Minutes IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IEEE 802.11 TGbh Meeting Minutes, October 11, 2022  Randomized and Changing MAC addresses (RCM) | | | | |
| Date: 2022-10-11 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Peter Yee | NSA-CSD | Mountain View, CA |  | peter@akayla.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh telecon meeting of October 11, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting October 11, 2022 9:30 a.m. to 11:30 a.m. ET**

**Chair: Mark Hamilton (Ruckus/CommScope)**

**Vice Chair: Peter Yee (NSA-CSD/AKAYLA)**

**Vice Chair: Stephen Orr (Cisco)**

**Secretary: Peter Yee**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by the Chair at 9:32 a.m. EDT.**

Agenda slide deck [11-22/1735r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1735-00-00bh-agenda-tgbh-2022-oct-11.pptx)

1. **Policies and procedures were presented by the chair. (Slides 4 to 14)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 10 and 11)

1. **Agenda:**

* **Attendance, noises/recording, meeting protocol reminders**
* **Policies, duty to inform, participation rules**
* **Organization topics (see Backup slides)**
  + Sept to Nov teleconferences: Tuesdays, every other week, 9:30-11:30 am ET (this time slot)
  + Timeline reminder (slide 20)
* **Issues Tracking:** [**11-21/0332r37**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Results of Comment Collection on D0.2:** [**11-22/0973r11**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-11-00bh-cc41-comments-against-d0-2.xlsx)
* **Continue discussion on resolutions of ones that are NOT on topics: Opt-in, Pre/un-association, Non-AP STA-generated ID**
  + [11-22/1599r2](https://mentor.ieee.org/802.11/dcn/22/11-22-1599-02-00bh-revisions-to-rsn-extension-element.docx) – Revisions to RSN Extension element (Kurt Lumbatis) (updates to be posted, for motion)
  + [11-22/1218r5](https://mentor.ieee.org/802.11/dcn/22/11-22-1218-05-00bh-device-id-synchronizatoin-and-control.pptx) – Device ID synchronization and control (Kurt Lumbatis) (flow diagram requested)
  + [11-22/1329r6](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-06-00bh-cid-resolutoins-for-12-2-11.docx) – CID resolutions for 12.2.11 (Kurt Lumbatis)
  + [11-22/1620r2](https://mentor.ieee.org/802.11/dcn/22/11-22-1620-02-00bh-device-id-ladder-diagram.pptx) – Device ID ladder diagram (Kurt Lumbatis)
  + [11-22/1588r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1588-00-00bh-resolution-comment-32-11bhd0-2.docx) – Resolution comment 32 (Antonio de la Oliva)
  + [11-22/1665r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1665-00-00bh-deviceid-renaming-discussion.pptx) – Device ID renaming discussion (Antonio de la Oliva)
  + Walk-through CIDs status
  + ~1 hour
* **Contributions on topics: Opt-in, Pre/un-associated, Non-AP STA-generated ID (slide 16)**
  + ~1 hour
* **WBA liaison response**

Any comments?

Q- 11-22/1732 is ready. Will it be discussed today?

A- It might be if Graham Smith doesn’t show up.

Q- It shouldn’t be considered controversial [yet] – we haven’t discussed unassociated use cases.

A- I disagree.

Q- Any other comments?

A- [None.]

Any objections to agenda? [None]

1. **Device ID Ladder Diagrams**

Kurt Lumbatis (ARRIS/CommScope) made a presentation ([11-22/1620r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1620-02-00bh-device-id-ladder-diagram.pptx)), which is based on a request during the September interim meeting for ladder diagrams to clarify what happens during the various scenarios of Device ID support. It covers these scenarios:

* No Device ID support
* Device ID support AP only
* Device ID support STA only
* Device ID support both AP and STA; STA has no ID or chooses not to send previous ID
* Device ID support both AP and STA; STA sends previously assigned ID
* Device ID support both AP and STA; STA is using FILS but has no ID or chooses not to send it
* Device ID support both AP and STA; STA is using FILS and provides previously assigned ID

C- In the Device ID support STA only, if the AP doesn’t support it, the STA won’t set the bit to one.

C- You are correct.

C- We could leave it as a don’t care.

C- I remember that if the AP doesn’t support the feature, then the STA doesn’t set the corresponding flag either.

C- I don’t feel strongly about it.

C- For both support and STA providing previous ID, the STA could provide some ID back to help against eavesdropping.

C- That’s covered in the list of three options of what the AP may do in response. Returning the same ID by the AP is positive feedback. The AP could always return a new ID if there’s a desire to hide any status information from an eavesdropper.

C- Option 2 (return the same ID) and option 3 (return no ID) on slide 8 seem the same. I think they can be merged into one option.

C- There was a desire to save on bandwidth, hence option 3’s existence.

Q- Is there consensus in the group to always return an ID and remove option 3.

A- [No objection.]

C- Please make that change in the next revision of the document.

C- I would assume that change also applies to slide 10 (FILS and Device ID both turned on).

C- That seems likely.

Kurt Lumbatis to revise the document and post to mentor, along with posting a note to the reflector.

C- After posting and mentioning this change on the mailing list, we will see if there are any objections.

Kurt Lumbatis to discuss offline with Mark Hamilton on a presentation for the resolution for CID 15.

1. **Resolution for CID 19 and CID 20**

Okan Mutgan presented [11-22/1732r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1732-00-00bh-resolution-for-cid19-and-cid20.pptx). Both CIDs focus on PASN (Pre-Association Security Negotiation). CID 19 asks for PASN support with Device ID. CID 20 wants 11bh not to break multi-AP ranging operations. Mutgan explained the PASN messages and how they are used to generate a key for FTM (fine timing measurement) protection.

Q- On slide 5, which messages are encrypted?

A- None of them are. The messages are just to set up a PTK (for FTM encryption purposes).

CID 19 covers the case of an unassociated STA that performs FTM. Because the STA does not do the 4-way handshake, it won’t have a Device ID. CID 20’s issue is that operations between a STA and multiple APs can have a different random MAC address per AP. The proposed solution for CID 19 is sending the Device ID in the PASN Authentication frames (messages 1 and 2). To be clear, these are not encrypted messages. Slide 9 covers the ladder diagram, with ‘aaa’ being the opaque form of the ID (‘111’). For CID 20, the solution is to assign a Device ID for each FTM session in the ESS, *i.e.*, for each AP with which the STA is performing ranging operations.

Q- Does slide 10 prevent simultaneous FTM sessions? Or is this PASN only that’s sequential?

A- This would be PASN probably. The sessions should be allowed to be simultaneous.

C- A separate question is whether each AP requires a PASN setup or one is used for all APs in the ESS.

Q- Are we trying to identify the device without knowing whether it actually wants to exchange data. In the pre-associated state for a STA that only wants to do ranging, what’s the benefit of a STA allowing itself to be identified.

A- In original FTM (IEEE 802.11-2016), there’s no PMK & PTK. The FTM is done in the clear. PASN adds PMK & PTK generation. The proposal is for Device ID exchange in the Authentication Request/Response frames. The frames shown on slide 4 are in the context of PASN.

C- There would have to be a decision on the STA side if it wants to do FTM.

C- PASN doesn’t have to be used for FTM only. And if we do Device ID, anything that uses PASN can benefit from that.

C- To be clear on slide 10, for FTM session 3, it should read Msg1 and Msg 2, not Msg 2 and Msg 3.

C- If a STA needs to set up multiple sessions with different APs, each one will get a different PTK.

Q- I think we still have the question if there are separate PASNs and whether the FTM sessions can happen in parallel. I think they can. Does our ID scheme work if the STA gets a different Device ID each time it does a PASN? Will it all still work?

Okan Mutgan will check that.

Q- This violates a core value that the Device ID should be encrypted. Is the group okay with using such a scheme?

A- One thought is that the scheme works fine as long as the STA understands it is sending information in the clear and does so willingly. With an opaque ID changed frequently, a third party wouldn’t be able to track the STA. The alternative is to wait until the PASN is established and then using the PTK to protect the transmission of the Device ID.

C- I was thinking that once the PTK was established, the identifier comes across encrypted in message 3.

C- That would be ideal, but it’s not defined here.

C- I don’t think having the opaque ID really solves the problem. There’s still enough information for an eavesdropper to determine that it is a returning session. The other aspect is that the opaque ID that’s being returned in association 2, even if randomized, it will show that it is the same device returning.

C- If the group has concerns about the security of sending the ID in message 1, it can be moved to message 3, although that looks a little odd in terms of the sequencing of events. But message 3 can be used to encrypt the Device ID from the STA to the AP.

C- Even in message 3, you can sniff the information element. We could use encryption in message 2 for sending the new Device ID and message 3 for sending the Device ID.

C- But that doesn’t work initially. It’s a chicken-and-egg problem. If the STA doesn’t have an ID and the AP wants to set one, it could use the derived PTK.

C- That’s similar to how the 4-way handshake works.

C- Yes, except the directions are reversed. We could say the AP always sends it encrypted in message 2 and acknowledges it in message 3.

C- Message 1 could also say, “I have an ID.”

Q- Do we have consensus that we want to encrypt the device ID?

A- I don’t think it matters that the STA has a Device ID in message 1. In message 2, the AP always assigns a new Device ID. The STA always sends its current Device ID in message 3. I think it always works.

C- [Chat] We have to encrypt the Device ID.

C- If I understand correctly [on slide 9], the 2nd association doesn’t have to an encrypted message 1 because the content is already opaque because the information was sent encrypted in message 2 of the previous association.

C- Sending things unencrypted is unsatisfying. It would seem that there could be trackability. Of course, the AP could also be tracking. RCM added some level of privacy from an eavesdropper. Whether you want the AP to know that a STA is returning should be a choice of the STA’s user. I’m finding the slides confusing as to when things are encrypted and not encrypted.

[Mutgan revised the presentation to show encrypted and unencrypted solutions for CID 19.]

C- Please show the new slide for CID 19 with encryption of the Device ID in message 2. With the opaque version of the ID encrypted in message, on the 2nd association, sending the unencrypted opaque ID doesn’t reveal any information, at least as long as a new ID is used every single time. There’s no chain of unencrypted IDs being transmitted that can be tracked by a third party.

Q- How does the original key for the first encryption get set?

A- That’s the PTK set during the PASN process. In message 2, the AP has already derived the PTK.

C- The problem with that is that you have encrypted and unencrypted versions of the ID that have been transmitted over the air. You should avoid that. [Otherwise there would be plaintext and ciphertext pairs available to an eavesdropper.]

C- This is one option. The eavesdropper hears the encrypted opaque ID in message 2 of the first association. Then, hearing the unencrypted version in the next association, over time, the password might be weakened. If the MAC addresses are randomized on every FTM procedure, that might help.

C- Even that might not be sufficient to break correlation.

Q- Is that only if they want to use PASN?

A- Yes, PASN and with this scheme in particular.

Q- Is there anything in 11bi we need to know about?

A- We have not motioned any solutions in 11bi. But we do have requirements.

Q- Thank you for capturing all of this in real time. We should have security people look at it. Do we think the revised slide 10 is complete at this point?

A- That version uses encrypted frames, although on the 2nd association, the AP generates an ID even though it doesn’t know if the STA is going to use it.

C- I like that message 1 carries an unencrypted bit that says, “I have an identifier”. Then the AP doesn’t have to send one in message 2.

C- Remember that we said that the AP would always send an identifier.

Q- Why does the STA send the old identifier in message 3 after receiving a new identifier in message 2?

A- So that the AP can correlate the two, even though it looks backwards.

C- This was helpful. Okan, please post the update. Let’s get some security folks to look at it.

Q- Should we have some cooperation with 11az to make sure things work?

A- There’s no question that 11az will be standardized before our amendment. I don’t think we have to talk to anyone in 11az, but maybe because we are encrypting part of the message, which is new, we might?

C- We could just say that we encrypt only the Device ID information element.

C- That was my assumption. It would be on top of 11az and wouldn’t perturb anything in 11az. They are nearly done with their standard.

C- My suggestion is that we don’t change the Authentication frame body, just add a Device ID information element that doesn’t clash with 11az.

Q- Should this new version be presented in the next meeting to straw poll which version of the encrypted scheme is desired? Or should text be prepared now?

A- Let’s post the new version to the reflector and see what the security folks think. Then we can decide to generate text.

C- Please move the assignment of CIDs 19 and 20 from Jay Yang to Okan Mutgan.

C- Okay.

1. **WBA liaison response**

We will come back to this when we have something substantive to tell them.

**Meeting adjoined at 11:09 a.m. EDT.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 10/11 | Ansley, Carol | Cox |
| TGbh | 10/11 | Baron, Stephane | Canon |
| TGbh | 10/11 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 10/11 | Kain, Carl | USDOT, Noblis |
| TGbh | 10/11 | Lumbatis, Kurt | ARRIS/CommScope, Inc. |
| TGbh | 10/11 | McCann, Stephen | Huawei |
| TGbh | 10/11 | Mutgan, Okan | Nokia |
| TGbh | 10/11 | Nezou, Patrice | Canon |
| TGbh | 10/11 | Orr, Stephen | Cisco |
| TGbh | 10/11 | Sam, Harvey | Broadcom Corporation |
| TGbh | 10/11 | Sevin, Julien | Canon |
| TGbh | 10/11 | Smith, Luther | CableLabs |
| TGbh | 10/11 | Stanley, Dorothy | HPE |
| TGbh | 10/11 | Sun, Bo | Sanechips |
| TGbh | 10/11 | Thakore, Darshak | CableLabs |
| TGbh | 10/11 | Thakur, Sidharth | Apple |
| TGbh | 10/11 | Yang, Jay | Nokia |
| TGbh | 10/11 | Yee, Peter | NSA-CSD |