IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Some TGm CC35 CRs | | | | |
| Date: October 25 2021 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom | 250 Innovation Drive, San Jose CA | +1 408 391 2159 | [nehru.bhandaru@broadcom.com](mailto:nehru.bhandaru@broadcom.com) |

Abstract

This document contains discussion and proposed resolutions for the following comment 37 from TGme CC35 on IEEE P802.11-REVme/D0.0.

Revision Notes

R0 – initial version

References

[1] IEEE P802.11-REVme/D0.0, March 2021

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CID | Clause/Page | Comment | Proposed Change | Resolution |
| 37 | 12.5.3.3.2  2572.38 | The fixed version of PV1 CCMP in REVmd still has a potential security flaw due to CCM nonce reuse. From an email from Jouni: The language we use for enforcing unique PN values for the same TK, Priority pair is using "TID", not "PTID". As such, there might be a case where two different TID values (e.g., 1 and 9) getting mapped to the same PTID value (1). The current language would allow the same PN to be used for frames using those two TIDs and this would result in CCM nonce reuse and loss of CCMP security protection. I hope that no one would be allowing TIDs 9..15 to be used with PV1 QoS Data frames, but if those are allowed, we do need to fix this by modifying the rule on PN reuse to not allow reuse for same TK/PTID instead TK/TID. | As suggested by Jouni, change the sentence: "For PV1 MPDUs, the PN shall never repeat for a series of encrypted MPDUs using the same temporal key and TID/ACI." to: "For PV1 MPDUs, the PN shall never repeat for a series of encrypted MPDUs using the same temporal key and PTID/ACI." | Resolution: Revise  Agree with the commentor. Some information about the relevant context is provided in the discussion below.  There are two instances of this statement. The proposal is extended to include both the instances.  TGm Editor: Please make the change as specified in  https://mentor.ieee.org/802.11/dcn/21/11-21-1732-00-000m-cc35-crs-37.docx |

**CID 37**

p2572.38

For PV1 MPDUs, the PN shall never repeat for a series of encrypted MPDUs using the same temporal key and TID/ACI.

For PV1, PN can be reused used for frames using two TIDs but same PTID and this would result in CCM nonce reuse and loss of CCMP security protection.

**Discussion**

CCM Nonce construction uses TID/Priority (p2574.59)

![Graphical user interface, application, table

Description automatically generated]()

PV0 frames construct CCM nonce using TID value for the priority (p2571.28)

PV1 frames have PTID in frame control – PTID is the 3 LSBs of the TID (p1679.5)

PV1 frames use PTID as the priority value in CCM nonce construction (pp2571.60)

For PV1, the statement re: not using the same PN for the same TK/TID might imply that PN could be reused for the same TK/PTID combination.

**Proposed Changes**

TGm Editor Replace TID/ACI with PTID/ as shown below at p2572.38

series of encrypted MPDUs using the same temporal key. For PV1 MPDUs, the PN shall never repeat for a

series of encrypted MPDUs using the same temporal key and PTID/ACI.

TGm Editor Replace TID/ACI with PTID/ as shown below at p2571.42

b) For secure PV1 MPDUs, CCMP encrypts the Frame Body field of a plaintext MPDU and

encapsulates the resulting cipher text using the following steps:

1) When the sequence number of the MPDU is less than the previous sequence number and

satisfies the BPN update conditions in 12.5.3.3.6 (Construct CCMP header for PV1 MPDUs)

for that PTID/ACI, increment the base PN so that the PN never repeats for the same temporal

key and PTID/ACI.