Management Message Integrity Check for Multi-hop Relay System

IEEE 802.16 Presentation Submission Template (Rev. 8.3)

Document Number:

IEEE C802.16j-07/069

Date Submitted: 2007-01-08

Source:

Kanchei (Ken) Loa, Frank C.D. Tsai, Yi-Hsueh Tsai, Shiann-Tsong Sheu, Hua-Chiang Yin, Yung-Ting Lee, Chih-Chiang Hsieh, Heng-Iang Hsu, Youn-Tai Lee

Voice: 886-2-2739-9616
Fax: 886-2-2378-2328
E-mail: loa@iii.org.tw

Institute for Information Industry
8F., No. 218, Sec. 2, Dunhua S. Rd.,
Taipei City, Taiwan.

[add co-authors here]

Venue:

IEEE 802.16 Session #47, London, UK

Base Document:

None

Purpose:

Propose the text regarding Management Message Integrity Check for Multi-hop Relay System.

Brief

- This presentation briefly describes the existing integrity check mechanism for 802.16e management messages
- This presentation is informational for Relay designers when designing 802.16j Relay protocols
- Backward compatibility for MS shall be maintained per 802.16j PAR

MAC (Message Authentication Code)

- MAC is applied to a management message for ensuring the integrity of the message
- In 802.16d, MAC is achieved through *HMAC*
- In 802.16e, an additional option *CMAC* is added
- In 802.16e, application of HMAC or CMAC is determined during Basic Capability Negotiation phase of Network Entry Procedure, where MS (note: before PKM phase) via SBS-REQ and SBC-RSP (p. 712 of Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands And Corrigendum 1)
- SBC-RSP indicate BS's decision

Application of MAC

- In TLV, if no such attribute, then HMAC is supported
- If SBC-RSP set ALL bits 0, then no message authentication code is applied.
  - Both the MS and the BS does NOT need to authenticate the MAC (Medium Access Control) messages.

Type	Length	Value
25.3	1	Bit# 0: HMAC Bit# 1: CMAC Bit# 2: 64-bit short-HMAC* Bit# 3: 80-bit short-HMAC* Bit# 4: 96-bit short-HMAC* Bit# 5-7: Reserved. Set to 0

- If the short-HMAC mode is selected, then it is used for
  - MOB_SLP-REQ/RSP, MOB_SCN-REQ/RSP, MOB_MSHO-REQ, MOB_BSHO-REQ/RSP, MOB_HO-IND, RNG-REQ/RSP.
  - Otherwise, the HMAC Tuple shall be applied.

HAMC and CMAC

- Both derived from AK – if PKM is disabled, no HMAC or CMAC is needed
- HMAC (IETF RFC 2104)
  - IETF **RFC 2104**, "HMAC: Keyed-Hashing for Message Authentication," H. Krawczyk, M. Bellare, R.Canetti, February 1997.
  - HMAC (*key*, *message*) ➔ *digest*
    - key → 20 bytes
    - message → variable
    - digest → 20 bytes
- CMAC (draft SP 800-38B)
  - NIST **Special Publication 800-38B** — Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication.
  - the CMAC-Digest attribute and the CMAC Tuple shall use the CMAC Algorithm with **AES**.
  - CMAC (*key*, *message*) ➔ *digest*
    - key → 16 bytes
    - message → variable
    - digest → 16 bytes
- Both HMAC and CMAC applied only to the message, excluding the MPDU's GMH (Generic MAC Header) and CRC (Cyclic Redundancy Checking)
  - *However, note that the generation of CMAC includes also CID*

Message Authentication Code (HMAC)

HMAC value ⇐ HMAC (HMAC_KEY_*, ***MAC_Management_Message***))

Type	Length	Value (string)
11	20 bytes	A 160-bit (20 byte) keyed SHA hash

Table 348—HMAC Tuple value field

Field	Length	Notes
reserved	4 bits	
HMAC Key Sequence Number	4 bits	
HMAC-Digest	160 bits	HMAC with SHA-1

Message Authentication Code (Short-HMAC)

Short-HMAC value ⇐

Truncate64(HMAC (HMAC_KEY_*, ***MAC_Management_Message***))

Truncate80(HMAC (HMAC_KEY_*, ***MAC_Management_Message***))

Truncate96(HMAC (HMAC_KEY_*, ***MAC_Management_Message***))

Type	Length	Value (uint16)
11	variable(8, 10, or 12 bytes as described in 11.1.2.3)	The highest order bytes of the truncated HMAC-SHA1 keyed hash

Table 348d—Short-HMAC Tuple definition

Field	Length (bits)	Note
Reserved	4	—
HMAC Key Sequence Number	4	—
HMAC Packet Number Counter HMAC_PN_*	32	Replay counter
Short-HMAC Digest	*variable*	0—Truncate HMAC to 8 bytes in Short HMAC Tuple 1—Truncate to 10 bytes 2—Truncate to 12 bytes

Message Authentication Code (CMAC)

CMAC value ⇐ Truncate64 (CMAC (CMAC_KEY_*, AKID | CMAC_PN | ***CID*** |16-bit zero padding | **MAC_Management_Message**))

Type	Length	Value
40	12	See that follows

Field	Length (bits)	Note
CMAC Packet Number counter, CMAC_PN_*	32	This context is different in UL, DL
CMAC value	64	CMAC with AES 128

Table 348b—CMAC Tuple definition

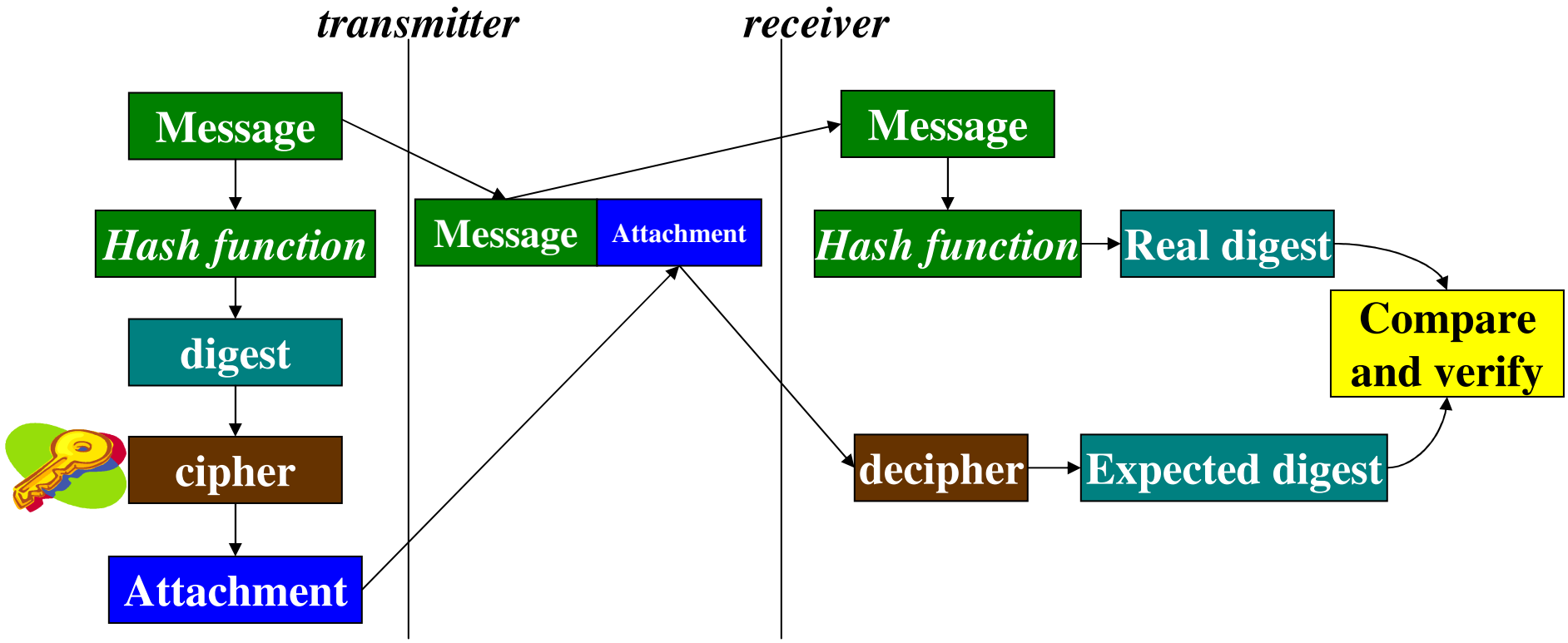
Field	Length (bits)	Note
Reserved	4	Set to 0
CMAC Key Sequence Number	4	CMAC key sequence number
BSID	48	Only used in case of MDHO zone—optional
CMAC Packet Number Counter, CMAC_PN_*	32	This context is different UL, DL
CMAC Value	64	CMAC with AES 128

Outline

- (Short-)HMAC
  - (Short-)HMAC Tuple definition
  - (Short-)HMAC Tuple value field
- CMAC
  - CMAC Tuple definition
  - CMAC Tuple value field
- Summary

MAC/HMAC

MAC	Message Authentication Codes
HMAC	cryptographically hashed MAC



HMAC

- This parameter contains the HMAC Key Sequence Number concatenated with an HMAC-Digest used formessage authentication.
- The HMAC Key Sequence Number is stored in the four least significant bits of the first byte of the HMAC Tuple, and the most significant four bits are reserved.
- The HMAC-Tuple attribute format is shown in the following tables.
- When PKM is disabled, the content of this field shall be ignored and the message considered authenticated.

(*Short-*)*HMAC Tuple definition*

Type	*Length*	*Value*	*Scope*
149	21 (*HMAC*)		DSx-REQ, DSx-RSP, DSx-ACK, REG-REQ, REG-RSP, RES-CMD, DREG-REQ, DREG-CMD, TFTP-CPLT, MOB_SLP-REQ, MOB_SLP-RSP, MOB_SCN-REQ, MOB_SCN-RSP, MOB_BSHO-REQ, MOB_MSHO-REQ, MOB_BSHO-RSP,MOB HO-IND, DREG-REQ
151	*variable* (*13*/*15*/*17*) (*Short-HMAC*)		MOB_SLP-REQ, MOB_SLP-RSP, MOB_SCN-REQ,MOB_SCN-RSP, MOB_MSHO-REQ, MOB_BSHO-RSP, MOB_HO-IND, RNG-REQ, RNG-RSP, PKM-REQ, PKM-RSP

(*Short-*)*HMAC Tuple value field*

Field (*HMAC*)	**Length**	**Notes**
reserved	4 bits	
HMAC Key Sequence Number	4 bits	
HMAC-Digest	160 bits	HMAC with SHA-1
Field (*Short-HMAC*)	**Length**	**Notes**
Reserved	4 bits	
HMAC Key Sequence Number	4 bits	
HMAC Packet Number Counter HMAC_PN_*	32 bits	Replay counter
Short-HMAC Digest	*variable*	0—Truncate HMAC to 8 bytes in Short HMAC Tuple 1—Truncate to 10 bytes 2—Truncate to 12 bytes

CMAC

- This parameter contains the CMAC key sequence number, the CMAC Packet Number Counter (CMAC_PN_*), and the CMAC value used for message authentication.
- The CMAC Tuple attribute format is shown in the following tables.
- A message received, that contains an CMAC Tuple, shall not be considered authentic if the length field of the tuple is incorrect, or if the locally computed value of the digest does not match the digest in the message.

CMAC Tuple definition

Type	*Length*	*Value*	*Scope*
150	13 or 19 (*CMAC*)		DSx-REQ, DSx-RSP, DSx-ACK, REG-REQ, REG-RSP, RES-CMD, DREG-CMD, TFTP-CPLT, PKM-REQ, PKM-RSP, MOB_SLP-REQ, MOB_SLP-RSP, MOB_SCN-REQ, MOB_SCN-RSP, MOB_BSHO-REQ, MOB_MSHO-REQ, MOB_BSHO-RSP, MOB_HO-IND, DREG-REQ

CMAC Tuple value field

Field (*CMAC*)	**Length (bits)**	**Notes**
Reserved 4	4	Set to 0
CMAC Key Sequence Number	4	CMAC key sequence number
BSID	48	Only used in case of MDHO zone (optional)
CMAC Packet Number Counter, CMAC_PN_*	32	This context is different UL, DL
CMAC Value	64	CMAC with AES 128

Summary

- We described the ‘scope’ where HMAC and CMAC applies
- Almost all management messages, via basic connection or primary management connection, need integrity check in general (unless waived)
- Only limited control message manipulation, other than simply relaying, is possible by an RS unless Relay holds the same HMAC key or CMAC key as MR-BS (or, AK which derives HMAC and CMAC)
- Manipulation by altering CID in an RS can be challenging when CMAC is used.