IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protected LMR/FTM Replay Counter | | | | |
| Date: June 18, 2020 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom Inc. | 250 Innovation Drive, San Jose CA | +1 408 391 2159 | [nehru.bhandaru@broadcom.com](mailto:nehru.bhandaru@broadcom.com) |
| Ali Raissinia | Qualcomm Inc. |  | 408-410-6328 |  |

Abstract

This submission proposes a set of changes to addresses certain re-ordering issues with FTM/LMR transmission and reception that cause management frames to be lost. Protected FTM and LMR frames or other management frames may be lost because of frame re-ordering resulting from timing constraints on when FTM and LMR transmissions must occur. When re-ordered, the receiver discards frames received out of order because they are currently checked against a single replay counter that applies to unicast protected management frames (PMFs), possibly on a TID basis if QOS for management frames (QMF) is enabled. Similar issue applies to unprotected or protected LMR/FTM from duplicate detection based on on 802.11 sequence numbers.

**Revision Notes**

00 – Initial version

01 – Update related to sequence number spaces

02 – Update related to indication in Ext IV/Key ID octet

03 – Minor updates as part of strawpoll

04 – Clarification based on email discussion w/ Liwen and Ali

**References**

[1] IEEE P802.11-REVmd™/D3.3, May 2020

[2] P802.11az™/D2.2 – Amendment for Positioning

[3] Document 11-20/0797r0 - LMR/FTM Replay Counter

**Discussion**

Document 11-20/0797r0 presented to the group summarizes the issue and some options. Following summarizes the issue and some of the feedback received from the group.

In 11az [2], protected link measurement reports (p-LMR) are part of a frame sequence that has timing constraints.

In secure Non-TB ranging, a p-LMR needs to be transmitted by an RSTA in response to a sequence initiated by an ISTA. On RSTA, there may be protected management frames (PMFs) that are being transmitted when the p-LMR is queued and there may be additional PMFs that are transmitted after the p-LMR is queued, but before the LMR is transmitted. If the LMR is protected by software or firmware and queued, then the frames would be out of order when transmitted or re-transmitted. Similar issue occurs with I2R p-LMR transmission on ISTA if that option is negotiated.

Similarly, in the secure TB ranging case, an RSTA needs to begin the frame sequence upon the arrival of the availability window and transmit the p-LMR frame that is part of the sequene, regardless of the status of other PMFs to be transmitted. Additionally, if I2R p-LMR is negotiated, its transmission on ISTA has a similar issue.

Passive ranging is non-secure; so, this consideration currently does not apply to passive ranging.

Protected FTM frames, especially when used with EDMG, have similar constraints.

0797r0 presents a options

* Lose some pending protected management frames.
* Transmit LMR separately – relax the timing constraints
* Add new Replay counter(s) specifically for LMR and FTM transmissions
* Have a different Key & PN number space exclusive for LMR

Additional options were suggested during 0797r0 presentation

* Use a different MAC address to transmit FTM/LMR
* Use a different network interface

Considering packet loss, time for measurement, complexity of specification, implementation and deployment, the preferred option, as indicated by a Strawpoll in 11az (06/10/20) is to add a replay counter specific to FTM/LMR transmissions.

In order to simplify selection of the frames to which the new replay counter applies, a new action category ‘Protected Fine Timing’ is created. It’s action field supports a protected iFTMR, protected iFTM and protected LMR.

--

Typically replay checking occurs after decryption (see [1] - Figure 5-1 MAC data plane architecture). However, as an optimization for early discard, without loss of security, some implementations may check for replays before decryption. Some options [preferred proposal TBD] to support those are:

* Change the implementation to decrypt before replay check. Or do this just for protected action frames because the category field is encrypted and needs to be known to select the replay counter to check against. This may introduce additional denial of service scenarios.
* Add a bit in CCMP/GCMP Extended IV field in CCMP/GCMP header to indicate that the frame is a protected fine timing frame. There are 5 reserved bits in the header. When the frame is received, replay counter can be checked before decryption (or after decryption), but the receiver must ensure that the right replay counter was picked before accepting the frame after decryption – otherwise an attacker may replay a frame which the receiver will accept by flipping this bit
* Use a different management frame subtype for protected fine timing.

It is desirable to preserve the ability to replay check without decryption and not to use up another management frame category – with its associated specification and implementation complexity. We propose to add a bit in Extended IVs to indicate a protected fine timing frame.

--

Similarly, to allow re-transmissions with or without security, FTM/LMR frames should use their own sequence number (SN) space. SN used for duplicate detection for both secure & unsecure packets at MPDU level

1. LMR/FTM transmissions that occur based on constraint transmission – e.g. as a result of a trigger or part of NTB/TB frame sequence would need separate SNS segment
2. Table referring to TX Sequence should have a reference for LMR/FTM (both protected and unprotected)
3. Table for Receive cache should also have reference for LMR/FTM (both protected and unprotected)

Some relevant sections from 802.11 spec [1] related to replay detection and some notes related to the new counter are below.

[1] § **4.5.4.7 Replay Detection**

Replay detection PMF reception against duplicate processing, possibly from re-transmissions by an MITM attacker.

In an RSNA p-LMR is a unicast management frame that is protected by CCMP or GCMP. The same TK (part of PTK) is used to protect the frame as that is used for unicast data frame protection. Since PMF is required to transmit a p-LMR, ciphers such as WEP, TKIP etc. do not apply to 11az ranging.

[1] § **6.3.19.1 MLME-SETKEYS.request**

Replay counters are initialized to 0 when a new key is set. Unlike group keys, there is no protocol exchange to alter the replay counters for pairwise keys except updates based on frame reception.

**[1] § 9.4.2.24.4 RSN capabilities**

PTKSA replay counters are advertised in RSN capabilities of RSNE. The advertised values apply to unicast data frame protection for a given key and there is a single additional counter for unicat PMFs.

**[1] § 12.5.3.3.7 CCM originator processing**

“The PN values sequentially number each MPDU. Each transmitter shall maintain a single PN (48-bit counter)

for each PTKSA and GTKSA(#59). The PN shall be implemented as a 48-bit strictly increasing integer,

initialized to 1 when the corresponding temporal key is initialized or refreshed.

…

The transmitter shall not reorder CCMP

protected frames that are transmitted to the same RA within a replay counter, but may reorder frames across

replay counters. One possible reason for reordering frames is the IEEE 802.11 MSDU or A-MSDU priority.

…

The transmitter shall preserve the order of protected robust Management frames that are transmitted to the

same DA without the QMF service. When the QMF service is used, the transmitter shall not reorder robust

IQMFs within an AC when the frames are transmitted to the same RA.

…

A CCMP protected individually addressed robust Management frame shall be protected using the same TK as

a Data frame.”

Unicast PMFs and protected data frames share the same PN space that of the the key they share. They are not re-ordered unless QMF service is used.

**[1] § 12.5.3.4.4 PN and replay detection(#2720)**

“To effect replay detection, the receiver extracts the PN from the CCMP header.

(11ah)NOTE—The CCMP header is not present in secure PV1 MPDUs, but constructed locally at the STA as defined in

(#2720)12.5.3.3.6 (Construct CCMP header for PV1 MPDUs(#2720)(11ah)).

(11ah)See 12.5.3.2 (CCMP MPDU format) for a description of how the PN is encoded in the CCMP header.

The following processing rules are used to detect replay:

a) The receiver shall maintain a separate set of replay counters for each PTKSA, GTKSA,

(#59)(11ah)and protocol version value. The receiver initializes these replay counters to 0 when it

resets the temporal key for a peer. The replay counter is set to the PN value of accepted CCMP

MPDUs.

b) For each PTKSA, GTKSA, (#59)(11ah)and protocol version value, the recipient shall maintain a

separate replay counter for each TID, subject to the limitation of the number of supported replay

counters indicated in the RSN Capabilities field (see 9.4.2.24 (RSNE)), and shall use the PN from a

received frame to detect replayed frames. A replayed frame occurs when the PN from a received

frame is less than or equal to the current replay counter value for the frame’s MSDU or A-MSDU

priority and frame type.

c) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a single

replay counter for received individually addressed robust Management frames that are received with

the To DS subfield equal to 0(11ah), and a single replay counter for received individually addressed

robust PV1 Management frames and shall use the PN from the received frame to detect replays. If

dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each

ACI for received individually addressed robust Management frames and (11ah)robust PV1

Management frames that are received with the To DS subfield equal to 1. The QMF receiver shall

use the ACI encoded in the Sequence Number field of the received frame to select the replay counter

to use for the received frame, and shall use the PN from the received frame to detect replays. A

replayed frame occurs when the PN from the frame is less than or equal to the current value of the

management frame replay counter that corresponds to the ACI of the frame.

…

e) When discarding a frame, the receiver shall increment by 1 dot11RSNAStatsCCMPReplays for Data

frames or dot11RSNAStatsRobustMgmtCCMPReplays for robust Management frames.”

When PMF is activated (dot11RSNAProtectedManagementFramesActivated), PMFs use a separate replay counter for PV0 and PV1 frames. If QMF is used, then there is a separate replay counter for each ACI.

**[1] § 12.5.5.4.4 PN and replay detection**

When PMF is activated, similar protection as in **§ 12.5.3.4.4 PN and replay detection** (for CCMP) applies also to GCMP. The behavior and text are the same.

Additionally, p-LMR needs to be assigned QMF AC, and LMR as well. If not defined in default QMF policy – table 11-17 in [1] – then they will be assigned to AC\_BE.

**[2] § 9.4.2.26 Extended Capabilities element – Table 9-153 …**

Whenever PMF is activated, ranging negotiation and measurement frames are protected.

**Proposed Changes**

***TGaz Editor - Remove this change from TGaz Draft 2.2***

**~~9.6.10 Protected Dual of Public Action frames~~**

***~~Insert the following new rows into Table 9-402 (Public Action field values defined for~~*** ~~25~~ ***~~Protected Dual of Public Action frames) (header row shown for convenience):~~* ~~(~~**~~#~~**~~2523~~**~~, #~~**~~2524~~**~~)~~

~~… changes to table~~

***TGaz Editor -Add a new action category for protected ranging frames to Table 9-53 p919.18 before the Vendor-Specific Protected row***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Code** | **Meaning** | **See subclause** | **Robust** | **Group Addressed Privacy** |
| … |  |  |  |  |
| <ANA-protected-fine-timing-action-frame> | Protected Fine Timing Frame | 9.6.xx | Yes | No |
| … |  |  |  |  |

***TGaz Editor -Add a subclause 9.6.xx for protected fine timing frames p1686.26***

**9.6.xx Protected Fine Timing Frame details**

**9.6.xx.1 Protected Fine Timing Frame Action field**

The Protected Fine Timing Frame Action field, in the one octet immediately after the category field, differentiates between various Protected Fine Timing frames as shown in the Table 9-yy (Protected Fine Timing Frame Action Field values)

**Table 9-yy Protected Fine Timing Frame Action Field values**

|  |  |
| --- | --- |
| **Value** | **Meaning** |
| 0 | Reserved |
| 1 | A protected Fine Timing Measurement Request. The format of frame after the action field is identical to the format of Fine Timing Measurement Request public action (9.6.7.32 Fine Timing Measurement Request frame format). It is carried in a Management Action frame. |
| 2 | A protected Fine Timing Measurement. The format of frame after the action field is identical to the format of Fine Timing Measurement public action (9.6.7.33 Fine Timing Measurement frame format). It is carried in a Management Action frame. |
| 3 | A protected Location Measurement Report. The format of the frame after the action field is identical to the format of Location Measurement Report public action (9.6.7.48 Location Measurement Report frame format). It is carried in a Management Action No Ack frame. |
| 4-255 | Reserved |

***TGaz Editor - Change the draft p103.6 as follows***

***Modify the Class 2 frames as follows:***

***…***

iv) Unicast Protected Dual of Public Action frames (9.6.10) and Protected Fine Timing frames (9.6.xx) when PTKSA from PASN authentication exists.

…

***TGaz Editor – Change the Fine Timing Measurement section as follows***

**11.22.6.3 Fine Timing Measurement procedure negotiation** 16

***Insert a new subclause heading 11.22.6.3.1 and move the first two and the fourth paragraph*** 17 ***(along with the note) of 11.22.6.3 to 11.22.6.3.1*** 18

**11.22.6.3.1 General**

*…*

***p116.22***

A Secure Fine Timing Measurement Session is established when an ISTA and an RSTA establish a security context and use it to exchange ~~the IFTMR frame and the corresponding initial Fine Timing Measurement frame in the Protected Dual of Public Action frame format in 9.6.10 (Protect Dual of Public Action frames)~~ a Protected Fine Timing Request and the corresponding Protected Fine Timing Measurement in the Protected Fine Timing Frame Action format (9.6.xx Protected Fine Timing Action Frame details) and the negotiation completes successfully.

~~An ISTA shall only initiate a Fine Timing Measurement Negotiation with a Protected Dual of Fine Timing Measurement Request frame for Trigger-Based, a non-Trigger-Based, or an EDCA based ranging measurement with a Format and Bandwidth field indicating DMG or EDMG format; see Table 9-281 (Format And Bandwidth field).~~

An ISTA shall not initiate FTM Negotiation with a Protected Fine Timing frame, i.e. setup a secure FTM session, unless the session is non-Trigger based or Trigger based or an EDCA based ranging measurement with a Format and Bandwidth field indicating DMG or EDMG  format (see Table 9-281 (Format And Bandwidth field)). Protected Fine Timing frames may be used with DMG and EDMG EDCA based ranging sessions.

***TGaz Editor – Change the secure LTF negotiation as follows***

***Insert the new subclauses 11.22.6.3.4 as shown below:***

**11.22.6.3.4 Negotiation for Secure LTF in the TB and Non-TB Ranging measurement exchange (#1817, #1818, #1824, #2321)**

**…**

***p124.2***

When Management Frame Protection is negotiated for TB and Non-TB Ranging negotiation, a STA shall use Protected ~~Dual of Public~~ Fine Timing Action frames for an IFTMR, an initial Fine Timing Measurement, and a Location Measurement Report.

...

***TGaz Editor – Change p124.27 as follows***

…

An ISTA may request a Secure ToF measurement by setting the Secure ToF Measurement subfield in the Measurement Parameters field in the initial (#**1449**) Protected ~~Dual of the~~ Fine Timing Measurement Request frame. An ISTA shall not set the Secure ToF Measurement subfield in a request to an RSTA if the RSTA has not set the Secure ToF Supported field in the EDMG Capabilities field to 1. The ISTA shall generate a 32 octet random Secret Key and include it in the Secure Ranging Operation Parameters field; see Figure 9-619e (Ranging Operation Parameters field format), in the initial Protected ~~Dual of the~~ Fine Timing Measurement Request frame. (#**1454**, #**1455**, #**1456**, #**1450**, #**1089**) An RSTA that supports Secure ToF measurement shall acknowledge a request for Secure ToF measurement by setting the Secure ToF Measurement subfield in the Measurement Parameters field in the initial (#**1449**) Protected ~~Dual of the~~ Fine Timing Measurement frame.

…

***TGaz Editor – Change as follows***

**11.22.6.4.2 EDCA based ranging measurement exchange**

***Insert the whole subclause “11.22.6.4 Measurement exchange” in REVmd 3.0 into subclause 11.22.6.4.2***

***Insert at the end of Cl. 11.22.6.4.2 as shown below (Note that 11.22.6.4.2 describes the legacy*** ***FTM Measurement exchange which contains the content from the baseline 11.22.6.4***  ***Measurement exchange):***

When a Secure Fine Timing Measurement Session is established as described in 11.22.6.3.1 (General), the Fine Timing Measurement frames transmitted during the execution of Measurement Exchange shall be Protected ~~Dual of Public~~ Fine Timing Action frames; see ~~9.6.10 (Protected Dual of Public Action frames)~~ 9.6.xx (Protected Fine Timing Frame details) …

***TGaz Editor – Change 11.22.6.4.2.1.6 Secure measurement exchange for EDMG STAs - p132.21 as follows***

Setup of the Secure EDMG Measurement exchange is described in 11.22.6.3.5 (Negotiation of secure EDMG TRN in EDCA based measurement exchange.) The Secure EDMG Measurement exchange protocol follows the procedure as described in 11.22.6.4.2 (EDCA based ranging measurement exchange) with the following changes:

— The Protected ~~dual of the~~ Fine Timing Measurement Request frame shall be used by the ISTA to initiate the exchange

— The ISTA shall use the Protected ~~dual of the~~ Fine Timing Measurement frame during the exchange.

— The PPDUs carrying the Protected ~~Dual of~~ Fine Timing Measurement frames transmitted by the RSTA and the Acks transmitted by the ISTA shall be based on the format as

***p133***

described in 28.9.3 (PDMG secure ranging PPDU). In these PPDUs, the SECURED\_TRN parameter of the TXVECTOR shall be set to SECURED\_TRN.

— The PPDU carrying the protected ~~dual of~~ FTM frames transmitted by the responder to initiator shall use the first path AWVs obtained during first path beamforming training as described in 10.42.10.6 (First Path Beamforming Training).

…

***TGaz Editor – Change p142.25 as follows***

**11.22.6.4.3.4 Reporting phase of TB Ranging measurement (#2158)**

The last phase of each polling/sounding/reporting triplet is the measurement reporting phase, which is transmitted a SIFS time after the measurement sounding phase; see Figure 11-36c (TB

…

frames shall be transmitted using the Protected ~~Dual of Public~~ Fine Timing Action frames; see 9.6.xx (Protected Fine Timing Frame details) ~~9.6.10 (Protected Dual of Public Action frames)~~. (#**2523**, #**2524**) The feedback type of the ISTA2RSTA and RSTA2ISTA LMRs…

…

***p148.6***

**11.22.6.4.4.3 Non-TB Ranging Measurement Reporting phase**

If the Range Reporting is performed in the context of a Secure Fine Timing Measurement Session, the corresponding LMR frames shall be transmitted as Protected Fine Timing Action frames; see 9.6.xx (Protected Fine Timing Frame details) ~~Protected Dual of Public Action frames; see 9.6.10 (Protected Dual of Public Action frames)~~.(#**2523**, #**2524**)

…

***p174.11***

**11.22.6.6.1 EDCA-based Ranging session termination**

When the FTM session is a Secure Fine Timing Measurement Session, the Fine Timing Measurement frames transmitted shall be the Protected Fine Timing Action frames; see 9.6.xx (Protected Fine Timing Frame details)~~Protected Dual of Public Action frames; see subclause 9.6.10 (Protected Dual of Public Action frames)~~ (#**2523**, #**2524**)

…

***p175.6***

If the ranging session is a Secure Fine Timing Measurement Session, the corresponding Fine Timing Measurement frames transmitted shall be ~~Protected Dual of Public Action frames, see 9.6.10 (Protected Dual of Public Action frames)~~ Protected Fine Timing Action frames; see 9.6.xx (Protected Fine Timing Frame details) (#**2523**, #**2524,** #**1475**).

***TGaz Editor – Add the following change to the draft***

***Change* 12.5.3.4.4 PN and replay detection (2603.25) *as follows***

**…**

The following processing rules are used to detect replay:

a) The receiver shall maintain a separate set of replay counters for each PTKSA, GTKSA, (#59)(11ah)and protocol version value. The receiver initializes these replay counters to 0 when it resets the temporal key for a peer. The replay counter is set to the PN value of **accepted** CCMP MPDUs.

b) For each PTKSA, GTKSA, (#59)(11ah)and protocol version value, the recipient shall maintain a separate replay counter for each TID, subject to the limitation of the number of supported replay counters indicated in the RSN Capabilities field (see 9.4.2.24 (RSNE)), and shall use the PN from a received frame to detect replayed frames. A replayed frame occurs when the PN from a received frame is less than or equal to the current replay counter value for the frame’s MSDU or A-MSDU priority and frame type.

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 (9.6.xx Protected Fine Timing Frame details **)** that are received with the To DS subfield equal to 0(11ah), and a single replay counter for received individually addressed robust PV1 Management frames except Protected Fine Timing frames (9.6.xx Protected Fine Timing Frame details **)** and shall use the PN from the received frame to detect replays.

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.xx Protected Fine Timing Frame details **)**  and (11ah)robust PV1 Management frames except protected PV1 Protected Fine Timing frames (9.6.xx Protected Fine Timing Frame details **)** that are received with the To DS subfield equal to 1.

The QMF receiver shall use the ACI encoded in the Sequence Number field of the received frame to select the replay counter to use for the received frame, and shall use the PN from the received frame to detect replays. A replayed frame occurs when the PN from the frame is less than or equal to the current value of the management frame replay counter that corresponds to the ACI of the frame.

e) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for receiving individually addressed Protected Fine Timing frames (9.6.xx Protected Fine Timing Frame details **)** and shall use the PN from the received frame to detect replays.

~~c) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a single~~

~~replay counter for received individually addressed robust Management frames that are received with~~

~~the To DS subfield equal to 0(11ah), and a single replay counter for received individually addressed~~

~~robust PV1 Management frames and shall use the PN from the received frame to detect replays. If~~

~~dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each~~

~~ACI for received individually addressed robust Management frames and (11ah)robust PV1~~

~~Management frames that are received with the To DS subfield equal to 1. The QMF receiver shall~~

~~use the ACI encoded in the Sequence Number field of the received frame to select the replay counter~~

~~to use for the received frame, and shall use the PN from the received frame to detect replays. A~~

~~replayed frame occurs when the PN from the frame is less than or equal to the current value of the~~

~~management frame replay counter that corresponds to the ACI of the frame.~~

~~df~~) The receiver shall discard any Data frame that is received with its PN less than or equal to the value of the replay counter that is associated with the TA and priority value of the received MPDU. The receiver shall discard MSDUs and MMPDUs whose constituent MPDU PN values are not incrementing in steps of 1. If dot11RSNAProtectedManagementFramesActivated is true, the receiver shall discard an individually addressed robust Management frame that is received with its PN less than or equal to the value of the replay counter associated with the TA of that individually addressed Management frame.

~~eg~~) When discarding a frame, the receiver shall increment by 1 dot11RSNAStatsCCMPReplays for Data frames or dot11RSNAStatsRobustMgmtCCMPReplays for robust Management frames.

~~f~~h) For MSDUs or A-MSDUs sent using the block ack feature, reordering of received MSDUs or A-MSDUs according to the block ack receiver operation (Ed#57)is performed prior to replay detection.

i) If the receiver performs replay detection prior to decryption, then the receiver shall check that the replay counter used to detect replays is correct and discard the frame if incorrect. In particular, the separate replay counter for individually addressed Protected Fine Timing frames shall be used if and only if the FTM subfield of CCMP Header (Figure 12-16—Expanded CCMP MPDU) signals that the management PDU is a Protected Fine Timing Frame.

***Change* 12.5.5.4.4 PN and replay detection *(p2612.32) as follows***

a) The receiver shall maintain a separate set of replay counters for each PTKSA and GTKSA(#59). The receiver initializes these replay counters to 0 when it resets the temporal key for a peer. The replay counter is set to the PN value of **accepted** GCMP MPDUs.

b) For each PTKSA and GTKSA(#59), the recipient shall maintain a separate replay counter for each TID, subject to the limitation of the number of supported replay counters indicated in the RSN Capabilities field (see 9.4.2.24 (RSNE)), and shall use the PN from a received frame to detect replayed frames. A replayed frame occurs when the PN from a received frame is less than or equal to the current replay counter value for the frame’s MSDU or A-MSDU priority and frame type.

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 (9.6.xx Protected Fine Timing Frame details **)** that are received with the To DS subfield equal to 0(11ah), and a single replay counter for received individually addressed robust PV1 Management frames except PV1 Protected Fine Timing frames (9.6.xx Protected Fine Timing Frame details **)** and shall use the PN from the received frame to detect replays.

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.xx Protected Fine Timing Frame details **)**and (11ah)robust PV1 Management frames except Protected Fine Timing frames (9.6.xx Protected Fine Timing Frame details **)** that are received with the To DS subfield equal to 1.

The QMF receiver shall use the ACI encoded in the Sequence Number field of the received frame to select the replay counter to use for the received frame, and shall use the PN from the received frame to detect replays. A replayed frame occurs when the PN from the frame is less than or equal to the current value of the management frame replay counter that corresponds to the ACI of the frame.

e) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a separate replay counter for received individually addressed Protected Fine Timing frames (9.6.xx Protected Fine Timing Frame details **)** and shall use the PN from the received frame to detect replays.

~~c) If dot11RSNAProtectedManagementFramesActivated is true, the recipient shall maintain a single~~

~~replay counter for received individually addressed robust Management frames that are received with~~

~~the To DS subfield equal to 0 and shall use the PN from the received frame to detect replays. If~~

~~dot11QMFActivated is also true, the recipient shall maintain an additional replay counter for each~~

~~ACI for received individually addressed robust Management frames that are received with the To~~

~~DS subfield equal to 1. The QMF receiver shall use the ACI encoded in the Sequence Number field~~

~~of the received frame to select the replay counter to use for the received frame, and shall use the PN~~

~~from the received frame to detect replays. A replayed frame occurs when the PN from the frame is~~

~~less than or equal to the current value of the management frame replay counter that corresponds to~~

~~the ACI of the frame.~~

f~~d~~) The receiver shall discard any Data frame that is received with its PN less than or equal to the value of the replay counter that is associated with the TA and priority value of the received MPDU. The receiver shall discard MSDUs and MMPDUs whose constituent MPDU PN values are not incrementing in steps of 1. If dot11RSNAProtectedManagementFramesActivated is true, the receiver shall discard any individually addressed robust Management frame that is received with its PN less than or equal to the value of the replay counter associated with the TA of that individually addressed Management frame.

g~~e~~) When discarding a frame, the receiver shall increment by 1 dot11RSNAStatsGCMPReplays for Data frames or dot11RSNAStatsRobustMgmtGCMPReplays for robust Management frames.

h~~f~~) For MSDUs or A-MSDUs sent using the block ack feature, reordering of received MSDUs or A-MSDUs according to the block ack receiver operation (Ed#57)is performed prior to replay detection.

i) If the receiver performs replay detection prior to decryption, then the receiver shall check that the replay counter used to detect replays is correct and discard the frame if incorrect. In particular, the separate replay counter for individually addressed Protected Fine Timing frames shall be used if and only if the FTM subfield of GCMP Header (Figure 12-26—Expanded GCMP MPDU) signals that the management PDU is a Protected Fine Timing Frame.

***TGaz Editor: Insert the following into the draft***

***Update*** Figure 12-16—Expanded CCMP MPDU ***with the following and change text around p2594.54 as follows***

A picture containing screenshot

Description automatically generated

…

The ExtIV subfield (bit 5) of the Key ID octet signals that the CCMP Header field extends the MPDU header by a total of 8 octets, compared to the 4 octets added to the MPDU header when WEP is used. The ExtIV bit

(bit 5) is always set to 1 for CCMP.

Bits 6–7 of the Key ID octet are for the Key ID subfield.

In a protected unicast management Action frame, Bit 4 of the Key ID octet signals that the MPDU is a Protected Fine Timing Frame – see Table 9-53 (Category values). Otherwise it is reserved.

The remaining bits of the Key ID octet are reserved.

***TGaz Editor: Insert the following into the draft***

***Update*** Figure 12-26—Expanded GCMP MPDU ***with the following and change text around p2608.37 as follows***

A picture containing screenshot

Description automatically generated

…

GCMP processing expands the original MPDU size by 24 octets, 8 octets for the GCMP Header field and 16

octets for the MIC field. The GCMP Header field is constructed from the PN and Key ID subfields. The 48-bit

PN is represented as an array of 6 octets. PN5 is the most significant octet of the PN, and PN0 is the least

significant.

The ExtIV subfield (bit 5) of the Key ID octet is always set to 1 for GCMP.

Bits 6–7 of the Key ID octet are for the Key ID subfield.

In a protected unicast management Action frame, Bit 4 of the Key ID octet signals that the MPDU is a Protected Fine Timing Frame – see Table 9-53 (Category values). Otherwise it is reserved.

The remaining bits of the Key ID octet are reserved.

***TGaz Editor: Change* 11.25.1.2 Default QMF Policy Table 11-17  *(p2432.10) as follows by adding rows for LMR and p-LMR***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Description** | **Management Frame**  **Subtype value from**  **Table 9-1 (Valid**  **type and subtype**  **combinations)** | **Category value**  **from Table 9-53**  **(Category values)** | **Action Field** | **QMF access**  **category** |
| **…** | **…** | **…** |  | **…** |
| Public Action - Location Measurement Report | 1101 | 4 | <ANA> | AC\_VO |
| Protected Fine Timing Frame | 1101 | <ANA-protected-fine-timing-action-frame> | any | AC\_VO for Protected FTM Request and Protected FTM. N/A for Protected LMR. |

***TGaz Editor: Insert the following change (to TGmd baseline) into TGaz draft***

***Insert the following new row into Table 10-5 (p1744.1)-Transmitter sequence number spaces (header row shown for convenience)***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sequence Number Space Identifier** | **Sequence Number Space** | **Applies to** | **Status** | **Multiplicity** | **Transmitter Requirements** |
| ***…*** |  |  |  |  |  |
| SNS4 | QMF | QMF STA transmitting a  QMF that is neither a Protected Fine Timing Frame nor a Public Action LMR | Mandatory | Indexed by  <Address 1,  AC> | TR2 |
| ***…*** |  |  |  |  |  |
| SNS8 | Protected Fine Timing Frame and Public Action LMR | A STA Transmitting Protected Fine Timing Frames or Public Action LMR | Mandatory | Single Instance |  |

***TGaz Editor: Insert the following change (to TGmd baseline) into TGaz draft***

***Insert the following new row into Table 10-6 (p1745.17)-Receiver caches (header row shown for convenience)***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Receiver cache Identifier** | **Cache name** | **Applies to** | **Status** | **Multiplicity/Cache size** | **Receiver Requirements** |
| ***…*** |  |  |  |  |  |
| RC6 | QMFs | A STA receiving an  individually addressed  QMF that is neither a Protected Fine Timing Frame nor a Public Action LMR | Mandatory | Indexed by: <Address 2,  AC, sequence number,  fragment number>  The most recent cache  entry per <Address 2,  AC, sequence-number,  fragment-number> | RR2  RR3  RR5 |
| ***…*** |  |  |  |  |  |
| RC13 | Protected Fine Timing Frame and Public Action LMR | A STA receiving Protected Fine Timing Frames or Public Action LMR | Mandatory | Indexed by: <Address 2,  sequence number,  fragment number>.  At least the most recent  cache entry per  <Address 2> | RR1  RR2  RR5 |