IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Teleconference Minutes 14 April 2022 |
| Date: 2022-04-25 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Amelia Andersdotter | Sky UK Group | Brussels, Belgium |  | amelia.ieee@andersdotter.cc |

**Chair: Carol Ansley, Cox Communications**

Abstract

This document contains the minutes for the IEEE 802.11bi task group meeting that took place on 14 April 2022 at 09:00 ET.

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

Yellow highlight - action point

**Secretary: Amelia Andersdotter, Sky UK**

**Vice-chairs: Jerome Henri, Cisco; Stephen McCann, Huawei**

**Technical editor: Po-Kai Huang, Intel**

Chair calls meeting to order at 09:03 ET.

Agenda slide deck: 11-22-622r1:

1. Reminder to do attendance
2. Review of policies and procedures.
3. The chair mentioned the call for essential patents
	1. No one responded to the call for essential patents
4. The chair covered the IEEE copyright and participation rules.
	1. No questions
5. **Discussion of agenda 11-22-622r1 (slide #16)**
	1. Submission 11-22-623 from Jarkko Knecht uploaded on mentor.
		1. Contains new requirements.Is there agreement to cover ahead of requirements covering issues 1-3 from Requirements document 11-21-1848r6 as in proposed agenda for today?
	2. Agenda amended to review 11-22-623.
	3. Adoption of agenda 11-22-622r1 slide #16 as amended by unanimous consent (17 participants).
6. **Presentation**
	1. **Privacy Requirements (11-22-623r0), Jarkko Knecht (Apple)**The split between CPE and BPE proposed in 11-22-107r2 endorsed. Adds requirements to the ones already proposed.

**Discussion:**

**Q:** Comment on the client-side requirements. For sensing and ranging stuff, I was wondering in your proposed requirements F2 and F3, the MAC header is mentioned in F2. I mean, MAC headers will already be implicated by the first proposal in CPE-F1 requirements, right?
**A:** F1 was built to target sensing measurements, and F2 takes into account that these measurements affect other fields too. What we've tried to capture is that it's not just data frames but also other frames. Perhaps we could collapse F1 and F2, but it was for clarity here.
**Q:** But now if you go back to C-requirements, you don't have the same level of specifity?
**A:** I'll go back and have a look at this. I think CPE-F1 is clear since it deals with data transmissions and changing MAC addresses - here we'd have different MAC addresses for different measurements so that simultaneous measurement procedures don't lead to data leakage.
**Q:** Ah, but you want to be more clear here. We also have COUNSEL frames(?) for instance and they're not mentioned, it makes me wonder. But the key thing here is that you want yet another MAC address for sensing?
**A:** Yes, essentially, yes. You could have different MAC address sets for different sensing and measurements operations, or groups of operations.
**Q:** It seems you want to treat sensing completely different from all the other things, but the MAC header is like. But anyway, the thing is it's not clear to me what you're targetting here with the difference. You might want different keys even.
**A:** We can introduce new keys, new sequence numbers, etc. We're open to discussion on all these things even if I believe the same keys can continue to be used. The idea here is only to not make cross-correlation possible from multiple simultaneous sensing operations.
**Q:** Further on the MAC header, SN/PN related to issue 3... There are a number of requirements that relate to MAC addresses over-the-air here and I'm wondering if they don't cover issue 7 as well.
**A:** That is possible, we're open to that modification. The classification of issue 3 is straight-forward here though, since a change of MAC address to avoid tracking requires all these changes to happen that are described here. The SN/PN stuff that is listed here needs to be here as covering issue 3 since they're incremented over time, predictably, and following that would allow tracking over time. So I don't think that classification is wrong.
**A:** With SN/PN fields you can detect that they belong to a specific MAC address since they monotonically increase, so issue 3 is the correct classification. For TID it's different, since there is no straight connection to the MAC address. We could add an issue 7 classification too, and we can keep discussing that of course.
**C:** I think the original proposal was to have SN/PN and TID classified as both issue 3 or issue 7, but it can be discussed. On the BSS side it was definitely originally proposed as addressing both.
**Q:** You've struck out "minimum IE in Beacon and Probe response" and I was wondering if we could keep that for now? We may not be able to encrypt all of that information so just wondering if as a safe-guard we could keep this.
A: In the beacon frames I agree that we're discussing what we can keep and encrypt. My view is that it's possible to encrypt everything for the moment, and I discussed with some people. Perhaps in real-time we need to be more flexible, or for probe responses. It may even be necessary to explore other ways entirely of doing this.
**Q:** I also want to ask about randomizing TBTT? Quite a lot of features rely on this so that could bring a host of follow-on challenges?
**A:** Yes, we thought about it. Maybe we can control the extent of randomization in the same way that we calculate the next MAC address, for instance. What we want to avoid is having very long times between transmitting two beacons.
**Q:** Many of these changes could challenge existing implementations quite a bit. You have some PHY layer proposals as well. We would need some more time to evaluate that. Currently, when the AP wants to retransmit, the frame is not re-encrypted. But if we encrypt the re-try bit we may have to do that and that will imply some pretty big changes.
**A:** We added the encryption of the re-try bit for completion and it could be an optional requirement, for instance.
**Q:** On slide 11, do you mean we could have different MAC addresses for different purposes?
**A:** Yes, a new kind of address that would be purpose-specific for sensing. To separate data transmissions from sensing.
**Q:** And is that extensible to other frames too? Or just two?
**A:** We propose two here, but we'd be hoping to change the unicast addresses one by one too, and then we would end up with different MAC addresses that the AP would use for unicast and group-addressed messages to the same non-AP STA, for instance.
**Q:** I think if we randomize beacon transmission times, that, in my view, should be randomized only from the outside point of view, but the non-AP STA and AP need to be able to predict this somehow.
**A:** Agreed - the aim here is to introduce some low level of predictability, or avoiding perfect regularity.
**C:** Thank you for clarification.
**C:** For encrypting the MAC header we would need a new cipher or key management, I don't think this is a trivial change at all.
**A:** We can discuss that of course. Let's keep on talking on that point.

**Chair:** We are almost out of time. We will pick up the rest of our agenda next week.

1. AoB
	1. No other business.
2. Chair adjourned the meeting at 09:58 ET.

**Attendance**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Andersdotter, Amelia | Sky UK Group |
| Ansley, Carol | Cox Communications Inc. |
| baron, stephane | Canon Research Centre France |
| Halasz, David | Morse Micro |
| Ho, Duncan | Qualcomm Incorporated |
| Huang, Po-Kai | Intel Corporation |
| Kain, Carl | USDOT; Noblis, Inc |
| Levy, Joseph | InterDigital, Inc. |
| Lumbatis, Kurt | CommScope, Inc. |
| Luo, Chaoming | Beijing OPPO telecommunications corp., ltd. |
| Mutgan, Okan | Nokia |
| Rosdahl, Jon | Qualcomm Technologies, Inc. |
| Sam, Harvey | Broadcom Corporation |
| Sevin, Julien | Canon Research Centre France |
| Smith, Graham | SRT Wireless |
| Smith, Luther | Cable Television Laboratories Inc. (CableLabs) |
| Stanley, Dorothy | Hewlett Packard Enterprise |
| Yee, Peter | NSA-CSD |