IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CR for CID 1580, CID 2283 and CID 1163 | | | | |
| Date: 2019-04-12 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Feng Jiang | Intel | 3600 Juliette Ln, Santa Clara, CA 95054 |  | feng1.jiang@intel.com |
| Yongho Seok | Mediatek | 2840 Junction Ave, San Jose, CA |  | yongho.seok@mediatek.com |
| Christian Berger | Marvell | 5488 Marvell Ln, Santa Clara, CA, 95054 |  | crberger@marvell.com |
| Qinghua Li | Intel | 3600 Juliette Ln, Santa Clara, CA 95054 |  | qinghua.li@intel.com |

Abstract

This submission addresses the CID 1580, CID 2283 and CID 1163 in TGaz LB240 based on TGaz draft 1.0.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause | Comment | Proposed Change | Resolution |
| 1580 | 116 | 11.22.6.4.6.2 | In the secured TB measurement sequence, assume there are two ISTA taking measurement with the RSTA. The DL NDP include two HE-LTF fields, and in the NDPA frame, the RSTA allocates HE-LTF1 to ISTA1 and allocates HE-LTF2 to ISTA2. An attacker may generate some fake NDPA frame to allocate HE-LTF1 to ISTA2 and allocate HE-LTF2 to ISTA1 and the attacker may transmit the fake NDPA frame to jam the original NDPA frame from RSTA. After ISTA1 and ISTA2 receiving the fake NDPA frame, the ISTA1 will receive the HE-LTF2 of the DL NDP and the ISTA2 will receive the HE-LTF1 of DL NDP. Assume that the RSTA doesn't know the existence of the attacker, and still send the DL NDP with HE-LTF1 for ISTA1 and HE-LTF2 for ISTA2, then the attacker can first copy the HE-LTF1 and replay the HE-LTF1 during the HE-LTF2 to initiate an attack to ISTA1. | This threat model need to be considered and addressed for the security protection purpose. | Revised-  Agree in principle.  To detect a replay attacker specified in the comment, the LMR frame may include the HE-LTF Offset value. If the Offest values in the LMR are not the same with that of the DL NDPA, then there may exist replay attack and the corresponding measurement results shall be ignored.  TGaz editor makes changes as specified in 11-19/0603r2 for CID 1580. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause | Comment | Proposed Change | Resolution |
| 2283 | 25 | 9.3.1.19 | "The Offset subfield can take values between 0 and 63 and indicates the number of HE-LTF to skip when processing the following NDP and is set 0 in all cases except the secure variant of the TB Ranging measurement exchange." Because DL NDPA is an unprotected control frame, the offset value can be altered by a fake DL NDPA transmitted by an attacker. After modifying the offset value of a specific iSTA\_x to a larger value, the attacker can replay the HE-LTF that was intended for iSTA\_x at a later time specified by the altered (i.e., fake) offset to alter the distance measurement of iSTA\_x. This is a security hole in the spec. | Modify the spec to resolve the problem. | Revised-  Agree in principle.  To detect a replay attacker specified in the comment, the LMR frame may include the HE-LTF Offset value. If the Offest values in the LMR are not the same with that of the DL NDPA, then there may exist replay attack and the corresponding measurement results shall be ignored.  TGaz editor makes changes as specified in 11-19/0603r2 for CID 2283. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause | Comment | Proposed Change | Resolution |
| 1163 | 112 | 11.22.6.4.6.2 | TB Secure ranging mode is prone to attack as DL NDP is concatenated to serve multiple users in a TDMA fashion where a skilled attacker can replay NDPA and an NDP by changing the 'the start reference' (i.e. legacy preamble) which is used to identify the corresponding LTF sequence using offset value. | Solution should address this type of attack while one such a solution can be independent NDPA/NDP pair, one per user although it is inefficient but it might be a good tradeoff. | Revised-  Agree in principle.  To detect a replay attacker specified in the comment, the LMR frame may include the HE-LTF Offset value. If the Offest values in the LMR are not the same with that of the DL NDPA, then there may exist replay attack and the corresponding measurement results shall be ignored.  TGaz editor makes changes as specified in 11-19/0603r2 for CID 1163. |

**Discussion**

In the submission IEEE 802.11-19-0461, the replay attack model mentioned in CID 1580, CID 2283, and CID 1163 have been investigated. An example of secured TB ranging sequence is shown in Figure 1.

* For DL NDP, NDPA allocates HE-LTF 1 to ISTA1 and HE-LTF2 to ISTA2.

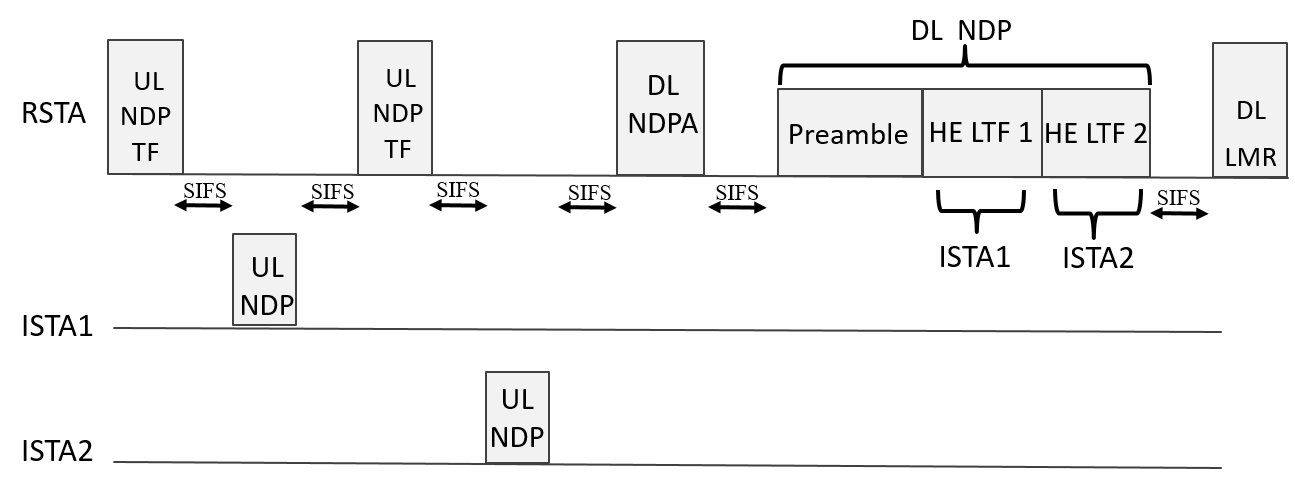


Figure 1 Secured TB Ranging with Two ISTA

The replay attacher is shown in Figure 2.

* Fake NDPA allocates HE-LTF 1 to ISTA2 and HE-LTF2 to ISTA1
* Attacker copies HE-LTF1 of DL NDP and replays HE-LTF1 during HE-LTF2 of DL NDP
* ISTA1’s ToA is attacked and ISTA2 gets an invalid ToA

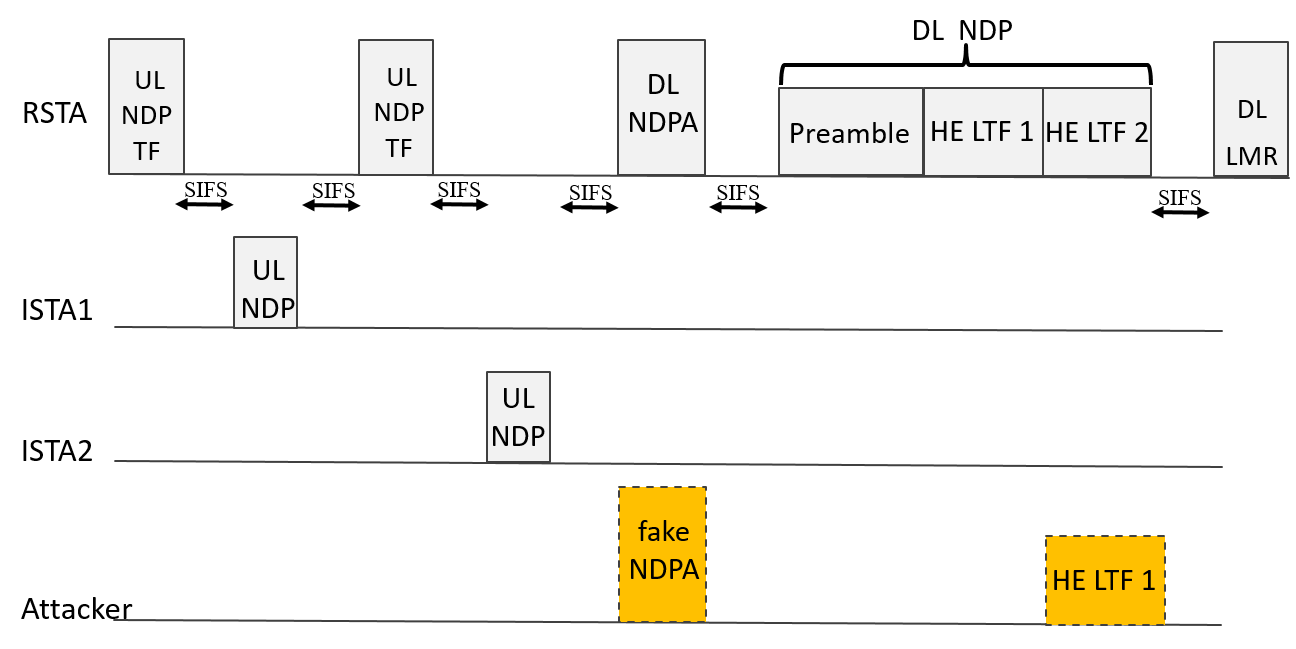


Figure 2 Replay Attacker in Secured TB Ranging

The successfullness of this replay attack depends on that there is no authtentication for the HE-LTF allocation information (Offset value) in the DL NDPA frame. To detect such a replay attacker, the LMR frame can include the HE-LTF Offset value. If the Offest values in the LMR and in DL NDPA are not the same, then there may exist replay attack and the corresponding measurement results shall be ignored.

**Proposed Text Updates for CID 1580, CID 2283 and CID 1163:**

*TGaz Editor: please replace Figure 9-1012 Secure LTF Parameters element format in section 9.4.2.280 Secure LTF Parameters with the following figure.*



Figure 9-1012 Secure LTF Parameters element format

*TGaz Editor: please insert the following paragraph after the last paragraph of section 9.4.2.280 Secure LTF Parameters on page 54 of 11az D1.0*

The Measurement Results LTF Offset field is used to verify that the measurement results of the Location Measurement Report frame in TB Ranging are calculated using the same LTF Offset for HE Ranging NDP beween ISTA and RSTA. The Measurent Result LTF Offset field has the same value as the Offset subfield in the corresponding STA Info field of Ranging NDP Announcement frame preceding the HE Ranging NDP frame, which is used for estimating the measurement results in the Location Measurement Report frame. The Measurement Result LTF Offset field is structured as shown in Figure 9-1012a. This field is not present in the initial Fine Timing Measurement Frame and in the Location Measurement Report Frame in non-TB Ranging.



Figure 9-1012a Measurement Result LTF Offset field format

*TGaz Editor: Please change the first paragraph on page 115 in section 11.22.6.4.6.2 Secure TB ranging mode in 11az D1.0 as below*

When a Location Measurement Report frame contains range measurement results measured from an UL NDP and a DL NDP, a RSTA or ISTA that transmits the RSTA-to-ISTA or ISTA-to-RSTA Location Measurement Report frame shall include the Secure LTF Parameters field in the Location Measurement Report frame and the Range Measurement SAC subfield in the Secure LTF Parameters field in the Location Measurement Report frame to the same value as in the SAC subfield in the Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame that solicited the UL NDP and the DL NDP. The Measurement Result LTF Offset field in the Secure LTF Parameter element in the Location Measurement Report frame shall set to the same value as in the Offset subfield of User Info field in the Ranging NDP Announcement frame that preceds the DL NDP. When an ISTA or RSTA receives RSTA-to-ISTA or ISTA-to-RSTA Location Measuremnt Report frame, the ISTA or RSTA shall compare the value of Measurement Result LTF Offest field with the value of Offset subfield in the corresponding User Info field of Ranging NDP Announcement frame, and if these two values don’t match each other, the ISTA or RSTA shall discard the measurement results carried in the Location Measruemnt Report frame.