Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**A Key Management Method for the Multicast Service**
Data Submitted	**2004-03-16**
Source(s)	Seokheon Cho Ae Soon Park Chulsik Yoon SungCheol Chang Kyung Soo Kim ETRI 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr aspark@etri.re.kr
Re:	This is a response to a Ballot #14 Announcement IEEE 802.16-04/06 on IEEE P802.16e-D1.
Abstract	The document contains suggestions on the changes in IEEE P802.16e-D1 that would support efficient key management method for the multicast service.
Purpose	The document is submitted for review by 802.16 Working Group members.
Notice	
Release	
Patent Policy and Procedures	

A Key Management Method for the Multicast Service

Seokheon Cho, Ae Soon Park, Chulsik Yoon, SungCheol Chang, and Kyung Soo Kim
ETRI

Introduction

1. Current structure of the TEK management for the multicast service

In order to provide a downlink multicast service safely, the key management for the multicast service is needed. The IEEE 802.16 considers that the key management for the multicast service is equal to that of the unicast service.

Current structure of the TEK management for the multicast service is shown as the <Figure 1>.

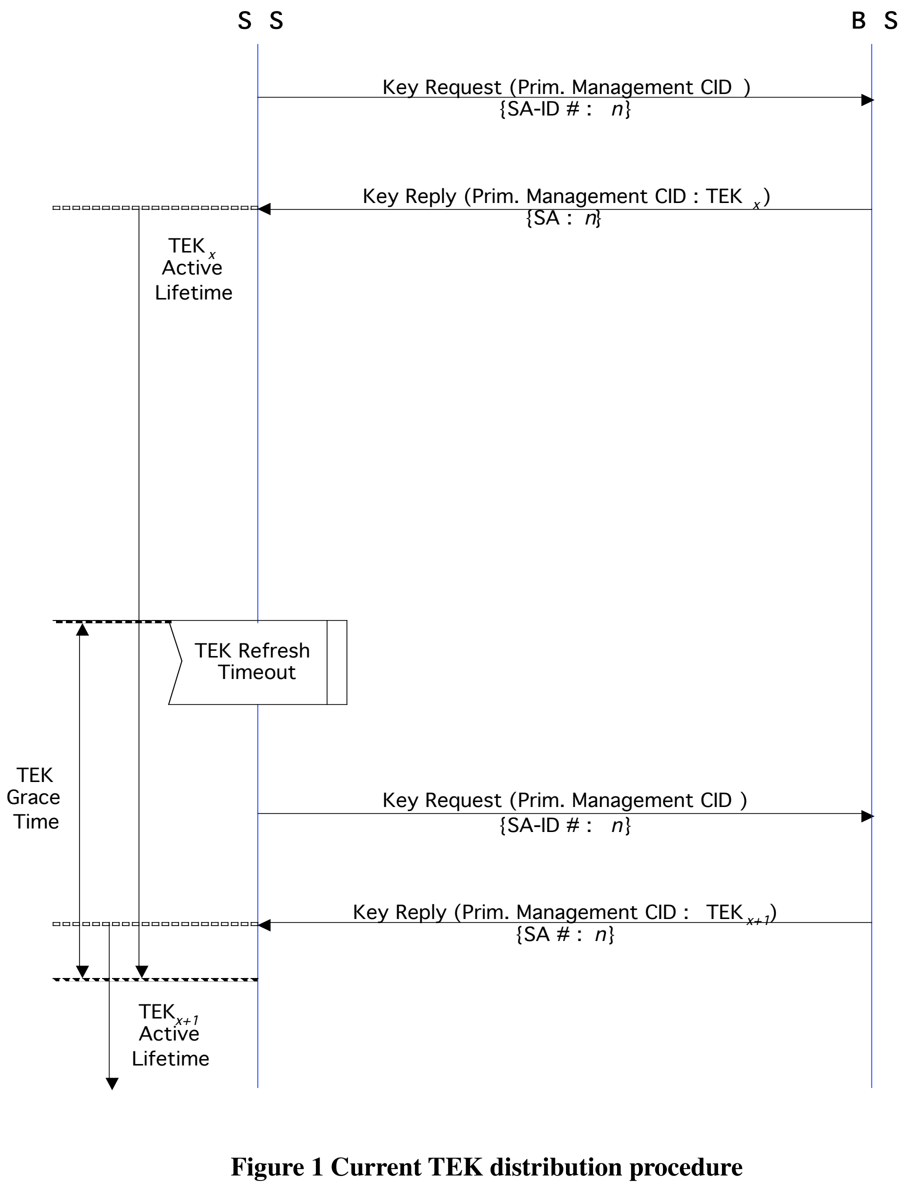

Figure 1 Current TEK distribution procedure

An SS tries to get the TEK before an SS is served with the specific multicast service. The SS sends the Key Request message to the BS through the primary management connection, requesting the TEK for the specific multicast service. This Key Request message should contain the SA-ID (if being equal to *n*) mapped to the specific multicast service. In response to this message, the BS sends the Key Reply message, including the n^{th} SA. The SS gets the TEK_x in the n^{th} SA (The TEK_x denotes the x^{th} assigned TEK for the n^{th} SA from the BS.) The Key Reply message is also carried on the primary management connection. So, both the SS and the BS share the TEK for the specific multicast service.

The SS can get the new TEK continuously by the above procedure. An SS periodically informs the BS to refresh key material for the n^{th} SA-ID at the TEK Grace Time by sending the Key Request message. BS responds to this message with the Key Reply message, containing the BS's active keying material for a specific SA-ID. The Key Request and Key Reply messages are also carried on the specific primary management connection between an SS and the BS. Hence, the TEK management for the multicast service follows this keying distribution procedure.

However, if the key management for the multicast service follows this procedure, then there are some inefficient problems. In this contribution, two suggestions are proposed about mapping relationship between the multicast service and the SA and the TEK management of the multicast service.

2. Relationship between the multicast service and the SA

1). Mapping a multicast connection to different SAs

In the IEEE 802.16 Wireless MAN Standard, it is mentioned that multicast transport connections may be mapped to any static or dynamic SA. This means that a multicast transport connection can be mapped to one or more static or dynamic SA. A multicast service may be mapped to different SAs or only one SA.

When a multicast service is mapped to different SAs, the key distribution flow is shown as the <figure 2>.

We assume that multiple users ($SS_1 \sim SS_z$) are simultaneously served with a specific multicast service, for example "A." However, different SAs are assigned to individual SSs. In this case, the BS should encrypt the same multicast traffic data with different SA, especially different TEK. Therefore, the BS is heavily burdened to do so.

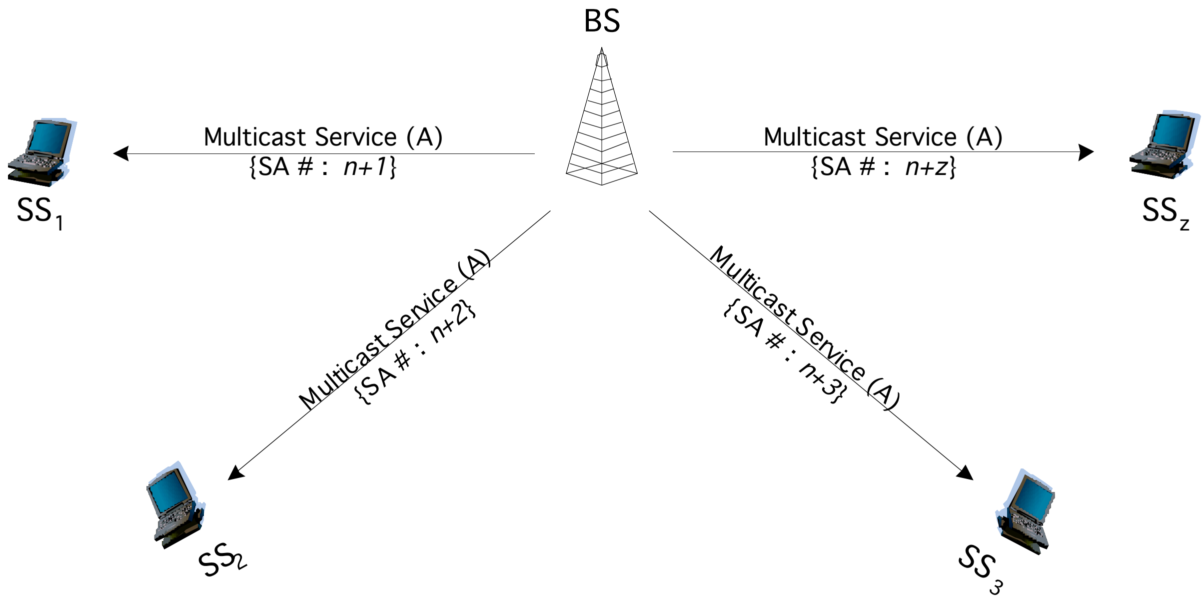

Figure 2 Multicast service example (A multicast service: different SAs)

2). Mapping a multicast connection to the same SA (Proposed solution)

We propose that a specific multicast service should be mapped to only one SA as shown in the <figure 3>.

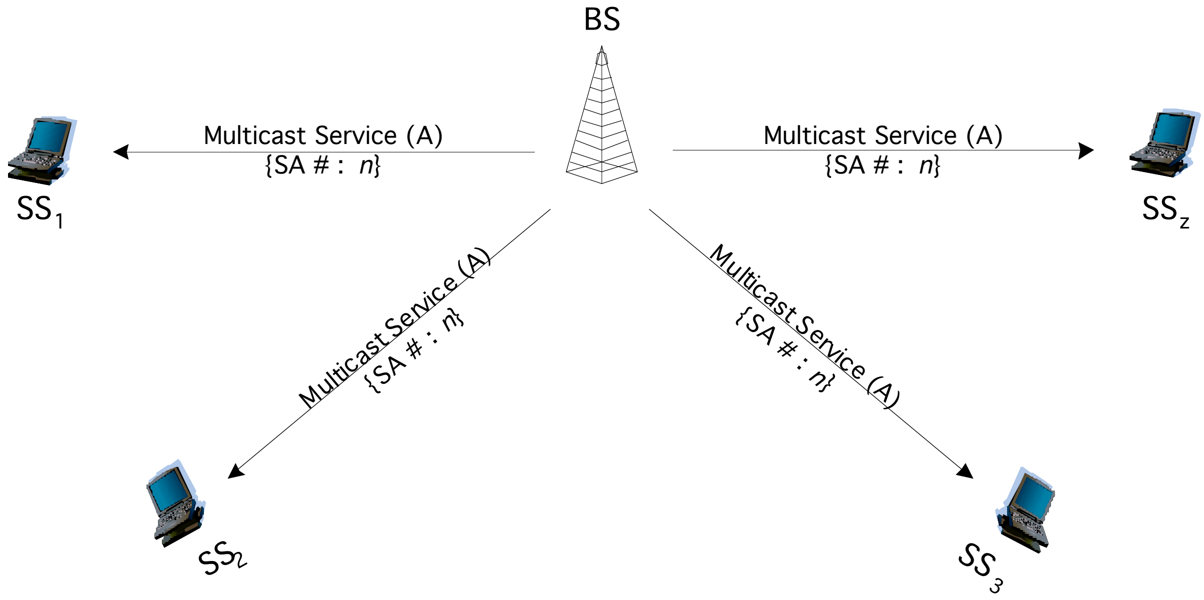

Figure 3 Multicast service example (A multicast service: equal SA)

The BS can mitigate the processing burden for encrypting multicast traffic data by using the equal SA.

3. The Key Refreshment and Distribution for the Multicast Service

1). Carried on the primary management connection (existing method)

The TEK distribution method is specified as shown in the <figure 1> in the IEEE 802.16. The Key Request and Key Reply messages used for the TEK refreshment are carried on the primary management connection. The TEK updating and distribution procedure is shown as the <figure 4>.

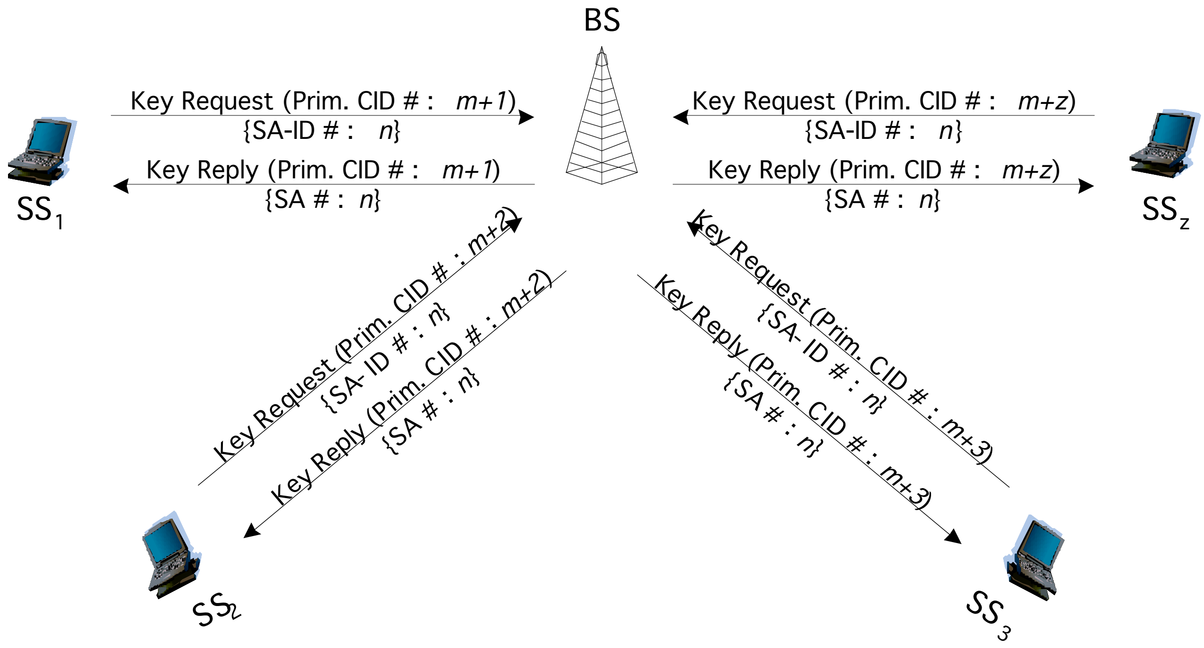

Figure 4 TEK updating and distribution procedure (primary management connection)

All SSs (SS_1 ~ SS_z) and the BS share the same n^{th} SA, because the BS provides a specific multicast service. All SSs try to send the Key Request message for the new and same TEK simultaneously, especially at the TEK Grace Time for the specific multicast service. Besides, the BS tries to send the Key Reply messages to the requested SSs at a time.

If the key management for the multicast service follows the above procedure, the key management encounters some problems.
First, all SSs served with the specific multicast service attempt to get bandwidth to send the Key Request message by using the CDMA code. Since so many SSs try to request bandwidth simultaneously, some CDMA codes can be collided with each other. Some SSs cannot send the Key Request message and get the new TEK, because of the constant bandwidth request failure. So, some SSs may not be served the multicast service any more.
Second, unnecessary signaling resources are used to refresh TEK that shall be the same between the BS and multiple SSs (SS_1 ~ SS_z). In order to share the new TEK with z SSs, the individual total size of the MAC PDU containing the Key Request and the Key Reply message on wireless channel is shown as the <table 1>.

Table 1 MAC PDU total size (primary management connection)

Message	Size (bytes)	Total size (bytes)
Key Request	36 * z	114 * z
Key Reply	78 * z	

Note: The number of SSs is the *Z*.

Third, it needs several frames for the BS to receive the Key Request messages from all SSs and send the Key Reply messages to them. For example, we assume a system as shown in the <table 2>.

Table 2 System parameters

	Value
System	OFDMA
Bandwidth	10 MHz
Frame size	5 msec
DL : UL	15 : 9
Modulation	QPSK
Code rate	1/2
The number of SSs	100

If 100 SSs are currently served with the specific multicast service, then the total size of the MAC PDU used to send the Key Request message and the Key Reply message on the primary management connection is individually 3600 bytes and 7800 bytes. And, the MAC PDU for the UL-MAP message needs 6500 bytes totally. So, it should use about 19 symbols for the Key Request messages, about 34 symbols for the UL-MAP messages, and about 41 symbols for the Key Reply messages. It may need more than two frames, in order for the BS to send the UL-MAP messages and for all SSs to send the Key Request messages without any other traffic data transmission. And, it may need more than two frames, in order for the BS to send the Key Reply messages without any other traffic data transmission. Therefore, at least six frames should be assigned to all served 100 SSs for the safe TEK refreshment, especially under no other traffic data transmission. It is very inefficient not to transmit any traffic data for at least six frames so that all SSs may refresh the new TEK.

Table 3 Used values for the TEK refreshment

Message	Total size of the MAP PDU (bytes)	Total symbols (symbols)	Total frame (frames)
Key Request message	3600	≈ 19	≈ 2.1
UL-MAP message	6500	≈ 34	≈ 2.3
Key Reply message	7800	≈ 41	≈ 2.7

Fourth, the BS should instantaneously waste excessive processing capacity, because the BS shall receive so many Key Request messages at the TEK Grace Time simultaneously. In addition, the BS has to refresh and distribute new TEK to individual SSs through the primary management connection for a moment.

The existing TEK updating and distribution procedure to carry the Key Request message and the Key Reply message on the dedicate channel, the primary management connection, is inefficient by above mentioned problems.

2). Carried on the broadcast connection (Proposed method)

Therefore, an alternative key method is proposed to solve those mentioned problems.

The proposed structure of the TEK management for the multicast service is shown as the <Figure 5>.

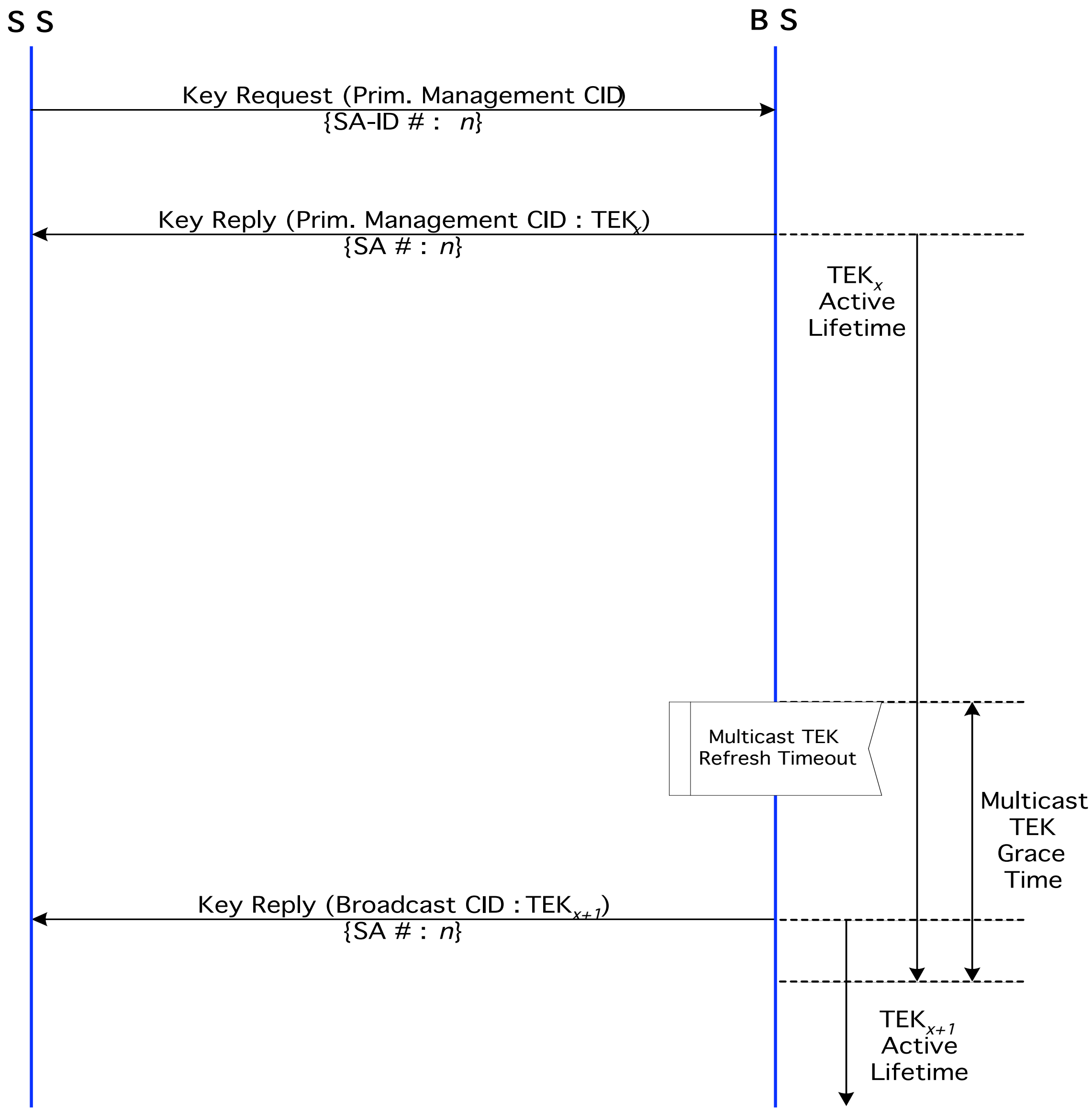

Figure 5 Proposed TEK distribution procedure

An SS tries to get the TEK before an SS is served with the specific multicast service. The first TEK distribution procedure is equal to that of the <figure 1>. Both the SS and the BS share the new TEK_x in the n^{th} SA by using the Key Request and Key Reply messages that are carried on the primary management connection.

The BS manages the Multicast TEK Grace Time for the respective SA-ID in itself. This Multicast TEK Grace Time is defined only for the multicast service in the BS. This parameter means time interval (in seconds) before the estimated expiration of an old distributed TEK. Since the Multicast TEK Grace Time is longer than the TEK Grace Time in an SS, the BS starts rekeying for a new TEK earlier than an SS does.

The BS shall periodically begin to refresh TEK for the multicast service at the Multicast TEK Grace Time. The BS shall send only one Key Reply message, containing updated TEK_{x+1} in the n^{th} SA, to all SSs being served with the relevant multicast service through not the primary management connection but the broadcast connection.

The proposed TEK updating and distribution procedure between multiple SSs and the BS is shown as the <figure 6>.

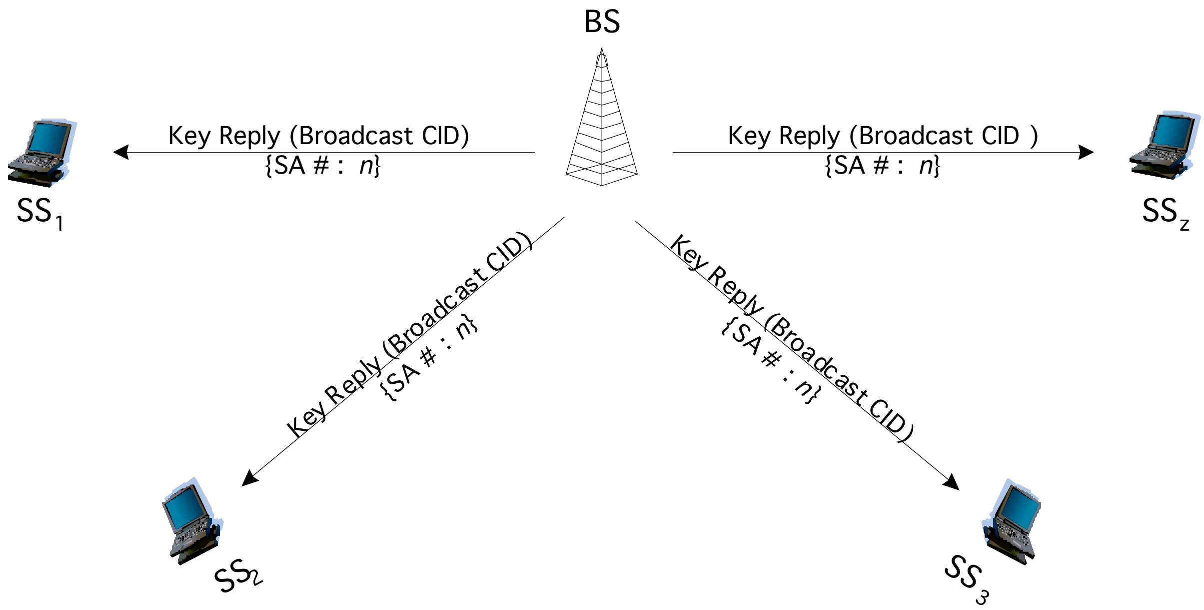

Figure 6 TEK updating and distribution procedure (broadcast connection)

The BS can distribute the new TEK to all served SSs with the specific multicast service by sending the Key Reply message on the broadcast connection. The Key Request messages sent from all SSs are not needed in this scheme. In addition, the new TEK can be sent by only one Key Reply message to all SSs.

As compared with the existing key refreshment scheme, there is no need that all served SSs try to request bandwidth to send the Key Request message. And, since the Key Reply message is carried on the broadcast connection, the MAC PDU size of that message to distribute the new TEK is only 78 bytes. In other words, it is enough to transmit the Key Reply message within one frame. Moreover, these results are independent of the number of SSs. The result of proposed TEK refreshment scheme is shown as the <figure 4>. Accordingly, the BS doesn't need to have excessive processing capacity and only a few resources are needed to distribute the new TEK in the proposed key method.

Table 4 Used values for the proposed TEK refreshment

Message	Total size of the MAP PDU (bytes)	Total frame (frames)
Key Reply message	78	_ 1

In the sent Key Reply message, the newly updated TEK should be encrypted, because the new TEK itself is safely provided to SSs. The TEK shall be encrypted using two-key triple DES in the encrypt-decrypt-encrypt mode. Two input keys in the 3-DES are the KEK, when the Key Reply message is carried on the primary management connection. However, two input keys are two old distributed TEKs, when the Key Reply message is carried on the broadcast connection. The common input keys should be used to encrypt the new TEK, because a new identical TEK is transmitted to all served SSs (SS_1 ~ SS_z) carried on the broadcast connection. In addition, these common input keys should be known to only served SSs with the specific multicast service, because the new encrypted TEKs are transmitted to the authorized SSs as well as the unauthorized SSs for that service. Owing to satisfaction of these requirements, old distributed TEKs for the multicast service is proper as the input keys of the 3-DES. The used input key according to connection transmitted the Key Reply message is described as shown the <table 5>.

Table 5 Used input key according to transport connection

Connection	Input key of the triple DES
Primary management connection	KEK
Broadcast connection	Old distributed TEK

Proposed changes to IEEE 802.16-REVd/D3-2004

6.2.2.3 MAC Management Messages
[Change to Table 14]

Table 14 - MAC Management Messages

Type	Message name	Message description	Connection
10	PKM-RSP	Privacy Key Management Response	Primary Management, Basic

NOTE: The Key Reply PKM message of the PKM-RSP message can be carried on the Basic connection only for the multicast service.

7.1.4 Mapping of connections to SAs
[Change the second particulars]

2) Multicast Transport Connections may be mapped to Static or Dynamic SA. However, each of Multicast Transport Connections should be mapped to only one SA.

7.2.5 TEK state machine
[Change the Figure 127]

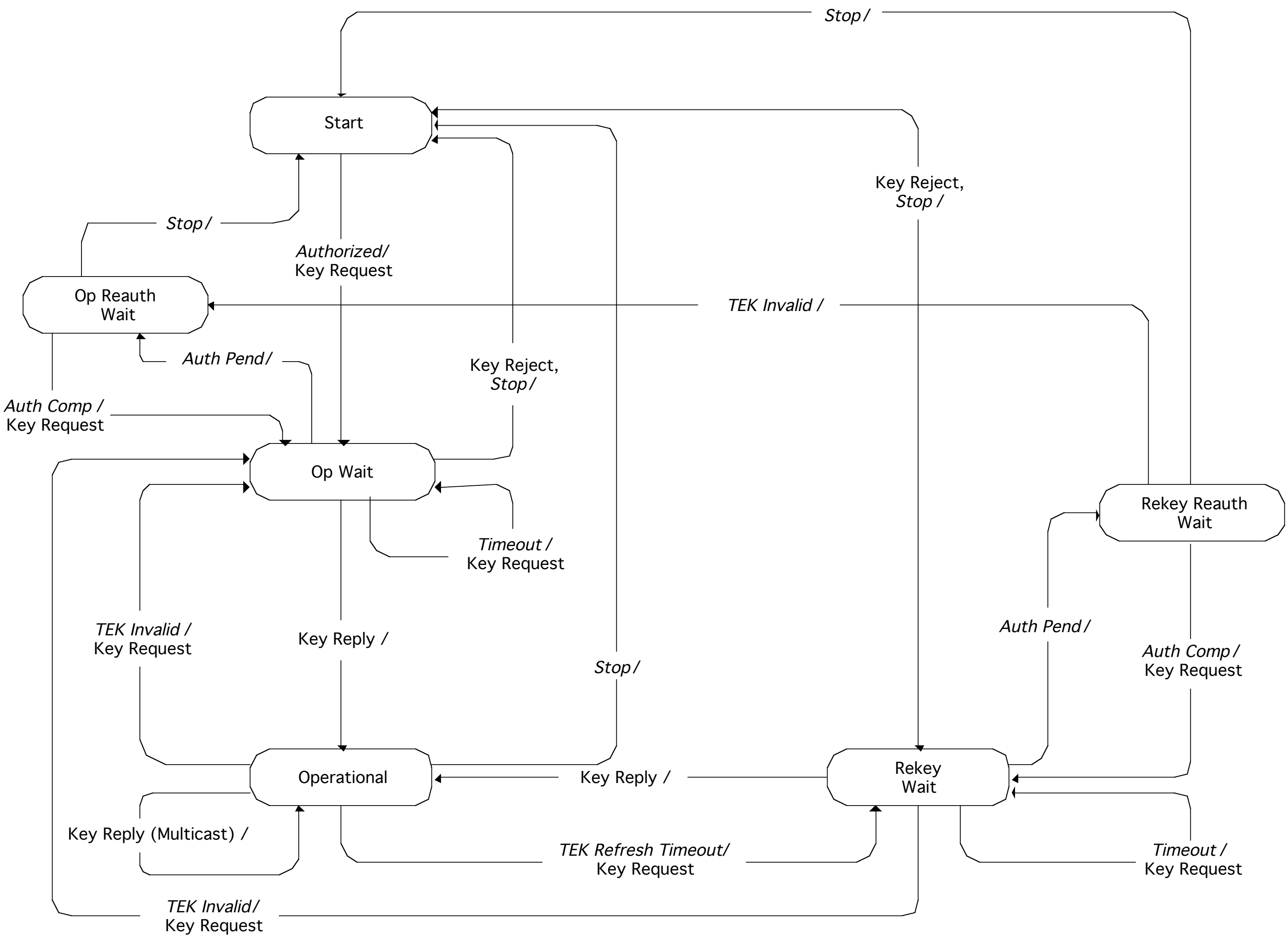

Figure 127 - TEK state machine flow diagram

[Change the Table 111]

Table 111 - TEK FSM state transition matrix

State Event or Rcvd Message	**(A) Start**	**(B) Op Wait**	**(C) Op Reauth Wait**	**(D) Op**	**(E) Rekey Wait**	**(F) Rekey Reauth Wait**
(1) Stop		Start	Start	Start	Start	Start
(2) Authorized	Op Wait					

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait
(3) Auth Pend		Op Reauth Wait			Rekey Reauth Wait	
(4) Auth Comp			Op Wait			Rekey Wait
(5) TEK Invalid				Op Wait	Op Wait	Op Reauth Wait
(6) Timeout		Op Wait			Rekey Wait	
(7) TEK Refresh Timeout				Rekey Wait		
(8) Key Reply		Operational		Operational	Operational	
(9) Key Reject		Start			Start	

NOTE: The state, Operational (D), can be transited to the “Operational” state by receiving the Key Reply message for the multicast transport service such as “8-D”.

7.2.5.3 Events
[Insert at the end of this section]

Multicast TEK Refresh Timeout: This event is defined only for the multicast service in BS. The TEK refresh timer for the multicast service timed out. This timer event signals the MAC in BS to refresh new keying material. The refresh timer is set to fire a configurable duration of time (*Multicast TEK Grace Time*) before the expiration of the TEK the BS currently holds.

7.2.5.4 Parameters
[Insert at the end of this section]

Multicast TEK Grace Time: This parameter is defined only for the multicast service in BS. The Multicast TEK Grace Time is time interval (in seconds) before the estimated expiration of a TEK that the BS starts rekeying for a new TEK. This parameter is vendor-specific and is the same across all SAIDs related to the multicast service.

7.2.5.5 Actions
[Insert between “8-B” and “8-E”]

8-D Operational (Key Reply: Multicast) → Operational
a) process contents of Key Reply message and incorporate new keying material into key database
b) set the TEK refresh timer to go off “TEK Grace Time” seconds prior to the key’s scheduled expiration

7.5.2 Encryption of TEK with 3-DES
[Insert after the second paragraph]

The Key Reply message is generally carried on the primary management connection. When the BS periodically begins to refresh keying and distributes this TEK only for the multicast service, the Key Reply message is carried on the basic connection. The method of encrypting the TEK is differently used by the connection carrying the Key Reply message.

Encryption: C = Ek1[Dk2[Ek1[P]]]
Decryption: P = Dk1[Ek2[Dk1[C]]]
P = Plaintext 64-bit TEK
C = Ciphertext 64-bit TEK
k1 = left-most 64 bits of the 128-bit KEK (primary management connection)

= an old distributed TEK (basic connection)
k2 = right-most 64 bits of the 128-bit KEK (primary management connection)
= an old distributed TEK (basic connection)
E[] = 56-big DES ECB (electronic code block) mode encryption
P[] = 56-bit DES ECB decryption

10.2 PKM parameter values
[Change to Table 270]

Table 270 – Operational ranges for privacy configuration settings

System	Name	Description	Minimum value	Default value	Maximum value
BS	Multicast TEK Grace Time	Time prior to TEK (for the multicast service) expiration BS begins rekeying. This time is bigger than the TEK Grace Time.	Vendor-specific value	Vendor-specific value	Vendor-specific value