IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Comments on 802.11az Functional Requirements | | | | |
| Date: 2017-07-12 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Roy Want | Google Inc. |  |  | roywant@google.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Abstract

This submission includes the comments on the 802.11az Functional Requirements document IEEE 802.11/16-0425r5. This submission is written with respect to IEEE 802.11/16-0425r5.

1. **Introduction**
   1. **Purpose**

This document proposes requirements for solutions addressing functionality to be provided by the 802.11az amendment, referred to as the TGaz Functional Requirements (FRs).

* 1. **Scope**

The scope for deriving functional requirements is set by the P802.11az PAR [Ref-1] and CSD [Ref-2], as well as by the TGaz use case document [Ref-3].

The functional requirements as stated in this document cover the following aspects of 802.11az:

1. System performance
2. Bands of Operation
3. Backward compatibility and Coexistence
4. Compliance to PAR
   1. **Notation**

Requirements are identified by a preceding unique number in the format of “TGaz R*n*” , where *n* is an integer number representing the ID of the requirements.

1. **Functional Requirements**

All range and positioning measurement and medium usage performance improvements for 2.4Ghz band shall be compared with FTM executed using 802.11n over the same bandwidth and deployment scenario using SISO.

All range measurement and positioning performance improvements for 5Ghz band shall be compared with FTM executed using 802.11ac over the same bandwidth and deployment scenario using SISO.

All range measurement and positioning performance improvements for the 60Ghz band shall be compared with FTM executed using 802.11ad over the same bandwidth and deployment scenario.

The TGaz use cases are described in the TGaz Usage Models document [Ref-5]

* 1. **System Performance**
     1. **Range Measurement and coverage**

1. For the purpose of simulation, 802.11az shall use 802.11n/11ac channel model D NLOS with 20MHz, 40MHz, 80MHz and 160MHz bandwidths. Other channel models may be used if they become available and are deemed applicable. [Ref-4]
2. The 802.11az range measurement protocol shall support legacy REVmc Fine Timing Measurement in order to interoperate with legacy peers that do not support the 802.11az range measurement protocol. [Ref-4]
3. The 802.11az range measurement protocol shall have a mechanism to obtain a range measurement that is more accurate than that obtained using legacy REVmc Fine Timing Measurement under the same conditions. [Ref-4]
4. The 802.11az range measurement protocol shall support concurrent sessions in order for an Initiator to be able to perform range measurements with multiple Responders (each operating in the same or different channels). [Ref-4]
5. The 802.11az range measurement protocol shall support range measurement in both the associated and the unassociated modes. [Ref-4]
6. The 802.11az range measurement protocol shall support range measurement with an upper bound error of <TBD> m for 90% of uniformly sampled measurements. [Ref-4]
7. The 802.11az range measurement protocol shall under all conditions perform no worse than the legacy REVmc Fine Timing Measurement protocol (i.e. the resulting range measurement accuracy is as good as the legacy REVmc Fine Timing Measurement protocol). [Ref-4]
8. The 802.11az protocol shall support at least one mode of operation that enables AoA/AoD measurements in the 2.4GHz and 5GHz bands, alone or in conjunction with range measurements.[Ref-10]
   * 1. **60Ghz Bands**
9. Decrease units of Min Delta FTM for 60 GHz while maintaining backwards compatibility. [Ref-5]
10. Allow for smaller Burst Duration for 60 GHz while maintaining backwards compatibility. [Ref-5]
11. Add additional rotational angle (ROLL) to measurement reports. [Ref-5]
12. Define TOD for T1 & T3 and TOA for T2 & T4 to reduce effect of drift on ranging computation. [Ref-5]
13. The 802.11az amendment shall support at least one mode of operation that enables range measurement in the 60GHz band with an accuracy of 1cm, @90%.[Ref-6]
14. The 802.11az amendment shall support at least one mode of operation that enables AOA/DOA measurement in the 60GHz band with an accuracy of 5deg, @90%.[Ref-6]
15. The 802.11az amendment shall support at least one mode of operation that enables range/AOA measurement in the 60GHz band with a latency of 10ms. [Ref-6]
16. The 802.11az amendment shall support at least one mode of operation that provides location using a single link range and angle measurement. [Ref-6]
17. The 802.11az amendment shall support at least one mode of operation at 60GHz that enables range measurement at a minimum distance of at most 5 cm. [Ref-6]
18. The 802.11az amendment shall support at least one mode of operation at 60GHz that enables concurrent location measurement of 12 users and 7APs over the same 60GHz channel. [Ref-6]
    * 1. **Scalability**

The scalable mode of the 802.11az range measurement protocol shall support at least one mode which allows for scalable positioning, meeting the following scalability mode requirements.

1. Support locating and tracking all associated and at least 200 unassociated STAs per AP concurrently. [Ref-10]
2. Achieve improved accuracy of 1st fixed time of a STA with greater number of APs involved. [Ref-7]
3. Support configuration of the network to modify performance parameters such as the frequency and number of STAs tracked to achieve network resource usage over a range from less than 5% or to greater than 50% in cases were a dedicated AP is present. [Ref-10]
4. Operate with tracking refresh rates ranging from 0.1 to 0.5Hz with higher refresh rates available in APs dedicated to providing location.[Ref-10]
5. Maintain stability with up to 5% STAs joining and leaving the coverage of the AP. [Ref-7]
6. The scalable mode of the 802.11az positioning measurement protocol should minimize the STA‘s power consumption. [Ref-9]
7. The scalable mode of the 802.11az positioning measurement protocol should minimize the off-channel time of an associated STA. Off-channel time is the time an associated STA is required to spend on channel(s) other than the one used by the AP it's associated to for the purpose of location measurement exchange. [Ref-9]
8. Determining initial STA location within (TBD, but not greater than 10s) in APs dedicated to providing location.[Ref-10]
9. Support continuous tracking of STAs with a latency of <= 500ms [Ref-10]
10. In a scalable mode with STA centric location calculation, i.e. STA terminated location calculation, the 802.11az protocol shall support an unlimited number of STAs to concurrently compute their location.[Ref-12]
    * 1. **Functional requirements derived from 802.11ax**
11. The location protocol shall support positioning measurement of unassociated and associated STAs in the HE MU mode.[Ref-8]
12. The 11az amendment shall have a mode supporting concurrent positioning measurements of multiple STAs, in both associated and unassociated states in the HE MU mode.[Ref-8]
13. The 11az amendment shall have a mode supporting concurrent measurement from several transmit chains of an AP in HE operation mode. The same requirement shall also apply to VHT operation mode.[Ref-8]
14. The 11az amendment shall have a mode supporting concurrent measurement from several transmit chains of each non-AP STA in the HE operation mode. The same requirement shall also apply to the VHT operation mode.[Ref-8]
15. The 11az amendment shall have a mode enabling positioning measurements on all supported channel bandwidths.[Ref-8]
    * 1. **Legacy**
16. Legacy operation with REVmc FTM devices
    * 1. **Security and Privacy**
17. The 11az positioning protocol shall have at least one secured mode that meets all of the following security requirements in the associated state:[Ref-11]
18. Authentication - Mutual authentication of initiator and responder.
19. Encryption Algorithm - The cryptographic cipher combined with various methods for encrypting the message\* used in 11az-positing protocol.
20. Key Management - Create, distribute and maintain the keys.
21. Message Integrity - Ensures that the encrypted message\* has not been tampered with.

(\* Message refers to frame and/or field(s) within the frame.)

1. The 11az positioning protocol shall have at least one secured mode that meets all of the following security requirements in the unassociated state:[Ref-11]
2. Authentication - Mutual authentication of initiator and responder (provided there is a prior security context established).
3. Encryption Algorithm - The cryptographic cipher combined with various methods for encrypting the message\* used in 11az-positing protocol.
4. Key Management - Create, distribute and maintain the keys.
5. Message Integrity - Ensures that the encrypted message\* has not been tampered with.

(\* Message refers to frame and/or field(s) within the frame.)

1. The 11az protocol shall have at least one secured mode that protects against adversaries with capabilities as specified by R1 to R4 below and with the following response time.[Ref-11]
   1. Type A Adversary is assumed to have response time to standard-specified OTA events or scenario dependent fields of 1 msec or longer.
   2. Type B Adversary is assumed to have response time to known OTA events or known pre-defined fields of 1usec or longer (up to 1msec).

Note: the STA capabilities is TBD (for both types of adversaries).

An adversary may have at least one or more of the following capabilities and limitations:

[R1] An adversary that uses commercial NIC/Sniffer;

[R2] At most, the adversary may deploy/use two non-co-located Tx and Rx chains;

[R3] The adversary shall be TOA and TOD capable on all received/transmitted frames;

[R4] The adversary shall be able to compose and transmit any 802.11 packet or part of it.

TGaz R38 (OPT 1) The 11az protocol shall have secured mode options that in combination\* concurrently protects against the following security attacks (but not limited to):

1 PHY Layer Attacks

1. Replay PHY header or its fields
2. PHY Header fields substitution
3. Sub-symbol replay or manipulation

2. MAC Layer Attack

a. Packet Replay

b. Man-in-the-middle (1 or 2 coordinated attackers)

d. ID Spoofing

e. Packet Forging

\* The choice of secured mode options, and the resulting security attacks protections, is implementation dependent

TBD: Provide suitable references/exacpples to describe each of the attacks

TGaz R38 (OPT 2) The 11az protocol shall have at least one secured mode that protects against the following security attacks:

1. Both PHY and MAC Layer Attacks
2. MAC Layer Attack

Where PHY Layer Attacks and MAC Layer attacks are listed below (but not limited to):

1 PHY Layer Attacks

1. Replay PHY header or its fields
2. PHY Header fields substitution
3. Sub-symbol replay or manipulation

(example: CP-Replay)

2. MAC Layer Attack

a. Packet Replay

b. Man-in-the-middle (1 or 2 coordinated attackers)

d. ID Spoofing

e. Packet Forging

* 1. **Compliance to PAR and CSD**

1. The 802.11az amendment shall comply with the PAR [Ref-1] and the CSD [Ref-2].
2. **References**
3. **11-15-0030-09-0ngp-ngp-par-draft**
4. **11-15-0262-04-0ngp-csd-working-draft**
6. **11-16-0134-03-00az-accuracy-and-coverage-functional-requirements**
7. **11-16-0148-01-00az-60-ghz-focus-area**
8. **11-16-0309-00-00az-60ghz-functional-requirements**
9. **11-16-0448-01-00az-functional-requirement-for-scalability-operation**
10. **11-16-0593-00-00az-11ax-derived-functional-requirements**
11. **11-16-0448-02-00az-functional-requirement-for-scalability-operation**
12. **11-16-0579-02-00az-functional-requirements-for-802-11az**
13. **11-17-0120-02-00az-secured-location-threat-model**
14. **11-17-0778-01-00az-scalable-location**