IEEE P802.11
Wireless LANs

|  |
| --- |
| TGaz Ad Hoc Meeting MinutesMarch 9th-11th, 2020Santa Clara, CA |
| Date: 2020-03-09 |
| Author(s): |
| Name | Affiliation | Address | Phone | Email |
| Roy Want  | Google Inc | 1541 Morton Ave, Los Altos,CA 94024 | +1-650-691-3600 | roywant@google.com |

Abstract

Minutes for the TGaz Ad Hoc meeting, beginning on Monday March 9th.

**IEEE 802.11 Task Group AZ**

**Mar 9-11th, 2020**

1. **TGaz Ad Hoc – Monday Mar 9th, 2020 – DAY #1**
	1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **10.40am PST** (some technical delays for telecom/network); Vice Chair (Assaf Kasher) – on bridge; Technical Co-Editor: Roy Want (Google Inc.); Acting Secretary: Roy Want (Google Inc).
	2. Agenda Doc. **IEEE 802.11-19/0237r1 (in progress)**
	3. Review Patent Policy and logistics
		1. Chair reviewed the IEEE-SA Patent Policy, and logistics – no clarifications requested.
		2. Chair called for any potentially essential patents, no one stepped up.
		3. Chair reviewed IEEE 802 WG participation as an individual professional, and anti-trust requirements – no clarification requested.
		4. Recorded Participation requirement
			1. Headcount: 14 = 8 present, 6 people on webex-telecon.
	4. Review Agenda
		1. Agenda review and setting: reviewed submissions for the ad hoc meeting.
		2. Chair called for any additional feedback and changes to agenda.
			1. Agenda agreed – no objections.
		3. C. What will we do for the March IEEE Meeting?
		4. R. Meeting cancelled – no electronic method to replace it.
		5. However, we’ll have a face-to-face meeting with an extra AdHoc in April.
	5. Nehru Bhandaru (Broadcom) presented document **11-20/0255r0**
		1. **Title**: Proposed Resolution for some LB249 CRs
		2. **Summary:** This document contains proposed resolutions for following CIDs against TGaz Draft 2.0 from LB249: 3517, 3514, 3515, 3522, 3406, 3519, 3407, 3408, 3524, 3525, 3526, 3536, 3409, 3414, 3833, 3448, 3521, 3880

The baseline documents for changes in this document are TGaz Draft 2.0 and Draft P802.11REVmd D3.0. The text in red are the instructions to the editor.

* + 1. C. [3517] Does this cover all frames when using PASN?
		2. R. Yes for 11az, but it doesn’t cover 802.11REVmc.
		3. C. [3407] Discussion if disassociation is allowed in State 1a (or State 1 from the baseline).
		4. R. This new text just clarifies the effect of Disassociation.
		5. C. [3536]. Resolved in discussion as: SA query is used to determine if there is a PTKSA security association. The intent is to have this be available in State 1a. Since SA Query is a robust management frame (Table 9-53), we need to declare it as a class 2 frame in 11.3.3 (Frame filtering based on STA state.
	1. **Lunch 12.30 – 1.15pm**
	2. Nehru Bhandaru (Broadcom) presented document **11-20/0255r0** – **Continued #1**
	3. **Break 2.55-3.10pm**
	4. Nehru Bhandaru (Broadcom) presented document **11-20/0255r0** – **Continued #2**
		1. […3448, 3521] – discussed, but not 3880 which will be considered at a later time
		2. [3524, 3525 3526] were also removed
		3. **Strawpoll**

Agree to the resolutions depicted by document **11-20-255r1** for CIDs 3517, 3514, 3515, 3522, 3406, 3519, 3407, 3408, 3536, 3409, 3414, 3833, 3448 and 3521.

* + 1. **Results** (Y/N/A): **7/0/1**
	1. Christian Berger (NXP) presented document **11-20/368r1**
		1. **Title**: 11az LB249 Comment Resolution Section 11.22.6.4.3 Part 2
		2. **Summary**: This submission proposes comment resolution for CIDs in LB249 related to section 11.22.6.4.3.

CIDs:

11.22.6.4.3.1: 3115, 3242, 3719

11.22.6.4.3.3: 3702, 3906, 3703, 3705, 3706,

 3707, 3711, 3712, 3685, 3686

11.22.6.4.3.4: 3713, 3657, 3714, 3715, 3718, 3247, 3907

* + 1. [3686] Discussion: **Rejected**: It is specifically limited to MU-MIMO only and not OFDMA
	1. **Break 4.25- 4.40pm**
		1. [3657] Discussion: **Accepted**: As proposed: “Change to "NOTE---LMR feedback is carried in Action No Ack frames (see 9.6.7.37) and is therefore neither acknowledged nor retransmitted."
	2. **Recess at 5.30pm**.

1. **TGaz Ad Hoc – Monday Mar 10th, 2020 – DAY #2**
	1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **10.15am PST**; Vice Chair (Assaf Kasher) – on bridge; Technical Co-Editor: Roy Want (Google Inc.); Acting Secretary: Roy Want (Google Inc).
	2. Agenda Doc. **IEEE 802.11-19/0237r2 (in progress)**
	3. Review Patent Policy and logistics
		1. Chair reviewed the IEEE-SA Patent Policy, and logistics – no clarifications requested.
		2. Chair called for any potentially essential patents, no one stepped up.
		3. Chair reviewed IEEE 802 WG participation as an individual professional, and anti-trust requirements – no clarification requested.
		4. Recorded Participation requirement
			1. Headcount: 21 = 9 present, 12 people on webex-telecon.
	4. Review Agenda
		1. Agenda review and setting: reviewed submissions for the ad hoc meeting.
		2. Reviewed logistics for the day.
		3. Chair called for any additional feedback and changes to agenda.
			1. Agenda agreed – no objections.
	5. Ahmet Cepni (Apple) presented document **11-20**/**374r0**
		1. **Title:** Computational Attacks on 11az PHY Secure Ranging
		2. **Summary:** Identifies security vulnerabilities associated with 11az PHY Secure Ranging operating in 2.4/5/6 GHz band. 1) These vulnerabilities could be very detrimental to secure ranging use cases envisioned by the industry (e.g., auto unlock, access control), 2) This is due to the nature of the OFDM waveform, which can be easily subject to computational attacks. 3) Imposing structure on the payload with low entropy makes the overall signaling subject to computational attacks. Presentation includes the attack model and analysis.
		3. C. For an attacker to be successful they must be close – correct?
		4. R. We assume a flat channel with directional antenna’s.
		5. C. You said computation is going to increase in capability. Why won’t new approaches be subject to the same?
		6. R. There will be a larger search space, that is computationally more challenging.
		7. C. Assumption is that the space is flat: You would have to figure out the LTF sequence 8 times (max repetition setting) in a row to be successful, with less than 1% chance.
		8. C. If go up to 80MHz (from 20MHz) the entropy is larger and reduces the problem.
		9. C. The Viterbi algorithm can be used to break any OFDM sounding signal, its not limited to a Golay sequence.
		10. C. You talked about a high-performance computational attack. How much do we need to increase the complexity to be unbreakable?
		11. C. A large horn antenna is required for high SNR, and this will be visible.
		12. R. Assume LOS, and no multipath; but the attacker only needs to find one successful example to break it.
		13. R. Repetition – won’t help.
		14. R. 20 to 80 – this makes it harder, but not that much.
		15. R A horn antenna doesn’t need to be that big.
		16. R. We need to increase entropy, a random QPSK subcarrier approach will provide that.
		17. C. What accuracy does the clock synchronization needed in the simulation?
		18. R. We did not model this part (assumed perfect).
		19. C. Assume channel flat – why can it be modelled as flat?
		20. R. Because a horn antenna provides line of sight signal capture.
		21. C. You only consider the single antenna case – what if there are two antennas?
		22. R. Only a single antenna was assumed.
		23. C. For a two antenna case it will be more secure.
	6. **Break 11-25-11-35am**
	7. Tianyu Wu (Apple) presented document **11-20/375r0**
		1. **Title**: Improved Secure LTF
		2. **Summary**: Entropy of random code (20-80MHz) is 31-43 bits. Since secured LTF is transmitted without any coding, there is a high probability that a receiver (Rx) will NOT receive all the bits correctly. So detection algorithms at Rx will need to specify a lower threshold (≪ 100%), thereby reducing the overall effective entropy of system. Assume only 80%, then the probability that a random attacker can break secure LTF is not insignificant.
		3. C. You try to increase random entropy bits from 30 to 200 bits. You can filter the 80MHz into 4 parallel 20MHz signals – Won’t this be equivalent?
		4. R. There are always ways to add resources to increase the attack. The reason we can do a fast detect is based on the Golay encoding (the main weakness).
		5. C. Perhaps focus on the Receiver as another approach.
		6. C. Considering a sub-band attack. QPSK is easier than 8PSK. It’s not easy to interpret the signal.
		7. C. As a result of using a repetition of 8 LTFs, the attack probability is negligible.
		8. C. The additional random bits also jeopardize the PAPR making it worse (reducing range).
		9. R. Perhaps its not easy to break it now, but in 5 years it would be. The new design prevents that.
		10. R. Issue similar to UWB, and by the time the protocol was finished, somebody could spoof the attack. For example, the standard was created 2007 – 2008, and the paper was published and in 2011.
		11. R. The entropy is not strong enough – we need to address this now.
		12. R. The search space is not x(250/30) but x2^(251-30). The parallel attack has its own problems with the filter shaping and ISI resulting from band bleed through. When we removed the CP that helped but it’s a Band-Aid; we need more entropy.
		13. C. There is a bottleneck in data transfer of the code for a 250 bit solution.
		14. C. There is a proposal is to remove the Golay sequence – problems?
		15. R. Other security schemes have found they need to increase the number of bits.
		16. R. How are you going to increase entropy?
		17. R. Breaking up the signal into pieces: The problem is really the Golay sequence ISI. I don’t think using repetitions is a good approach e.g. 8 – because it creates too much delay.
		18. R. 20MHz band comment: With the extra bits, the attack is not 10x, but a huge 2^200 increase in complexity.
		19. C. Filter comment: You can use a band-pass filter, and decode it into 10 units. For 250, the result would be 25 bit accurately. Then the attacker could still have a good chance.
		20. C. Repetitions of the LTF comment: The delayed LMR is about 10ms, the extra latency from the LTF repetition is much less, so not a problem.
		21. R. Don’t agree with this analysis. With a band pass filter, there will be a delay spread with ISI, so can’t rely on this as the approach.
		22. C. You are arguing 30 is not enough, but 250 is not enough using this approach; you would need even more bits. At 80MHz, perhaps 1000 bits.
		23. C. The attacker can listen to the channel, so the Viterbi approach can be used to attack too, and you would need antennas with high gain.
		24. R. A receiver should know the sequence it will receive. We want this to be a valid security solution in 10 years. Everything in the standard should be known. Repetition does not help, as it can be broken 8 times in a row.
	8. **Lunch 12.25 - 1.10pm**
	9. Christian Berger (NXP) presented document **11-20/0378r0**
		1. **Title**: Secure LTF Attacker Simulation
		2. **Summary:** Attacker tries to modify the measured range by making the STA appear closer to the AP. To fake proximity detection, the attacker can spoof time-stamps t2 or t4. However, here we focus on a physical layer attack, and assume that the MAC level is authenticated/encrypted, and includes time-stamps t1and t4 send back to the initiator.
		3. C. Several definitions need to be explained. For example, what is X?
		4. R. It’s the subcarrier for a particular tone.
		5. C. What does amplitude on slide 7 (Example: GI Replay Attack) indicate.
		6. R. It’s the attacker SINR relative to the LOS.
		7. C. You only evaluated single LTF, not the repetition
		8. R. You could get a predictable result based on this approach.
		9. C. What does the cyclic copy do (clarification)? R. See slide 8
		10. C. Does the attacker create a peak at the receiver?
		11. R. The attacker could cause a peak, or even noise could cause a peak.
		12. C. If there is a false peak, the repetition helps solve the chance of a random peak.
		13. R. Slide 24 - shows the CDF chance of this happening.

* 1. Qinghua Li (intel) presented Document **11-20/381r1**
		1. **Title:** On Brute Force Attack to 11az Secured Mode
		2. **Summary:** A concern was raised as to the strength of the secured mode against the time-domain brute force (computational intensive) attack at the sub-symbol level. This submission addresses the concern related to CID 3911.
		3. C. You are providing both mitigation of the attack and claim it’s not a problem.
		4. R. Not really – just responding to the various comments.
		5. C. Decoy start of packet approach: before the packet really beings (for attack mitigation): How does the receiver know when to start decoding the packet?
		6. R. The signal is just spread out over the real data parts, so not a problem.
		7. C. Does the staggered signal in the example (slide 17) add to the noise-floor? I have a concern the noise floor may impact the decoding of the signal.
		8. R. The extra signal can be really small (10%).
		9. C. Concern that subtracting the signals will lead to false alarms – how do you ensure they do a good job?
		10. R. The implementer needs to do a good job.
		11. C. Note the Apple approach does not do use a complex correlation attack, simply a brute force random choice attack.
		12. C. Even when attacks are computationally expensive, there will eventually be a solution.
		13. C. If we use a mitigation approach, it must be in the standard.
		14. C. Deploy now, and fix later, is not a good way for Wi-Fi to proceed.
		15. C. You don’t want to discuss proprietary solutions here.
		16. R. The current/base design is a Golay sequence, what does the new additional signal do to the PAPR?
		17. R. The additional new signal could still be Golay.
	2. **Break** **14.55 – 15.10pm**
	3. Discussion: request for additional discussion on presentations
		1. Chair: The agenda will be revised tomorrow morning and can allocate time then.
	4. Feng Jiang (Intel) presented document **11-20/383r0**.
		1. **Title**: Attacker Detections using Secured NDP
		2. **Summary**: In the secured ranging of 11az, the random HE-LTF sequence and multiple HE-LTF fields are utilized for PHY security protection.

CIDs 3354 and 3911 in LB 249 raised concerns for the security protections of ranging NDP. To resolve these CIDs, this submission evaluates the secured NDP detection performance for three different types of PHY attacks. The simulation results show that the detection performance of the current design is quite robust.

* + 1. C. What will an attack do at 0dBm? (slide 14 PRSS attack)
		2. R. Unclear need to do some additional work.
		3. C. Detection of attacker: if noise is too high, is this a denial of service attack?
		4. R. You could use a threshold to decide.
		5. C. You could consider having an estimate of the increase in noise power.
		6. C. Slide 10: Use 0.8us left of the CP: This doesn’t work if the capture signal does not go outside of the delay window.
		7. C. You could generate a fake path that can be 10dBm down that came from an attacker; this does not generate excessive noise.
		8. C. These solutions need to be in the standard. Best to increase entropy in the design. People won’t go back and read the standard on this.
		9. C. How much power is in the Attacker signal? ATMs etc are short distance applications.
		10. R. The attacker is likely to be further away and 3dBm down.
		11. C. Sending out random noise beforehand may create the issue of a false alarm.
	1. Ganesh Venkatesan (Intel) presented document **11-20/187r0**
		1. **Title**: Resolution to CID 3578
		2. **Summary**: Clarification of the various types of ranging process used in draft. The solution attempts to define each one.
		3. Presenter comment: The trigger based paragraph has some issues and will be brought back later.
		4. C. Please clarify 1) Secure TB ranging 2) Protected TB ranging.
		5. Discussion:
			1. C. TB Ranging refers to both non-protected and protected frames.
			2. Proposed definitions to be ratified later.
			Secure TB ranging session. (protected frames)
			Secure LTF TB ranging (protected frames with LTF protection)

Passive TB ranging (uses open TB Ranging).

1. **TGaz Ad Hoc – Wednesday Mar 11th, 2020 – DAY #3**
	1. Called to order by TGaz chair, Jonathan Segev (Intel Corporation) at **9.15am PST**; Vice Chair (Assaf Kasher) – on bridge; Technical Co-Editor: Roy Want (Google Inc.); Acting Secretary: Roy Want (Google Inc).
	2. Agenda Doc. **IEEE 802.11-19/0237r3 (in progress)**
	3. Review Patent Policy and logistics
		1. Chair reviewed the IEEE-SA Patent Policy, and logistics – no clarifications requested.
		2. Chair called for any potentially essential patents, no one stepped up.
		3. Chair reviewed IEEE 802 WG participation as an individual professional, and anti-trust requirements – no clarification requested.
		4. Recorded Participation requirement.
		5. Headcount: 20 = 8 present, 12 people on skype-telecon.
	4. Review Agenda
		1. Agenda review and setting: reviewed submissions for the ad hoc meeting.
		2. Chair called for any additional feedback and changes to agenda.
			1. Agenda agreed – no objections.
	5. Roy Want (Google) gave a summary of Draft D2.0 revisions based on **11-20/0017r0** comments.
		1. Technical comments completed/motioned as of Jan meeting: 70/460
		2. Editorials 438/546 (nice work from ChaoChun).
		3. We will shortly release D2.1 for the group to check, and then vote on the validity of the Editorial comments as a single batch, shown in **11-20/0017r4**, two weeks after posting to the 802.11 members area.
	6. Girish Madpuwar (Broadcom) Presented **11-20/340r2**
		1. **Title:** CR for Location
		2. **Summary:** This submission proposes resolutions of comments received from TGaz LB 249 and total 30 listed here: 3066, 3450, 3123, 3754, 3760, 3842, 3843, 3912, 3913, 3914, 3771, 3124, 3777, 3778, 3779, 3780, 3782, 3783, 3625, 3768

The comments are based on TGaz Draft 2.0 and “IEEE P802.11-REVmd/D2.4, August 2019”.

* + 1. [3450, 3123] Discussion about changes to figures – some debate.
		2. C. We should fix capitalization on field names.
		3. C. [3760 – 3913] The FTM frames contain a lot of information -- we can’t put all this in the figure, so there needs to be some compromise.
		4. Due to timing, the presentation will continue later today.
	1. Strawpoll from yesterday’s meeting for document **11-20/0375r0**
		1. Process comment rounds: 1 minute per person in queue.
			1. General summary for the two viewpoints: 1) more entropy in the secured PHY is better to address the attacks 2) the attacks can be mitigated by using the existing protocol with some additional mitigation steps (which could be up to the implementer).
		2. Request that we have a roll call.
			1. R. [Vice chair] Roll calls are limited to motions.
		3. **Strawpoll**
		4. Do you agree to remove the Golay structure and increase the entropy of a secure LTF symbol to a minimum of 244 bits?
		5. **Results** (Y/N/A): 11/16/8

* 1. Girish Madpuwar (Broadcom) Presented **11-20/340r2 - Continued**
		1. C. [3124] Suggest to remove STA info field as referenced here.
		2. C. Modifications to figures 11-36n proposed, seem old?
		3. C. Looks like some of these comments are referring to a document prior to D2.0
		4. No Strawpoll at this time as the revision of the base document is not correct.
	2. Break 10.55 – 11.10
	3. Assaf Kasher (Qualcomm) presented document **11-20/388r1**
		1. **Title: LB249-Clause-9-4-CIDs**
		2. **Summary:** This document proposes resolutions to LB249 comments on subclause 9.4. The base is TGaz D2.0. The CIDs are 3648, 3026, 3027, 3262, 3573, 3574, 3575, 3028, 3029, 3638, 3870, 3916, 3918, 4000, 4001, 4002, 3042, 4003.
		3. C. [3648] Revised with additions: “The LOS Assessment TX subfield is set to 1 to indicate that the STA can participate as an RSTA in a…”
		4. C. [3575] We don’t need to have the HE TB in this table as it has its own table.
		5. C. Why does it say format for EDCA? There is no EDCA PDU.
		6. C. Add a note to qualify the EDCA SU-PDU content.
		7. C. [3940] The RSN bit should be separate from the PMF extended capabilities bit.
	4. **Lunch 12.20 -1.10pm**
	5. Assaf Kasher (Qualcomm) presented document **11-20/388r1 - continued**
		1. C. No discussion on proposed Strawpoll.
		2. **Strawpoll**
		3. We agree to the resolution depicted in document **11-20-0388r2** for CIDs 3648, 3026, 3027, 3262, 3573, 3574, 3575, 3028, 3029, 3638, 3916, 3918, 4002, 3042 and 4003.
		4. **Results** (Y/N/A): 9/0/1
	6. Christian Berger (NXP) – unavailable - presentation slot switched below:
	7. Niranjan Grandhe (NXP) presented document **11-20/379r0**
		1. **Title**: 11az LB249 Comment Resolution Section 11.22.6.4.4
		2. **Summary** : This submission proposes the comment resolution of CIDs (3722, 3727, 3728, 3730, 3731, 3732, 3733, 3735, 3738, 3739, 3908, 3255, 3256, 3257, 3258, 3742, 3743, 3745, 3746, 3467, 3259, 3747, 3260) in LB249 apropos section 11.22.6.4.4.
		3. General Discussion.
		4. [3908] Reject: This part just defines the RTT equation at RSTA and there is no need to add anything about ISTA2RSTA LMR feedback and it is obvious that timestamps t1, t4 won’t be available at RSTA.
		5. **Strawpoll**
		6. In the formula computing the RSTA RTT do we need to specify conditional sharing of I2R LMR?
		7. **Results** (Y/N/A): 4/5/2
	8. **Break at 3.30 – 3.45pm**
	9. Niranjan Grandhe (NXP) presented document **11-20/379r0**
		1. C. General discussion. No discussion of Strawpoll needed.
		2. **Strawpoll**

We agree to the resolution depicted in document **11-20-0379r1** for CIDs 3722, 3727, 3728, 3730, 3731, 3732, 3733, 3735, 3738, 3739, 3908, 3255, 3256, 3257, 3258, 3742, 3743, 3745, 3746, 3467, 3259, 3747 and 3260.

* + 1. **Results** (Y/N/A): 9/0/2
		2. Note: represents a batch of 5% of the total technical CIDS.
	1. Christian Berger (NXP) presented document **11-20/366r0**
		1. **Title**: 11az LB249 Comment Resolution Section 9.3.1.19
		2. **Summary**: This submission proposes the comment resolution of CIDs in LB240 related to Section 9.1.3.1.19. CIDs for Section 9.3.1.19: 3503, 3504, 3193, 3009, 3101, 3192, 3848, 3894, 3010, 3011, 3222, 3431, 3710. Revisions: Added text to section 11 to specify how to populate STA Info fields in the Ranging NDP Announcement frame.
		3. **Strawpoll**We agree to the resolution depicted in document **11-20-0366r2** for CIDs 3503, 3504, 3193, 3009, 3101, 3192, 3848, 3894, 3010, 3011, 3222, 3431 and 3710.
		4. **Results** (Y/N/A): **10/0/1**
	2. **Any other Business (AOB)** : None
	3. **Adjourned 5.30pm**.

**References**

1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0237-03-00az-tgaz-march-ad-hoc-agenda.pptx>
2. <https://mentor.ieee.org/802.11/dcn/20/11-20-0255-01-00az-lb249-crs-nb.docx>
3. <https://mentor.ieee.org/802.11/dcn/20/11-20-0368-01-00az-comment-resolution-lb249-section-11-22-6-4-3-part-2.docx>
4. <https://mentor.ieee.org/802.11/dcn/20/11-20-0374-00-00az-computational-attacks-on-11az-phy-secure-ranging.pptx>
5. <https://mentor.ieee.org/802.11/dcn/20/11-20-0375-01-00az-improved-secure-ltf.pptx>
6. <https://mentor.ieee.org/802.11/dcn/20/11-20-0378-00-00az-secure-ltf-attacker-simulation.pptx>
7. <https://mentor.ieee.org/802.11/dcn/20/11-20-0381-00-00az-on-brute-force-attack-to-11az-secured-mode.pptx>
8. <https://mentor.ieee.org/802.11/dcn/20/11-20-0383-00-00az-attacker-detection-using-secured-ndp.ppt>
9. <https://mentor.ieee.org/802.11/dcn/20/11-20-0187-00-00az-resolution-to-cid-3578.docx>
10. <https://mentor.ieee.org/802.11/dcn/20/11-20-0017-04-00az-lb249-comment.xlsx>
11. <https://mentor.ieee.org/802.11/dcn/20/11-20-0340-02-00az-lb249-ftm-negotiation-and-exchange.docx>
12. <https://mentor.ieee.org/802.11/dcn/20/11-20-0388-02-00az-lb249-clause-9-4-cids.docx>
13. <https://mentor.ieee.org/802.11/dcn/20/11-20-0379-01-00az-cr-for-section-11-22-6-4-4.docx>
14. <https://mentor.ieee.org/802.11/dcn/20/11-20-0366-02-00az-comment-resolution-lb249-section-9-1-3-1-19.docx>