A Key Management for the Multicast Service

WLAN

IEEE S802.16e-04/23r2

2004. 03

Seokheon Cho

Chosh@etri.re.kr

한국전자통신연구원

Contents

¢√ **Introduction**

¢√ **Relationship between the multicast service and the SA**

- ¢¬ Mapping a multicast connection to different SAs
- ¢¬ Mapping a multicast connection to the same SA

¢√ **Key Refreshment and Distribution for the Multicast service**

- ¢¬ Carried on the primary management connection
- ¢¬ Carried on the broadcast connection

¢√ **Conclusions**

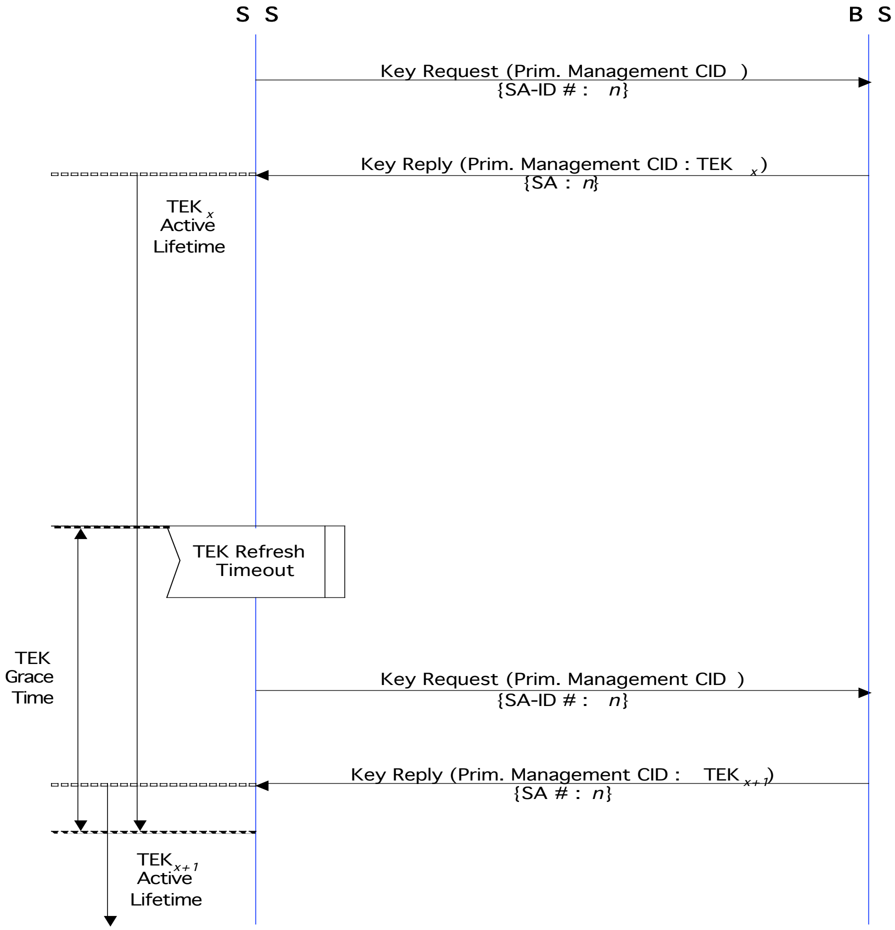
Introduction (I)

¢√ **Current structure of the TEK management for the multicast service**

- ¢¬ Purpose : To provide a downlink multicast service safely
- ¢¬ MAC message : PKM-REQ / PKM-RSP
  - □ Key Request
  - □ Key Reply / Key Reject
- ¢¬ Characteristics
  - □ An SS begins to refresh keying at the TEK Grace Time
  - □ The messages are carried on the dedicated channel, especially the primary management connection

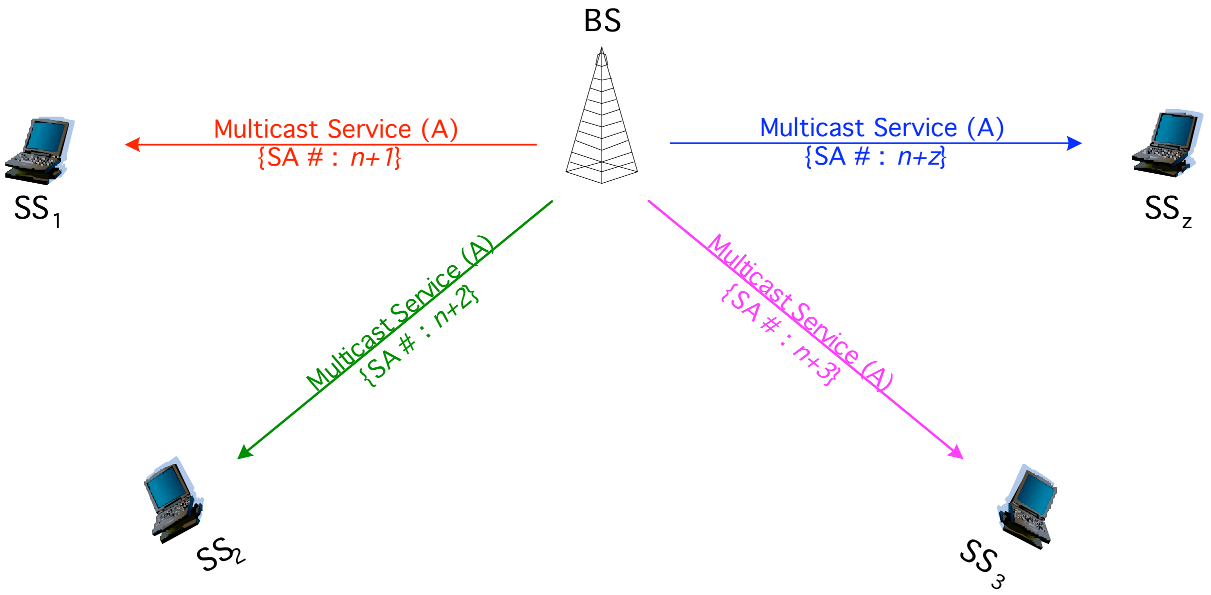
Introduction (II)

¢√ Current structure of the TEK management for the multicast service


SS
BS
Key Request (Prim. Management CID)
{SA-ID # : n}
Key Reply (Prim. Management CID : TEK x)
{SA : n}
TEK x
Active
Lifetime
TEK Refresh
Timeout
TEK
Grace
Time
Key Request (Prim. Management CID)
{SA-ID # : n}
Key Reply (Prim. Management CID : TEK x+1)
{SA # : n}
TEK x+1
Active
Lifetime

Relationship between the multicast service and the SA (I)

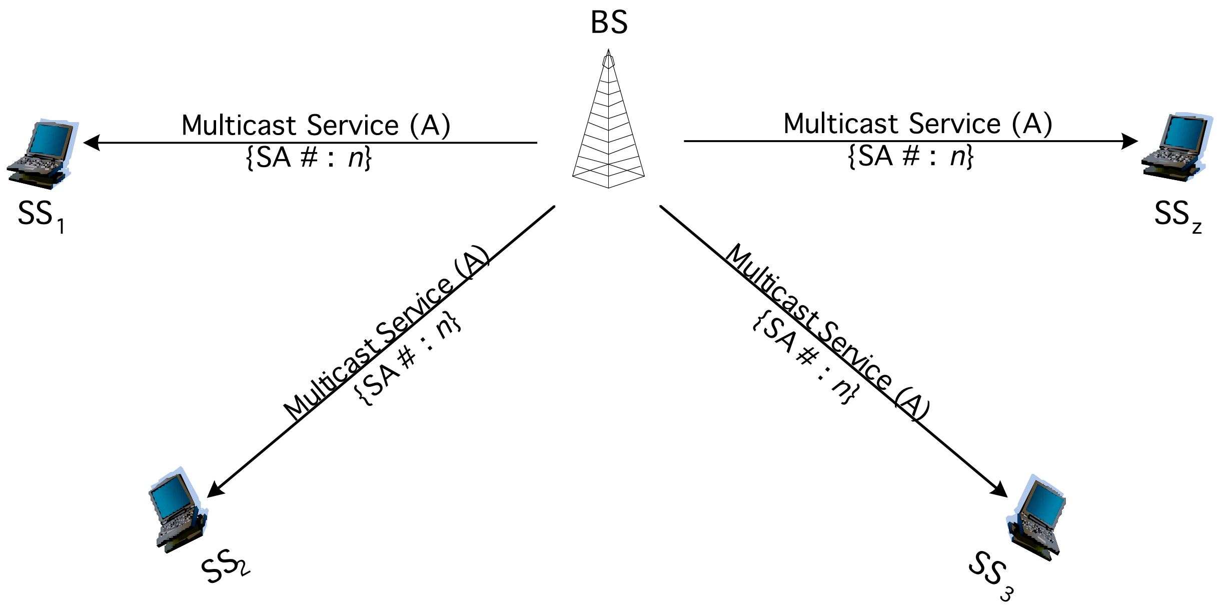
¢√ **Mapping a multicast connection to different SAs**



¢¬ Problems : The BS should encrypt the multicast traffic data with different SA, especially different TEK. Therefore, the BS is heavily burdened.

Relationship between the multicast service an d the SA (II)

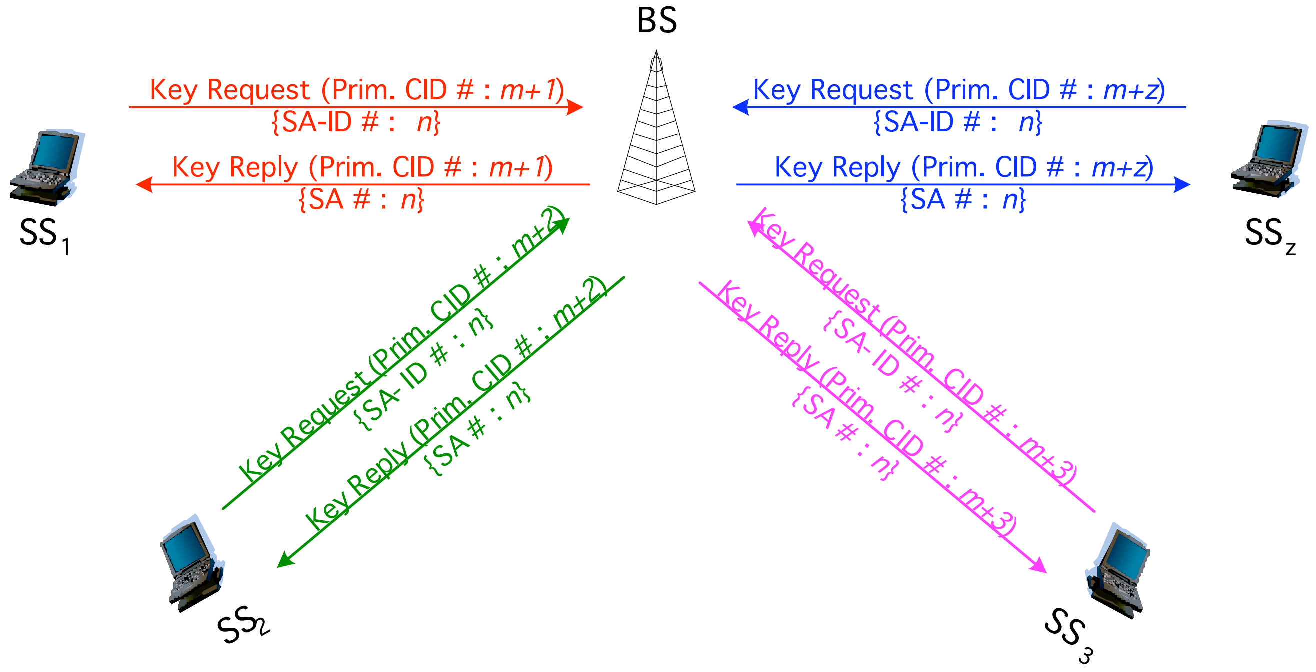
¢√ Mapping a multicast connection to the same SA



¢¬ Advantage : The BS can mitigate the processing burden for e ncrypting multicast traffic data by using the equal SA.

Key Refreshment and Distribution (I)

¢√ **Carried on the primary management connection**



BS

Key Request (Prim. CID # : *m+1*)
{SA-ID # : *n*}

Key Reply (Prim. CID # : *m+1*)
{SA # : *n*}

SS_1

Key Request (Prim. CID # : *m+z*)
{SA-ID # : *n*}

Key Reply (Prim. CID # : *m+z*)
{SA # : *n*}

SS_z

Key Request (Prim. CID # : *m+2*)
{SA- ID # : *n*}

Key Reply (Prim. CID # : *m+2*)
{SA # : *n*}

SS_2

Key Request (Prim. CID # : *m+3*)
{SA- ID # : *n*}

Key Reply (Prim. CID # : *m+3*)
{SA # : *n*}

SS_3

¢¬ Messages : Key Request and Key Reply

¢¬ Timer : TEK Grace Time (SS)

¢¬ Connection : Primary management connection

Key Refreshment and Distribution (II)

¢√ **Carried on the primary management connection**

¢¬ Problems

 Assumed system parameters

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

Key Refreshment and Distribution (III)

¢√ **Carried on the primary management connection**

¢¬ Problems

1. When all served SSs try to request bandwidth for the Key Request message, some of used CDMA codes may be collided.
2. Unnecessary signaling resources are used.
3. It needs several frames to refresh new TEK in spite of no other traffic data transmission.
4. The BS should instantaneously have excessive processing capacity.

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

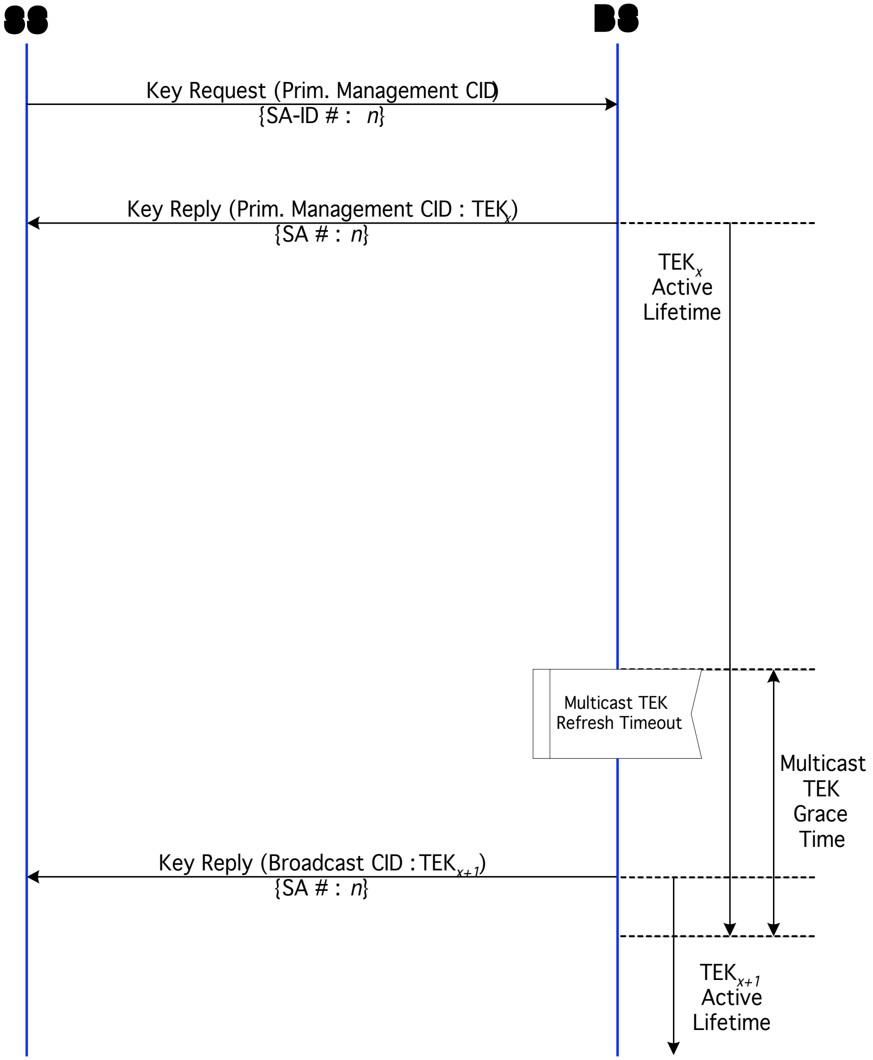
Key Refreshment and Distribution (IV)

¢√ **Carried on the broadcast connection**

- ¢¬ The first TEK distribution procedure is equal to the existing TEK distribution procedure using the primary management connection
- ¢¬ The next TEK refreshment and distribution procedure is fulfilled by using not the primary management connection but the broadcast connection.
- ¢¬ Multicast TEK Grace Time : Time interval before the estimated expiration of an old distributed TEK. Since this is longer than the TEK Grace Time in an SS, the BS starts rekeying for a new TEK earlier than an SS does

Key Refreshment and Distribution (V)

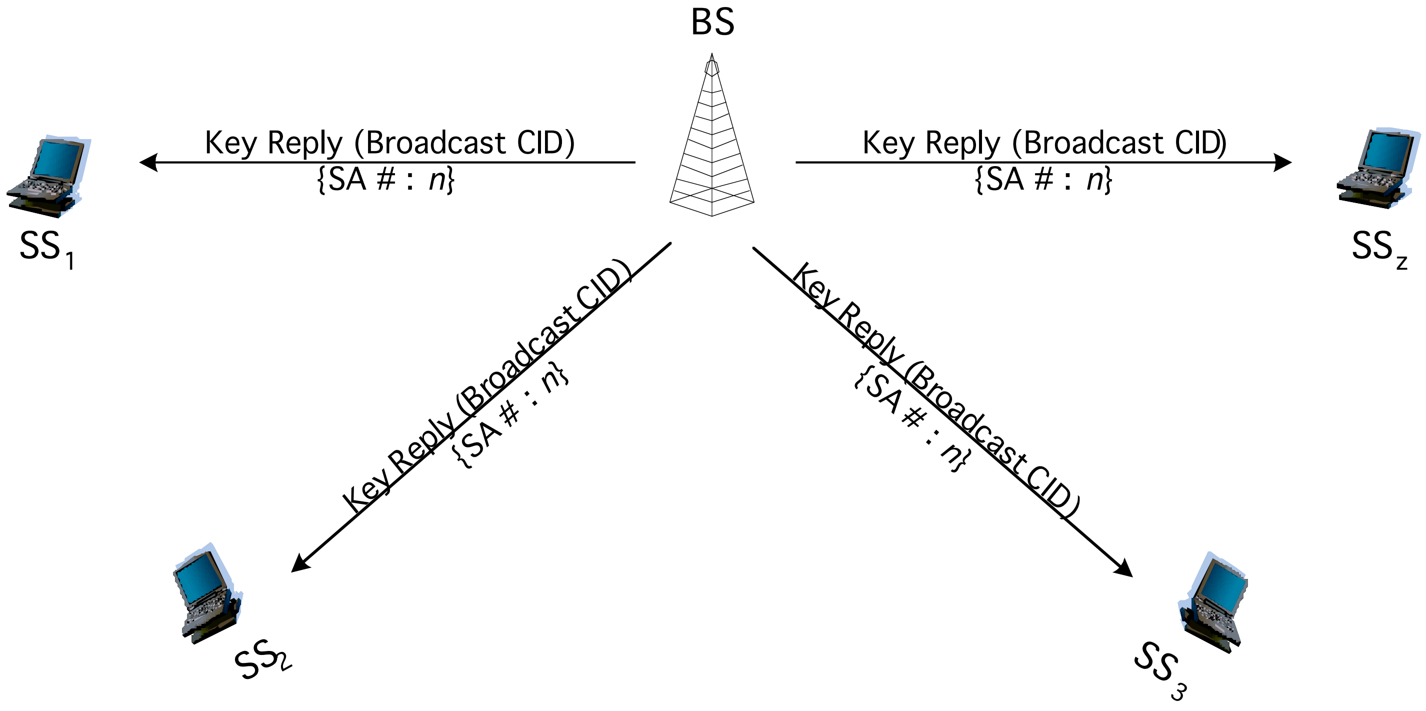
- ¢√ **Carried on the broadcast connection**
  - ¢¬ Proposed key procedure


SS
BS
Key Request (Prim. Management CID)
{SA-ID # : n}
Key Reply (Prim. Management CID : TEK_x)
{SA # : n}
TEK_x Active Lifetime
Multicast TEK Refresh Timeout
Multicast TEK Grace Time
Key Reply (Broadcast CID : TEK_{x+1})
{SA # : n}
TEK_{x+1} Active Lifetime

Key Refreshment and Distribution (VI)

¢√ **Carried on the broadcast connection**

- ¢¬ Proposed key procedure


BS
Key Reply (Broadcast CID)
{SA # : *n*}
Key Reply (Broadcast CID)
{SA # : *n*}
Key Reply (Broadcast CID)
{SA # : *n*}
Key Reply (Broadcast CID)
{SA # : *n*}
SS1
SSz
SS2
SS3

Key Refreshment and Distribution (VII)

¢√ **Carried on the broadcast connection**

- ¢¬ Advantages
  - There is no need that all SSs try to request bandwidth (No Key Request message)
  - The total size used for key refreshment is only 78 bytes. (Independent of the number of users)
  - The key refreshment procedure is executed within only one frame.
  - The BS doesn’t need to have excessive processing capacity to execute the key management procedure.

Message	**Total size of the MAP PDU (bytes)**	**Total frame (frames)**
Key Reply message	78	°Ï1

Key Refreshment and Distribution (VIII)

- ¢√ **Carried on the broadcast connection**
  - ¢¬ Encryption of TEK
    - Primary management connection : KEK
    - Broadcast connection : Old distributed TEK

Conclusion

1. **Mapping a multicast transport connection to only one SA**
2. **Carried on the broadcast connection**
   ¢¬ Multicast TEK Grace Time in the BS
   ¢¬ Not use the Key Request message
   ¢¬ Send the Key Reply message on the broadcast connection
3. **Encryption of TEK**
   ¢¬ Primary management connection : KEK
   ¢¬ Broadcast connection : Old distributed TEK