IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGaz Meeting Minutes  January 16th-18th, 2018  Irvine, California, USA | | | | |
| Date: 2018-01-16 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Roy Want | Google | 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA | 650-691-3600 | roywant@google.com |

Abstract

Minutes for the TGaz meeting beginning on January 16th, 2018.

**IEEE 802.11 Task Group AZ**

**January 16th-18th, 2018**

1. **TGaz – 16th January, 2018 – Slot #1**
   1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **4.00pm PT**, Vice Chair Carlos Aldana (Intel Corporation) – not attending, Roy Want (Google) Secretary.
   2. Agenda Doc. **IEEE 802.11-18/1843r2**
   3. Review Patent Policy and logistics
      1. Chair reviewed the IEEE-SA Patency Policy, additional guidelines about IEEE-SA meeting and logistics – no clarifications requested.
      2. Chair called for any potentially essential patent, no one stepped up.
      3. Chair reviewed IEEE 802 WG participation as individual professional – no clarification requested.
      4. Chair reminded all to record their attendance
      5. Recorded Participation requirement
         1. Headcount: ~22 present
   4. Review Agenda
      1. Called for any additional submissions for the week.
      2. Reviewed and modified the agenda
      3. The group agreed to have a 5th group meeting slot for the week in addition to the 4 planned.
      4. Chair called for any additional feedback and changes to agenda.
      5. **Motion: We approve the agenda for document 11-18/1843r2**
         1. **Approved** by unanimous consent
   5. Approve previous meeting minutes (posted Nov 17th, 2017 updated Jan 1st, 2018)
      1. Roy Want (Google) reviewed November Meeting Minutes **11-17/1757r1**
         1. **Motion: Move to approve document 11-17-1757r1 as TG meeting minutes for the Nov meeting**
         2. Mover: Roy Want, Seconder: Chou Chen.
         3. Discussion of the motion: none
         4. **Results:** Y: 17, N: 0, A: 1; **motion passes**
      2. Roy Want (Google) reviewed Dec 20th Telecon Minutes **11-17/1892r0** posted on Jan 7th, 2018
         1. **Motion: Move to approve document 11-17-1892r0 as TG meeting minutes for the Dec 20th Telecon.**
         2. Mover: Roy Want, Seconder: Assaf Kasher
         3. Discussion of the motion: none
         4. **Results:** Y: 17, N: 0, A: 1; **motion passes**

* 1. Review of SFD Working Draft **11-17/0462r11** presented by Choa Chun Wang (MediaTek) **r10** posted on 9th Nov 2018, posted **r11** on 7th Jan 2018.
     1. ‘Or’ to ‘Nor’ updated for LMR … (2 places)
     2. C. Noted that there are two (5)s in the list
        1. R. list will be corrected later.
     3. Will clean up and remove the angular arrival / departure text from the general description. This will only be associated with the 60GHz text in the future.
  2. Assaf Kasher (Qualcomm) presented document **11-18/0140r0**
     1. Title: **60GHz Direction Measurement SFD text**
     2. Summary: proposes the changes required to the SFD to enable angle of arrival and departure measurement for location estimation in 60GHz.
     3. Discussion of presentation:
        1. C. We need to resolve the terminology here for 60Hz with the other sections of the SFD text e.g DMG, EDMG.
     4. **Strawpoll:  
        Do you agree to add to the SFD?  
         The capabilities element as defined in slide 6**

**The measurement parameters as defined in slide 9**

**The AOA results element as defined in slide 12**

* + 1. Discussion of strawpoll: None.
    2. **Results:** Y:16, N: 0, A: 3.
    3. **Motion:  
       Move to adopt the set of spec framework requirements listed in slides 6, 9 and 12 of submission 11-18-140r0 and instruct the SFD editor to include it in the TGaz SFD under the section 4 (Positioning Protocol while operating in the 60GHz band) and grant editorial license to 11az editor.**
    4. Mover: Assaf Kasher, Seconder: Ganesh Venkatesan
    5. **Results:** Y: 12, N: 0, A: 2; **motion passes**.
  1. Feng Jiang (Intel Corporation) presented document **11-18/0208r0**
     1. Title: **Replay Attack Detection Using LTF with Zero Prefix**
     2. Summary: To avoid the CP-replay attack, Mingguang proposed to use zero-padded waveform for channel estimation; Option (1): Zero prefix + core symbol + zero postfix; Option (2): Zero prefix + core symbol. We propose an energy detector for option (2) for detecting a replay attack, and provide a complexity analysis and simulation of performance.
     3. Conclusion: (1) An energy detector is proposed for detecting the replay attack to the LTF with zero prefix; (2) Simulation results show that for SIR as high as 15dB, the probability of miss detecting the ‘bad’ channel is almost 0; 3) The complexity of the energy detector can be reduced through setting a smaller window for energy calculation or selecting the large enough taps for LTF subtraction; 4) Future work includes evaluating the detection performance using the more realistic 11n data channel.
     4. Discussion of presentation:
        1. C. Implementation (s8). Do you have to estimate the SNR first?
        2. R. Yes.
        3. C. If attacker can interfere with the noise estimation, it could interfere with the attack detection.
        4. R. Could use a fixed SNR threshold value instead.
        5. C. Then the energy detection process will not perform well.
        6. R. Could use a small SNR threshold value to be safe.
        7. C. There is a danger the false trigger is too high – but it’s a trade off, and we have some performance concerns about this.
        8. C. On slide 9. Don’t have time to do two FFTs except on last symbol.
        9. C. Slide 11 peaks fall exactly on channel taps. Generally, they spread over the channels.
        10. R. Simulation was designed this way.
        11. C. You might see the effects of adjoining taps in further evaluation.
  2. Mingguang Xu (Apple) presented document **11-18/0222r0**
     1. Title: **Consistency Check Across Multiple Channel Estimates**
     2. Summary: The FRD describes Type A and Type B adversaries that are characterized according to the attacker’s response time. A CP Relay attack is an example of a Type A attack. Consider how to combat noise + a jammer. Possible solution: “Consistency check” across multiple channel estimates within the channel coherence time.
     3. **Strawpoll #1:  
        For operation in the sub 7GHz and 60GHz bands, do you agree to add support for transmission of multiple zero padded waveforms in a single packet for channel estimation in a single Tx antenna case?**
     4. Discussion of presentation and strawpoll
        1. C. Please clarify multiple zero padded waveform
        2. R. For a consistency check the channel needs to be estimated twice (slide 7).
     5. **Results**: Y: 19, N: 0, A: 4
     6. Converted to a motion
     7. **Motion #1;**
     8. **Move to adopt the set of spec framework requirements listed below instruct the SFD editor to include it in the TGaz SFD under the sub-section 6 (security) for the .11az protocol:**

**“For operation in the sub 7Ghz and 60Ghz bands, multiple zero padded waveforms in a single packet shall be transmitted for channel estimation in a single Tx antenna case.”**

* + 1. Mover: Assaf Kasher, Seconder: SK Yong
    2. **Results**: Y: 12, N: 0, A: 2; **motion passes**.
  1. Reminder to do attendance
  2. At recess 5.59pm.

1. **TGaz – 17th Jan, 2018 – Slot #2**
   1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **8.00am PT**; Vice Chair, Carlos Aldana (Intel Corporation) – not present; Roy Want (Google) Secretary.
   2. Agenda Doc. **Now working revision at 11-17/1843r3**
   3. Review Patent Policy and logistics
      1. Chair reviewed the IEEE-SA Patency Policy, additional guidelines about IEEE-SA meeting and logistics – no clarifications requested.
      2. Chair called for any potentially essential patent, no one stepped up.
      3. Chair reviewed IEEE 802 WG participation as individual professional – no clarification requested.
      4. Chair reminded all to record their attendance
      5. Recorded Participation requirement
         1. Headcount: ~24 present
   4. Reviewed submission order and updated agenda
      1. Updated agenda presentation order and feedback requested: none received
      2. Approved agenda.
   5. SK Yong (Apple) cont. presentation of document **11-18/0222r0** – Mingguang being unavailable this morning.
      1. **Strawpoll #2:**  
         **For operation in the sub 7GHz band, do you agree to support transmission of multiple P-matrix encoded and zero padded training symbol sets in a single packet to enable multiple channel estimates in a multiple Tx antenna case?**
      2. **Results**:  Y:  19    N:  0    A:  6
      3. Converted to a motion.
      4. **Motion #2 (proposed):**

**Move to adopt the set of spec framework requirements listed below instruct the SFD editor to include it in the TGaz SFD under the sub-section 6 (security) for the .11az protocol and grant editorial license to 11az editor.**

**“For operation in the sub 7GHz band, multiple P-matrix encoded and zero padded training symbol sets in a single packet shall be transmitted to enable multiple channel estimates in a multiple Tx antenna case.”**

* + 1. Discussion of motion
       1. C. Should it be ‘may’ rather than ‘shall’. Amount of data in a 4x4 case would be considerable if mandated.
       2. R. Yes – okay with ‘may’.
       3. C. Perhaps for the 2x2 case it could be ‘shall’ and for greater antenna dimensions, e.g. in the 4x4 case it would be negotiated.
       4. C. Need to add language that 2 antennas imply two P-matrix and zero padded symbol sets.
    2. **Motion #2 (final):**

**Move to adopt the set of spec framework requirements listed below instruct the SFD editor to include it in the TGaz SFD under the sub-section 6 (security) for the .11az protocol and grant editorial license to 11az editor.**

**“For operation in the sub 7GHz band, multiple P-matrix encoded and zero padded training symbol sets in a single packet shall be transmitted to enable multiple channel estimates in a multiple Tx antenna case if negotiated during ranging session negotiation. At least two Tx antennas, i.e. two P-matrix encoded and zero padded symbol sets, shall be supported.”**

* + 1. Mover: SK Yong, Seconder: Nehru Bhandaru
    2. **Results:** Y: 12, N: 0: A: 5; **motion passes**
  1. Review (continued) of SFD Working Draft **11-17/0462r12** presented by Choa Chun Wang (MediaTek)
     1. Frame format in section 7: discussion of possible move of behavioral description to section 3.2, but decided not to change this.
     2. Discussion: None.
     3. **Motion  
        Move to adopt document 11-17-462r12 as TGaz Spec Framework working draft document.**

Mover: Chao Chun Wang, Seconder: Assaf Kasher

* + 1. **Results:** Y: 18, N: 0, A: 1; **motion passes**
  1. Nehru Bhandaru (Broadcom) presented document **11-17/1879r1**
     1. Title**: Pre-association Security Negotiation for 11az SFD Follow up**
     2. Summary: Considering discussion items that were surfaced in version 0.
     3. Discussion: none
     4. **Motion**

**Move to adopt the following text in the TGaz SFD under Section 6 – Security - and grant the SFD editor editorial license:**

**• Pre-association Security Negotiation (PASN) authentication allows message authentication, encryption, and message integrity to be provided for selected 802.11 frames that require such protection.**

**• Whether such protection is required for a frame is determined by the security parameters negotiated for the exchange (e.g. 11az Protocol Negotiation) to which the frame belongs.**

**• An AP indicates PASN support by advertising a [TBD] PASN AKM in RSNIE that is included in Beacons and Probe Responses, and also in neighbor reports and reduced neighbor reports where supported.**

**• A non-AP STA selects use of PASN authentication based on the security requirements of features that need pre-association security. 11az protocol security for an un-associated STA requires PASN.**

**• A non-AP STA and an AP use 802.11 authentication frames with the Authentication algorithm number set to [TBD] (PASN Authentication) for the protocol exchange.**

**• A non-AP STA optionally, via PASN protocol, proposes to an AP a base AKM and PMKID(s) used to identify the PMK used for derivation of PTK for key confirmation and frame protection.**

**• An AP optionally, via PASN protocol, indicates to the non-AP STA, a base AKM and PMKID corresponding to the PMK used for derivation of PTK for key confirmation and frame protection.**

**• PASN protocol allows a FILS base AKM using shared key (See 12.12.2.3 of [1])**

**• PASN protocol allows any base protocol with a PMK – e.g. FT base AKM using PMKr1**

**• A non-AP STA and AP exchange ephemeral public keys to derive protection keys via PASN.**

**• The PTK for the exchange is derived from PMK, if any, and the shared secret from the ephemeral key exchange.**

**• If 11az measurement security for type A or type B attackers is required, the IEEE 802.11az negotiation protocol and measurement reports shall be integrity protected and encrypted for privacy.**

**• If 11az measurement security for type B attacker is required, the fields over which measurements are performed shall be protected (e.g. LTF sequence derived using the keys from PASN protocol).**

* + 1. Discussion of motion: none
    2. Mover: Nehru Bhandaru; Seconder: Chao Chun Wang
    3. **Results:** Y: 15, N: 0, A: 3; **motion passes**
  1. Chao Chun Wang (MediaTek) presented **11-17/0235r0**
     1. Title: **Amendment text submissions formatting conventions**
     2. Summary: To facilitate the development of 11ax amendment, it is preferable that all submissions follow the same formatting convention
     3. Discussion of presentation
        1. C. How do you want to refer to SFD text?
        2. R. For all the differences, put brackets before the changes and list the clause number.
        3. C. Pleas clarify the editing process.
        4. R. Edits: Additions: Blue underline, Deletions: Red strike-through. In revision modifications use track changes.
        5. C. Do we have a document editing guideline from 802.11?
        6. R. There are no official rules how to do this (it’s a suggestion for 11az).
        7. C: do figures needs to follow specific format?
        8. R: Figures should be in vision format embedded in the word text document.
     4. **Guideline by the chair to follow these conventions for all submissions of SFD amendment text.**
  2. Assaf Kasser (Qualcomm) **continued** presentation of document **11-17/1884r1**
     1. Title: **First Path FTM SFD Text**
     2. Summary:This presentation proposes the protocol and signaling needed to enable first path usage with the FTM protocol.
     3. Submission reviewed during the Dec. 20th telecon.
     4. Executing the motion informed by earlier strawpoll in Dec 20th Telecon.
     5. Discussion: none
     6. **Motion**

**Move to adopt the set of SFD requirements depicted in slide 6 of submission 11-17-1884r1 to the TGaz SFD document under Section 4 (60GHz Positioning Protocol) and grant the SFD editor editorial license.**

* + 1. Mover: Assaf Kasher, Seconder: SK Yong
    2. **Results**: Y: 15, N: 0 A: 1; **motion passes**
  1. Reminder to do attendance
  2. Recess at 9.55am (returning 5mins to the group).

1. **TGaz – 17th Jan, 2018 – Slot #3**
   1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **1.30pm PT**; Vice Chair, Carlos Aldana (Intel Corporation) – not present; Roy Want (Google) Secretary.
   2. Agenda Doc. **Now working revision is at 11-17/1843r4**
   3. Review Patent Policy and logistics
      1. Chair reviewed the IEEE-SA Patency Policy, additional guidelines about IEEE-SA meeting and logistics – no clarifications requested.
      2. Chair called for any potentially essential patent, no one stepped up.
      3. Chair reviewed IEEE 802 WG participation as individual professional – no clarification requested.
      4. Chair reminded all to record their attendance
      5. Recorded Participation requirement
         1. Headcount: ~25 Present
   4. Reviewed submission order and updated agenda
      1. Allocated an additional slot on Thursday: AM2 (total of 5 slots)
      2. Updated agenda presentation order and feedback requested: none received
      3. Approved agenda.
   5. Chou Chan (MediaTek) presented document **11-18/0236r0** informed by **11-18/1171r1** November 2017 minutes
      1. Title: **802.11az Negotiation Protocol (relative to REVmd D0.5)**
      2. Summary: Summarized the additional edits made (Blue) to the document and the deletions (Red) to date.
      3. Volunteers for amendment text:
         1. Assaf Kasser: **Section 4. 60GHz ranging**
         2. Christian Berger: section VHTz **Section 6. Security**
         3. Ganesh Venkatesan: **Section 3.2.1** negotiation
         4. Jonathan Segev: 3.2.3 HEz protocol description
         5. SK Yong: **Section 6. PHY Security**
   6. Mingguang Xu (Apple) presented document **11-18/0223r0**
      1. Title: **Performance Evaluation on Zero-Padded Waveform**
      2. Summary: Zero-padded waveform and random sequence shall be used for ranging measurement in the Security Mode to protect against PHY-level attacks. This contribution provides numerical results for evaluating different types of zero-padded waveforms.
      3. C. slide 11: on the receive side we may be able to do better.
      4. R. Transform pilot sequence 256 points with 256 zeros.
      5. C. Keep 256 points with BPSK modulated symbols – then there is no reason to use the pi/2 offset. Performance may be just as good (but will take this offline to discuss further).
      6. **Strawpoll #1  
         For VHTz and HEz, we prefer the design of Null CP on the Tx side only, and have an implementation specific Rx FFT size (i.e. not specified by the standard).**
      7. **Results:** Y: 11, N: 0, A: 10
      8. Converted to a motion.
      9. **Motion #1**

**Move to adopt the set of spec framework requirements listed below, instruct the SFD editor to include it in the TGaz SFD under the sub-section 6 (security) for the .11az protocol and grant editorial license to SFD editor.**

**“For VHTz and HEz, the secured PHY VHT and HE LTF shall have a Null GI on the Tx side only, and have an implementation specific Rx FFT size (i.e. not specified by the standard).”**

* + 1. Discussion of motion:
       1. C: Edit addition: PHY VHT and HE LTF
       2. R. Edited (in final motion shown above)
    2. Mover: SK Yong, Seconder: Erik Lindskog
    3. **Results**: Y:7, N: 0, A: 5; **motion passes**
    4. **Strawpoll #2**:  
       **For DMGz and EDMGz secured PHY TRN field we prefer the design of Null GI on the Tx side only, and have the receive processing stay unchanged (e.g., Rx FFT size).  For example:   GI is 72ns, core symbol is 218ns.**

**–For DMGz, Lzero pad=128, Lcore=384, and NFFT,rx=512;**

**–For EDMGz with channel bonding: Lzero pad =128\*nCB, Lcore=384\*nCB, and NFFT, rx=512\*nCB.**

* + 1. Discussion of Strawpoll
       1. C. We don’t have Lzero pad = 128 in 60GHz
       2. R: Final strawpoll modified as shown above.
    2. **Results**: Y: 12, N: 0, A: 5.
    3. Converted to a motion.
    4. **Motion #2  
       Move to adopt the set of spec framework requirements listed below, instruct the SFD editor to include it in the TGaz SFD under the section 6 (security) for the .11az protocol and grant editorial license to the SFD editor.**

**“The DMGz and EDMGz secured PHY TRN field shall have a Null GI on the Tx side only, and the receive processing shall remain unchanged (e.g., Rx FFT size).  For example:   GI is 72ns, core symbol is 218ns.**

**–For DMGz, Lzero pad=128, Lcore=384, and NFFT, rx=512;**

**–For EDMGz with channel bonding: Lzero pad=128\*NCB, Lcore=384\*NCB, and NFFT, rx=512\*NCB.”**

* + 1. Mover: SK Yong, Seconder: Assaf Kasher
    2. **Results**: Y: 7, N: 0; A: 4; **motion passes**.
    3. Discussion
       1. C. There is one additional strawpoll to consider.
    4. **Strawpoll #3**

**For secure ranging over the 60GHz band, do you agree to use SC-PHY with zero padded waveforms included in the TRN field as shown in slide 7 of submission 11-28-223r0?**

* + 1. Discussion
       1. C. We need the presentation number in the strawpoll
       2. R. Now added in strawpoll text.
    2. **Results:** Y: 13, N: 0, A: 1.
    3. Converted to a motion
    4. **Motion #3**

**Move to adopt the set of spec framework requirements listed below, instruct the SFD editor to include it in the TGaz SFD under the section 6 (security) for the .11az protocol and grant editorial license to the SFD editor:**

**“For secure ranging over the 60GHz band, a SC-PHY mode with zero padded waveforms included in the TRN field shall be used as shown in slide 7 of 11/18-0223r0”**

* + 1. Mover: SK Yong, Seconder: Assaf Kasher
    2. **Results**: Y: 8, N: 0, A: 1; **motion passes**
  1. Ganesh Venkatesan (Intel Corporation) presented **11-18/0215r1**
     1. Title: **802.11az Negotiation Protocol relate to REVmd DO-.4**
     2. Summary: Listing main new additions appearing in 11-18/0215r1
        1. Added figures 6-17a and 6-17b.
        2. Added MLME parameters: 5-parameters described in table
        3. Corresponding indication also has 5-parameters, and described in the table below.
        4. Add Table 9.77 for the 5-parameters added (tentatively labelled extensible)
        5. NGP Parameter section description added (various)
        6. VHTz Specific Parameters
        7. HEz Specific Parameters
        8. DMGz & EDMG Specific Parameters (to be fleshed out later)
        9. FTM Request Frame format.
        10. FTM Procedure overview
        11. FTM Capabilities (SU and MU should be changed to VHTz and HEz terms – updates coming).
  2. Reminder to do attendance
  3. Recess at 3.29pm.

1. **TGaz – 18th Jan, 2018 – Slot #4**
   1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **8.00am PT**; Vice Chair, Carlos Aldana (Intel Corporation) – not present; Roy Want (Google) Secretary.
   2. Agenda Doc. **Now working revision at 11-17/1843r5**
   3. Review Patent Policy and logistics
      1. Chair reviewed the IEEE-SA Patency Policy, additional guidelines about IEEE-SA meeting and logistics – no clarifications requested.
      2. Chair called for any potentially essential patent, no one stepped up.
      3. Chair reviewed IEEE 802 WG participation as individual professional – no clarification requested.
      4. Chair reminded all to record their attendance
      5. Recorded Participation requirement
         1. Headcount: ~24 present
   4. Reviewed submission order and updated agenda
      1. Updated agenda presentation order and feedback requested: none received
      2. Approved agenda.
   5. Chitto Ghosh (Intel Corporation) presented document **11-18/0229r1** part 1(SU), Yongho Seok (MediaTek) presented part 2 (MU):
      1. Title: **Secure SU and MU Ranging Measurement Procedure**
      2. Summary: In previous discussions, 11az has agreed: (1) In HEz and VHTz FTM modes, the fields over which range measurements are performed shall be protected against a VHT/HE Type B adversary attack; (2) For the purpose of PHY Security Mode, the field used for channel/ToA measurement shall not include any form of repetition in time domain or structure that is predictable. This presentation proposes how to signal between the iSTA and rSTA to enable LTF protection.
      3. Discussion: none
      4. **Strawpoll #1**

**Do you support the following SFD texts for secure VHTz ranging measurement?**

**For normal operation of secure VHTz ranging:**

**–The keys or cipher sequence (if needed) for LTF sequence generation are the result of the FTM negotiation**

**–Sequence generation information for the first measurement instance is part of the IFTM, the measurement phase only commences once the negotiation is successful**

**–The frame used to deliver subsequent LTF sequence generation information is the protected LMR frame**

**–The specifics of LTF sequence generation information is TBD, this information is associated with a Sequence Authentication Code (SAC).**

**–The NDPA carries the SAC indication, a specific reserved value indicates “New LTF generation information is needed”. The SAC is also included in the IFTM for the first measurement instance and in the LMR for subsequent measurement instances.**

* + 1. **Results:** Y: 21 N: 0 Y: 3
    2. Converted to a motion.
    3. **Motion #1**

**Move to adopt the following SFD text, instruct the editor to include it in the 11az SFD and grant editorial license to the editor:**

**“For normal operation of secure VHTz ranging:**

**–The keys or cipher sequence (if needed) for LTF sequence generation are the result of the FTM negotiation**

**–Sequence generation information for the first measurement instance is part of the IFTM, the measurement phase only commences once the negotiation is successful**

**–The frame used to deliver subsequent LTF sequence generation information is the protected LMR frame**

**–The specifics of LTF sequence generation information is TBD, this information is associated with a Sequence Authentication Code (SAC).**

**–The NDPA carries the SAC indication; a specific reserved value indicates “New LTF generation information is needed”. The SAC is also included in the IFTM for the first measurement instance and in the LMR for subsequent measurement instances.”**

* + 1. Discussion of motion: none.
    2. Mover: Chitto Ghosh, Seconder: Yongho Seok
    3. **Results** Y: 17, N:0, A: 3; **motion passes**
    4. **Strawpoll #2**

**Do you support the following SFD text for secure VHTz ranging measurement (SAC operation)?**

**–The size of the SAC should be sufficiently long to prevent simple guessing**

**–An adversary doesn’t know the SAC and is unable to predict it and thus can’t trigger the measurement instance (DOS). In addition the SAC and its associated measurement results are carried in the LMR.**

**–If an incorrect SAC is received by the RSTA, the RSTA discards the NDPA (no DL NDP) and keep the current SAC and associated LTF sequence generation information.**

* + 1. **Results**: Y: 22, N:0, A: 1.
    2. Converted to a Motion
    3. **Motion #2**

**Move to adopt the following SFD text, instruct the editor to include it in the 11az SFD and grant editorial license to the editor:**

**“For secure VHTz ranging measurement (SAC operation):**

**–The size of the SAC should be sufficiently long to prevent simple guessing**

**–An adversary doesn’t know the SAC and is unable to predict it and thus can’t trigger the measurement instance (DOS). In addition the SAC and its associated measurement results are carried in the LMR.**

**–If an incorrect SAC is received by the RSTA, the RSTA discards the NDPA (no DL NDP) and keep the current SAC and associated LTF sequence generation information.**

* + 1. Mover: Chitto Ghosh
    2. Seconder: Yongho Seok
    3. **Results:** Y: 19, N: 0, A: 1; **motion passes**
    4. **Strawpoll #3**

**• Do you support the following SFD texts for secure VHTz ranging measurement (LMR error recovery operation)?**

**–The LMR is an Action No ACK frame**

**–If the LMR was not correctly received:**

* **The iSTA comes back to the channel and transmit an NDPA indicating “New LTF generation information is needed”. The previous LTF generation information is invalidated.**
* **For UL NDP the iSTA uses a known UL NDP LTF sequence (not suitable for measurement).**
* **For DL NDP the rSTA may use the secured DL NDP LTF sequence (not suitable for measurement).**
* **The rSTA sends a new PMF protected LMR frame with a new SAC and new sequence generation information (measurements results included in the LMR are invalid only for the immediate VHTz case).**
* **The iSTA may come back to the channel and initiate a new sounding sequence minToaReady time after.**
  + 1. **Results** Y: 18, N: 0, A: 0.
    2. Converted to a motion.
    3. **Motion #3**

**Move to adopt the following SFD text, instruct the editor to include it in the 11az SFD, and grant editorial license to the editor:**

**“For secure VHTz ranging measurement (LMR error recovery operation):**

**–The LMR is an Action No ACK frame**

**–If the LMR was not correctly received:**

* + **The iSTA comes back to the channel and transmit an NDPA indicating “New LTF generation information is needed”. The previous LTF generation information is invalidated.**
  + **For UL NDP the iSTA uses a known UL NDP LTF sequence (not suitable for measurement).**
  + **For DL NDP the rSTA may use the secured DL NDP LTF sequence (not suitable for measurement).**
  + **The rSTA sends a new PMF protected LMR frame with a new SAC and new sequence generation information (measurements results included in the LMR are invalid only for the immediate VHTz case).**
  + **The iSTA may come back to the channel and initiate a new sounding sequence minToaReady time after.”**
    1. Mover: Chitto Ghosh, Seconder: Yongho Seok
    2. **Results:** Y: 14, N: 0, A: 1; **motion passes**
    3. **Strawpoll #4**

**• Do you support the following SFD texts for secure HEz ranging measurement (general operation)?**

**–For normal operation of secure HEz ranging,**

**–Secure HEz ranging measurement procedure is limited to a single ISTA (extension to multiple ISTA is TBD):**

**–The delayed sequence generation where sequence generation information is carried in the previous sounding sequence instance.**

**–The keys or cipher sequence (if needed) for LTF sequence generation are the result of the FTM negotiation.**

**–LTF sequence generation information for the first measurement instance is a part of an IFTM, the measurement phase only commences once the negotiation is successful.**

**–The frame used to deliver subsequent LTF sequence generation information is the protected LMR frame.**

* + 1. **Results:** Y: 17, N: 0, A: 1.
    2. Converted to a Motion.
    3. **Motion #4**

**Move to adopt the following SFD text, instruct the editor to include it in the 11az SFD and grant editorial license to the editor:**

**For secure HEz ranging measurement (general operation):**

**–Secure HEz ranging measurement procedure is limited to a single ISTA (extension to multiple ISTAs is TBD):**

**–The delayed sequence generation where sequence generation information is carried in the previous sounding sequence instance.**

**–The keys or cipher sequence (if needed) for LTF sequence generation are the result of the FTM negotiation.**

**–LTF sequence generation information for the first measurement instance is a part of an IFTM, the measurement phase only commences once the negotiation is successful.**

**–The frame used to deliver subsequent LTF sequence generation information is the protected LMR frame.**

* + 1. Mover: Yongho Seok, Seconder: Chitto Ghosh.
    2. **Results:** Y: 13, N: 0, A: 1; **motion passes**
    3. **Strawpoll #5**

**Do you support the following SFD texts for secure HEz ranging measurement (normal operation)?**

**–The specifics of LTF sequence generation information are TBD, but this information is associated with a Sequence Authentication Code (SAC).**

**–The Trigger Frame (TF) -> Location Uplink Sounding indicates the SAC for the following NDP frame corresponding to the LTF generation information.**

**–The SAC is also included in the IFTM for the first measurement instance and in the LMR for subsequent measurement instances.**

**–An adversary doesn’t know the SAC and is unable to predict it.**

**–In addition, the SAC and its associated measurement results are carried in the LMR.**

**–If an incorrect SAC is received by the ISTA, the ISTA may respond with a known LTF sequence or with any other LTF sequence and discards the current SAC and associated LTF sequence generation information.**

**–The size of the SAC should be sufficiently long to prevent simple guessing.**

* + 1. **Results** Y: 19, N: 0, A: 1
    2. Converted to a motion.
    3. **Motion #5**

**Move to adopt the following SFD text, instruct the editor to include it in the 11azSFD and grant editorial license to the editor:**

**“For secure HEz ranging measurement (normal operation):**

**–The specifics of LTF sequence generation information are TBD, but this information is associated with a Sequence Authentication Code (SAC).**

**–The Trigger Frame (TF) -> Location Uplink Sounding indicates the SAC for the following NDP frame corresponding to the LTF generation information.**

**–The SAC is also included in the IFTM for the first measurement instance and in the LMR for subsequent measurement instances.**

**–An adversary doesn’t know the SAC and is unable to predict it.**

**–In addition, the SAC and its associated measurement results are carried in the LMR.**

**–If an incorrect SAC is received by the ISTA, the ISTA may respond with a known LTF sequence or with any other LTF sequence and discards the current SAC and associated LTF sequence generation information.**

**–The size of the SAC should be sufficiently long to prevent simple guessing.”**

* + 1. Mover: Yongho Seok, Seconder: Chitto Ghosh.
    2. **Results** Y: 12, N: 0, A: 1; **motion passes**.
    3. **Strawpoll #6**

**Do you support the following SFD texts for secure HEz ranging measurement (LMR error recovery operation)?**

**– The LMR is an Action No ACK frame**

**– If the LMR was not correctly received:**

**• For UL NDP, the ISTA uses a known UL NDP LTF sequence (not suitable for measurement).**

**• For DL NDP, the RSTA may use the secured DL NDP LTF sequence (not suitable for measurement).**

**• If two sided LMR is used, the ISTA indicates measurements are invalidated.**

**• The RSTA sends a new PMF protected LMR frame with a new SAC and new sequence generation information (measurements results included in the LMR are invalid only for the immediate HEz case).**

**• The ISTA may come back to the channel and participate in a new sounding sequence at the next availability interval by responding to a future TF Location -> Poll.**

* + 1. **Results**: Y: 15, N: 0, A: 0
    2. Converted to a motion.
    3. **Motion #6**

**Move to adopt the following SFD text, instruct the editor to include it in the 11az SFD and grant editorial license to the editor:**

**For secure HEz ranging measurement (LMR error recovery operation):**

**–The LMR is an Action No ACK frame**

**–If the LMR was not correctly received:**

**• For UL NDP, the ISTA uses a known UL NDP LTF sequence (not suitable for measurement).**

**• For DL NDP, the RSTA may use the secured DL NDP LTF sequence (not suitable for measurement).**

**• If two sided LMR is used, the ISTA indicates measurements are invalidated.**

**• The RSTA sends a new PMF protected LMR frame with a new SAC and new sequence generation information (measurements results included in the LMR are invalid only for the immediate HEz case).**

**• The ISTA may come back to the channel and participate in a new sounding sequence at the next availability interval by responding to a future TF Location -> Poll.**

* + 1. Mover: Yongho Seok, Seconder: Chitto Ghosh.
    2. **Results**: Y: 11, N: 0, A: 0; **motion passes**
  1. Ganesh Venkatesan (Intel Corporation) presented WIP document **11-18/0215r1** with edits presented yesterday, and now uploaded to mentor.
     1. Any questions on document from yesterday: None
     2. Summary of main changes:
        1. SU –> VHTz ranging
        2. MU –> HEz ranging
        3. Text for description of additional parameters in FTM ranging. Negotiation protocol.
        4. Measurement exchange placeholders will be replaced by sections currently presented to TGaz and approved.
  2. Qinghua Li (Intel Corporation) presented document **11-18/0209r0**
     1. Title: **Long Token for Secure Ranging**
     2. Summary: Existing token is 6-bits long. After 64 measurements, the token may repeat. Attacker may replay recorded LMR with the same token to make an attack. So the token needs to be extended.
     3. Discussion:
        1. C. Does PMF have its own sequence number?
        2. R. Depends on the strategy for updating the PM number.
        3. C. Similar question: Is token inserted into PHY or MAC layer?
        4. R. MAC layer.
        5. C. Using the PM counter may solve this issue.
        6. R. Counter is replayed along with the associated LMF.
        7. C. Consider complexity
        8. C. Where do the 6 bits come from?
        9. R. From the measurement token (8 bits with 2 bits reserved)
        10. C. Not sure how this attack would work. The SAC would take care of this.
        11. C. The suggested16 bits is not enough, as with a location estimate once per second, it would wrap in 18hrs.
        12. R. 48-bits would cover it (agreed).

1. **TGaz – 18th Jan, 2018 – Slot #5**
   1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **4.00pm PT**; Vice Chair, Carlos Aldana (Intel Corporation) – not present; Roy Want (Google) Secretary.
   2. Agenda Doc. **Now working revision at 11-17/1843r7**
   3. Review Patent Policy and logistics
      1. Chair reviewed the IEEE-SA Patency Policy, additional guidelines about IEEE-SA meeting and logistics – no clarifications requested.
      2. Chair called for any potentially essential patent, no one stepped up.
      3. Chair reviewed IEEE 802 WG participation as individual professional – no clarification requested.
      4. Chair reminded all to record their attendance
      5. Recorded Participation requirement
         1. Headcount: ~12 present
   4. Reviewed submission order and updated agenda
      1. Updated agenda presentation order and feedback requested: none received
      2. Agenda agreed.
   5. Alan Zhu (Huawei) Amendment Text. presented document **11-18/0207r1**
      1. Title: **802.11az VHTz Measurement Exchange Protocol**
      2. Summary changes listed that have questions (edits made in r2):
         1. Measurement Exchange Sequence.
         2. C: Optionally, LMR feedback calculation (ToA) and its delivery may require a scheduling mechanism (TBD: what is it? Should we define it, or we consider it out-of-scope?).
         3. R: believe this was an early discussion of the protocol development stage, later on deprecated as discussion and clarity moved advanced.
         4. R. We should remove it up to the end of the sentence **–** not needed anymore (and remove from SFD).
         5. C: When using delayed reporting in VHTz mode, an iSTA shall not initiate a subsequent measurement sequence earlier than MinToaReady after receiving the current LMR (Okay?)
         6. R: Change to ‘…channel sounding’.
         7. R: TBD: make sure to define MinToaReady and MaxToaAvailable.
         8. C: (from Editor): The form of report used is agreed upon during negotiation phase (TBD: did we already cover this?).
         9. R: Postponed (need additional input from group).
      3. Next steps: give this text to Choa Chun Wang (Editor) to be included in D.0.1 Spec of Amendment Text.
   6. Eitan Alecsander (Qualcomm) presented document **11-18/0220r1**
      1. Title: **60GHz Passive Location**
      2. Summary: This presentation presents various concepts of passive location in the 60GHz band.
      3. C. Why don’t you transmit omni-directionally in opt 2?
      4. R. It’s a trade-off of power vs number of antennas.
   7. Chair reviewed status of 11az in **11-18/1843r7**
      1. Reviewed current timelines
         1. Next milestone Draft D0.1 out in March 2018 meeting.
      2. Reviewed achievements of January Meeting.
      3. Goals for March Meeting.
      4. **Motion**

**We commit for the March meeting goals as the TG Plan of Record.**

* + 1. Mover: Roy Want, Seconder: Erik Lindskog.
    2. Results: Y: 10, N: 0, A: 0; **motion passes**
    3. Proposal: **Telecons planned on: Wed Feb 21st and Wed Feb 28th**
       1. **No objections**
    4. Reminder to do attendance.
    5. Any other business? None
    6. Adjourn at 5pm.

**References:**

1. <https://mentor.ieee.org/802.11/dcn/17/11-17-1843-07-00az-tgaz-jan-agenda.pptx>
2. <https://mentor.ieee.org/802.11/dcn/17/11-17-1757-01-00az-meeting-minutes-november-2017-session.docx>
3. <https://mentor.ieee.org/802.11/dcn/17/11-17-1892-00-00az-tgaz-teleconference-minutes-dec-20th-2017.docx>
4. <https://mentor.ieee.org/802.11/dcn/17/11-17-0462-12-00az-11-az-tg-sfd.doc>
5. <https://mentor.ieee.org/802.11/dcn/18/11-18-0140-00-00az-60ghz-direction-measurement-sfd-text.pptx>
6. <https://mentor.ieee.org/802.11/dcn/18/11-18-0208-00-00az-replay-attack-detection-using-ltf-with-zero-prefix.pptx>
7. <https://mentor.ieee.org/802.11/dcn/18/11-18-0222-01-00az-consistency-check-across-multiple-channel-estimates.ppt>
8. <https://mentor.ieee.org/802.11/dcn/17/11-17-1879-01-00az-pre-association-security-negotiation-for-11az-sfd.pptx>
9. <https://mentor.ieee.org/802.11/dcn/18/11-18-0235-01-00az-amendment-text-submissions-formatting-conventions.pptx>
10. <https://mentor.ieee.org/802.11/dcn/17/11-17-1884-01-00az-first-path-ftm-sfd-text.pptx>
11. <https://mentor.ieee.org/802.11/dcn/18/11-18-0236-00-00az-ftm-overview-and-hez-measurement-phase.doc>
12. <https://mentor.ieee.org/802.11/dcn/18/11-18-0223-00-00az-performance-evaluation-on-zero-padded-waveform.ppt>
13. <https://mentor.ieee.org/802.11/dcn/18/11-18-0215-02-00az-802-11az-negotiation-protocol-amendment-text.doc>
14. <https://mentor.ieee.org/802.11/dcn/18/11-18-0229-01-00az-sequence-authentication-code-sac-signaling-in-su-and-mu-ranging.pptx>
15. <https://mentor.ieee.org/802.11/dcn/18/11-18-0215-02-00az-802-11az-negotiation-protocol-amendment-text.doc>
16. <https://mentor.ieee.org/802.11/dcn/18/11-18-0209-00-00az-long-token-for-secure-ranging.pptx>
17. <https://mentor.ieee.org/802.11/dcn/18/11-18-0207-02-00az-802-11az-vhtz-measurement-exchange-protocol.doc>
18. <https://mentor.ieee.org/802.11/dcn/18/11-18-0220-00-00az-60ghz-passive-location.pptx>