SS to initiate the setup of the service flows. When admitted or active, service flows are uniquely associated with transport connections. MAC management messages shall never be transferred over transport connections. Bearer or data services shall never be transferred on the basic, primary, or secondary management connections.

Bearer connection CID reassignments during handover or network re-entry shall be sent using the REG-RSP encodings TLV in the RNG-RSP message, ~~ or~~ the REG-RSP message, or reassigned autonomously without explicit assignment in any message (see 6.3.22.2.11).

Requests for transmission are based on these CIDs, since the allowable bandwidth may differ for different connections, even within the same service type. For example, an SS unit serving multiple tenants in an office building would make requests on behalf of all of them, though the contractual service limits and other connection parameters may be different for each of them.

Many higher layer sessions may operate over the same wireless CID. For example, many users within a company may be communicating with Transmission Control Protocol (TCP)/IP to different destinations, but since they all operate within the same overall service parameters, all of their traffic is pooled for request/ grant

purposes. Since the original local area network (LAN) source and destination addresses are encapsulated in the payload portion of the transmission, there is no problem in identifying different user sessions.

The type of service and other current parameters of a service are implicit in the CID; they may be accessed by a lookup indexed by the CID.

[Add new section 6.3.22.2.11 as indicated:]

6.3.22.2.11 Seamless HO

In addition to Optimized HO, MS and BS may perform Seamless HO to reduce HO latency and message overhead. The capability of Seamless HO is negotiated by REG-REQ/RSP message (see 11.7.13.5).

If any authorization policy, except "No Authorization," is negotiated between MS and BS, seamless HO also requires support for counter-based TEK Generation for HO (see 7.2.2.2.6.1).

To perform Seamless HO for an MS in serving BS, target BS(s) and the MS shall support Seamless HO as well. A BS supporting Seamless HO shall include Connection identifier descriptor TLV in DCD message. In the Seamless HO, a target BS calculates Primary management CID, Secondary management CID, and Transport CIDs for an MS by using the descriptor.

During Seamless HO, a serving BS shall include Pre-allocated Basic CID in MOB_BSHO-REQ/RSP for an MS. When a BS pre-allocates a Basic CID to an MS during Seamless HO, primary management CID is allocated autonomously without explicit assignment in the message. If *n*-th Basic CID within the range 0x0001– *m* (see Table 528) is allocated, the *n*-th Primary Management CID in the range *m*+1 – 2*m* shall be allocated to the same MS in ascending order. The Primary management CID is derived by adding '*m*' to the Basic CID, where the '*m*' is given by Connection identifier descriptor in DCD message.

When a BS assigns Pre-allocated Basic CID, it also reserves a block of continuous transport CIDs, where the number of CIDs is '*a*' within the range *2m*+1–0xFE9F (see Table 528). The block of continuous transport CIDs starts from the 2*m*+1 and each block consists of continuous '*a*' number of CIDs, where '*a*' is given by Connection identifier descriptor in DCD message.

Once CIDs have been pre-allocated BS shall determine and indicate whether it will perform Seamless HO by including Seamless HO mode flag into MOB-BSHO-REQ/RSP message. When MS receives MOB_BSHO-REQ or MOB_BSHO-RSP message with the Seamless HO mode flag set to 1 (support), MS can perform Seamless HO by transmitting HO-IND message including the BS-ID of a BS among the recommended BSs that indicate support for seamless HO (i.e. a BS for which Seamless HO mode flag was set to 1 in the BSHO-REQ/RSP message). If MS transmits HO-IND message including the BS-ID of any BS other than the recommended BSs which indicate support for Seamless HO then Seamless HO is not applied for this BS.

The MOB_BSHO-REQ or MOB_BSHO-RSP message may contain specific action time. If this value is specified, pre-allocated CIDs are valid at the target BS after the time specified by the action time. Value of 0 indicates that the pre-allocated CIDs are already valid and MS may initiate Seamless HO at anytime.

During seamless HO, the target BS (T-BS) may allocate downlink and uplink resource for the MS before the RNG-REQ/RSP message transaction, as shown in figure A.

During Seamless HO, the MS is required to initiate the RNG-REQ/RSP message transaction by sending RNG-REQ message before the deadline specified by the “Seamless HO Ranging Initiation Deadline” attribute included in BSHO-REQ/RSP message during handover preparation. The time is measured from the time the BSHO-REQ/RSP message is transmitted. If the T-BS does not receive a RNG-REQ message by the MS within the deadline defined by the “Seamless HO Ranging Initiation Deadline” attribute, it considers the seamless HO as failed and stops allocating bandwidth to the MS. It is recommended that the BS allows time equal to T3 timer (table 544) before it reuses the CIDs that were allocated to the MS. The MS considers the seamless HO as failed if it does not transmit RNG-REQ message before the deadline. If the MS transmits RNG-REQ within the deadline, it may still consider the HO as failed if it does not receive a RNG-RSP within T3 time after the last (re)transmission of RNG-REQ that was performed within the deadline. When the MS considers the seamless HO as failed, it invalidates the pre-allocated CIDs. In all cases, even when the RNG-REQ/RSP message transaction is initiated before the deadline, the Seamless HO is considered failed if the RNG-REQ/RSP procedure fails.

When data packets are exchanged before the RNG-REQ/RSP transaction is completed, the recipient (MS or BS) should store the received data packets and not release them to the upper layers until the sender is authenticated. If the data packets belong to a service flow associated with an SA that supports data authentication (as indicated by the data authentication algorithm identifier in the cryptographic suite of the SA) the receiver can authenticate the sender by verifying that the ciphertext authentication code included in each data packet was produced with the TEK associated with this SA. If the data packets belong to a service flow associated with an SA that does not support data authentication the receiver can authenticate the sender when the RNG-REQ/RSP transaction completes successfully. In all cases, if the sender is authenticated, the decrypted data packets are released to the upper layer in the recipient, and if the sender is not authenticated the data packets are discarded.

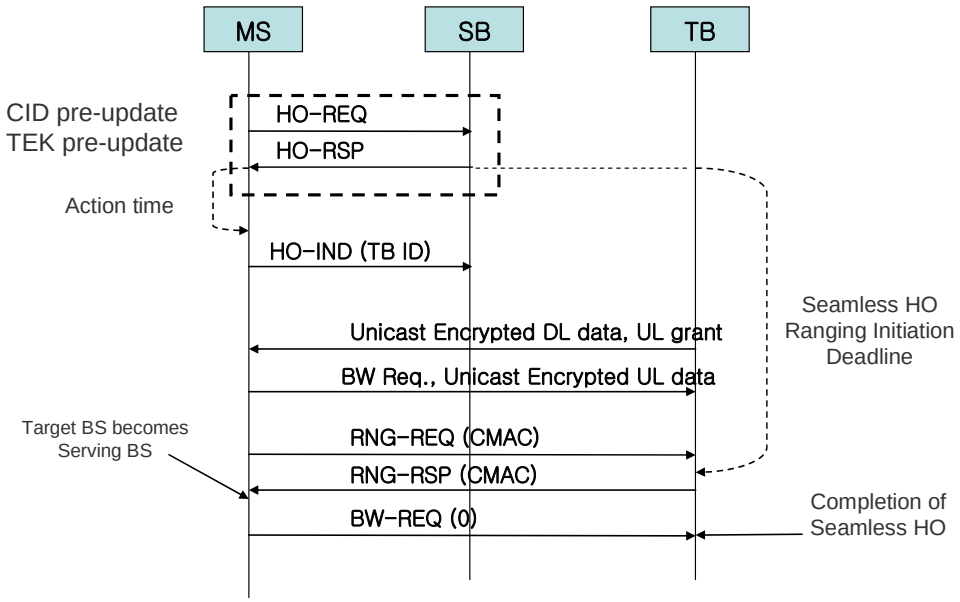


Figure A - Seamless HO call flow

The RNG-REQ/RSP transaction for Seamless HO is shown in Figure A. MS shall initiate RNG-REQ/RSP transaction by transmitting RNG-REQ message to target BS before the deadline specified by the "Seamless HO Ranging Initiation Deadline" attribute included in BSHO-REQ/RSP message during handover preparation. The RNG-REQ message shall include Basic CID, CMAC_KEY_COUNT and valid HMAC/CMAC tuple. Ranging Purpose Indication TLV with Bit #2 set to 1, but not include MS MAC address or previous serving BS-ID. When BS receives the RNG-REQ message, BS shall respond to the RNG-REQ message by transmitting RNG-RSP message with valid HMAC/CMAC tuple. The RNG-RSP message does not need to include any CID update TLV or SA-TEK-Update TLV.

When MS receives the RNG-RSP message from the target BS, the target BS becomes serving BS of the MS and MS shall transmit a BR header with 0 bandwidth request. When BS receives the BR header, the Seamless HO procedure completes successfully.

Remedy 2:

A flag bit is used to indicate whether each recommended neighbor BS accept Seamless HO. If this bit is set to 1, **Pre-allocated Basic CID** field shall be included.

[Adopt the following changes in line 45 on pp. 215, Table 149—MOB_BSHO-REQ message format (continued):]

HO_authorization policy indicator	1	To indicate whether security-related negotiation is used in HO procedure. 0: Same authorization policy and MAC mode as in the serving BS 1: The authorization policy for the target BS is negotiated.
~~**Padding**~~ Seamless HO mode flag	1	~~To ensure nibble alignment.~~ To indicate whether Seamless HO mode is supported 0 : not supported 1 : supported

[Adopt the following changes in line 29 on pp.229, Table 151—MOB_BSHO-RSP message format (continued):]

HO authorization policy indicator	1	To indicate whether security-related negotiation is used in HO procedure. 0: Same authorization policy and MAC mode as in the serving BS 1: The authorization policy for the target BS is negotiated.
Seamless HO mode flag	1	To indicate whether Seamless HO mode is supported 0 : not supported 1 : supported
Reserved	~~5~~4	Shall be set to zero

[Adopt the following changes

(1) in line 8 on page 216 for MOB_BSHO-REQ and

(2) in line 50 on page 229 for MOB_BSHO-RSP message format:]

If (HO_authorization policy indicator == 1) {	—	—
HO_authorization_policy_support	8	Bit #0: RSA authorization Bit #1: EAP authorization Bit #2: Reserved Bit #3: HMAC supported Bit #4: CMAC supported Bit #5: 64-bit Short-HMAC Bit #6: 80-bit Short-HMAC Bit #7: 96-bit Short-HMAC
}		
If (Seamless HO mode flag ==1) {		
CID update mode indicator	*1*	0 : autonomous derivation 1 : block allocation
Pre-allocated Basic CID	*16*	Basic CID allocated by the target BS
Rejected Transport CID bitmap size	*4*	Length to be read (in bytes) 0 : all the Tranport CIDs are accepted 1-15 : bitmap size in bytes
If (CID update mode indicator=0){		
Reserved	*3*	-
}		
If (CID update mode indicator==1) {		
N_block	*3*	Number of blocks
If (N_block==1){		
First Transport CID in block	*16*	
}		
If (N_block >1){		
For (j = 0 ; j < N_block; j++) {		
First Transport CID in block	*16*	The first Transport CID in the block

Number of Transport CIDs	*8*	Number of contiguous Transport CIDs in the block
}		
}		
Rejected Transport CID bitmap	Variable	This bitmap indicated Transport CID which is not accepted by the BS. The length of the parameter is defined by **Rejected Transport CID bitmap size** field.
}		
Seamless HO Ranging Initiation Deadline	*8*	Time allowed for the MS to transmit RNG-REQ at the target BS during seamless HO. The time is specified in units of 10 msec. Time starts at the time the message it is contained in (i.e. BSHO-REQ/RSP) is transmitted
}		

[Adopt the following changes in 6.3.2.3.47 MOB_BSHO-REQ (BS HO request) message (pp. 223):]

HO_ID included indicator

Indicates whether HO_ID is included in this message.

HO_ID

ID assigned for use in initial ranging to the target BS once this BS is selected as the target BS (see 11.5).

Seamless HO mode flag

Indicates whether Seamless HO is performed at the recommended neighbor BS. When the flag set to 1, the Pre-allocated Basic CID is included in the message.

Pre-allocated Basic CID

Basic CID allocated by recommended neighbor BS.

Seamless HO Ranging Initiation Deadline

Time allowed for the MS to transmit RNG-REQ at the target BS during seamless HO. The time is specified in units of 10 msec. Time starts at the time the message it is contained in (i.e. BSHO-REQ/RSP) is transmitted.

AK Change Indicator

Indicates whether the authorization key being used should change when switching to a new anchor BS. If set to 0, the MS should continue to use the AK currently in use; if set to 1, the MS should use the AK derived for use with the new anchor BS.

[Adopt the following changes in 6.3.2.3.49 MOB_BSHO-RSP (BS HO response) message (pp. 236):]

HO_ID_included_indicator

Indicates whether HO_ID is included in this message.

Seamless HO mode flag

Indicates whether Seamless HO is performed at the recommended neighbor BS. When the flag set to 1, the Pre-allocated Basic CID is included in the message.

Pre-allocated Basic CID

Basic CID allocated by recommended neighbor BS.

The MOB_BSHO-RSP may contain the following TLV:

Resource Retain Time (see 11.15.1)

Remedy 3:

[Adopt the following changes in 6.3.22.2.2 HO decision and initiation:]

An HO begins with a decision for an MS to HO from a serving BS to a target BS. The decision may originate either at the MS, the serving BS, or on the network. The HO may proceed with a notification through either MOB_MSHO-REQ or MOB_BSHO-REQ messages. The HO notification is recommended, but not required. Acknowledgement of MOB_MSHO-REQ with MOB_BSHO-RSP is required. After MS transmits MOB_MSHO-REQ, MS shall not transmit any MOB_MSHO-REQ prior to expiration of timer MS_handover_retransmission_timer. MS shall deactivate timer MS HO retransmission timer on MS transmission of MOB_HO-IND or MS receipt of MOB_BSHO-RSP.

If an MS that transmitted a MOB_MSHO-REQ message detects an incoming MOB_BSHO-REQ message before the MS_handover_retransmission_timer (see 11.7.13.3) expires, it shall ignore that MOB_BSHOREQ message. A BS that transmitted a MOB_BSHO-REQ message and detects an incoming MOB_MSHOREQ message from the same MS shall ignore its MOB_BSHO-REQ. A BS that transmitted a MOB_BSHOREQ message and detects an incoming MOB_HO-IND message from the same MS shall ignore its own previous request. While a handover is in progress, an MS that has transmitted a MOB_HO-IND message and detects an incoming MOB_BSHO-REQ message from the Serving BS shall ignore that MOB_BSHO-REQ.

When MOB_MSHO-REQ is sent by an MS, the MS may indicate one or more possible target BS. When MOB_BSHO-REQ is sent by a BS, the BS may indicate one or more possible target BSs. MS may evaluate possible target BS(s) through previously performed scanning and Association activity.

Serving BS criteria for recommendation of target BS may include factors such as expected MS performance at potential target BS, BS and network loading conditions, and MS QoS requirements. The serving BS may obtain expected MS performance, ~~and~~ BS and network loading conditions at a potential target BS and Basic CID to be used at a potential target BS through the exchange of messages with that BS over the backbone network. The serving BS may negotiate location of common time interval where dedicated initial ranging transmission opportunity for the MS will be provided by all potential target BSs. This information may be included into MOB_BSHO-RSP message, and is indicated by Action Time. The Pre-allocated Basic CID shall be included into MOB_BSHO-REQ/RSP if the recommended target BS supports Seamless HO mode.

If the Basic CID is pre-allocated at the serving BS, the MS should update its primary management CID and transport CIDs autonomously at the target BS without using CID_update or Compressed CID_update encodings. An MS can derive the new CIDs at a target BS from the Pre-allocated Basic CID by using the Connection identifier descriptor TLV in DCD message. The new primary management CID should be derived by adding *'m'* to the Pre-allocated Basic CID.

There are two modes in deriving new transport CIDs at a target BS. If autonomous derivation mode is set, the new transport CIDs are derived with *'m'* and *'a'* parameters broadcasted in DCD message. The recommended BS reserves contiguous *'a'* number of transport CIDs for each MS. An MS can derive the first transport CID by using the equation {(2*m*+1) + (Basic CID-1) * *a*} and it autonomously updates its transport CIDs in ascending order from the first transport CID.

If the number of transport connections of an MS is greater than *'a'*, the block allocation mode should be used. If the block allocation mode is set in MOB_BSHO-REQ/RSP, the first CID at the head of the block shall be included in MOB_BSHO-REQ/RSP. The MS should update all the transport CIDs from the first CID followed by continuous CIDs in the block. A BS may allocate multiple blocks in the MOB_BSHO-REQ/RSP. When a BS allocates multiple blocks, it shall include the first Transport CID and number of Transport CIDs in MOB_BSHO-REQ/RSP for each block.

[Add the following parameter in Table 563—DCD channel encoding:]

Name	Type (1byte)	Length	Value	PHY scope
Connection identifier descriptor	155	2	MSB 11 bits = *m* (See Table 548) LSB 5 bits = *a* (number of reserved transport CIDs per MS)	OFDMA

Remedy 4:

[Adopt the following changes in 11.7.13.5 Handover Supported field:]

Type (1byte)	Length	Value	Scope
27	1	Bit #0: MDHO/FBSS HO supported when it is set to 1. When this bit is set to 0, the BS shall ignore ~~all other b~~Bits #1~#4. Bit #1: MDHO DL RF Combining supported with monitoring MAPs from active BSs when this bit is set to 1 Bit #2: MDHO DL soft Combining supported with monitoring single MAP from anchor BS when this bit is set to 1. Bit #3: MDHO DL soft combining supported with monitoring MAPs from active BSs when this bit is set to 1 Bit #4: MDHO UL Multiple transmission Bit #5: Seamless HO is supported when this bit is set to 1. Bits #~~5~~6-7: *Reserved*, shall be set to zero	REG-REQ REG-RSP

Remedy 4:

[Modify the following entry in table 569 – RNG-REQ message encodings as indicated.]

Name	Type	Length	Value (variable-length)	PHY Scope
Ranging Purpose Indication	6	1	Bit 0: HO indication (when this bit is set to 1 in combi-nation with other included information elements indi-cates the MS is currently attempting to HO or network reentry from idle mode to the BS) Bit 1: Location update request (when this bit is set to 1, it indicates MS action of idle mode location update pro-cess) Bit 2: Seamless HO indication (when this bit is set to 1 in combi-nation with other included information elements indicates the MS is currently initiating ranging as part of seamless HO procedure) Bits ~~2~~3–7: *Reserved*	-

Remedy 5:

[Add 7.2.2.2.6.1 as follows:]

7.2.2.2.6.1 Counter-based TEK Generation for HO

When both sides (MS and BS) indicate support for Seamless Handover, the TEKs during handover shall be generated by the BS and MS respectively using the following formula:

TEK*i*= Dot16KDF (KEK', CMAC_KEY_COUNT_T, SAID, "TEK*i* Generation") (A)

In the above formula KEK' is a simple transformation of KEK in order to cryptographically isolate the KEK used for encrypting the TEK (legacy) from KEK' used for generating the TEKs during HO. KEK' is computed as follows: KEK' = Dot16KDF(KEK).

The generated TEKs shall not be transferred between the BS and MS.

In the above equation, CMAC_KEY_COUNT_T (CMAC_KEY_COUNT for Traffic) is defined as follows: After the exchange of RNG-REQ and RNG-RSP messages that is used to establish a value for the CMAC_KEY_COUNT at the MS and the BS, CMAC_KEY_COUNT_T = CMAC_KEY_COUNT. During handover before the exchange of RNG-REQ and RNG-RSP messages, $CMAC\_KEY\_COUNT\_T_M = CMAC\_KEY\_COUNT_M + 1$ and $CMAC\_KEY\_COUNT\_T_B = CMAC\_KEY\_COUNT_N$, where $CMAC\_KEY\_COUNT\_T_M$ and $CMAC\_KEY\_COUNT\_T_B$ are the values of CMAC_KEY_COUNT_T at the MS and the BS respectively.

Both the MS and the BS shall compute the TEKs based on the current values of CMAC_KEY_COUNT_T. Initially, TEK0 and TEK1 Lifetimes are set to 1/8 and 1/2 of the PKM lifetime respectively. PN0, PN1, RxPN0, and RxPN1 shall be initialized to 0.

During handover before any transmission of data between the MS and the target BS, the MS shall set $CMAC\_KEY\_COUNT\_T_M = CMAC\_KEY\_COUNT_M + 1$ and $TEK\_COUNT_M = 0$ and the target BS shall set $CMAC\_KEY\_COUNT\_T_B = CMAC\_KEY\_COUNT_N$ and $TEK\text{-}COUNT_B = 0$. Unless the MS has cached a TEK context associated with the target BS and the current value of $CMAC\_KEY\_COUNT\_T_M$, the MS shall generate new values for the TEKs using the above formula. Unless the target BS has cached a TEK context associated with the MS and the current value of $CMAC\_KEY\_COUNT\_T_B$, the BS shall generate new values for the TEKs using the above formula. Otherwise the MS and BS shall apply the TEKs and associated parameters, including PN windows, from the cached contexts.

Occasionally, $CMAC\_KEY\_COUNT\_T_M$ and $CMAC\_KEY\_COUNT\_T_B$ are not equal, in which case the generated TEKs will be different too. In such cases, the target BS may attempt self-synchronizing the value of $CMAC\_KEY\_COUNT\_T_B$ by increasing the value until it can properly decode UL traffic.

If the target BS receives a valid RNG-REQ message including a CMAC_KEY_COUNT TLV (see 7.2.2.2.9.1) from the MS, and the received CMAC_KEY_COUNT value is different from $CMAC\_KEY\_COUNT\_T_B$ it shall set $CMAC\_KEY\_COUNT\_T_B$ to the received CMAC_KEY_COUNT value and regenerate new values for the TEKs using the above formula.

If the handover is not completed at the target BS, the target BS shall cache the TEK context until it can determine that CMAC_KEY_COUNT$_N$ has been incremented (e.g., by receiving a backbone message from the Authenticator). Likewise, the MS shall cache the TEK context until it increments CMAC_KEY_COUNT$_M$. See section 7.2.2.2.9.1 for further details on CMAC_KEY_COUNT handling.