IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Minutes Mixed Mode Plenary Session 15-19 May 2023 |
| Date: 2023-05-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Stephen McCann | Huawei Technologies Co., Ltd  | Southampton, United Kingdom |  | stephen.mccann@ieee.org |
| Lili Hervieu | CableLabs |  |  | l.hervieu@cablelabs.com |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |

Abstract

This document contains the minutes for the IEEE 802.11bi task group meeting that took place during the IEEE 802 Mixed Mode Plenary Session 15-19 May 2023. The on-site location for the meeting was Orlando, Florida, USA.

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

Yellow highlight - action point

**Chair: Carol Ansley, Cox Communications**

**Secretary: Amelia Andersdotter, Sky UK**

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

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

**1st slot. Monday 15 May 2023, 13:30 local time.**

Chair calls meeting to order at 13:32 local time.

Agenda slide deck: [11-23-0574r2](https://mentor.ieee.org/802.11/dcn/23/11-23-0574-02-00bi-may-interim-agenda.pptx):

1. Reminder to do attendance. Reminder to register for the session and to not attend the virtual meeting without paying appropriate meeting fees.
2. The chair mentioned the call for essential patents
	1. No one responded to the call for essential patents
3. The chair covered the IEEE copyright and participation rules.
4. **Discussion of agenda 11-23-0574r2**
	1. Further submissions added to the agenda.
	2. Agenda as amended approved by unanimous consent (30 remote participants, 20 in-room)
5. **Administration**
	1. **Motion #30**

	**Approve the minutes for:**

**2023 March 802.11 Plenary: 11-23/500r0,**

**TGbi Teleconferences: 11-23/819r0 (11 May)**

Moved: Stephen McCann, Seconded: Antonio de la Oliva

Approved by unanimous consent (35 remote participants, 20 in-room)

* 1. Discussion about the meeting slots this week.

An extra submission was added.

There was some discussion about whether the Wednesday PM2 slot should be cancelled or not. The conclusion was to wait until Tuesday to decide this.

1. **Technical Presentations**
	1. **Support for rotating MAC addresses (**[**11-23/0850r0**](https://mentor.ieee.org/802.11/dcn/23/11-23-0850-00-00bi-ccmp-mac-rotation-spec-text.docx))**,** Antonio de la Oliva (InterDigital)

	This submission tackles the required modifications to the standard to support modification of the A2 MAC Address while the STA is associated. This contribution tackles MLD and non-MLD cases, and PV0 frames. Baseline for this document is REVme\_D2.0.

**Discussion:**

Q: As the over the air MAC address corresponds to the lower MAC address, wouldn’t it be better to protect the upper MAC address?

A: This has been discussed before and it’s the address over the air that requires protection.

C: The question is whether TGbi should apply to pre TGbe (legacy STAs). I think it should only apply to MLDs.

Chair: Perhaps 11bi should apply to legacy devices?

C: I think that 802.11 is a toolbox of solutions for the Wi-Fi industry. I don’t think privacy should be restricted to MLD devices. I think it should be also applicable to STAs.

C: I think applying privacy for only MLD devices, then stops many IoT devices from having privacy.

C: Perhaps privacy could be optional for legacy devices, but mandatory for MLD.

C: The optional/mandatory issue is usually decided in the PICs of the draft. However, TGbi is only making a recommendation of what products do in the market.

C: I think there are legacy APs that require privacy. Therefore, I think we need to have privacy for both STAs and MLDs.

C: I would like to point out that 11be defines an MLD as a separate entity to a STA. Therefore, a change to the TGbi PAR may be required.

C: Privacy is an abstract concept, so it should be applicable to all devices.

Chair: Some of the technical submissions are discussing MAC addresses, which can be implemented.

C: Therefore TGbi should be talking in terms of supplicants and authenticators, and not STAs and MLDs. In otherwords privacy should be abstracted away from device types.

C: Yes, but TGbi needs to deal with specific MAC addresses from affiliated STAs in MLDs. These are legacy MAC addresses. For tracking purposes, we are still dealing with STA MAC addresses.

C: I think there should be different approaches for dual radio devices, as opposed to mobile APs?

I think updating legacy devices to 11be should be possible.

C: This submission really sets out to rotate MAC addresses for MLDs.

* 1. **Anonymizing Frames (**[**11-23/0414r2**](https://mentor.ieee.org/802.11/dcn/23/11-23-0414-02-00bi-a1-filtering-for-rotating-mac-addresses.pptx))**,** Antonio de la Oliva (InterDigital)

	This document proposes a mechanism enabling A1 filtering.

Proposal includes discussion on the anonymization/de-anonymization block.

**Discussion:**

Q: If the AP receives a frame from the STA that has a MAC address change, does the AP know?

A: Yes, as the AP knows the block of addresses that are being used.

Q: Therefore, the AP needs to keep track of n addresses.

A: Yes.

Q: This is using a set of addresses for each frame transmission. The submission says that a DSMAC can be used over the air (slide #12). I think this will be a bad thing.

A: The submission should only transit mapped addresses and not the DSMAC. I need to change to figure on Slide #8.

C: This method requires more resources such as memory and proposing.

Q: I think this submission is similar to the previous submissions. How do you select the set of addresses and how long are they valid for? Therefore, if the sets are used for a long time, then they can be tracked.

A: The scheme uses n addresses at the same time. All of these addresses are used all the time. They do not need to be changed.

Q: The scheme uses a fixed set of addresses which do not change. Therefore, they can be correlated over a period of time. Refreshing them may be useful?

A: Every time you re-associate, the set is changed.

C: The pair of STAs can exchange the set whenever they wish. It’s like a soft handover. When a MAC address times out, you can exchange anyone of them. The pool of addresses can change. However, the basic mechanism is valid.

Chair: I think queue management is essential in this situation. In addition to the MAC addresses, other values such as sequence or packet numbers also have to be changed.

A: This will be dealt with by an anonymization block.

Q: When the MAC address changes, how do you change any associated values?

A: This mechanism is just for the MAC addresses. Associated values (e.g. frame numbers) would have to be dealt with by another mechanism.

1. **AoB

802.15 Privacy Study Group**

During the Tuesday AM2 meeting, 802.15 will be having a meeting of their privacy study group. They would like to invite TGbi members to attend.

1. **Recess 15:15 local time.**

**2nd slot. Tuesday 17 May 2023 08:00 local time.**

1. **Meeting called to order at 08:09 local time.**
2. **Reminder of policies and procedures (see para 1-3 above under 1st slot).**
	1. Reminder to do attendance issued, together with reminder to register for meeting.
	2. No response to call for essential patents.
	3. Reminder of policies and procedures.
	4. Copyright policy was presented.
3. **Review of agenda** [**11-23-0189r4**](https://mentor.ieee.org/802.11/dcn/23/11-23-0189-04-00bi-march-plenary-agenda.pptx) **(slide #18)**
	1. Agenda approved by unanimous consent (21 participants online, 13 in the room).
4. **Technical presentations**
	1. **Proposed spec texts for protected version of unicast management frames** ([11-22-1975r4](https://mentor.ieee.org/802.11/dcn/22/11-22-1975-04-00bi-proposed-spec-texts-for-protected-version-of-unicast-management-frames.docx)), Po-Kai Huang (Intel)

	The proposed spec text contains an update to the previously presented proposal to introduce protected management frames.

	**Discussion:**

	**C:** We should advertise this more broadly. This will have many applications outside of enhanced data privacy. We don't want to have to do this per frame in future.

	**Strawpoll:** Approve text in 22/1975r4 to go into Draft 0.1?
	Result: Yes: 10, No: 2, Abstain: 5, No Answer: 5
	2. **Proposed spec texts for 802.1X authentication utilizing authentication frame** ([11-23-0031r3](https://mentor.ieee.org/802.11/dcn/23/11-23-0031-03-00bi-proposed-spec-texts-for-802-1x-authentication-utilizing-authentication-frame.docx)), Po-Kai Huang (Intel)

	Proposal introduces a mechanism for using authentication frames for 802.1X authentication.

	**Discussion:**

	**C:** This is authentication algorithm number 8. .1X authentication is a very specific thing, is this still it?
	**C:** .1X establishes EAPOL key after association. This proposal changes the container of that key.
	**Q:** There are a number of references to AKMP? Is the outcome of the exchange you're specifying defined?
	**A:** The AKMP is to verify the AKM. Derivation of the PMK is not defined here, because this proposal only covers the container.
	**C:** In .1X the authenticator always initiates the authentication. This proposal calls for authenticator to signal supplicant to initiate authentication. This needs to be revised.
	**A:** This is fine. We could simplify this.
	**C:** I need to make the point that all these frames are authentication frames and therefore use EAP. The order of the messages in the presentation are incorrect.

**Chair:** Do you want to have any straw polls about this submission?

**C:** No, I don’t think it’s necessary.

**Q:** Are you planning to use SAE at the same time?

**A:** No, this has nothing to do with SAE. This is about 802.1X.

* 1. **AID modification upon MAC address change** ([11-23-0336r1](https://mentor.ieee.org/802.11/dcn/23/11-23-0336-01-00bi-aid-modification-upon-mac-address-change.pptx)), Stephane Baron (Canon)

	Proposal is a mechanism for changing the AID when the MAC is changed. Both sides computes a new MAC and a new AID. This computation is done locally at each STA to avoid transmitting correlatable information.

	**Discussion:**

	**Q:** Why not just let the AP compute the new AID and send it back? Then you simplify the computation burden on the non-AP STA side.
	**A:** That may require disclosing that you are changing the identity. The benefit in this mechanism is that the information is internal to the AP/non-AP interaction.
	**Q:** Is the AID sent in clear apart from during association?
	**A:** Yes, in trigger frames.
	**C:** There is a protected version of AID as well. In REVme and TGbh.
	**C:** We have close to 2000 AIDs. Adding a TID bitmap to Beacon Frames will make those frames large.
	**C:** A specified range on AID values increases the risk of attacks.

	**Strawpoll: Do you support AID generation mechanism as described in slide 6?**Results:
	Yes: 9, No:5, Abstain: 13, No Answer: 5
1. **Any other business**No other business.
2. **Recess 9:55 local time.**

 **3rd slot. Wednesday 18 May 2023 10:30 local time.**

1. **Meeting is called to order at 10:32 local time.**
2. **Reminder of policies and procedures (see para 1-3 above under 1st slot, or para 10).**
3. **Review of the agenda** [**11-23-0189r5**](https://mentor.ieee.org/802.11/dcn/23/11-23-0189-05-00bi-march-plenary-agenda.pptx) **(slide #18)**
	1. Agenda is approved by unanimous consent (21 online participants, 12 onsite)
4. **Technical presentations**
	1. **Obfuscation of Multiple CPE Parameters** ([11-23-0411r1](https://mentor.ieee.org/802.11/dcn/23/11-23-0411-01-00bi-obfuscation-of-multiple-cpe-parameters.pptx)), Julien Sevin (Canon)

	Proposal is to introduce a new key (SERCM key) to allow the simultaneous change of several CPE parameters, and transmit them, without having to obfuscate the parameters separately.

	**Discussion:**

	**C:** This seems to be already included in the standard. The scrambler seed should be reset and the PN should be reset to 0. When the MAC address is generated while associated the same should apply. **C:** During association we can't easily reset the sequence number to zero. At the receiver side it is used for handling BlockAck and organizing packets. For re-transmissions, we need to have SN continuity.
	**Q:** How are the changes signaled? What happens if the AP and non-AP are out of sync with respect to the number of times a change has happened?
	**A:** The changes are computed locally at the AP and non-AP using a standardized PRF. A beacon counter be used to synchronize.
	**Q:** If either AP or non-AP is not able to perform the rotation when requested by the other party, is there a final arbitrator of that decision?
	**A:** The idea is to have a new action frame to initiate the procedure.
	**C:** The non-AP will typically not know if there is an AID collision, but the AP would know. There is a risk that non-AP will be kept waiting for confirmation from the AP.
	**Q:** Would the action frame request be per-STA or could it also be issued to all STA?
	**A:** It could be either.
	**C:** AID is a difficult parameter to change, because it can only assume a limited range of values.
	**C:** If we have one SN over-the-air which is changed back to it's "real" state when received, that does not have an impact on any other procedures already in the specification.
	2. **CCMP MLO MAC rotation** ([11-23-0416r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0416-00-00bi-ccmp-mlo-mac-rotation.pptx)), Antonio de la Oliva (Interdigital, UC3M)

	Proposal is to use an association and authentication MAC (aaMAC) for CCMP encapsulation. It considers using the MLD MAC of the MLO for CCMP encapsulation while potentially randomizing all constituent MAC addresses. Using the MLD MAC as aaMAC for CCMP encapsulation does not require modifications of existing procedures. For non-MLD STA modifications are needed.

	**Discussion:**
	 **C:** The aaMAC conforms with the DS MAC we are mentioning in our requirements, and high-level it seems reasonable to target efforts at randomization of the OTA MAC.
	**Q:** In the MLO, how will SNs filter down to constituent devices?
	**A:** Filtering considerations will be considered in the next presentation.
	**C:** The key used for encapsulation will be the key associated with the aaMAC.
	**Q:** Does this imply that applying enhanced data privacy on .11be would be simple?
	**A:** Yes, I believe. But many devices will not be MLD, so we need to support both things.
	**C:** If the aaMAC is used for association, it can be sniffed during association. Even if it's later obfuscated or hidden, correlation attacks could be made on any new OTA MAC that show up afterwards.
	**A:** Will be addressed in the next presentation.
	**C:** There is more work needed on the AAD and Nonce. This seems to be the question. Should ADD and Nonce be based on OTA MAC, or should they be based on DS MAC/aaMAC?
	**C:** Supporting enhanced data privacy for legacy devices will be challenging.

	**Strawpoll:** Do you prefer
	 Option A: ADD and Nonce be based on OTA MAC (slide 4)
	 Option B: ADD and Nonce be based on DS MAC (aaMAC) (slide 6)
	 Option C: More information needed

	 Results:
	 Option A: 0, Option B: 8, Option C: 22, No Answer: 5

	**C:** I will work on option B and present the text proposals necessary in the CCMP clause of the specification.
	3. **A1 filtering for rotating MAC addresses** ([11-23-0414r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0414-00-00bi-a1-filtering-for-rotating-mac-addresses.pptx)), Antonio de la Oliva (Interdigital, UC3M)

	Proposal is to communicate new values of rotating MAC addresses to associated peers in a network by using a MIB structure to store possible over-the-air MAC addresses and the association and authentication MAC address. BlockAck Scoreboarding and A1 filtering can be achieved by comparing the seen MAC address with the members of the defined sets.

	**Discussion:**

	**Q:** The AP address is also changed here. Does that not have implications for Address 3 as well?
	**A:** The mechanism does not impose an AP (OTA) MAC address change. The mechanism allows you to preserve the aaMAC for all AP transmissions. The MAC address set allows for returning a OTA MAC to an aaMAC before performing A1 filtering and BlockAck Scoreboarding.
	**C:** The MAC addresses are not the only values that may need to change. The associated parameters may also need to be changed. In large deployments we face scalability.
	**C:** We can use tables for this. The memory requirements are low, comparatively. Other mechanisms are more complex and require hashes and calculations.
	**Chair:** We are out of time, but we will allocate some minutes to this in the beginning of our next slot.
5. **Recess at 12:31 local time.**

**4th slot. Thursday 18 May 2023, 13:30 local time.**

**20 Chair calls meeting to order at 13:31 local time.**

**21 Agenda slide deck:11-23-574r6:**

Reminder to do attendance. Reminder to register for the session and to not attend the virtual meeting without paying appropriate meeting fees.

The chair mentioned the call for essential patents

* No one responded to the call for essential patents

The chair covered the IEEE copyright and participation rules.

**Discussion of agenda 11-23-0574r6**

1. Teleconference planning
2. Discuss requirements and issues – 23/892r0

Agenda approved by unanimous consent

**22 Administration**

1. Discuss teleconference plan

C: Comment to have teleconference

C: Someone announces plans to present during teleconference

C: Chair summarize plan to have a least 2 telecons before July plenary

**23 Presentations**

1. Discuss 892r0 on requirements and issues tracking

C: Chair reviews the requirement tracking document

C: Chair reviews the issues of baseline for 11bi

C: The baseline will be included due to amendment order.

C: Whether we mandate MLD for 11bi is a different question.

C: May need to discuss what parameters needs to be changed or obfuscated is enough

Q: How to deal with the issues?

A: The document is a starting point to track them.

Q: Should we have a column to indicate the progress?

A: undecided about whether we need a date column or not.

C: Need a solution for AID.

C: May need to take into account of DMG

C: May be just about MLD and non-MLD and hopefully non-MLD does not have DMG differentiation

C: Hopefully like 11aq privacy, the sentence can be generic

C: Discussion on separate clause for 11bi or touching baseline.

C: May need to have hybrid approach and depend on the solutions

Q: Do we need in depth discussion of MLD vs non-MLD?

Q: Can we also group BPE and CPE, and inside CPE, we group the relevant discussions together?

C: comment on focusing on MLD

C: comment on for CPE if we have proposals, then maybe we focus on those

C: comment on for CPE, it means client, so it includes both MLD and non-MLD

Q: comment on are there other things beyond CCMP

C: comment on we have to consider relevant items and not just CCMP

C: Need to be careful if say privacy is just part of .11 and potential future headline

**24 Recess at 14:22 local time.**