Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Modified TEK State Machine for the MBRA (Multicast & Broadcast Rekeying Algorithm)**
Data Submitted	**2004-11-15**
Source(s)	Seokheon Cho Sungcheol Chang Chulsik Yoon, ETRI 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr
Re:	IEEE 802.16 Security Ad Hoc
Abstract	The modified TEK state diagram and TEK state transition for the efficient rekeying method for the multicast service and the broadcast service
Purpose	The document is submitted for review by 802.16 Working Group members
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) 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 and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard. "Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chiar@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Modified TEK State Machine for the MBRA

Seokheon Cho, Sungcheol Chang, and Chulsik Yoon
ETRI

Introduction

The MBRA (Multicast & Broadcast Rekeying Algorithm) is defined in the IEEE P802.16e/D5.

The TEK State Machine is needed to be modified for the multicast service or the broadcast service.

In this contribution, we suggest the modified TEK state machine so that the MBRA is fully operated for the multicast service and broadcast service.

Proposed changes

[Change section 7.2.5 as described below:]
7.2.5 MAC Management messages

The TEK state machine consists of ~~six~~ seven states and ~~nine~~ eleven events (including receipt of messages) that can trigger state transitions. Like the Authorization state machine, the TEK state machine is presented in both a state flow diagram (Figure 132a) and a state transition matrix (Table 132a). As was the case for the Authorization state machine, the state transition matrix shall be used as the definitive specification of protocol actions associated with each state transition.

Shaded states in Figure 132 (Operational, Rekey Wait, ~~and Rekey Reauthorize Wait~~ Rekey Reauthorize Wait, and M&B Rekey Interim Wait) have valid keying material and encrypted traffic can be passed.

The SAID can be replaced by the GSAID for the multicast service or the broadcast service. And, the TEK can be also replaced by the GTEK for the multicast service or the broadcast service.

The Authorization state machine starts an independent TEK state machine for each of its authorized SAIDs. As mentioned in 7.2.2, the BS maintains two active TEKs per SAID. ~~The BS includes in its Key Replies both of these TEKs, along with their remaining lifetimes. The BS encrypts downlink traffic with the older of its two TEKs and decrypts uplink traffic with either the older or newer TEK, depending upon which of the two keys the SS was using at the time. The SS encrypts uplink traffic with the newer of its two TEKs and decrypts downlink traffic with either the older or newer TEK, depending upon which of the two keys the BS was using at the time. See 7.4 for details on SS and BS key usage requirements.~~

For the unicast service, the BS includes in its Key Replies both of these TEKs, along with their remaining lifetimes. The BS encrypts downlink traffic with the older of its two TEKs and decrypts uplink traffic with either the older or newer TEK, depending upon which of the two keys the SS was using at the time. The SS encrypts uplink traffic with the newer of its two TEKs and decrypts downlink traffic with either the older or newer TEK, depending upon which of the two keys the BS was using at the time. See 7.4 for details on SS and BS key usage requirements.

For the multicast service or the broadcast service, the BS may include both of GTEKs in its Key Reply messages, when an SS request traffic keying material. And, the BS may include the newer GTEK in the Key Update Command message, when the BS transmits the new traffic keying material in key push mode. The BS encrypts downlink traffic with current GTEK. The SS decrypts downlink traffic with either the older or newer GTEK, depending upon which of the two keys the BS is using at the time. See 7.9 for details on SS and BS key usage requirements.

Through operation of a TEK state machine, the SS attempts to keep its copies of an SAID's TEKs synchronized with those of its BS. A TEK state machine issues Key Requests to refresh copies of its SAID's keying material soon after the scheduled expiration time of the older of its two TEKs and before the expiration of its newer TEK. To accommodate for SS/BS clock skew and other system processing and transmission delays, the SS schedules its Key Requests a configurable number of seconds before the newer TEK's estimated expiration in the BS. With the receipt of the Key Reply, the SS shall always update its records with the TEK Parameters from both TEKs contained in the Key Reply message. ~~Figure 132 illustrates the SS's scheduling of its key refreshes in conjunction with its management of an SA's active TEKs.~~ With the receipt of the two Key Update Command messages, the SS shall always update its records with the TEK Parameters contained in the two Key Update Command messages for the multicast service or the broadcast service.

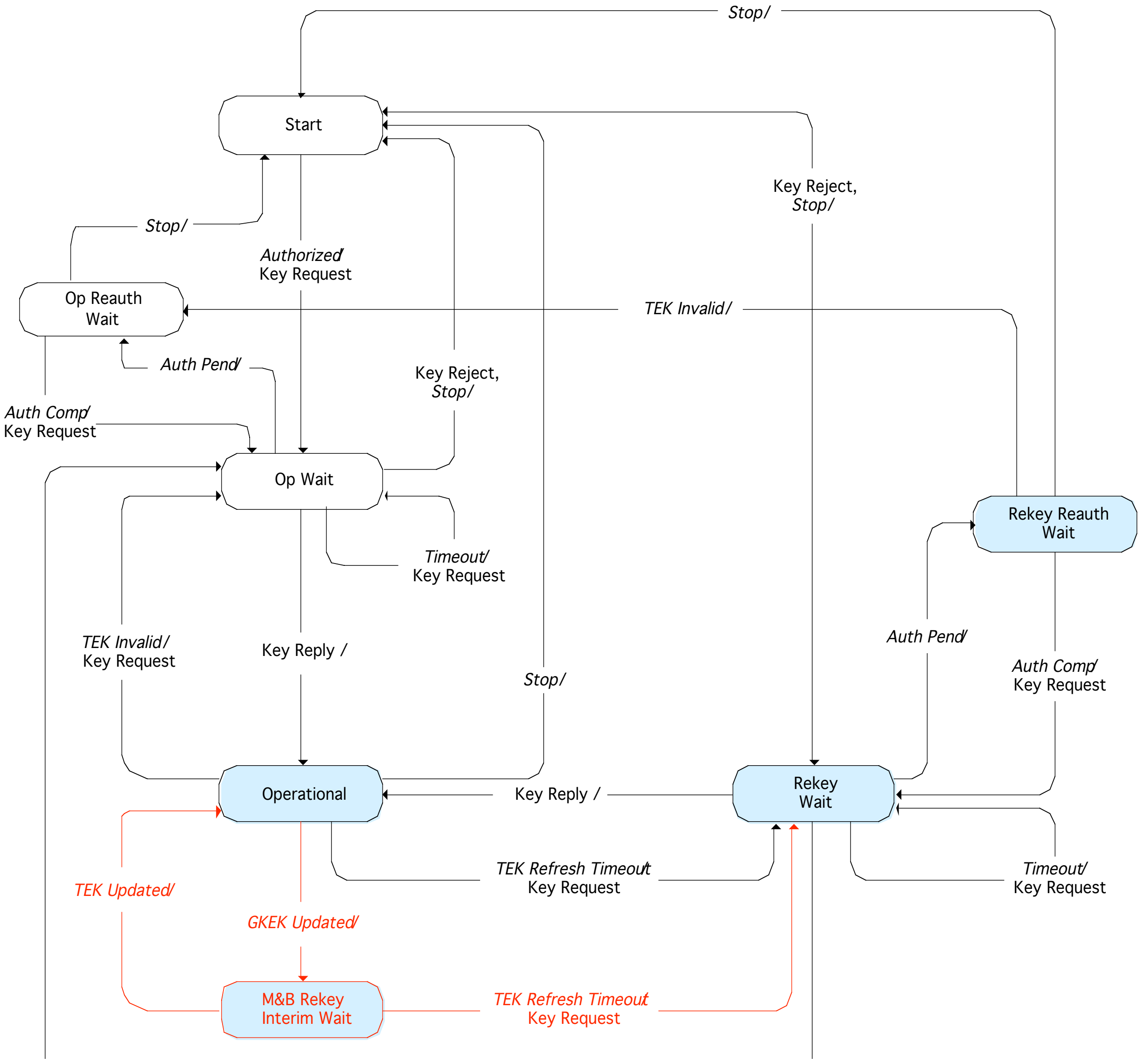

Figure 132a-TEK state machine flow diagram

Table 132a-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**	**(G) M&B Rekey Interim Wait**
(1) Stop		Start	Start	Start	Start	Start	
(2) Authorized	Op Wait						
(3) Auth Pend		Op Reauth Wait			Rekey Reauth Wait		
(4) Auth Comp			Op Wait			Rekey Wait	
(5)				Op Wait	Op Wait	Op Reauth	

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait	(G) M&B Rekey Interim Wait
TEK Invalid						Wait	
(6) Timeout		Op Wait			Rekey Wait		
(7) TEK Refresh Timeout				Rekey Wait			Rekey wait
(8) Key Reply		Operational			Operational		
(9) Key Reject		Start			Start		
(10) GKEK Updated				M&B Rekey Interim Wait			
(11) GTEK Updated							Operational

7.2.5.1 States

[Add the following the end of section 7.2.5.1:]

M&B Rekey Interim Wait (Multicast & Broadcast Rekey Interim Wait): This state is defined only for the multicast service or the broadcast service. This state is the wait state the TEK state machine is placed in if the TEK state machine has valid traffic keying material and receives the new GKEK from the BS.

7.2.5.2 Messages

[Change section 7.2.5.1 as described below:]

Note that the message formats are defined in detail in 6.3.2.3.9.

Key Request: Request a TEK for this SAID. Sent by the SS to the BS and authenticated with keyed message digest. The message authentication key is derived from the AK.

Key Reply: Response from the BS carrying the two active sets of traffic keying material for this SAID. Sent by the BS to the SS, it includes the SAID's TEKs, encrypted with a KEK derived from the AK or the GSAID's GTEK, encrypted with a GKEK randomly generated from the BS or the ASA server. The Key Reply message is authenticated with a keyed message digest; the authentication key is derived from the AK.

Key Reject: Response from the BS to the SS to indicate this SAID is no longer valid and no key will be sent. The Key Reject message is authenticated with a keyed message digest; the authentication key is derived from the AK.

TEK Invalid: The BS sends an SS this message if it determines that the SS encrypted an uplink PDU with an invalid TEK, i.e., an SAID's TEK key sequence number, contained within the received PDU's MAC Header, is out of the BS's range of known, valid sequence numbers for that SAID.

Key Update Command: Push a GTEK for this GSAID for the multicast service or the broadcast service. Sent by the BS to the SS and authenticate with keyed message digest. The message authentication key is derived from the AK in the Key Update Command message for the GKEK update mode. The message authentication key is derived from the GKEK in the Key Update Command message for the GTEK update mode.

7.2.5.3 Events

[Add the following the end of section 7.2.5.3:]

GKEK Updated: This event is triggered when the SS receives the new GKEK through the Key Update Command message for the GKEK update mode.
GTEK Updated: This event is triggered when the SS receives the new GTEK and traffic keying material through the Key Update Command message for the GTEK update mode.

7.2.5.4 Parameters

[Add the following the end of section 7.2.5.4:]

M&B TEK Grace Time (Multicast & Broadcast TEK Grace Time): Time interval, in seconds, before the estimated expiration of an old distributed GTEK.

7.2.5.5 Actions

[Add the following the end of section 7.2.5.5:]

7-G M&B Rekey Interim Wait (*TEK Refresh Timeout*) -> Rekey Wait

a) send Key Request message to BS
b) set Key Request retry timer to Rekey Wait Timeout

10-D Operational (*GKEK Updated*) -> M&B Rekey Interim Wait

a) process contents of Key Update Command message for the GKEK update mode and incorporate new GKEK into key database

11-G M&B Rekey Interim Wait (*GTEK Updated*) -> Operational

a) clear Key Request retry timer
b) process contents of Key Update Command message for the GTEK update mode and incorporate new traffic keying material into key database
c) set the TEK refresh timer to go off “TEK Grace Time” seconds prior to the key’s scheduled expiration