IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGaz Meeting Minutes  November 7th-9th, 2017  Orlando, Florida, USA | | | | |
| Date: 2017-11-07 | | | | |
| 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 November 7th, 2017.

**IEEE 802.11 Task Group AZ**

**November 7th-9th, 2017**

1. **TGaz – 7th November 2017 – Slot #1**
   1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **4.00pm EST**, Vice Chair Carlos Aldana (Intel Corporation), Roy Want (Google) Secretary.
   2. Agenda Doc. **IEEE 802.11-17/1552r02**
   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: ~56 present
   4. Review Agenda
      1. Called for any additional submissions for the week.
      2. Reviewed and modified the agenda
      3. Chair called for any additional feedback and changes to agenda.
      4. An additional slot (5th) will be requested for Wed PM2. In AM1 we will review the needed for one more slots depending on progress.
      5. **Motion: We approve the agenda for document 11-17/1552r02**
      6. Approved by unanimous consent
   5. Approve previous meeting minutes (posted Sept 21st)
      1. Roy Want (Google) reviewed Sept Meeting Minutes **11-17/1481r0**
         1. **Motion: Move to approve document 11-17-1481r0 as TG meeting minutes for the Sept meeting**
         2. Mover: Roy Want, Seconder: Assaf Kasher
         3. Discussion of the motion: none
         4. **Vote:** Y: 20, N: 0, A: 2; **motion passes**
   6. No telecom last month, and so no minutes to approve
   7. Review of SFD Working Draft **11-17/0462r9** presented by Yongho Seok on behalf of Chao-Chun Want (MediaTek) **r8** posted on Nov 3rd, **r9** on Nov 6th.
      1. Additions were summarized in highlighted text for r8, and r9 (w/ one section name updated).
      2. Discussion: no comments or feedback on Working draft
      3. No motion at this time to allow additional time for members to review.
   8. Feng Jiang (Intel Corporation) presented document **11-17/1700r0**
      1. Title: **Power Control for Multiuser Ranging**
      2. Summary: Reuse 11ax power control, timing and frequency synchronization for 11az. Minimize hardware changes.
      3. **Strawpoll #1  
         For 11az MU operation in the unassociated mode following mechanisms are reused and active:**

* **UL Power control.**
* **Timing and frequency synchronization for UL transmission.**
* **Supported trigger subtypes for 11az trigger type:**
  + - * + **TF Location -> Poll**
        + **TF Location -> Uplink Sounding**
        + **TF Location -> LMR**
        + **TF Location -> (Loc. negotiation using RA) and behavior to follow RA access. Details TBD.**
* **Note: this list may be extended in the future to accommodate OBSS operation.**
  + 1. Discussion of strawpoll: none.
    2. **Results:** Y: 19, N: 0, A: 7
    3. **Motion:   
       Move to adopt the text below to the 11az SFD, instruct the editor to include it in the TGaz SFD under the sub-section 3.2 (Protocol description) and grant editorial license to the SFD editor:**

**“For HEz operation in the unassociated mode the following mechanisms are reused and active:**

**–UL Power control.**

**–Timing and frequency synchronization for UL transmission.**

**–Supported trigger subtypes for 11az trigger type:**

* **TF Location -> Poll**
* **TF Location -> Uplink Sounding**
* **TF Location -> LMR**
* **TF Location -> (Loc. negotiation using RA) and behavior to follow RA access. Details TBD.”**

**Note: this list may be extended in the future to accommodate OBSS operation.**

* + 1. Discussion of motion: none.
    2. Mover: Ganesh Venkatesan, Seconder: Chitto Ghosh
    3. **Vote:** Y: 13, N: 0, A: 4; **motion passes**
  1. Nehru Bhandaru (Broadcom) presented document **11-17/1737r0**
     1. Title: **Pre-association Security Negotiation for 11az**
     2. Summary: Defining a preassociation security negotiation protocol for 11az based on protocol options that are already used by 802.11 Specification. It provides Authentication, Key Management, Encryption and Message Integrity in the unassociated state.
     3. Discussion of presentation:
     4. C. Why isn’t standard 802.11u, E911 used to generate the preassoiciation key.
     5. R. Not familiar with that standard, and will follow-up.
     6. C. It won’t protect against man-in-the-middle (MitM), perhaps by a station transmiting at high power.
     7. R. True, it does not protect against that; you need integrated protection.
     8. C. Re: Like FILS (slide 7); is this only for the FTM session?
     9. R. Yes, this will be a little different to FILS (Fast Initial Link Setup) in TGai. FILS is about getting the STA to associate fast, 11az FTM executes in the unassociated mode as well as associated mode.
     10. **Strawpoll 0:  
         Add to SFD Security section:**

**“PASN Authentication**

**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.”**

* + 1. Discussion of strawpoll: none.
    2. **Results:** Y: 22, N: 0, A: 6
    3. **Strawpoll 1:**  
       **Add to SFD PASN Authentication section:  
         
       “An AP indicates PASN support by advertising a TBD PASN AKM in RSNIE that is included in some of the Beacons and in 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.”**
    4. Discussion of Strawpoll:
    5. C. Given we are trying to reduce beacon bloat you don’t need to advertise PASN in every beacon or probe response.
    6. R. This change is now reflected in the strawpoll text (above) e.g. “… in some of the beacons and in probe responses …” vs “…in beacons …”
    7. **Results:** Y: 20, N: 0, A: 4
    8. **Strawpoll #2:   
       Add to SFD PASN Authentication section:  
         
       “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.”**  
       Discussion of strawpoll: none  
       Results: Y:18, N:0, A: 6
    9. **Strawpoll #3:  
       Add to SFD PASN Authentication section:**

**“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.**

**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.”**

* + 1. Discussion of strawpoll: none
    2. **Results:** Y: 18, N: 0, A: 4.
    3. **Strawpoll #4:  
       Add to SFD Security section:  
       “802.11az protocol negotiation and measurement reports shall be integrity protected and optionally encrypted for privacy.**
    4. Discusion of strawpoll: none
    5. **Results:** Y: 22, N: 0, A: 1.
  1. Ganesh Venkatesan (Intel Corportion) presented document **11-17/1733r0**
     1. Title: **Ranging ID and its Lifetime Management**
     2. Summary: The assignment and maintenance of the Ranging ID consumes resources in the AP. To conserve resources AP’s would like to release resources associated with inactive Ranging IDs as soon as possible. This submission discusses Ranging ID lifetime and management.
     3. **Strawpoll:**   
        **We support:**

–**Ranging IDs are of the same size and range as AIDs and following same rules and limitations.**

**–Ranging IDs and AIDs are from same space and non-conflicting.**

**–the assignment of Ranging IDs by a RSTA to unassociated ISTA resulting in the execution MU HEz Ranging protocol with the RSTA:**

**• the assigned Ranging ID is included in the HEz Specific subelement contained in iFTM.**

**–the RSTA may advertise a Ranging ID lifetime which defines the duration for which the Ranging ID remains valid**

**• the mechanism to advertise Ranging ID lifetime is TBD**

**• the best choice for Ranging ID lifetime value is implementation dependent**

**–the Ranging ID is retired at both ISTA and RSTA when the corresponding Ranging ID Lifetime expires which also terminates the FTM session.**

**–Ranging ID lifetime may be equal to MAX BSS IDLE PERIOD.**

**–When an FTM session terminates or aborts the Ranging ID expires.**

**–Termination may be explicit (i.e. using FTM or FTM Req) or implicit due to Ranging ID Lifetime expiration.**

**–Support of the Ranging ID Lifetime is optional**.

* + 1. Discussion of strawpoll:
    2. C. Before we do this, how is the ranging ID assigned in unassociated mode.
    3. R. The ranging ID is assigned in an initial FTM frame. In assoc mode the association ID is used.
    4. C. Are you making the FTM exchange based purely on beam forming?
    5. R. This proposal is not excluding other forms of protocol exchange.
    6. C. Is it based on HEz which relies on a trigger frame?
    7. R. Yes.
    8. C. Are the ranging IDs for WiFi all the same lifetime.
    9. R. The AP assigns it and it will be the same for all STAs.
    10. C. We could make it the same as the Max BSS idle operation parameter.
    11. R. We need to check if this is negotiated – will get back to you. Strawpoll continues on the assumption its not based on this parameter.
    12. **Results:** Y: 14, N: 1, A: 4
  1. No time for the remaining motion in this slot – deferred to later.
  2. The meeting agenda will be uploaded as document **11-17/1552r2** after this slot
  3. We are a recess for slot #1 at 18.02pm.

1. **TGaz – 8th Nov, 2017 – Slot #2**
   1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **8.00am EST**; Vice Chair, Carlos Aldana (Intel Corporation); Roy Want (Google) Secretary.
   2. Agenda Doc. **Now working revsion at 11-17/1552r3**
   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: ~26 present
   4. Reviewed submission order and updated agenda
      1. Haven’t received feedback on CSD from Jon Rosedahl topic moved to PM1.
      2. Updated agenda presentation order and feedback requested: none received
      3. Approved agenda.
   5. Ganesh Venkatesan (Intel Corportion) cont. presentation of document **11-17/1733r1**
      1. Figure on slide 4 is now updated with ranging ID lifetime
      2. **Motion: Move to add the following text to the 802.11az SFD (Cl. 3.2 Protocol Description), granting the SFD Editor editorial license:**
      * **Ranging IDs are of the same size and range as AIDs and following same rules and limitations.**
      * **Ranging IDs and AIDs are from same space and non-conflicting.  
        the assignment of Ranging IDs by a RSTA to unassociated ISTA resulting in the execution MU HEz Ranging protocol with the RSTA:**
      * **the assigned Ranging ID is included in the HEz Specific subelement contained in iFTM.**
      * **the RSTA may advertise a Ranging ID lifetime which defines the duration for which the Ranging ID remains valid**
        + **the mechanism to advertise Ranging ID lifetime is TBD**
        + **the best choice for Ranging ID lifetime value is implementation dependent**
      * **the Ranging ID is retired at both ISTA and RSTA when the corresponding Ranging ID Lifetime expires which also terminates the FTM session.**
      * **Ranging ID lifetime may be equal to MAX BSS IDLE PERIOD.**
      * **When an FTM session terminates or aborts the Ranging ID expires.**
      * **Termination may be explicit (i.e. using FTM or FTM Req) or implicit due to Ranging ID Lifetime expiration.**
      * **Support of the Ranging ID Lifetime is optional.**
      1. Discussion of motion: none
      2. Mover: Ganesh Venkatesan, Seconder: SK Yong
      3. **Votes**: Y: 14, N: 0, A: 1; **motion passes**
   6. SK Yong (Apple) presented document **11-17/1767r0**
      1. Title: **PHY Security SRD Text Update**
      2. Summary: Proposed additional text related to protecting PHY against an attack
      3. Text referred to in strawpoll:   
         (5) **In the PHY Security mode (VHTz, HEz, DMGz, EDMGz), the training waveform shall be transmitted with zero power (no signal) guard intervals preceding and following the field(s) used for channel/ToA measurement. (Note that zero power guard interval shall be inserted following the last sounding symbol if the last sounding symbol is followed by non-zero power signal)**
      4. **(6) In the PHY Security mode (VHTz, HEz, DMGz, EDMGz), the field used for channel/ToA measurement shall be derived from (a) random sequence(s) known by the authorized I-STA and R-STA only**
      5. C. We think this is too stringent. There are other methods that could be applied. This is too restricted.
      6. R. We discussed this. This will be a significant change and will require additional implementation. Considered other options, but they are not secure, and led to this requirement.
      7. **Strawpoll:   
         Do you support to add the proposed text as shown in slide 4 & 5 to the SFD?   
         Results**:Y: 15, N: 0, A 14.
      8. **Motion:** **Move to adopt the text, instruct the editor to include it in the TGaz SFD under section 6 (security) and grant the SFD Editor editorial license:**

(5) In the PHY Security mode (VHTz, HEz, DMGz, EDMGz), the training waveform shall be transmitted with zero power (no signal) guard intervals preceding and following the field(s) used for channel/ToAmeasurement. (Note that zero power guard interval shall be inserted following the last sounding   
symbol if the last sounding symbol is followed by non-zero power signal)

(6) In the PHY Security mode (VHTz, HEz, DMGz, EDMGz), the field used for channel/ToA measurement shall be derived from (a) random sequence(s) known by the authorized I-STA and R-STA only.

* + 1. Mover: SK Yong, Yongho Seok.
    2. **Votes**: Y: 11, N: 0, A: 7; **motion passes**
  1. Chitto Ghosh (Intel Corporation) presented document **11-17/1739r0**
     1. Title: **Power Save Operation for Ranging Measurements**
     2. Summary: proposes a power efficient scheduling mechanism for power save STAs that intend to perform 11az-based measurement. Uses a frame exchange sequence within a single availability window. In case of limited BW availability, it uses a Cascade Indication subfield to extend the availability window.

**Strawpoll:   
Do you agree to include the following text in the TGax SFD?**  
“• **In each availability window there is nominally a single poll, each poll is to all STAs assigned to the availability window.**• **If the available BW does not allow for the polling of all STAs within the group there is an indication within the TF Poll that an additional TF Poll is expected within the availability window.**

• **Within the availability window there is a single measurement for those STAs responding to the poll (and correctly received) with the relevant LMRs feedbacks.”**

* + 1. Discussion of the strawpoll: none
    2. **Result**: Y: 15, N: 1, A: 4.
    3. **Motion:   
       Move to adopt the text, instruct the editor to include it in the TGaz SF under section 3.2 (Protocol Description) and grant the SFD Editor editorial license:**

“• **In each availability window, there is nominally a single poll, each poll is to all STAs assigned to the availability window.**

• **If the available BW does not allow for the polling of all STAs within the group there is an indication within the TF Poll that an additional TF Poll is expected within the availability window.**

• **Within the availability window there is a single measurement for those STAs responding to the poll (and correctly received) with the relevant LMRs feedbacks.”**

* + 1. Mover: Ganesh Venkatesan, Seconder: Rob Sun
    2. Discussion: none
    3. **Vote**: Y: 11, N: 0, A: 4; **motion passes**
  1. Erik Lindskog (Qualcomm) presented document **11-17/1741r2**
     1. Title: **MU Ranging Sequence**
     2. Summary: Some of the details in the MU ranging sequence need to be specifed, such as: 1) Polling phase 2) STA to AP LMR feedback, 3) ACK-ing of LMR feedback, 4) Sequence specification.
     3. Discussion of presentation: none.
     4. Strawpoll:
     5. **We support the following specifications for MU ranging:**

• **Polling:**

• There is a single polling phase prior to the measurement phase.

• **STA to AP LMR feedback:**

• STA to LMR feedback is supported.

• Is negotiated at service establishment.

• **ACK-ing of LMR feedback:**

• AP to STA or STA to AP LMR feedback is neither acknowledged nor retransmitted

• **Sequence:**

• [TF Poll -> Poll Rsp. -> (TF Sound -> UL NDP) x N -> DL NDPA -> DL NDP -> AP2STA LMRs] x M

• **Where:**

• The arrow ‘->’ denotes a SIFS interval

• The AP2STA LMRs are unicast report frames

• Supported PHY frame formats TBD

• M is the number of MU ranging groups and is constraint by availability window size.

• N is the number of STA groupings, separated in time for UL sounding.

• **Sequence with for STA to AP LMR feedback:**

• [TF Poll -> Poll Rsp. -> (TF Sound -> UL NDP) x N -> DL NDPA -> DL NDP -> AP2STA LMRs -> TF LMR -> STA2AP LMRs]

**Note:** AP to STA LMR feedback are carried in an HE MU PPDU.

* + 1. **Results**: Y: 15, N: 0, A: 1.
    2. **Motion:   
       Move to adopt the following text in the TGaz SFD under Section 3.2 and grant the SFD editor editorial license:  
       For MU ranging:**

**We support the following specifications for MU ranging:**

• **Polling:**

• There is a single polling phase prior to the measurement phase.

• **STA to AP LMR feedback:**

• STA to LMR feedback is supported.

• Is negotiated at service establishment.

• **ACK-ing of LMR feedback:**

• AP to STA or STA to AP LMR feedback is neither acknowledged nor retransmitted

• **Sequence:**

• [TF Poll -> Poll Rsp. -> (TF Sound -> UL NDP) x N -> DL NDPA -> DL NDP -> AP2STA LMRs] x M

• **Where:**

• The arrow ‘->’ denotes a SIFS interval

• The AP2STA LMRs are unicast report frames

• Supported PHY frame formats TBD

• M is the number of MU ranging groups and is constraint by availability window size.

• N is the number of STA groupings, separated in time for UL sounding.

• **Sequence with for STA to AP LMR feedback:**

• [TF Poll -> Poll Rsp. -> (TF Sound -> UL NDP) x N -> DL NDPA -> DL NDP -> AP2STA LMRs -> TF LMR -> STA2AP LMRs] x M

• **Note:**

• AP to STA LMR feedbacks are carried in an HE MU PPDU.

* + 1. Discussion of motion:
    2. C. In the last bullet the sequence is missing the multiplier M
    3. C (opposite). It should not have M because it’s a station responding in the last bullet
    4. R. Decided to add xM to indicate the sequence could happen multiple times.
    5. R. The LMR(s) refers to multiple measurements rather than multiple frames.
    6. C. It would be helpful to clarify the terminology and format of the descripton.
    7. Mover: Yongho Seok, Seconder: Ganesh Venkatesan
    8. **Votes**: Y: 12 N: 0, A: 3; **motion passes**.
  1. Erik Lindskog (Qualcomm) presented document **11-17/1742r1**
     1. Title: SU Ranging Feedback
     2. Summary: **Similarly, as for MU ranging: 1)** There is a need for SU iSTA to rSTA LMR feedback 2) There is no need for ACK-ing or retransmission of SU LMR feedback.
     3. Discusion of presentation: none.
     4. **Strawpoll:   
        We support the following specifications for SU ranging:  
          
        • ISTA2RSTA LMR feedback:  
         - ISTA2RSTA LMR feedback is supported and is negotiated at service establishment.**

**• Acknowledgement of LMR feedback:**

**-AP to STA or STA to AP LMR feedback is neither acknowledged nor retransmitted**

* + 1. Discussion of strawpoll: none.
    2. Results: Y: 16, N: 0, A: 0
    3. **Motion:**

**Move to adopt the text to the TGaz SFD and grant the SFD editor editorial license:**

**ISTA2RSTA LMR feedback:  
 - ISTA2RSTA LMR feedback is supported and is negotiated at service establishment.**

**Acknowledgement of LMR feedback:**

**-RSTA2ISTA or ISTA2RSTA LMR feedback is neither acknowledged nor retransmitted.**

* + 1. Discussion of motion: none
    2. Mover: Chitton Ghosh, Seconder: Assaf Kasher
    3. **Votes**: Y: 13, N: 0, A: 0; **motion passes**
  1. Chitto Ghosh (Intel Corporation) presented document **11-17/1770r0**
     1. Title: **Protected LTF Using PMF in SU and MU Modes**
     2. Summary: Discussion of the LTF protection for both SU and MU ranging and its relation to the MAC security and security negotiation. This includes 1) key exchange in negotiation phase, and 2) Randomization seed in measurement phase
     3. Disucssion of presentation:
     4. C. Slide 6: during the protocol hand-shakes you reference cryto functions – what are those functions
     5. R. The function definition is TBD.
     6. C. Slide 7. Between DL and UP there are only SIFS, you may need to increase this time.
     7. R. Correct. One option is to derive the LTF in the next packet
     8. C. One option is to use an EXOR function and precalculated encryption field to save time.
     9. R. Yes, this is another method that can be used.
     10. C. Time issue is a valid point for creating next key
     11. C. But its important to ensure the key is strong and secure. We don’t want to reduce the protection in order to save time.
     12. This is informational; No poll or motion at this time.
  2. Reminder to do attendance
  3. At recess at 10.01am.

1. **TGaz – 8th Nov, 2017 – Slot #3**
   1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **1.30pm EST**; Vice Chair, Carlos Aldana (Intel Corporation); Roy Want (Google) Secretary.
   2. Agenda Doc. **Now uploaded at revsion 11-17/1552r3**
   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: ~23 present
   4. Reviewed submission order and updated agenda **11-17/1552r4**
      1. Note 2-slots added – please note room updates on online calendar
      2. CSD change update from Jon Rosendahl. There are no changes to review from other work groups. Its been added to the EC calendar.
      3. Updated agenda with revisions above ongoing in **r4**
   5. Yongho Seok (MediaTek) prepared with Chao-Chun Wang presented **11-17/1771r0**.
      1. Title: **Proposed Draft Specification**
      2. Summary: Draft amendment text proposed for the SFD.
      3. The goal is to have this merged into the SFD text.
   6. Yongho Seok (MediaTek) presented document **11-17/1725r0**.
      1. Title: **Ranging ID Management**
      2. Summary: An association ID-like value (Ranging ID) is assigned to an unassociated STA by an rSTA to facilitate the negotiation phase and subsequently the ranging phase.
      3. Discussion of presentation: none
      4. **Strawpoll:**

**Do you support the following SFD text?**

-**When an HEz FTM session is terminated, the Ranging-ID assigned for a MU ranging operation of an unassociated STA is released.**

* + 1. Discussion of strawpoll:
    2. C. We have discussed this earlier and was included in the motion this morning.
    3. R. The version in this strawpoll is clearer, and would like to go ahead anyway.
    4. C. Update strawpoll text to use “…the Ranging-ID..” rather than “…a …”
    5. R. Text updated.
    6. Results: Y: 7, N: 0, A: 0
    7. **Motion:**

**Move to adopt the following text to TGaz under sub-section 3.2 (Protocol Description) and grant the SFD editor editorial license:**  
**“When an HEz FTM session is terminated, the Ranging-ID assigned for a MU ranging operation of an unassociated STA is released.**

* + 1. Discussion of motion: none.
    2. Mover Yongho Seok, Seconder: Ganesh Venkatesan
    3. **Votes**: Y: 11, N: 0, A: 0; **motion passes**
  1. Liwen Chu (Marvell) presented document **11-17/1754r0**
     1. Title: **Frame Responding Rules for NDP Ranging**.
     2. Summary: Potentially TOA+TOD and CSI can be used for LMR.

We need to define which one should be used for NDP ranging.

* + 1. Discussion of presentation: none
    2. **Strawpoll:  
       Do you agree to add the following text to 11az SFD:  
       ‒For MU Ranging AP2STA LMR feedback consists of TOA and TOD reporting only**

**‒For MU Ranging STA2AP LMR feedback consists of TOA and TOD reporting only**

* + 1. Discussion of strawpoll: none.
    2. **Results**: Y: 12, N: 0, A: 0.
    3. **Motion:**   
       **Move to adopt the following text to TGaz under sub-section 3.2 (Protocol Description) and grant the SFD editor editorial license:  
       ‒For MU Ranging RSTA2ISTA LMR feedback consists of TOA and TOD reporting only**

**‒For MU Ranging ISTA2RSTA LMR feedback consists of TOA and TOD reporting only**

* + 1. Discussion of the motion: none
       1. station roles are changed from strawpoll to be consistent with SFD.
    2. **Vote**: Y: 10, N 0 , A: 1; **motion passes**
    3. **Strawpoll:   
       Do you agree to add the following text to 11az SFD:**

**“For RSTA2ISTA SU LMR feedback, support of TOA and TOD is mandatory and CSI report is optional for both ISTA and RSTA and agreed upon during negotiation”**

* + 1. **Results**: Y: 11, N: 0, A: 0.
    2. **Motion:**  
       **Move to adopt the following text to TGaz under sub-section 3.2 (Protocol Description) and grant the SFD editor editorial license:**

**“For RSTA2ISTA SU LMR feedback, support of TOA and TOD is mandatory and CSI report is optional for both ISTA and RSTA and agreed upon during negotiation”**

* + 1. Discussion of the motion: none.
    2. Mover: Yongho Seok, Seconder: Qinghua Li.
    3. Vote: Y: 11, N: 0, A, 1; motion passes
    4. **Strawpoll:**

**Do you agree to add the following text to 11az SFD?**

* **The bandwidth and the MCS/rate of the SU NDP ranging report are defined by:**
* **The data rate/MCS of Ranging Report is solely decided by the RSTA.**
* **The bandwidth of ranging report is not wider than the bandwidth of the soliciting NDPA.**
  + 1. Discusion of strawpoll:
    2. C. Remove the word “immediate” before SU NDP
    3. R. Text edited above.
    4. **Results**: Y: 12, N: 0, A: 0
    5. **Motion:**
    6. **Move to adopt the following text to TGaz under sub-section 3.2 (Protocol Description) and grant the SFD editor editorial license:**

**“-The bandwidth and the MCS/rate of the SU NDP ranging report are defined by:**

**-The data rate/MCS of Ranging Report is solely decided by the RSTA.**

**-The bandwidth of ranging report is not wider than the bandwidth of the soliciting NDPA.”**

* + 1. Mover: Yongho Seok, Seconder: Feng Jiang
    2. **Vote**: Y: 13, N: 0, A: 0; **motion passes**
  1. Feng Jiang (Intel Corporation) presented document **11-17/1701r0**
     1. Title: **Two-sided LMR Feedback between AP and STA**
     2. Summary: proposal for detailed design of two-sided LMR feedback for negotiation indication, measurement resource allocation, and LMR exchange sequence.
     3. Discussion of presentation: none.
     4. No strawpoll or motion at this time. Will follow up in the future.
  2. Yongho Seok (MediaTek) presented document **11-17/1726r0**
     1. Title: **Secure Ranging Measurement**
     2. Summary: This document discusses the replay attack problem and possible solutions. Three options are presented.
     3. Discussion of the presentation: none
     4. Next meeting a preferred option will be presented with strawpoll/motion.
  3. Agenda revised for slot #4 in Bonaire 1/2
  4. Reminder to complete attendance
  5. At recess 3.16pm.

1. **TGaz – 8th Nov, 2017 – Slot #4**
   1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **4.00pm EST**; Vice Chair, Carlos Aldana (Intel Corporation); Roy Want (Google) Secretary.
   2. Agenda Doc. **Now uploaded as revsion 11-17/1552r4**
   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: ~11 present
   4. Agenda reviewed and working with **11-17/1552r5**
      1. Presendation order adjusted.
      2. Request for comments – none
   5. Erik Landskog (Qualcomm) presented document **17-11/1758r0**
      1. Title: **Futher Scalable Location Performamce Analysis**
      2. Summary: Comparison of DToA and CToA protocol for various geometric arrangement of client and APs, with an analysis of a client outside of the polygon enclosing the APs.
      3. Discussion of presentation:
      4. C. Who is tracking the client?
      5. R. The client is making its own location estimate.
      6. C. Its a simulation that is making a location estimate (LE), not the client, comparing that to the simulated groundtruth resulting in a simulated positioning error.
      7. R. The simulation only uses information available to a client for the LE.
      8. C. What does D and C stand for in DToA and CToA respectively?
      9. R. D= Differential vs C=Collaborative ToA=Time of Arrival.
      10. C. What is the convergence: number of values, time?
      11. R. This simulation uses about 100 iterations to guarantee convergence, but in practice its likely to be a much smaller, and bounded by short time (<1s). However, this depends on various system parameters that would need to be agreed to provide a quantitative answer.
      12. C. Why was CToA slightly better than DToA in the first graph shown.
      13. R. Because in this simulation we have not added client tracking.
      14. C. What do you mean by adding client tracking?
      15. R. The current simulation is just tracking the clock offset. Adding a location (x, y) state in a Kalman filter would likely make the client location estimate more accurate.
   6. Rob Sun (Huawei) presented document **17-11/1747r0**
      1. Title: **FTM Secuity with Distance Bounding Protocol**
      2. Summary: A distance bounding protocol achieved by 1) modifying the FTM frames with extra fields to accommodate the FDB protocol 2) defining a new Ack, 3) defining extensions so that the FTM protocol can transmit and receive a NAck, 4) defining the FDB protocol and process parameters.
      3. Discussion of presentation:
      4. C. Why are you proposing a protocol that is more than a secure key exchange.
      5. R. Because preshared keys may not have been shared. And the protocol needs to be performed rapidly, as quickly as a SIFS interval.
      6. C. You are assuming that a distance bound has been set, alternatively if the timestamp is being protected, there is no concern for distance fraud.
      7. R. Yes and No, if the timestamp is actually protected, then the issue can be addressed at that level without using the timing information within the preamble. However, for the unassociated STAs, when no encryption is available to provide timestamp protection, the distance bounding protocol should be able to provide a level of distance fraud protection.
      8. C. What about Trigger frame and NDP exchanges vs FTM and ACKs, to carry out the measurement?
      9. R. I can investiage more about this. When using the Trigger frame and NDP, the system needs to respond in the SIFS, and therefore the protocol needs to be fast and power efficient.
      10. C. Delays of the order of milliseconds – that would be very large distance. Tryng to understand applicability of that to cars etc.
      11. R. The best tools can’t do better than a couple of milliseconds. These techniques can be used to bound the time.
      12. C. Processing speed of 2mS would be too long as this is equivalent to 200K feet
      13. No proposal today - presentation is only for information at this time

* 1. Nehru Bhandaru (Broadcom) presented document **11-17/1776r0**
     1. Title: **Frame Protection for 11az**
     2. Summary: Need some highlevel agreement on frame protection
     3. **Strawpoll:  
        We agree that for the ranging protocol:  
          
        –Security keys for 11az Management Frame Protection and range measurement field protection are derived based on security negotiation and never shared OTA (associated mode or pre-association security negotiation).**

**– Range measurement field sequence is generated from some shared information and derived from the range measurement field protection key(s).**

**–Keys used for data exchange and 11az management protection may be different from keys used for range measurement field protection**

**–PMF framework is used for FTM Req, FTM, and LMR management frames; the key may either be derived from associated or pre-associated security negotiation.**

* + 1. Discussion of strawpoll:
    2. C (various): edits made to arrive at text above.
    3. C. Should it be PMF framework “is used” vs “maybe used” because PMF may take too long in some cases
    4. R. No
    5. **Result:** Y: 10, N: 0, A: 0
    6. **Motion  
       Move to adopt the following text in the TGaz SFD under Section 6 – Security - and grant the SFD editor editorial license:  
         
       “Security keys for 11az Management Frame Protection and range measurement field protection are derived based on security negotiation and never shared OTA (associated mode or pre-association security negotiation).**

**Range measurement field sequence is generated from some shared information and derived from the range measurement field protection key(s).**

**Keys used for data exchange and 11az management protection may be different from keys used for range measurement field protection.**

**PMF framework is used for FTM Req, FTM and LMR management frames; the key may either be derived from associated or pre-associated security negotiation.”**

* + 1. Mover: Nehru Bhandaru, Seconder: Chitto Ghosh
    2. **Vote**: Y: 9, N: 0, A: 0; **motion passes**
  1. Agenda slide deck will be uploaded as version **11-17/1552r05** based on changes made during this session.
  2. Attendance Reminder
  3. Reviewed tasks for slot #5
  4. Recess at 5.50pm.

1. **TGaz – 9th Nov, 2017 – Slot #5.**
   1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **10.35am EST**; Vice Chair, Carlos Aldana (Intel Corporation); Roy Want (Google) Secretary.
   2. Agenda Doc. **Now uploaded as revsion 11-17/1552r5**
   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: ~14 present.
   4. Agenda reviewed
      1. Presentation order reviewed.
      2. Request for comments – none
      3. Working draft **11-17/1552r5**
   5. Nehru Bhandaru (Broadcom) presented an update to document **11-17/1776r0** in **1776r1**
      1. Request to make clarification on the measurement field in previous motion.
      2. **Motion:**

**Move to amend the adopted text in the TGaz SFD under Section 6 (Security) with the following underlined addition, and grant the SFD editor editorial license:  
  
“Security keys for 11az Management Frame Protection and range measurement field protection are derived based on security negotiation and never shared OTA (associated mode or pre-association security negotiation).  
  
Note:**

**For HEz and VHTz PPDUs the measurement field refers to HE LTF and VHT LTF respectively”.**

* + 1. Discussion of motion:
    2. C. (various): edits to arrive at text above.
    3. C. We will discuss DMG at a later point; submissions will be requested.
    4. Mover: Nehru Bhandaru, Seconder: Chitto Ghosh
    5. Vote: Y: 11, N: 0, A: 1; **motion passes**
  1. Presentation schedule now complete – returning to agenda items.
  2. Review the timelines
     1. FRD freeze was Q3-2017, and SFD freeze scheduled for Q3-2018
     2. Good progress on schedule for proposals for range accuracy (70%) and security (30%).
  3. Goals for January 2018 meeting
     1. -SFD development
     2. -Consider amendment text proposals based on SFD text
     3. -Review technical proposals
     4. **Motion  
        We commit for the Jan. meeting goals as the TG Plan of Record.**
     5. Mover: Assaf Kasher, Seconder: Yongho Seok
     6. **Vote**: Y: 12, N: 0, A: 0: **motion passes**
  4. Teleconference planning
     1. TGaz Telecon set for Dec 20th Wed, 11am ET. More calls will be added if necessary and event will be cancelled if there are no submissions.
  5. Reminder to record attendance
  6. Any other business? – None
  7. Agenda will be uploaded as **11-17/1552r6**
  8. Recess at 11.08am

**References:**

1. <https://mentor.ieee.org/802.11/dcn/17/11-17-1552-06-00az-tgaz-nov-meeting-agenda.pptx>
2. <https://mentor.ieee.org/802.11/dcn/17/11-17-1481-00-00az-meeting-minutes-september-2017-session.docx>
3. <https://mentor.ieee.org/802.11/dcn/17/11-17-0462-10-00az-11-az-tg-sfd.doc>
4. https://mentor.ieee.org/802.11/dcn/17/11-17-1700-01-00az-power-control-for-multiuser-ranging.pptx
5. https://mentor.ieee.org/802.11/dcn/17/11-17-1737-00-00az-pre-association-security-negotiation-for-11az.pptx
6. https://mentor.ieee.org/802.11/dcn/17/11-17-1733-01-00az-ranging-id-and-its-lifetime-management.pptx
7. https://mentor.ieee.org/802.11/dcn/17/11-17-1767-01-00az-phy-security-srd-text-update.pptx
8. https://mentor.ieee.org/802.11/dcn/17/11-17-1739-00-00az-power-save-operation-for-ranging-measurements.pptx
9. https://mentor.ieee.org/802.11/dcn/17/11-17-1741-02-00az-mu-ranging-sequence.pptx
10. https://mentor.ieee.org/802.11/dcn/17/11-17-1742-01-00az-su-ranging-feedback.pptx
11. https://mentor.ieee.org/802.11/dcn/17/11-17-1770-00-00az-protected-ltf-using-pmf-in-su-and-mu-modes.pptx
12. https://mentor.ieee.org/802.11/dcn/17/11-17-1771-00-00az-proposed-draft-specification.doc
13. https://mentor.ieee.org/802.11/dcn/17/11-17-1725-00-00az-ranging-id-management.pptx
14. https://mentor.ieee.org/802.11/dcn/17/11-17-1754-00-00az-frame-responding-rules-for-ndp-ranging.pptx
15. https://mentor.ieee.org/802.11/dcn/17/11-17-1701-00-00az-two-sided-lmr-feedback-between-ap-and-sta.pptx
16. https://mentor.ieee.org/802.11/dcn/17/11-17-1726-00-00az-secure-ranging-measurement.pptx
17. https://mentor.ieee.org/802.11/dcn/17/11-17-1758-00-00az-further-scalable-location-performance-analysis.pptx
18. https://mentor.ieee.org/802.11/dcn/17/11-17-1747-00-00az-ftm-with-distance-bounding-protocol.pptx
19. https://mentor.ieee.org/802.11/dcn/17/11-17-1776-01-00az-frame-protection-for-11az.pptx