IEEE P802.11
Wireless LANs

|  |
| --- |
| **Specification Framework for TGaz** |
| **Date:** 2017-07-10 |
| **Author(s):** |
| **Name** | **Affiliation** | **Address** | **Phone** | **email** |
| Chao-Chun Wang | MediaTek Inc | 2840 Junction Ave, San Jose, CA | +1-408-526-1899 | chao-chun.wang@mediatek.com  |

Abstract

This document provides the framework from which sections of the draft TGaz amendment.

The document provides an outline of each the functional blocks that will be a part of the final amendment. The document is intended to reflect the working consensus of the group on the broad outline for the draft specification and is derived from the set of functional requirements. As such it is expected to begin with minimal detail reflecting agreement on specific techniques and highlighting areas on which agreement is still required (<TBD> in the document). It may also begin with an incomplete feature list with additional features added as they are justified. The document will evolve over time until it includes sufficient detail on all the functional blocks and their inter-dependencies so that work can begin on the draft amendment itself.

**Revision history**

|  |  |  |
| --- | --- | --- |
| Revision | Date | Changes |
| 0 | Mar 14, 2016 | Initial Version |
| 1 | March 13, 2017 |  |
| 1.1 | May 11th , 2017 | 02 |
| 1.2 | June 25th, 2017 | R5 |
| 1.3 |  | R6 |

Contents

[1 Definitions 5](#_Toc490059140)

[2 Abbreviations and acronyms 6](#_Toc490059141)

[3 Positioning Protocol for Improved Accuracy and Coverage over 2.4 and 5 GHz bands 6](#_Toc490059142)

[3.1 General 6](#_Toc490059143)

[3.2 Protocol Description 6](#_Toc490059144)

[4 Positioning Protocol while operating in the 60 GHz band 8](#_Toc490059145)

[4.1 General 8](#_Toc490059146)

[5 Scalability aspects of the Positioning Protocol 10](#_Toc490059147)

[6 Security [May 2017] 11](#_Toc490059148)

[7 Using Angle of Departure and Angle of Arrival to estimate position 11](#_Toc490059149)

[8 Positioning Protocol for STA to STA topologies 12](#_Toc490059150)

[9 Frame formats 13](#_Toc490059151)

[10 References 14](#_Toc490059152)

# Definitions

FTM Initiator – the STA initiating the FTM procedure.

FTM Responder – the STA responding to the FTM Procedure establishment request

IFTM – Initial FTM frame.

IFTMR – Initial FTM Request frame.

**Type A Adversary – The attacker** is assumed to have response time to standard-specified OTA events or scenario dependent fields of 1 msec or longer.

**Type B Adversary - The attacker** is assumed to have response time to known OTA events or known pre-defined fields of 1usec or longer (up to 1msec). [2017/0120r2]

# Abbreviations and acronyms

MU – Multi User

SU – Single User

NDP – Null Data Packet

NDPA – NDP Announcement

VHT NDP Sounding-based .11az SU protocol (VHTz)

HEW NDP Sounding-based .11az MU protocol (HEWz)

TOF – Time Of Flight

BRP – Beam Refinement Protocol

# Positioning Protocol for Improved Accuracy and Coverage over 2.4 and 5 GHz bands

## General

1. The .11az protocol shall extend the REVmc iFTMR/iFTM for .11az ToF measurement parameter negotiation
2. The .11az protocol shall define the following phases
* Negation Phase (Capability discovery)
* Measurement Phase (a Time of Flight (ToF) measurement parameter negotiation)
* A set of ToF measurement exchanges

Note: Other protocol phases may be defined as needed and is <TBD> based on more discussion(s)

1. In the HEz mode, the protocol shall define a polling phase for ranging request feedback prior to NDP sounding-based measurement. [May 2017]
2. Within the MU measurement phase the UL sounding shall use one or more of the following multiplexing techniques:
	1. 1) Spatial Multiplexing using P-Matrix encoding,
	2. 2) OFDMA multiplexing,
	3. 3) TDMA multiplexing (various methods, TBD) [May 2017]

## Protocol Description

1. Negotiation phase shall support an enhancement to FTM Request frame in both SU and MU modes for both associated and unassociated STAs
2. The resource allocation for initial FTM request in MU negotiation for unassociated STAs to be based on OFDMA random access [May 2017]
3. The SU – SU negotiation procedure in the 11az shall have the following properties:
	1. Frame exchange sequence is the same as REVmc:
		1. FTM Request and Response frame formats needs to be updated, for example the response frame for unassociated STAs carry an ID (Ranging, Pre) and the NGP IE.
4. The 11az protocol shall include a mode to support multiple STAs sending FTM Request in SU mode (SU PPDU) and the AP sends FTM Response in a SU PPDU to address multiple STAs” [July 2017]
5. The Measurement phase for the ranging protocol for MU shall be only based on NDP sounding and have the following frame exchange sequence:



* Note : the detailed design of DL Trigger, DL NDPA, UL NDP, DL NDP are TBD.
1. The measurement phase for the ranging protocol for SU shall be based on IEEE 802.11 VHT sounding protocol and have the following frame exchange sequence



Note: the contents of NDP Announce (.11az), NDP (.11az) and Measurement Feedback; and the spacing between the NDP (.11az) and Measurement Feedback are TBD.

1. The measurement phase for the MU ranging protocol shall consists of one or more rounds of uplink sounding followed by one round of downlink sounding, where each round of uplink sounding includes one trigger frame soliciting one, or more NDP sounding frame(s) from STA(s) and the downlink sounding consists of one NDPA frame and one NDP sounding frame.
	1. Details of the NDP sounding structure are TBD. [May 2017]



1. The 11az protocol shall support a measurement phase that based on individual TWT mechanism
	1. Each STA negotiates TWT for ranging with the AP
	2. Polling is always the first phase within a TWT SP
	3. Number of measurement phases within a TWT SP is dependent on number of STAs responded to polling [July 2017]

# Positioning Protocol while operating in the 60 GHz band

## General

1. The 11az protocol shall define at least one mode in which LOS/NLOS estimation (an estimation likelihood that the measurement is performed on a LOS path) is provided as part of the measurement.”
2. The 11az protocol shall define at least one mode in which BRP training may operate on the LOS path (rather than on the strongest path).”

# Scalability aspects of the Positioning Protocol

This section describes the protocol features that enable operation in a dense environment.

# Security [May 2017]

1. The security setup to be negotiated in a separate optional step prior to the 802.11az protocol parameter negotiation
	1. Note that in lieu of security negotiation, keys derived using an out-of-band mechanism may be used to secure the exchange between the initiator and the responder [May 2017]
2. The REVmc, HEz, and VHTz FTM modes, the fields over which range measurements are performed shall be protected against a Type B adversary attack [May 2017]

# Using Angle of Departure and Angle of Arrival to estimate position

# Positioning Protocol for STA to STA topologies

# Frame formats

1. The Initial FTM Request shall include
	1. at least one of

 -FTM Parameters element

 *-NGP* Parameters element (optional subelements for ranging protocol- specific parameters)

* 1. optionally LCI and/or Location Civic Measurement Request element

-Trigger Field

 -Trigger field set to 1 (for 802.11-2016 FTM backward compatibility)

1. In 11az NDP ranging measurement phase, the NDPA has the following properties

B0 B1 bits value of the Sounding Dialog Token field shall be set to 0b10 to indicate 11az sequence

AID field will be used to indicate the receiver participating in the sounding exchange

Feedback Type field will be in 4-byte per STA info field (refer to the figure below)

Reserved

Reserved

Feedback

Type

B26

1. The ID for ranging operation for an unassociated STA used for measurement phase will be in the FTM Rsp frame
2. The protocol shall define a single Trigger Type field value for the 11az amendment and a Trigger Sub-type subfield in Trigger Dependent Common Info field [May 2017]

# References

Missing refrences to submissions the SFD description comes from.