IEEE 802.11az Meeting Minutes January 2017 Session P802.11
Wireless LANs

|  |
| --- |
| TGaz meeting minutes – January meeting |
| Date: 2017-01-17 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Carlos Aldana | Intel Corporation | 3600 Juliette Lane, Santa Clara, CA 95054 | 408-765-6692 | carlos.h.aldana@intel.com |

Abstract

Minutes for the TGaz meeting in Atlanta.

**IEEE 802.11 Task Group AZ**

**January 2017 Atlanta Interim**

**January 16-20, 2017**

1. TGaz – 17 January 2017 – PM1
	1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at 13:30 local time.
	2. TGaz secretary (acting) Carlos Aldana (Qualcomm).
	3. Agenda Doc. IEEE 802.11-16/1599
	4. Review Patent Policy and logistics
		1. Chair reviewed the IEEE-SA Patency Policy, additional guidelines about IEEE-SA meeting and logistics
		2. Chair called for any potentially essential patent, no one stepped up.
		3. Chair reminded all to record their attendance.
	5. Review Agenda
		1. Called for any additional submissions for the week.
		2. Reviewed the agenda based on doc 11-16/1599
		3. Chair called for any additional feedback and changes to agenda – none identified, agenda for the week approved.
	6. Previous meeting minutes approval:
		1. Document 11-16/1563r2 posted to Mentor November 23rd
		2. **Motion (#1):**

**To approve document 11-16/1563r2 as TG meeting minutes for the Nov. meeting.**

* + 1. **Moved: Ganesh Venkatesan, 2nd: Assaf Kasher**
		2. **Results (Y/N/A): 17/0/0**

Motion passes

* 1. Nehru Bhandaru presented submission [11-16-1643](https://mentor.ieee.org/802.11/dcn/16/11-16-1643-00-00az-pre-association-negotiation-of-management-frame-protection.pptx)
		1. C: how about protection of the Ack frame?
		2. R: this is not sufficient for all 11az usages.
		3. C: this is not meeting requirement
		4. R: this is a subset of what could be used. If there are proposals that protect the Ack, those could be used. Intent of proposal is to explain how to establish keys.
		5. C: how is this different from fast BSStransition (802.11r)?
		6. R: my understanding is that 802.11r does not define much for initial negotiation. The fast BSS would confirm key in assoc frame. Post auth is where keys get confirmed. My proposal is moving key confirmation logic into authentication.
		7. C: how does capability exchange happen?
		8. R: advertised in beacon and provided in probe response
		9. C: why not associate?
		10. R: you might need to perform ranging measurement before assoc.
		11. C: standard MFP requires assoc.
		12. C: class 2 robust action frame might cause problems.
		13. C: FILS use case. Key confirmation with 3 frames? Usually requires 4 frames
		14. R: ERP exchange that established PMK takes 2 messages.
		15. C: AP does not do key confirmation?
		16. R: auth(2, PANMFP,…) frame in Slide 4 has MIC.
		17. C: what are next steps?
		18. R: strawpoll to gauge what people think.
		19. Strawpoll:

The 802.11 authentication method described here should be used for negotiating pre-association security (Keys, SA) used to secure FTM

Result(Y/N/A):7/0/18

* 1. 35 attendees in the room.
	2. Feng Jiang presented submission [11-17-50](https://mentor.ieee.org/802.11/dcn/17/11-17-0050-03-00az-ndp-based-measurement-protocol.pptx).
		1. **Motion (#2):**

**We agree to the following text for 11az SFD under the “Accuracy and Coverage over 2.4 and 5GHz” subsection:**

**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.**

**Moved: Chittabrata Ghosh, 2nd: Carlos Cordeiro**

**Results(Y/N/A): 8/1/8**

**Motion passes**

* 1. Chittabrata Ghosh presented submission [11-17-120](https://mentor.ieee.org/802.11/dcn/17/11-17-0120-02-00az-secured-location-threat-model.pptx).
		1. C: on first strawpoll, are we married to an authentication algorithm?
		2. R: auth from location perspective. Mechanism is TBD.
		3. C: this is mutual authentication, right?
		4. R: authenticate the client side. Initiating STA (iSTA) is being authenticated to Access Point.
		5. C: is client authenticating AP?
		6. R: apparently that has been done through association
		7. C: slide 13: what is asterisk?
		8. R: can be LTF or it might not be. Keep it as an option.
		9. C: seems that there is a solution that this strawpoll is binding us to.
		10. R: the TG has been considering several solutions over the last couple of meetings. This submission is targeted to give a problem statement.
		11. C: ambiguity about authentication: is it iSTA or responding STA (rSTA)?
		12. C: for strawpoll 2, there are cases where not knowing the other side might be useful.
		13. R: we want to be able to get correct information.
		14. C: 911 call before you’re assoc and authenticated. AP does not know who you are. You are given a certificate for that temporary amount of time.
		15. C: What do you mean by encryption algorithm?
		16. R: the text of the frame.
		17. C: which frame and which field are you talking about?
		18. R: proposal doesn’t say what is protected or how it is protected. Whatever info is exchanged needs to be protected. Protocol should allow for these things to happen.
		19. Strawpoll:

We support the following FRD requirements:

The 11az positioning protocol shall have at least one secured mode that meets all of the following security requirements in associated state:

Authentication - Authenticates user identity.

Encryption Algorithm - The cryptographic cipher combined with various methods for encrypting the text.

Key Management - Create, distribute and maintain the keys.

Message Integrity - Ensures that the encrypted message\* has not been tampered with.
\* - message refers to frame and/or field(s) within the frame.

Results(Y/N/A): 19/0/5

* + 1. **Motion (#3)**

**To amend the motion in slide 14 to read:**

**Move to agree that the FRD of the 11az positioning protocol shall have at least one secured mode that meets all of the following security requirements in the associated state:**

**Authentication – Mutual authentication of initiator and responder**

**Encryption Algorithm - The cryptographic cipher combined with various methods for encrypting the text.**

**Key Management - Create, distribute and maintain the keys.**

**Message Integrity - Ensures that the protected message\* has not been tampered with.
\* - message refers to frame and/or field(s) within the frame.**

**Moved: Nehru Bhandaru 2nd: Jouni Malinen**

**Results (Y/N/A): 17/0/0**

**Motion to amend passes**

* + 1. **Motion (#4):**

**Move to agree that the FRD of the 11az positioning protocol shall have at least one secured mode that meets all of the following security requirements in the associated state:**

**Authentication – Mutual authentication of initiator and responder**

**Encryption Algorithm - The cryptographic cipher combined with various methods for encrypting the text.**

**Key Management - Create, distribute and maintain the keys.**

**Message Integrity - Ensures that the protected message\* has not been tampered with.
\* - message refers to frame and/or field(s) within the frame.**

**Moved: Chris Hartman, 2nd: Chao-Chun Wang**

**Results(Y/N/A):16/2/1**

Motion passes.

* 1. Chair remind members to log their attendance.
	2. TG recess until Jan. 18th PM1.
1. TGaz – 18 January 2017 – PM1
	1. Review Patent Policy and logistics
		1. Chair reviewed the IEEE-SA Patency Policy, additional guidelines about IEEE-SA meeting and logistics
		2. Chair called for any potentially essential patent, no one stepped up.
		3. Chair reminded all to record their attendance.
		4. Chair went through time allocation and agreed on presented time allocation for this slot.
	2. 25 people in the room
	3. Chittabrata Ghosh continued presenting 11-17-120, after posting an r1 based on feedback from yesterday.
		1. Strawpoll 2

We support the following FRD requirements:

The 11az positioning protocol shall have at least one secured mode that meets all of the following security requirements in the unassociated state:

* + - * Authentication - Mutual authentication of initiator and responder (provided there is a prior security context established).
			* Encryption Algorithm - The cryptographic cipher combined with various methods for encrypting the message\* used in 11az-positing protocol.
			* Key Management - Create, distribute and maintain the keys.
			* Message Integrity - Ensures that the protected message\* has not been tampered with
			\* - message refers to frame and/or field(s) within the frame.

Results (16/0/3)

* + 1. **Motion (#5):**

**Move to agree that the FRD of the 11az positioning protocol shall have at least one secured mode that meets all of the following security requirements in the unassociated state:**

**Authentication - Mutual authentication of initiator and responder (provided there is a prior security context established).**

**Encryption Algorithm - The cryptographic cipher combined with various methods for encrypting the message\* used in 11az-positing protocol.**

**Key Management - Create, distribute and maintain the keys.**

**Message Integrity - Ensures that the encrypted message\* has not been tampered with.
\* - message refers to frame and/or field(s) within the frame.**

**Moved: SK Yong 2nd: Assaf Kasher**

**Results(Y/N/A): 16/1/1**

**Motion passes**

* + 1. C: On Strawpoll 3, are you saying proposed solution will only be able to address these cases?
		2. R: not only, but it should be at least. This is a minimum
		3. C: what is the actual functional requirement? Encryption guarantees what?
		4. R: more details are coming in motion 4 (slide 22). This is mainly about device capability of adversary.
		5. C: can you connect strawpoll 3 and 4?
		6. R: we will do it in the motion.
		7. Strawpoll 3:

We agree that 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.

Results(Y/N/A): 13/1/9

* + 1. **Motion (#6):**

**Move to agree that 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.**

**Moved by: SK Young 2nd: Assaf Kasher**

**Results(Y/N/A) 14/2/5**

**Motion passes**

* + 1. Strawpoll 4:

The 11az protocol shall have at least one secured mode that supports privacy, authenticity and integrity against adversaries with the following response time.

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

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).

Results: 18/0/4

* + 1. **Motion (#7):**

**Move to agree that the 11az protocol shall have at least one secured mode that protects against adversaries with capabilities mentioned in Slide 20 and with the following response time.**

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

**and grant editorial rights to the FRD Editor**

**Moved by: Chittabrata Ghosh, 2nd: SK Yong**

**Results(Y/N/A): 15/1/2**

**Motion passes**

* 1. Assaf Kasher presented 11-17-[142](https://mentor.ieee.org/802.11/dcn/17/11-17-0142-01-00az-60ghz-additional-functional-requirements-for-los.pptx)
		1. C: how is likelihood calculated?
		2. R: expectation is that this is built over time. The first measurement you can have is delay spread. As time passes, there are several indicators. When you have 20 measurements, you have more information and can provide a more accurate estimate.
		3. C: what is probability of false alarm?
		4. R: what we have is based on channel measurement. We are getting 80% success ratio.
		5. C: are timestamps different in 60 vs 2.4/5?
		6. R: measurements have been done on frames without timestamps. It could be on the order of 100ms. It is performed in SW. It is not yet available on the field.
		7. C: how do you use the likelihood as opposed to binary?
		8. R: up to location server whether to include the measurement in the positioning estimation. If security disconnects me based on range, we would need higher probability of being LOS.
		9. C: what is algorithm to estimating probability?
		10. R: implementation specific.
		11. C: do you assume genie aided (LOS and NLOS knowledge)?
		12. R: the first 20 will have no information provided.
		13. C: does it also apply to SLS?
		14. R: In 11ay, we have the capability to have SLS done with TRN sequences. When SLS is done using TRN sequences, it is much faster/easier to do LOS detection.
		15. Strawpoll in slide 6:

Do you agree to add the following functional requirements to the SFD:

“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.”

“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).”

Results: 11/0/9

* + 1. **Motion (#8):**

**Do you agree to add the following functional requirements to the SFD:**

**“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.”**

**“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).”**

**Moved: Solomon Trainin 2nd: Allan Zhu**

**Results(Y/N/A): 10/0/8**

**Motion passes**

* 1. Ganesh Venkatesan presented submission 11-17-[141](https://mentor.ieee.org/802.11/dcn/17/11-17-0141-01-00az-a-proposal-for-the-11az-protocol-negotiation-phase.pptx)
		1. C: how about relative position of antennas?
		2. R: LCI would be LCI for the reference antenna. Other antennas may be located by the reference antenna.
		3. C: Is a 4 bit field enough to support antenna configuration?
		4. R: 4 bits is probably incorrect and will likely need more. This is work in progress.
		5. C: since you’re talking about adding MIMO support, the placement of antenna of client needs to be provided.
	2. Feng Jiang presented submission 11-17-[144](https://mentor.ieee.org/802.11/dcn/17/11-17-0144-00-00az-he-ftm-mesurement-phase.pptx)
		1. C: slide 4 is different from what is there in 11ax, how is the timing for UL transmission obtained?
		2. R: each STA derives timing from trigger frame on its own, the STAs are independent of each other
		3. C: consider polling in slide 4.
		4. R: reduces efficiency, but can ease complexity
		5. C: in case of SU, you wouldn’t use trigger frame as in slide 4. Trigger frame is not used for SU.
		6. C: this is only for MU?
		7. R: yes.
	3. Chair remind members to log their attendance.
	4. TG recess until Jan. 19th AM2.
1. TGaz – 19 January 2017 – AM2
	1. Review Patent Policy and logistics
		1. Chair reviewed the IEEE-SA Patency Policy, additional guidelines about IEEE-SA meeting and logistics
		2. Chair called for any potentially essential patent, no one stepped up.
		3. Reviewed the antitrust
		4. Reviewed individual voting rules.
		5. Chair reminded all to record their attendance.
	2. Chair reviewed program timelines:
		1. Timelines require update.
		2. Show of hands: when is it believable the group will complete SFD development and freeze the SFD?
			1. 4 voted for SFD freeze target should be July
			2. 3 voted for SFD freeze target should be September
		3. Review historical TG performance from PAR to D1.0.
		4. Show of hands: what is the believable PAR to D1.0 interval?
			1. Smaller than 34 months from PAR to Draft 1.0?
			2. 1 hand
			3. 34 months from PAR to Draft 1.0?
			4. 5 hands
			5. Longer than 34 months from PAR to Draft 1.0?
			6. 0 hands
	3. Group discussed what defines a Draft 0.1 and a Draft 1.0.
	4. **Motion (#9) :**

**TGaz agrees that its POR for D0.1 will meet the following criteria:**

**SFD feature freeze worthy (actual freeze happens on D1.0) in at least 2 of the focus areas.**

**The protocol is 50% complete, but not sufficiently mature to go to internal TG CR (no formal process).**

**Moved: Assaf Kasher, 2nd: Naveen Kakani**

**Results(Y/N/A): 12/0/3**

**Motion passes**

* 1. **Motion (#10) :**

**We commit to TGaz timelines as depicted in slide 36 of submission 1599r2.**

**Moved: Assaf Kasher, 2nd: Naveen Kakani**

**Results(Y/N/A): 15/0/0**

**Motion passes**

* 1. Chair went through Goals for March meeting.
	2. Teleconference schedule for March 8th at 10 AM ET for 1 hour.
	3. Chair called for any other business – none identified.
	4. Task Group meeting adjourned.