IEEE P802.11
Wireless LANs

|  |
| --- |
| Comment resoultion for PN, SN and AC |
| Date: 2022-10-14 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Chaoming Luo | OPPO |  |  | luochaoming@oppo.com |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This submission resolves comments of CID 601, 642.

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Add CID 642 and update the resolution accordingly.
* Rev 2:
	+ Remove ‘PV1 Protected Sensing frames’ related replay checking descriptions since we do not have PV1 sensing frames.
	+ Make (protected) sensing frame(s) using AC\_VO.
	+ Remove CID 744.
	+ Remove the modification on CCMP/GCMP header
	+ Remove the replay check for sensing frames before frame decryption.

# CIDs-601, 642

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| **601** | Chaoming Luo | 10.3.2.14.2 | 11bf should specify transmitter sequence number spaces and receiver caches for sensing frames. | As proposed by https://mentor.ieee.org/802.11/dcn/22/11-22-0556-05-00bf-pn-and-sn-for-sensing.pptx | ***Revised****:* As discussed, only modifications to *“Table 11-18 Default QMF policy”* is required.*TGbf editor to make the changes shown in IEEE 802.11-22/891r2 under all headings that include CID 601.* |
| **642** | Chaoming Luo | 12.5.3 and 12.5.5 | 11bf should add rules to deal with PN and replay detection for sensing measurement report frame. | As proposed by https://mentor.ieee.org/802.11/dcn/22/11-22-0556-05-00bf-pn-and-sn-for-sensing.pptx | ***Revised****:* Agree with the commentor in principle.*TGbf editor to make the changes shown in IEEE 802.11-22/891r2 under all headings that include CID 642* |

# Discussion

Two SPs show majority support for the proposal in 22/0556:

**Straw Poll 1:** Do you agree to add the following into 11bf SFD?

* + A new **replay counter** is introduced and applies to the new action category ‘Protected Sensing Frame’. 11bf shall not define any additional replay counter for other sensing management frames.
	+ Protected sensing measurement report frame belongs to the new action category ‘Protected Sensing Frame’, while other protected sensing Action frames belong to the action category ‘Protected Dual of Public Action’.
	+ Use the **B3 and B4** of ‘Key ID Octet’ in the CCMP/GCMP Header to indicate a frame of the new action category ‘Protected Sensing Frame’.
		- 01 indicates protected ranging
		- 10 indicates protected sensing
		- 11 is reserved

**Result:** SP supported unanimously.

**Straw Poll 2:** Do you agree to add the following into 11bf SFD?

* For a QMF STA, the ‘**SNS4**’ (SNS for QMFs) in ‘*Table 10-5 Transmitter sequence number spaces*’ and ‘**RC6**’ (RC for QMFs) in ‘*Table 10-6—Receiver caches*’ shall be used for sensing Management frames (both public and protected).
* **Two new entries** are added into ‘*Table 11-18 Default QMF policy*’ correspondingly as shown in slide 9. (The exact frame types are TBD)
* For a non-QMF STA, the ‘**SNS1**’ (SNS for Baseline) in ‘*Table 10-5 Transmitter sequence number spaces*’ and ‘**RC1**’ (RC for Not QoS Data) in ‘*Table 10-6—Receiver caches*’ shall be used for sensing Management frames (both public and protected).
* *Note: the referenced tables are in ‘P802.11REVme\_D1.2’*

**Result:** Y/N/A: 16/1/25

**Q1**: Any modification to Table 10-5 and Table 10-6?

**A**: No modification is required.

**Q2**: Why and which frames should use AC\_VO?

**A:** According to Clause 4.5.6.2, in general, Management frames are expected to use AC\_VO, exceptions (e.g., lower priority frames) are specified in QMF policy. There is no evidence that sensing frames belong to the exceptions, so they should use AC\_VO. However, Clause 11.24.1.2 says ‘QMFs not included in this table shall be assigned an access category AC\_BE’, so we shall modify the Table 11-18 to specify sensing frames with AC\_VO.

**C:** It’s better to make only (protected) sensing report frame(s) using AC\_VO, other sensing frames could be AC\_BE.

**C:** It might be better to allow sensing management frames to use AC-VO instead of AC-BE, as depending on the situation it is important for the sensing management frame to be sent out to close the agreement.

**4.5.6.2 Quality-of-service management frame support**

When the quality-of-service management frame (QMF) service is enabled, some Management frames might be transmitted using an access category other than the access category assigned to voice traffic (access category AC\_VO, see 9.4.2.28 (EDCA Parameter Set element)) in order to improve the quality of service of other traffic streams. This is achievable by the use of a QMF policy. A QMF policy defines the access categories of different Management frames. Only QoS STAs are able to implement QMF policy. A non-AP QMF STA uses the default QMF policy or the QMF policy accepted from a peer QMF STA to transmit Management frames to that peer QMF STA. A QMF AP sets its own QMF policy for the transmission of QMFs to its associated STAs. A QMF STA uses access category AC\_VO to transmit Management frames to STAs that do not support the QMF service.

**11.24.1.2 Default QMF policy**

The default QMF policy is defined in Table 11-18 (Default QMF policy). It defines the access category of each Management frame based on management subtype value, category value, and action value. QMFs not included in this table shall be assigned an access category AC\_BE.

**Q3:** We require a simple solution for the receiver to detect sensing frames as easily as possible without any decryption. Therefore, using the ToDS & FromDS bits seems to be an easy way to achieve this.

**A:** Unfortunately, for CCMP, by the nature of the algorithm, you just cannot do MIC check before you decrypt the frame. Whilst you could do the check before decryption for GCMP, but, as disclosed by the KRACK attack, MIC in GCMP is kind of weaker than CCMP, so it’s still better do verify the decrypted frame.

**C:** For GCMP, the separation of the computation of the MIC and encryption/decryption is for doing it in parallel. So, the result is faster than in CCMP. The assumption of having the MIC first for verifying some stuff does not make sense.

**C:** The spec can indicate that a specific category management frames would require a different PN space hence no real need for additional bit i.e. SM bit in the KeyID field. let’s have the PN space per category and NOT to detect replay before the decryption.

# Resolution

**11.24.1.2 Default QMF Policy**

*TGbf Editor: Please modify “Table 11-18 Default QMF Policy” in 11.24.1.2 (Default QMF Policy) of 11REVme D1.2 by adding the following rows before the Vendor-Specific Protected row (header row shown for convenience):*

**Table 11-18—Default QMF policy (#601)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Description** | **Management FrameSubtype value fromTable 9-1 (Validtype and subtypecombinations)** | **Category valuefrom Table 9-79(Category values)** | **Action Field** | **QMF accesscategory** |
| Public Action- Sensing Frame | 1101 | 4 | <ANA>,.., <ANA> | AC\_VO |
| Protected Dual of Public Action-Sensing Frame | 1101 | 9 | <ANA>,.., <ANA> | AC\_VO |
| Protected Sensing Frame | 1101 | <ANA> | <ANA> | AC\_VO |

**12.5.3.4 CCMP decapsulation**

**12.5.3.4.4 PN and replay detection**

*TGbf Editor: Please modify 12.5.3.4.4 PN and replay detection of 11az D5.0 as follows:*

…

The following processing rules are used to detect replay:

…

c) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a single replay counter for received individually addressed robust Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)) that are received with the To DS subfield equal to 0, and a single replay counter for received individually addressed robust PV1 Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)), and shall use the PN from the received frame to detect replays. **(#642)**

d) If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received individually addressed robust Management frames ~~except Protected Fine Timing frames (9.6.34 Protected Fine Timing Frame details )~~ and robust PV1 Management frames ~~except protected PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details))~~ that are received with the To DS subfield equal to 1, except Protected Fine Timing frames (9.6.34 Protected Fine Timing Frame details), protected PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)), Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)). **(#642)**

e) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and shall use the PN from the received frame to detect replays.

*TGbf Editor: Please insert the following as subbullet f) into 12.5.3.4.4 PN and replay detection of 11az D5.0, and modify the existing subbullets accordingly:*

f) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)) and shall use the PN from the received frame to detect replays. **(#642)**

**12.5.5.4 GCMP decapsulation**

**12.5.5.4.4 PN and replay detection**

*TGbf Editor: Please modify 12.5.4.4.4 PN and replay detection of 11az D5.0 as follows:*

…

The following processing rules are used to detect replay:

…

c) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a single replay counter for received individually addressed robust Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)) that are received with the To DS subfield equal to 0, and a single replay counter for received individually addressed robust PV1 Management frames except Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)), and shall use the PN from the received frame to detect replays. **(#642)**

d) If dot11RSNAProtectedManagementFramesActivated is true and dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each ACI for received individually addressed robust Management frames ~~except Protected Fine Timing frames (9.6.34 Protected Fine Timing Frame details )~~ and robust PV1 Management frames ~~except protected PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details))~~ that are received with the To DS subfield equal to 1, except Protected Fine Timing frames (9.6.34 Protected Fine Timing Frame details), protected PV1 Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)), Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)). **(#642)**

e) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Fine Timing frames (see 9.6.34 (Protected Fine Timing Frame details)) and shall use the PN from the received frame to detect replays.

*TGbf Editor: Please insert the following as subbullet f) into 12.5.5.4.4 PN and replay detection of 11az D5.0, and modify the existing subbullets accordingly:*

f) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Sensing frames (see 9.6.36 (Protected Sensing Frame details)) and shall use the PN from the received frame to detect replays. **(#642)**

SP:

Do you support resolutions to the following CIDs and incorporate the text changes into the latest TGbf draft: 601, 642, in 11-22/891r2 [2 CIDs]

Y/N/A