IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protected Sensing frame replay counters | | | | |
| Date: 2024-03-08 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Henry Ptasinski | Element78 Communications LLC |  |  | henry@e78com.com |

Abstract

This submission presents a proposed resolution for the following CIDs from LB281 on P802.11bf:

4187

4188

regarding replay sequence counter management for Protected Sensing frames.

The proposed changes are based on Draft P802.11bf\_D3.0.pdf, Draft P802.11REVme\_D5.0.pdf, and submission 11-24/342r1.

Revision history:

R0 – Initial version

R1 – Added discusion

## P802.11bf CIDs 4187 and 4188:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 4187 | 12.5.4.4.4 | 201 | 15 | The Sequence Number field is not protected by CCMP or GCMP. The replay counter must be selected based on protected fields. | Define a new key specifically for Protected Sensing Frames. |
| 4188 | 12.5.2.4.4 | 200 | 37 | The Sequence Number field is not protected by CCMP or GCMP. The replay counter must be selected based on protected fields. | Define a new key specifically for Protected Sensing frames. |

## Discussion:

For Protected Sensing frames, 11bf requires the use of a special replay counter that’s distinct from the QMF replay counters. Unlike FTM, 11bf does not add a bit in the CCMP header to indicate that the frame is a Sensing frame vs. some other Action frame. There seem to be a number of issues with respect to replay counters for QMFs, part stemming from 11bf, part from FTM, and part from GCMP support for QMFs in the baseline:

No early discard of replayed protected Action frames:

Unlike FTM, 11bf does not include a bit in the CCMP header to identify Protected Sensing frames. As a result, selection of the correct replay counter (the sensing-specific one vs. the regular QMF replay counter for the ACI of the frame) cannot be done until after the frame has been decrypted. However, the standard explicitly allows discard before decrypt (REVme 12.5.2.4.4 and 12.5.4.4.4). Discard before decrypt allows receiving STAs to save power by not decrypting frames that will be immediately discarded post-decrypt.

Scalability:

One bit of the few remaining in the CCMP Header was already consumed for FTM. Adding another bit for Protected Sensing frames would chip away at the remaining reserved bits, and is not scalable to future services that need similar functionality. A multipurpose approach should be used that can be used by multiple services without individually allocating CCMP Header bits for each service.

ACI not protected in GCMP:

For QMFs, the ACI is used to select the replay counter (REVme Clause 12.5.2.4.4 PN and replay detection, step (f)). The ACI is bits 10-11 of the Sequence Number field (REVme 9.2.4.4.3 Sequence Number field Figure 9-9), so it’s bits 14-15 of the Sequence Control field. But those bits are masked out when the AAD is constructed (REVme 12.5.2.3.3 Construct AAD):

5) SC – MPDU Sequence Control field, with the Sequence Number subfield (bits 4–15 of the Sequence Control field) masked out. The Fragment Number subfield is not modified.

The AAD construction is performed the same for CCMP and GCMP.

Since the ACI is not included in the AAD, CCMP protects the ACI by including it in the Priority field of the CCM Nonce Flags field. The GCM nonce, however, does not include a priority field, so ACI is not included in the nonce construction. As a result, the ACI is not protected at all when GCMP is used.

*Disallowing GCMP for QMF would mean that GCMP could not be used by STAs when FTM or Sensing are enabled.*

This proposal defines change for P802.11bf to use the multipurpose alternate replay counter (MARC) solution being considered in TGme, which adds four alternative counters which can be used with in addition to the existing four ACI replay counter for robust IQMFs.

## Proposed Resolution for CIDs 4187 and 4188:

REVISED. Request the TGbf editor to apply the changes below:

Delete all changes in 12.5.2.4.4 (PN and replay detection).

Delete all changes in 12.5.4.4.4 (PN and replay detection).

Insert the following text as the second paragraph in 11.55.1.2 (Dependencies and timing-related parameters):

A sensing STA shall support QMF and MARC. A sensing STA shall set dot11QMFActivated to true, shall set dot11QosOptionImplemented to true, and shall set dot11MultipurposeAlternateReplayCountersActivated to true.

Insert the following text at the end of 11.55.1.5.1 (General):

A sensing STA shall use MARC for Protected Sensing frames. A sensing STA shall set the FTM/MARC bit in the CCMP header or GCMP header of transmitted Protected Sensing frames. A sensing STA shall use the same MARC Index for all transmitted Protected Sensing frames in a Sensing measurement exchange.

NOTE 1 – The sensing STA may select any MARC Index to use for the Protected Sensing frames that it transmits in a Sensing measurement exchange, subject to the reordering rules in 12.5.2.3.7 (CCM originator processing) and 12.5.4.3.6 (GCM originator processing). The sensing STA does not need to use the same MARC Index across multiple Sensing measurement exchanges.

NOTE 2 – For the Protected Sensing frames that it transmits, a sensing responder may use a different MARC Index than is being used by the sensing initiator.

**References:**

[Draft P802.11bf\_D3.0.pdf](https://grouper.ieee.org/groups/802/11/private/Draft_Standards/11bf/Draft P802.11bf_D3.0.pdf)

[Draft P802.11REVme\_D5.0.pdf](https://grouper.ieee.org/groups/802/11/private/Draft_Standards/11me/Draft P802.11REVme_D5.0.pdf)