IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Comment Resolution on clause 30.9.2 and 30.9.3 Protected WUR frames | | | | |
| Date: 2019-03-07 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Rojan Chitrakar | Panasonic |  |  | Rojan.chitrakar@sg.panasonic.com |
| Lei Huang |  |  |  |
| Yoshio Urabe |  |  |  |
| Alfred Asterjadhi | Qualcomm Inc. |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission proposes resolutions of comments received from TGba comment collection (TGba Draft 2.0).

* CIDs: 2558, 2562, 2584, 2585, 2586, , 2638, 2639 (7 CIDs)

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Few editorial changes based on feedbacks. Changed resolution of CID 2639 to Accepted.

1. **Introduction**

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGba Draft. The introduction and the explanation of the proposed changes are not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGba Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGba Editor: Editing instructions preceded by “TGba Editor” are instructions to the TGba editor to modify existing material in the TGba draft. As a result of adopting the changes, the TGba editor will execute the instructions rather than copy them to the TGba Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CID | Commenter | Page.Line | Clause | Comment | Proposed Change | Resolution |
| 2558 | Po-Kai Huang | 78.29 | 30.9.2 | Similar to page 67 line 5, the modular operation should be added to the AT +2^7. | As in comment. | **Revised.**  Agree with the commenter. Modular operation is added.    TGba editor to make the changes shown in 11-19/0352r1 under all headings that include CID 2558. |
| 2562 | Po-Kai Huang | 79.41 | 30.9.2 | Similar to page 67 line 5, the modular operation should be added to the PN0 +2^7. | As in comment. | **Revised.**  Agree with the commenter. Modular operation is added.    TGba editor to make the changes shown in 11-19/0352r1 under all headings that include CID 2562. |
| 2584 | Rojan Chitrakar | 77.62 | 30.9.2 | dot11RSNAStatsCMACWURReplays is not defined. | Added definition of dot11RSNAStatsCMACWURReplays in Annex C. | **Revised.**  Agree with the commenter. Definition of dot11RSNAStatsCMACWURReplays is added in Annex C.    TGba editor to make the changes shown in 11-19/0352r1 under all headings that include CID 2584. |
| 2585 | Rojan Chitrakar | 77.62 | 30.9.2 | If the replay protection failed (i.e. if the IPN is less than or equal to the RC), the STA should not proceed to the next step (construct AAD). | Add to the end of the paragraph: "..., and terminate BIP processing for this reception." | **Revised.**  Agree with the commenter. Frame reception process should be terminated if the replay protection fails.    TGba editor to make the changes shown in 11-19/0352r1 under all headings that include CID 2585. |
| 2586 | Rojan Chitrakar | 78.1 | 30.9.2 | If the MIC value does not match, the STA should not proceed to the next step (Update the RC). | Add to the end of the paragraph: "..., and terminate BIP processing for this reception." | **Revised.**  Agree with the commenter. Frame reception process should be terminated if the MIC values do not match.    TGba editor to make the changes shown in 11-19/0352r1 under all headings that include CID 2586. |
| 2638 | Stephan Sand | 78.42 | 30.9.2 | Acronym "cdo" is introduced but never used: "clock drift offset (cdo)" | remove "(cdo)" | **Accepted.** |
| 2639 | Stephan Sand | 78.43 | 30.9.2 | Acronym "ecd" is introduced and only used once | Remove "(ecd)" in line 43 and replace "ecd" with "estimated clock drift" in line 45 | **Accepted.** |

**Discussion:** None

**Propose:**

Revised for CIDs 2558, 2562, 2585, 2586 as per discussion and editing instructions in 11-19/0352r1.

* Protected WUR frames
* Protected WUR frame reception (CIDs 2558, 2585, 2586, 2587, 2638)

***TGba editor: Modify the section as the following (Track Changes ON):***

A WUR non-AP STA that receives a protected WUR frame shall follow the rules in 12.5.4.6 (BIP reception) except that the WUR non-AP STA shall:

* Use the appropriate integrity key associated to protected WUR frames (see 30.9 (Protected WUR frames)), and associated state based on Key ID equal to the current Key ID value.
* Perform replay protection on the received WUR frame as defined in 12.5.4.4 (BIP replay protection) except that the WUR non-AP STA shall construct the IPN locally as defined in 30.9.3.2 (Construction of the IPN by a WUR non-AP STA). The WUR non-AP STA shall use a replay counter, *RC*, that is equal to the IPN prior to any update due to the WUR frame. If IPN is less than or equal to *RC* then the WUR non-AP STA shall discard the WUR frame, increment its internal dot11RSNAStatsCMACWURReplays counter by 1, and terminate BIP processing for this reception. (#2585)
* Construct the AAD as defined in Figure 30-2 (AAD construction for WUR frames).
* Extract and save the received MIC value from the FCS field of the WUR frame and compute a verifier over the concatenation of AAD, Frame Body field (if present), and the locally constructed IPN. If the result does not match the received MIC value, then the receiver shall discard the frame, increment its internal MIC error counter by 1, and terminate BIP processing for this reception. (#2586)
* Update the *RC* for the integrity key associated to protected WUR frames identified by Key ID equal to the current Key ID value to the IPN.
* If the Common IPN subfield is equal to 1, update the local TSF timer as follows:
* The received partial TSF timestamp, obtained from the Sequence Number subfield of the Type Dependent Control field of the WUR Wake-up frame, is adjusted to consider the WUR non-AP STA’s delay as shown below:
* The CMAC output for BIP-CMAC-128 shall be truncated to 16 bits: *MIC = Truncate-16 (CMAC Output)*. The MIC shall be included in the FCS field of the protected WUR frame.
* IPN = PN0||PN1||PN2||PN3||PN4||PN5 = TSF timer [9: 56], where the TSF timer is obtained as defined in 30.5.1 (General).

—The adjusted value of the received partial TSF timestamp is set as the value of bit position 9 to 16 of the temporary timestamp.

* If the most significant bit (MSB) of the adjusted value of the received partial TSF timestamp is not equal to the bit 16 of the local TSF timer then the value of bits 17 to 63 of the local TSF timer shall be adjusted to account for roll over as follows:

—The value shall be increased by one unit (modulo 247) if LT [9:16] > AT and LT [9:16] > ((AT + 27) modulo 28)

—The value shall be decreased by one unit (modulo 247) if LT [9:16] < AT and LT [9:16] < ((AT–27) modulo 28)

where AT is the adjusted value of the received partial TSF timestamp and LT [9:16] is the value of bits 9 to 16 of the local TSF timer (#2558)

* The bits 9 to 16 of the STA’s local TSF timer shall be set to the adjusted value of the received partial TSF timestamp.

NOTE—Before the adjusted value of the received partial TSF timestamp is set as the value of bit position 9 to 16 of the temporary timestamp, the temporary timestamp may be further compensated for a clock drift offset between the WUR AP and the WUR non-AP STA, which is determined by multiplying the estimated clock drift by the time between receiving the latest TSF from the WUR AP and the time at which the WUR frame is received from the WUR AP, where the estimated clock driftis determined based on two or more received TSF values from the WUR AP and comparing these to the internal TSF at the WUR non-AP STA. (#2638, 2639)

* Generation and construction of IPN for WUR frames

(#338, #903, #904, #1250)

* Construction of the IPN by a WUR non-AP STA (CID 2562)

If a WUR non-AP STA is in WUR mode, then:

* If the Common IPN subfield is equal to 1, the IPN is obtained as follows:
* PN0 is set as the Sequence Number subfield of the Type Dependent Control field of the WUR Wake-up frame
* BPN is set as the value of bits 17 to 56 of the local TSF timer
* If the most significant bit (MSB) of the PN0 is not equal to the bit 16 of the local TSF timer then the value BPN shall be adjusted to account for roll over as follows:

—The value shall be increased by one unit (modulo 240) if LT[9:16] > PN0 and LT[9:16] > ((PN0 + 27) modulo 28)

—The value shall be decreased by one unit (modulo 240) if LT[9:16] < PN0 and LT[9:16] < ((PN0 – 27) modulo 28)

where LT[9:16] is the value of bits 9 to 16 of the local TSF timer (#2562)

* The IPN=PN0||BPN where PN1||PN2||PN3||PN4||PN5 = BPN
* If the Common IPN subfield is equal to 0, the IPN is obtained as follows:
* The IPN is obtained as PPN||BPN, where PPN is equal to the value of the Type Dependent Control field of the received WUR frame, and BPN is retrieved from the locally stored BPN at the receiver for the <ID, Embedded BSSID> duple
* PN0||PN1[0:3] = PPN, and PN1[4:7]||PN2||PN3||PN4||PN5 = BPN

The locally stored IPN at the WUR non-AP STA is initialized to 0 when the WUR mode link is established (see 30.7.2 (WUR Mode Setup)), and the most recently received WUR Operation element has the Common IPN subfield equal to 0.(#905, #906, #907, #1250)

The locally stored IPN at the WUR non-AP STA is initialized to the value of the local TSF timer [9: 56] when the WUR mode link is established (see 30.7.2 (WUR Mode Setup)), and the most recently received WUR Operation element has the Common IPN subfield equal to 1.(#905, #906, #907, #1250)

The BPN and the Key ID may be updated explicitly through a secure header compression request/response exchange by using only the CCMP Update field of the exchange as defined in 10.59 (Generation of PV1 MPDUs and header compression procedure).

***TGba editor: Change Annex C as the following (Track changes on):***

**Annex C (normative) (CID 2584)**

**ASN.1 encoding of the MAC and PHY MIB**

**C.3 MIB Detail**

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* dot11RSNAStats TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Dot11RSNAStatsEntry ::=

SEQUENCE {

…,

dot11RSNAStatsCMACWURReplays Counter32

}

...

dot11RSNAStatsCMACWURReplays OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This is a status variable.

It is written by the MAC when the condition described below occurs.

The number of received WUR frame discarded due to replay errors."

::= { dot11RSNAStatsEntry <ANA> }

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* End of dot11RSNAStats TABLE

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*